Abelian varieties and cryptography

GERHARD FREY

Institut fr Experimentelle Mathematik,
Universitt Duisburg-Essen,
45326 Essen, Germany.

TONY SHASKA

Department of Mathematics and Statistics,
Oakland University,
Rochester, MI 48309, USA.

Abstract. The main purpose of this paper is to give the latest developments in the theory of abelian varieties and their usage in cryptography. In the first part we provide the necessary mathematical background on abelian varieties, their torsion points, Honda-Tate theory, Galois representations, with emphasis on Jacobian varieties and hyperelliptic Jacobians. In the second part we focus on applications of abelian varieties on cryptography and treating separately, elliptic curve cryptography, hyperelliptic curve cryptography for genus 2 and 3, and isogenies of Jacobians via correspondences. Many open problems are suggested through the paper.

Contents

E-mail addresses: `frey@iem.uni-due.de, shaska@oakland.edu`.

2010 *Mathematics Subject Classification.* 14H10,14H45.

Preface

There has been a continued interest on Abelian varieties in mathematics during the last century. Such interest is renewed in the last few years, mostly due to applications of abelian varieties in cryptography. In these notes we give a brief introduction to the mathematical background on abelian varieties and their applications on cryptography with the twofold aim of introducing abelian varieties to the experts in cryptography and introducing methods of cryptography to the mathematicians working in algebraic geometry and related areas.

A word about cryptography. Information security will continue to be one of the greatest challenges of the modern world with implications in technology, politics, economy, and every aspect of everyday life. Developments and drawbacks of the last decade in the area will continue to put emphasis on searching for safer and more efficient crypto-systems. The idea and lure of the quantum computer makes things more exciting, but at the same time frightening.

There are two main methods to achieve secure transmission of information: *secret-key cryptography* (*symmetric-key*) and *public-key cryptography* (*asymmetric-key*). The main disadvantage of symmetric-key cryptography is that a shared key must be exchanged beforehand in a secure way. In addition, managing keys in a large public network becomes a very complex matter. Public-key cryptography is used as a complement to secret-key cryptography for signatures of authentication or key-exchange. There are two main methods used in public-key cryptography, namely RSA and the discrete logarithm problem (DLP) in cyclic groups of prime order which are embedded on abelian varieties. The last method is usually referred to as *curve-based cryptography*.

In addition, there is always the concern about the post-quantum world. What will be the crypto-systems which can resist the quantum algorithms? Should we develop such systems now? There is enthusiasm in the last decade that some aspects of curve-based cryptography can be adapted successfully to the post-quantum world. Supersingular Isogeny Diffie-Hellman (SIDH), for example, is based on isogenies of supersingular elliptic curves and is one of the promising schemes for post-quantum cryptography. Isogenies of hyperelliptic Jacobians of dimension 2 or 3 have also been studied extensively in the last decade and a lot of progress has been made. In this paper we give an overview of recent developments in these topics.

Audience. Computer security and cryptography courses for mathematics and computer science majors are being introduced in all major universities. Curve-based cryptography has become a big part of such courses and a popular area even among professional mathematicians who want to get involved in cryptography. The main difficulty that these newcomers is the advanced mathematical background needed to be introduced to curve-based cryptography.

Our target audience is advanced graduate students and researchers from mathematics or computer science departments who work with curve-based cryptography. Many researchers from other areas of mathematics who want to learn about abelian varieties and their use in cryptography will find these notes useful.

Notations and bibliography. The symbols $\mathbb{N}$ and $\mathbb{Z}$ will denote the natural numbers and the ring of integers while $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ the fields of rationals, reals, and complex numbers. $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ will denote the field of p elements, for a prime number p and $\mathbb{F}_q$ a field of q elements, where $q = p^n$ is a power of p.

In general a field will be denoted by k. We shall always assume that k is a perfect field, i.e., every algebraic extension of k is separable.
Denote its characteristic by char k, and its algebraic closure by $\bar{k}$. The Galois group $\mathrm{Gal}(\bar{k}/k)$ will be denoted by G_k. A number field will be denoted by K and its ring of integers by $\mathcal{O}_K$.

By a "curve" we mean an irreducible, smooth, algebraic curve. A genus $g \geq 2$ curve defined over k will be denoted by $\mathcal{X}/k$ or sometimes by $\mathcal{X}_g$ and its Jacobian by $\mathrm{Jac}\,\mathcal{X}$. The automorphism group of $\mathcal{X}$, is denoted by $\mathrm{Aut}\,\mathcal{X}$ and it means the full group of automorphisms of $\mathcal{X}$ over the algebraic closure $\bar{k}$.

We will use $\mathcal{A}$, $\mathcal{B}$ to denoted Abelian varieties defined over a field k and $k(\mathcal{A})$, $k(\mathcal{B})$ their function fields. The set of n-torsion points of $\mathcal{A}$ will be denoted by $\mathcal{A}[n]$. For a subgroup G of $\mathcal{A}$, the quotient variety is denoted by $\mathcal{A}/G$.

Background and preliminaries. We assume the reader is familiar with the basic tools from algebra and algebraic geometry. Familiarity with algebraic curves in the level of [25] is expected and the ability to read some of the classical works on the subject [48], [47].

Organization of these notes. In Part 1 we give the mathematical background on Abelian varieties, their torsion points, and isogenies. We focus mostly on Abelian varieties defined over fields of positive characteristic. The main references here are [47], [48], and [22].

We give a brief introduction of abelian varieties as complex tori and period matrices in Section 1. In Section 2 we focus on endomorphism rings of abelian varieties and isogenies. We define the characteristic polynomial of the Frobenius, l-adic Tate module, and Tate's result on determining necessary and sufficient conditions for two Abelian varieties to be isogenous.

Jacobian varieties are treated in detail in Section 3, including Picard groups on curves, the group of divisors, canonical divisors, and the definition of the Jacobians. In Section **??** we focus on the hyperelliptic Jacobians. We give an explicit construction of the group law, including a geometric interpretation analogue to that of the elliptic curves from [37], and a generalization of division polynomials from [5] and more recent work [32]. In Section 5 is given a brief introduction to modular curves and their compactification.

In Part 2 we focus on applications of abelian varieties on cryptography. Our main reference is [7] and the material provided in Part 1. In Section 7 we describe the methods of index calculus in Picard groups and their use in cryptography. Such methods have been quite successful due to work of Diem, Gaudry, et al. As consequence one sees that only elliptic and hyperelliptic curves of genus ≤ 3 provide candidates for secure crypto systems based on discrete logarithms. Hence we shall discuss these curves in detail. In Section 8 we focus on isogenies of Jacobians via correspondences. We discuss the Weil descent, modular correspondences, and correspondences via monodromy groups. It is an open and difficult problem to find interesting correspondences of low degree between Jacobian varieties induced by correspondences between curves.

In Section 9 we focus on the elliptic curves and elliptic curve cryptography. We give an explicit description of the methods used in supersingular isogeny-based cryptography. We describe the necessary background including Velu's formula, ordinary and supersingular elliptic curves and the more recent results [11], [10], [12] among others. The reason why isogeny-based cryptography could lead to some very interesting applications is because the isogeny graphs of supersingular elliptic curves are Ramanujan graphs with very interesting properties. We describe the length of a random walk in such graphs in proposition 9 which is due to results in [12].

In Section 10 we focus on dimension 2 Jacobians and their use in cryptography. We give a brief geometric interpretation of the addition in a 2-dimensional Jacobian and determine explicit formulas for $[n]D$, when D is a reduced divisor. Methods based on [39] of how to compute the endomorphism ring of a dimension 2 Jacobian are described. Moreover, we describe in detail the modular polynomials of genus 2 introduced by Gaudry, Dupont, Lauter and others. For a fixed prime p denominators of these modular polynomials are divisible by the equation of the Hurwitz space of the Frey-Kani covers, introduced by the first author of this paper in [23] and computed by the second author for $p = 3, 5$ in [52], [44]. We continue with the study of endomorphisms and in particular isogenies of Abelian surfaces via Donagi-Livné approach and some recent results of Smith [59].

In Section 11 we study hyperelliptic Jacobians of dimension 3. We give a short introduction of non-hyperelliptic and hyperelliptic genus 3 curves and their plane equations. Then we define Picard groups of genus 3 curves and their use in cryptography and results of Diem and Hess. In the following part we describe the index-calculus attacks applied to genus 3 and results of Diem, Gaudry, Thomé, Thériault. We also discuss isogenies via S_4-covers and work of Frey and Kani [23], [24] and Smith [59].

Throughout these notes we have aimed at giving brief accounts of some of the recent trends of research taking place on abelian varieties and their applications in cryptography. The reader is encouraged to check the original works for further details.

Part 1. Abelian varieties

In the first part of these notes we give the basic theory of abelian varieties, their endomorphisms, torsion points, characteristic polynomial of the Frobenius, Tate models, and then focus on Jacobian varieties and hyperelliptic Jacobians. While there are many good references on the topic, we mostly use [48], [47], [62].

1. Definitions and basic properties

We shall use projective respectively affine *schemes* defined over k. Let $n \in \mathbb{N}$ and I_h (respectively I) be a homogeneous ideal in $k[Y_0, \cdots, Y_n]$ different from $< Y_0, \dots Y_n >$ (respectively an arbitrary ideal in $k[X_1, \dots, X_n]$). Let $R_h := k[Y_0, \dots, Y_n]/I_h$ (respectively $R := k[X_1, \dots, X_n]/I$) be the quotients. By assumption, R_h is a graded ring, and so localizations $R_{h,\mathfrak{A}}$ with respect to homogeneous ideals $\mathfrak{A}$ are graded, too. Let $R_{h,\mathfrak{A}\ 0}$ be the ring of elements of grade 0.

The projective scheme $\mathcal{S}_h$ (respectively the affine scheme $\mathcal{S}$) defined by I_h (I) consists of

(1) the topological space $V_h := \text{Proj}(R_h)$ $(V := \text{Spec(R)})$ consisting of homogeneous prime ideals in R_h with pre-image in $k[Y_0, \dots, Y_n]$ different from $< Y_0, \dots Y_n >$ (prime ideals in R) endowed with the Zariski topology and
(2) the sheaf of rings of holomorphic functions given on Zariski-open sets $U \subset V_h$ $(U \subset V)$ as elements of grade 0 in localization of $R_{h,0}$ (R) with respect to the elements that become invertible when restricted to U.

Examples:

1) The projective space $\mathbb{P}^n$ over k of dimension n is given by the ideal $< 0 > \subset k[Y_0, \dots, Y_n]$. The ring of holomorphic functions on $\mathbb{P}^n$ (take $U = \mathbb{P}^n$) is k.

Next take $U = \emptyset$ to get the ring of *meromorphic* functions on $\mathbb{P}^n$: It consists of the quotients

$$f/g \text{ with } f, g \text{ homogeneous of degree d with } g \neq 0.$$

2) The affine space $\mathbb{A}^n$ of dimension n over k is the topological space

$$\text{Spec}(k[X_1, \dots X_n]).$$

The ring of holomorphic functions on A^n is $k[X_1, \dots, X_n]$, where polynomials are interpreted as polynomial functions. The ring of meromorphic functions on $\mathbb{A}^n$ (take $U = \emptyset$) is the field of rational functions $k(X_1, \dots, X_n)$.

3) The easiest but important example for an affine scheme: Take $n = 1$, $I =< X_1 >$, $V = \text{Spec}(k) = \{(0)\}$ and $O_{(0)} = k^*$.

Morphisms of affine or projective schemes are continuous maps between the underlying topological spaces induced (locally) by (in the projective case, quotients of the same degree) of polynomial maps of the sheaves.

Rational maps f between affine or projective schemes $\mathcal{S}$ and $\mathcal{T}$ are equivalence classes of morphisms defined on open subschemes U_i of $\mathcal{S}$ with image in $\mathcal{T}$ and compatible with restrictions to $U_i \cap U_j$. If f is invertible (as rational maps from $\mathcal{T}$ to $\mathcal{S}$), then f is *birational*, and $\mathcal{S}$ and $\mathcal{T}$ are birationally equivalent.

The k-rational points $\mathcal{S}(k)$ of a scheme $\mathcal{S}$ is the set of morphisms from Spec(k) to $\mathcal{S}$. The reader should verify that for projective schemes defined by the ideal I_h the set $\mathcal{S}(k)$ is, in a natural way, identified with points $(y_0 : y_1 \cdots : y_n)$ with k-rational homogeneous coordinates in the projective space of dimension n which are common zeros of the polynomials in I_h, and an analogous statement holds for affine schemes.

Constant field extensions: Let $k \overset{\iota}{\hookrightarrow} L$ be an embedding of k into a field L (or $k \subset L$ if the embedding is clear) of k. Let $\mathcal{S}$ be a projective (affine) scheme defined over k with ring R. ι induces a morphism $\mathfrak{f}_\iota$ from R in $R \otimes_k L =: R_\iota$ given by the interpretation via ι of polynomials with coefficients in k as polynomials with coefficients in L. The prime ideal $I_{\mathcal{S}}$ extends to a prime ideal in R_ι and hence we get in a natural way a projective variety $\mathcal{S}_\iota$ with a morphism

$$\mathcal{S}_\iota \to \mathcal{S}$$

as Spec(k) schemes. $\mathcal{S}_\iota$ is again a projective (affine) scheme now defined over L, which is denoted as *scalar extension* by ι. If there is no confusion possible (for instance if $k \subset L \subset \bar{k}$ and ι is the inclusion) we denote $\mathcal{S}_\iota$ by $\mathcal{S}_L$.

