

# On the Decisional Diffie-Hellman Problem in genus 2

Jordi Pujolàs Boix

Technical Report  
RHUL-MA-2009-13  
4 March 2009



Department of Mathematics  
Royal Holloway, University of London  
Egham, Surrey TW20 0EX, England  
<http://www.rhul.ac.uk/mathematics/techreports>

**On the Decisional Diffie-Hellman Problem  
in genus 2**

Jordi Pujolàs Boix

UNIVERSITAT POLITÈCNICA DE CATALUNYA  
Departament de Matemàtica Aplicada IV

ROYAL HOLLOWAY- UNIVERSITY OF LONDON  
Mathematics Department



**On the Decisional Diffie-Hellman Problem  
in genus 2**

Jordi Pujolàs Boix

Memòria presentada per optar  
al grau de Doctor en Matemàtiques.  
Barcelona, juliol de 2006.

Directors: Dra. Paz Morillo, Dr. Steven Galbraith



## Resum

En aquesta tesi tractem el problema Decisional de Diffie-Hellman en el grup de punts de la varietat Jacobiana de corbes supersingulars de gènere dos sobre cossos finits. La solució a aquest problema és interessant per a criptografia de clau pública, especialment en signatures digitals i en sistemes de criptografia basada en la identitat. L'existència d'un aparellament bilineal i no degenerat en aquests grups redueix la solució del problema DDH a l'existència de prou funcions de distorsió. Aquestes funcions es troben a l'anell d'endomorfismes de la varietat Jacobiana. Mostrem exemples de corbes supersingulars, sobre cossos finits de característica parell i de característica senar, tals que l'àlgebra d'endomorfismes té dimensió 16 sobre els racionals i solucionem el problema DDH en alguns d'aquests exemples.

## Abstract

We investigate the Decisional Diffie-Hellman problem in the Jacobian variety of supersingular curves of genus two over finite fields. A solution to this problem is useful in Public Key Cryptography, for example in Digital Signatures and Identity-Based Cryptography. The existence of a non-degenerate, bilinear pairing reduces the solution to DDH to the existence of sufficiently many distortion maps. These maps are found in the endomorphism ring of the Jacobian variety. We show examples of supersingular curves over finite fields of both even and odd characteristics such that the endomorphism algebra is 16-dimensional over the rationals, and we solve DDH in some cases.



## Acknowledgements

This work is the result of a collaboration between Universitat Politècnica de Catalunya and Royal Holloway– University of London set under the Socrates exchange programme of the European Union. I want to thank both my supervisors Dr. Steven Galbraith and Dra. Paz Morillo for their guidance and encouragement through this agreement. This work is indebted to the generosity of Steven Galbraith. I want to thank him for giving me the opportunity to work with him and his insight, ideas and results. I want to thank Paz Morillo and all the research group at MAK, for their generous support. I want to thank the Mathematics Department at Royal Holloway for such a nice stay in London, and the High Education Research Programme of the EU to make the exchange program happen.

I am grateful to the organizers of the Oberwolfach Seminar “Arithmetic Geometry and Public Key Cryptography” and to the organizers of the “Seminar On Geometric Methods in Cryptography” at CRM to give me the opportunity to attend those events, to Victor Rotger for some useful discussions and to Ben Smith for many interesting comments and proofreading.

Finally, I want to thank all my friends and family for their unconditional support, and I would like to dedicate this work to my parents.

Barcelona, 5 de juliol de 2006.



# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	The Decisional Diffie-Hellman Problem . . . . .	2
<b>2</b>	<b>Curves of genus two</b>	<b>5</b>
2.1	Background . . . . .	5
2.2	Hyperelliptic curves . . . . .	7
2.3	Models under extra assumptions . . . . .	8
2.4	Ramification divisor . . . . .	8
2.5	Kummer and Artin-Schreier extensions . . . . .	10
2.6	Curves of genus 2 . . . . .	11
2.7	Fields of odd characteristic . . . . .	12
2.8	Fields of even characteristic . . . . .	13
<b>3</b>	<b>Crossed-product algebras</b>	<b>19</b>
3.1	The double centralizer theorem . . . . .	19
3.2	The Brauer group . . . . .	21
3.3	Maximal subfields . . . . .	22
3.4	Self-centralizing maximal subfields . . . . .	23
3.5	Crossed-product algebras . . . . .	24
3.6	The Skolem-Noether theorem . . . . .	26
3.7	Examples . . . . .	29
<b>4</b>	<b>Algebraic groups for cryptography</b>	<b>31</b>
4.1	The ideal class group . . . . .	31
4.2	Representation in the ideal class group . . . . .	34
4.3	Cantor's algorithms . . . . .	37
4.4	The Jacobian variety . . . . .	39
4.5	Isogenies . . . . .	41
4.6	The Frobenius isogeny . . . . .	44

<b>5</b>	<b>Structure of distortion maps</b>	<b>49</b>
5.1	Endomorphisms . . . . .	49
5.2	Tate's theorem . . . . .	54
5.3	A family of supersingular curves . . . . .	58
5.4	Families of supersingular curves . . . . .	64
5.5	A non-central example in even characteristic . . . . .	69
5.6	Endomorphism algebras with zero divisors . . . . .	75
<b>6</b>	<b>The Tate pairing and DDH</b>	<b>77</b>
6.1	The Tate pairing . . . . .	77
6.2	Endomorphisms on the $l$ -torsion . . . . .	79
6.3	Distortion maps and DDH . . . . .	83
<b>A</b>	<b>Appendix</b>	<b>87</b>
	References . . . . .	93

# Chapter 1

## Introduction

The purpose of Public Key Cryptography is that anybody who knows the public key of Alice is able to send messages to her, but she is the only one able to read them. To prevent everybody else to read the messages, Alice has another key -the private key- related to her public key. To be able to read the messages, an adversary needs to solve a hard computational problem, and in practice this is not feasible without the private key. The knowledge of the private key gives Alice the only way to read the messages sent to her.

Several public key cryptographic primitives of current use today, including encryption, digital signature and key agreement, rely on hard problems from Number Theory which can be formulated in terms of a computational one way function. For example, the RSA problem takes  $n = pq$  the product of two large primes of similar size and  $e$  an integer coprime to the Euler totient function value  $\varphi(n)$ . For any given  $y \in (\mathbb{Z}/n\mathbb{Z})^*$ , to find  $x \in (\mathbb{Z}/n\mathbb{Z})^*$  such that  $x^e = y$  modulo  $n$  is hard if the factorization of  $n$  is unknown. To solve this problem, one can work out the inverse of  $e$  modulo  $\varphi(n)$ . The knowledge of the factorization of  $n$  in the two primes  $p, q$  gives a trapdoor to compute  $\varphi(n) = (p - 1)(q - 1)$  and thus provides a solution to the RSA problem.

Other interesting hard problems are related to the Discrete Logarithm Problem in a cyclic group  $\langle g \rangle$ : given  $g' \in \langle g \rangle$ , find the exponent  $e$  such that  $g' = g^e$ . This problem is believed to be hard in certain subgroups if the order of  $\langle g \rangle$  has a large prime divisor. For example, the Discrete Logarithm Problem in the multiplicative group  $\mathbb{F}_p^*$  for  $p$  a 1024-bit prime such that  $p - 1$  has a 200-bit prime factor is resistant to the techniques in use today.

A much wider range of examples of groups where the Discrete Logarithm Problem is believed to be hard is given by the subgroup of points of

elliptic curves over finite fields. The best known algorithms to solve the Discrete Logarithm Problem for general elliptic curves today have exponential complexity. Apart from the hardness of the Discrete Logarithm Problem, the groups of points of elliptic curves benefit from the theorems of Arithmetic Geometry. The rich structure of elliptic curves is extendable to other groups of divisors (up to linear equivalence) of algebraic curves over finite fields. These groups have an essential property: one knows how to represent the group elements, and also how to operate them, in an efficient way. In this document, we are interested in large prime order subgroups  $\mathbb{G}$  of the group of divisor classes on hyperelliptic curves over finite fields. In this setting, the element representation and the group law are given in terms of polynomials, and this makes divisor class groups suitable for algorithmic treatment.

Closely related to the Discrete Logarithm Problem is the family of Diffie-Hellman Problems, around which Public Key Cryptography appeared thirty years ago. The Computational Diffie-Hellman Problem is to compute the element  $g^{ab}$  from the triplet  $g, g^a, g^b$ . Assuming the Computational Diffie-Hellman Problem to be hard in  $\langle g \rangle$ , it is possible, for example, to set a key exchange protocol. Two communicating parties  $A$  and  $B$  choose private keys  $a$  and  $b$ , and they publish the elements  $g^a$  and  $g^b$  respectively. To generate a common key,  $A$  computes  $(g^b)^a$  and  $B$  computes  $(g^a)^b$ . If the Computational Diffie-Hellman Problem is hard, then an adversary with knowledge of  $g, g^a, g^b$  is not able to compute the shared key.

Other problems in the Diffie-Hellman family arise due to the rich structure of divisor class groups  $\mathbb{G}$ . Notably, in such groups there exists an efficiently computable bilinear, non-degenerate pairing  $e_l(\cdot, \cdot)$ . The Bilinear Diffie-Hellman Problem is to compute  $e_l(g, g)^{abc}$  from  $g, g^a, g^b, g^c$ . Groups where the Bilinear Diffie-Hellman Problem is hard are interesting because their structure sustains the Identity-Based Encryption Scheme [BF01]. A key step for this protocol is a pairing computation in the Encryption and Decryption algorithms. The Computational Diffie-Hellman and the Bilinear Diffie-Hellman Problems are believed to be hard in the groups of divisor classes in appropriately chosen algebraic curves. For a survey on pairings in Cryptography, see [Gag03], [Pat02], [Pat05].

## 1.1 The Decisional Diffie-Hellman Problem

The problem that motivated our work is the Decisional Diffie-Hellman Problem: given the elements  $g, g^a, g^b$  and any element  $g^c$ , decide if  $g^{ab} = g^c$  or

not. The significance of the DDH Problem in Cryptography was noticed in [Bon98].

Clearly, if one knows how to solve CDH then a solution to DDH follows. However, the assumption that the Computational Diffie-Hellman Problem is solvable does not hold for us. It is interesting to try to solve DDH without the assumption that CDH is solvable (see [JN03]). In [BLS01], a short digital signature scheme is given for groups where the assumption that CDH is hard and DDH is easy is required.

It was first noted in [Jou00] that non-degeneracy of  $e_l(\cdot, \cdot)$  is useful to solve DDH: if  $e_l(g^a, g^b)$  is not trivial, then by non-degeneracy, the equality  $e_l(g^a, g^b) = e_l(g, g^c)$  implies  $ab = c$ . A solution to DDH reduces to finding a pairing such that  $e_l(g^a, g^b) \neq 1$ .

Let  $g_1, g_2 \in \mathbb{G}$ . A distortion map for  $(g_1, g_2)$  is a group homomorphism  $\varphi$  such that  $e_l(g_1, \varphi(g_2)) \neq 1$ . The groups  $\mathbb{G}$  are typically a product of cyclic groups, and the name of distortion maps comes from the fact that they send elements from one cyclic subgroup to a different one. The notion of distortion map was introduced by Verheul [Ver04] for  $l$ -torsion subgroups of points in elliptic curves and the first examples for curves of genus two were given in [CL04] and in [DL03].

A solution to DDH in a group  $\mathbb{G}$  is in this way reduced to the existence of sufficiently many distortion maps in  $\mathbb{G}$ . Distortion maps are known to exist only in some cases. In the setting of divisor class groups of algebraic curves, distortion maps are interpreted as elements in the endomorphism ring of the Jacobian variety  $\text{Jac}(C)$ .

The elliptic curve case is rather simple. If  $D_1, D_2 \neq 0$  and  $e_l(D_1, D_2) = 1$ , then any divisor  $D_3$  which is independent of  $D_2$  (i.e.,  $\langle D_2 \rangle \cap \langle D_3 \rangle = \{0\}$ ) satisfies  $e_l(D_1, D_3) \neq 1$ . This is true because the  $l$ -torsion has rank 2. An algorithm to find distortion maps for any supersingular elliptic curve was given by Galbraith and Rotger in [GR04].

For curves of genus  $g > 1$  the  $l$ -torsion subgroup  $\text{Jac}(C)[l]$  has rank  $2g$  and so independence of points is not sufficient to imply non-triviality of their pairing. Indeed, elementary linear algebra implies that for every non-trivial divisor  $D$  of order  $l$  there is a generating set  $\{D_1, \dots, D_{2g}\}$  for  $\text{Jac}(C)[l]$  such that  $e_l(D, D_1) \neq 1$  but  $e_l(D, D_i) = 1$  for  $2 \leq i \leq 2g$ . Furthermore, the elements of  $\text{End}(\text{Jac}(C))$  may be difficult to handle as they do not necessarily correspond to maps from  $C$  to itself, and also in some cases  $\text{End}(\text{Jac}(C))$  contains zero divisors.

Our contribution is the following. In Section 6.3 we show that distortion maps always exist for supersingular curves of genus  $g > 1$ . The problem is then to construct distortion maps for given curves. We study a number

of examples and, in each case, exhibit distortion maps and prove that they are sufficient to solve DDH problems. The most important result we use is Theorem 5.2.6. We are able to exhibit enough distortion maps if the endomorphism algebra of  $\text{Jac}(C)$  is a crossed-product algebra of dimension 16 over  $\mathbb{Q}$ . In Sections 5.3 and 5.4 we show that for the examples studied, the endomorphism algebra of  $\text{Jac}(C)$  is a crossed-product algebra. In Section 5.5 we show enough distortion maps for a curve such that the endomorphism algebra of  $\text{Jac}(C)$  is not a crossed-product. We solve DDH for some cases in Section 6.3.

Before giving the new results, we recall the necessary background mathematics. We study crossed-product algebras in Chapter 3. In Chapter 2 we give a survey on curves of genus 2 over finite fields of even and odd characteristic. Our examples are in genus two but our approach should generalise to higher genera. In Chapter 4 we review the definitions and the main properties concerning  $\text{Jac}(C)$ .

## Chapter 2

# Curves of genus two

The algebraic groups we are interested in are associated to the affine coordinate rings  $\mathcal{O}_C$  of genus two curves over finite fields. In this chapter we survey the models of curves of genus two over finite fields in both even and odd characteristics. The relationship between  $\mathcal{O}_C$ , the sets of points of the Jacobian variety  $\text{Jac}(C)$  and our divisor class groups is given in Chapter 4. The main reference for this chapter is [Sti93].

### 2.1 Background

Throughout this document  $C$  is a projective, geometrically irreducible, nonsingular curve defined over a finite field  $k$ . We let  $\mathcal{O}_C(U)$  be the affine coordinate ring in an affine open subset  $U \subset C$  and we write  $k(C)$  for the function field of  $C$ . A place  $P$  in  $k(C)$  is the maximal ideal of some valuation ring  $\mathcal{O}_P$  of  $k(C)$ . By a point of degree one in  $U$  we mean a maximal ideal of the affine coordinate ring  $\mathcal{O}_C(U)$ , and we identify places and Galois-orbits of points.

We use the following equivalence. On one hand, projective nonsingular curves defined over  $k$  up to  $k$ -isomorphism, together with non-constant rational maps between them. On the other hand, function fields of transcendence degree one with field of constants  $k$ , together with field injections fixing  $k$ . For details on this equivalence we refer to [Har77, Chapter I, §6], [Sil86, page 26].

Let  $\mathcal{V}(k(C))$  denote the set of surjective valuations of  $k(C)$  that are trivial on  $k$ .

**Definition 2.1.1.** The free abelian group generated by the places  $\{P_v \mid v \in$

$\mathcal{V}(k(C))\}$  is

$$Div(k(C)) := \bigoplus_{v \in \mathcal{V}(k(C))} \mathbb{Z}P_v$$

and is called the group of divisors of  $k(C)$ .

We write  $Div(C/k) := Div(k(C)) = \bigoplus_{P \in C} \mathbb{Z}P$ . An element  $D$  in  $Div(C/k)$  is a sum  $D = \sum_{v \in \mathcal{V}(k(C))} a_P P_v$  with  $a_P \in \mathbb{Z}$ , almost all zero. The set of those  $P$  for which  $a_P \neq 0$  is called the support of  $D$ . If  $a_P \geq 0 \forall P$  in the support of  $D$ , then  $D$  is called an effective divisor. There is a natural  $\text{Gal}(\bar{k}/k)$ -action on points and divisors.

The degree of a divisor  $D$  is  $\deg(D) = \sum a_P \deg(P)$ . The map which associates every divisor with its degree is a homomorphism. We denote its kernel by  $Div^0(k(C))$ .

There is a well defined map from the nonzero functions  $\alpha \in k(C)^*$  to the group of divisors on  $C$

$$\begin{aligned} div: k(C)^* &\longrightarrow Div(k(C)) \\ \alpha &\longmapsto div(\alpha) := \sum_{v \in \mathcal{V}(k(C))} v_P(\alpha) P_v \end{aligned}$$

where  $v_P(\alpha)$  is the order of the pole or the order of vanishing of  $\alpha$  at  $P_v$ . The divisors in the image of  $div$  are called principal divisors and form a subgroup of  $Div(C/k)$ .

For any nonzero function  $\alpha \in k(C)^*$  of a curve  $C$  over any field  $k$ , the number of poles equals the number of zeros and in particular  $\deg(div(\alpha)) = 0$  for all  $\alpha$ . The principal divisors form a subgroup in  $Div^0(k(C))$ .

The quotient of the group  $Div(C/k)$  by the subgroup of principal divisors is called the Picard group of the curve  $C/k$ . However, we consider only the divisors of degree zero.

**Definition 2.1.2.** The degree zero divisor class group  $Pic^0(k(C))$  is the quotient of the group  $Div^0(k(C))$  by the image of the map  $div$ .

Given an effective divisor  $D$ , one can give the set of divisors a partial order:  $D' \geq D$  if and only if  $D' - D$  is effective. With this ordering, one considers, for any divisor  $D$ , the  $k$ -vector space

$$\mathcal{L}(D) := \{\alpha \in k(C)^* \mid div(\alpha) + D \geq 0\} \cup \{0\}$$

and we write  $\ell(D) := \dim_k(\mathcal{L}(D))$ .

**Theorem 2.1.3** (Riemann-Roch). *Let  $C$  be a curve over  $k$ . There exists a divisor  $K \in \text{Div}(k(C))$  and a non-negative integer  $g$  such that, for all  $D \in \text{Div}(k(C))$ ,*

$$\ell(D) = \deg(D) + 1 - g + \ell(K - D).$$

The integer  $g$  in the Riemann-Roch Theorem is called the genus of the curve  $C$ . For us  $C$  denotes a curve of genus 2. The divisor  $K$  is unique up to principal divisors, and any such  $K$  is called a canonical divisor of  $C$ . With the Riemann-Roch Theorem one proves the following crucial result (see [Lor96] for a proof).

**Theorem 2.1.4.** *Let  $k$  be a finite field. Let  $C$  be a curve over  $k$ . Then the group  $\text{Pic}^0(C/k)$  is finite.*

When  $k$  is a finite field, the order of  $\text{Pic}^0(C/k)$  is called the *class number* of  $C/k$ .

## 2.2 Hyperelliptic curves

Hyperelliptic curves are, by definition, those curves that admit a morphism  $\pi$  of degree 2 to the projective line. The algebraic description of this is an extension of fields  $k(C)/k(\mathbb{P}^1)$  of degree 2. As  $k$  is perfect and our curves have genus 2, this extension is separable [Sti93, III.9.2]. It is a normal extension because the degree is 2. Hence it is Galois.

The geometric object corresponding to the nontrivial element of the Galois group  $\text{Gal}(k(C)/k(\mathbb{P}^1)) = \{id, \iota^*\}$  is an involution  $\iota$  of  $C$  called the *hyperelliptic involution*. This involution matches any point  $P \in C(\bar{k})$  with the other point  $P^\iota$  having the same image under the morphism of degree 2,  $\pi(P) = \pi(P^\iota)$ .

The fixed points of  $\iota$  are “repeated” under the  $2 : 1$  morphism  $\pi$ . These points are *ramification points* of  $\pi$  and the set of all of them (counting multiplicities) forms a divisor  $D$  called *ramification divisor*.

One can prove that  $\iota$  is independent of  $\pi$ . This particular fact makes hyperelliptic curves special. It forces  $D$  to be the same for all possible  $\pi$ 's. Indeed,  $D$  coincides with an “intrinsic” set, that is, a set which is defined without mentioning  $\pi$  at all: the set of Weierstrass points  $W := \{P \in C \mid \ell(2P) = 2\}$ . Every hyperelliptic curve has one intrinsic structure for  $D = W$ , and these sets are well known for hyperelliptic curves. A recent description of Weierstrass points of generic curves of any genus can be found in [GKR05].

### 2.3 Models under extra assumptions

In this paragraph we recall the equations of hyperelliptic curves obtained under a certain assumption. However, we are going to work without such extra assumptions, and these special models are not going to be essential for us. We will see how to obtain an equation for any hyperelliptic curve of genus 2 in the next paragraphs.

One obtains equations working with the function fields  $k(C)/k(\mathbb{P}^1)$ . The field  $k(\mathbb{P}^1)$  is identified with  $k(x)$  by fixing a point in  $\mathbb{P}^1(k)$  and calling it infinity. This identifies our quadratic extension with  $k(C)/k(x)$ . From now,  $x$  is the function giving the first coordinate of a point  $P \in C$ .

The Riemann-Roch Theorem is useful to find models for hyperelliptic curves of any genus if one makes the extra assumption for such a curve to have a Weierstrass point  $P_\infty$  defined over  $k$ . Under this assumption, the Riemann-Roch Theorem shows the existence of another function  $y \in k(C)$  such that there is a relation of the type  $y^2 + h(x)y = f(x)$  with  $\deg h(x) \leq g$  and  $\deg f(x) = 2g + 1$ .

The way to deduce this relation is as follows. As  $\text{ord}_{P_\infty}(x) = -2$ , then by Riemann-Roch  $\ell((2g + 1)P_\infty) = g + 2$ . As  $\{1, x, \dots, x^g\}$  is the maximal set of powers of  $x$  having a pole of order less or equal to  $2g + 1$  at  $P_\infty$ , there must be another  $y \in k(C)$  linearly independent to  $1, x, \dots, x^g$  in the vector space  $\mathcal{L}((2g + 1)P_\infty)$ . This implies that the whole set of  $3g + 4$  functions  $\{1, x, \dots, x^{2g+1}, y, yx, \dots, yx^g, y^2\}$  are in  $\mathcal{L}((4g + 2)P_\infty)$ , while Riemann-Roch tells this is a  $3g + 3$ -dimensional space. Hence a linear combination between the above functions exists, and the claimed relation follows.

To find models in full generality one needs more tools. The key character is the ramification divisor  $D$ . We will next survey the algebraic description of  $D$ . This is purely in terms of extensions of function fields. The algebraic counterpart of  $D$  is the different of the extension  $k(C)/k(\mathbb{P}^1)$ . We follow [Sti93].

### 2.4 Ramification divisor

We need some concepts from the general theory of algebraic extensions  $F'/F$  of function fields with the same field of constants  $k$ .

Call  $\mathbb{P}_F$  the set of places of  $F$ . A place  $P' \in \mathbb{P}_{F'}$  is said to lie above a place  $P \in \mathbb{P}_F$  if  $P \subseteq P'$ . Usually  $P'$  is called an extension of  $P$  and one writes  $P'|P$ .

**Definition 2.4.1.** For any  $P'|P$ , there exists a positive integer  $e(P'|P)$

such that  $v_{P'}(x) = e \cdot v_P(x)$  for every  $x \in F$ .  $e(P'|P)$  is the ramification index of  $P'$  above  $P$ . One calls  $P'|P$  ramified if  $e(P'|P) > 1$  and unramified otherwise. If in addition  $\text{char}(k) \mid e(P'|P)$ , one says the ramification is wild.

**Remark 2.4.2.** One has the well known formula  $[F' : F] = \sum_{P'|P} e(P'|P) \deg(P')$ . From this formula it is clear that for quadratic extensions  $F'/F$ , there is just one  $P'$  above any ramified place  $P$ . One then says that  $P$  is totally ramified in  $F'/F$ . This is precisely the case for hyperelliptic curves as then our extension  $k(C)/k(\mathbb{P}^1)$  is quadratic. Hence, for hyperelliptic curves the ramification places  $P'|P$  are totally ramified in  $k(C)/k(\mathbb{P}^1)$ . We have  $e(P'|P) = [k(C) : k(\mathbb{P}^1)] = 2$  in every ramification place  $P'|P$ .

**Definition 2.4.3.** For any place  $P \in \mathbb{P}_F$ ,  $\mathcal{O}'_P$  denotes the integral closure of  $\mathcal{O}_P$  in  $F'$ . The set

$$\mathcal{C}_P := \{z \in F' \mid \text{Tr}_{F'/F}(z \cdot \mathcal{O}'_P) \subseteq \mathcal{O}_P\}$$

is called the complementary module over  $\mathcal{O}_P$ .

**Proposition 2.4.4.** *With the notation above,*

- (a)  $\mathcal{C}_P$  is a  $\mathcal{O}'_P$ -module and  $\mathcal{O}'_P \subseteq \mathcal{C}_P$ .
- (b) There exists an element  $t \in F'$  (depending on  $P$ ) such that  $\mathcal{C}_P = t \cdot \mathcal{O}'_P$ . Moreover,  $v_{P'}(t) \leq 0$  for all  $P'|P$ .
- (c)  $\mathcal{C}_P = \mathcal{O}'_P$  for almost all  $P$ .

*Proof.* [Sti93, III.3.8] □

**Definition 2.4.5.** Let  $\mathcal{C}_P = t \cdot \mathcal{O}'_P$  the complementary module over  $\mathcal{O}_P$ . Then, the different exponent of  $P'$  over  $P$  is  $d(P'|P) = -v_{P'}(t)$ .

Clearly  $d(P'|P) \geq 0$  and it is 0 for almost every  $P$  and  $P'|P$ .

**Definition 2.4.6.** The divisor in  $F'$  given by

$$\text{Diff}(F'/F) = \sum_{P \in \mathbb{P}_F} \left( \sum_{P'|P} d(P'|P) P' \right)$$

is called the *different* or *ramification divisor* of the extension  $F'/F$ .

The coefficients  $d(P'|P)$  are called *the exponents of the different* and they are described in terms of the ramification indexes  $e(P'|P)$ .

**Theorem 2.4.7.** (*Dedekind's Different Theorem*) For all  $P'|P$  then

$$(a) \ d(P'|P) \geq e(P'|P) - 1.$$

$$(b) \ d(P'|P) = e(P'|P) - 1 \text{ if and only if } e(P'|P) \text{ is not divisible by } \text{char}(k).$$

*Proof.* [Sti93, III.5.1] □

In case (b) one says that the ramification is tame. Wild ramification happens thus when the different exponents are just (strictly) bounded from below.

The following powerful result, which we just reproduce for function field extensions with the same fields of constants, tells more about the different exponents, and allows to deal with the wild case:

**Theorem 2.4.8.** (*Hurwitz Genus Formula*) Let  $F'/F$  be a finite separable extension of function fields of genus  $g'$  and  $g$  respectively. Then  $2g' - 2 = [F' : F](2g - 2) + \deg(\text{Diff}(F'/F))$ .

*Proof.* [Sti93, III.4.12] □

## 2.5 Kummer and Artin-Schreier extensions

In order to give models of hyperelliptic curves one describes the generators of the extension  $k(\mathbb{C})/k(x)$ . The results in this section are due to Hasse [Has34]. He showed that cyclic Galois extensions of  $k(x)$  of any degree  $n$ , for fields  $k$  containing the  $n$ -th roots of 1, do admit a generator satisfying a relation of the type  $y^n = u(x)$  for certain  $u(x) \in k(x)$  defined up to multiplication by elements of the form  $g(x)^n$ ,  $g(x) \in k(x)^*$ . This particular definition of  $u(x)$  is because a change like

$$u(x) \leftrightarrow u(x)g(x)^n \tag{2.5.1}$$

can be seen just as a change of generator  $y \leftrightarrow yg(x)$ . Moreover, as we will see a few lines below,  $u(x)$  is linked to  $\text{Diff}(k(\mathbb{C})/k(\mathbb{P}^1))$ . These are called Kummer extensions.

If  $k$  does not contain  $n$ th-roots of 1 (that is, if  $\gcd(\text{char}(k) - 1, n) = 1$ ), no such simple equation is available. Hasse showed that in this case such extensions do always admit a generator  $y$  satisfying  $y^p - y = u(x)$  for certain  $u(x) \in k(x)$  related to  $\text{Diff}(k(\mathbb{C})/k(\mathbb{P}^1))$ . Now a change of generator  $y \leftrightarrow y + g(x)$  implies a change

$$u(x) \leftrightarrow u(x) + g(x)^p - g(x) \tag{2.5.2}$$

In general, for any field  $F$  of characteristic  $p$ , the set  $AS(F) := \{f^p - f, f \in F\}$  is a subgroup of  $F$  called the Artin-Schreier subgroup of  $F$ . Note that if  $u(x) \in AS(k(x))$  then  $y^p - y = u(x)$  is a trivial extension. Hence, for nontrivial extensions one can think  $u(x) \in k(x) \setminus AS(k(x))$ , and  $u(x)$  to be defined up to addition of elements in  $AS(k(x))$ . These are called Artin-Schreier extensions. For a review of both types, see [Sti93].

The precise link between  $u(x)$  and  $\text{Diff}(k(\mathbb{C})/k(x))$  for tame ramification is obtained by making Dedekind's Different Theorem explicit for Kummer extensions. One obtains  $d(P'|P) = n/\text{gcd}(n, v_P(u(x))) - 1$  (recall that  $u(x)$  is free of  $n$ th-powers) [Sti93, III.7.3]. Taking advantage of the transformations (2.5.1), which leave the extensions unchanged, one easily removes all poles from  $u(x)$  until a  $n$ -th power free polynomial is obtained.

If the ramification is wild, using transformations (2.5.2), one can remove the poles of order  $p$ . One proves that  $d(P'|P) = 1 + m_P$ , where  $m_P$  is the order of the remaining poles of  $u(x)$  at  $P$  (so  $m_P$  is coprime with  $p$ ) [Sti93, III.7.8].

In both cases, with the Hurwitz genus formula it is easy to bound the degree of  $\text{Diff}(k(\mathbb{C})/k(\mathbb{P}^1))$  in terms of the genus of the curve  $C$ . This gives just finitely many options for  $u(x)$  and gives the model for  $C$ . We will see an example of this in the next paragraph, just for curves of genus 2.

Note that because of the  $2 : 1$  morphism, we are only interested in extensions of degree two. Hyperelliptic curves of any genus have essentially two types of models:  $y^2 = u(x)$  for fields of characteristic different to 2, and  $y^2 + y = u(x)$  for fields of characteristic equal to 2. Whatever the case, these equations provide a description of the  $2 : 1$  morphism. Indeed, for a given  $x$ , the two preimages  $P_1, P_2 \in C$  are given by  $(x, y)$  where  $y$  is any of the two solutions of the quadratic equations above. The hyperelliptic involution  $\iota$  permutes  $P_1$  and  $P_2$ .

## 2.6 Curves of genus 2

Every genus 2 curve  $C$  is hyperelliptic. This is because Riemann-Roch Theorem implies that any canonical divisor  $K$  has degree 2 and also  $\ell(K) = 2$ . As the complete linear system  $|K|$  has no base points, it follows that the canonical morphism

$$\pi = \pi_K : C \longrightarrow \mathbb{P}^1$$

has degree 2 [Har77].

Another straight Riemann-Roch argument valid in every characteristic produces, for any genus 2 curve  $C$  (and just for genus 2!), a model

$y^2 + h(x)y = f(x)$  with  $\deg h(x) \leq 3$  and  $\deg f(x) = 6$ . This is similar to the previous argument in which the curve was assumed to have a  $k$ -rational point. Take now the canonical divisor  $K$  of  $C$  instead. By Riemann-Roch,  $K$  has degree 2 and  $\ell(K) = 2$ . As  $K$  is defined over  $k$  [Har77], there is a function  $X$  defined over  $k$  such that  $1, X, \dots, X^3$  are in  $\mathcal{L}(3K)$ . But  $\ell(3K) = 5$ . Hence there is another function  $Y$  defined over  $k$  in  $\mathcal{L}(3K)$ . But then  $1, X, \dots, X^6, Y, YX, \dots, YX^3, Y^2$  are all in  $\mathcal{L}(6K)$  and they form a 11-dimensional space by Riemann-Roch. Hence a linear combination between these functions has to exist.

For a description of the models of curves of genus 2 in full generality, one specialises the results for hyperelliptic curves to genus 2. Over an algebraically closed field, this was done in [Igu60]. We need a similar description for non algebraically closed fields.

By the Hurwitz genus formula, the degree of the ramification divisor of any curve  $C$  of genus two is equal to 6. The Galois structure of possible ramification divisors of genus 2 curves is restricted to Galois subsets of six ramification points in the curve.

## 2.7 Fields of odd characteristic

By the theory of Kummer extensions,  $k(C)/k(x)$  has always a generator  $y \in k(C)$  satisfying  $y^2 = f(x)$  for a certain squarefree  $f(x) \in k(x)$ . One can always choose  $f(x) \in k[x]$  of degree 5 or 6. As  $\text{char}(k) \neq 2$ , the ramification is tame. Thus, the different exponents are all equal to 1 by Dedekind's Different Theorem. This implies that there are always six different points in the support of  $D$ , not necessarily defined over  $k$ . For instance, there could be no point over  $k$ , but after an extension of  $k$  of degree 2, 3, 4, 5 or 6, six different points would appear. The support of  $D$  is organized in Galois orbits according to the irreducible factors of  $f(x)$ .

With the description of the  $2 : 1$  morphism given above, the zeros of  $f(x)$  provide the  $x$ -coordinates of the points in the support of  $D$ . For  $\deg f(x) = 5$ , the point at infinity is also in  $D$ .

Note that the projective closure of the affine curve given by this plane model is always singular at  $[0, 1, 0]$ . To get rid of this singularity and obtain what we called a curve, we use the nonsingular model in  $\mathbb{P}^4$  described in the first pages of [CF96]. We briefly recall this model. Suppose  $f(x) = a_6x^6 + \dots + a_1x + a_0$  with  $a_i \in k$ . Then the (projective, smooth, geometrically irreducible) curve  $C$  associated to  $f$  is given by the zeros of the following set

of homogeneous polynomials:

$$\begin{cases} Y^2 - a_6 X_3^2 - a_5 X_2 X_3 - a_4 X_2^2 - a_3 X_1 X_2 - a_2 X_1^2 - a_1 X_0 X_1 - a_0 X_0^2 = 0 \\ X_0 X_2 - X_1^2 = 0 \\ X_0 X_3 - X_1 X_2 = 0 \\ X_1 X_3 - X_2^2 = 0 \end{cases}$$

One recovers the singular plane model in the  $X_0 \neq 0$  hyperplane setting  $Y = y$ ,  $X_i = x^i$ ,  $i = 0, 1, 2, 3$ . It is immediate that  $[0, 0, 0, 1, \pm\sqrt{a_6}]$  maps to the singular point  $[0, 1, 0]$  in the plane model. Hence, if  $\deg f(x) = 6$  there are two different points above  $[0, 1, 0]$  which are defined over a quadratic extension of  $k$ . If  $\deg f(x) = 5$  there is just one -then necessarily Weierstrass-point above  $[0, 1, 0]$  defined over  $k$ .

In the next chapters we consider the affine coordinate rings in affine, dense open sets  $U \subset \mathbb{C}$  of these curves. One example is the polynomial ring  $k[X_0, X_1, X_2, X_3, Y]$  modulo the ideal generated by the polynomials above. It is well known that the affine coordinate rings of nonsingular curves are Dedekind domains. We denote them by  $\mathcal{O}_{C_f}(U)$  or simply  $\mathcal{O}_{C_f}$ .

## 2.8 Fields of even characteristic

Any nontrivial Artin-Schreier extension  $k(\mathbb{C})/k(x)$  admits a generator  $y \in k(\mathbb{C})$  satisfying  $y^2 + y = u(x)$  for a certain  $u(x) \in k(x) \setminus AS(k(x))$  determined up to addition of elements in  $AS(k(x))$  (see Section 2.5).

Taking advantage of the fact that the left hand side is of the form  $y^2 + y$ , one can always choose  $u(x)$  without poles of even order. As  $\text{char}(k) = 2$ , the ramification is wild. Hence the different exponents are odd and satisfy  $d(P'|P) > 1$  in all ramified places by Dedekind's Different Theorem. Recall that for the unramified points one has  $m_P = -1$  by definition. We will now enumerate the possibilities for a divisor of degree six with such specific coefficients. Note that the degree of a divisor depends on the degree of the places in its support. Recall Hurwitz formula for genus two implies

$$6 = \sum_{P \in k(\mathbb{P}^1)} \left( \sum_{P'|P} (m_{P'} + 1) \deg P' \right)$$

From this formula, there are just a few possibilities for the structure of the ramification divisor.

In Table 2.1 below, all the possible structures of the ramification divisor are displayed. The first column are just names. The others describe the

Case name	$\text{Diff}(k(C)/k(x))$	Degrees and exponents
(1, 1, 1) simple	$2P'_1 + 2P'_2 + 2P'_3$	$\deg P'_1 = \deg P'_2 = \deg P'_3 = 1$ $m_{P'_1} = m_{P'_2} = m_{P'_3} = 1$
(1, 1, 1) quadratic	$2P'_1 + 2P'_2$	$\deg P'_1 = 1, \deg P'_2 = 2$ $m_{P'_1} = 1, m_{P'_2} = 1$
(1, 1, 1) cubic	$2P'$	$\deg P' = 3$ $m_{P'} = 1$
(1, 3)	$2P'_1 + 4P'_2$	$\deg P'_1 = \deg P'_2 = 1$ $m_{P'_1} = 1, m_{P'_2} = 3$
(5)	$6P'$	$\deg P' = 1$ $m_{P'} = 5$

Table 2.1: The possible structures of the Ramification Divisor for curves of genus two over fields of even characteristic.

support, the degree and the coefficients of each point in terms of the different exponent.

**Remark 2.8.1.** The cases (1, 1, 1) quadratic and cubic become (1, 1, 1) simple after a quadratic/cubic extension of the base field  $k$ .

One is tempted to write down  $u(x)$ 's in Laurent Series whose divisor of poles is like the ones in Table 2.1. The resulting equation  $y^2 + y = u(x)$  defines then a function field which is of the Artin-Schreier type. These Artin-Schreier models then obviously ramify according to each prescription. One can try to build up models that realize each of the ramification structures above.

Note that an Artin-Schreier model does not define an affine curve because

$u(x)$  is not a polynomial. Despite of this, away from the poles of  $u(x)$  one obtains a nonsingular object in two variables. In all cases, the polynomials obtained from these Artin-Schreier models after clearing denominators have singularities. The projective closure of this nonaffine object is a curve with singularities, for which there is nonsingular model.

The genus of the nonsingular curve obtained after desingularization is given in terms of the poles of odd order of  $u(x)$  and the Hurwitz formula 2.4.8, and it is equal to 2. So for each of these Artin-Schreier models, there is a curve of genus 2 which we call  $C_{u(x)}$ . This curve has a model in  $\mathbb{P}^4$  very similar to the one in Section 2.7.

However, it could still happen that many of the  $u(x)$ 's we wrote down gave rise to  $k$ -isomorphic curves  $C_{u(x)}$ . This actually is the case and depends on the structure of  $k$  and, in particular, of the Artin-Schreier subgroup  $AS(k)$  of  $k$ . Recall that this is the group of elements in  $k$  of the form  $AS(k) := \{\kappa^2 + \kappa \mid \kappa \in k\}$ .

**Theorem 2.8.2.** *Two hyperelliptic curves  $C_{u(x)}$ ,  $C_{u'(x)}$  are  $k$ -isomorphic if and only if*

$$u'(x) \cong u(\gamma(x)) \text{ mod } AS(k(x))$$

for some  $\gamma \in PGL_2(k)$ .

*Proof.* We noted in Section 2.5 that  $u(x)$  and  $u'(x)$  define the same extension  $y^2 + y = u(x)$  if they belong to the same class modulo  $AS(k(x))$ . Further, if one changes  $x$  by  $\gamma(x)$  for some  $\gamma \in \text{Aut}_k(\mathbb{P}^1) \cong PGL_2(k)$  then  $k(x) \cong k(\gamma(x))$ , and one obtains an isomorphic field extension. So the curves are isomorphic. If two hyperelliptic curves are isomorphic then the field extensions  $k(C_{u(x)})/k(x)$ ,  $k(C_{u'(x)})/k(x)$  are isomorphic. The two degree 2 morphisms to  $\mathbb{P}^1$  differ by an element  $\gamma \in \text{Aut}_k(\mathbb{P}^1)$ . Hence  $x' = \gamma(x)$  and necessarily  $u'(x) \cong u(\gamma(x)) \text{ mod } AS(k(x))$ .  $\square$

The classification of the rational functions  $u(x)$  under the double action of  $PGL_2(k)$  and  $AS(k(x))$ , and hence the classification of the curves  $C_u$  modulo  $k$ -isomorphism, is shown in [CNP05]. The complete, faithful list of Artin-Schreier models is given in Table 2.2 below.

The study of the above models for the case (5) was carried out thoroughly in [GV92a], [GV92b] for  $k$  a finite field of characteristic 2. For the remaining four cases, the classification into  $k$ -isomorphism classes and the determination of the number of such  $k$ -isomorphism classes over finite fields of characteristic 2 was obtained in [Puj02]. This work later appeared in [Hur03] and in [CNP05].

Case name	$u(x)$ in $y^2 + y = u(x)$	Parameter conditions
(1, 1, 1) simple	$ax + b/x + c/(x + 1) + d$	$abc \neq 0, d \in k/AS(k)$
(1, 1, 1) quadratic	$ax + (bx + c)/(x^2 + x + u) + d$	$a \neq 0, (b, c) \neq (0, 0),$ $d \in k/AS(k), u \notin AS(k)$
(1, 1, 1) cubic	$(ax^2 + bx + c)/(x^3 + ux + u) + d$	$(a, b, c) \neq (0, 0, 0),$ $d \in k/AS(k), u \neq 0$ such that $x^3 + ux + u$ is irreducible in $k[x]$
(1, 3)	$ax^3 + bx + c/x + d$	$ac \neq 0, d \in k/AS(k)$
(5)	$ax^5 + bx^3 + cx^2 + d$	$a \neq 0, d \in k/AS(k)$

Table 2.2: Complete, faithful list of Artin-Schreier models realizing each of the ramification divisor structures in Table 2.1.

We are going to use the nonsingular models above in the next chapters. As before, for a given affine open set  $U \subset \mathbb{C}$ , we call  $\mathcal{O}_{C_u}(U)$  the affine coordinate ring associated to  $U$ .



## Chapter 3

# Crossed-product algebras

In this chapter we give a survey on crossed-product algebras, splitting fields and the Brauer group. These are subjects with a long history. Crossed-product algebras can be found in the works of Albert [Alb39], and also in [Her68], [Wei67] and many others. Our main reference is [Rei75]. This chapter consists of an extract of some results in [Rei75] which turned necessary for this dissertation.

We will show in Chapter 5 that in some cases, the endomorphism algebras of the Jacobian variety of some curves in Chapter 2 are crossed-product algebras.

As we pointed out in the Introduction, we will find our distortion maps among the endomorphisms of the Jacobian variety of genus two curves. Hence the understanding of crossed-product algebras is relevant for our interests. On the other hand, we will see in Chapter 6 that our main tool to solve the Decisional Diffie-Hellman Problem – the Tate pairing – is closely related to the Brauer Group.

### 3.1 The double centralizer theorem

We assume that all rings are semisimple, left Artinian, Noetherian, with unity and associative, but not necessarily commutative. Recall that a  $k$ -algebra  $A$  is a ring provided with an additional structure of  $k$ -vector space

$$k(aa') = (ka)a' = a(ka')$$

so that the elements of  $k$  do commute with any element in the  $k$ -algebra. For us,  $A$  will always be finite dimensional over  $k$ .

Along with any  $k$ -algebra  $A$  there is a twin  $k$ -algebra  $A^{opp}$  called the opposite algebra of  $A$ . It is defined from  $A$  in the following way: if  $(x, y) \mapsto xy$  is the product in  $A$ , then  $(x, y) \mapsto yx$  is the product in  $A^{opp}$ .

$A$  is called simple if the only bilateral ideals of  $A$  are  $A$  and  $(0)$ . A (non commutative)  $k$ -algebra in which every nonzero element is invertible is called division  $k$ -algebra or skewfield. We will denote skewfields by  $D$ . The theorem upon which all the following relies is the Wedderburn Structure Theorem for (left artinian) simple rings. We state the following version:

**Theorem 3.1.1** (Wedderburn). *Every simple ring  $A$  is isomorphic to an algebra  $M_n(D)$  of  $n \times n$  matrices over a division algebra  $D$ . The ring  $A$  determines  $n$  uniquely and determines  $D$  up to isomorphism.*

The center of a  $k$ -algebra  $A$  is defined as

$$Z(A) := \{x \in A \mid xa = ax \forall a \in A\}$$

We mentioned above that  $k$  lies in the center of any  $k$ -algebra. If exactly  $k = Z(A)$  one calls  $A$  a central  $k$ -algebra. Since our algebras are finite dimensional and artinian, it is true that tensor products of central simple algebras are again central simple.

**Definition 3.1.2.** For any simple subring  $B$  of a central simple  $k$ -algebra  $A$ , the centralizer of  $B$  in  $A$  is

$$B' = \{x \in A \mid xb = bx \forall b \in B\}.$$

Centralizers are important for the structure of the endomorphism algebras that we will find in Chapter 5. A fundamental result on centralizers is given by the following version of the Double Centralizer Theorem.

**Theorem 3.1.3.** *Let  $B$  be a simple subring of a central simple  $k$ -algebra  $A$ . Then the centralizer  $B'$  of  $B$  in  $A$  is a simple ring and  $B$  is its centralizer in  $A$ .*

*Proof.* [Rei75, Theorem (7.11)]. □

We will not proceed without sketching some of the ideas behind this theorem. Note first that any  $A$ -module  $V$  is a  $k$ -vector space. By  $\text{Hom}_A(V, V)$  we mean the  $A$ -module formed by the homomorphisms from  $V$  to itself. A (left)  $A$ -module  $V$  is called faithful if its annihilator ideal is trivial or, equivalently if  $A \hookrightarrow \text{Hom}_k(V, V)$ . Hence, if  $A$  is simple, then any non-trivial (left)  $A$ -module  $V$  is faithful. Faithful modules are notable because of the

fundamental double centralizer property. This is a property which holds in a very general situation and states that if  $V$  is a finitely generated, faithful module over an artinian semisimple ring  $A$  then  $A \cong \text{Hom}_D(V, V)$  with  $D = \text{Hom}_A(V, V)$ . On the other hand, if  $V$  is a simple  $A$ -module then  $\text{Hom}_A(V, V)$  is a skewfield with center  $k$  – this is Schur’s Lemma. Further, it is shown that  $V$  can be provided with a structure of a module over a certain ring  $S$  which is isomorphic to  $D \otimes_k B$ . Then it is shown that  $B' = \text{Hom}_S(V, V)$  and the simplicity of  $B'$  follows. Next, the double centralizer property holds for  $S$  and  $V$  and states  $S = \text{Hom}_{B'}(V, V)$ . From this, every element in  $B'$  can be embedded in  $S$  and centralizes  $D \otimes 1$  in  $S$ . But then it must be contained in  $Z(D) \otimes_k B = k \otimes_k B \cong B$ .

An accurate account of the ranks involved gives the following corollary.

**Corollary 3.1.4.** *Let  $V$  be a simple left  $A$ -module and  $D = \text{Hom}_A(V, V)$ . Then  $D \otimes_k B \cong \text{Hom}_{B'}(V, V)$  and  $[B : k][B' : k] = [A : k]$ .*

*Proof.* [Rei75, Corollary (7.13)] □

At a certain point we will need also the following.

**Corollary 3.1.5.**

$$A \otimes_k B^{\text{opp}} \cong M_r(B')$$

where  $r = [B : k]$ .

*Proof.* [Rei75, Corollary (7.14)] □

## 3.2 The Brauer group

We recall now the definition of the Brauer group. Wedderburn’s Theorem motivates the following equivalence relation: two central, simple  $k$ -algebras  $A, A'$  are called similar if there exist two integers  $m, m'$  such that  $A \otimes_k M_m(k) \cong A' \otimes_k M_{m'}(k)$ . Taking the set of equivalence classes  $[A]$  by this relation one obtains the Brauer group:

**Theorem 3.2.1.** *The classes of central simple  $k$ -algebras form an abelian group  $Br(k)$  called the Brauer group of  $k$ . The group operation is given by  $[A][A'] = [A \otimes_k A']$ , the inverse of the class  $[A]$  is the class of the opposite algebra  $[A^{\text{opp}}]$  and the identity is given by  $[k]$ .*

It is interesting to consider the Brauer group of algebraic extensions  $k'$  of  $k$ . As  $A \otimes_k k'$  is a  $k'$ -algebra, there is a well defined map

$$\begin{aligned} \text{res}_{k'/k} : Br(k) &\longrightarrow Br(k') \\ [A] &\longmapsto [A \otimes_k k'] \end{aligned}$$

which is a homomorphism of groups.

**Definition 3.2.2.** A field extension  $L$  of  $k$  is called a splitting field for a  $k$ -algebra  $A$  if  $[A] \in \ker(\text{res}_{L/k})$ .

**Remark 3.2.3.** One calls  $\ker(\text{res}_{L/k})$  the relative Brauer group with respect to  $L/k$ . It is common to write  $Br(L/k)$  for  $\ker(\text{res}_{L/k})$ .

It is a consequence of Wedderburn's Theorem that  $L$  splits  $A$  if and only if  $L$  splits the corresponding skewfield  $D$ . For example, any algebraic closure of  $k$  is a splitting field for  $A$ . But one can give a better description of the necessary and sufficient conditions for a field to be a splitting field. We next continue following [Rei75] to see how splitting fields are related to centralizers.

### 3.3 Maximal subfields

The first step is to show that maximal fields inside a skewfield  $D$  - we call such fields  $F$  from now on - are splitting fields for  $D$ . In principle,  $D$  may not necessarily contain subfields at all apart from  $k$ . However, if one requires  $[D : k]$  to be finite, then it is shown that one can always build one separable, nontrivial extension  $E/k$  inside  $D$ . Using the Double Centralizer Theorem 3.1.3 for  $E$  one proves then the existence of a maximal separable subfield  $F/k$  inside  $D$  by induction. We do not reproduce this construction [Rei75, pages 97 & 98].

The fact that  $D$  contains  $F$ , provides  $D$  with a natural structure as an  $F$  vector space. Write  $r = [D : F]$  for the rank of  $D$  as an  $F$ -vector space. A very particular relation between the dimensions  $[D : F]$  and  $[F : k]$  is to be noticed. Namely, maximality for  $F$  is a strong assumption and implies that  $F'$  must equal  $F$ . This is because any simple field extension  $F(x)$ , for  $x \in F'$ , is a subfield of  $D$  containing  $F$ . On the other hand, Corollary 3.1.4 with  $A = D$ ,  $B = F$  and  $V = D$  as a (left)  $D$ -module states  $D \otimes_k F \cong \text{Hom}_F(D, D)$  and  $[F : k]^2 = [D : k]$ . But  $\text{Hom}_F(D, D)$  is trivially isomorphic to  $M_r(F)$ . Hence, as  $r^2 = [D \otimes_k F : F] = [D : k] = [F : k]^2$ , then necessarily  $r = [F : k]$  as well. All together is stated in the following theorem.

**Theorem 3.3.1.** *Let  $D$  be a skewfield with center  $k$ , and let  $[D : k]$  be finite.*

- (i) Every maximal subfield  $F$  of  $D$  contains  $k$ , and is a splitting field for  $D$ . Further, if  $m = [F : k]$ , then

$$[D : k] = m^2, \quad F \otimes_k D \cong M_m(F).$$

- (ii) There exists a maximal subfield  $F$  of  $D$  which is separable over  $k$ .

*Proof.* [Rei75, Theorem (7.15)]. □

By Theorem 3.3.1 above, it makes sense to define the index of a skewfield  $D$  with center  $k$  and  $k$ -rank  $[D : k]$  to be the integer  $m := \sqrt{[D : k]}$ .

### 3.4 Self-centralizing maximal subfields

The next step is to study splitting fields for  $D$  that are not maximal subfields of  $D$ . Take now  $E$  any splitting field for  $D$ , so that the central simple  $E$ -algebra  $S := D \otimes_k E$  is isomorphic to a matrix algebra of a certain size over  $E$ . Note, though, that  $[S : k] = [D : k][E : k] = m^2[E : k]$ . This implies that for any  $E$ , the size of the split  $D$  must be  $m$ :  $S = D \otimes_k E \cong M_m(E)$ .

We will next see that splitting fields cannot have smaller degrees than the maximal fields. Finally, we will see that splitting fields  $E$  for  $D$  can be embedded as maximal fields in an algebra “close” to  $D$  in such a way that their centralizer  $E'$  in this new algebra is equal to themselves. We follow [Rei75].

**Theorem 3.4.1.** *Let  $D$  be a skewfield with center  $k$ , and let  $m = \sqrt{[D : k]}$ . Let  $E$  be a finite extension of  $k$ .*

- (i) *If  $E$  splits  $D$ , then  $m \mid [E : k]$ .*
- (ii) *There exists a smallest positive integer  $r$  for which there is an embedding  $E \subset M_r(D)$  as  $k$ -algebras. With this choice of  $r$ ,  $E$  splits  $D$  if and only if  $E$  is a maximal subfield of  $M_r(D)$ . Furthermore, the centralizer  $E'$  of  $E$  in  $M_r(D)$  is a skewfield, and  $E$  is a maximal subfield of  $M_r(D)$  if and only if  $E = E'$ .*

*Proof.* The proof can be found in [Rei75, Theorem (28.5)], and we now sketch it.

Via the identification of  $D$  with  $D \otimes_k 1$  in  $S$ , any simple (right)  $S$ -module  $V$  is naturally a vector space over  $D$  with, say,  $r = [V : D]$ . This double interpretation of  $V$  is useful. On one hand, identifying  $E$  with  $E \otimes_k 1$  in  $S$  then  $E \subset \text{Hom}_S(V, V)$ . Then  $M_m(E)$  can be seen as  $\text{Hom}_S(V^m, V^m)$ , and

so  $S = E \otimes_k D \cong M_m(E) \cong V^m$  as right  $S$ -modules. On the other hand, with the ranks of  $S$  and  $V$  as  $D$ -modules one obtains  $mr = m[V : D] = [S : D] = [E : k]$ . Hence  $m \mid [E : k]$ .

Moreover, as  $E$  and  $D$  commute in  $S$ , and as  $V$  is an  $S$ -module by construction, so  $E$  can be seen also as  $E \subset \text{Hom}_D(V, V) \cong M_r(D)$ . Now consider  $E'$  the centralizer of  $E$  in  $B := \text{Hom}_D(V, V)$ . Note  $E'$  is a ring (containing  $E$ ) right now. The elements in  $E'$  are in  $\text{Hom}_S(V, V)$  because by definition they commute with  $E$  and hence with  $D$  in  $S$ . Actually one has  $E' = \text{Hom}_S(V, V)$  and this is now a skewfield by Schur's Lemma. Moreover, for any  $x \in E' \setminus E$  then  $E(x)$  is a commutative extension of  $E$  inside a skewfield, and hence a field extension of  $E$ . It follows that  $E' = E$  if and only if  $E$  is a maximal subfield in  $B$ .

Note also that  $B$  has rank  $r^2$  as a  $D$ -module and thus rank  $r^2m^2$  as a  $k$ -module. Hence, by Corollary 3.1.4 above with  $A = B$  and  $B = E$  one has  $[E : k][E' : k] = [B : k] = r^2m^2$ . But above we saw that if  $E$  is a splitting field then  $[E : k] = mr$ . And as  $E \subset E'$ , also  $[E' : k] = [E' : E][E : k]$ . So necessarily  $E' = E$  and hence  $E$  is forced to be a maximal subfield of  $B$ . Reciprocally, if  $E$  is a maximal subfield of  $B$  then  $E = E'$ . But  $B \otimes_k E = B \otimes_k E^{opp} \cong M_s(E') = M_s(E)$  for  $s = [E : k]$ . So  $E$  splits  $B$ . But  $B \cong M_r(D)$ , and therefore  $E$  splits  $D$ .  $\square$

**Remark 3.4.2.** Hence, if  $E$  splits  $D$ , then  $E$  can be embedded as a maximal subfield in a full matrix algebra  $B$  over  $D$ , in such a way that  $[B : k] = [E : k]^2$  and that  $E$  coincides with its centralizer in  $B$ . Such  $E$  is called a self-centralizing maximal subfield of  $B$ . Note that requiring  $A$  to be split by a field  $E$  such that  $[A : k] = [E : k]^2$  then necessarily  $B \cong A$ . We will meet examples of this situation in Sections 5.3, 5.4 and 5.5. However, note that the splitting field may well not lie in  $A$ . In Section 5.6 we give examples where this situation may rise.

**Corollary 3.4.3.** *Let  $A$  be a central simple  $k$ -algebra split by  $E$ , where  $k \subset E$ , and where  $[A : k] = [E : k]^2$ . Then  $E$  can be embedded in  $A$  as a self-centralizing maximal subfield of  $A$ .*

*Proof.* [Rei75, Corollary (28.10)]  $\square$

### 3.5 Crossed-product algebras

Let  $A$  be a central simple algebra. Each class  $[A] \in Br(F/k)$  contains a representative  $B$  in which the splitting field  $F$  is embedded as a self-centralizing maximal subfield.  $B$  is in general just similar to  $A$ . Moreover,

if by any chance we find a field  $F$  embedded in  $A$  and such that  $[A : k] = [F : k]^2$ , then  $B \cong A$  and  $F$  is a self-centralizing maximal subfield of  $A$ .

One also shows that, extending to the normal closure if necessary, the maximal subfield  $F$  can be taken finite and Galois without changing the similarity class of  $A$ . Such algebras  $A$  are called crossed-products.

**Definition 3.5.1.** A crossed-product  $k$ -algebra is a central simple  $k$ -algebra  $A$  that contains a subfield  $F$  Galois over  $k$  such that  $[F : k] = [A : F]$ .

Note that  $[A : k] = [F : k]^2$  trivially holds true. Moreover, by Theorem 3.3.1 there exists a maximal field  $E$  in  $A$  which splits  $A$  and such that  $[A : k] = [E : k]^2$ . From this,  $F \cong E$  and  $F$  splits  $A$  as well. Also, as  $F$  is contained in  $A$  by assumption, then  $B = A$  in the preceding discussion, and by Corollary 3.4.3 above,  $F$  is a self-centralizing maximal subfield of  $A$ . Note also that the  $F$ -basis of  $A$  is closely related to the Galois group  $G := \text{Gal}(F/k)$ . Recall that Galois extensions satisfy  $\#G = [F : k]$  and hence the cardinality of any  $F$ -basis of  $A$  is  $\#G$  as well. The connection between the  $F$ -basis and  $G$  is given by the Skolem-Noether Theorem in the next section.

**Remark 3.5.2.** If  $A$  is a crossed-product algebra, then  $A$  is written as

$$(F, \text{Gal}(F/k), f)$$

and we will call  $A$  a crossed-product over  $F$  for short. The role of  $f$  will be explained later.

**Remark 3.5.3.** (Aside) As  $F$  is exactly the set of elements which commute with  $F$  in  $(F, \text{Gal}(F/k), f)$ , then if we make them become the *scalars*—that is, we declare them to commute with every element or, in other words, we build the  $F$ -algebra  $(F, \text{Gal}(F/k), f) \otimes_k F$ —then  $F$  becomes exactly the set of all elements which commute with every element, that is  $Z((F, \text{Gal}(F/k), f) \otimes_k F) = F$ . In other words,  $((F, \text{Gal}(F/k), f) \otimes_k F)$  is a central  $F$ -algebra.

We will see in Chapter 5 that some curves in Chapter 2 are supersingular. We are going to show that this arithmetic property ensures that the endomorphism algebras of the jacobian variety of these curves has dimension 16 (see Theorem 5.2.6).

On the other hand, we will show in Chapter 5 that there are some supersingular curves of genus two whose Jacobian variety has an endomorphism algebra which contains Galois subfields of degree 4. Assuming simple and central, these two facts imply that the endomorphism algebra of the Jacobian variety of such curves of genus two is a crossed-product algebra (see Corollary 5.2.9).

### 3.6 The Skolem-Noether theorem

An automorphism of  $k$ -algebras  $\phi$  is called inner if there exists an invertible element  $u \in A$  such that  $\phi(x) = uxu^{-1} \forall x \in A$ .

**Theorem 3.6.1** (Skolem-Noether). *Any automorphism of simple, central  $k$ -algebras is inner.*

*Proof.* See [Rei75]. □

Note that taking any element  $x$  of a maximal field  $F$  of a crossed product  $k$ -algebra  $A$ , and  $\sigma$  is an automorphism of  $A$  that restricts to an element of  $\text{Gal}(F/k)$ , then  $\sigma(x) = uxu^{-1}$  for certain invertible element  $u \in A$ . Write  $u_\sigma$  for such an invertible  $u$ . It is obvious that  $u_\sigma u_\tau$  and  $u_{\sigma\tau}$  have the same effect in the elements  $x \in F$ . Indeed, they both act as  $x \mapsto \sigma(\tau(x)) = \sigma\tau(x)$ . But this does *not* imply  $u_\sigma u_\tau = u_{\sigma\tau}$ .

It is easy to show that any  $u_\sigma$  attached to any *nontrivial* element of the Galois group does *not* belong to the maximal self-centralizing subfield.

**Lemma 3.6.2.** *Let  $\sigma$  be an element in  $\text{Gal}(F/k)$  different from the identity. Then, for any  $u_\sigma \in (F, \text{Gal}(F/k), f)^*$  such that  $u_\sigma x u_\sigma^{-1} = \sigma(x)$  one has  $u_\sigma \notin F^*$ .*

*Proof.* If not, then  $u_\sigma \in F$  and  $u_\sigma x u_\sigma^{-1} = x$  because  $F$  is a field. □

**Remark 3.6.3.** It is obvious that  $u_{\sigma^{-1}} u_\sigma$  centralizes any  $x \in F$  and  $u_{\sigma^{-1}} u_\sigma = u_\sigma u_{\sigma^{-1}}$ . This implies, for example, that Galois groups in which all elements have order two are associated with  $u_\sigma$ 's such that  $u_\sigma^2 \in F^*$ .

Trivially  $u_\sigma u_\tau u_{\sigma\tau}^{-1}$  centralizes the self-centralizing maximal subfield  $F$ . Hence there is  $f_{\sigma,\tau} \in F^*$  such that  $u_\sigma u_\tau u_{\sigma\tau}^{-1} = f_{\sigma,\tau}$ .

Now recall that our algebras are associative by assumption. In particular  $u_\rho(u_\sigma u_\tau) = (u_\rho u_\sigma)u_\tau$  must hold for any  $\rho, \sigma, \tau \in \text{Gal}(F/k)$ . But above we just saw  $u_\sigma u_\tau = f_{\sigma,\tau} u_{\sigma\tau}$  for a certain  $f_{\sigma,\tau} \in F^*$ . This allows to foresee a certain behaviour of the  $f$ 's. Namely, as

$$\begin{aligned} f_{\rho,\sigma} f_{\rho\sigma,\tau} u_{\rho\sigma\tau} &= (f_{\rho,\sigma} u_{\rho\sigma}) u_\tau = (u_\rho u_\sigma) u_\tau = \\ &= u_\rho (u_\sigma u_\tau) = u_\rho (f_{\sigma,\tau} u_{\sigma\tau}) = \rho(f_{\sigma,\tau}) u_\rho u_{\sigma\tau} = \rho(f_{\sigma,\tau}) f_{\rho,\sigma\tau} u_{\rho\sigma\tau} \end{aligned}$$

then one has

$$f_{\rho,\sigma} f_{\rho\sigma,\tau} = \rho(f_{\sigma,\tau}) f_{\rho,\sigma\tau}.$$

Sets of elements  $f \in F^*$  as above were known as *factor sets* in the past, and they have other nice properties. They are closed under multiplication

$$(fg)_{\sigma,\tau} = f_{\sigma,\tau}g_{\sigma,\tau}$$

and there is a special type of them, the ones of the form

$$(\delta c)_{\sigma,\tau} := c_\sigma \sigma(c_\tau) c_{\sigma\tau}^{-1}$$

for any set  $\{c_\sigma\}_{\sigma \in G}$  of elements in  $F^*$ , which form a subgroup. Moreover, one checks that  $(F, G, f) \cong (F, G, (\delta c)f)$ .