A scheme $\mathcal{S}$ is irreducible if the ideal I_h (respectively I) is a prime ideal. $\mathcal{S}$ is absolutely irreducible if $\mathcal{S}_{\bar{k}}$ is irreducible. This is the case if and only if k is algebraically closed in R. Classically, irreducible schemes are called *irreducible varieties.*

Affine covers There are many possibilities to embed $\mathbb{A}^n$ into $\mathbb{P}^n$, and there is no "canonical" way to do this. But after having chosen coordinates there is a standard way to construct a covering of $\mathbb{P}^n$ by $n+1$ copies of $\mathbb{A}^n$. Every homogeneous polynomial $P(Y_0, ..., Y_n)$ can be transformed into $n+1$ polynomials $p_j(X)$ $(j = 0, ..., n)$ in n variables by the transformation

$$t_j : Y_i \mapsto X_i := Y_i/Y_j.$$

Define U_j as open subscheme of $\mathbb{P}^n$ which is the complement of the projective scheme attached to the ideal $< Y_j >$. Then $t_j\,_{|U_j}$ is holomorphic and bijective and its image is isomorphic to $\mathbb{A}^n$: This image is the intersection of $\mathbb{P}^n$ with the *hyperplane* given by the homogeneous equation $Y_j = 0$.

By the inverse transform ι_j we embed $\mathbb{A}^n$ into $\mathbb{P}^n$ and so U_j is isomorphic to $\mathbb{A}^n$ as affine variety. Taking the collection $(\iota_0, \ldots \iota_n)$ we get a finite open covering of $\mathbb{P}^n$ by $n+1$ affine subspaces.

Having an affine cover U_j of $\mathbb{P}^n$ one can intersect it with projective varieties V and get

$$V = \bigcup_j V_{j,a} \text{with } V_{j,a} := V \cap U_j$$

as union of affine varieties.

Converse process: Given a polynomial $p(X_1, ..., X_n)$ of degree d we get a homogeneous polynomial $p^h(Y_0, ..., Y_n)$ of degree d by the transformation

$$X_i \mapsto Y_i/Y_0 \text{ for } i = 1, ..., n$$

and then clearing denominators. Assume that V_a is an affine variety with ideal $I_a \subset K[X_1, ..., X_n]$. By applying the homogenization explained above to all polynomials in I_a we get a homogeneous ideal $I_a^h \subset K[Y_0, ..., Y_n]$ and a projective variety V with ideal I_a^h containing V_a in a natural way. V is called a projective closure of V_a. By abuse of language one calls $V \cap U_0 = V \setminus V_a$ "infinite points" of V_a.

Function Fields: Let $\mathcal{S} \subset \mathbb{A}^n$ be an affine irreducible variety with ring R . In particular, R is an integral domain. The function field $k(\mathcal{S})$ is the quotient field of

R. It consists of the meromorphic functions of $\mathbb{A}^n$ restricted to $\mathcal{S}$. $\mathcal{T}$ is birational equivalent to $\mathcal{S}$ if and only if $k(\mathcal{S}) = k(\mathcal{T})$.

If $\emptyset \neq U$ is affine and open in a projective variety $\mathcal{S}$ then the field of meromorphic functions $k(V)$ is equal to $k(U)$. In particular, it is independent of the choice of U.

Definition 1. Let $\mathcal{S}$ be an irreducible variety. The dimension of $\mathcal{S}$ is the transcendental degree of $k(\mathcal{S})$ over k.

Group schemes: A projective (affine) group scheme G defined over k is a projective (affine) scheme over k endowed with

i) addition, i.e., a morphism

$$m: \; G \times G \to G$$

ii) inverse, i.e., a morphism

$$i: \; G \to G$$

iii) the identity, i. e., a k-rational point $0 \in G(k)$,

such that it satisfies group laws. The group law is uniquely determined by the choice of the identity element.

A morphism of group schemes that is compatible with the addition law is a homomorphism.

Let L be a field extension of k. $G(L)$ denotes the set of L-rational points of G and it is also a group. A homomorphism between groups schemes induces a homomorphism between the group of rational points. If G is a projective variety, then the group law m is commutative.

Definition 2. An Abelian variety defined over k is an absolutely irreducible projective variety defined over k which is a group scheme.

We will denote an Abelian variety defined over a field k by $\mathcal{A}_k$ or simply $\mathcal{A}$ when there is no confusion. From now on the addition $m(P, Q)$ in an abelian variety will be denoted by $P \oplus Q$ or simply $P + Q$ and the inversion $i(P)$ by $\ominus P$ or simply by $-P$.

Fact: A morphism from the Abelian varieties $\mathcal{A}_1$ to the Abelian variety $\mathcal{A}_2$ is a homomorphism if and only if it maps the neutral element of $\mathcal{A}_1$ to the neutral element of $\mathcal{A}_2$.

An abelian variety over a field k is called **simple** if it has no proper nonzero Abelian subvariety over k, it is called **absolutely simple** (or **geometrically simple**) if it is simple over the algebraic closure of k.

1.1. Complex tori and abelian varieties. Though we are interested in Abelian varieties over arbitrary fields k or in particular, over finite fields, it is helpful to look at the origin of the whole theory, namely the theory of Abelian varieties over the complex numbers. Abelian varieties are connected, projective algebraic group schemes. Their analytic counterparts are the connected compact Lie groups.

Let d be a positive integer and $\mathbb{C}^d$ the complex Lie group (i.e., with vector addition as group composition). The group $\mathbb{C}^d$ is not compact, but we can find quotients which are compact. Choose a lattice $\Lambda \subset \mathbb{C}^d$ which is a $\mathbb{Z}$-submodule of rank $2d$. The quotient $\mathbb{C}^d/\Lambda$ is a complex, connected Lie group which is called a *complex d-dimensional torus.* Every connected, compact Lie group of dimension d is isomorphic to a torus $\mathbb{C}^d/\Lambda$.

A hermitian form H on $\mathbb{C}^d \times \mathbb{C}^d$ is a form that can be decomposed as

$$H(x,y) = E(ix,y) + i\,E(x,y),$$

where E is a skew symmetric real form on $\mathbb{C}^d$ satisfying $E(ix,iy) = E(x,y)$. E is called the imaginary part $\mathrm{Img}(H)$ of H.

The torus C^d/Λ can be embedded into a projective space if and only if there exists a positive Hermitian form H on $\mathbb{C}^d$ with $E = \mathrm{Img}(H)$ such that restricted to $\Lambda \times \Lambda$ has values in $\mathbb{Z}$. Let $\mathbb{H}_g$ be the Siegel upper half plane

$$\mathbb{H}_d = \{\tau \in \mathrm{Mat}_d(\mathbb{C}) \mid \tau^T = \tau,\, \mathrm{Img}(\tau) > 0\}.$$

Then, we have the following.

Lemma 1. *Let $\mathbb{C}^d/\Lambda$ be a complex torus attached to an abelian variety $\mathcal{A}$. Then Λ is isomorphic to $\mathbb{Z}^d \oplus \Omega \cdot \mathbb{Z}^d$, where $\Omega \in \mathbb{H}_d$.*

The matrix Ω is called the **period matrix** of $\mathcal{A}$. The lattice $\hat{\mathcal{A}}$ given by

$$\hat{\mathcal{A}} := \{x \in \mathbb{C}^d \,|\, E(x,y) \in \mathbb{Z}, \;\; \text{for all} \;\; y \in \lambda\}$$

is called the **dual lattice** of Λ. If $\hat{\mathcal{A}} = \mathcal{A}$ then $\mathcal{A}$ is called a **principally polarized** abelian variety.

For a principally polarized abelian variety $\mathcal{A}$ there exists a basis $\{\mu_1, \dots, \mu_{2d}\}$ of Λ such that

$$J := [E(\mu_i, \mu_j)]_{1 \le i,j \le 2d} = \begin{bmatrix} 0 & I_d \\ -I_d & 0 \end{bmatrix}.$$

The symplectic group

$$Sp(2d,\mathbb{Z}) = \{M \in GL(2d,\mathbb{Z}) \mid MJM^T = J\}$$

acts on $\mathbb{H}_d$, via

$$\begin{gathered} Sp(2d,\mathbb{Z}) \times \mathcal{H}_d \to \mathcal{H}_d \\ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \times \tau \to (a\tau + b)(c\tau + d)^-1 \end{gathered}$$

where a,b,c,d,τ are $d \times d$ matrices. The moduli space of d-dimensional abelian varieties is

$$\mathbf{A}_g := \mathbb{H}_d / Sp(2d,\mathbb{Z}).$$

The Jacobian of a projective irreducible nonsingular curve is a principally polarized abelian variety. We will see Jacobian varieties in more detail in section 3.

2. Endomorphisms and isogenies

Let $\mathcal{A}$, $\mathcal{B}$ be abelian varieties over a field k. We denote the $\mathbb{Z}$-module of homomorphisms $\mathcal{A} \mapsto \mathcal{B}$ by $\mathrm{Hom}(\mathcal{A},\mathcal{B})$ and the ring of endomorphisms $\mathcal{A} \mapsto \mathcal{A}$ by $\mathrm{End}\,\mathcal{A}$.

In the context of Linear Algebra it can be more convenient to work with the vector spaces $\mathrm{Hom}^0(A,B) := \mathrm{Hom}(A,B) \otimes_{\mathbb{Z}} \mathbb{Q}$, and $\mathrm{End}^0 A := \mathrm{End}\,A \otimes_{\mathbb{Z}} \mathbb{Q}$. Determining $\mathrm{End}\,\mathcal{A}$ or $\mathrm{End}^0 A$ is an interesting problem on its own; see [50].

For any abelian variety $\mathcal{A}$ defined over a a number field K, computing $\mathrm{End}_K(\mathcal{A})$ is a harder problem than computation of $\mathrm{End}_{\bar{K}}(\mathcal{A})$; see [39, lemma 5.1] for details.

Lemma 2. *If there exists an algorithm to compute* $\operatorname{End}_K(\mathcal{A})$ *for any abelian variety of dimension* $g \geq 1$ *defined over a number field* K*, then there is an algorithm to compute* $\operatorname{End}_{\bar{K}}(\mathcal{A})$*.*

2.1. Isogenies. A homomorphism $f : \mathcal{A} \to \mathcal{B}$ is called an **isogeny** if $\operatorname{Img} f = \mathcal{B}$ and $\ker f$ is a finite group scheme. If an isogeny $\mathcal{A} \to \mathcal{B}$ exists we say that $\mathcal{A}$ and $\mathcal{B}$ are isogenous. We remark that this relation is symmetric, see Lemma lemma 6.

The degree of an isogeny $f : \mathcal{A} \to \mathcal{B}$ is the degree of the function field extension

$$\deg f := [K(\mathcal{A}) : f^\star K(\mathcal{B})].$$

It is equal to the order of the group scheme $\ker(f)$.

The group of $\bar{k}$rational points has order $\#(\ker f)(\bar{k}) = [K(A) : f^\star K(B)]^{sep}$, where $[K(A) : f^\star K(B)]^{sep}$ is the degree of the maximally separable extension in $K(\mathcal{A})/f^\star K(\mathcal{B})$. f is a **separable isogeny** iff

$$\# \ker f(\bar{k}) = \deg f.$$

Equivalently: The group scheme $\ker f$ is étale.

The following result should be compared with the well known result of quotient groups of abelian groups.

Lemma 3. *For any Abelian variety* $\mathcal{A}/k$ *there is a one to one correspondence between the finite subgroup schemes* $\mathcal{K} \leq \mathcal{A}$ *and isogenies* $f : \mathcal{A} \to \mathcal{B}$*, where* $\mathcal{B}$ *is determined up to isomorphism. Moreover,* $\mathcal{K} = \ker f$ *and* $\mathcal{B} = \mathcal{A}/\mathcal{K}$*.*

f is separable if and only if $\mathcal{K}$ is étale, and then $\deg f = \#\mathcal{K}(\bar{k})$*.*

Isogenous Abelian varieties have commensurable endomorphism rings.

Lemma 4. *If* $\mathcal{A}$ *and* $\mathcal{B}$ *are isogenous then* $\operatorname{End}^0(\mathcal{A}) \cong \operatorname{End}^0(\mathcal{B})$*.*

Lemma 5. *If* $\mathcal{A}$ *is a absolutely simple Abelian variety then every endomorphism not equal* 0 *is an isogeny.*

We can assume that $k = \bar{k}$. Let f be an isogeny $\neq 0$ of $\mathcal{A}$. Its kernel $\ker f$ is a subgroup scheme of $\mathcal{A}$ (since it is closed in the Zariski topology because of continuity and under $\oplus$ because of homomorphy). It contains $0_{\mathcal{A}}$ and so its connected component, which is, by definition, an Abelian variety.