Factor sets belong to the theory of Galois Cohomology. The standard constructions of chains, cochains, cocycles and coboundaries can be found in many books such as [Ser94] or [NSW86]. The  $f_{\sigma,\tau}$ 's are elements of the second cohomology group  $H^2(G, F^*)$ , which is defined as the quotient of the multiplicative group of the factor sets (2-cocycles nowadays) by the 2-coboundaries  $(\delta c)$ .

As the  $f_{\sigma,\tau}$ 's are defined up to 2-coboundaries, this allows to normalize the  $f_{\sigma,\tau}$ 's: if one takes  $c_1 := f_{1,1}^{-1}$  and  $c_\sigma := 1$  for the other  $\sigma \in G$ , then the 2-coboundary  $(\delta c)_{\sigma,1} := \sigma(c_1) = f_{\sigma,1}^{-1}$ ,  $\sigma \in G$  makes the values of the equivalent 2-cocycle  $g = (\delta c)f$  to be  $g_{1,1} = g_{\sigma,1} = g_{1,\sigma} = 1$  for all  $\sigma \in G$ .

From now on, all the 2-cocycles are going to be normalized. In this way,  $u_\sigma u_1 = f_{\sigma,1} u_\sigma = u_\sigma = f_{1,\sigma} u_\sigma = u_1 u_\sigma$ , and  $u_1$  is the unit element in  $A$ . Recall that by the Skolem-Noether Theorem the  $u_\sigma$ 's are (left and right) invertible, so units in  $A$ . After normalization, one identifies  $u_1$  with  $1_A$ . Moreover,  $u_1 F$  is  $F$  and hence  $u_1 = 1_A = 1_F = 1_k = 1$ .

By the previous discussion, all crossed-products have a 2-cocycle in their structure.

**Theorem 3.6.4.** *Let  $A$  be a crossed product  $k$ -algebra and  $F$  a maximal field of  $A$ . Then there exists a set  $\{u_\sigma\}_{\sigma \in G}$  of elements of  $A$  which is a  $F$ -basis of  $A$ . These elements satisfy*

$$u_\sigma x = \sigma(x) u_\sigma \quad \forall x \in F, \forall \sigma \in G$$

and

$$u_\sigma u_\tau = f_{\sigma,\tau} u_{\sigma\tau} \quad \forall \sigma, \tau \in G$$

where  $f_{\sigma,\tau}$  is a 2-cocycle.

*Proof.* See [Rei75, Chapter VII, §29]. □

Reciprocally, for any 2-cocycle  $f \in H^2(G, F^*)$  and any set  $\{u_\sigma\}_{\sigma \in G}$  behaving like above, then  $(F, G, f) := \bigoplus_{\sigma \in G} u_\sigma F$  is a crossed-product algebra with self-centralizing maximal subfield equal to  $F$ .

Two crossed-product algebras  $(F, G, f)$ ,  $(F, G, g)$  are isomorphic if and only if the factor sets  $f$  and  $g$  differ by a 2-coboundary [Rei75, Theorem (29.6)]. Moreover, it is shown that  $(F, G, f) \otimes_k (F, G, g)$  and  $(F, G, fg)$  belong to the same class in the Brauer Group [Rei75, Theorem (29.9)]. Thus there is a well defined monomorphism of groups  $H^2(G, F^*) \hookrightarrow Br(F/k)$  which is an isomorphism.

**Theorem 3.6.5.** *Let  $F$  be a Galois extension of  $k$ , with Galois group  $G$ . Then*

$$H^2(G, F^*) \cong Br(F/k),$$

and the isomorphism is given by mapping  $[f] \in H^2(G, F^*)$  onto the class  $[(F, G, f)] \in Br(F/k)$ .

*Proof.* [Rei75, Theorem (29.12)] □

**Example 3.6.6.** Take  $\{c_\sigma\}_{\sigma \in G} = \{\pi_\sigma\}_{\sigma \in \text{Gal}(F/k)}$  the set of roots of the irreducible polynomial defining  $F$ . Assume  $\text{Gal}(F/k) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  with  $\sigma, \tau$  two nontrivial elements in  $\text{Gal}(F/k)$ , both of order 2, and such that  $\sigma(\pi_1) = \pi_\sigma, \tau(\pi_1) = \pi_\tau, \sigma\tau(\pi_1) = \pi_{\sigma\tau}$ . Then

$$\pi_\sigma \sigma(\pi_\tau) \pi_{\sigma\tau}^{-1} = \pi_\sigma, \pi_\tau \tau(\pi_\sigma) \pi_{\tau\sigma}^{-1} = \pi_\tau$$

$$\pi_{\sigma\tau} \sigma\tau(\pi_\tau) \pi_\sigma^{-1} = \pi_{\sigma\tau}, \pi_1(\pi_1) \pi_1^{-1} = \pi_1$$

This shows that the set  $\{\pi_\sigma\}_{\sigma \in \text{Gal}(F/k)}$  is a 2-coboundary. Further, after normalization, the 2-coboundary is  $\{1, \frac{\pi_\sigma}{\pi_1}, \frac{\pi_\tau}{\pi_1}, \frac{\pi_{\sigma\tau}}{\pi_1}\} \subseteq F^*$ . For any invertible element  $u \in (F, \text{Gal}(F/k), f)^*$ , the elements

$$\left\{ u, u \frac{\pi_\sigma}{\pi_1}, u \frac{\pi_\tau}{\pi_1}, u \frac{\pi_{\sigma\tau}}{\pi_1} \right\}$$

lie in the same class modulo  $F^*$ , and they are units in the subring  $uF \subseteq (F, \text{Gal}(F/k), f)$ . The elements  $\{1, \frac{\pi_\sigma}{\pi_1}, \frac{\pi_\tau}{\pi_1}, \frac{\pi_{\sigma\tau}}{\pi_1}\} \in [1]$  attached to the identity element of  $\text{Gal}(F/k)$  are in  $F$ , and by Lemma 3.6.2 they are the only ones.

When the Galois group of the self-centralizing maximal subfield  $F$  of a crossed-product  $k$ -algebra  $A$  is cyclic, the 2-cocycles are of a special shape. Assume  $\text{Gal}(F/k) = \langle \sigma \rangle$  is cyclic of order  $n$ . Take any  $x \in F$  and  $u_\sigma \in A$  a unit that acts as  $u_\sigma^n x u_\sigma^{-n} = \sigma(x)^n = x$  in the Skolem-Noether Theorem.

This implies at once that  $u_\sigma^n$  must lie in  $F^*$ . But the expression of the intermediate powers of  $u_\sigma$

$$\begin{aligned} u_\sigma^2 &= u_\sigma u_\sigma = f_{\sigma,\sigma} u_{\sigma^2} \\ u_\sigma^3 &= u_\sigma^2 u_\sigma = f_{\sigma,\sigma} u_{\sigma^2} u_\sigma = f_{\sigma,\sigma} f_{\sigma^2,\sigma} u_{\sigma^3} \\ &\dots \\ u_\sigma^n &= \prod_{j=0}^{n-1} f_{\sigma^j,\sigma} u_{\sigma^n} = \prod_{j=0}^{n-1} f_{\sigma^j,\sigma} u_1 = \prod_{j=0}^{n-1} f_{\sigma^j,\sigma} \end{aligned}$$

and Galois invariance imply that  $u_\sigma^n \in k^*$ .

**Remark 3.6.7.** However, we will show in Chapter 6 that the cyclic/noncyclic character of the Galois group of the crossed-product algebra is not relevant for a solution to DDH.

### 3.7 Examples

We borrow two examples of crossed-product algebras of dimension 4 over  $\mathbb{Q}$  from [AB04].

**Example 3.7.1.** Consider  $H$  the central simple  $\mathbb{Q}$ -algebra of dimension 4 with  $\mathbb{Q}$ -basis  $\{1, u, v, uv\}$  such that  $u^2 = 1, v^2 = -1, uv = -vu$ . This is a quaternion algebra over  $\mathbb{Q}$  called  $(\frac{1,-1}{\mathbb{Q}})$ . One has the  $\mathbb{Q}$ -isomorphism

$$\begin{array}{ccc} M_2(\mathbb{Q}) & \cong & (\frac{1,-1}{\mathbb{Q}}) \\ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} & \longmapsto & \frac{1}{2}((\alpha + \delta) + (\alpha - \delta)u + (\beta - \gamma)v + (\beta + \gamma)uv) \\ \begin{pmatrix} x + y & z + t \\ t - z & x - y \end{pmatrix} & \longleftarrow & x + yu + zv + tuv \end{array}$$

and trivially every quadratic extension  $\mathbb{Q}(\sqrt{\xi})$ , for every  $\xi \in \mathbb{Q}, \xi < 0$  splits  $(\frac{1,-1}{\mathbb{Q}})$  as  $\mathbb{Q}(\sqrt{\xi})$  is embedded in  $(\frac{1,-1}{\mathbb{Q}})$  via

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{\xi}) & \hookrightarrow & M_2(\mathbb{Q}) \\ x + y\sqrt{\xi} & \longmapsto & \begin{pmatrix} x & y \\ \xi y & x \end{pmatrix} \end{array}$$

**Example 3.7.2.** Take now  $H := (\frac{p,q}{\mathbb{Q}})$  with  $p, q$  two different primes such that one of them is congruent to 1 mod 4 and such that  $(\frac{p}{q}) = -1$ . Then it is shown in [AB04] that  $H$  is not isomorphic to a  $2 \times 2$  matrix algebra (and

moreover, as the dimension is 4, this implies that  $H$  is a skewfield). Further, to give a splitting field  $F$  embedded in  $H$  (via  $\Phi$ , say) one needs to find an element  $h \in H$  such that  $N(\Phi^{-1}(h)) = N(h)$  and  $Tr(\Phi^{-1}(h)) = Tr(h)$ . One finds  $h$  in the conjugation class of  $h$  in the group of units of  $H$ .

**Example 3.7.3.** It is very well known that Quaternion algebras arise as the endomorphism algebras of supersingular elliptic curves over finite fields.

In analogy with elliptic curves over finite fields, curves of genus two over finite fields provide examples of crossed-product algebras (see Corollary 5.2.9).

**Example 3.7.4.** In Section 5.3 we will show a cyclic crossed-product algebra over a subfield associated with an automorphism of a curve. We will consider the endomorphism algebra of the Jacobian variety of the genus two curve  $C : y^2 = x^5 + 1$  defined over a finite field  $\mathbb{F}_p$ . We will show that if  $p \equiv 2, 3 \pmod{5}$  then  $\text{End}^0(\text{Jac}(C))$  contains a cyclic maximal subfield  $\mathbb{Q}(\xi_5)$  and also a non-cyclic maximal subfield generated by the Frobenius endomorphism. We show that  $\text{End}^0(\text{Jac}(C))$  is a crossed-product algebra.

**Example 3.7.5.** In Section 5.4 we will show other examples of crossed-product algebras associated to curves over finite fields without extra automorphisms. The role of the extra automorphisms is played in these examples by the CM-isogenies.

**Example 3.7.6.** In Section 5.5 we consider the algebra  $\text{End}^0(\text{Jac}(C))$  associated with the supersingular curve  $C : y^2 + y = x^5 + x^3 + 1$  defined over a finite field  $\mathbb{F}_{2^m}$ . In this example,  $\text{End}^0(\text{Jac}(C))$  is 16 dimensional and contains a degree 4 field generated by the Frobenius endomorphism. However, we will see that  $\text{End}^0(\text{Jac}(C))$  is not a crossed-product algebra as it fails to be central.

## Chapter 4

# Algebraic groups for cryptography

In Chapter 2 we described the affine coordinate rings  $\mathcal{O}_{C_u}$ ,  $\mathcal{O}_{C_f}$  of genus two curves  $C$  defined over a field  $\mathbb{F}_q$  of even or odd characteristic respectively. In this chapter we consider the ideal class group  $Cl(\mathcal{O}_C)$  of these Dedekind domains. We review how the group  $Cl(\mathcal{O}_C)$  is related to the degree zero divisor class group  $Pic^0(C/\mathbb{F}_q)$  of the curves  $C$ , how to represent the elements in the group  $Cl(\mathcal{O}_C)$  and how to compute in  $Cl(\mathcal{O}_C)$ .

When there is a rational point at infinity, the group  $Cl(\mathcal{O}_C)$  is isomorphic to the group of  $\mathbb{F}_q$ -rational points of the abelian variety  $Jac(C)$ . In this chapter we review some properties of  $Jac(C)$  and recall what supersingular and  $\mathbb{F}_q$ -simple abelian varieties are. We recall the notions of endomorphism, isogeny, characteristic polynomial associated to an endomorphism and how to interpret automorphisms of curves  $C$  as isogenies of  $Jac(C)$ . We review the Frobenius endomorphism, its characteristic polynomial and how to read supersingularity from it. The Frobenius endomorphism plays a major role in Chapter 5.

The main references for this chapter are [Lor96], [CS86] and [GM06].

### 4.1 The ideal class group

In this section we recall the definition of the ideal class group  $Cl(\mathcal{O}_C)$  and recall why is it a finite group in our situation. We also review the relation between the ideal class group and the degree zero divisor class group  $Pic^0(C)$  of curves of genus two over finite fields.

Unique factorization into prime ideals  $\neq 0$  in Dedekind domains  $\mathcal{O}_K$

provides the set of ideals in  $\mathcal{O}_K$  with a multiplicative structure similar to that of  $\mathbb{Z}$ . As in the integers, the multiplicative inverses do not lie in  $\mathcal{O}_K$  but in its field of fractions  $K$ . The common notion of an ideal and its inverse is that of a fractional ideal.

**Definition 4.1.1.** A fractional ideal of  $K$  is a finitely generated  $\mathcal{O}_K$ -submodule  $\mathfrak{a} \neq 0$  of  $K$ .

Any element  $a \in K$  defines a fractional principal ideal  $(a) = a\mathcal{O}_K$  of  $K$  and, as  $\mathcal{O}_K$  is Noetherian, any  $\mathcal{O}_K$ -submodule  $\mathfrak{a} \neq 0$  of  $K$  is a fractional ideal if and only if there exists  $c \in \mathcal{O}_K$ ,  $c \neq 0$ , such that  $c\mathfrak{a} \subseteq \mathcal{O}_K$  is an ideal of the ring  $\mathcal{O}_K$ . Fractional ideals are multiplied just as the ideals in  $\mathcal{O}_K$  are. We say that a fractional ideal is *integral* if it is also an ideal of  $\mathcal{O}_K$ .

**Proposition 4.1.2.** *The fractional ideals of  $K$  form an abelian group  $J_K$ , called the ideal group of  $K$ . The identity element is  $(1) = \mathcal{O}$  and the inverse of  $\mathfrak{a}$  is  $\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subseteq \mathcal{O}\}$ .*

*Proof.* [Neu99, Chapter I, Proposition (3.8)]. □

**Definition 4.1.3.** The ideal class group  $Cl(\mathcal{O})$  of the Dedekind domain  $\mathcal{O}$  is the quotient group  $J_K/P_K$  of the group of fractional ideals of the field of fractions  $K$  of  $\mathcal{O}$  by the subgroup of the principal fractional ideals.

Our interest is in Dedekind domains coming from curves of genus two over finite fields  $\mathbb{F}_q$ . Recall that Dedekind domains are attached to curves as affine coordinate rings. Given a dense open affine subset  $U \subset C$ , the affine coordinate ring of functions defined everywhere on  $U$  is a Dedekind domain  $\mathcal{O}_C(U)$  with a natural  $\mathbb{F}_q$ -algebra structure, as the functions are quotients of polynomials over  $\mathbb{F}_q$ .

We noted in Chapter 2 that any curve  $C$  of genus two over a finite field has a nonsingular model in  $\mathbb{P}^4$ , and for them the Dedekind domain  $\mathcal{O}_C$  is given by an affine part of the homogeneous coordinate ring given by  $\mathbb{F}_q[X_0, X_1, X_2, X_3, Y]$  modulo some relations (see Sections 2.7 and 2.8 in Chapter 2). The field of fractions  $\mathbb{F}_q(\mathcal{O}_C) = \mathbb{F}_q(C)$  of  $\mathcal{O}_C$  is a finite extension of  $\mathbb{F}_q(x)$ . The Dedekind domains  $\mathcal{O}_C$  correspond to the desingularization of certain plane Kummer/Artin-Schreier models, and  $\mathcal{O}_C$  is the integral closure of  $\mathbb{F}_q[x]$  in  $\mathbb{F}_q(C)$ . In this situation one knows how to prove that  $Cl(\mathcal{O}_C)$  is a finite group in two different ways.

**Theorem 4.1.4.** *The ideal class group  $Cl(\mathcal{O}_C)$  of a curve over a finite field is a finite group.*

*Proof.* (Sketch) The first way to prove this theorem parallels the case of number fields. The crucial fact is that for curves over finite fields, the Dedekind domains  $\mathcal{O}_C$  have finite quotients. As a consequence, if  $\mathcal{O}_C$  is the integral closure of  $\mathbb{F}_q[x]$  in a finite separable extension  $\mathbb{F}_q(C)/\mathbb{F}_q(x)$  then  $Cl(\mathcal{O}_C)$  is finite [Lor96, Chapter V, Theorem 3.10]. One then shows that purely inseparable extensions have no real effect on the ideal class group [Lor96, Chapter X, Proposition 1.6].

The second way is to use the Riemann-Roch Theorem. In 2.1.4 we noted that the Riemann-Roch Theorem implies that  $Pic^0(\mathbb{F}_q(C))$  is finite. It turns out that the two groups  $Cl(\mathcal{O}_C)$  and  $Pic^0(\mathbb{F}_q(C))$  are related via a map

$$\begin{aligned} \varphi: Pic^0(\mathbb{F}_q(C)) &\longrightarrow Cl(\mathcal{O}_C) \\ [\sum_{P \in C} a_P P] &\longmapsto \prod_{P \in U} [\mathcal{M}_P \cap \mathcal{O}_C]^{a_P} \end{aligned}$$

where  $\mathcal{M}_P$  is the maximal ideal of the point  $P$ . As a consequence, the orders of these two groups are related by a formula involving the regulator  $R$  of the function field extension  $\mathbb{F}_q(C)/\mathbb{F}_q(x)$  and the number  $r$  of points  $\pi^{-1}(\infty) = \{P_1, \dots, P_r\}$  which map to  $\infty \in \mathbb{P}^1$  under the degree two morphism.  $\square$

**Corollary 4.1.5.**  $|Cl(\mathcal{O}_C)| \cdot |R| = |Pic^0(C)| \cdot \prod_{i=1}^r \deg(P_i) \cdot \log(q)^{r-1}$

*Proof.* [Lor96, Chapter VIII, Lemma 9.8 and Corollary 9.9]  $\square$

**Definition 4.1.6.** A quadratic extension  $\mathbb{F}_q(C)/\mathbb{F}_q(x)$  of function fields is called real or imaginary depending on the ramified/split behaviour of  $\infty \in \mathbb{P}^1$ . If  $\infty$  ramifies it is called imaginary and if  $\infty$  splits it is called real.

**Remark 4.1.7.** As in the imaginary case the Weierstrass point  $P_\infty$  is defined over  $\mathbb{F}_q$ , and as the choice of the point  $\infty \in \mathbb{P}^1$  is arbitrary, all genus 2 curves with at least one Weierstrass point over  $\mathbb{F}_q$  give rise to imaginary quadratic function field extensions.

For curves of genus 2, the two groups  $Pic^0(\mathbb{F}_q(C))$  and  $Cl(\mathcal{O}_C)$  are isomorphic in the case of imaginary quadratic extensions. Recall that we are interested in the case that the order of these groups is a prime number.

**Proposition 4.1.8.** *If  $C$  is a curve of genus 2 over a finite field of odd characteristic given by a polynomial  $f$  of degree 5, then  $Pic^0(\mathbb{F}_q(C_f))$  and  $Cl(\mathcal{O}_{C_f})$  are isomorphic. If  $C$  is a curve of genus 2 over a finite field of even characteristic, then  $Pic^0(\mathbb{F}_q(C_u))$  and  $Cl(\mathcal{O}_{C_u})$  are isomorphic in all cases but for the  $(1, 1, 1)$  cubic.*

*Proof.* If  $\text{char}(\mathbb{F}_q) \neq 2$ , then we saw in Chapter 2 that the number  $r$  of points above infinity depends on the degree of the defining polynomial  $f$ . Indeed, if the degree of  $f$  is 6, then the point at infinity  $\infty \in \mathbb{P}^1$  is not ramified in  $\mathbb{F}_q(C_f)/\mathbb{F}_q(\mathbb{P}^1)$  (see Section 2.7 in Chapter 2) and there are two conjugated points of degree two in  $\pi^{-1}(\infty)$ . So  $r = 2$  in these cases. By Corollary 4.1.5, this does not guarantee the two orders to be equal. If, instead, the degree of  $f$  is 5, then  $\infty \in \mathbb{P}^1$  ramifies and there is just one point in  $\pi^{-1}(\infty)$ , so  $r = 1$ . It is defined over  $\mathbb{F}_q$  and hence has degree one. As also  $R = 1$ , Corollary 4.1.5 forces  $\text{Pic}^0(\mathbb{F}_q(C_f))$  and  $\text{Cl}(\mathcal{O}_{C_f})$  to have the same order.

If  $\text{char}(\mathbb{F}_q) = 2$ , then  $\infty \in \mathbb{P}^1$  is always ramified in all cases but one. That is, there is always one point of  $C$  lying above  $\infty \in \mathbb{P}^1$  for all the  $u(x)$  defining Artin-Schreier models but one (see Section 2.8 in Chapter 2). The exception is the  $(1, 1, 1)$  cubic case

$$y^2 + y = (ax^2 + bx + c)/(x^3 + ux + u) + d$$

with  $d \in \mathbb{F}_q/\text{AS}(\mathbb{F}_q)$  and  $u \in \mathbb{F}_q \setminus \{0\}$  such that  $x^3 + ux + u$  is irreducible in  $k[x]$ . After clearing denominators, the point  $[1 : 0 : 0]$  is double ordinary but not ramified, and there are two points  $P_\infty, P'_\infty$  above it in the nonsingular model.  $\square$

**Remark 4.1.9.** While for arbitrary degree six polynomials  $f$  there is *a priori* no reason why the two groups  $\text{Pic}^0(\mathbb{F}_q(C_f))$  and  $\text{Cl}(\mathcal{O}_{C_f})$  should be isomorphic, in the case we are given a degree 6 polynomial  $f$  with a root in the same field as the coefficients of  $f$  (in other words, there is a rational Weierstrass point), then under a certain change of variables one transforms  $f$  to a degree 5 polynomial  $f'$  defined over the same field as  $f$  [CF96]. For these particular polynomials  $f$ , the two groups above are isomorphic.

## 4.2 Representation in the ideal class group

Recall that our Dedekind domains  $\mathcal{O}_{C_f}$  and  $\mathcal{O}_{C_u}$  from Chapter 2 are affine coordinate rings in some affine open set of a genus two curve  $C$ . Further, recall that if  $C$  has just one point mapping to  $\infty \in \mathbb{P}^1$  under the degree two morphism  $\pi: C \rightarrow \mathbb{P}^1$ —in which case such a point is necessarily double and defined over the base field  $k$ —then, regardless of the characteristic of the base field,  $C$  has a plane model given by  $y^2 + h(x)y = f(x)$  with  $\deg f(x) = 5$  and  $\deg h(x) \leq 2$ . If there are two different points mapping to  $\infty \in \mathbb{P}^1$  under  $\pi$  then the plane model is  $y^2 + h(x)y = f(x)$  with  $\deg f(x) = 5$  and  $\deg h(x) = 3$  in even characteristic and  $h(x) = 0$ ,  $\deg f(x) = 6$  in odd characteristic.

Regardless of the number of points at infinity, the integral ideals  $\mathfrak{a}$  in the affine coordinate ring  $\mathcal{O}_C$  of a hyperelliptic curve over  $\mathbb{F}_q$  of any genus  $g$ , have the following expression as polynomials in two variables  $x, y$  with coefficients in  $\mathbb{F}_q$

$$\mathfrak{a} = s(a\mathbb{F}_q[x] + (b+y)\mathbb{F}_q[x])$$

with  $s(x), a(x), b(x) \in \mathbb{F}_q[x]$ ,  $s(x)$  and  $a(x)$  monic, and  $a(x), b(x)$  satisfying the divisibility condition  $a(x) \mid (b(x)^2 - b(x)h(x) - f(x))$  for  $f, h$  the hyperelliptic polynomials corresponding to  $C$  (see for example [JMS04]). Note that the degree in  $y$  is at most one.

**Definition 4.2.1.** If, in the above expression  $s = 1$ , the integral ideal  $\mathfrak{a}$  is called *primitive*. If, further,  $\deg a(x) \leq g$  and  $\deg b(x) < \deg a(x)$  then  $\mathfrak{a}$  is called *reduced*.

The polynomials  $a, b$  specify the class of the ideal  $\mathfrak{a}$  modulo principal ideals, and there is a bijective correspondence between pairs  $a, b$  defining reduced ideals and ideal classes. We take the primitive representative in its class and write

$$\mathfrak{a} = [a(x), b(x)].$$

**Definition 4.2.2.** The polynomials  $a, b$  are called the coordinates of the integral fractional ideal  $\mathfrak{a}$ .

**Remark 4.2.3.** The coordinates  $a, b$  for the ideal  $\mathfrak{a}$  are given the name *Mumford Representation* after [Mum84].

For curves of genus 2 over  $\mathbb{F}_q$ , a typical integral ideal class has a representative of the form

$$[x^2 + \alpha x + \alpha', \beta x + \beta']$$

with  $\alpha, \alpha', \beta, \beta' \in \mathbb{F}_q$ .

The number of reduced representatives in every ideal class  $[\mathfrak{a}]$  in  $Cl(\mathcal{O}_C)$  varies according to the ramified/split behaviour of  $\infty \in \mathbb{P}^1$  in the extension  $\mathbb{F}_q(C)/\mathbb{F}_q(x)$ . In the imaginary case every ideal class contains one reduced representative, while in the real case there are up to two reduced representatives per class (recall that the regulator is at most two for us). The arithmetic in these two cases is different. In the imaginary case, Cantor's algorithms (see below) are the exact translation into algebraic terms of the natural arithmetic-geometric laws in  $Pic^0(C)$  due to the fact that  $Pic^0(C) \cong Cl(\mathcal{O}_C)$ .

The real case is an area of active research, with specific problems interesting for cryptographers [Sch00], [SSW96]. For real quadratic function fields of any genus in odd characteristic, see [JSW05]. In even characteristic, see [MVZ98], [Zuc97] and [Zuc98]. It would be interesting to work out explicitly the results in [MVZ98] and [Zuc97] in the  $(1, 1, 1)$  cubic case.

The isomorphism  $Pic^0(C) \cong Cl(\mathcal{O}_C)$  allows a geometric interpretation of integral ideal classes in the imaginary quadratic case, that is, for hyperelliptic curves with one point  $P_\infty$  above  $\infty \in \mathbb{P}^1$ . Recall that  $P_\infty$  is defined over  $\mathbb{F}_q$ .

**Proposition 4.2.4** (Riemann-Roch Reduction). *In every  $\mathbb{F}_q$ -rational divisor class of degree 0 of a curve  $C$  over  $\mathbb{F}_q$  of genus  $g$  there exists a divisor  $D - gP_\infty$  with  $D = \sum_{i=1}^k n_i P_i$ , with  $n_i \in \mathbb{N}$  and  $\sum n_i = g$ .*

*Proof.* See for example [Vol95, Proposition 7] or [FL03, Lemma 3.5]. The idea is that any degree zero divisor class of such curves has a representative of the form

$$D = \sum_i \deg(P_i)P_i - \left(\sum_i n_i\right)P_\infty,$$

and the coefficient  $(\sum_i n_i)$  can be converted into a quantity which is less than or equal to the genus  $g$  of  $C$ . The way to do so is by adding divisors of appropriate functions if required. Firstly, by the Riemann-Roch Theorem one can assume that the coefficients of a representative of the class of  $D$  in  $Pic^0(C)$  are all positive. That is, one can assume the part  $\sum_i n_i P_i$  to be an effective divisor. By the isomorphism  $Pic^0(C) \cong Cl(\mathcal{O}_C)$ , any ideal class corresponds to a degree zero divisor  $D$ , as above, but free of divisors from functions in its support. If one detects divisors from functions in the support of  $D$ , one can remove them without changing the class of  $D$ . By the Riemann-Roch Theorem, with this procedure it is possible to “reduce” any divisor  $D \in Div^0(C)$  to another divisor  $D' \in Div^0(C)$  of the form

$$D' = \sum_i \deg(P'_i)P'_i - gP_\infty$$

belonging to the same class of  $D$ . □

**Example 4.2.5.** Take a point  $P$  of a genus two curve  $C$  with one point  $P_\infty$  at infinity, and consider the point  $P^\iota$  (recall that  $P^\iota$  has the same image as  $P$  under the degree two morphism  $\pi$  to  $\mathbb{P}^1$ ). The divisor  $P + P^\iota$  is called a *hyperelliptic divisor* and it is very close to a principal divisor. Indeed, the divisor of the function  $x - x(P)$  is  $(x - x(P)) = P + P^\iota - 2P_\infty$ . Take

two arbitrary points  $P_1, P_2$  in  $C$  and consider the degree zero divisors  $D_1 = P_1 + P - 2P_\infty$  and  $D_2 = P_2 + P^\iota - 2P_\infty$ . Then the degree zero divisor

$$\begin{aligned} D = D_1 + D_2 &= P_1 + P_2 + P + P^\iota - 4P_\infty = P_1 + P_2 - 2P_\infty + P + P^\iota - 2P_\infty = \\ &= P_1 + P_2 - 2P_\infty + \operatorname{div}(x - x(P)) \end{aligned}$$

is equivalent to  $D' = P_1 + P_2 - 2P_\infty$  in  $\operatorname{Pic}^0(C)$ . Divisors in  $\operatorname{Div}(C)$  without hyperelliptic divisors in their support are sometimes called semireduced divisors.  $D'$  is thus a semireduced divisor linearly equivalent to  $D$  (in fact,  $D'$  is also reduced). Note that  $(x - x(P)) = P + P^\iota - (P_\infty + P_{\infty^\iota})$  for curves with two points above infinity, and in this case all divisors containing  $\pi^{-1}(\infty) = \{P_\infty, P_{\infty^\iota}\}$  in their support are not semireduced, that is, they contain the hyperelliptic divisor  $P_\infty + P_{\infty^\iota}$ .

**Remark 4.2.6.** For curves of genus two with one point at infinity, the geometric interpretation of ideal classes is given explicitly as follows: reduced divisors

$$P_1 + P_2 - 2P_\infty$$

correspond to the integral ideal with coordinates

$$\left[ (u - x(P_1))(u - x(P_2)), \frac{y(P_2)(u - x(P_1))}{x(P_2) - x(P_1)} + \frac{y(P_1)(u - x(P_2))}{x(P_1) - x(P_2)} \right].$$

Note that the coordinates of the points may lie in a quadratic extension. The above bijection takes place over the algebraic closure of the base field, at the geometric points.

### 4.3 Cantor's algorithms

In this section we recall how the geometric procedure of Riemann-Roch reduction of divisors is translated into an operation in terms of coordinates of ideals.

In [Can87], two algorithms implementing the operation in the ideal class group  $Cl(\mathcal{O}_C)$  for hyperelliptic curves with one point at infinity were introduced. These algorithms are inspired in the procedures of composition and reduction of quadratic forms of Gauss (see for example [Zag81]).

Cantor's algorithms do the following. Given the representatives  $\mathfrak{a}, \mathfrak{b}$  of two ideal classes  $[\mathfrak{a}], [\mathfrak{b}]$  in  $Cl(\mathcal{O}_C)$ , the first algorithm takes  $\mathfrak{a}$  and  $\mathfrak{b}$  as inputs and returns the multiplication of the ideals  $\mathfrak{a}\mathfrak{b}$ , which of course lies in the class  $[\mathfrak{a}\mathfrak{b}]$ . This step corresponds to the composition of quadratic forms.

The second algorithm takes the ideal  $\mathfrak{ab}$  as input and returns *the* reduced representative in the class  $[\mathfrak{ab}]$ . This step corresponds to the reduction of a quadratic form. Note that uniqueness of reduced representatives in each class is important. For a proof of correctness, see [MWZ98].

**Remark 4.3.1.** Cantor's algorithms represent addition in  $\text{Pic}^0(C/\mathbb{F}_q)$  if  $C$  has a  $k$ -rational Weierstrass point at least. In such a case, the composition law of quadratic forms can be given a geometric interpretation in terms of divisors on curves as formal addition together with Riemann-Roch reduction. The geometric object related to this is the Jacobian variety of  $C$ , which we recall in Section 4.4.

The following is a transcription of the Magma code implementing Cantor's algorithms. We use them for the computation of the Tate pairing for divisor classes on genus two curves (see Chapter 6). Note the use of the extended Euclidean algorithm XGCD.

**Algorithm 4.3.2.** Input: Mumford coordinates of two reduced divisors in the ideal class group of a curve  $C$  over  $\mathbb{F}_q$  with one point over  $\mathbb{F}_q$  at least. Output: unreduced Mumford coordinates of the sum of the two divisors.

```
compose:=function(a1,b1,a2,b2,C);
  f,h:=HyperellipticPolynomials(C);
  d1,e1,e2:=XGCD(a1,a2);
  b3:=b1+b2+h;
  d,c1,c2:=XGCD(d1,b3);
  s1:=c1*e1;
  s2:=c1*e2;
  s3:=c2;
  d2:=d*d;
  a3:=a1*a2;
  a:=a3 div d2;
  g1:=s1*a1*b2;
  g2:=s2*a2*b1;
  g3:=b1*b2+f;
  g4:=s3*g3;
  g5:=g1+g2+g4;
  g6:=g5 div d;
  b:=g6 mod a;
  return a,b;
end function;
```

**Algorithm 4.3.3.** Input: the coordinates  $u, v$  of a divisor  $D$  with no divisors of functions on its support.

Output: the reduced representative in the class of  $D$  modulo principals.

```

reduce:=function(u, v, C);
  f, h:=HyperellipticPolynomials(C);
  g:=Genus(C);
  while Degree(u) gt g do
    u1:=v * v;
    u2:=v * h;
    u3:=f - u2 - u1;
    u4:=u3 div u;
    v1:=h + v;
    v2:=-v1;
    v3:=v2 mod u4;
    u5:=LeadingCoefficient(u4);
    u6:=1/u5;
    u4:=u6 * u4;
    u:=u4;
    v:=v3;
  end while;
  return u, v;
end function;

```

## 4.4 The Jacobian variety

The elements in the degree zero divisor class group  $Pic^0(C/\bar{k})$  of a curve  $C/\bar{k}$  over the algebraic closure  $\bar{k}$  are in bijection with the  $\bar{k}$ -points of certain algebraic variety  $Jac(C)$  in a functorial way. This correspondence between the elements of the group  $Pic^0(C/\bar{k})$  and the set of points  $Jac(C)(\bar{k})$  is valid for all fields  $k'$  between  $k$  and  $\bar{k}$ , in the sense that the points  $Jac(C)(k')$  are in bijection with the subset  $Pic^0(C/\bar{k})^{Gal(\bar{k}/k')}$  of elements of  $Pic^0(C/\bar{k})$  fixed under the Galois action.

We now briefly recall these notions. Every open affine set  $U$  of a  $g$ -dimensional, smooth variety  $X$  has associated a  $k$ -algebra  $\mathcal{O}(U)$  which is Noetherian and  $g$ -dimensional. These are the affine coordinate rings. They are the algebraic equivalents of the local charts of an atlas in differential geometry. The elements of  $\mathcal{O}(U)$  are called sections; they are the rational maps everywhere defined in  $U$ .

The  $k$ -algebras  $\mathcal{O}(U)$  are isomorphic to quotients of the polynomial ring over  $k$  in several variables by some ideal  $(f_1, \dots, f_l)$ . We say that a variety  $X$  is a variety over  $k$  if these polynomial rings have coefficients in  $k$ , and we call  $k$  the ground field. The  $k$ -algebras  $\mathcal{O}(U)$  endow  $X$  with a structure of a locally ringed space of  $k$ -algebras.

By  $\text{Spec}(k)$  we mean an abstract point over  $k$ , and by the  $k$ -valued points of a variety  $X$  we mean the set of morphisms from  $\text{Spec}(k)$  into  $X$  whose composition with the natural map from  $X$  to  $\text{Spec}(k)$  is the identity. These morphisms correspond to the closed points with residue field  $k$ . We write  $X(k)$  for the set of  $k$ -valued points of  $X$ , and  $X(k')$  for the points of  $X$  over a finite extension  $k'$  of  $k$ . Whenever we omit the field  $k$ , we mean  $P \in X(\bar{k})$ .

By a morphism  $\varphi$  of varieties over  $k$  we mean a regular map. The coordinates of  $\varphi$  are given by rational maps. We say that a morphism is defined over  $k$  if it can be expressed as rational maps with coefficients in  $k$ . We also say that such morphisms are  $k$ -rational morphisms. By an isomorphism of varieties we mean a morphism with an inverse. This is also called a biregular map.

**Definition 4.4.1.** We define  $\text{Mor}(A, B)$  to be the set of morphisms between the varieties  $A$  and  $B$ , and  $\text{Mor}_k(A, B)$  to be the set of  $k$ -rational morphisms from  $A$  to  $B$ .

**Definition 4.4.2.** A *group variety* over  $k$  is a variety  $V$  together with  $k$ -morphisms

$$\begin{aligned} +: V \times V &\rightarrow V \\ -: V &\rightarrow V \\ 1: \text{Spec}(k) &\rightarrow V \end{aligned}$$

inducing a group structure on  $V(\bar{k})$ .

An abelian variety is a complete group variety [CS86, Chapter V]. Abelian varieties are nonsingular, projective and commutative, and the coordinate rings  $\mathcal{O}(U)$  are Hopf algebras for each open affine  $U \subset V$  (see [Wat79], [GM06, Example (3.9)]).

The Jacobian variety  $\text{Jac}(C)$  of a curve  $C/k$  is the abelian variety such that  $\text{Jac}(C)(k')$  is isomorphic to  $\text{Pic}^0(C/k)^{\text{Gal}(k'/k)}$  for every finite extension  $k'$  of  $k$  [CS86, Chapter VII, page 168]. If the curve  $C$  is defined over  $k$ , then  $\text{Jac}(C)$  is also defined over  $k$  and the dimension of  $\text{Jac}(C)$  is equal to the genus of  $C$ . After a careful study of the sections of  $\text{Jac}(C)$  and of the set of 2-torsion points, it is possible to give a set of 72 quadratic equations in 16 variables for  $\text{Jac}(C)$  [CF96]. A geometric interpretation of the Jacobian

variety of genus two curves as surfaces and the group law in geometric terms can be found in [CF96] and [GM06, Example (1.9)].

**Remark 4.4.3.** By Proposition 4.2.4 and Galois compatibility, we have

$$\mathrm{Jac}(C)(\bar{k}) \sim \underbrace{(C(\bar{k}) \times \cdots \times C(\bar{k}))}_{g \text{ times}} / \mathcal{S}_g$$

where  $\mathcal{S}_g$  is the symmetric group of permutations of  $g$  elements and  $\sim$  means birational equivalence.

**Remark 4.4.4.** The properties of  $C$  and  $\mathrm{Jac}(C)$  under base extension can be quite different over the range of fields  $k'$  from  $k$  to  $\bar{k}$ . For example, if  $C(k)$  contains an element  $e \in C(k)$  (see 4.1.7), then there exists a  $k$ -morphism  $C \rightarrow \mathrm{Jac}(C)$  sending  $e$  to the identity element of  $\mathrm{Jac}(C)$ , and such morphism does not necessarily exist if  $C(k)$  is empty [CS86, Chapter VII, page 168]. These different behaviours of  $C$  and  $\mathrm{Jac}(C)$  over the field extensions from  $k$  to  $\bar{k}$  have a direct impact on the solution of our DDH problem. Indeed, we will see below that depending on  $q$  and on the numbers of points  $\#C(\mathbb{F}_q)$  and  $\#C(\mathbb{F}_{q^2})$  of a genus two curve  $C$ , then the jacobian  $\mathrm{Jac}(C)$  sometimes “contains” elliptic curves over  $\mathbb{F}_q$  and sometimes doesn’t (see Sections 5.3, 5.5 and 5.6 in Chapter 5). This fact has a direct effect on the difficulty of exhibiting explicit distortion maps, and ultimately on the effectiveness of a solution to the DDH problem.

As far as the group operation is concerned, the law morphisms are given by Cantor’s algorithms of composition and reduction together with the isomorphisms between  $\mathrm{Jac}(C)$  and  $\mathrm{Pic}^0(C)$ .

## 4.5 Isogenies

We let  $\mathrm{Hom}(A, B)$  denote the set of abelian variety homomorphisms from  $A$  to  $B$ : that is, morphisms from  $A$  to  $B$  that are also group homomorphisms. We write  $\mathrm{Hom}_k(A, B)$  for the set of  $k$ -rational elements of  $\mathrm{Hom}(A, B)$ .

One may compose morphisms from an abelian variety to itself. This composition operation plus the law morphisms provide  $\mathrm{End}(A) = \mathrm{Hom}(A, A)$  with a ring structure which we will investigate in Chapter 5.

**Definition 4.5.1.** The surjective homomorphisms between abelian varieties of the same dimension are called *isogenies*. Two abelian varieties related via an isogeny are called *isogenous*. Two abelian varieties over  $k$  related via a  $k$ -rational isogeny are called isogenous *over  $k$*  or  *$k$ -isogenous*.

**Definition 4.5.2.** An abelian surface is said to *split* over  $k$  if it is  $k$ -isogenous to a product of abelian varieties of smaller dimension. An abelian variety  $A$  over  $k$  is  $k$ -*simple* if it does not split over  $k$ .  $\bar{k}$ -simple abelian varieties are called *simple*.

**Remark 4.5.3.** It is well known that an abelian variety is isogenous to a product of powers of nonisogenous simple abelian varieties (see [CS86, page 122] or [Tat66]).

**Remark 4.5.4.** We are going to work specifically with the endomorphism rings of  $\mathbb{F}_q$ -simple abelian varieties  $A$  that split over some finite extension of the ground field.  $\mathbb{F}_{q^k}$ .

**Definition 4.5.5.** The degree of an isogeny  $\varphi$  is the order  $n$  of its kernel or, equivalently, the degree of the induced function field extension  $n = [k(B) : \varphi^*(k(A))]$ . The isogeny is called separable or purely inseparable if the associated field extension  $k(B)/\varphi^*(k(A))$  is.

**Example 4.5.6.** Any nontrivial automorphism  $\phi$  of a curve  $C$  of genus  $> 1$  over a finite field with a point induces an isogeny  $\varphi$  of degree 1 on  $\text{Jac}(C)$  which is not the identity. This follows from the existence of the natural map  $C \rightarrow \text{Jac}(C)$  (see Remark 4.4.4) and the properties of the Jacobian.

**Example 4.5.7.** Consider the hyperelliptic involution  $\iota : C \rightarrow C$  of a curve of genus 2 given by  $y^2 = f(x)$ . Recall that for a point  $P$  with coordinates  $(x, y)$ ,  $\iota(P) = \iota((x, y)) = (x, -y)$  (see Section 2.2). By Proposition 4.2.4, any element  $D \in \text{Jac}(C)$  has an expression as  $D = P_1 + P_2 - 2P_\infty$ . As noted in Remark 4.2.6, any  $D$  corresponds to the integral ideal with coordinates

$$[(u - x(P_1))(u - x(P_2)), \frac{y(P_2)(u - x(P_1))}{x(P_2) - x(P_1)} + \frac{y(P_1)(u - x(P_2))}{x(P_1) - x(P_2)}].$$

The divisor  $D^\iota = \iota(P_1) + \iota(P_2) - 2\infty$  has coordinates

$$[(u - x(P_1))(u - x(P_2)), \frac{-y(P_2)(u - x(P_1))}{x(P_2) - x(P_1)} + \frac{-y(P_1)(u - x(P_2))}{x(P_1) - x(P_2)}].$$

So  $\iota$  at the level of divisors acts as  $[a, b] \rightarrow [a, -b]$ . The minimal polynomial of  $\iota$  over  $\mathbb{Q}$  (see Theorem 5.1.7) is  $(X + 1)$ . In the next chapter we will see that the characteristic polynomial of  $\iota$  is  $(X + 1)^4$ .

Note that  $D + D^\iota$  is a principal divisor, as in Example 4.2.5. Hence the divisor classes  $[D]$  and  $[D^\iota]$  are opposite in the group  $\text{Pic}^0(C)$ .

**Definition 4.5.8.** Let  $A$  be an abelian variety. We define  $n_A$  to be the endomorphisms of  $A$  given in terms of the morphism  $+$  as

$$\begin{aligned} n_A : A &\longrightarrow A \\ a &\longmapsto \underbrace{a + \dots + a}_n. \end{aligned}$$

The kernel of  $n_A$  is denoted  $A[n]$ , and it is a group subvariety of  $A$ .

**Theorem 4.5.9.** For  $n \neq 0$ , the morphism  $n_A : A \rightarrow A$  is an isogeny. If  $\dim(A) = g$ , then  $n_A$  has degree  $n^{2g}$ . If  $(\text{char}(k), n) = 1$  then  $n_A$  is separable.

*Proof.* See [CS86, Chapter V, Theorem 8.2] or [GM06, Proposition (5.9)]  $\square$

The next result provides a kind of inverse to every isogeny.

**Proposition 4.5.10.** Given any isogeny  $f : A \rightarrow B$  of degree  $n$ , then there always exists another isogeny  $f^\vee : B \rightarrow A$  such that the composition  $f^\vee f$  is  $n_A$  and  $f f^\vee$  is  $n_B$ .

*Proof.* A proof of this fact can be found in [GM06, Proposition (5.12)].  $\square$

**Definition 4.5.11.** The isogeny  $f^\vee$  of Proposition 4.5.10 above is called the *dual isogeny* of  $f$ .

**Proposition 4.5.12.** If  $(\text{char}(k), n) = 1$  then  $A[n](\bar{k}) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$ .

*Proof.* See [CS86, Chapter V, Remark 8.4] or [GM06, Corollary (5.11)]  $\square$

Let  $l$  be a prime, not equal to the characteristic of  $k$ . The subgroups  $A[l^m]$  inherit the natural  $\text{Gal}(\bar{k}/k)$ -action on the points. The groups  $A[l^m]$  together with the maps  $l_A : A[l^{m+1}] \rightarrow A[l^m]$  form a projective system compatible with the Galois action.

**Definition 4.5.13.** The *Tate module* is the projective limit

$$T_l A = \varprojlim_m A[l^m].$$

As the rank of all the members of the projective system is  $2g$  when  $l \neq p$ ,  $T_l A$  is a free  $\mathbb{Z}_l$ -module of rank  $2g$ , where  $\mathbb{Z}_l$  is the ring of  $l$ -adic integers. The endomorphisms of  $T_l A$  as a  $\mathbb{Z}_l$ -module for  $l \neq p$  are thus the matrices  $M_{2g}(\mathbb{Z}_l)$ .

**Remark 4.5.14.** When  $l$  is a prime different from  $p = \text{char}(k)$ , then Theorem (4.5.9) says that  $A[l]$  is the spectrum of an *étale*  $k$ -algebra (i.e. products of finite extensions of  $k$ ) or, in terms of schemes, that  $A[l]$  is an *étale*  $k$  group scheme. Étale group schemes over  $k$  form a category which is equivalent to the category of sets with  $\text{Gal}(\bar{k}/k)$ -action [GM06, Proposition (3.25)].

## 4.6 The Frobenius isogeny

For abelian varieties over fields of prime characteristic  $p$ , the structure of the  $p$ -torsion is different from the structure of the  $l$ -torsion. For such varieties a key role is played by the *Frobenius homomorphism*.

Let  $k$  be any finite field of characteristic  $p$  and let  $f$  be an (absolutely) irreducible polynomial over  $k$  in two variables  $x, y$ , monic in  $y$ . If  $f$  defines a nonsingular affine curve, then the quotient  $k[x, y]/(f)$  is a Dedekind domain and a  $k$ -algebra at the same time. We saw the examples  $\mathcal{O}_{C_f}$  in Chapter 2, and they correspond to nonsingular curves  $C$  over  $k$ .

As  $k$  is perfect, the polynomial  $f^{(p^m)}$  obtained raising the coefficients of  $f$  to the  $p$  power  $m$  times is also irreducible (for any  $m$ ) because raising to the  $p$  power is an automorphism in fields of characteristic  $p$ . The polynomial  $f^{(p^m)}$  defines a  $k$ -algebra  $\mathcal{O}_{C_{f^{(p^m)}}}$ . There is a well defined injective ring homomorphism

$$\begin{aligned} \varphi : \mathcal{O}_{C_{f^{(p^m)}}} &\rightarrow \mathcal{O}_{C_f} \\ [g(x, y)] &\mapsto [g(x^{p^m}, y^{p^m})]. \end{aligned}$$

Note that  $\varphi$  is defined over  $k$ . The image of this map is exactly  $(\mathcal{O}_{C_f})^{p^m}$ . Thus, the field of fractions of  $\mathcal{O}_{C_{f^{(p^m)}}}$  is  $k(\mathcal{O}_{C_f})^{p^m}$ , which is a subfield of  $k(C_f)$ .

The field  $k(\mathcal{O}_{C_f})^{p^m}$  is a function field, and thus the  $k$ -algebra  $\mathcal{O}_{C_{f^{(p^m)}}}$  corresponds to a nonsingular curve  $C^{(p^m)}$ . The function field extension  $k(\mathcal{O}_{C_f})/k(\mathcal{O}_{C_f})^{p^m}$  is purely inseparable of degree  $p^m$  [Lor96, Chapter X]. Hence  $\varphi$  is a homomorphism of  $k$ -algebras which is not the identity. This extension of function fields corresponds to a nontrivial morphism of curves  $C \rightarrow C^{(p^m)}$  defined over  $k$ .

**Definition 4.6.1.** The morphism of curves  $C \rightarrow C^{(p^m)}$  constructed above is called the  *$m$ -th Frobenius morphism*. For  $m = 1$  it is called the *relative Frobenius morphism*.

Let now  $q$  be the power  $p^n$  and let  $k$  be the field of  $q$  elements. Let  $C$  be a curve over  $k$  defined by some polynomial  $f$  over  $k$ . The image  $(\mathcal{O}_{C_f})^{p^n}$  of  $\mathcal{O}_{C_f}$  under the *absolute Frobenius* ring automorphism

$$\begin{aligned} \text{Frob} : \mathcal{O}_{C_f} &\rightarrow \mathcal{O}_{C_f} \\ \alpha &\mapsto (\alpha)^p \end{aligned}$$

iterated  $n$  times, is a  $k$ -subalgebra of  $\mathcal{O}_{C_f}$  because raising to the  $p$ -power is an automorphism of the field  $k$ . The ring  $(\mathcal{O}_{C_f})^{p^n}$  defines a function field. Call  $C^{(p^n)}$  the curve corresponding to  $(\mathcal{O}_{C_f})^{p^n}$ .

For any field of characteristic  $p$ ,  $n$ -times-absolute-Frobenius  $(\text{Frob})^n$  is a ring automorphism. Moreover, if  $k$  is the field of  $p^n$  elements, then  $(\text{Frob})^n$  is the identity on the coefficient ring  $k$  of  $\mathcal{O}_{C_f}$  as a  $k$ -algebra, and hence  $(\text{Frob})^n$  is an automorphism of  $k$ -algebras from  $\mathcal{O}_{C_f}$  to  $(\mathcal{O}_{C_f})^{p^n}$ .

One can define this  $k$ -algebra automorphism for every coordinate ring of every affine open set, and one can do so in a compatible way in the intersections, etc. One defines the homoemorphism in the set of points to be the identity. This defines a nontrivial endomorphism of curves  $C^{(p^n)} \rightarrow C$  defined over  $k$ .

**Definition 4.6.2.** The endomorphism above is called the  $q$ -power Frobenius endomorphism or also the *Frobenius over  $k$* .

In an analogous way, one can define the varieties  $X^{(p^m)}$  from a variety  $X$  over  $k$  and also define, as morphisms over  $k$ , the  $m$ -th Frobenius morphisms  $X \rightarrow X^{(p^m)}$ , which raise the coordinates to the  $p^m$ -th power. As before, this is called relative Frobenius morphism when  $m = 1$ .

As in dimension 1, the  $n$ -times-absolute-Frobenius ring automorphisms

$$\begin{aligned} (\text{Frob})^n : \mathcal{O}_X(U) &\rightarrow \mathcal{O}_X(U) \\ \alpha &\mapsto (\alpha)^{p^n} \end{aligned}$$

in the coordinate rings  $\mathcal{O}_X(U)$  of a variety  $X$  over  $k = \mathbb{F}_q$  are  $k$ -algebra automorphisms. Together with the identity at the level of points  $X(k)$ , these series of  $k$ -algebra homomorphisms correspond to an endomorphism of  $X$  called  $q$ -power Frobenius. It commutes with every morphism defined over  $k$ , including the group law of an abelian variety, so it is a well-defined endomorphism of Abelian varieties.

**Proposition 4.6.3.** *Let  $A$  be a  $g$ -dimensional abelian variety over a field  $k$  with  $\text{char}(k) = p > 0$ . Then the relative Frobenius homomorphism  $F_{A/k} : A \rightarrow A^{(p)}$  is a purely inseparable isogeny of degree  $p^g$ .*

*Proof.* [GM06, Proposition (5.15)]

□

**Remark 4.6.4.** The absolute Frobenius raises the sections (given in coordinates by rational maps) to the  $q$ -power. Raising the *coefficients* of these polynomials to the  $q$ -power is given the name *arithmetic* Frobenius. Raising the *variables* of these polynomials to the  $q$ -power is what the relative Frobenius does. Thus, the absolute Frobenius is the composition of the arithmetic Frobenius and the relative Frobenius. The inverse of the arithmetic Frobenius is usually called the *geometric* Frobenius and corresponds to taking  $q$ th roots to the coefficients. It is only defined over  $\bar{k}$ .

**Proposition 4.6.5.** *Let  $k$  be the field of  $q$  elements and  $A$  an abelian variety over  $k$ . Then  $q$ -power Frobenius induces the  $\text{Gal}(\bar{k}/k)$ -action in the Tate module  $T_l A$  for all  $l$  coprime to the characteristic of  $k$ .*

*Proof.* Recall that when  $k$  is the finite field of  $q$  elements then the automorphism  $x \mapsto x^q$  of  $\bar{k}$  is a topological generator of  $\text{Gal}(\bar{k}/k)$ . The action of  $\text{Gal}(\bar{k}/k)$  on  $A(\bar{k})$  provides  $T_l A$  with a Galois module structure. As  $q$ -power Frobenius on  $A(\bar{k})$  raises the coordinates of the points to the  $q$ -power,  $q$ -power Frobenius is the generator of the Galois action on  $T_l(A)$ .  $\square$

**Proposition 4.6.6.** *Let  $A$  be an abelian variety over  $k$  with  $\text{char}(k) = p > 0$ . Then there is an integer  $s = s(A)$ , with  $0 \leq s \leq g = \dim(A)$ , such that  $A[p^m](\bar{k}) \cong (\mathbb{Z}/p^m\mathbb{Z})^s$  for all  $m \geq 0$ .*

*Proof.* See [GM06, Proposition (5.21)]  $\square$

It is known that the number  $s$  in Proposition 4.6.6 above is independent of the field  $\mathbb{F}_p$  in the sense that  $f$  remains the same under base extension. The number  $s$  is called *the  $p$ -rank* of the abelian variety  $A$ . An abelian variety with  $p$ -rank zero is called *very special*. If  $s = g$  (so that  $\#A[p](\bar{k}) = p^g$ ) then  $A$  is called *ordinary*.

Let  $l$  be a prime not equal to the characteristic of  $k$ . The Galois action on the Tate module  $T_l A$  may be expressed using  $2g \times 2g$  matrices with coefficients in  $\mathbb{Z}_l$ . In what follows (see Theorem 5.2.6 below) we are going to work with  $T_l A$  for  $l \neq p$  and we are *not* going to work with the Tate module when  $l = p$ .

Elliptic curves are abelian varieties of dimension one. An elliptic curve  $E$  over  $\mathbb{F}_q$  is called a *supersingular* elliptic curve over  $\mathbb{F}_q$  if it has  $p$  rank zero. One extends the notion of supersingular elliptic curves to abelian varieties in the following way.

**Definition 4.6.7.** [Oor70] An abelian variety  $A$  over  $\mathbb{F}_q$  is called *supersingular* if  $A$  is isogenous over  $\bar{\mathbb{F}}_q$  to a product of supersingular elliptic curves. A curve  $C$  over  $\mathbb{F}_q$  is called *supersingular* if  $\text{Jac}(C)$  is supersingular.

In the next section we will see how to determine if an abelian variety  $A$  over  $k$  is supersingular. The following is a way to tell if the Jacobian variety of a curve  $C$  given by  $y^2 = f(x)$  with one point at infinity is ordinary or not purely in terms of the coefficients of  $f(x)$ .

**Definition 4.6.8.** The  $m$ -th Frobenius morphism on a curve  $C$  over a field  $\mathbb{F}_q$  of odd characteristic  $p$  induces a homomorphism in the first sheaf cohomology groups

$$H^1(C^{(p^m)}, (\mathcal{O}_f)^{p^m}) \rightarrow H^1(C, \mathcal{O}_f)$$

called the *Hasse-Witt* transformation of  $\text{Jac}(C_f)$ .

A matrix representation of this transformation (called *Cartier-Manin* matrix) for a genus 2 curve defined by a polynomial  $f$  of degree 5 is obtained as follows. Let  $c_i$  denote the coefficient of  $x^i$  in the polynomial  $f^{(p-1)/2}$ . Then the Cartier–Manin matrix of  $C$  is defined to be

$$\begin{pmatrix} c_{p-1} & c_{p-2} \\ c_{2p-1} & c_{2p-2} \end{pmatrix}$$

**Theorem 4.6.9.** *The jacobian of a genus two curve over a field  $k$  of  $q = p^n$  elements with  $p > 2$  with one point at infinity is ordinary if and only if*

$$\begin{pmatrix} c_{p-1} & c_{p-2} \\ c_{2p-1} & c_{2p-2} \end{pmatrix} \begin{pmatrix} c_{p-1}^p & c_{p-2}^p \\ c_{2p-1}^p & c_{2p-2}^p \end{pmatrix} \cdots \begin{pmatrix} c_{p-1}^{p^{n-1}} & c_{p-2}^{p^{n-1}} \\ c_{2p-1}^{p^{n-1}} & c_{2p-2}^{p^{n-1}} \end{pmatrix}$$

*is invertible.*

*Proof.* See [Yui78]. □

Further, one can determine the supersingularity of the Jacobian of a genus two curve from the Cartier–Manin matrix in some cases.

**Theorem 4.6.10.** *Let  $C$  be a hyperelliptic curve of genus two over  $\mathbb{F}_q$  with  $q = p^n$  and  $p > 2$ . Then*

- i) if  $C$  is supersingular, then  $c_{p+1} c_{2p} = c_p c_{2p+1}$ .*
- ii) if  $C$  is defined over a prime field  $\mathbb{F}_p$  then  $C$  is supersingular if and only if  $c_{p+1} c_{2p} = c_p c_{2p+1}$  and  $c_{p+1} + c_{2p} = 0$ .*

*Proof.* See [CJL00] □



## Chapter 5

# Structure of distortion maps

In this chapter we show that the structure of the endomorphism algebra of some supersingular curves is that of a crossed-product algebra. We describe the endomorphism algebras  $\text{End}^0(\text{Jac}(C))$  for some of the curves in Chapter 2. In our examples, we show that  $\text{End}^0(\text{Jac}(C))$  are 16-dimensional over  $\mathbb{Q}$ , that they contain a Galois subfield  $F$  of degree 4, and we exhibit an explicit  $F$ -basis. This is done in Theorem 5.2.6 and in Corollaries 5.2.9, 5.3.8, 5.3.11, 5.4.5, 5.4.8 and 5.5.11. The crossed-product algebra structure and the explicit  $F$ -basis allows us to give a solution to the Decisional Diffie-Hellman Problem in Chapter 6.

### 5.1 Endomorphisms

Let  $A$  be an abelian variety over a finite field  $k$ . Addition and composition of morphisms of abelian varieties provides the set

$$\text{End}(A) := \text{Hom}(A, A)$$

of endomorphisms of an abelian variety with a ring structure. The ring  $\text{End}(A)$  is called the full ring of endomorphisms. Recall that the morphisms need not necessarily be defined over the ground field  $k$ .

The subset  $\text{End}_k(A)$  of endomorphisms defined over  $k$  forms a subring in  $\text{End}(A)$ . The endomorphisms  $n_A$  are defined over  $k$  (since the law morphism  $+$  is defined over  $k$ ). Hence  $\text{End}_k(A)$  contains a subring isomorphic to  $\mathbb{Z}$ .

**Remark 5.1.1.** Given any extension of fields  $k'/k$  then

$$\text{End}_k(A) \subseteq \text{End}_{k'}(A) \subseteq \text{End}_{\bar{k}}(A).$$

The isogenies  $n_A$  are *not* invertible elements of  $\text{End}(A)$  in general, because they have a finite kernel (see [CS86, Chapter V, page 115], [GM06, Proposition (5.2)]). It is convenient to work in a ring where the elements  $n_A$  are invertible. As  $\mathbb{Z}$  is naturally in  $\text{End}_k(A)$ , a natural way to construct such a ring is  $\text{End}^0(A) := \text{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ . This  $\mathbb{Q}$ -algebra is called the full algebra of endomorphisms.

**Remark 5.1.2.** Note that  $\text{End}^0(A)$  may contain zero divisors. The existence of zero divisors in  $\text{End}^0(A)$  is related to  $A$  failing to be  $k$ -simple (see Section 5.6).

**Remark 5.1.3.** The following is well known (see [CS86, Chapter V, §12.]).

- i) For any abelian variety  $A$ ,  $\text{End}^0(A)$  is a semisimple algebra over  $\mathbb{Q}$ .
- ii) If  $A$  is a simple abelian variety, then  $\text{End}^0(A)$  is a skewfield.
- iii) If  $A$  is a power of a simple abelian variety, then  $\text{End}^0(A)$  is a matrix algebra over a skewfield.

**Proposition 5.1.4.** *Any isogeny  $\varphi \in \text{End}(A)$  of an abelian variety  $A$  of dimension  $g$  generates a field in  $\text{End}^0(A)$ .*

*Proof.* Let  $n$  be the degree of  $\varphi$ . Then the elements  $\varphi \otimes 1$  and  $\varphi^\vee \otimes 1/n^{2g}$  are multiplicative inverses one of each other in  $\text{End}^0(A)$  by Proposition 4.5.10. The  $\mathbb{Q}$ -algebra generated by  $\varphi$  is commutative because it is a simple extension. Hence it is a field.  $\square$

**Remark 5.1.5.** If  $\varphi$  is an endomorphism of an abelian variety  $A$ , we should write  $\varphi \otimes 1$  for the corresponding element in  $\text{End}^0(A)$ . However, from now on this will be implicitly understood and we will simply write  $\varphi$  for  $\varphi \otimes 1$ .

The subrings  $\text{End}_k(A)$  are orders in the semisimple algebra  $\text{End}^0(A)$ . We will give examples of such orders in Sections 5.3 and 5.4. In the case of elliptic curves, Deuring [Deu41] showed that if  $E$  is ordinary then  $\text{End}(E)$  is an order in an imaginary quadratic extension, and that if  $E$  is supersingular then  $\text{End}(E)$  is an order in a quaternion algebra.