Since $\mathcal{A}$ is simple and $f \neq 0$ this component is equal to $\{0_{\mathcal{A}}\}$. But it has finite index in $\ker f$ (Noether property) and so $\ker f$ is a finite group scheme.

2.1.1. *Computing isogenies between Abelian varieties.* Fix a field k and let $\mathcal{A}$ be an Abelian variety over k. Let H denote a finite subgroup of $\mathcal{A}$. From the computational point of view we have the following problems:

- Compute all Abelian varieties $\mathcal{B}$ over k such that there exists an isogeny $\mathcal{A} \to \mathcal{B}$ whose kernel is isomorphic to H.
- Given $\mathcal{A}$ and H, determine the quotient $\mathcal{B} := \mathcal{A}/H$ and the isogeny $\mathcal{A} \to \mathcal{B}$.
- Given two Abelian varieties $\mathcal{A}$ and $\mathcal{B}$, determine if they are isogenous and compute a rational expression for an isogeny $\mathcal{A} \to \mathcal{B}$.

There is a flurry of research activity in the last decade to solve these problems explicitly for low dimensional Abelian varieties; see [40], [42] among many others. For a survey and some famous conjectures on isogenies see [22].

Remark 1. *For elliptic curves (Abelian varieties of dimension* 1*) and for Jacobians of curves of genus* 2 *we shall come back to these questions in more detail.*

2.2. Torsion points and Tate modules. The most classical example of a separable isogeny is the scalar multiplication by n map:

$$[n] : \mathcal{A} \to \mathcal{A}$$

The kernel of $[n]$ is a group scheme of order $n^{2 \dim \mathcal{A}}$ (see [48]). We denote by $\mathcal{A}[n]$ the group $\ker[n](\bar{k})$. The elements in $\mathcal{A}[n]$ are called n-**torsion points** of $\mathcal{A}$.

Lemma 6. *Let* $f : \mathcal{A} \to \mathcal{B}$ *be a degree* n *isogeny. Then there exists an isogeny* $\hat{f} : \mathcal{B} \to \mathcal{A}$ *such that*

$$f \circ \hat{f} = \hat{f} \circ f = [n].$$

Corollary 1. *Let* $\mathcal{A}$ *be an (absolutely) simple Abelian variety. Then* $\mathrm{End}(\mathcal{A})^0$ *is a skew field.*

Proof. Every endomorphism $\neq 0$ of $\mathcal{A}$ is an isogeny, hence invertible in $\mathrm{End}(\mathcal{A})^0$. □

Theorem 3. *Let* $\mathcal{A}/k$ *be an Abelian variety,* $p = char\ k$*, and* $\dim \mathcal{A} = g$*.*

i) If $p \nmid n$*, then* $[n]$ *is separable,* $\#\mathcal{A}[n] = n^{2g}$ *and* $\mathcal{A}[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$*.*

ii) If $p \mid n$*, then* $[n]$ *is inseparable. Moreover, there is an integer* $0 \leq i \leq g$ *such that*

$$\mathcal{A}[p^m] \cong (\mathbb{Z}/p^m\mathbb{Z})^i, \text{ for all } m \geq 1.$$

If $i = g$ then $\mathcal{A}$ is called **ordinary**. If $\mathcal{A}[p^s](\bar{K}) = \mathbb{Z}/p^{ts}\mathbb{Z}$ then the abelian variety has p-**rank** t. If $\dim \mathcal{A} = 1$ (elliptic curve) then it is called **supersingular** if it has p-rank 0.[1] An abelian variety $\mathcal{A}$ is called **supersingular** if it is isogenous to a product of supersingular elliptic curves.

Remark 2. *If* $\dim \mathcal{A} \leq 2$ *and* $\mathcal{A}$ *has* p*-rank 0 then* $\mathcal{A}$ *is supersingular. This is not true for* $\dim \mathcal{A} \geq 3$*.*

Let l be a prime different from $p = \text{char } K$ and $k \in \mathbb{N}$. Then,

$$[l]\mathcal{A}\left[l^{k+1}\right] = \mathcal{A}[l^k].$$

Hence, the collection of groups

$$\dots \mathcal{A}[l^{k+1}], \dots, \mathcal{A}[l^k], \dots$$

forms a projective system. The l-adic Tate module of $\mathcal{A}$ is

$$T_l(\mathcal{A}) := \varprojlim \mathcal{A}[l^k].$$

Lemma 7. *The Tate module* $T_l(\mathcal{A})$ *is a* $\mathbb{Z}_l$*-module isomorphic to* $\mathbb{Z}_l^{2 \dim \mathcal{A}}$*.*

Next we will see another interpretation of the Tate module in terms of the Galois representation.

2.3. l-adic representations and characteristic polynomials.

[1] For an alternative definition see theorem 36.

2.3.1. *Galois representations.* Torsion points on abelian varieties are used to construct very important representations of the Galois group of k. Let n be relatively prime to p. Then G_k acts on $\mathcal{A}[n]$ which gives rise to a representation

$$\rho_{\mathcal{A},n} : G_k \to \operatorname{Aut}\left((\mathbb{Z}/n\mathbb{Z})^{2g}\right)$$

and after a choice of basis in $\mathcal{A}[n]$ yields a representation

$$\rho_{\mathcal{A},n} : G_k \to GL_{2g}(\mathbb{Z}/n\mathbb{Z})$$

This action extends in a natural way to $T_l(\mathcal{A}) \otimes \mathbb{Q}_\ell$ and therefore to a ℓ-adic representation $\tilde{\rho}_{\mathcal{A},l}$ which is called the **l-adic Galois representation attached to $\mathcal{A}$.**

2.3.2. *Representations of endomorphisms.* Let ϕ be an endomorphism of the g-dimensional Abelian variety $\mathcal{A}$. By restriction ϕ induces a $\mathbb{Z}$-linear map ϕ_n on $\mathcal{A}[n]$. Since the collection (ϕ_{ℓ^k}) is compatible with the system defining $T_\ell(\mathcal{A})$ it yields a $\mathbb{Z}_\ell$-linear map $\tilde{phi}_\ell$ on $T_\ell(\mathcal{A})$.

Applying this construction to all elements in $\operatorname{End}(\mathcal{A})$ we get an injection (since $\mathcal{A}[\lambda^\infty]$) is Zariski-dense in $\mathcal{A}$) from $\operatorname{End}(\mathcal{A})$ into $Gl(2g, \mathbb{Z}_\ell)$. By tensorizing with $\mathbb{Q}_\ell$ we get the ℓ-adic representation

$$\tilde{\eta}_\ell : \operatorname{End}(\mathcal{A}) \otimes \mathbb{Q}_\ell \to Gl_{2g}(\mathbb{Q}_\ell).$$

THEOREM 4. *$\tilde{\eta}_\ell$ is injective.*

For a proof see in [48, Theorem 3, p.176]. This result has important consequences for the structure of $\operatorname{End}^0(\mathcal{A})$, more precisely $\operatorname{End}^0(\mathcal{A})$ is a $\mathbb{Q}$-algebra of dimension $\leq 4\dim(\mathcal{A})^2$.

Adding more information (see Corollary 2 in [48]) one gets that $\operatorname{End}^(\mathcal{A})$ is a semi-simple algebra, and by duality (key word Rosati-involution) one can apply a complete classification due to Albert of *possible* algebra structures on $\operatorname{End}^0(\mathcal{A})$, which can be found on [48, p.202].

The question is: Which algebras occur as endomorphism algebras? The situation is well understood if k has characteristic 0 (due to Albert) but wide open in characteristic $p > 0$. For $g = 1$ (elliptic curves) everything is explicitly known due to M. Deuring. We describe the results in theorem 36.

Characteristic Polynomial: For $\phi \in \operatorname{End}^0(\mathcal{A})$ let $\tilde{\phi}_\ell$ its ℓ-adic representation. Denote its characteristic polynomial by $\chi_{\ell,\phi}(T) \in \mathbb{Z}_\ell[T]$.

THEOREM 5 (Weil). *$\chi_{\ell,\phi}(T)$ is a monic polynomial $\chi_\phi(T) \in \mathbb{Z}[T]$ which is independent of ℓ. We have*

$$\chi_\phi(\phi) \equiv 0 \text{ on } \mathcal{A},$$

*and so it is justified to call $\chi_\phi(T)$ the **characteristic polynomial** of ϕ.*

The degree of $\chi_\phi(T)$ is $2\dim(\mathcal{A})$, the second-highest coefficient is the negative of the trace of ϕ, and the constant coefficient is equal to the determinant of ϕ.

2.3.3. *Frobenius representations.* Let $\mathcal{A}$ be a g-dimensional Abelian variety defined over $\mathbb{F}_q$, where $q = p^d$ for a prime p and $\bar{\mathbb{F}}_q$ the algebraic closure of $\mathbb{F}_q$. Let $\pi \in \operatorname{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ be the Frobenius automorphism of $\mathbb{F}_q$, given by

$$\pi : x \to x^p.$$

Since $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ is topologically generated by π and because of continuity of $\rho_{\mathcal{A},n}$ it is determined by $\rho_{\mathcal{A},n}(\pi)$.

$$\chi_{\mathcal{A},q}(T) := \chi(T)\left(\tilde{\rho}_{\mathcal{A},l}(\pi)\right) \in \mathbb{Z}_\ell[T] \tag{1}$$

is the characteristic polynomial of the image of π under $\tilde{\rho}_{\mathcal{A},l}$.

Lemma 8 (Weil). *$\chi_{\mathcal{A},q}(T)$ is a monic polynomial of degree $2g$ in $\mathbb{Z}[T]$, independent of ℓ, and for all $n \in \mathbb{N}$ we get*

$$\chi_{\mathcal{A},q}(T) \equiv \chi(\rho_{\mathcal{A},n}(\pi) \mod n.$$

In the coming sections (cf. Eq. 11) we will see in more detail some of the properties of the characteristic polynomial of the Frobenius.

Lemma 9 (Tate). *We continue to take $k = \mathbb{F}_q$. The ℓ-adic representation $\tilde{\rho}_{\mathcal{A},l}$ is semi-simple and so is determined by their characteristic polynomials of the Frobenius, $\chi(T)\left(\tilde{\rho}_{\mathcal{A},l}(\pi)\right)$.*[2]

Next we have the following important result:

Theorem 6 (Tate). *Let $\mathcal{A}$ and $\mathcal{B}$ be Abelian varieties over a finite field $\mathbb{F}_q$ and $\chi_{\mathcal{A}}$ and $\chi_{\mathcal{B}}$ the characteristic polynomials of their Frobenius endomorphism and $l \neq p$ a prime. The following are equivalent.*
i) $\mathcal{A}$ and $\mathcal{B}$ are isogenous.
ii) $\chi_{\mathcal{A},q}(T) \equiv \chi_{\mathcal{B},q}(T)$
iii) The zeta-functions for $\mathcal{A}$ and $\mathcal{B}$ are the same. Moreover, $\#\mathcal{A}(\mathbb{F}_{q^n}) = \#\mathcal{B}(\mathbb{F}_{q^n)}$ for any positive integer n.
iv) $T_l(\mathcal{A}) \otimes \mathbb{Q} \cong T_l(\mathcal{B}) \otimes \mathbb{Q}$

Geometric Interpretation: We continue to assume that $\mathcal{A}$ is an Abelian variety defined over $\mathbb{F}_q$ Hence π acts on the algebraic points of $\mathcal{A}$ by exponentiation on coordinates with q. This action induces an action on the function field $\mathbb{F}_q(\mathcal{A})$ given again by exponentiation by q.

This action is polynomial, and so it induces a morphism on $\mathcal{A}$. Without loss of generality we can assume that this morphism fixes $0_{\mathcal{A}}$ and so is an endomorphism ϕ_q called the **Frobenius endomorphism**.

So for given $\mathcal{A}$, the Frobenius automorphism plays a double role as Galois element and as endomorphism, and this is of great importance for the arithmetic of Abelian varieties over finite fields.

The explicit knowledge of ϕ_q yields immediately that it is purely inseparable and

$$\deg \phi_q = [K(\mathcal{A}) : \pi^\star K(\mathcal{A})] = q^g.$$

As endomorphism ϕ_q has an ℓ-adic representation. By construction its characteristic polynomial is equal to $\chi_{\mathcal{A},q}(T)$. It follows that $\chi_{\mathcal{A},q}(\phi_q) \equiv 0$ as endomorphism. This motivates the following definition.

Definition 7. $\chi_{\mathcal{A},q}(T)$ is the characteristic polynomial of the Frobenius endomorphism ϕ_q of $\mathcal{A}$.

[2] An analogous result for $k = K$ a number field is the main result of Faltings on his way to prove Mordell's conjecture.

This polynomial can be used for **counting points** on $\mathcal{A}(\mathbb{F}_q)$: Since ϕ_q is purely inseparable the endomorphism $\phi_q - id_{\mathcal{A}}$ is separable, and hence $\deg\ker(\phi_q - id_{\mathcal{A}})$ is equal to the number of elements in its kernel. Since π fixes exactly the elements of $\mathbb{F}_q$ the endomorphism ϕ_q fixes exactly $\mathcal{A}(\mathbb{F}_q)$ and so $\ker(\phi_q - id_{\mathcal{A}})(\bar{\mathbb{F}_q}) = \mathcal{A}(\mathbb{F}_q)$. By linear algebra it follows

Theorem 8.

$$\#(\mathcal{A}(\mathbb{F}_q) = \chi_{\mathcal{A},q}(1).$$

In the next few sections we will focus on some special cases of Abelian varieties, namely Jacobian varieties and more specifically on Jacobian varieties of hyperelliptic curves.

3. Projective Curves and Jacobian Varieties

Our main focus in the next few sections will be on Jacobian varieties or Jacobians of curves.

3.1. Curves.

First let us establish some notation and basic facts about algebraic curves.

Convention: In this paper the notion *curve* is an absolutely irreducible projective variety of dimension 1 without singularities.

At some rare points of the following discussion it is convenient to have that $\mathcal{C}(k) \neq \emptyset$, and without loss of generality we then can assume that there is a point P_∞ "at infinity", i.e. in $\mathcal{C}(k) \setminus U_0$. If we have to study curves with different properties (like being affine of having singularities) we shall state this explicitly.

Let $\mathcal{C}$ be a curve defined over k. Hence there is $n \in \mathbb{N}$ and a homogeneous *prime* ideal $< X_0, X_1, \ldots, x_n > \neq I_{\mathcal{C}} \subset k[X_0, \ldots, X_n]$ such that, with $R = k[X_0, \ldots, X_n]/I_{\mathbb{C}}$, we have

1. $\mathcal{C}$ is the scheme consisting of the topological space $\mathrm{Proj}(R)$ and the sheaf of holomorphic functions given on open subsets U of $\mathrm{Proj}(R)$ by the localization with respect to the functions in R not vanishing on U.
2. The dimension of $\mathcal{C}$ is one, i.e. for every non-empty affine open subset $U \subset \mathrm{Proj}(R)$ the ring of holomorphic functions R_U on U is a ring with Krull dimension 1.
3. $\mathcal{C}$ is regular, i.e. the localization of R with respect to every maximal ideal M in R is a discrete valuation ring R_M of rank 1. The equivalence class of the valuations attached to R_M is the *place* $\mathfrak{p}$ of $\mathcal{C}$, in this class the valuation with value group $\mathbb{Z}$ is denoted by w_M. Alternatively we use the notation $R_{\mathfrak{p}}$ and $w_{\mathfrak{p}}$. A place $\mathfrak{p}$ of $\mathcal{C}$ is also called *prime divisor* of $\mathcal{C}$.
4. (Absolute irreducibility) $I_{\mathcal{C}} \cdot \bar{k}[X_0, \ldots, X_n]$ is a prime ideal in $\bar{k}[X_0, \ldots, X_n]$. This is equivalent with: k is algebraically closed in $\mathrm{Quot}(R)$.

As important consequence we note that for all open $\emptyset \neq U \neq \mathcal{C}$ the ring R_U is a *Dedekind domain.*

3.1.1. *Prime Divisors and Points.* The set of all places $\mathfrak{p}$ of the curve $\mathcal{C}$ is denoted by $\Sigma_{\mathcal{C}}(k)$. The *completeness* of projective varieties yields

Proposition 1. *There is a one-to-one correspondence between $\Sigma_{\mathcal{C}}(k)$ and the equivalence classes of valuations of $k(\mathcal{C})$, which are trivial on k.*

Let $\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)$ be a prime divisor with corresponding maximal ideal $M_{\mathfrak{p}}$ and valuation ring $R_{\mathfrak{p}}$. We have a homomorphism

$$r_{\mathfrak{p}} : R_{\mathfrak{p}} \to R_p/M_{\mathfrak{p}} =: L$$

where L is a finite algebraic overfield of k.

Definition 9. The degree of the prime divisor $\mathfrak{p}$ is $\deg(\mathfrak{p}) := [L : k]$.

If $\deg(\mathfrak{p}) = 1$ then $L = k$ and $r_{\mathfrak{p}}$ induces a morphism from $\mathrm{Spec}(k)$ into $\mathcal{C}$ and so corresponds to a point $P \in \mathcal{C}(k)$, uniquely determined by $\mathfrak{p}$.

More explicitly: The point P has the homogeneous coordinates $(y_0 : y_1 : \dots, : y_n)$ with $y_i = r_{\mathfrak{p}}(Y_i)$.

Lemma 10. *The set $\Sigma^1_{\mathcal{C}}(k)$ of prime divisors of $\mathcal{C}$ of degree 1 is in bijective correspondence with the set of k-rational points $\mathcal{C}(k)$ of the curve $\mathcal{C}$.*

Now look at $\mathcal{C}_{\bar{k}}$, the curve obtained from $\mathcal{C}$ by constant field extension to the algebraic closure of k. Obviously, every prime divisor of $\mathcal{C}_{\bar{k}}$ has degree 1, and so

Corollary 2. *The set of prime divisors of $\mathcal{C}_{\bar{k}}$ corresponds one-to-one to the points in $\mathcal{C}_{\bar{k}}(\bar{k})$.*

Let us go back to k. Since $\bar{k}/k$ is separable we get that every equivalence classes $\mathfrak{p}$ of valuations of $k(\mathcal{C})$, which are trivial on k has $\deg(\mathfrak{p}) = d$ extensions to $\bar{k}$, and these extensions are conjugate under the operation of G_k (Hilbert theory of valuations). Denote these extension by $(\tilde{\mathfrak{p}}_1, \dots, \tilde{\mathfrak{p}}_d$ and the corresponding points in $\mathcal{C}_{\bar{k}}(\bar{k})$ by $(P_1, \dots, P_d)$. Then $\{P_1, \dots, P_d\}$ is an orbit under the action of G_k and it is clear how to get

Corollary 3. *$\Sigma_{\mathcal{C}}(k)$ corresponds one-to-one to the G_k-orbits of $\mathcal{C}_{\bar{k}}(\bar{k})$.*

3.2. Divisors and Picard groups.

Let $\mathcal{C}$ be curve over k. A group of k-rational divisors $\mathrm{Div}_{\mathcal{C}}(k)$ of $\mathcal{C}$ is defined by

Definition 10. $\mathrm{Div}_{\mathcal{C}}(k) = \bigoplus_{\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)} \mathbb{Z} \cdot \mathfrak{p}$, i.e. $\mathrm{Div}_{\mathcal{C}}(k)$ is the free abelian group with base $\Sigma_{\mathcal{C}}(k)$.

Hence a **divisor** D of $\mathcal{C}$ is a formal sum

$$D = \sum_{\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)} z_{\mathfrak{p}} P$$

where $z_{\mathfrak{p}} \in \mathbb{Z}$ and $z_{\mathfrak{p}} = 0$ for all but finitely many prime divisors $\mathfrak{p}$. So it makes sense to define

$$\deg(D) = \sum_{\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)} z_{\mathfrak{p}}.$$

As we have seen in Corollary 3 we can interpret divisors as formal sum of G_k-orbits in $\mathcal{C}_{\bar{k}}(\bar{(k)})$. But we remark that taking points in $\mathcal{C}(k)$ is in general not enough to get all k-rational divisors of $\mathcal{C}$.

The map

$$D \mapsto \deg(D)$$

is a homomorphism from $\mathrm{Div}_{\mathcal{C}}(k)$ to $\mathbb{Z}$. Its kernel is the subgroup $\mathrm{Div}_{\mathcal{C}}(k)^0$ of divisors of degree 0.

Example 1. *Let $f \in k(\mathcal{C})^*$ be a meromorphic function on $\mathcal{C}$. For $\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)$ we have defined the normalized valuation $w_{\mathfrak{p}}$. The* divisor of f *is defined as*

$$(f) = \sum_{\Sigma_{\mathcal{C}}(k)} w_{\mathfrak{p}} \cdot \mathfrak{p}.$$

It is not difficult to verify that (f) is a divisor, and that its degree is 0, see [60]. Moreover $(f \cdot g) = (f) + (g)$ for functions f, g, and $(f^{-1}) = -(f)$. The completeness of $\mathcal{C}$ implies that $(f) = 0$ if and only if $f \in k^*$, and so (f) determines f up to scalars $\neq 0$.

So the set of principal divisors $\mathrm{PDiv}_{\mathcal{C}}(k)$ consisting of all divisors (f) with $f \in k(\mathcal{C})$ is a subgroup of $\mathrm{Div}^0_{\mathcal{C}}(k)$.

Definition 11. The group of divisor classes of $\mathcal{C}$ is defined by

$$\mathrm{Pic}_{\mathcal{C}}(k) := \mathrm{Div}_{\mathcal{C}}(k)/\mathrm{PDiv}_{\mathcal{C}}(k)$$

and is called the **divisor class group** of $\mathcal{C}$.

The group of divisor classes of degree 0 of $\mathcal{C}$ is defined by

$$\mathrm{Pic}^0_{\mathcal{C}}(k) := \mathrm{Div}^0_{\mathcal{C}}(k)/\mathrm{PDiv}_{\mathcal{C}}(k)$$

and is called the **Picard group** (of degree 0) of $\mathcal{C}$.

The Picard Functor: Let L be a finite algebraic overfield of k and $\mathcal{C}_L$ the curve obtained from $\mathcal{C}$ by constant field extension. Then places of $K(\mathcal{C})$ can be extended to places of $L(\mathcal{C}_L)$ and by the conorm map we get an injection of $\mathrm{Div}_{\mathcal{C}}(k)$ to $\mathrm{Div}_{\mathcal{C}_L}(L)$. The well known formulas for the extensions of places yield that $\mathrm{conorm}_{L/k}(\mathrm{Div}^0_{\mathcal{C}}(k)) \subset \mathrm{Div}^0_{\mathcal{C}_L}(L)$ and that principal divisors are mapped to principal divisors. Hence we get a homomorphism

$$\mathrm{conorm}_{L/k} : \mathrm{Pic}^0_{\mathcal{C}}(k) \to \mathrm{Pic}^0_{\mathcal{C}_L}(L)$$

and so we get a functor

$$\mathrm{Pic}^0 : L \mapsto \mathrm{Pic}^0_{\mathcal{C}_L}(L)$$

from the category of algebraic extension fields of k to the category of abelian groups. Coming "from above" we have a Galois theoretical description of this functor:

Clearly

$$\mathrm{Div}_{\mathcal{C}_L}(L) = \mathrm{Div}_{\mathcal{C}_{\{}\bar{k}}(\bar{k})^{G_L}$$

and the same is true for functions. With a little bit of more work one sees that an analogue result is true for $\mathrm{PDiv}_{\mathcal{C}_L}(L)$ and for $\mathrm{Pic}^0_{\mathcal{C}_L}(L)$:

Theorem 12. *Under the assumption made for curves $\mathcal{C}$ we have that for finite extension fields L with $k \subset L \subset \bar{k}$ the functor*

$$L \mapsto \mathrm{Pic}^0_{\mathcal{C}_L}(L)$$

is the same as the functor

$$L \mapsto \mathrm{Pic}^0_{\mathcal{C}_{\bar{k}}}(\bar{k})^{G_L}.$$

In particular, we have

$$\mathrm{Pic}^0_{\mathcal{C}_{\bar{k}}}(\bar{k}) = \bigcup_{k \subset L \subset \bar{k}} \mathrm{Pic}^0_{\mathcal{C}_L}(L)$$

where inclusions are obtained via conorm maps.

Remark 3. *For L/k finite algebraic we have also the norm map of places of $\mathcal{C}_L$ to places of $\mathcal{C}_k$, which induces a homomorphism from $\mathrm{Pic}^0_{\mathcal{C}_L}(L)$ to $\mathrm{Pic}^0_{\mathcal{C}}(k)$. In general, this map will be neither injective nor surjective.*

It is one of the most important facts for the theory of curves that the functor Pic^0 can be represented: There is a variety $\mathcal{J}_{\mathcal{C}}$ defined over k such that for all extension fields L of K we have a functorial equality

$$\mathcal{J}_{\mathcal{C}}(L) = \mathrm{Pic}^0_{\mathcal{C}_L}(L).$$

$J_{\mathcal{C}}$ is the **Jacobian variety** of $\mathcal{C}$. This variety will be discussed soon.

3.3. The Theorem of Riemann-Roch. In this subsection we take as guideline the book [60] of H. Stichtenoth.

3.3.1. *Riemann-Roch Spaces.* We define a partial ordering of elements in $\mathrm{Div}_{\mathcal{C}}(k)$ as follows; $D = \sum_{\mathfrak{p}\in\Sigma_{\mathcal{C}}(k)} z_{\mathfrak{p}}$ is *effective* $(D \geq 0)$ if $z_{\mathfrak{p}} \geq 0$ for every $\mathfrak{p}$, and $D_1 \geq D_2$ if $D_1 - D_2 \geq 0$.

Definition 13. Let $D = \sum_{\mathfrak{p}\in\Sigma_{\mathcal{C}}(k)} z_{\mathfrak{p}} \in \mathrm{Div}_{\mathcal{C}}(k)$. The **Riemann-Roch space** associated to D is

$$\mathcal{L}(D) = \{f \in k(\mathcal{C})^* \text{ with } (f) \geq -D\} \cup \{0\}.$$

So the elements $x \in \mathcal{L}(D)$ are defined by the property that $w_{\mathfrak{p}}(x) \geq -z_{\mathfrak{p}}$ for all $\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)$.