We show an example of a supersingular curve  $C$  of genus 2 such that  $\text{End}^0(\text{Jac}(C))$  is central, simple and contains a Galois extension  $F/\mathbb{Q}$  of degree 4. Then  $\text{End}^0(\text{Jac}(C))$  is a crossed-product algebra over  $F$  (see Corollary 5.2.9) and we solve DDH in this case. Later we give an example of a supersingular curve of genus 2 such that  $\text{End}^0(\text{Jac}(C))$  is simple and contains a subfield of degree 4, but is not central. We solve DDH in this case as well.

**Proposition 5.1.6.**  $\text{End}^0(A)$  has dimension at most  $(2\dim(A))^2$  over  $\mathbb{Q}$ .

*Proof.* As  $\text{End}(A) \hookrightarrow \text{End}_{\mathbb{Z}_l}(T_l A)$ , one can show that  $\text{End}(A) \otimes \mathbb{Z}_l \rightarrow \text{End}(T_l A)$  is injective [CS86, Chapter V, Theorem 12.5]. In particular  $\text{End}(A)$  is free  $\mathbb{Z}$ -module of rank  $\leq (2\dim(A))^2$  and the claim follows. See also [GM06, Chapter XII, Corollary (12.10)].  $\square$

We will show below that the subring  $\text{End}_K(A)$  of  $\text{End}(A)$  formed by the endomorphisms defined over a certain extension  $K$  of the ground field  $k$  has rank exactly  $(2\dim(A))^2$  when  $A$  is supersingular (Theorem 5.2.6).

**Theorem 5.1.7** (Characteristic polynomials). *Any endomorphism  $f$  of an abelian variety  $A$  of dimension  $g$  satisfies a polynomial of degree  $2g$  with integer coefficients.*

*Proof.* (Sketch) The degree map on endomorphisms is a homogeneous polynomial function of degree  $2g$  and extends naturally to  $\text{End}^0(A)$  [CS86, Chapter V, Proposition 12.4]. The function  $X \mapsto \deg(X - \alpha)$  is therefore equal to  $X \mapsto P_\alpha(X)$  for some polynomial  $P_\alpha$  of degree  $2g$ . The function  $P_\alpha(X)$  coincides with the characteristic polynomial of  $\alpha$  acting on the  $\mathbb{Q}_l$ -vector space  $V_l := T_l A \otimes \mathbb{Q}_l$ . The determinant and trace of the matrix representation  $\rho_l \in GL_{2g}(\mathbb{Q}_l)$  of  $\alpha$  in  $V_l$  are independent of  $l$ , so they are really in  $\mathbb{Q}$ . For elements in  $\text{End}(A)$  the norm and trace lie in  $\mathbb{Z}$ .  $\square$

**Remark 5.1.8.** Let  $\pi_A$  be the Frobenius endomorphism of an abelian variety  $A$  over  $k$ . Evaluating the characteristic polynomial  $P_{\pi_A}(X)$  of  $\pi_A$  at 1, we obtain  $\#A(k)$ . This is because the Frobenius endomorphism  $\pi_A$  of the abelian variety  $A$  over  $k$  is the identity at the level of  $k$ -rational points and because the degree of a separable isogeny is the order of its kernel.

The characteristic polynomial  $P_\pi(X)$  encodes a lot of information about an abelian variety. For example, supersingular elliptic curves satisfy the following series of equivalent characterizations, many of them due to Deuring.

**Theorem 5.1.9.** *Let  $k$  be a the field of  $q = p^n$  elements and let  $E$  be an elliptic curve over  $k$ . Let  $\pi$  be the Frobenius endomorphism of  $E$ . Then the following statements are equivalent.*

- i)  $E[p^r] = \{0\}$  for all  $r \geq 1$ .
- ii) The dual of  $\pi$  is purely inseparable.
- iii) The trace of the characteristic polynomial of  $\pi$  is divisible by  $p$ .

v)  $\text{End}(E)$  is an order in a quaternion algebra.

vi) There exists an integer  $\kappa$  such that  $\pi^\kappa = \pm q^{\kappa/2}$ .

*Proof.* [Sil86, Chapter V, Theorem 3.1] □

In dimension bigger than one,  $P_{\pi_A}(X)$  describes the splitting behaviour of  $A$ , and one also knows how to read supersingularity in any dimension from  $P_{\pi_A}(X)$ . We later use the following results.

**Theorem 5.1.10.** *Let  $P_\pi(X)$  be the characteristic polynomial of the Frobenius endomorphism of a supersingular abelian variety defined over  $\mathbb{F}_q$ . Then  $P_\pi(X/\sqrt{q})$  is a cyclotomic polynomial.*

*Proof.* See [Man63]. □

**Remark 5.1.11.** It follows that if  $P_\pi(X)$  is the characteristic polynomial of the Frobenius endomorphism of a supersingular abelian variety defined over a finite field and is irreducible, then it generates a Galois extension of  $\mathbb{Q}$ . Note also that the roots of  $P_\pi(X)$  are  $\sqrt{q}$  times a root of unity  $\xi$  in the supersingular case. Hence the roots of  $P_\pi(X)$  raised to the order of  $\xi$  are a power of  $\sqrt{q}$ .

**Theorem 5.1.12.** *The following conditions on an abelian variety  $A$  over  $\mathbb{F}_q$  of dimension  $g$  are equivalent.*

i)  $A$  is isogenous (over some finite extension of  $\mathbb{F}_q$ ) to  $E^g$  for some supersingular elliptic curve  $E$  (i.e.,  $A$  is supersingular).

ii) There is some integer  $\kappa$  such that the characteristic polynomial of Frobenius on  $A$  over  $\mathbb{F}_{q^\kappa}$  is  $P(X) = (X \pm q^{\kappa/2})^{2g}$ .

iii) There is some integer  $\kappa$  such that  $\pi^\kappa = \pm q^{\kappa/2}$ .

iv) For some positive integer  $\kappa$  we have  $\#A(\mathbb{F}_{q^\kappa}) = (q^{\kappa/2} \pm 1)^{2g}$

*Proof.* This follows from Theorem 5.1.9 above and Tate's isogeny Theorem. □

**Definition 5.1.13.** We call the smallest integer  $\kappa$  from the Theorem above the *Frobenius-to-integer* exponent of the supersingular abelian variety  $A$ . We call the extension  $k'$  of the base field  $k$  for which the Frobenius endomorphism of  $A$  becomes an integer, the *Frobenius-to-integer* extension.

**Remark 5.1.14.** Note that “becomes an integer” in the above definition means that it is an endomorphism obtained as composition of several times the law morphism  $+$ . Note that  $\kappa$  is  $\text{ord}(\xi)$  if  $q$  is a square and  $\text{ord}(\xi)/\text{gcd}(2, \text{ord}(\xi))$  if not.

**Definition 5.1.15.** The exponent  $c_A := \kappa/2$  is called the *cryptographic exponent* of the supersingular abelian variety  $A$ , and  $c_A/\dim(A)$  is called the *security parameter* of  $A$ .

Rubin and Silverberg [RS02] show that if  $A$  is  $\mathbb{F}_q$ -simple and supersingular then the exponent of  $A(\mathbb{F}_q)$  divides  $q^{c_A} - 1$ . They also show the following.

**Theorem 5.1.16** (Rubin and Silverberg). *Assume  $A$  is a  $\mathbb{F}_q$ -simple supersingular abelian variety over  $\mathbb{F}_q$ ,  $l$  is a prime number,  $l \mid \#A(\mathbb{F}_q)$  and  $l$  does not divide  $\kappa$ . Then  $c_A$  is the smallest half-integer  $k$  such that  $q^k - 1$  is an integer divisible by  $l$ .*

*Proof.* See [RS02]. □

The cryptographic exponent and the security parameter may in this way be generalized to other Jacobian varieties.

**Definition 5.1.17.** Let  $C$  be a curve over a finite field  $\mathbb{F}_q$  of  $q = p^n$  elements. Let  $l$  be a prime number satisfying  $l \mid \#\text{Jac}(C)(\mathbb{F}_q)$ . The *embedding degree* of the curve  $C$  is the smallest integer  $k$  such that  $l \mid q^k - 1$ .

**Remark 5.1.18.** Alternatively, the embedding degree may be defined to be the degree of the extension  $\mathbb{F}_{q^k}$  generated over  $\mathbb{F}_q$  adjoining the  $l$ -th roots of unity.

**Theorem 5.1.19.** *If  $q = p^n$  and  $A$  is an abelian variety of dimension  $g$  over  $\mathbb{F}_q$  and*

$$P_\pi(X) = X^{2g} + a_1X^{2g-1} + a_2X^{2g-2} + \dots + a_gX^g + \dots + q^{g-1}a_1X + q^g$$

*is the characteristic polynomial of the Frobenius endomorphism on  $A$ , then  $A$  is supersingular if and only if  $p^{\lceil rn/2 \rceil} \mid a_r$  for all  $1 \leq r \leq g$ .*

*Proof.* See [SX95]. □

Moreover, if an abelian variety  $A$  over  $\mathbb{F}_q$  is the Jacobian variety of some curve  $C$  of genus  $g$  over  $\mathbb{F}_q$ , then knowing the number of points of  $C$  over the range of fields from  $\mathbb{F}_q$  to  $\mathbb{F}_{q^g}$  is equivalent to knowing the coefficients  $a_i$  in  $P_\pi(X)$ . Usually the points over the range of fields from  $\mathbb{F}_q$  to  $\mathbb{F}_{q^g}$  are given

the name  $N_1, N_2, \dots, N_g$ . In genus two the relationship between the  $a_i$ 's and the  $N_i$ 's is

$$N_1 = q + 1 + a_1, N_2 = q^2 + 1 + 2a_2 - a_1^2.$$

**Remark 5.1.20.** It is very difficult to determine if an arbitrary abelian surface  $A$  is or is not the Jacobian of a curve of genus two.

In [Gal01] Galbraith gives many examples of supersingular curves of genus two over fields of even characteristic.

**Theorem 5.1.21.** *Let  $C$  be a genus 2 curve over  $\mathbb{F}_{2^n}$  of the form  $y^2 + y = f(x)$  where  $f(x)$  is monic of degree 5. Then  $C$  is supersingular.*

*Proof.* [Gal01, Theorem 9.1] □

## 5.2 Tate's theorem

In this section we recall an important theorem of Tate. We show that Tate's theorem implies that supersingular abelian varieties have an endomorphism algebra that is as large as possible, that is, they are  $(2g)^2$ -dimensional over  $\mathbb{Q}$  (see Proposition 5.1.6). The  $\mathbb{Q}$ -algebra  $\text{End}^0(\text{Jac}(C))$  is then a crossed-product algebra if it is central, simple and contains a subfield which is Galois and of degree  $2g$  over  $\mathbb{Q}$ . The endomorphism algebra  $\text{End}^0(\text{Jac}(C))$  may contain several maximal subfields, which may or may not be isomorphic. If  $\text{End}^0(\text{Jac}(C))$  is central, simple and as large as possible, then for every maximal subfield  $F$  in  $\text{End}^0(\text{Jac}(C))$ ,  $\text{End}^0(\text{Jac}(C))$  admits a crossed-product algebra structure over  $F$ . Below we show examples of central simple algebras  $\text{End}^0(\text{Jac}(C))$  as big as possible containing two maximal subfields, one cyclic and one non-cyclic.

We later show a non-central simple algebra containing one non-cyclic subfield of degree 4. The existence of central simple algebras that contain only non-cyclic maximal fields is prohibited by Class Field Theory. Indeed, as a consequence of the Grunwald–Wang Theorem, every central simple algebra over a number field contains a cyclic maximal subfield (see [Pie82, page 359]).

Let  $A$  be an abelian variety over a finite field  $k$  of characteristic  $p$ . Let  $G = \text{Gal}(\bar{k}/k)$ . Let  $l$  be a prime such that  $l \neq p$  and let  $T_l(A)$  be the Tate module of  $A$ . Recall that  $\text{End}_k(A)$  denotes the ring of homomorphisms from  $A$  to itself which are defined over  $k$ . Define  $\text{End}_G(T_l(A))$  to be the ring of homomorphisms from  $T_l(A)$  to itself which commute with the action of  $G$ .

**Theorem 5.2.1.** (Tate) *The canonical map*

$$\mathrm{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Z}_l \rightarrow \mathrm{End}_G(T_l(A))$$

*is a bijection.*

*Proof.* See [Tat66]. □

As a consequence of this theorem, Tate gave the following application.

**Theorem 5.2.2.** *Let  $A$  and  $B$  be abelian varieties over a finite field  $k$ , and let  $P_{\pi_A}(X)$  and  $P_{\pi_B}(X)$  be the characteristic polynomials of their Frobenius endomorphisms relative to  $k$ . Then the following statements are equivalent:*

- i)  $B$  is  $k$ -isogenous to an abelian subvariety of  $A$  defined over  $k$ .*
- ii)  $V_l(B)$  is  $\mathrm{Gal}(\bar{k}/k)$ -isomorphic to a  $\mathrm{Gal}(\bar{k}/k)$ -subspace of  $V_l(A)$  for some  $l$ .*
- iii)  $P_{\pi_B}(X)$  divides  $P_{\pi_A}(X)$*

*Proof.* See [Tat66, page 139]. □

**Corollary 5.2.3.** *If the characteristic polynomial of the Frobenius endomorphism of  $\mathrm{Jac}(C)$  is irreducible then  $\mathrm{Jac}(C)$  is  $k$ -simple and  $\mathrm{End}^0(\mathrm{Jac}(C))$  contains a field of degree  $2g$  over  $\mathbb{Q}$ .*

*Proof.* The Frobenius endomorphism  $\pi$  is an isogeny (see Section 4.6) and together with the dual, it generates a field  $\mathbb{Q}(\pi)$  in  $\mathrm{End}^0(\mathrm{Jac}(C))$ . If the characteristic polynomial of Frobenius is irreducible, then the field  $\mathbb{Q}(\pi)$  is an extension of  $\mathbb{Q}$  of degree  $2g$  because of Theorem 5.1.7. The equivalence between *i)* and *iii)* in Theorem 5.2.2 shows that the characteristic polynomial of the Frobenius endomorphism  $\pi$  of an abelian variety  $A$  which splits over  $k$  (see Definition 4.5.2), splits as a product of other two characteristic polynomials of abelian varieties of smaller dimension. Hence, if the characteristic polynomial of Frobenius does not split in any way, then  $A$  cannot split over  $k$  and is thus  $k$ -simple. □

**Remark 5.2.4.** The field generated by the Frobenius endomorphism  $\pi$  is in fact a subfield of  $\mathrm{End}_k^0(\mathrm{Jac}(C))$ , since the Frobenius endomorphism is defined over  $k$ .

**Remark 5.2.5.** If  $C$  is supersingular, then Theorem 5.1.10 implies that the field generated by Frobenius is a Galois extension of  $\mathbb{Q}$ . Note also that any isogeny with irreducible characteristic polynomial generates a field of degree  $2g$  in the endomorphism algebra.

The following result is due to Weil, Deuring and Tate. Recall the definition of the Frobenius-to-integer exponent (Theorem 5.1.12). Let  $\kappa$  denote the Frobenius-to-integer exponent, and let  $K = \mathbb{F}_{q^\kappa}$  be the Frobenius-to-integer extension of  $k$ .

**Theorem 5.2.6.** *Let  $C$  be a supersingular curve of genus  $g$  over  $\mathbb{F}_q$ . Then  $\text{End}(\text{Jac}(C))$  has rank  $(2g)^2$  as a  $\mathbb{Z}$ -module.*

*Proof.*  $\text{Jac}(C)$  is supersingular and defined over  $\mathbb{F}_q$ . Let  $G = \text{Gal}(\bar{K}/K)$ . Call  $\text{Jac}(C)^\kappa$  the abelian variety  $\text{Jac}(C)$  over  $K$ . Recall that the endomorphisms of  $\text{Jac}(C)$  defined over  $K$  become rational in  $\text{Jac}(C)^\kappa$ .

By Tate's theorem on  $\text{Jac}(C)^\kappa$ ,  $\text{End}_K(\text{Jac}(C)^\kappa) \otimes_{\mathbb{Z}} \mathbb{Z}_l$  is isomorphic to  $\text{End}_G(T_l(\text{Jac}(C)^\kappa))$ . Note that  $T_l(\text{Jac}(C)) \cong T_l(\text{Jac}(C)^\kappa)$  and that the generator of  $\text{Gal}(\bar{k}/K)$  is the  $\kappa$ -th power of the generator of  $\text{Gal}(\bar{k}/k)$ . Hence the Frobenius endomorphism relative to  $K$  is the  $\kappa$ -th power of the Frobenius endomorphism relative to  $k$ .

Since  $l \neq p$ , the endomorphism algebra  $\text{End}(T_l(\text{Jac}(C)^\kappa))$  is isomorphic to  $M_{2g}(\mathbb{Z}_l)$ , and the subset  $\text{End}_G(T_l(\text{Jac}(C)^\kappa))$  is a subset of  $M_{2g}(\mathbb{Z}_l)$ . This is also holds for  $T_l(\text{Jac}(C))$ .

As  $\text{Jac}(C)$  is supersingular,  $\text{End}(\text{Jac}(C)) \otimes_{\mathbb{Z}} \mathbb{Z}_l$  has rank  $(2g)^2$  as a  $\mathbb{Z}_l$ -module. We have the commutative diagram with the vertical arrows injective (see Remark 5.1.6):

$$\begin{array}{ccc}
 \text{End}_K(\text{Jac}(C)) \otimes_{\mathbb{Z}} \mathbb{Z}_l & \xrightarrow[\cong]{\text{Tate}} & \text{End}_G(T_l(\text{Jac}(C)^\kappa)) \\
 \cong \downarrow & & \cong \downarrow \\
 \text{End}_K(\text{Jac}(C)^\kappa) \otimes_{\mathbb{Z}} \mathbb{Z}_l & & \text{End}_G(T_l(\text{Jac}(C))) \\
 \varphi \downarrow & & \downarrow \varphi \\
 \\ \\
 \text{End}(\text{Jac}(C)^\kappa) \otimes_{\mathbb{Z}} \mathbb{Z}_l & \xrightarrow[\cong]{\text{supersingular}} & \text{End}_{\mathbb{Z}_l}(T_l(\text{Jac}(C))) \\
 \cong \downarrow & & \cong \downarrow \\
 \text{End}(\text{Jac}(C)) \otimes_{\mathbb{Z}} \mathbb{Z}_l & & M_{2g}(\mathbb{Z}_l)
 \end{array}$$

Since  $\text{Jac}(C)$  is supersingular, the Frobenius endomorphism of  $\text{Jac}(C)^\kappa$  relative to the Frobenius-to-integer extension  $K$  is the integer multiplication-by- $-q^{\kappa/2}$  endomorphism because it is the  $\kappa$ -th power of the Frobenius endomorphism in  $\text{Jac}(C)$ , and so it commutes with any other endomorphism.

As Frobenius is the generator of the Galois action in the Tate module, it follows that

$$\text{End}_G(T_l(\text{Jac}(C)^\kappa)) \cong M_{2g}(\mathbb{Z}_l).$$

Hence by Tate's Theorem  $\text{End}_K(\text{Jac}(C)) \otimes_{\mathbb{Z}} \mathbb{Z}_l$  has rank  $(2g)^2$  as a  $\mathbb{Z}_l$ -module. Over the Frobenius-to-integer extension  $K$  the diagram above becomes

$$\begin{array}{ccc} \text{End}_K(\text{Jac}(C)) \otimes_{\mathbb{Z}} \mathbb{Z}_l & \xrightarrow[\text{Tate}]{\cong} & M_{2g}(\mathbb{Z}_l) \\ \varphi \downarrow & & \downarrow \cong \\ \text{End}(\text{Jac}(C)) \otimes_{\mathbb{Z}} \mathbb{Z}_l & \xrightarrow[\text{supersingular}]{\cong} & M_{2g}(\mathbb{Z}_l) \end{array}$$

Hence  $\text{End}_K(\text{Jac}(C)) \cong \text{End}(\text{Jac}(C))$  has rank  $(2g)^2$  as a  $\mathbb{Z}$ -module and the claim follows.  $\square$

**Remark 5.2.7.** Note that by restriction we have

$$\text{End}_K(\text{Jac}(C)) \otimes_{\mathbb{Z}} \mathbb{Z}/l\mathbb{Z} \cong M_{2g}(\mathbb{Z}/l\mathbb{Z}).$$

This gives a way of representing the endomorphisms of the  $l$ -torsion of  $\text{Jac}(C)$ . See some examples in Chapter 6.

**Remark 5.2.8.** Note that over the Frobenius-to-integer extension  $\mathbb{F}_{q^k}$ , the characteristic polynomial of the Frobenius endomorphism of the abelian variety  $\text{Jac}(C)^k$  splits into linear factors, but we are not concerned about this because we are working with the variety defined over the ground field  $\mathbb{F}_q$ .

**Corollary 5.2.9.** *Let  $\text{Jac}(C)$  be the jacobian of a supersingular curve of genus  $g$  over  $k = \mathbb{F}_q$ . Suppose  $\varphi$  is an endomorphism of  $\text{Jac}(C)$  such that the characteristic polynomial  $P_{\varphi}(X)$  is irreducible and  $\mathbb{Q}(\varphi)$  is a Galois extension of  $\mathbb{Q}$ . If  $\text{End}^0(\text{Jac}(C))$  is central and simple, then it is a Crossed-product algebra over  $\mathbb{Q}(\varphi)$ .*

*Proof.* If the characteristic polynomial of the endomorphism  $\varphi$  of  $\text{Jac}(C)$  is irreducible, the endomorphism  $\varphi$  generates a number field  $\mathbb{Q}(\varphi)$  of degree  $2g$  in  $\text{End}^0(\text{Jac}(C))$ . By Theorem 5.2.6, as  $C$  is supersingular,  $\text{End}^0(\text{Jac}(C))$  has rank  $(2g)^2$  as a  $\mathbb{Z}$ -module, and  $\text{End}^0(\text{Jac}(C))$  is a  $(2g)^2$ -dimensional  $\mathbb{Q}$ -algebra. Hence the  $\mathbb{Q}$ -algebra  $\text{End}^0(\text{Jac}(C))$  is simple, central and contains a Galois subfield of degree equal to the square root of its dimension. By the definition of crossed-product algebra in Chapter 3 (see Definition 3.5.1), the  $\mathbb{Q}$ -algebra  $\text{End}^0(\text{Jac}(C))$  is a crossed-product algebra over  $\mathbb{Q}(\varphi)$ .  $\square$

**Remark 5.2.10.** Note that the subfield of  $\text{End}^0(A)$  generated by an isogeny may or may not be maximal. In the next sections we will see two different examples of abelian surfaces  $\text{Jac}(C)$  where the Frobenius endomorphism

satisfies an irreducible characteristic polynomial in both cases. Hence  $\text{Jac}(C)$  is  $\mathbb{F}_q$ -simple by Corollary 5.2.3. However, in one example there are isogenies that generate other maximal subfields (see Section 5.3) and in the other example there are isogenies that do not generate subfields of the highest possible degree (see Section 5.5).

### 5.3 A family of supersingular curves

In the next two sections we give examples of curves  $C$  of genus two over finite fields for which the endomorphism algebra  $\text{End}^0(\text{Jac}(C))$  is a crossed-product algebra containing both a cyclic and a non-cyclic maximal subfield. We exhibit generators of  $\text{End}^0(\text{Jac}(C))$  both as a cyclic and a non-cyclic algebra.

Recall that crossed-product algebras  $(F, \text{Gal}(F/\mathbb{Q}), f)$  have the structure

$$F \oplus u_1F \oplus u_2F \oplus u_3F$$

and the  $u_i$ 's are invertible elements acting on  $F$  by conjugation as elements of  $\text{Gal}(F/\mathbb{Q})$ . The  $u_i$ 's thus reflect the structure of the group  $\text{Gal}(F/\mathbb{Q})$ . Recall that a crossed-product algebra is called cyclic if  $\text{Gal}(F/\mathbb{Q})$  is cyclic and non-cyclic if  $\text{Gal}(F/\mathbb{Q})$  is non-cyclic. Recall that once a central simple algebra contains a cyclic maximal subfield then it may also contain non-cyclic maximal subfields. In our setting, the  $u_i$ 's are isogenies in  $\text{End}^0(\text{Jac}(C))$ .

The next examples are obtained as supersingular reduction of the CM curves over  $\mathbb{Q}$  listed in [Wam99a]. The CM fields in [Wam99a] are generated by the characteristic polynomial of an isogeny  $\varphi$ , and  $\mathbb{Q}(\varphi)/\mathbb{Q}$  is a cyclic extension. This is the reason why the endomorphism algebras in the next examples do admit a cyclic crossed-product algebra structure over the CM field  $\mathbb{Q}(\varphi)$ . On the other hand, when the Frobenius endomorphism  $\pi$  does also generate a maximal field, then supersingularity and the CM structure of the field  $\mathbb{Q}(\varphi)$  force the Galois group of the characteristic polynomial of the Frobenius endomorphism to be non-cyclic. In such cases,  $\text{End}^0(\text{Jac}(C))$  admits also a non-cyclic crossed-product algebra structure over  $\mathbb{Q}(\pi)$ . We first deal with an obvious example of a CM curve in genus two. We then deal with Van Wamelen's examples.

For the remainder of this section,  $q = p$  is a prime such that  $p \equiv 2, 3 \pmod{5}$ . Let  $A$  be a nonzero rational number and consider the curve

$$\tilde{C}: y^2 = x^5 + A$$

over  $\mathbb{Q}$ . Reducing  $\tilde{C}$  modulo  $p$  one obtains a curve  $C$  defined over  $\mathbb{F}_p$ .

Let  $\xi_5$  be a fifth root of unity. The curve  $\tilde{C}$  has the automorphism  $(x, y) \mapsto (\xi_5 x, y)$  which we call  $\xi_5$ . This automorphism extends to give an element of  $\text{End}(\text{Jac}(\tilde{C}))$  which we again call  $\xi_5$ . Moreover, since  $p \not\equiv 1 \pmod{5}$  then  $\xi_5$  reduces to a nonrational endomorphism of  $\text{Jac}(C)$  which we call  $\xi_5$  yet again. The map  $\xi_5$  provides the reduced curve  $C$  over  $\mathbb{F}_p$  with complex multiplication. As we have the point-wise description of  $\xi_5$ , it is straightforward to implement  $\xi_5$  as an endomorphism with Magma, using the Mumford representation of the elements in  $\text{Jac}(C)$  (see Algorithm A.0.4).

**Remark 5.3.1.** We are interested in finding distortion maps to solve the Decisional Diffie-Hellman Problem in the Jacobian variety of genus two curves. The automorphism  $\xi_5$  was first used as a distortion map by Choie and Lee [CL04].

We next show that the powers of the  $p$ -power Frobenius map  $\pi$  and the automorphism  $\xi_5$  generate the full algebra of endomorphisms.

**Lemma 5.3.2.** *If  $p \equiv 2, 3 \pmod{5}$  then  $\text{Jac}(C)$  is supersingular, the characteristic polynomial of the Frobenius endomorphism in  $\text{Jac}(C)$  is irreducible, and generates a Galois extension of  $\mathbb{Q}$ . Further,  $\text{Jac}(C)$  has embedding degree equal to 4.*

*Proof.* Since 5 is coprime to  $p - 1$  it follows that, for every  $y \in \mathbb{F}_p$ , there is a unique value  $x = (y^2 - A)^{1/5}$ . Hence, since  $C$  has a single point at infinity,  $N_1 = \#C(\mathbb{F}_p) = p + 1$ . Since 5 is also coprime to  $p^2 - 1$  we obtain  $N_2 = \#C(\mathbb{F}_{p^2}) = p^2 + 1$ .

Hence, the characteristic polynomial of the  $p$ -power Frobenius endomorphism  $\pi \in \text{End}(\text{Jac}(C))$  is  $P(T) = T^4 + p^2$  (see paragraph after Theorem 5.1.19). It is easy to show that this polynomial is irreducible over  $\mathbb{Z}$ . Moreover, its roots are  $\sqrt{p}$  times an eighth root of unity as predicted in Theorem 5.1.10. Hence the Frobenius endomorphism generates a Galois extension of  $\mathbb{Q}$ . Theorem 5.1.19 also implies that  $C$  is supersingular. If  $l \mid \#\text{Jac}(C)(\mathbb{F}_p) = p^2 + 1$  then  $l \mid p^4 - 1$  and so the embedding degree is  $k = 4$ .  $\square$

**Remark 5.3.3.** It can be checked that, while  $\text{Jac}(C)$  is  $\mathbb{F}_p$ -simple, it is not  $\mathbb{F}_{p^4}$ -simple. On the other hand, if  $p \equiv 1 \pmod{5}$  then  $C$  is ordinary.

Write  $\mathbb{Z}[\xi_5, \pi]$  for the non-commutative ring generated over  $\mathbb{Z}$  by the endomorphisms  $\xi_5$  and  $\pi$ . By definition,  $\mathbb{Z}[\xi_5, \pi] \subseteq \text{End}(\text{Jac}(C))$ . In fact  $\mathbb{Z}[\xi_5, \pi] \subseteq \text{End}_{\mathbb{F}_{p^4}}(\text{Jac}(C))$ .

**Lemma 5.3.4.** *For  $p \not\equiv 1 \pmod{5}$  and  $j \in \{0, 1, 2, 3\}$  we have*

$$\xi_5 \pi^j = \pi^j \xi_5^{(p^j)^{-1}}.$$

*Proof.* In the ring  $\text{End}(\text{Jac}(C)) \otimes_{\mathbb{Z}} \mathbb{Q}$ , for  $j \in \{0, 1, 2, 3\}$ ,  $(\pi^j)^{-1} \xi_5 \pi^j$  is a fifth root of unity. Indeed, by considering the explicit equations we determine that

$$(\pi^j)^{-1} \xi_5 \pi^j : (x, y) \longmapsto ((\xi_5 x^{p^j})^{1/p^j}, (y^{p^j})^{1/p^j}) = (\xi_5^{1/p^j} x, y).$$

and so the precise root is  $(\xi_5)^{1/p^j}$ .  $\square$

Recall that if  $p \equiv 2, 3 \pmod{5}$ , then the CM isogeny  $\xi_5$  generates a subfield of degree 4. Moreover, the characteristic polynomial of  $\xi_5$  is  $x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$  and this is a cyclotomic polynomial. Therefore  $\xi_5$  generates a Galois extension of  $\mathbb{Q}$ .

We next illustrate Theorem 5.2.6 to the curve  $C$ . We show that  $\text{End}^0(\text{Jac}(C))$  admits a crossed-product algebra structure over  $\mathbb{Q}(\xi_5)$  if  $p \equiv 2, 3 \pmod{5}$ , and we exhibit a  $\mathbb{Q}(\xi_5)$ -basis. The subfield generated by  $\xi_5$  will be a maximal subfield.

By Proposition 5.1.1,  $\text{End}_{\mathbb{F}_{p^4}}(\text{Jac}(C))$  contains the  $\mathbb{F}_p$ -rational endomorphisms  $\text{End}_{\mathbb{F}_p}(\text{Jac}(C))$ . Hence  $\text{End}_{\mathbb{F}_{p^4}}(\text{Jac}(C))$  contains the Frobenius endomorphism  $\pi$  of  $\text{Jac}(C)$ . Note that  $\text{End}_{\mathbb{F}_{p^4}}(\text{Jac}(C))$  also contains the endomorphism  $\xi_5$  because  $\xi_5$  lies in  $\mathbb{F}_{p^4}$ . Hence  $\text{End}_{\mathbb{F}_{p^4}}(\text{Jac}(C)) \otimes_{\mathbb{Z}} \mathbb{Q}$  is a  $\mathbb{Q}$ -algebra containing the fields generated by the endomorphisms  $\pi$  and  $\xi_5$ . We will show that the rank of  $\text{End}_{\mathbb{F}_{p^4}}(\text{Jac}(C))$  as a  $\mathbb{Z}$ -module is 16. This implies that the dimension of  $\text{End}^0(\text{Jac}(C))$  over  $\mathbb{Q}$  is 16 as predicted in Theorem 5.2.6.

Write  $\mathbb{Q}[\xi_5, \pi]$  for the non-commutative algebra  $\mathbb{Z}[\xi_5, \pi] \otimes_{\mathbb{Z}} \mathbb{Q}$ .