Basic properties of valuations imply immediately that $\mathcal{L}(D)$ is a vector space over k. This vector space has positive dimension if and only if there is a function $f \in k(\mathcal{C})^*$ with $D + (f) \geq 0$, or equivalently, $D \sim D_1$ with $D_1 \geq 0$.

Here are some immediately obtained facts: $\mathcal{L}(0) = k$ and if $\deg(D) < 0$ we get $\mathcal{L}(D) = \{0\}$. If $\deg(D) = 0$ then either D is a principal divisor or $\mathcal{L}(D) = \{0\}$.

The following result is not difficult to prove but fundamental.

Proposition 2. [60, Proposition 1.4.9] *Let $D = D_1 - D_2$ with $D_i \geq 0$. Then*

$$\dim(\mathcal{L}(D)) \leq \deg(D_1) + 1.$$

We remark that for $D \sim D'$ we have $\ell(D) \sim \ell(D')$. In particular $\mathcal{L}(D)$ is a finite-dimensional k-vector space.

Definition 14. $\ell(D) := \dim_k(\mathcal{L}(D))$.

To compute $\ell(D)$ is a fundamental problem in the theory of curves. It is solved by the Theorem of Riemann-Roch. A first estimate is a generalization of the proposition above: For all divisors D we have the inequality

$$\ell(D) \leq \deg(D) + 1.$$

For a proof one can assume that $\ell(D) > 0$ and so $D \sim D' > 0$. The important fact is that one can estimate the interval given by the inequality.

Theorem 15 (Riemann). *For given curve $\mathcal{C}$ there is a minimal number $g_C \in \mathbb{N} \cup \{0\}$ such that for all $D \in Div_{\mathcal{C}}$ we have*

$$\ell(D) \geq \deg(D) + 1 - g_{\mathcal{C}}.$$

For a proof see [60, Proposition 1.4.14]. So

$$g_{\mathbb{C}} = \max\{\deg D - \ell(D) + 1;\ D \in \mathrm{Div}_{\mathcal{C}}(k)\}$$

exists and is a non-negative integer independent of D.

Definition 16. $g_{\mathcal{C}}$ is the *genus* of $\mathcal{C}$.

We remark that the genus does not change under constant field extensions because we have assumed that k is perfect. This can be wrong in general if the constant field of $\mathcal{C}$ has inseparable algebraic extensions.

There is a corollary of the theorem.

Corollary 4. *There is a number $n_{\mathcal{C}}$ such that for* $\deg(D) > n_{\mathcal{C}}$ *we get equality*

$$\ell(D) = \deg(D) + 1 - g_{\mathcal{C}}.$$

Theorem 15 together with its corollary i the “Riemann part ” of the Theorem of Riemann-Roch for curves. To determine $n_{\mathcal{C}}$ and to get more information about the inequality for small degrees one needs canonical divisors.

3.3.2. *Canonical Divisors.* Let $k(\mathcal{C})$ be the function field of a curve C defined over k. To every $f \in k(\mathcal{C})$ we attach a symbol df, the *differential* of f lying in a $k(\mathcal{C})$-vector space $\Omega(k(\mathcal{C}))$ generated by the symbols df modulo the following relations: For $f, g \in k(\mathcal{C})$ and $\lambda \in k$ we have

i)$d(\lambda f + g) = \lambda df + dg$

ii)$d(f \cdot g) = f dg + g df$.

The relation between derivations and differentials is given by the

Definition 17 (Chain rule)**.** Let x be as above and $f \in k(\mathcal{C})$. Then $df = (\partial f/\partial x)dx$.

As in calculus one shows that the $k(\mathcal{C})$-vector space of differentials $\Omega(k(\mathcal{C}))$ has dimension 1 and it is generated by dx for any $x \in k(\mathcal{C})$ for which $k(\mathcal{C})/k(x)$ is finite separable.

We use a well known fact from the theory of function fields F in one variable i.e finitely generated fields of transcendence degree 1 over a perfect field k:

Let $\mathfrak{p}$ be a place of F, i.e. an equivalence class of discrete rank one valuations of F trivial on k). Then there exist a function $t_{\mathfrak{p}} \in F$ with $w_{\mathfrak{p}}(t_{\mathbb{P}}) = 1$ and $[F : k(t_{\mathfrak{p}})$ separable. We apply this to $F = k(\mathcal{C})$. For all $\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)$ we choose a function $t_{\mathfrak{p}}$ as above. For a differential $0 \neq \omega \in \Omega(k(\mathcal{C})$ we get $\omega = f_{\mathfrak{p}} \cdot dt_{\mathfrak{p}}$.

Definition 18. The divisor (ω) is given by

$$(\omega) := \sum_{\mathfrak{p} \in \Sigma_{\mathfrak{p}}} w_{\mathfrak{p}}(f_{\mathfrak{p}}) \cdot \mathfrak{p}.$$

ω is a called a **canonical divisor** of $\mathcal{C}$.

The chain rule implies that this definition is independent of the choices, and the relation to differentials yields that (ω) is a divisor.

Since $\Omega(k(\mathcal{C})$ is one-dimensional over $k(\mathcal{C})$ it follows that the set of canonical divisors of $\mathcal{C}$ form a divisor class $\mathcal{K}_{\mathcal{C}} \in \mathrm{Pic}_{\mathcal{C}}(k)$ called the **canonical class** of $\mathcal{C}$.

We are now ready to formulate the **Theorem of Riemann-Roch**

Theorem 19. *Let (W) be a canonical divisor of $\mathcal{C}$. For all $D \in Div_{\mathcal{C}}(k)$ we have*

$$\ell(D) = \deg(D) + 1 - g_{\mathcal{C}} + \ell(W - D).$$

For a proof see Section 1.5 in the book [60].

A differential ω is *holomorphic* if (ω) is an effective divisor. The set of holomorphic differentials is a k-vector space denoted by $\Omega^0_{\mathcal{C}}$ which is equal to $\mathcal{L}(W)$.

Take $D = 0$ respectively $D = W$ in the theorem of Riemann-Roch to get

Corollary 5. *$\Omega^0_{\mathcal{C}}$ is a $g_{\mathcal{C}}$- dimensional k- vector space and* $\deg(W) = 2g_{\mathcal{C}} - 2$.

For the applications we have in mind there are two further consequences of the Riemann-Roch theorem important.

Corollary 6. *The following are true:*

(1) *If* $\deg(D) > 2g_{\mathcal{C}} - 2$ *then* $\ell(D) = \deg(D) + 1 - g_{\mathcal{C}}$.
(2) *In every divisor class of degree g there is a positive divisor.*

Proof. Take D with $\deg(D) \geq 2g_{\mathcal{C}} - 1$. So $\deg(W - D) \leq -1$ and so $\ell(W - D) = 0$. Take D with $\deg(D) = g_{\mathcal{C}}$. Then $\ell(D) = 1 + \ell(W - D) \geq 1$ and so there is a positive divisor in the class of D. □

4. Applications of the Theorem of Riemann-Roch

4.1. The Hurwitz genus formula.

In the theory of curves the notion of a cover is important.

Definition 20. Let $\mathcal{C}$, $\mathcal{D}$ be curves defined over k, with $\mathcal{D}$ not necessarily irreducible. A finite surjective morphism

$$\eta : \mathcal{D} \to \mathcal{C}$$

from $\mathcal{D}$ to $\mathcal{C}$ is a *cover morphism*, and if such a morphism exists we call $\mathcal{D}$ a **cover** $\mathcal{C}$.

As usual, we denote by

$$\eta^* : k(\mathcal{C}) \hookrightarrow k(\mathcal{D})$$

the induced monomorphism of the function fields and identify $k(\mathcal{C})$ with its image. η is separable iff $k(\mathcal{D})$ is a separable extension of $k(\mathcal{C})$, and η is Galois with Galois group G if $k(\mathcal{D})/k(\mathcal{C})$ is Galois with group G. The cover η is geometric if k is algebraically closed in $k(\mathcal{D})$.

Assume in the following that η is separable. We shall use the well known relations between prime divisors of $k(\mathcal{C})$ and those of $k(\mathcal{D})$ such as extensions, ramifications and sum formulas for the degrees. In particular we get:

Let $\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)$ be a prime divisor. Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ be the primes divisors in $\Sigma_{\mathcal{D}}(k)$ which extend $\mathfrak{p}$, written as $\mathfrak{P}|\mathfrak{p}$. Let $t_{\mathfrak{p}}$ an element in $k(\mathcal{C})$ with $w_{\mathfrak{p}}(t_{\mathfrak{p}}) = 1$. The ramification number $e(\mathfrak{P}_i/\mathfrak{p}) =: e_i$ is defined as $e_i = w_{\mathfrak{P}_i}(t_{\mathfrak{p}})$, hence there is a function $t_{\mathfrak{P}_i}$ on $\mathcal{D}$ such that $t_{\mathfrak{P}_i}^{e_i} = t_{\mathfrak{p}} \cdot u$ with $w_{\mathfrak{P}_i}(u) = 0$. The *conorm* of $\mathfrak{p}$ is the divisor $\mathrm{conorm}(\mathfrak{p}) = \sum_i \mathfrak{P}_i^{e_i}$ and its degree is $[k(\mathcal{D}) : k(\mathcal{C})]$, the norm of $\mathfrak{P}_i$ is $\mathfrak{p}$.

η is *tamely ramified* if for all $\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)$ the ramification numbers of all extensions are prime to char(k).

We want to relate the genus of $\mathcal{D}$ to the genus of $\mathcal{C}$. Let $x \in k(\mathcal{C})$ be such that $k(\mathcal{C})/k(x)$ is finite separable, and let $dx_{\mathcal{C}}$ respectively $dx_{\mathcal{D}}$ be corresponding differentials with divisors $(dx)\mathcal{C}$ and dx_D. We know that

$$2g_{\mathbb{C}} - 2 = \deg(dx)_{\mathcal{C}} \text{ and } 2g_{\mathcal{D}} - 2 = \deg(dx)_{\mathcal{D}}.$$

We compute the value $z_{\mathfrak{p}}$ respectively $z_{\mathfrak{P}_i}$ of these divisors at $\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)$ and in the extensions $\mathfrak{P}_1, \dots \mathfrak{P}_r$ with ramification numbers e_i: To easy notation we take $\mathfrak{P} := \mathfrak{P}_i$, $e_i = e_{\mathfrak{P}}$ and $t_{\mathfrak{P}} \in k(\mathcal{D})$ with $w_{\mathfrak{P}} = 1$. Then we can choose

$$t_{\mathfrak{p}} = u \cdot t_{\mathfrak{P}}^{e_{\mathfrak{P}}} \in k(\mathcal{C}),$$

with $w_{\mathfrak{p}}(u) = 0$. By the rules for differentials we get $dt_p = (e_{\mathfrak{P}} \cdot u \cdot t_{\mathfrak{P}}^{e_{\mathfrak{P}}-1} + u' \cdot t_{\mathfrak{P}}^{e_{\mathfrak{P}}}) dt_{\mathfrak{P}}$ and so

$$w_{\mathfrak{P}}(dx) = e_{\mathfrak{P}} \cdot w_{\mathfrak{p}}(dx) + e_{\mathfrak{P}} - 1.$$

Summing up over $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ we get that

$$\deg(\sum_{\mathfrak{P}|\mathfrak{p}} z_{\mathfrak{P}}) = \deg(\sum_{i=1}^{r} z_{\mathfrak{p}} \mathfrak{P}_i^{e}) + \sum_{i=1}^{r} (e_i - 1).$$

Summing up over all $\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)$ we get

THEOREM 21 (Hurwitz). *Let*

$$\eta : \mathcal{D} \to \mathcal{C}$$

be a separable tamely ramified cover of degree n and denote by $e_{\mathfrak{P}}$ the ramification order of $\mathfrak{P} \in \Sigma_{\mathcal{D}}(k)$. Then

$$2g_{\mathcal{D}} - 2 = n \cdot (2g_{\mathcal{C}} - 2) + \sum_{\mathfrak{P} \in \Sigma_{\mathcal{D}}} (e_{\mathfrak{P}} - 1).$$

EXAMPLE 2. *Assume that $\mathcal{C} = \mathbb{P}^1$. One sees easily that $g_{\mathbb{P}^1} = 0$. Let $\mathcal{D}$ be tamely ramified cover of degree n of $\mathbb{P}^1$. Then*

$$g_{\mathbb{C}} = -n + 1/2 \sum_{\mathfrak{P} \in \Sigma_{\mathcal{D}}(k)} (e_{\mathfrak{P}} - 1) + 1.$$

In particular $\mathbb{P}^1$ has no unramified extensions.

The special case $n = 2$ will be important for us. Assume that char(k) $\neq 2$. Then we can apply the Hurwitz formula and get

$$g_{\mathcal{D}} = 1/2r - 1$$

where r is the number of prime divisors of $\mathbb{P}^1$ (or of $\mathcal{D}$) which are ramified (i.e. ramification order is larger than 1) under η.

4.2. Gonality of curves and Hurwitz spaces.

We fix a curve $\mathcal{C}$ defined over k and look at covers

$$\eta : \mathcal{C} \to \mathbb{P}^1.$$

In this subsection we use the assumption that $\mathcal{C}$ has a k-rational point $\mathbb{P}_\infty$ and hence a prime divisor $\mathfrak{p}_\infty$ of degree 1.

Definition 22. The gonality $\gamma_{\mathcal{C}}$ is defined by

$$\gamma_{\mathcal{C}} = \min \left\{ \deg(\eta : \mathcal{C} \to \mathbb{P}^1 \right\} = \min \left\{ [k(\mathcal{C}) : k(x)],\ x \in k(\mathcal{C}) \right\}.$$

For $x \in k(\mathcal{C})^*$ define the pole divisor $(x)_\infty$ by

$$(x)_\infty = \sum_{\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)} \max(0, -w_{\mathfrak{p}}(x)) \cdot \mathfrak{p}.$$

By the property of conorms of divisors we get $\deg((x)_\infty) = [k(\mathcal{C}) : k(x)]$ if $x \notin k$ and so

$$\gamma_{\mathcal{C}} = \min(\deg((x)_\infty)),\ x \in k(\mathcal{C}) \setminus k.$$

Proposition 3. *For $\gamma_{\mathcal{C}} \geq 2$ we have $\gamma_{\mathcal{C}} \leq g$.*

Proof. By the theorem of Riemann-Roch $\ell(g_{\mathcal{C}} \cdot \mathbb{P}_\infty) = 1 + \ell(W - g_{\mathcal{C}} \cdot \mathbb{P}_\infty)$ and since $g_{\mathcal{C}} \geq 2$ the divisor $W - g_{\mathcal{C}} \cdot \mathbb{P}_\infty)$ has degree ≥ 0 and so $\ell(W - g_{\mathcal{C}} \cdot \mathbb{P}_\infty) \geq 1$. But then $\ell(g_{\mathcal{C}} \cdot \mathbb{P}_\infty) \geq 2$ and there is a non-constant function x whose pole divisor is a multiple of $\mathfrak{p}_\infty$ of order $\leq g_{\mathcal{C}}$. □

This proves more than the proposition.

Corollary 1. *For curves $\mathcal{C}$ of genus ≥ 2 with prime divisor $\mathfrak{p}_\infty$ of degree 1 there exists a cover*

$$\eta : \mathcal{C} \to \mathbb{P}^1$$

with $\deg(\eta) = n \leq g_{\mathcal{C}}$ *such that* $\mathfrak{p}_\infty$ *is ramified of order* n *and so the point* $P_\infty \in \mathcal{C}(k)$ *attached to* $\mathfrak{p}_\infty$ *is the only point on* $\mathcal{C}$ *lying over the infinite point* $(0:1)$ *of* $\mathbb{P}^1$.

In general, the inequality in the proposition is not sharp but of size $g/2$ as we shall see below. Curves with smaller gonality are special and so per se interesting.

4.2.1. *Gonality of the generic curve.* In this subsection we shall assume that k is algebraically closed.

We are interested in the classification of isomorphic classes of projective irreducible regular curves of genus $g \geq 2$.

The moduli scheme $\mathcal{M}_g$ is a scheme defined over k with the property that is parametrizes these classes: To every point P there is a unique class of a curve $\mathcal{C}$ of genus g. The coordinates of $\mathcal{C}$ (chosen in an appropriate affine open neighborhood) are the invariants of $\mathcal{C}$. It is a classical task to determine such systems of invariants and then to find the curve $\mathcal{C}$ with these invariants. We shall come back to this in the case of curves of small genus.

Remark 4. *The scheme $\mathcal{M}_g$ is defined over non-algebraically closed fields k but then it is only a coarse moduli scheme.*

The construction of $\mathcal{M}_g$ is done over $\mathbb{C}$ either by Teichmller theory or, more classically, by Hurwitz spaces (see below), and so over algebraically closed fields of characteristic 0 by the so-called Lefschetz principle. Its existence in the abstract setting of algebraic geometry uses deep methods of geometric invariant theory as developed and studied by Deligne and Mumford in [13].

One knows that $\mathcal{M}_g$ is irreducible and so there exists a generic curve of genus g. Moreover the dimension of $\mathcal{M}_g$ is equal to $3g-3$. Curves with special properties (i.e. non-trivial automorphisms or small gonality) define interesting subschemes of $\mathcal{M}_g$. be the moduli space of curves of genus $g \geq 2$ defined over k. Here is one example.

Definition 23. A curve $\mathcal{C}$ with genus ≥ 2 is hyperelliptic iff it has gonality 2.

The subspace of hyperelliptic curves in $\mathcal{M}_g$ is the *hyperelliptic locus* $\mathcal{M}_{g,h}$. We shall see below that this locus has dimension $2g-1$.

Hurwitz spaces: We continue to assume that k is algebraically closed.
We look at curves $\mathcal{C}$ and separable covers $\eta : \mathcal{C} \to \mathbb{P}^1$ of degree n.
η^* allows to identify $k(\mathbb{P}^1) =: k(x)$ with a subfield of $K(\mathcal{C})$.
First, we introduce equivalence: $\eta \sim \eta'$ if there are isomorphisms $\alpha : \mathcal{C} \to CC'$ and $\beta \in \operatorname{Aut}(\mathbb{P}^1)$ with

$$\beta \circ \eta = \eta' \circ \alpha.$$

The *monodromy group* of η is the Galois group of the Galois closure L of $k(\mathcal{C})/k(x)$. We embed G into S_n, the symmetric group with n letters.
We fix the ramification type of the covers η we look at. We assume that exactly $r \geq 3$ points in $\mathbb{P}^1(k)$ are ramified (i.e. the corresponding prime divisors have at least one extension to $k(\mathcal{C})$ with ramification order > 1 and that all ramification orders are prime to char(k). It follows that the ramification groups are cyclic.

By the classical theory of covers of Riemann surfaces, which can be transferred to the algebraic setting by the results of Grothendieck (here one needs tameness of ramification) it follows that there is a tuple $(\sigma_1, \dots, \sigma_r)$ in S_n such that $\sigma_1 \cdots \sigma_r = 1$, $\mathrm{ord}(\sigma_i) = e_i$ is the ramification order of the i-th ramification point P_i in L and $G := \langle \sigma_1, \dots, \sigma_r \rangle$ is a transitive group in S_n.
We call such a tuple the signature σ of the covering η.
We remark that such tuples are determined up to conjugation in S_n, and that the genus of $\mathcal{C}$ is determined by the signature because of the Hurwitz genus formula.

Let $\mathcal{H}_\sigma$ be the set of pairs $([\eta], (p_1, \dots, p_r)$, where $[\eta]$ is an equivalence class of covers of type σ, and $p_1, \dots, p_r$ is an ordering of the branch points of ϕ modulo automorphisms of $\mathbb{P}^1$. This set carries the structure of a algebraic scheme., in fact it is a quasi-projective variety, the *Hurwitz space* $\mathcal{H}_\sigma$. We have the forgetful morphism

$$\Phi_\sigma : \mathcal{H}_\sigma \to \mathcal{M}_g$$

mapping $([\eta], (p_1, \dots, p_r)$ to the isomorphic class $[\mathcal{C}]$ in the moduli space $\mathcal{M}_g$. Each component of $\mathcal{H}_\sigma$ has the same image in $\mathcal{M}_g$.
We define the **moduli dimension of** σ (denoted by $\dim(\sigma)$) as the dimension of $\Phi_\sigma(\mathcal{H}_\sigma)$; i.e., the dimension of the locus of genus g curves admitting a cover to $\mathbb{P}^1$ of type σ. We say σ has **full moduli dimension** if $\dim(\sigma) = \dim \mathcal{M}_g$.

Example 3. *Take $n = 2$, so $G = S_2$, $r \geq 6$ and* char(k) $\neq 2$ *and the notations from above. A signature σ is completely determined by the r ramification points $P_1, \cdots, P_r$. Hence $\mathcal{H}_\sigma$ consists of classes of hyperelliptic curves of genus $g_r = r/2 - 1$ (so r is even). Since we can apply automorphisms of $\mathbb{P}^1$ we can assume that $P_1 = (1:0), P_2 = (1,1), P_3 = (0:1)$ and so we have $r - 3$ free parameters modulo a finite permutation group.*

So the moduli dimension is $r - 3 = 2g + 2$, and the hyperelliptic locus $\mathcal{M}_{g,h}$ has dimension $2g - 1$ and codimension $g - 2$. Hence all curves of genus 2 are hyperelliptic, and for $g \geq$ the locus of the hyperelliptic curves has positive codimension.

For a fixed $g \geq 3$, we want to find σ of full moduli dimension and of minimal degree. This would give a generic covering of minimal degree for a generic curves of genus g and so its gonality.
A first condition is that $r = 3g$. Because of the Hurwitz genus formula this yields conditions for the ramification cycles, which have to have minimal order. This is worked out in [56].

Lemma 11. *For any $g \geq 3$ there is a minimal degree $d = \lfloor \frac{g+3}{2} \rfloor$ generic cover*

$$\psi_g : \mathcal{C}_g \to \mathbb{P}^1$$

of full moduli dimension from a genus g curve $\mathcal{C}_g$ such that it has $r = 3g$ branch points and signature:

i) If g is odd, then $\sigma = (\sigma_1, \dots, \sigma_r)$ such that $\sigma_1, \dots, \sigma_{r-1} \in S_d$ are transpositions and $\sigma_r \in S_d$ is a 3-cycle.

ii) If g is even, then $\sigma = (\sigma_1, \dots, \sigma_r)$ such that $\sigma_1, \dots, \sigma_r \in S_d$ are transpositions.

4.2.2. *Equations for Curves.* There is a one-to-one correspondence between function fields F of transcendence degree 1 over the field of constants k (which is assumed to be algebraically closed in F and isomorphic classes of projective regular absolutely irreducible curves $\mathcal{C}$ with $k(\mathcal{C}) = F$. The natural question is: Given F, how can one find $\mathcal{C}$ as embedded projective curve in an appropriate $\mathbb{P}^n$?

The main tool to solve this question are Riemann-Roch systems. Let D with $\ell(D) = d + 1 > 0$ and $(f_0, f_1, \dots, f_d)$ a base of $\mathcal{L}(D)$. Then

$$\Phi_D : \mathcal{C}(\bar{k}) \to \mathbb{P}^d(\bar(k)$$
$$P \mapsto (f_0(P) : f_1(p) : \cdots : f_d(P))$$

is a rational map defined in all points for which $f_0, \dots, f_d$ do not vanish simultaneously. $\mathcal{L}(D)$ is without base points if this set is empty, and then Φ_D is a morphism from $\mathcal{C}$ in $\mathbb{P}^d$.

Lemma 12. *For $g \geq 3$ and $D = W_{\mathcal{C}}$ the space $\mathcal{L}(W) = \Omega^0_{\mathcal{C}}$ is without base points, and so Φ_W is a morphism from $\mathcal{C}$ to $\mathbb{P}^{g_{\mathcal{C}}-1}$.*

Φ_W may not be an embedding but the only exception is that $\mathcal{C}$ is hyperelliptic, and than the image of Φ_W is the projective line.

Theorem 24. *Let $\mathcal{C}$ be a curve of genus $g_{\mathcal{C}} > 2$ and assume that $\mathcal{C}$ is not hyperelliptic. Then Φ_W is an embedding of $\mathcal{C}$ into $P^{g_{\mathcal{C}}-1}$ and the image is a projective regular curve of degree $2g_{\mathcal{C}} - 2$ (i.e. the intersection with a generic hyperplane has $2g_{\mathcal{C}} - 2$ points).*

So having determined a base of the canonical class of $\mathcal{C}$ one gets a parameter representation of $\mathcal{C}$ and then one can determine the prime ideal in $k[Y_0, \dots, y_{g_{\mathcal{C}}}]$ vanishing on $\Phi_W(\mathcal{C})$. Φ_W is the **canonical embedding** of $\mathcal{C}$.

Example 4. *Take $g_{\mathcal{C}} = 3$ and assume that $\mathcal{C}$ is not hyperelliptic. Then the canonical embedding maps $\mathcal{C}$ to a regular projective plane curve of degree 4. In other words: All non-hyperelliptic curves of genus 3 are isomorphic to non-singular quartics in $\mathbb{P}^2$.*

Plane Curves: Only very special values of the genus of $\mathcal{C}$ allow to find plane regular projective curves isomorphic to $\mathcal{C}$. We have just seen that $g = 3$ is such a value. The reason behind is the Plcker formula, which relates degree, genus and singularities of plane curves. But of course, there are many projective plane curves which are birationally equivalent to $\mathcal{C}$:

Take $x \in k(CC) \setminus k$ with $k(\mathcal{C})/k(x)$ separable. Then there is an element $y \in k(\mathcal{C})$ with $k(x, y) = k(\mathcal{C})$, and by clearing denominators we find a polynomial $G(x, y) \in k[X, Y]$ with $G(x, y) = 0$. Then the curve $\mathcal{C}'$ given by the homogenized polynomial

$$G_h(X, Y, Z) = 0$$

is a plane projective curve birationally equivalent to $\mathcal{C}$ but, in general, with singularities. Using the gonality results we can chose $G(X, Y)$ such that the degree in Y is $\lfloor \frac{g+3}{2} \rfloor$.