**Proposition 5.3.5.** *Let  $p \equiv 2, 3 \pmod{5}$ . Then  $\mathbb{Q}[\xi_5, \pi] = \mathbb{Q}(\xi_5) \oplus \pi \mathbb{Q}(\xi_5) \oplus \pi^2 \mathbb{Q}(\xi_5) \oplus \pi^3 \mathbb{Q}(\xi_5)$  as  $\mathbb{Q}$ -vector spaces.*

*Proof.* We will prove that for every  $0 \leq r \leq 3$  the sum  $\bigoplus_{i=0}^r \pi^i \mathbb{Q}(\xi_5)$  is direct. For  $r = 0$  there is nothing to prove. For  $r \geq 1$ , we assume we have a direct sum  $U_t = \bigoplus_{i=0}^t \pi^i \mathbb{Q}(\xi_5)$  for  $0 \leq t < r$  and we make the following claim: for every  $j > t$  then  $U_t \cap \pi^j \mathbb{Q}(\xi_5) = \{0\}$ . If we can prove this claim then the claim follows.

Suppose the contrary:  $U_t \cap \pi^j \mathbb{Q}(\xi_5) \neq \{0\}$ . Then  $\pi^j \mathbb{Q}(\xi_5)$  contains a nonzero element  $\pi^j z \in U_t$ , for some nonzero  $z \in \mathbb{Q}(\xi_5)$ . This means  $\pi^j \in U_t$  and hence we can write  $\pi^j = z_0 + \pi z_1 + \dots + \pi^t z_t$  with  $z_k \in \mathbb{Q}(\xi_5)$  for  $0 \leq k \leq t$  and some  $z_k \neq 0$ . By Lemma 5.3.4 we have

$$\begin{aligned}
0 &= \xi_5 \pi^j - \pi^j \xi_5^{(p^j)^{-1}} \\
&= \xi_5 z_0 + \xi_5 \pi z_1 + \dots + \xi_5 \pi^t z_t - z_0 \xi_5^{(p^j)^{-1}} - \pi z_1 \xi_5^{(p^j)^{-1}} - \dots - \pi^t z_t \xi_5^{(p^j)^{-1}} \\
&= z_0 \xi_5 + \pi z_1 \xi_5^{p^{-1}} + \dots + \pi^t z_t \xi_5^{(p^t)^{-1}} - z_0 \xi_5^{(p^j)^{-1}} - \pi z_1 \xi_5^{(p^j)^{-1}} - \dots - \pi^t z_t \xi_5^{(p^j)^{-1}} \\
&= z_0 (\xi_5 - \xi_5^{(p^j)^{-1}}) + \pi z_1 (\xi_5^{p^{-1}} - \xi_5^{(p^j)^{-1}}) + \dots + \pi^t z_t (\xi_5^{(p^t)^{-1}} - \xi_5^{(p^j)^{-1}}).
\end{aligned}$$

Since  $\xi_5^{[p^k]^{-1}} \neq \xi_5^{[p^j]^{-1}}$  for  $1 \leq k \leq t < j$  (because we are assuming  $p \equiv 2, 3 \pmod{5}$  and not  $p \equiv 4 \pmod{5}$ ), and since  $U_t$  is a direct sum, this implies that  $z_0 = z_1 = \dots = z_t = 0$  which is a contradiction.

Compare with Albert's work [Alb39].

□

**Remark 5.3.6.** Note we are using  $p \equiv 2, 3 \pmod{5}$  to obtain a contradiction, and that such primes are inert in the extension  $\mathbb{Q}(\xi_5)/\mathbb{Q}$ . We will show below that this is far from a mere coincidence. By Lemma 5.3.4, conjugation by  $\pi$  is a generator of  $\text{Gal}(\mathbb{Q}(\xi_5)/\mathbb{Q})$  if  $p \equiv 2, 3 \pmod{5}$ .

**Corollary 5.3.7.** *Let  $p \equiv 2, 3 \pmod{5}$ . Then  $\text{End}^0(\text{Jac}(C)) = \mathbb{Q}[\xi_5, \pi]$  and*

$$\mathbb{Q}[\xi_5, \pi] \cong \left\{ \sum_{0 \leq i, j \leq 3} \lambda_{i,j} \pi^i \xi_5^j : \lambda_{i,j} \in \mathbb{Q} \right\}.$$

*Proof.* We know that  $\text{End}^0(\text{Jac}(C))$  is a 16-dimensional  $\mathbb{Q}$ -algebra at most. As  $\dim_{\mathbb{Q}} \mathbb{Q}(\xi_5) = 4$ , Proposition 5.3.5 implies that the dimension of  $\mathbb{Q}[\xi_5, \pi]$  is 16. As  $\mathbb{Q}[\xi_5, \pi]$  is contained in  $\text{End}^0(\text{Jac}(C))$ , the result follows.

The claim about the structure of  $\mathbb{Q}[\xi_5, \pi]$  also follows from Proposition 5.3.5 since  $\{1, \xi_5, \xi_5^2, \xi_5^3\}$  is a  $\mathbb{Q}$ -basis for  $\mathbb{Q}(\xi_5)$ . □

**Corollary 5.3.8.** *If  $p \equiv 2, 3 \pmod{5}$ ,  $\text{End}^0(\text{Jac}(C))$  admits a crossed-product algebra structure over  $\mathbb{Q}(\xi_5)$  with  $\mathbb{Q}(\xi_5)$ -basis  $\{1, \pi, \pi^2, \pi^3\}$ .*

*Proof.* By Proposition 5.3.5 above,  $\text{End}^0(\text{Jac}(C))$  is 16 dimensional over  $\mathbb{Q}$  and contains the Galois subfield  $\mathbb{Q}(\xi_5)$  of degree 4. By Lemma 5.3.4, it is a central  $\mathbb{Q}$ -algebra, so  $\mathbb{Q}(\xi_5)$  is a maximal subfield. The claim about the basis follows also from Proposition 5.3.5. □

**Remark 5.3.9.** Note that the  $\mathbb{Q}(\xi_5)$ -basis  $\{1, \pi, \pi^2, \pi^3\}$  of  $\mathbb{Q}[\xi_5, \pi]$  is a cyclic basis. This reflects the cyclic structure of  $\text{Gal}(\mathbb{Q}(\xi_5)/\mathbb{Q})$ , because the units  $\{1, \pi, \pi^2, \pi^3\}$  act as elements of  $\text{Gal}(\mathbb{Q}(\xi_5)/\mathbb{Q})$  by conjugation. Note that  $\pi^2$  acts on  $\mathbb{Q}(\xi_5)$  by conjugation as complex conjugation.

**Corollary 5.3.10.** *If  $p \equiv 2, 3 \pmod{5}$  then conjugation by the elements  $1, \pi, \pi^2, \pi^3$  is a set of generators of  $\text{Gal}(\mathbb{Q}(\xi_5)/\mathbb{Q})$ .*

*Proof.* This follows from the structure of crossed-product algebras and the previous Corollary.  $\square$

In addition to the cyclic crossed-product algebra determined by the field generated by the endomorphism  $\xi_5$ , the algebra  $\text{End}^0(\text{Jac}(C))$  admits also a non-cyclic crossed-product structure where the maximal field is given by the Frobenius endomorphism. The only remaining task is to exhibit the  $\mathbb{Q}(\pi)$ -basis. Eventhough we use the previous one, we may use both structures to solve DDH.

**Corollary 5.3.11.**  *$\text{End}^0(\text{Jac}(C))$  admits a crossed-product algebra structure over  $\mathbb{Q}(\pi)$ , and*

$$\{1, (2\xi_5 + 2\xi_5^{-1} + 1), \xi_5 - p\xi_5^2\pi^2 + p\xi_5^3\pi^2, (2\xi_5 + 2\xi_5^{-1} + 1)(\xi_5 - p\xi_5^2\pi^2 + p\xi_5^3\pi^2)\}$$

*is a  $\mathbb{Q}(\pi)$ -basis for  $\text{End}^0(\text{Jac}(C))$ .*

*Proof.* The fact that  $\text{End}^0(\text{Jac}(C))$  is a crossed-product algebra over  $\mathbb{Q}(\pi)$  follows from Lemma 5.3.2 above and Corollary 5.2.9. Hence a  $\mathbb{Q}(\pi)$ -basis for  $\text{End}^0(\text{Jac}(C))$  exists because of Theorem 3.6.4. Let us now exhibit such a basis.

The characteristic polynomial of the endomorphism  $\xi_5$  is  $x^4 + x^3 + x^2 + x + 1$ , which is irreducible of degree 4. The field generated by  $\xi_5$  is a CM field, and thus contains a totally real subfield  $\mathbb{Q}(\frac{5+\sqrt{5}}{2})$  with defining polynomial  $x^2 - 5x + 5$ . The minimal polynomial in  $\mathbb{Q}(\frac{5+\sqrt{5}}{2})$  of both the elements  $\beta := -\xi_5^2 - \xi_5^3 = \frac{1+\sqrt{5}}{2}$  and  $\bar{\beta} := -\xi_5 - \xi_5^4 = \frac{1-\sqrt{5}}{2}$  is  $x^2 - x - 1$ , and we have  $\beta\bar{\beta} = -1$ .

Note that by Lemma 5.3.4,  $\beta$  and  $\bar{\beta}$  are conjugate under the action of Frobenius. In fact, we have

$$\begin{aligned} \beta\pi &= -\xi_5^2\pi - \xi_5^3\pi = -\pi\xi_5^{2p-1} - \pi\xi_5^{3p-1} \\ &= \pi(-\xi_5 - \xi_5^4) = \pi\bar{\beta} \end{aligned}$$

since we are assuming  $p \equiv 2, 3 \pmod{5}$ .

This implies that the  $\mathbb{Q}$ -algebra  $\mathbb{Q}[\beta, \pi]$  is 8-dimensional over  $\mathbb{Q}$ . Note that  $\sqrt{5}$ ,  $\beta$  and  $\bar{\beta}$  all lie in the same field and  $\pi\sqrt{5} = -\sqrt{5}\pi$ . This shows that the action of  $\sqrt{5}$  by conjugation in the field  $\mathbb{Q}(\pi)$  is

$$x \longmapsto -x$$

and we take  $\sqrt{5}$  as the first nontrivial element of the  $\mathbb{Q}(\pi)$ -basis for  $\text{End}^0(\text{Jac}(\mathbb{C}))$ . Note that complex conjugation permutes the roots of  $X^4 + p^2$ . To exhibit the full  $\mathbb{Q}(\pi)$ -basis for  $\text{End}^0(\text{Jac}(\mathbb{C}))$  we need to find an element whose action by conjugation in  $\mathbb{Q}(\pi)$  is

$$x \longmapsto \bar{x}.$$

But if  $\pi$  is a root of  $X^4 + p^2$  then  $\bar{\pi} = -\pi^3/p$ . Notice that here we are using the fact that  $X^4 + p^2$  is almost a cyclotomic polynomial (see Theorem 5.1.10). We are looking for an invertible element  $\alpha \in \text{End}^0(\text{Jac}(\mathbb{C}))$  such that

$$\alpha\pi\alpha^{-1} = -\frac{\pi^3}{p}.$$

From Proposition 5.3.5 above, there exist sixteen rational numbers  $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, r \in \mathbb{Q}$  such that

$$\begin{aligned} \alpha &= a + b\pi + c\pi^2 + d\pi^3 + e\xi_5 + f\xi_5\pi + g\xi_5\pi^2 + h\xi_5\pi^3 + i\xi_5^2 \\ &\quad + j\xi_5^2\pi + k\xi_5^2\pi^2 + l\xi_5^2\pi^3 + m\xi_5^3 + n\xi_5^3\pi + o\xi_5^3\pi^2 + r\xi_5^3\pi^3. \end{aligned}$$

Moreover, the action by the elements of  $\mathbb{Q}(\pi)$  upon  $\alpha$  on the right and on the left permutes the  $\mathbb{Q}$ -basis. Indeed,

$$\begin{aligned} \alpha\pi &= -p^2d + a\pi + b\pi^2 + c\pi^3 - p^2h\xi_5 + e\xi_5\pi + f\xi_5\pi^2 + g\xi_5\pi^3 - p^2l\xi_5^2 \\ &\quad + i\xi_5^2\pi + j\xi_5^2\pi^2 + k\xi_5^2\pi^3 - p^2r\xi_5^3 + m\xi_5^3\pi + n\xi_5^3\pi^2 + r\xi_5^3\pi^3 \end{aligned}$$

and

$$\begin{aligned} \frac{\pi^3\alpha}{p} &= (pj - pb) + (pk - pc)\pi + (pl - pd)\pi^2 + \left(\frac{a-i}{p}\right)\pi^3 \\ &\quad + (pj - pn)\xi_5 + (pk - po)\xi_5\pi + (pl - pr)\xi_5\pi^2 + \left(\frac{m-i}{p}\right)\xi_5\pi^3 \\ &\quad + (pj - pf)l\xi_5^2 + (pk - pg)\xi_5^2\pi + (pl - ph)\xi_5^2\pi^2 + \left(\frac{e-i}{p}\right)\xi_5^2\pi^3 \\ &\quad + (pj)\xi_5^3 + (pk)\xi_5^3\pi + (pl)\xi_5^3\pi^2 + \left(\frac{-i}{p}\right)\xi_5^3\pi^3. \end{aligned}$$

We are thus lead to solve a homogeneous linear system with matrix

$$\begin{pmatrix} 0 & -p & 0 & -p^2 & 0 & 0 & 0 & 0 & 0 & p & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & -p & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -p & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p & p & p & p \\ \frac{1}{p} & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \frac{-1}{p} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -p^2 & 0 & p & 0 & 0 & 0 & -p & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & p & 0 & 0 & 0 & -p \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & p & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \frac{-1}{p} & 0 & 0 & 0 & \frac{1}{p} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -p & 0 & 0 & 0 & p & 0 & -p^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -p & 0 & 1 & 0 & p & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -p & 0 & 1 & 0 & p & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{p} & 0 & 0 & 0 & \frac{-1}{p} & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p & 0 & 0 & 0 & 0 & -p^2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{-1}{p} & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

and kernel

$$\langle \xi_5 - p\xi_5^2\pi^2 + p\xi_5^3\pi^2, \xi_5\pi - p\xi_5^2\pi^3 + p\xi_5^3\pi^3, \xi_5\pi^2 + \frac{1}{p}\xi_5^2 - \frac{1}{p}\xi_5^3, \xi_5\pi^3 + \frac{1}{p}\xi_5^2\pi - \frac{1}{p}\xi_5^3\pi \rangle.$$

□

## 5.4 Families of supersingular curves

The automorphisms of the curve in the previous section are just a particular case of isogenies in the Jacobian variety. In this section we derive completely analogous results for other CM isogenies  $\varphi$ .

Up to isomorphism there are exactly 18 more curves  $C$  of genus two over  $\mathbb{Q}$  with Complex Multiplication by an order in a CM field  $F$  of degree 4 [Wam99a], [Wam99b].

**Example 5.4.1.** The Jacobian variety of the first curve of [Wam99a],

$$\tilde{C}_{vw1} : y^2 = x^5 - 3x^4 - 2x^3 + 6x^2 + 3x - 1$$

over  $\mathbb{Q}$ , has an endomorphism algebra which contains the ring of integers of the number field  $\mathbb{Q}(z)$  where  $z^4 + 4z^2 + 2 = 0$ .

As in the previous section, reducing the coefficients of  $\tilde{C}_{vw1}$  modulo certain primes  $p$ , one obtains supersingular curves  $C$  over a finite field whose Jacobian has endomorphism ring isomorphic to an order in the CM-field  $\mathbb{Q}(z)$ .

The description of the primes of supersingular reduction for CM curves of genus two can be found in [Gor97] and [GHKRW05]. The abelian variety  $\bar{A}$  obtained after reduction modulo a rational prime  $p$  depends on the splitting behaviour of the ideal generated by  $p$  in the CM field  $F$  with totally real subfield  $F_0$ .

**Theorem 5.4.2.** *With the notation as above, then*

- i) *if  $p$  splits completely in  $F$ , then  $\bar{A}$  is ordinary and has complex multiplication by the ring of integers of  $F$ .*
- ii) *if  $p$  is unramified, inert or splits only in  $F_0/\mathbb{Q}$  but not any further, then  $\bar{A}$  is supersingular. The same is true if  $p$  ramifies completely, if  $(p) = \mathfrak{p}^2$  and if  $(p) = \mathfrak{p}_1\mathfrak{p}_2^2$  but  $p$  does not ramify in  $F_0/\mathbb{Q}$ .*
- iii) *if  $p$  splits into three prime ideals, then  $\bar{A}$  has  $p$ -rank 1 and the same is true if  $(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^2$ .*
- iv) *if  $p$  is inert in  $F_0/\mathbb{Q}$  but splits in  $F/F_0$ , then  $\bar{A}$  is supersingular or ordinary with complex multiplication by  $\mathcal{O}_F$ , and the same happens if  $(p) = \mathfrak{p}_1^2\mathfrak{p}_2^2$  where  $p$  ramifies in the extension  $F_0/\mathbb{Q}$ .*

*Proof.* See [GHKRW05], [Gor97]. □

**Proposition 5.4.3.** *Assume  $F/\mathbb{Q}$  is a Galois extension. If  $p$  is inert in  $F$  with inertia degree  $f$ , then  $\text{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p) \cong \text{Gal}(F/\mathbb{Q})$ .*

*Proof.* This is standard and can be found for example in [Neu99]. Let  $p$  be a rational prime. As  $F/\mathbb{Q}$  is Galois, the decomposition of the ideal  $p\mathcal{O}_F$  into prime ideals is

$$p\mathcal{O}_F = (\mathfrak{p}_1 \dots \mathfrak{p}_r)^e$$

with  $4 = efr$ , where  $e$  is the ramification degree,  $r$  is the number of different primes and  $f = [\mathcal{O}_L/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}]$  is the inertia degree. Let  $G := \text{Gal}(F/\mathbb{Q})$ . The decomposition subgroup at a prime  $\mathfrak{p}$  is

$$D_{\mathfrak{p}} = \{\sigma \in G \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}$$

and the inertia subgroup at  $\mathfrak{p}$  is

$$I_{\mathfrak{p}} = \ker(D_{\mathfrak{p}} \rightarrow \text{Gal}((\mathcal{O}_F/\mathfrak{p})/(\mathbb{Z}/p\mathbb{Z}))).$$

It is well known that  $|G/D_{\mathfrak{p}}| = r$ ,  $|D_{\mathfrak{p}}| = ef$  and  $|I_{\mathfrak{p}}| = e$ . It is also well known that if  $e = 1$  then  $D_{\mathfrak{p}}$  is isomorphic to  $\mathcal{G} := \text{Gal}((\mathcal{O}_L/\mathfrak{p})/(\mathbb{Z}/p\mathbb{Z}))$  and, moreover, in such a case the Frobenius automorphism

$$\sigma_{\mathfrak{p}}(a) = a^p \bmod \mathfrak{p}$$

is a canonical generator for  $D_{\mathfrak{p}}$ . Thus in the unramified case the group  $\mathcal{G}$  can be thought of as a subgroup of  $G$ . Hence, if  $r = 1$  then  $D_{\mathfrak{p}} \cong G$ .  $\square$

**Proposition 5.4.4.** *The characteristic polynomial  $P_{\pi}(X)$  of the Frobenius endomorphism of the reduction at an inert prime  $p$  of the Jacobian of the curves  $\tilde{C}$  over  $\mathbb{Q}$  with CM by a cyclic CM field of order 4 is  $X^4 + p^2$ .*

*Proof.* This follows from [Lan83, Chapter 4, Theorem 6.2].  $\square$

With Theorem 5.4.2 one knows when a curve  $\tilde{C}$  in Van Wamelen's list reduces to a supersingular curve  $C$  over a finite field. With Proposition 5.4.3 we can generalize the results of the previous section.

**Theorem 5.4.5.** *Let  $p$  be a rational prime inert in the quartic CM field  $\mathbb{Q}(\varphi)$ . Then the endomorphism algebra of the Jacobian variety of the reduction modulo  $p$  of a curve  $\tilde{C}$  over  $\mathbb{Q}$  with CM by the cyclic extension  $\mathbb{Q}(\varphi)$ , admits a crossed-product algebra structure over  $\mathbb{Q}(\varphi)$  and a  $\mathbb{Q}(\varphi)$ -basis for  $\text{End}^0(\text{Jac}(C))$  is given by  $\{1, \pi, \pi^2, \pi^3\}$ .*

*Proof.* By Theorem 5.4.2,  $\text{Jac}(C)$  is supersingular. We have the relation

$$\pi\varphi\pi^{-1} = (\varphi)^p$$

where  $(\varphi)^p$  is the endomorphism obtained from  $\varphi$  by conjugating its coefficients by the Frobenius automorphism  $x \mapsto x^p \in \text{Gal}(\mathbb{F}_{p^4}/\mathbb{F}_p)$ . It now follows from Proposition 5.4.3 above that if  $p$  is inert then conjugation by  $\pi$  has order four and the analogous proofs as in Proposition 5.3.5 and Corollary 5.3.8 above apply.  $\square$

**Corollary 5.4.6.** *Let  $p$  be rational prime inert in a quartic cyclic CM field  $\mathbb{Q}(\varphi)$  as above. Then  $\text{End}^0(\text{Jac}(C)) = \mathbb{Q}[\varphi, \pi]$  and*

$$\mathbb{Q}[\varphi, \pi] \cong \left\{ \sum_{0 \leq i, j \leq 3} \lambda_{i,j} \pi^i \varphi^j : \lambda_{i,j} \in \mathbb{Q} \right\}.$$

*Proof.* We know that  $\text{End}^0(\text{Jac}(C))$  is an at most 16-dimensional  $\mathbb{Q}$ -algebra. As  $\dim_{\mathbb{Q}} \mathbb{Q}(\varphi) = 4$ , Theorem 5.4.5 implies that  $\mathbb{Q}[\varphi, \pi]$  is also 16-dimensional. As  $\mathbb{Q}[\varphi, \pi]$  is contained in  $\text{End}^0(\text{Jac}(C))$  the result follows.

The claim about the structure of  $\mathbb{Q}[\varphi, \pi]$  also follows from Proposition 5.4.5 since  $\{1, \varphi, \varphi^2, \varphi^3\}$  is a  $\mathbb{Q}$ -basis for  $\mathbb{Q}(\varphi)$ .  $\square$

**Proposition 5.4.7.** *Let  $p$  be a rational prime inert in the CM field  $\mathbb{Q}(\varphi)$  as above. Then there exists an isogeny  $\rho$  in  $\text{End}^0(\text{Jac}(C))$  which acts by conjugation in  $\mathbb{Q}(\pi)$  as the complex conjugation  $x \mapsto \bar{x}$ .*

*Proof.* By Proposition 5.4.4, the characteristic polynomial of  $\pi$  is  $X^4 + p^2$ . The set of roots of this polynomial is fixed under complex conjugation, and if  $\pi$  is one of them then  $\bar{\pi} = -\pi^3/p$ . Since in a crossed-product algebra over  $\mathbb{Q}(\pi)$  the elements of a  $\mathbb{Q}(\pi)$ -basis act by conjugation as elements of  $\text{Gal}(\mathbb{Q}(\pi)/\mathbb{Q})$ , there must exist an element  $\rho$  such that  $\rho\pi\rho^{-1} = \bar{\pi}$ . Writing these elements in terms of the full  $\mathbb{Q}$ -basis provided by Theorem 5.4.5, one translates the previous equation into the solvable linear system  $\rho\pi\rho^{-1} = -\pi^3/p$ .  $\square$

**Corollary 5.4.8.** *Let  $p$  be a rational prime inert in the CM field  $\mathbb{Q}(\varphi)$  as above. Then  $\text{End}^0(\text{Jac}(C))$  admits a crossed-product algebra structure over  $\mathbb{Q}(\pi)$ . Write  $\Delta$  for the discriminant of the totally real subfield of  $\mathbb{Q}(\varphi)$  and  $\rho$  for the isogeny which acts by conjugation in  $\mathbb{Q}(\pi)$  as complex conjugation  $x \mapsto \bar{x}$ . Then a  $\mathbb{Q}(\pi)$ -basis for  $\text{End}^0(\text{Jac}(C))$  is given by  $\{1, \Delta, \rho, \Delta\rho\}$ .*

*Proof.* The field  $\mathbb{Q}(\pi)$  is generated by the polynomial  $X^4 + p^2$  and is thus a quartic extension over  $\mathbb{Q}$  and Galois. The field  $\mathbb{Q}(\pi)$  lies naturally inside the central simple algebra  $\text{End}^0(\text{Jac}(C))$ , which is 16-dimensional by Theorem 5.4.5. Hence  $\text{End}^0(\text{Jac}(C))$  is a crossed-product algebra over  $\mathbb{Q}(\pi)$ . A  $\mathbb{Q}(\pi)$ -basis for  $\text{End}^0(\text{Jac}(C))$  exists because of Theorem 3.6.4. Similarly as in Corollary 5.3.11, the discriminant  $\Delta$  and  $\pi$  do not commute, and the claimed element  $\rho$  in the  $\mathbb{Q}(\pi)$ -basis exists by Proposition 5.4.7 above.  $\square$

The roots of the CM polynomials of any other quartic, cyclic CM field are analogous to the endomorphism  $\xi_5$  in the previous section. In each curve of van Wamelen's list the CM-isogeny  $\varphi$  induced in the Jacobian is computable. Indeed in [Wam99a], [Wam99b] the expression of the first coordinate of  $\varphi$  was calculated. With help of Magma, the second coordinate, and thus the whole CM-isogeny, is explicitly computable over  $\mathbb{Q}$ , and this provides a source of examples of isogenies over finite fields reducing modulo a prime.

**Example 5.4.9.** Take the first curve in van Wamelen's list:

$$\tilde{C}: y^2 = x^5 - 3x^4 - 2x^3 + 6x^2 + 3x - 1.$$

Van Wamelen showed that the endomorphisms of the Jacobian of this curve contains the ring of integers of the CM field  $F$  given by  $z^4 + 4z^2 + 2$ . He exhibited the first coordinate of an isogeny  $\varphi \in \mathcal{O}_F$ , i.e. the description of the first Mumford coordinate of the image under  $\varphi$

$$\varphi(D) = P_1 + P_2 - 2\infty \in \text{Jac}(C), P_1 = (x_1, y_1), P_2 = (x_2, y_2)$$

(see Section 4.2) of a divisor of the form

$$D = P - \infty \in \text{Jac}(C), P = (x, y).$$

He gave the trace  $s_1$  and norm  $s_2$  functions of the first coordinate  $a(u) = u^2 + s_1(x)u + s_2(x)$  of  $\varphi(D) = [a(u), b(u)]$  in terms of  $x$ . For the curve  $\tilde{C}$ , the  $s_i(x)$  are

$$s_1(x) = (4 + z^2 + x(-2 - z^2)), s_2(x) = (2 + x^2 + z^2 + x(-4 - z^2)).$$

Of course one recovers  $x_1$  and  $x_2$  as  $s_1 = x_1 + x_2$ ,  $s_2 = x_1x_2$ . With Magma it is easy to find also the second coordinates  $y_1, y_2$  of  $\varphi(D)$ , now in terms both of  $x$  and  $y$ , for each curve of van Wamelen's list. For the curve  $\tilde{C}$ , the  $y_i$ 's are

$$y_1(x, y) = 1/2(-z^3 - 4z)y/(x+1)x_1 + (1/2(-z^3 - 4z)xy + (z^3 + 3z)y)/(x+1)$$

$$y_2(x, y) = 1/2(-z^3 - 4z)y/(x+1)x_1 + (1/2(-z^3 - 2z)xy + (z^3 + 4z)y)/(x+1)$$

In this way, one can calculate the second coordinate  $b(u)$  and give  $\varphi$  explicitly as a transformation in Mumford coordinates

$$\alpha : [u - x, v - y] \mapsto [(u - x_1)(u - x_2), v - \left(\frac{y_2(u - x_1)}{(x_2 - x_1)} + \frac{y_1(u - x_2)}{(x_1 - x_2)}\right)]$$

which one can easily plug into Magma and obtain mod  $l$  representations of  $\varphi$ , for  $l$  a prime dividing the order of  $\text{Jac}(C)(\mathbb{F}_q)$ .

**Remark 5.4.10.** Working out  $b(u)$  from  $y_1$  and  $y_2$  is not straightforward. In some curves of van Wamelen’s list, sometimes the right  $b(u)$  is obtained interpolating  $[x_1, x_2]$  at  $[y_1, -y_2]$  for example, and not at  $[y_1, y_2]$  as one would expect.

**Remark 5.4.11.** The expression of the CM isogeny can be much more complicated than the one above. For example, the CM isogeny for the sixth curve in van Wamelen’s list requires twenty pages long to write down. It has degree 61.

Before Theorem 5.4.2 appeared, Theorems 4.6.9 or 4.6.10 helped to determine whether the reduced curve modulo a chosen prime  $p$  is supersingular, if Frobenius is irreducible, and if the CM isogeny still satisfies an irreducible polynomial of degree 4. Magma allows us to check all this quite easily (see Algorithms A.0.6 and A.0.7).

**Example 5.4.12.** Consider the curve

$$C_{vw1} : y^2 = x^5 - 3x^4 - 2x^3 + 6x^2 + 3x - 1$$

over  $\mathbb{F}_p$  obtained from the curve  $\tilde{C}_{vw1}$  in van Wamelen’s list [Wam99a] after reduction modulo an inert prime  $p$ . The algorithms A.0.8 and A.0.9 implement the CM-isogeny of  $\text{Jac}(C_{vw1})$ .

**Remark 5.4.13.** The fact that no other cyclic CM-polynomial of degree 4 has constant term equal to 1 (see [Wam99a]), shows that none of the curves in [Wam99a] reduce to a supersingular curve of genus 2 over a finite field with a non-rational automorphism except for  $y^2 = x^5 + 1$ .

## 5.5 A non-central example in even characteristic

While in the last two sections we showed examples of curves  $C$  such that  $\text{End}^0(\text{Jac}(C))$  admitted a double structure as a crossed-product algebra (with the Galois group of the maximal field being cyclic in one case and non-cyclic in the other), in this section we show an example of a supersingular curve of genus two whose Jacobian has an endomorphism algebra that contains a single non-cyclic subfield of degree 4. This subfield is given by the Frobenius endomorphism. For this curve, all the “extra” isogenies satisfy reducible characteristic polynomials, and they generate fields of degree strictly smaller than 4. The algebra  $\text{End}(\text{Jac}(C))$  in this section is not a crossed product because it is not central. The subfield of degree 4, eventhough Galois, is not properly a maximal subfield because we defined maximal subfields only for central simple algebras.

We consider the curve  $C : y^2 + y = x^5 + x^3 + 1$  over  $\mathbb{F}_{2^m}$ . This curve has been studied extensively (see [GV92a], [GV92b], [Gal01], [MN04]) and is of great interest for cryptographers (see [BGOS04]).

**Proposition 5.5.1.**  $C : y^2 + y = x^5 + x^3 + 1$  over  $\mathbb{F}_{2^m}$  is supersingular (for every  $m$ ).

*Proof.* This follows from Theorem 5.1.21. □

Over fields of even characteristic, it is known that the only curves of genus 2 with non- $\mathbb{F}_{2^m}$ -rational automorphisms are exactly those in the case (5) in Table 2.8 of Chapter 2. This follows from [Puj02], where the automorphisms of the other cases were calculated.

In this section we will describe the endomorphism algebra of the Jacobian variety of  $C$  over  $\mathbb{F}_{2^m}$  with  $m \equiv \pm 1 \pmod{6}$ .

**Proposition 5.5.2.** The non- $\mathbb{F}_{2^m}$ -rational automorphisms of the curve  $C : y^2 + y = x^5 + x^3 + 1$  over  $\mathbb{F}_{2^m}$  are given by

$$\sigma_\omega : (x, y) \mapsto (x + \omega, y + s_2x^2 + s_1x + s_0)$$

where  $\omega$  is any root of the linear separable polynomial  $x^{16} + x^8 + x^2 + x$ ,  $s_2 := \omega^8 + \omega^4 + \omega$ ,  $s_1 := \omega^4 + \omega^2$  and  $s_0$  satisfies  $s_0^2 + s_0 = \omega^5 + \omega^3$ .

*Proof.* See [GV92a],[GV92b]. □

The algorithm A.0.5 implements the non-rational automorphisms of this curve.