Using the canonical embedding for non hyperelliptic curves and general projections we can chose $G_h(X,Y,Z)$ as homogeneous polynomial of degree $2g_{\mathcal{C}}-2$.

In the next subsection we shall describe a systematic way to find plane equations for hyperelliptic curves.

4.2.3. *Plane equations for elliptic and hyperelliptic curves, Weierstrass normal forms.* We first focus on elliptic curves.

Elliptic Curves

We assume that $\mathcal{E}$ is a curve of genus 1 with a k-rational point P_∞ and corresponding prime divisor $\mathfrak{p}_\infty$. By definition, $\mathcal{E}$ is an *elliptic curve defined over k*. We look at the Riemann-Roch spaces $\mathcal{L}_i := \mathcal{L}(\imath \cdot \mathfrak{p}_\infty)$ and denote their dimension by ℓ_i. Since $2g_{\mathcal{E}}-2=0$ we can use the theorem of Riemann-Roch to get: $\ell_i = i$. Hence $\mathcal{L}_1 =< 1 >$, $\mathcal{L}_2 =< 1, x >$ with a function $x \in k(\mathcal{E})$ with $(x)_\infty = 2\mathfrak{p}_\infty$, $\mathcal{L}_3 = \langle 1, x, y\rangle$ with $(y)_\infty = 3\mathfrak{p}_\infty$ and $\mathcal{L}_5 = \langle 1, x, x^2, y, xy\rangle$ with 5 linearly independent functions.

Now look at $\mathcal{L}_6$. This is a vector space of dimension 6 over k. It contains the seven elements $\{1, x, x^2, x^3, y, xy, y^2\}$ and hence there is a non-trivial linear relation

$$\sum_{0\le i\le 3;\, 0\le j\le 2} a_{i,j}x^i y^2.$$

Because of the linear independence of $(1, x, x^2, y, xy)$ we get that either $a_{3,0}$ or $a_{0,2}$ are not equal 0, and since x^3 and y^2 have a pole of order 3 in $\mathfrak{p}_\infty$ it follows that $a_{0,2} \cdot a_{3,0} \neq 0$. By normalizing we get x and y satisfy the equation

$$Y^2 + a_1 X \cdot Y + a_3 Y = a_0 X^3 + a_2 X^2 + a_4 X + a_6.$$

By multiplying with a_0^2 and substituting (X, Y) by $(a_0 X, a_0 Y)$ we get an **affine Weierstrass equation** for $\mathcal{E}$:

$$W_{\mathcal{E}aff} : Y^2 + a_1 X \cdot Y + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6.$$

The homogenization give the cubic equation

$$W_{\mathcal{E}} : Y^2 \cdot Z + a_1 X \cdot Y \cdot Z + a_3 Y \cdot Z^2 = a_0 X^3 + a_2 X^2 \cdot Z + a_4 X \cdot Z^2 + a_6 \cdot Z^3$$

which defines a plane projective curve.

The infinite points of this curve have $Z = 0$, and so only infinite point is $P_\infty = (0, 1, 0)$ corresponding to the chosen $\mathfrak{p}_\infty$. Looking at the partial derivatives one verifies that $\mathcal{E}$ has no singularities iff the discriminant with of the affine equation $W_{\mathcal{E}aff}$ as polynomial in X is different from 0, and that this is equivalent with the condition that $k(\mathcal{E})$ is not a rational function field.

Theorem 25. *Elliptic curves defined over k correspond one-to-one the isomorphic classes of plane projective curves without singularities given by Weierstrass equations*

$$W_{\mathcal{E}} : Y^2 \cdot Z + a_1 X \cdot Y \cdot Z + a_3 Y \cdot Z^2 = a_0 X^3 + a_2 X^2 \cdot Z + a_4 X \cdot Z^2 + a_6 \cdot Z^3$$

with non-vanishing discriminant X-discriminant.

Since we are dealing with isogeny classes of such curves we can further normalize the equations and finally find invariants for the isomorphic class of a given $\mathcal{E}$. We shall come to this in Section ??.

Weierstrass equations for hyperelliptic curves: Let $\mathcal{C}$ be a curve over k of genus $g \geq 2$ with a cover

$$\eta : \mathcal{C} \to \mathbb{P}^1$$

of degree 2. We assume that there is a point $\mathbb{P}_\infty \in \mathcal{C}(k)$ corresponding to a prime divisor $\mathfrak{p}_\infty$ of $\mathcal{C}$ of degree 1. Take $Q_\infty = \eta(P_\infty) \in \mathbb{P}^1(k)$ and $x \in k(\mathbb{P}^1)$ with $(x)_\infty = \mathfrak{p}_{0,\infty}$ with $\mathfrak{p}_{0,\infty}$ a prime divisor of degree 1 of $\mathbb{P}^1$. Thus, $\mathrm{conorm}(\mathfrak{p}_{0,\infty}) = 2 \cdot \mathfrak{p}_\infty$ and so η is ramified in Q_0, or $\mathrm{conorm}(\mathfrak{p}_{0,\infty}) = \mathfrak{p}_\infty \cdot \mathfrak{p}'_\infty$. In any case $\mathrm{conorm}(\mathfrak{p}_{0,\infty}) =: D$ is a positive divisor of degree 2. We define the Riemann-Roch spaces $\mathcal{L}_i = \mathcal{L}(i \cdot D)$ and $\ell_i = \dim_k(\mathcal{L}_i)$.

By assumption $\mathcal{L}_1$ has as base $(1, x)$ and so $\ell_1 = 2$. Since $\deg(g+1) \cdot D > 2g-2$ the theorem of Riemann- Roch implies that $\ell_{g+1} = 2(g+1) - g + 1 = g + 3$. Hence there is a function $y \in \mathcal{L}_{g+1}$ linearly independent from powers of x. So $y \notin k[x]$. The space $\mathcal{L}_{2(g+1)}$ has dimension $3g + 3$ and contains the $3g + 4$ functions

$$\{1, x, x^{g+1}, y, x^{g+2}, xy, \dots, x^{2(g+1)}, x^{g+1}y, y^2\}.$$

So there is a nontrivial k-linear relation between these functions, in which y^2 has to have a non-trivial coefficient. We can normalize and get and equation

$$y^2 + h(x)y = f(x) \quad \textit{with} \quad h(x), f(x) \in k[x]$$

and $\deg(h(x) \leq g + 1$, $\deg(f) \leq 2g + 2$. So

$$W_{\mathcal{C}_{aff}} : Y^2 + h(X)Y = f(X)$$

is the equation for an affine part $\mathbb{C}_{aff}$ of a curve birationally equivalent to $\mathcal{C}$. It is called an *affine Weierstrass equation* for $\mathcal{C}$, and its homogenization is the equation of a projective plane curve $\mathcal{C}'$ birationally equivalent to $\mathcal{C}$.

The prime divisors of $\mathcal{C}$ are extensions of prime divisors of $k(x)$ and hence correspond (over $\bar{k}$) to points (x, y) in $\mathbb{A}^2$ or the points lying over $\mathfrak{p}_{0,\infty}$. To get more information we use the Hurwitz genus formula and assume for simplicity that char(k) $\neq 2$ and so η is tamely ramified and separable; for the general case see [7, Section 14.5.1].

Then we can apply the Tschirnhausen transformation and can assume that $h(x) = 0$. We know that η has to have $2g + 2$ ramification points. Ramification points of η are fixed points under the hyperelliptic involution ω which generates $G(k(\mathcal{C})/k(x)$. Since ω acts on points (x, y) by sending it to $(x, -y)$ and hence the affine ramification points correspond to the zeros of $f(X)$. If $\mathfrak{p}_{0,\infty}$ is unramified then it follows that $f(X)$ has to have $2g + 2$ zeros, and so $\deg(f(X)) = 2g + 2$ and all zeros are simple.

Assume that $\mathfrak{p}_{0,\infty}$ is ramified. Then there have to be $2g - 1$ places with norm $\neq \mathfrak{p}_{0,\infty}$ and so $\deg(f(X) = 2g + 1$ and again all zeros are different. Hence in both cases we have that $\mathcal{C}_{aff}$ is without singularities. This is not true for the point $(0, 1, 0)$, the only point at infinity of $\mathcal{C}'$. It is a singular point, and it corresponds to two points (over $\bar{k}$) on $\mathcal{C}$ if $\mathfrak{p}_{0,\infty}$ is unramified, and to one point on $\mathcal{C}(k)$ if $\mathfrak{p}_{0,\infty}$ is ramified.

For computational purposes the latter case is more accessible: The arithmetic in $K(\mathcal{C})$ is analogue to the arithmetic in imaginary quadratic fields; see **??**.

A last remark: Contrary to the case of elliptic curves the subfield $k(x)$ is uniquely determined by $k(\mathcal{C})$, and the ramification points of the cover η are the *Weierstrass points* of $\mathcal{C}$.

Minimal Degrees: We have seen above that non-hyperelliptic curves of genus ≥ 3 are birational equivalent to plane projective curves of degree $\leq 2g+2$.
But in general, this is not the minimal degree one can achieve. On the other side one has an estimate from below for the degree of plane curves birational equivalent to a hyperelliptic curve of genus $g \geq 3$; see [8] for details.

Proposition 4. *Let $\mathcal{C}$ be a hyperelliptic curve of genus g and let $\mathcal{C}'$ be a plane projective curve birationally equivalent to $\mathcal{C}$. Then the degree of the equation of $\mathcal{C}'$ is $\geq g+2$.*

4.2.4. *Addition in Picard groups over $\mathbb{F}_q$.* We take $k = \mathbb{F}_q$ and $\mathcal{C}$ a curve of genus g defined over $\mathbb{F}_q$. By a result of F.K. Schmidt (proved by using Zeta-functions) curves over finite fields have a rational divisor D_0 of degree 1 (Caution: this does only for curves of genus ≤ 1 imply that they have a rational point.) It is not difficult to show that this divisor can be computed effectively. We use this to present divisor classes c of degree O of $\mathcal{C}$.

Let $\mathcal{D}_{\mathcal{C}}(\mathbb{F}_q)^g_{>0}$ denote the positive divisors of degree g of $\mathcal{C}$. A consequence of the theorem of Riemann-Roch is that the map

$$\varphi : \mathcal{D}_{\mathcal{C}}(\mathbb{F}_q)^g_{>0} \to \mathrm{Pic}^0_{\mathcal{C}}(\mathbb{F}_q)$$

given by

$$D \mapsto \varphi(D) = D - g \cdot D_1$$

is surjective. A first consequence is that $\mathrm{Pic}^0_{\mathcal{C}}(\mathbb{F}_q)$ is a finite abelian group since there are only finitely many positive divisors of degree D rational over $\mathbb{F}_q$.

Our aim is to find an algorithm, which computes the addition in $\mathrm{Pic}^0_{\mathcal{C}}(\mathbb{F}_q)$ fast. The main task is the following *reduction*:

Given $D, D' \in \mathcal{D}_{\mathcal{C}}(\mathbb{F}_q)^g_{>0}$ find a divisor $S \in \mathcal{D}_{\mathcal{C}}(\mathbb{F}_q)^g_{>0}$ with

$$D + D' - 2D_1 \sim S - D_1.$$

Then $S - \mathcal{D}_1$ lies in the divisor class that is the sum of the divisor class of $D - D_1$ with the class of $D' - D_1$. An analogue reduction is well-known from computational number theory and ideal classes of orders. There one uses Minkowski's theorem instead of the Riemann-Roch theorem.

The idea of F. Heß in [30] and worked out with many additional details in [15] is to use the fact the holomorphic functions in affine open parts of $\mathcal{C}$ are Dedekind domains and that divisors with support on these parts can be identified with ideals of these rings. As first step compute (e.g. from the function field $k(\mathcal{C})$) a plane curve $\mathcal{C}'$ birationally equivalent to $\mathcal{C}$ of a degree d of size $\mathcal{O}(g)$ (see our arguments above).

The next step is to go to an affine part of $\mathcal{C}'$ which is without singularities and for which divisors can be identified with ideals in its coordinate ring. (Approximation properties of functions in function fields can be used since we are only interested in divisor classes).Now the algorithms known from number theory are applicable. The result is given by the following theorem.

Theorem 26 (Heß, Diem). *Let $\mathcal{C}$ be a curve of genus g over $\mathbb{F}_q$. The addition in the degree 0 class group of C can then be performed in an expected time which is polynomially bounded in g and $\log(q)$.*

This result is a highlight in algorithmic arithmetic geometry and it opens the access to the Picard groups as abelian groups for arbitrary curves.
Of course, it will be a challenge to implement it. In our context, namely to construct crypto systems, its importance is the *existence* of the algorithm which make certain attacks thinkable!

In the next sections we shall see how we can find explicit algorithms and even formulas to perform group operations in Picard groups of hyperelliptic curve very rapidly.