By Proposition 5.5.2, any root  $\omega$  of  $x^{16} + x^8 + x^2 + x$  determines two automorphisms corresponding to the two different solutions of  $s_0^2 + s_0 = \omega^5 + \omega^3$ , namely  $s_0$  and  $s_0 + 1$ . We write  $\sigma_\omega$  for the automorphism associated to an arbitrary  $s_0$ . The automorphism associated to  $s_0 + 1$  is then  $\sigma_\omega \iota$ , where  $\iota$  is the hyperelliptic involution on  $C$ , and both  $\sigma_\omega \iota$  and  $\sigma_\omega$  are identified in the reduced group of automorphisms  $\text{Aut}(C)/\langle \iota \rangle$ . By Proposition 5.5.2, the reduced group of automorphisms is isomorphic to the group of roots of  $x^{16} + x^8 + x^2 + x$ .

We denote the  $s_2, s_1, s_0$  appearing in the coordinates of the second component of the automorphism  $\sigma_\omega$  by  $s_2^\omega, s_1^\omega, s_0^\omega$ .

One knows how to find the inverse of the automorphisms  $\sigma_\omega$ .

**Lemma 5.5.3.** For any  $\sigma_\omega \in \text{Aut}(C)$  corresponding to each root  $\omega$  of  $x^{16} + x^8 + x^2 + x$ ,

$$\sigma_\omega^{-1} = \begin{cases} \sigma_\omega & \text{if } \omega(\omega^5 + \omega + 1) = 0 \\ \sigma_\omega \iota & \text{otherwise} \end{cases}$$

*Proof.* This follows from [GV92b]. Writing

$$x^{16} + x^8 + x^2 + x = x(x^5 + x + 1)(1 + x^5(x^5 + x + 1))$$

then the polynomial  $x^5(x^5 + x + 1)$  evaluates to 1 on exactly the 10 roots of  $x^{16} + x^8 + x^2 + x$  which are not a root of  $x^5 + x + 1$  nor 0. In particular, for any  $\sigma_\omega$ , the composition

$$\begin{aligned} \sigma_\omega^2: (x, y) &\longmapsto (x + \omega + \omega, y + s_2^\omega x^2 + s_1^\omega x + s_0^\omega + s_2^\omega (x + \omega)^2 + s_1^\omega (x + \omega) + s_0^\omega) \\ &= (x, y + \omega^5(\omega^5 + \omega + 1)) \end{aligned}$$

is the identity if  $\omega$  is 0 or a root of  $x^5 + x + 1$  and the hyperelliptic involution  $\iota$  otherwise. Similarly,

$$\begin{aligned} (\sigma_\omega \iota) \sigma_\omega: (x, y) &\longmapsto (x + \omega + \omega, y + s_2 x^2 + s_1 x + s_0 + s_2 (x + \omega)^2 + s_1 (x + \omega) + s_0 + 1) \\ &= (x, y + \omega^5(\omega^5 + \omega + 1) + 1) \end{aligned}$$

is the identity when  $\omega$  is not a root of  $x^5 + x + 1$  nor 0. One derives the inverse of  $\sigma_\omega \iota$  in a similar way.  $\square$

As in Section 5.3, we give the same name  $\sigma_\omega$  to the endomorphisms in  $\text{Jac}(\mathbb{C})$  induced by the automorphisms  $\sigma_\omega$  of  $\mathbb{C}$ . One can verify that they satisfy  $\sigma_\omega \sigma_{\omega'} = \sigma_{\omega'} \sigma_\omega = \pm \sigma_{\omega + \omega'}$ . The following statements use the description of the inverses given above.

**Corollary 5.5.4.** *The endomorphisms  $\sigma_\omega, \sigma_\omega \iota$  satisfy  $x^2 - 1 = 0$  if  $\omega(\omega^5 + \omega + 1) = 0$ , and  $x^2 + 1 = 0$  otherwise.*

*Proof.* Clear.  $\square$

**Corollary 5.5.5.** *The fields generated by the isogenies given by the automorphisms  $\sigma_\omega$  defined above are at most quadratic extensions of  $\mathbb{Q}$ .*

*Proof.* Clear.  $\square$

**Proposition 5.5.6.** *If  $m \equiv \pm 1, \pm 5 \pmod{12}$  then the characteristic polynomial of the Frobenius endomorphism of  $\text{Jac}(\mathbb{C})$  is irreducible.*

*Proof.* With point counting techniques, one finds that the characteristic polynomial of Frobenius  $P_\pi(X)$  is  $X^4 \pm 2^{(m+1)/2} X^3 + 2^m X^2 \pm 2^{(3m+1)/2} X + 2^{2m}$  (see [RS02]).  $\square$

**Remark 5.5.7.** Since the characteristic polynomial of the Frobenius endomorphism  $\pi$  over  $\mathbb{F}_{2^m}$  is

$$P_m^\pm(X) = X^4 \pm 2^{(m+1)/2}X^3 + 2^m X^2 \pm 2^{(3m+1)/2}X + 2^{2m},$$

the relations

$$P_m^+(X)P_m^-(X) = X^8 - 2^{2m}X^4 + 2^{4m}$$

and

$$(X^8 - 2^{4m})(X^8 + 2^{2m}X^4 + 2^{4m})P_m^+(X)P_m^-(X) = X^{24} - 2^{12m}$$

show that the embedding degree is  $k = 12$ .

In order to compute the Frobenius-to-integer exponent  $\kappa$  of  $C$ , one may describe the factorization of the polynomial  $E_{1,1}(x) := x^{16} + x^8 + x^2 + x$  over  $\mathbb{F}_{2^m}$ . Introducing all the roots of the polynomial  $E_{1,1}$  into the ground field  $\mathbb{F}_{2^m}$  we make sure that all the extra endomorphisms are being taken into account.

**Proposition 5.5.8.** *The factorization of*

$$E_{1,1}(x) := (x^6 + x^5 + x^3 + x^2 + 1)(x^3 + x^2 + 1)(x^3 + x + 1)(x^2 + x + 1)(x + 1)x$$

over  $\mathbb{F}_{2^m}$  is as follows:

- i) If  $m \equiv 1, 5 \pmod{6}$  then  $E_{1,1}(x)$  splits exactly as above.
- ii) If  $m \equiv 2, 4 \pmod{6}$  then  $E_{1,1}(x)$  splits as a product of four different factors of degree 3 and four different linear factors.
- iii) If  $m \equiv 3 \pmod{6}$  then  $E_{1,1}(x)$  splits as a product of four different quadratic factors and eight linear factors.
- iv) If  $m \equiv 0 \pmod{6}$  then  $E_{1,1}(x)$  splits into sixteen different linear factors.

*Proof.* If  $m$  is even then any  $\mathbb{F}_{2^{m/2}}$ -irreducible polynomial of degree two splits in  $\mathbb{F}_{2^m}$ . In particular  $x^2 + x + 1 = 0$  has solutions  $\{\theta, \theta + 1\}$  in  $\mathbb{F}_{2^m}$  and then  $x^6 + x^5 + x^3 + x^2 + 1 = (x^3 + \theta x^2 + \theta x + 1)(x^3 + (\theta + 1)x^2 + (\theta + 1)x + 1)$ . Similarly, if  $m \equiv 0 \pmod{3}$  then any  $\mathbb{F}_{2^{m/3}}$ -irreducible degree three polynomial splits over  $\mathbb{F}_{2^m}$ . In particular  $x^3 + x^2 + 1$  or  $x^3 + x + 1$  split over  $\mathbb{F}_{2^m}$ . Moreover, if  $\{\xi, \xi^2, \xi^4\}$  are the roots of one of these polynomials then  $\{\xi + 1, \xi^2 + 1, \xi^4 + 1\}$  are the roots of the other. Thus we have the factorization  $x^6 + x^5 + x^3 + x^2 + 1 = (x^2 + x + \xi(\xi + 1))(x^2 + x + \xi^2(\xi^2 + 1))(x^2 + x + \xi^4(\xi^4 + 1))$ .  $\square$

In Table 5.1 below we displayed each non-trivial irreducible factor of the polynomial  $x^{16} + x^8 + x^2 + x$  together with the set of its roots (in the algebraic closure) in the case  $m \equiv 1, 5 \pmod{6}$ . We gave the names  $\tau, \xi, \rho, \theta$  to a root of each nontrivial irreducible factor of  $x^{16} + x^8 + x^2 + x$  in the above factorization for later convenience.

As in Lemma 5.3.4, it is easy to describe how the automorphisms of  $C$  behave with respect to  $2^m$ -power Frobenius.

**Lemma 5.5.9.** *For any  $\omega$  and  $m$ , the coefficients  $s_i^\omega$  of the second coordinate of  $\sigma_\omega$  satisfy*

$$(s_i^\omega)^{2^m} = s_i^{(\omega^{2^m})}, \quad i = 1, 2$$

*Proof.* This is a trivial consequence of raising to powers of 2 being a linear operation in fields of even characteristic:

$$(s_2^\omega)^{2^m} = (\omega^8)^{2^m} + (\omega^4)^{2^m} + \omega^{2^m} = (\omega^{2^m})^8 + (\omega^{2^m})^4 + \omega^{2^m} = s_2^{\omega^{2^m}}$$

$$(s_1^\omega)^{2^m} = (\omega^4)^{2^m} + (\omega^2)^{2^m} = (\omega^{2^m})^4 + (\omega^{2^m})^2 = s_1^{\omega^{2^m}}$$

□

**Proposition 5.5.10.** *Let  $\pi$  be  $2^m$ -power Frobenius. For every  $\omega$  and  $m$ , the following relations between  $\pi$  and  $\sigma_\omega$  hold:*

$$\pi\sigma_\omega = \pm\sigma_{\omega^{2^m}}\pi$$

*Proof.* By Lemma 5.5.9 above,

$$\begin{aligned} \pi\sigma_\omega(x, y) &= (x^{2^m} + \omega^{2^m}, y^{2^m} + (s_2^\omega)^{2^m}(x^2)^{2^m} + (s_1^\omega)^{2^m}x^{2^m} + (s_0^\omega)^{2^m}) = \\ &= (x^{2^m} + \omega^{2^m}, y^{2^m} + s_2^{\omega^{2^m}}(x^{2^m})^2 + s_1^{\omega^{2^m}}x^{2^m} + s_0^{\omega^{2^m}} + \{0, 1\}) = \pm\sigma_{\omega^{2^m}}\pi(x, y) \end{aligned}$$

□

We write  $\mathbb{Q}[\pi, \sigma_\tau, \sigma_\theta]$  for the non-commutative algebra  $\mathbb{Z}[\pi, \sigma_\tau, \sigma_\theta] \otimes \mathbb{Q}$ .

**Proposition 5.5.11.** *Let  $m \equiv \pm 1 \pmod{6}$ . Then*

$$\mathbb{Q}[\pi, \sigma_\tau, \sigma_\theta] = \mathbb{Q}(\pi) \oplus \sigma_\tau\mathbb{Q}(\pi) \oplus \sigma_\theta\mathbb{Q}(\pi) \oplus \sigma_\xi\mathbb{Q}(\pi)$$

*as 16-dimensional  $\mathbb{Q}$ -vector space and  $\text{End}^0(\text{Jac}(C)) = \mathbb{Q}[\pi, \sigma_\tau, \sigma_\theta]$ .*

*Proof.* Since  $\sigma_\tau \notin \mathbb{Q}(\pi)$ ,  $A = \mathbb{Q}(\pi) \oplus \sigma_\tau \mathbb{Q}(\pi)$  is an 8-dimensional vector space over  $\mathbb{Q}$ .

We first show that  $A \oplus \sigma_\xi \mathbb{Q}(\pi)$  is direct. If we suppose the contrary, then there is some non-zero  $z \in \mathbb{Q}(\pi)$  such that  $\sigma_\xi z \in A$ . Then

$$\sigma_\xi = z_1 + \sigma_\tau z_2$$

for some  $z_1, z_2 \in \mathbb{Q}(\pi)$ . Note that

$$\pi^3 \sigma_\tau \pi^{-3} = \sigma_{\tau 2^3} = \sigma_{\tau+1} = \pm \sigma_\tau \sigma_1$$

where  $\sigma_1(x, y) = (x+1, y+x^2)$ . Also, since  $\xi \in \mathbb{F}_{2^3}$  we have  $\sigma_\xi = \pi^3 \sigma_\xi \pi^{-3}$ . Hence,

$$z_1 + \sigma_\tau z_2 = \pi^3 \sigma_\xi \pi^{-3} = \pi^3 (z_1 + \sigma_\tau z_2) \pi^{-3} = z_1 + \sigma_{\tau 2^3} z_2 = z_1 \pm \sigma_\tau \sigma_1 z_2.$$

Since  $A$  is a direct sum and  $\sigma_1 \neq \pm 1$ , then  $z_2 = 0$ , and this implies that  $\sigma_\xi \in \mathbb{Q}(\pi)$ , which is a contradiction since  $\sigma_\xi$  does not commute with  $\pi$ . Finally, we show that  $(A \oplus \sigma_\xi \mathbb{Q}(\pi)) \oplus \sigma_\theta$  is direct. If not, then

$$\sigma_\theta = z_1 + \sigma_\tau z_2 + \sigma_\xi z_3.$$

We have  $\pi \sigma_\theta \pi^{-1} = \pm \sigma_{\theta 2} = \pm \sigma_{\theta+1} = \pm \sigma_1 \sigma_\theta$ . Hence

$$\begin{aligned} 0 &= \sigma_1 \sigma_\theta \pi^3 - \pi^3 \sigma_\theta = \sigma_1 \sigma_\theta \pi^3 - \pi^3 (z_1 + \sigma_\tau z_2 + \sigma_\xi z_3) = \\ &= \sigma_1 (z_1 + \sigma_\tau z_2 + \sigma_\xi z_3) \pi^3 - (z_1 + \sigma_{\tau 2^3} z_2 + \sigma_{\xi 2^3} z_3) \pi^3 = \\ &= (\sigma_1 - 1) z_1 \pi^3 + (\sigma_1 - \sigma_1) \sigma_\tau z_2 \pi^3 + (\sigma_1 - 1) \sigma_\xi z_3 \pi^3. \end{aligned}$$

Since  $A \oplus \sigma_\xi \mathbb{Q}(\pi)$  is direct it follows that  $z_1 = z_3 = 0$ . So  $\sigma_\theta = \sigma_\tau z$  for some  $z \in \mathbb{Q}(\pi)$ . But this is a contradiction because  $\sigma_\theta$  is defined over  $\mathbb{F}_{2^2}$  and  $\sigma_\tau$  is defined over  $\mathbb{F}_{2^6}$ .

Hence  $A \oplus \sigma_\theta A$  is direct, and  $\mathbb{Q}(\pi) \oplus \sigma_\tau \mathbb{Q}(\pi) \oplus \sigma_\theta \mathbb{Q}(\pi) \oplus \sigma_\xi \mathbb{Q}(\pi)$  is 16-dimensional over  $\mathbb{Q}$ .  $\square$

$x^6 + x^5 + x^3 + x^2 + 1$	$\{\tau, \tau^2, \tau^4, \tau^8, \tau^{16}, \tau^{32}\}$ $\{\tau, \tau^2, \tau^4, \tau + 1, \tau^2 + 1, \tau^4 + 1\}$
$x^3 + x^2 + 1$	$\{\xi, \xi^2, \xi^4\}$ $\{\tau^4 + \tau^2, \tau^4 + \tau + 1, \tau^2 + \tau\}$
$x^3 + x + 1$	$\{\rho, \rho^2, \rho^4\}$ $\{\tau^2 + \tau + 1, \tau^4 + \tau^2 + 1, \tau^4 + \tau\}$
$x^2 + x + 1$	$\{\theta, \theta^2\}$ $\{\tau^4 + \tau^2 + \tau, \tau^4 + \tau^2 + \tau + 1\}$

Table 5.1: The roots of the non-trivial irreducible factors of  $x^{16} + x^8 + x^2 + x$  for  $m \equiv \pm 1, \pm 5 \pmod{12}$ .

## 5.6 Endomorphism algebras with zero divisors

In this section we give other examples of supersingular curves  $C$  of genus 2 for which the endomorphism algebra  $\text{End}^0(\text{Jac}(C))$  does not admit a crossed-product algebra structure. As all the examples we show are supersingular, by Theorem 5.2.6  $\text{End}^0(\text{Jac}(C))$  is 16-dimensional over  $\mathbb{Q}$ .

**Example 5.6.1.** Consider the curve  $C : y^2 = x^5 + 1$  over  $\mathbb{F}_p$  with  $p \equiv 4 \pmod{5}$ .  $C$  is supersingular, because  $P_\pi(X) = (X^2 + p)^2$ , but this polynomial is reducible. Obviously now Frobenius does not generate a subfield of degree 4. Neither do the extra isogenies generate a field of degree 4 because  $x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_p[x]$  splits as a product  $f(x)g(x)$  of two quadratic polynomials if  $p \equiv 4 \pmod{5}$ .

**Example 5.6.2.** Consider  $\tilde{C} : y^2 = x^6 + 1$  over  $\mathbb{Q}$ . This curve has the automorphism  $\varphi : (x, y) \mapsto (\xi_3 x, y)$ , where  $\xi_3$  is a cubic root of unity, and it also admits two rational maps to the elliptic curve  $E : y^2 = x^3 + 1$  given by

$$(x, y) \mapsto (x^2, y) \quad \text{and} \quad (x, y) \mapsto \left(\frac{1}{x^2}, \frac{y}{x^3}\right).$$

This pair of maps extend to an isogeny between  $\text{Jac}(C)$  and  $E^2$ . Reducing  $\tilde{C}$  modulo a prime congruent to  $2 \pmod{3}$  one obtains a supersingular curve  $C$  with characteristic polynomial of Frobenius equal to  $(X^2 + p)^2$ . Hence  $\text{End}^0(\text{Jac}(C))$  is 16-dimensional by Theorem 5.2.6. On the other hand, both the isogeny induced by  $\varphi$  and the Frobenius endomorphism satisfy quadratic polynomials, and therefore they cannot generate a maximal subfield— not even together as they do not commute.

Note that  $\text{End}^0(\text{Jac}(C)) \cong \text{End}^0(E^2) \cong M_2(\text{End}^0(E))$ .

The splitting as a product of elliptic curves makes  $\text{End}(\text{Jac}(C))$  contain zero divisors. Indeed, an isogeny of the elliptic curve gives place to an endomorphism of  $\text{Jac}(C)$  which is not surjective, and is therefore not an isogeny. Proposition 4.5.10 does not apply in this case. We do not provide a solution to the Decisional Diffie-Hellman Problem in such cases.

## Chapter 6

# The Tate pairing and DDH

In this final chapter, we show how to solve the Decisional Diffie-Hellman Problem for some curves of genus two over finite fields such that  $\text{End}^0(\text{Jac}(C))$  is a crossed-product algebra over a quartic field  $F$ . We show explicit solutions in genus two, but our approach should generalise readily to hyperelliptic curves of higher genus.

First, we recall the definition of the Tate pairing. We adapt an existing algorithm to compute the Tate Pairing from genus one to genus two. We then use the Tate pairing to show examples of representations of endomorphisms of Jacobians of genus two in the subgroup  $\text{Jac}(C)[l]$  of points of order  $l$ . Finally, we use distortion maps to solve the Decisional Diffie-Hellman Problem in some examples.

### 6.1 The Tate pairing

In this section we recall the definition of the Tate pairing, following [FOS04]. Details can be found in [FR94], [Gal05], [FL03]. We give an algorithm to compute the Tate pairing for curves  $C$  of genus two over finite fields in the appendix (see Algorithm A.0.10).

Let  $k$  be a field (not necessarily finite),  $\bar{k}$  the separable closure of  $k$  and  $G_k := \text{Gal}(\bar{k}/k)$ . Suppose  $A$  is the Jacobian variety of a curve over a field  $k$ . Its Cartier Dual,  $A^\vee$  is isomorphic to  $A$  and thus there is a natural pairing  $w_l: A[l] \times A[l] \rightarrow \mu_l \subseteq (\bar{k})^*$ , the *Weil pairing*.

Let  $l$  be an integer such that  $(l, \text{char}(k)) = 1$ . The Kummer exact sequence

$$0 \longrightarrow A[l] \longrightarrow A(\bar{k}) \xrightarrow{l} A(\bar{k}) \longrightarrow 0$$

gives the following exact sequence in cohomology:

$$0 \longrightarrow A(k)/l_A A(k) \xrightarrow{\delta} H^1(G_k, A[l]) \xrightarrow{\alpha} H^1(G_k, A(\bar{k}))[l] \longrightarrow 0$$

For each  $P \in A(k)$  there must exist a  $Q \in A(\bar{k})$  such that  $P = l_A(Q)$  (by exactness of the Kummer sequence); therefore, for each  $P$  we define the coboundary map  $\delta$  by  $\delta([P])(\sigma) = \sigma(Q) - Q \forall \sigma \in G_k$ .

**Definition 6.1.1.** Let  $\hat{c}$  denote any preimage of an element  $c \in H^1(G_k, A(\bar{k}))[l]$  by  $\alpha$ . For all  $\sigma, \tau \in G_k$ , all  $[P] \in A(k)/l_A A(k)$  and all  $c \in H^1(G_k, A(\bar{k}))[l]$ , the *Tate pairing* associated to the above sequences is

$$e_l([P], c)(\sigma, \tau) := w_l(\delta([P])(\sigma), \sigma \hat{c}(\tau))$$

Note that if we fix  $[P]$  and  $c$ , and let  $\sigma, \tau$  vary in  $G_k$ , one obtains a map  $h: G_k \times G_k \longrightarrow \mu_n \subseteq \bar{k}^*$  and in this way

$$e_l: \begin{array}{ccc} A(k)/l_A A(k) & \times & H^1(G_k, A(\bar{k}))[l] \\ \left( [P] \right) & , & \left( c \right) \end{array} \longrightarrow H^2(G_k, \bar{k}^*) \cong Br(k) \longmapsto e_l([P], c)$$

where  $Br(k)$  is the Brauer group (see Definition 3.2.1).

**Remark 6.1.2.** The above is a *cup product*, and sits in the broad context of arithmetic duality theorems and class formations (see [Mil86]). Note that if  $k$  is finite, then  $Br(k) = 0$ . This trivialises the Tate pairing as we have defined it above because we are interested in Jacobians of curves over finite fields. We now sketch how to overcome this situation.

Suppose  $k$  is a finite field of characteristic  $p$ , and let  $\tilde{k}$  be a local field such that the residue field of  $\tilde{k}$  is  $k$ . For an abelian variety  $A$  defined over  $k$ , write  $\tilde{A}$  for a lift of  $A$  defined over  $\tilde{k}$ . For lifts of abelian varieties, see [LST64].

If  $\tilde{A}$  has good reduction at  $p$  then

$$\tilde{A}(\tilde{k})/l_A \tilde{A}(\tilde{k}) \cong A(k)/l_A A(k)$$

by Hensel's Lemma. Let  $\tilde{e}_l$  denote the Tate pairing for  $\tilde{A}$ . It is known that  $\tilde{e}_l$  is non-degenerate. Moreover, extending to  $L = \tilde{k}(\xi_l)$  for  $\xi_l$  a  $l$ -th root of unity, then  $\tilde{e}_l$  becomes simpler. We have  $Br(L) \cong k^*/(k^*)^l$  (via the Hasse Invariant isomorphism *inv* [Rei75]), and also  $H^1(G_L, \tilde{A}(\tilde{k}))[l] \cong \tilde{A}(\tilde{k})[l]$ . This simplifies the Tate pairing considerably.

Suppose  $C$  is a curve of genus two defined over a finite field  $\mathbb{F}_q$ . Write  $\mathbb{F}_{q^k} = \mathbb{F}_q(\mu_l)$  where  $k$  is the embedding degree of  $C$ —that is smallest integer

such that  $l|q^k - 1$ . We work with the following version of the Tate pairing on the canonical lift of  $\text{Jac}(C)$  extended to  $L$  as above:

$$e_l: \begin{array}{ccc} \text{Jac}(C)(\mathbb{F}_{q^k})/l\text{Jac}(C)(\mathbb{F}_{q^k}) & \times & \text{Jac}(C)(\mathbb{F}_{q^k})[l] & \longrightarrow & \mathbb{F}_q^*/(\mathbb{F}_q^*)^l \\ ( [P] ) & , & ( Q ) & \longmapsto & e_l(P, Q) \end{array}$$

Proofs of the non-degeneracy of  $e_l$  can be found in [Hes04] and [Sch05]. The computation of  $e_l$  for Jacobians of curves originated in the works of Lichtenbaum, and the basic step is the evaluation at  $P$  of a certain function associated to  $Q$ . We use the slightly different definition  $e_l(P, Q)^{(q^k-1)/l}$  (see [Gal05]).

The Magma code A.0.10 implements an algorithm to compute the Tate pairing adapting Miller's algorithm [Mil04] to curves of genus two.

## 6.2 Endomorphisms on the $l$ -torsion

In this section we show how to use the Tate pairing to obtain representations of endomorphisms on the  $l$ -torsion subgroup of  $\text{Jac}(C)$ . We give some algorithms in Magma code to do this.

The first algorithm constructs a basis of the  $l$ -torsion  $\text{Jac}(C)(\mathbb{F}_{q^k})[l]$  for  $l \mid \#\text{Jac}(C)(\mathbb{F}_{q^k})$  assuming that the embedding degree is 4 and that the eigenvalues of the Frobenius endomorphism are  $1, -1, q, -q$ . The method works for supersingular curves of genus two over finite fields obtained after reduction at an prime  $p$  inert in the CM field as in Section 5.4.

**Algorithm 6.2.1.** Input: a divisor  $D \in \text{Jac}(C)(\mathbb{F}_{p^4})[l]$  in Mumford representation, where  $C$  is a supersingular CM curve of genus two defined over  $\mathbb{F}_{p^4}$  with embedding degree 4, and  $p$  is inert in the CM field. By BF we mean the ground field.

Output: a basis for the  $\mathbb{F}_l$ -vector space  $\text{Jac}(C)(\mathbb{F}_{p^4})[l]$ .

```
DBasis4:=function(D,q,l);
  PD:=Frobenius(D,BF);
  P2D:=Frobenius(PD,BF);
  P3D:=Frobenius(P2D,BF);
  Q1:=InverseMod(2*(q^2-1),l);
  D11:=(q^2 mod l)*D;
  D12:=(q^2 mod l)*PD;
  D13:=-P2D;
  D14:=-P3D;
  Q2:=InverseMod(2*(q^2-1),l);
```

```

D21:=(q2 mod l)*D;
D22:=- (q2 mod l)*PD;
D23:=-P2D;
D24:=P3D;
Q3:=InverseMod(2*q*(q2-1),l);
D31:=-q*D;
D32:=-PD;
D33:=q*P2D;
D34:=P3D;
Q4:=InverseMod(2*q*(q2-1),l);
D41:=-q*D;
D42:=PD;
D43:=q*P2D;
D44:=-P3D;
D1:=Q1*(D11+D12+D13+D14);
D2:=Q2*(D21+D22+D23+D24);
D3:=Q3*(D31+D32+D33+D34);
D4:=Q4*(D41+D42+D43+D44);
return D1,D2,D3,D4;
end function;

```

With the basis provided above, it is straightforward to build  $4 \times 4$  matrices over  $\mathbb{F}_l$  for  $\xi_5$  and also for the CM-isogenies  $\varphi$  as in 5.4.12. One just pairs the elements of the basis constructed by Algorithm 6.2.1 using the Tate pairing Algorithm A.0.10. The following algorithms do this. First, we provide a method for computing discrete logarithms.

**Algorithm 6.2.2.** Input: two values  $t, t_1$  in the group of  $l$ -th roots of unity. Output: the exponent  $\log$  such that  $t^{\log} = t_1$ .

```

log:=function(t,t1,l);
n:=1;
che:=true;
while n lt l+1 and che eq true do
t2:=tn;
if t2 eq t1 then
che:=false;
end if;
n:=n+1;
end while;
return n-1;

```

end function;

**Algorithm 6.2.3.** Input: a basis  $\{D_1, D_2, D_3, D_4\}$  and an arbitrary element  $D$  of the  $l$ -torsion of the Jacobian (over the embedding degree field extension of  $q^k$  elements) of a curve  $C$  defined over a base field  $BF$  of  $q$  elements, and the exponent  $h := (q^k - 1)/l$  in our working definition of the Tate pairing. Output: the components of  $D$  in the basis  $\{D_1, D_2, D_3, D_4\}$ .

Note the use of the Tate pairing algorithm A.0.10.

```

components:=function(D,D1,D2,D3,D4,C,l,q,h);
  td1:=TatePairing(D,D1,C,l,q,BF);
  TD1:=td1h;
  td2:=TatePairing(D,D2,C,l,q,BF);
  TD2:=td2h;
  td3:=TatePairing(D,D3,C,l,q,BF);
  TD3:=td3h;
  td4:=TatePairing(D,D4,C,l,q,BF);
  TD4:=td4h;
  t13:=TatePairing(D1,D3,C,l,q,BF);
  T13:=t13h;
  t24:=TatePairing(D2,D4,C,l,q,BF);
  T24:=t24h;
  t31:=TatePairing(D3,D1,C,l,q,BF);
  T31:=t31h;
  t42:=TatePairing(D4,D2,C,l,q,BF);
  T42:=t42h;
  n3:=log(T31,TD1,1);
  n4:=log(T42,TD2,1);
  n1:=log(T13,TD3,1);
  n2:=log(T24,TD4,1);
  return n1,n2,n3,n4;
end function;

```

**Algorithm 6.2.4.** This is a brute force variant of the above.

```

components:=function(D,D1,D2,D3,D4,C,ll);
  n1:=1;
  n2:=1;
  n3:=1;
  n4:=1;
  for n1:=1 to ll do

```

```

for n2:=1 to 11 do
  for n3:=1 to 11 do
    for n4:=1 to 11 do
      DD:=n1 * D1 + n2 * D2 + n3 * D3 + n4 * D4;
      if D eq DD then
        return n1,n2,n3,n4;
      end if;
    end for;
  end for;
end for;
end function;

```

Examples with degree 6 models with a rational root (see Remark 4.1.9) are more tedious to deal with because one has to find the coordinates of the endomorphisms in the degree 5 model. An example of this is the following.

**Example 6.2.5.** The curve  $C : y^2 = x^6 - 64$  over  $\mathbb{Q}$  is not in a suitable form to apply Cantor's algorithms because of the two points at infinity. After transforming to a degree-5 model (using the rational point  $(2, 0) \in C(\mathbb{Q})$ ), one obtains

$$C' : y^2 = x^5 + 240x^4 + 30720x^3 + 2211840x^2 + 84934656x + 1358954496$$

The automorphism given by a cubic root of unity  $\xi_3$  on the non singular model of  $C'$  (see Section 2.7) is

$$\begin{bmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \\ v \end{bmatrix} \mapsto \begin{bmatrix} u_0 - 6(\xi_3^2 - 1)u_1 + 36(1 + \xi_3)u_2 + 24(1 + 2\xi_3)u_3 \\ \xi_3^2 u_1 + 4\xi_3(\xi_3 - 1)u_2 - 12\xi_3 u_3 \\ \xi_3 u_2 + 2(\xi_3 - 1)u_3 \\ u_3 \\ v \end{bmatrix}$$

and one finds that the  $\xi_3$  automorphism in the projective closure of the degree-5 plane model is

$$\begin{pmatrix} u \\ v \\ w \end{pmatrix} \mapsto \begin{pmatrix} (-32\xi_3 - 64)u^3 - 6144u^2w + (98304\xi_3 - 98304)uw^2 \\ (-196608\xi_3 - 98304)vw^2 \\ u^3 + (-96\xi_3 + 96)u^2w - 9216\xi_3uw^2 + (-196608\xi_3 - 98304)w^3 \end{pmatrix}.$$

### 6.3 Distortion maps and DDH

In this final section we recall the definition of distortion maps, and show that for supersingular curves enough distortion maps exist to solve every instance of the Decisional Diffie-Hellman Problem. We show how to solve the Decisional Diffie-Hellman Problem in some examples.

**Definition 6.3.1.** A *distortion map* for the pairing  $e$  and non-zero divisor classes  $D_1, D_2$  on  $C$  is an endomorphism  $\phi$  of  $\text{Jac}(C)$  such that

$$e(D_1, \phi(D_2)) \neq 1.$$

Let  $p$  be an inert prime in a cyclic, quartic CM field. By Proposition 5.4.4, the Frobenius endomorphism  $\pi$  has eigenvalues  $\{1, -1, p, -p\}$ . We let  $(D_1, D_2, D_3, D_4)$  denote the associated  $\pi$ -eigenbasis of  $\text{Jac}(C)[l]$  for  $l \mid 1+p^2$ .

**Lemma 6.3.2.** *Let  $p$  be an inert prime and let  $l > 2$  be a prime such that  $l \mid p^2 + 1$ . Let  $(D_1, D_2, D_3, D_4)$  be the ordered  $\pi$ -eigenbasis as above. For  $1 \leq i, j \leq 4$ , we have  $e_l(D_i, D_j) = 1$  unless  $(i, j) = (1, 3), (3, 1), (2, 4)$  or  $(4, 2)$ .*

*Proof.* We use the Galois invariance of  $e_l$ . For example, for  $D_1$  one has

$$e_l(D_1, D_1) = \pi(e_l(D_1, D_1)) = e_l(\pi(D_1), \pi(D_1)) = e_l(D_1, D_1).$$

This implies  $e_l(D_1, D_1) \in \mathbb{F}_p \cap \mu_l$  and hence  $e_l(D_1, D_1) = 1$ .

Similarly,

$$\begin{aligned} e_l(D_1, D_2)^p &= \pi(e_l(D_1, D_2)) = e_l(\pi(D_1), \pi(D_2)) \\ &= e_l(D_1, -D_2) = e_l(D_1, D_2)^{-1}. \end{aligned}$$

Since  $l \nmid (p+1)$  this implies  $e_l(D_1, D_2) = 1$ .

Similarly,

$$\begin{aligned} e_l(D_1, D_4)^p &= \pi(e_l(D_1, D_4)) = e_l(\pi(D_1), \pi(D_4)) \\ &= e_l(D_1, -pD_4) = e_l(D_1, D_4)^{-p}. \end{aligned}$$

Since  $l \nmid 2p$  it follows that  $e_l(D_1, D_4) = 1$ .

By non-degeneracy of  $e_l$ , one must have  $e_l(D_1, D_3) \neq 1$ . The proof for the other cases is the same.  $\square$

The endomorphism  $\pi$  may be used as a distortion map. For example, suppose  $D = D_1 + D_2$  and  $D' = D_3 + mD_4$ , with respect to the basis above, where  $m \in \mathbb{Z}$  is such that  $e_l(D, D') = e_l(D_1, D_3)e_l(D_2, D_4)^m = 1$ . Then we have

$$e_l(D, \pi(D')) = e_l(D_1, pD_3)e_l(D_2, -pmD_4) = e_l(D_1, D_3)^p e_l(D_2, D_4)^{-pm}$$

which is not equal to 1 if  $m \not\equiv 0 \pmod{l}$ .

It was proven by Schoof and Verheul [Ver04] that distortion maps always exist for supersingular elliptic curves over  $\mathbb{F}_q$ . The following theorem generalises their result to curves of genus two.

**Theorem 6.3.3.** *Let  $C$  be a supersingular curve of genus 2 over  $\mathbb{F}_q$ . Let  $l \mid \#\text{Jac}(C)(\mathbb{F}_q)$  and let  $k$  be the embedding degree. Let  $D_1, D_2 \in \text{Jac}(C)(\mathbb{F}_{q^k})$  be non-trivial divisor classes of order  $l$ . Then there is an element  $\phi \in \text{End}(\text{Jac}(C))$  such that  $e_l(D_1, \phi(D_2)) \neq 1$ .*

*Proof.* Recall that  $G$  is the absolute Galois group of  $\mathbb{F}_q$ . By Theorem 5.2.6 we have

$$\text{End}_G(T_l(\text{Jac}(C))) \cong M_{2g}(\mathbb{Z}_l).$$

Hence  $\text{End}_K(\text{Jac}(C)) \otimes_{\mathbb{Z}} \mathbb{Z}_l \cong M_{2g}(\mathbb{Z}_l)$  and so  $\text{End}_K(\text{Jac}(C)) \cong \text{End}(\text{Jac}(C))$  is  $(2g)^2$ -dimensional. By restriction, we have

$$\text{End}_K(\text{Jac}(C)) \otimes_{\mathbb{Z}} \mathbb{Z}/l\mathbb{Z} \cong M_{2g}(\mathbb{Z}/l\mathbb{Z}).$$

Let  $D_3 \in \text{Jac}(C)[l]$  be such that  $e_l(D_1, D_3) \neq 1$ . There exists some matrix  $\Phi \in M_{2g}(\mathbb{Z}/l\mathbb{Z})$  which corresponds to mapping  $\langle D_2 \rangle$  to  $\langle D_3 \rangle$ . Let  $\phi$  be a preimage in  $\text{End}(\text{Jac}(C))$  of  $\Phi$ . Then  $e_l(D_1, \phi(D_2)) \neq 1$ .  $\square$

By Theorem 6.3.3 above, for every pair  $D_1, D_2$  of non-trivial divisors of order  $l$  on  $\text{Jac}(C)$  there is some  $\phi \in \text{End}(\text{Jac}(C))$  such that  $e_l(D_1, \phi(D_2)) \neq 1$ . For the curves in Section 5.4, we know that  $\text{End}(\text{Jac}(C))$  is an order  $\mathcal{O}$  in  $\mathbb{Q}[\varphi, \pi]$  which contains  $\mathbb{Z}[\varphi, \pi]$ . For them, Corollary 5.4.6 implies that

$$\phi = \sum_{i,j} \lambda_{i,j} \pi^i \varphi^j.$$

At this point we must make an assumption. Let  $m$  be the least common multiple of the denominators of the  $\lambda_{i,j}$ . Then  $m\phi \in \mathbb{Z}[\varphi, \pi]$ .

**Assumption:** We assume that  $\phi$  may be chosen such that  $\gcd(m, l) = 1$ .

We are requiring that the index of the order  $\mathbb{Z}[\pi, \varphi]$  in the maximal order is not divisible by  $l$ . In the case of elliptic curves, this cannot happen if  $l$  is sufficiently large. In the case of dimension 2 we do not expect it to occur for most examples. A better understanding of orders in algebras of degree 4 is needed to remove this assumption.

Under the assumption above, we have that

$$e_l(D_1, m\phi(D_2)) = e_l(D_1, \phi(D_2))^m \neq 1.$$

Since  $m\phi$  is an integer combination of the  $\pi^i \varphi^j$  it follows that for some pair  $(i, j)$  we have  $e_l(D_1, \pi^i \varphi^j(D_2)) \neq 1$  (otherwise, if all  $e_l(D_1, \pi^i \varphi^j(D_2)) = 1$  then  $e_l(D_1, m\phi(D_2)) = 1$ ).

For the example in Section 5.5, one has

$$\phi = \sum_{0 \leq i, j, k, l \leq 3} \lambda_i \pi^i + \lambda_j \pi^j \sigma_\tau + \lambda_k \pi^k \sigma_\theta + \lambda_l \pi^l \sigma_\xi.$$

and a similar solution follows.



# Appendix A

## Appendix

In this appendix we gathered some more algorithms in Magma code we referred to in the body of the dissertation. We include them as we used them at some point of our research, either to confirm or disprove working hypotheses. Our algorithms are far from optimized, but were tested in many instances and proved to work in all of them. As the reader may notice, most of them are fairly straightforward, except perhaps Algorithm A.0.10, which is a generalization of Miller's Algorithm [Mil04] to genus 2.

**Algorithm** A.0.4. Input: a divisor  $D$  of  $\text{Jac}(C)$  in Mumford representation, a fifth root of unity  $\xi_5$ , the polynomial ring  $R$  and the Jacobian  $J = \text{Jac}(C)$ . Output: the image of  $\xi_5(D)$ .

```
autoroot5:=function(D,xi5,P,J);
  a:=Coefficients(D[1])[1];
  b:=Coefficients(D[1])[2];
  p:=elt<P|x^2 + xi5 * b * x + xi5^2 * a>;
  c:=Coefficients(D[2])[1];
  d:=Coefficients(D[2])[2];
  q:=elt<P|(1/xi5) * d * x + c>;
  U:=J![p,q];
  return U;
end function;
```

**Algorithm** A.0.5. Inputs: a curve  $C$  over a finite field  $F$  of even characteristic as above, a point  $Q$  in  $C$ , the ring  $P$  of polynomials in one variable with coefficients in  $F$  and a root  $v$  of  $x^{16} + x^8 + x^2 + x$ . Output:  $\sigma_v(Q)$ .

```

autom32A:=function(Q,v,P,C);
  s2:=v8 + v4 + v;
  s1:=v4 + v2;
  S0:=elt<P|x2 + x + v5 + v3>;
  if IsIrreducible(S0) then
    FF:=ext<F|S0>;
    PP:=PolynomialRing(FF);
    S0:=PP!S0;
    s0:=Roots(S0);
    C:=BaseExtend(C,FF);
    QA1:=Q[1] + v;
    QA2:=Q[2] + s0[1][1] + s1Q[1] + s2Q[1]Q[1];
  else
    s0:=Roots(S0);
    QA1:=Q[1] + v;
    QA2:=Q[2] + s0[1][1] + s1Q[1] + s2Q[1]Q[1];
  end if;
  U1:=C![QA1,QA2];
  return U1;
end function;

```

**Algorithm** A.0.6. Input: a CM polynomial  $cmp(x)$  of degree four, a prime  $p$ .

Output: the roots, the irreducibility and the factors of  $cmp(x)$  as a polynomial over  $\mathbb{F}_p$ .

```

cmplitsmodp:=function(cmp,p);
  F:=GF(p);
  P<x>:=PolynomialRing(F);
  cmpp:=P!cmp;
  return Roots(cmpp),IsIrreducible(cmpp),Factorization(cmpp);
end function;

```

**Algorithm** A.0.7. Input: a prime  $p$  and a curve  $C$  over the finite field  $\mathbb{F}_p$ .

Output: the characteristic polynomial of the Frobenius endomorphism, the Cartier-Manin matrix  $HW$  of  $C$ , the associated matrix  $HW_p$  and the product  $HW \cdot HW_p$ .

```

IsSupersingularmodp:=function(C,p);
  f,h:=HyperellipticPolynomials(C);
  F:=GF(p);

```

```

P<x>:=PolynomialRing(F);
CF:=HyperellipticCurve(P!f,P!h);
ff:=ZetaFunction(CF);
sqf:=Sqrt(P!fp-1);
M:=MatrixAlgebra(F,2);
HWp:=elt<M|Coefficients(sqf)[p],Coefficients(sqf)[2*p],
Coefficients(sqf)[p-1],Coefficients(sqf)[2*p-1]>;
HW:=elt<M|(Coefficients(sqf)[p])p,(Coefficients(sqf)[2*p])p,
(Coefficients(sqf)[p-1])p,(Coefficients(sqf)[2*p-1])p>;
A:=HW*HWp;
return ff, sqf,HW,HWp,A;
end function;

```

**Algorithm A.0.8.** Input: the curve  $C_{vw1}$  defined over a base field  $BF = \mathbb{F}_p$  (see Example 5.4.12), the polynomialring  $P$  over  $BF$ , the Jacobian  $\text{Jac}(C_{vw1})$ , the root  $mu$  of the CM polynomial associated with  $C_{vw1}$  modulo  $p$ , the Frobenius-to-integer extension  $F = \mathbb{F}_{p^4}$ , the point wise CM-isogeny  $\varphi_{vw1}$  (see Algorithm A.0.9), the Mumford coordinates of a divisor  $D \in \text{Jac}(C_{vw1})(\mathbb{F}_{p^4})[l]$ .

Output:  $\varphi_{vw1}(D)$  in Mumford coordinates.

```

phivw1J:=function(D,mu,F,P,C,J,BF);
  ir:=IsIrreducible(D[1]);
  if ir eq true then
    F2:=ext<F|D[1]>;
    PP:=PolynomialRing(F2);
    D1:=PP!D[1];
    r1:=Roots(D1)[1][1];
    r2:=Roots(D1)[2][1];
    b1:=Evaluate(D[2],r1);
    b2:=Evaluate(D[2],r2);
    CF2:=BaseExtend(C,F2);
    JF2:=BaseExtend(J,F2);
    P1:=CF2![r1,b1];
    P2:=CF2![r2,b2];
    P1A:=phivw1(P1,mu,F2,PP,CF2,JF2,BF);
    P2A:=phivw1(P2,mu,F2,PP,CF2,JF2,BF);
    u1,u2:=compose(P1A[1],P1A[2],P2A[1],P2A[2],C);
    v1,v2:=reduce(u1,u2,C);
    aD:=J![v1,v2];
  end if;
end function;

```

```

else
  r1:=Roots(D[1])[1][1];
  r2:=Roots(D[1])[2][1];
  b1:=Evaluate(D[2],r1);
  b2:=Evaluate(D[2],r2);
  P1:=C![r1,b1];
  P2:=C![r2,b2];
  P1A:=phivw1(P1,mu,F,P,C,J,BF);
  P2A:=phivw1(P2,mu,F,P,C,J,BF);
  u1,u2:=compose(P1A[1],P1A[2],P2A[1],P2A[2],C);
  v1,v2:=reduce(u1,u2,C);
  aD:=J![v1,v2];
end if;
return aD;
end function;

```

**Algorithm** A.0.9. Input: the curve  $C_{vw1}$  defined over a base field  $BF = \mathbb{F}_p$  (see Example 5.4.12), the field extension  $F$  of  $BF$ , the polynomial ring  $P$  over  $BF$ , the Jacobian  $\text{Jac}(C_{vw1})$ , the root  $\mu$ , a point  $Q$  of the curve  $C_{vw1}$ , and the whole CM-isogeny description in terms of the coordinates  $x_1, x_2, y_1, y_2$  deducible from [Wam99a], [Wam99b].

Output:  $\varphi_{vw1}(Q)$  in Mumford coordinates.

```

phivw1:=function(Q,mu,F,P,CF,JF,BF);
  s1:=F!(4+mu^2+Q[1]*(-2-mu^2));
  s2:=F!(2+Q[1]^2+mu^2+Q[1]*(-4-mu^2));
  a:=elt<P|s2,-s1,1>;
  ir:=IsIrreducible(a);
  if ir eq true then
    F2:=ext<F|a>;
    P2:=PolynomialRing(F2);
    a:=P2!a;
    x1:=Roots(a)[1][1];
    x2:=Roots(a)[2][1];
    y1:=1/2*(-mu^3-4*mu)*Q[2]/(Q[1]+1)*x1+(1/2*(-mu^3-4*mu)*
      *Q[1]*Q[2]+(mu^3+3*mu)*Q[2])/(Q[1]+1);
    y2:=1/2*(-mu^3-4*mu)*Q[2]/(Q[1]+1)*x1+(1/2*(-mu^3-2*mu)*
      Q[1]*Q[2]+(mu^3+4*mu)*Q[2])/(Q[1]+1);
    b:=Interpolation([F2|x1,x2],[y1,-y2]);
    b:=P!b;
  end if;
end function;

```

```

a:=P!a;
CF2:=BaseExtend(CF,F2);
JF2:=BaseExtend(JF,F2);
aQ:=JF![a,b];
else
x1:=Roots(a)[1][1];
x2:=Roots(a)[2][1];
y1:=1/2*(-μ3-4*μ)*Q[2]/(Q[1]+1)*x1+(1/2*(-μ3-4*μ)*
*Q[1]*Q[2]+(μ3+3*μ)*Q[2])/(Q[1]+1);
y2:=1/2*(-μ3-4*μ)*Q[2]/(Q[1]+1)*x1+(1/2*(-μ3-2*μ)*
*Q[1]*Q[2]+(μ3+4*μ)*Q[2])/(Q[1]+1);
b:=Interpolation([F|x1,x2],[y1,-y2]);
b:=P!b;
a:=P!a;
aQ:=JF![a,b];
end if;
return aQ;
end function;

```

**Algorithm** A.0.10. Input: Two divisors  $P, Q$  on  $C$  ( which are representatives for points on  $\text{Jac}(C)(\mathbb{F}_{p^4})$  ), and a factor  $l$  of  $\#\text{Jac}(C)(\mathbb{F}_{p^4})$  of a curve  $C$  defined over  $BF = \mathbb{F}_q$ .

Output:  $e_l(P, Q)$ .

Note the use of Cantor's algorithms from Section 4.3 in Chapter 4.

```

TatePairing:=function(P,Q,C,l,q,BF);
f,h:=HyperellipticPolynomials(C);
J:=Jacobian(C);
S:=Random(J);
F:=BaseField(C);
R:=PolynomialRing(F);
m:=Ilog2(l)-1;
E:=Q+S;
T1:=P[1];
T2:=P[2];
func:=1;
W:=IntegerToString(1, 2);
U:=IntegerToString(2, 2);
while m ge 0 do
if m eq 0 then

```

```

if W[Ilog2(l)+1] eq U[2] then
  TT1,TT2,l1,l2:=compose(T1,T2,T1,T2,E,S,C,F);
  T1,T2,lq,ls:=reduce(TT1,TT2,E,S,C,F);
  func:=func*func*l1/l2;
else
  TT1,TT2,l1,l2:=compose(T1,T2,T1,T2,E,S,C,F);
  T1,T2,lq,ls:=reduce(TT1,TT2,E,S,C,F);
  func:=func*func*lq/ls*l1/l2;
  TT1,TT2,l1,l2:=compose(T1,T2,P[1],P[2],E,S,C,F);
  T1,T2,lq,ls:=reduce(TT1,TT2,E,S,C,F);
  func:=func*lq/ls*l1/l2;
end if;
else
  TT1,TT2,l1,l2:=compose(T1,T2,T1,T2,E,S,C,F);
  T1,T2,lq,ls:=reduce(TT1,TT2,E,S,C,F);
  func:=func*func*lq/ls*l1/l2;
  if W[Ilog2(l)+1-m] eq U[1] then
    TT1,TT2,l1,l2:=compose(T1,T2,P[1],P[2],E,S,C,F);
    T1,T2,lq,ls:=reduce(TT1,TT2,E,S,C,F);
    func:=func*lq/ls*l1/l2;
  end if;
end if;
m:=m-1;
end while;
return func;
end function;

```

# Bibliography

- [Alb39] A. Albert, “*Structure of Algebras*”, American Mathematical Society Colloquium Publications, vol. **24**, American Mathematical Society, New York (1939).
- [AB04] M. Alsina and P. Bayer, “*Quaternion orders, quadratic forms, and Shimura curves*”, CRM monograph series, vol. **22**, American Mathematical Society, Providence R.I. (2004).
- [BGOS04] P. Barreto, S. Galbraith, C. O’Eigeartaigh and M. Scott, “*Efficient Pairing Computation on Supersingular Abelian Varieties*”, eprint 2004/375.
- [BL04] C. Birkenhake and H. Lange, “*Complex Abelian Varieties*”, Grundlehren der mathematischen Wissenschaften, vol. **302** (second edition), Springer-Verlag, Berlin-Heidelberg (2004).
- [BSS04] I. Blake, G. Seroussi and N. Smart (eds.), “*Advances in Elliptic Curve Cryptography*”, London Mathematical Society Lecture Note Series, vol. **317**, Cambridge University Press, Cambridge (2004).
- [Bon98] D. Boneh, “*The decision Diffie-Hellman problem*”, in the Proceedings of the Third Algorithmic Number Theory Symposium, Lecture Notes in Computer Science, vol. **1423**, Springer (1998), 48–63.
- [BF01] D. Boneh and M. Franklin, “*Identity-based encryption from the Weil pairing*”, SIAM Journal of Computing, **48** Number 3 (2003), 586–615. Extended Abstract in Crypto 2001.
- [BLS01] D. Boneh, B. Lynn and H. Shacham, “*Short Signatures from the Weil Pairing*”, J. Cryptology, **17** Number 4 (2004), 297–319. First appeared in Proceedings Asiacrypt 2001.

- [Can87] D. Cantor, “*Computing in the Jacobian of a hyperelliptic curve*”, *Mathematics of computation*, **48** (1987), 95–101.
- [CNP05] G. Cardona, E. Nart and J. Pujolàs, “*Curves of genus two over fields of even characteristic*”, *Mathematische Zeitschrift*, **250** Number 1 (2005), 177–201.
- [CF96] J. W. S. Cassels and E. V. Flynn, “*Prolegomena to a middlebrow arithmetic of curves of genus 2*”, *London Mathematical Society Lecture Note Series*, vol. **230**, Cambridge University Press, Cambridge (1996).
- [CJL00] Y.-J. Choie, E. Jeong and E. Lee, “*Supersingular hyperelliptic curves of genus 2 over finite fields*”, preprint (2000)
- [CL04] Y.-J. Choie and E. Lee, “*Implementation of tate pairing on hyperelliptic curves of genus 2*”, in J. I. Lim and D. H. Lee (eds.), *ICISC 2003, Lecture Notes in Computer Science*, vol. **2971**, Springer (2004), 97–111.
- [CS86] G. Cornell and J. Silverman (eds.), “*Arithmetic Geometry*”, Springer (1986).
- [Deu41] M. Deuring, “*Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*”, *Abhandlungen aus dem Mathematischen Seminar der Univ. Hamburg*, **14** (1941), 197–272.
- [DL03] I. Duursma and H.-S. Lee, “*Tate-pairing implementations for tripartite key agreement*”, *Advances in cryptology—ASIACRYPT 2003, Lecture Notes in Computer Science*, vol. **2894**, Springer (2003), 111–123.
- [FOS04] Notes taken by J. Pujolàs during Prof. G. Frey’s lectures at the Oberwolfach Seminar “*Arithmetic Geometry and Public Key Cryptography*” (2004).
- [FL03] G. Frey and T. Lange, “*Mathematical Background of Public Key Cryptography*”, “*Séminaires et congrès*”, **11** (2003), 41–73.
- [FR94] G. Frey and H.-G. Rück, “*A remark concerning  $m$ -divisibility and the discrete logarithm problem in the divisor class group of curves*”, *Math. Comp.*, **52** (1994), 865–874.

- [Gag03] M. Gagné, “*Identity-Based Encryption: a Survey*”, CryptoBytes, **6** Number 1, RSA Laboratories (2003), 10–19.
- [Gal01] S. Galbraith, “*Supersingular Curves in Cryptography*”, in *Advances in Cryptology- ASIACRYPT 2001*, Lecture Notes in Computer Science, vol. **2248**, Springer (2001), 495–513.
- [Gal05] S. Galbraith, “*Pairings*”, in [BSS04].
- [GR04] S. Galbraith and V. Rotger, “*Easy decision Diffie-Hellman groups*”, LMS J. Comput. Math., **7** (2004), 201–218.
- [GHKRW05] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler and A. Weng, “*The  $p$ -adic CM-method for genus 2*”, available online at <http://www.arxiv.org/math.NT/0503148> (2005).
- [GM06] G. van der Geer and B. Moonen, preliminary versions of “*Abelian Varieties*”, book in preparation, available on-line at <http://staff.science.uva.nl/~bmoonen/boek/BookAV.html>.
- [GV92a] G. van der Geer and M. van der Vlugt, “*Supersingular Curves of Genus 2 over finite fields of Characteristic 2*”, Math. Nachr., **159** (1992), 73–81.
- [GV92b] G. van der Geer and M. van der Vlugt, “*Reed-Muller codes and supersingular curves. I*”, Compositio Math., **84** (1992), 333–367.
- [GKR05] M. Girard, D. Kohel and C. Ritzenthaler, “*The Weierstrass subgroup of a curve has maximal rank*”, available online at <http://www.arxiv.org/math.NT/0504130v1> (2005).
- [Gor97] E. Z. Goren, “*On certain reduction problems concerning abelian surfaces*” Manuscripta Mathematica, **94** (1997) 33–43.
- [Har77] R. Hartshorne, “*Algebraic Geometry*”, Graduate Texts in Mathematics, vol. **52**, Springer-Verlag, New York (1977).
- [Has34] H. Hasse, “*Theorie der relativ-zyklischen algebraischen Funktionkörper, insbesondere bei endlichem Konstantkörper*”, J. Reine Angew. Math., **172** (1934), 37–54.
- [Her68] I. Herstein, “*Noncommutative Rings*”, The Carus Mathematical Monographs, vol. **15**, The Mathematical Association of America (Distributed by John Wiley and Sons, Inc.) (1968).

- [Hes04] F. Hess, “A Note on the Tate pairing of Curves over Finite Fields”, Arch. Math., **82** (2004), 28–32 .
- [Hur03] N. Hurt, “*Many Rational Points: Coding Theory and Algebraic Geometry*”, Kluwer Academic Pub (2003).
- [Igu60] J. Igusa, “Arithmetic variety of moduli for genus two”, Ann. of Math., **72** (1960), 612–649.
- [JMS04] M. Jacobson, A. Menezes and A. Stein, “Hyperelliptic curve cryptosystems”, in “*High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams*”, Fields Institute Communications Series, **41** (2004), 255–282.
- [JSW05] M. Jacobson, R. Scheidler and H.C. Williams, “An Improved Real Quadratic Field Based Key Exchange Procedure”, available online at <http://www.math.ucalgary.ca/rscheidl/publications.html> (2005).
- [Jou00] A. Joux, “A one round protocol for tripartite Diffie-Hellman ”, in the Proceedings of the Fourth Algorithmic Number Theory Symposium , Lecture Notes in Computer Science, vol. **1838**, Springer (2000), 385–394.
- [JN03] A. Joux and K. Nguyen, “Separating decision Diffie-Hellman from computational Diffie-Hellman in cryptographic groups”, J. Cryptology, **16** Number 4 (2003), 39–47.
- [Kob98] N. Koblitz, “*Algebraic Aspects of Cryptography*”, Algorithms and computation in mathematics, **3**, Springer, Berlin-London (1998).
- [Lan83] S. Lang, “*Complex Multiplication*”, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen, vol. **255**, Springer-Verlag, Berlin- Heidelberg (1983).
- [LO98] K.-Z. Li and F. Oort, “*Moduli of supersingular abelian varieties*”, Lecture Notes in Mathematics, vol. **1680**, Springer (1998).
- [Lor96] D. Lorenzini, “*An Invitation to Arithmetic Geometry*”, Graduate Studies in Mathematics, vol. **9**, American Mathematical Society (1996).

- [LST64] J. Lubin, J.-P. Serre and J. Tate, “*Elliptic curves and formal groups*”, available online at <http://www.ma.utexas.edu/users/voloch/1st.html> (1964).
- [MN04] D. Maisner and E. Nart, “*Zeta functions of supersingular curves of genus two*”, available online at <http://www.arxiv.org/math.NT/0408383v1> (2004).
- [Man63] Y. Manin, “The theory of commutative formal groups over fields of finite characteristic”, *Usp. Math.*, **18** (1963), 3–90; *Russ. Math. Surveys*, **18** (1963), 1–80.
- [MWZ98] A. Menezes, Y.-H. Wu and R. Zuccherato, “*An Elementary Introduction to Hyperelliptic Curves*”, in [Kob98], 155–178.
- [Mil04] V. Miller, “*The Weil Pairing, and Its Efficient Calculation*”, *J. Cryptology*, **17** (2004), 235–261
- [Mil86] J. Milne, “*Arithmetic Duality Theorems*”, Academic Press (1986), Second Edition available online at <http://www.jmilne.org/math/> (2004).
- [MVZ98] V. Müller, S. Vanstone and R. Zuccherato, “*Discrete logarithm based cryptosystems in quadratic function fields of characteristic 2*”, *Des. Codes Cryptogr.*, **14** Number 2 (1998), 159–178.
- [Mum84] D. Mumford, “*Tata Lectures on Theta*”, vol. **2**, Birkhäuser (1992).
- [Neu99] J. Neukirch, “*Algebraic Number Theory*”, Die Grundlehren der mathematischen Wissenschaften, vol. **322**, Springer-Verlag, Berlin-London (1999).
- [NSW86] J. Neukirch, A. Schmidt and K. Wingberg, “*Cohomology of Number Fields*”, Die Grundlehren der mathematischen Wissenschaften, vol. **323**, Springer, Berlin-London (1986).
- [Oor70] F. Oort, “*Subvarieties of moduli spaces*”, *Inv. Math.*, **24** (1970), 95–119.
- [Pat02] K. Paterson, “*Cryptography from pairings: a snapshot of current research*”, Information Security Technical Report, **7** Number 3 (2002), 41–54.
- [Pat05] K. Paterson, “*Cryptography from pairings*”, in [BSS04].

- [Pie82] R. S. Pierce, “*Associative Algebras*”, Graduate Texts in Mathematics, vol. **88**, Springer, New York-Heidelberg-Berlin (1982).
- [Puj02] J. Pujolàs, “*Corbes de gènere dos sobre cossos de característica dos*”, Tesina, Universitat Autònoma de Barcelona (2002).
- [Rei75] I. Reiner, “*Maximal Orders*”, London Mathematical Society Monographs, Academic Press (1975).
- [RS02] K. Rubin and A. Silverberg, “*Supersingular abelian varieties in cryptology*”, in M. Yung (ed.), CRYPTO 2002, Lecture Notes in Computer Science, vol. **2442**, Springer (2002), 336–353.
- [Sch05] E. Schaefer, “*A new proof for the non-degeneracy of the Frey-Rück Pairing and a connection to isogenies over the base field*”, available online at <http://www.iacr.org>.
- [Sch00] R. Scheidler, “*Decision Problems in Quadratic Function Fields of High Genus*”, *Journal of Complexity*, **16** (2000), 411–423.
- [SSW96] R. Scheidler, A. Stein and H. C. Williams, “*Key exchange in real quadratic congruence function fields*”, *Des. Codes Cryptogr.*, **7** (1996), 153–174.
- [Ser94] J.-P. Serre, “*Cohomologie Galoisienne*”, Lecture Notes in Mathematics, Number **5**, Springer (1994) (reprint).
- [Sil86] J. Silverman, “*The arithmetic of elliptic curves*”, Graduate Texts in Mathematics, Springer (1986).
- [Sti93] H. Stichtenoth, “*Algebraic Function Fields and Codes*”, Springer-Verlag (1993).
- [SX95] H. Stichtenoth and C. Xing, “*On the structure of the divisor class group over a class of curves over finite fields*”, *Arch. Math.*, **65** (1995), 141–150.
- [Tat66] J. Tate, “*Endomorphisms of abelian varieties over finite fields*”, *Inv. Math.*, **2** (1966), 134–144.
- [Ver04] E. Verheul, “*Evidence that XTR is more secure than supersingular elliptic curve cryptosystems*”, *J. Cryptology*, **17** (2004), 277–296.

- [Vol95] E. Volcheck, “*Computing in the Jacobian of a plane algebraic curve*”, in the Proceedings of the First Algorithmic Number Theory Symposium, Lecture notes in Computer Science, vol. **877**, Springer (1998), 221–233.
- [Wam99a] P. van Wamelen, “*Examples of genus two CM curves defined over the rationals*”, Math. Comp. , **68** Number 225 (1999), 307–320.
- [Wam99b] P. van Wamelen, “*Proving that a genus 2 curve has Complex Multiplication*”, Math. Comp. , **68** Number 228 (1999), 1663–1677.
- [Wat79] W. C. Waterhouse, “*Introduction to Affine Group Schemes*”, Graduate Texts in Mathematics **2066**, Springer (1979).
- [Wei67] A. Weil, “*Basic Number Theory*”. Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen, vol. **144**, Springer-Verlag, Berlin- Heidelberg (1967).
- [Yui78] N. Yui, “*On the jacobian varieties of hyperelliptic curves over fields of characteristic  $p > 2$* ”, J. Alg., **52** (1978), 378–410.
- [Zag81] D. Zagier, “*Zetafunktionen und quadratische Körper. Eine Einführung in die höhere Zahlentheorie*”, Hochschultext, Springer-Verlag, Berlin-New York (1981).
- [Zuc97] R. Zuccherato, “*The continued fraction algorithm and regulator for quadratic function fields of characteristic 2*”, J. Algebra, **190** Number 2 (1997), 563–587.
- [Zuc98] R. Zuccherato, “*The Equivalence between Elliptic Curve and Quadratic Function Field Discrete Logarithms in Characteristic 2*”, Algorithmic number theory (Portland, OR, 1998), 621–638, in Lecture Notes in Computer Science, vol. **1423**, Springer, Berlin (1998).