4.2.5. *The Jacobian Variety of a Curve.* In subsection **??** we have defined the *Picard functor* $\mathrm{Pic}^0_{\mathcal{C}}$ from the category of extension fields L/k into the category of abelian groups given by

$$L \mapsto \mathrm{Pic}^0_{\mathcal{C}\,L}(L).$$

In addition we have stated that $\mathrm{Pic}^0_{\mathcal{C}}$ is a Galois functor, i.e. that if $k \subset L \subset \bar{k}$ then $\mathrm{Pic}^0_{\mathcal{C}\,L}(L) = \mathrm{Pic}^0_{\mathcal{C}bark}(\bar{k})^{G_L}$. We also announced that this functor is *representable* in terms of algebraic geometry.

More precisely: Let $\mathcal{C}$ be a curve of positive genus and assume that there exists a k-rational point $P_0 \in \mathcal{C}(k)$ with attached prime divisor $\mathfrak{p}_0$. There exists an abelian variety $\mathcal{J}_{\mathcal{C}}$ defined over k and a uniquely determined embedding

$$\phi_{P_0} : \mathcal{C} \to \mathcal{J}_{\mathcal{C}} \text{ with } \phi_{P_0}(P_0) = 0_{\mathcal{J}\mathcal{C}}$$

such that

(1) for all extension fields L of k we get $J_{\mathcal{C}}(L) = \mathrm{Pic}^0_{\mathcal{C}_L}(L)$ where this equality is given in a functorial way and
(2) if $\mathcal{A}$ is an Abelian variety and $\eta : \mathcal{C} \to \mathcal{A}$ is a morphism sending P_0 to $0_{\mathcal{A}}$ then there exists a uniquely determined homomorphism $\psi : \mathcal{J}_{\mathcal{C}} \to \mathcal{A}$ with $\psi \circ \phi_{P_0} = \eta$.

$\mathcal{J}_{\mathcal{C}}$ is uniquely determined by these conditions and is called the Jacobian variety of $\mathcal{C}$. The map ϕ_{P_0} is given by sending a prime divisor $\mathfrak{p}$ of degree 1 of $\mathcal{C}_{\mathcal{L}}$ to the class of $\mathfrak{p} - \mathfrak{p}_0$ in $\mathrm{Pic}^0_{\mathcal{C}_L}(L)$.

Properties of Jacobian varieties

From functoriality and universality of the Jacobian it follows that we can introduce coordinates for divisor classes of degree 0 such that the group law in $\mathrm{Pic}^0_{\mathcal{C}_L}(L)$ is given by rational functions defined over k and depending only on $\mathcal{C}$ (and not on $\mathcal{L}$).

Moreover we can interpret the norm and conorm maps on divisor classes geometrically: Let L/k be a finite algebraic extension. Then the Jacobian variety $\mathcal{J}_{\mathcal{C}_L}$ of $\mathcal{C}_L$ is the scalar extension of $\mathcal{J}_{\mathcal{C}}$ with L, hence a fiber product with projection p to $\mathcal{J}_{\mathcal{C}}$. The norm map is p_*, and the conorm map is p^*.

By universality we get

PROPOSITION 5. *Let $f : \mathcal{C} \to \mathcal{D}$ be a surjective morphism of curves sending P_0 to Q_0. Then there is a uniquely determined surjective homomorphism*

$$f_* : \mathcal{J}_{\mathcal{C}} \to J_{\mathcal{D}}$$

with $f_* \circ \phi_{P_0} = \phi_{Q_0}$.

PROOF. Apply the universal property to the morphism $\phi_{Q_0} \circ f$ to get f_*. The surjectivity follows from the fact that for $k = \bar{k}$ the sums of divisor classes of the form $\mathfrak{p} - \mathfrak{p}_0$ with $\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)$ generate $\mathrm{Pic}^0_{\mathcal{C}}(\bar{k}$. □

A useful observation is

Corollary 2. *Assume that $\mathcal{J}_{\mathcal{C}}$ is a simple abelian variety and that $\eta : \mathcal{C} \to \mathcal{D}$ is a cover. Then $\mathcal{D}$ is the projective line.*

What about the **existence** of Jacobian varieties?

Over the complex numbers the classical theory of curves (key words: Riemann surfaces and the Theorem of Abel-Jacobi) is used to prove the existence of Jacobian varieties in the 19-th century. In fact, this notion was historically earlier than the notion "Abelian variety" introduced by A. Weil as most important tool for his proof of the geometric Riemann hypothesis. By the Lefschetz principle the existence of Jacobian varieties follows for algebraically closed fields of characteristic 0.

For a prove in the frame work of Algebraic Geometry (and so over arbitrary ground fields k) see **??**. The important fact is that we "know" a birational affine model of $J_{\mathcal{C}}$:

By the Theorem of Riemann-Roch we have a surjective map from $\Sigma^g_{\mathcal{C}}(L)$ to $\mathrm{Pic}^0_{\mathcal{C}}(L)$ by sending positive divisor D of degree g to $D_g \cdot \mathfrak{p}_0$. We can interpret such positive divisors geometrically. Take the g-fold cartesian product $\mathcal{C}^g$ of the curve $\mathcal{C}$ of genus g and embed it (via Segre's map) into a projective space. On this variety we can permute the factors and so have an action of S_g, the symmetric group with g letters. Define the g-fold symmetric product $\mathcal{C}^{(g)}$ by $\mathcal{C}^g/\S_g$. Then we can identify $\mathcal{C}^{(g)}(L)$ with $\Sigma^g_{\mathcal{C}}(L)$ and so define a birational map from $\mathcal{C}^{(g)}$ to $\mathcal{J}_{\mathcal{C}}$. Taking an affine part of $\mathcal{C}$ (e.g. found as a regular part of a plane model of $\mathcal{C}$) we get an affine variety which is birational equivalent to $\mathcal{J}_{\mathcal{C}}$.

The Jacobian varieties connect the arithmetic in divisor classes of curves (which is very accessible to algorithms) with the very rich geometric structure of abelian varieties (e.g. isogenies, endomorphisms and ℓ-adic representations).

4.2.6. *Example: Elliptic Curves.* Let $\mathcal{E}$ be an elliptic curve, i.e. a curve of genus 1 with a k-rational point. As seen above, $\mathcal{E}$ is isomorphic to a plane curve $\mathcal{E}'$ given by a Weierstrass equation. We choose one k-rational point P_∞ with prime divisor $\mathfrak{p}_\infty$ and projective coordinates such that $P_\infty = (0:1:0)$ is the infinite point of the curve $\mathcal{E}'$ with equation

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

and identify $\mathcal{E}$ with $\mathcal{E}'$.

Let $\mathcal{J}_{\mathcal{E}}$ be the Jacobian variety of $\mathcal{E}$. We look at

$$\phi_{P_\infty} : \mathcal{E} \to \mathcal{J}_{\mathcal{E}}$$

given by

$$P \mapsto [\mathfrak{p} - \mathfrak{p}_\infty]$$

where [.] means divisor class.

Since $2g_{\mathcal{E}} - 2 = 0$ the theorem of Riemann-Roch implies that for all extension fields L of k in each L-rational divisor class of degree 1 there is exactly one prime divisor $\mathfrak{p}$ of degree 1 corresponding to a point $P \in \mathcal{E}(L)$, and to each divisor class c of degree 0 there is exactly one prime divisor $\mathfrak{p}$ of degree 1 with $c = [\mathfrak{p} - \mathfrak{p}_\infty]$. So ϕ_{P_∞} is injective and surjective and hence an isomorphism of projective varieties.

By transport of structure we endow $\mathcal{E}$ with a group structure:

For extension fields L of k and $P_1, P_2 \in \mathcal{E}(L)$ define $P_1 \oplus P_2$ as the point belonging to the prime divisor in the class $\mathfrak{p}_1 + \mathfrak{p}_2 - 2\mathfrak{p}_\infty$. It is obvious that this makes $\mathcal{E}(L)$ to an abelian group with neutral element P_∞.

We conclude: Three points P_1, P_2, P_3 sum up to 0 if $\mathfrak{p}_1 + \mathfrak{p}_2 + \mathfrak{p}_3 - 3\mathfrak{p}_\infty = (f)$ with $f \in k(\mathcal{E})$.

Now recall that $\mathcal{E}$ has degree 3 and so lines intersect with $\mathcal{E}$ in 3 points (counted with multiplicities) and so f defines a line in $\mathbb{P}^2$. Hence $P_1 + P_2 + P_3 = 0$ iff the three points are collinear, and then $P_1 \oplus P_2 = \ominus P_3$. Using coordinates we get an algebraic recipe for addition:

For given $P \neq P\infty$ take the line through P and P_∞ to get: $\ominus(P)$ is the third intersection point of the line with $\mathcal{E}$ (if this point is equal to P the line is a tangent and $P = \ominus P$ is an element of order 2). Given two points $P_1 \neq P_2$ compute the line through these two points, take its third intersection point P_3 with $\mathcal{E}$ to get $P_1 \oplus P_2 = \ominus P_3$.

By elementary algebra one can perform this recipe by writing down formulas in rational functions in (X, Y, Z) and so we get

Theorem 27. *After the choice of a base point P_∞ the elliptic curve $\mathcal{E}$ is an Abelian variety of dimension 1 with neutral element $P\infty$ which is equal to $\mathcal{J}_\mathcal{E}$.*

4.3. Cantor's Algorithm. Inspired by the group law on elliptic curves and its geometric interpretation we give an explicit algorithm for the group operations on Jacobian varieties of hyperelliptic curves.

Take a genus $g \geq 2$ hyperelliptic curve $\mathcal{C}$ with a least one rational Weierstra"s point given by the affine Weierstra"s equation

$$W_\mathcal{C}: \; y^2 + h(x)\, y = x^{2g+1} + a_{2g}x^{2g} + \cdots + a_1 x + a_0, \tag{2}$$

over k. We denote the prime divisor corresponding to $P_\infty = (0:1:0)$ by $\mathfrak{p}_\infty$.

We note that the affine coordinate ring of $W_\mathcal{C}$ is

$$\mathcal{O} = k[X,Y]/(Y^2 + h(X) < Y - (X^{2g+1} + a_{2g}X^{2g} + \cdots + a_1 X + a_0) >$$

and so prime divisors $\mathfrak{p}$ of degree d of $\mathcal{C}$ correspond to prime ideals $P \neq 0$ with $[\mathcal{O}/P : k] = d$.

Let ω be the hyperelliptic involution of $\mathcal{C}$. It operates on $\mathcal{O}$ and on $\mathrm{Spec}(\mathcal{O})$ and fixes exactly the prime ideals which "belong" to Weierstra"s points, i.e. split up in such points over $\bar{k}$.

Following Mumford [48] we introduce polynomial coordinates for points in $J_{CC}(k)$. The first step is to normalize representations of divisor classes. In each divisor class $c \in \mathrm{Pic}^0(k)$ we find a unique *reduced* divisor

$$D = n_1\mathfrak{p}_1 + \cdots + n_r\mathfrak{p}_r - d\mathfrak{p}\infty$$

with $\sum_{i=1}^r n_i \deg(\mathfrak{p}_i) = d \leq g$, $\mathfrak{p}_i \neq \omega(\mathfrak{p}_j$ for $i \neq j$ and $\mathfrak{p}_i \neq \mathfrak{p}_i nfty$. (We use Riemann-Roch and the fact that ω induces $-id_{J_\mathcal{C}}$.)

Using the relation between divisors and ideal in coordinate rings we get that $n_1\mathfrak{p}_1 + \cdots + n_r\mathfrak{p}_r$ corresponds to an ideal $I \subset \mathcal{O}$ of degree d and the property that if the prime ideal P_i is such that both P and $\omega(P)$ divide I then it belongs to a Weierstra"s point.

By algebra we get that the ideal I is a free $\mathcal{O}$-module of rank 2 and so

$$I = k[X]u(X) + k[x](v(X) - Y).$$

Fact: (see Theorem 4.143 in [7]) $u(X), v(X) \in k[X]$, u monic of degree d, $\deg(v) < d$ and u divides $v^2 + h(X)v - f(X)$.

Moreover, c is uniquely determined by I, I is uniquely determined by (u, v) and so we can *take* (u, v) *as coordinates for* c.

Theorem 28 (Mumford representation). *Let* $\mathcal{C}$ *be a hyperelliptic curve of genus* $g \geq 2$ *with affine equation*

$$y^2 + h(x)\, y \;=\; f(x),$$

where $h, f \in K[x]$, $\deg f = 2g + 1$, $\deg h \leq g$.
Every non-trivial group element $c \in \operatorname{Pic}^0_{\mathcal{C}}(k)$ *can be represented in a unique way by a pair of polynomials* $u, v \in K[x]$, *such that*

i) u *is a monic*
ii) $\deg v < \deg u \leq g$
iii) $u \,|\, v^2 + vh - f$

How to find the polynomials u, v?

We can assume without loss of generality that $k = \bar{k}$ and identify prime divisors $\mathfrak{p}_i$ with points $P_i = (x_i, y_i) \in k \times k$. Take the reduced divisor $D = n_1\mathfrak{p}_1 + \cdots + n_r\mathfrak{p}_r - d\mathfrak{p}\infty$ now with $r = d \leq g$. Then

$$u(X) = \prod_{i=1}^{r} (X - x_i)^{n_i}.$$

Since $(X - x_i)$ occurs with multiplicity n_i in $u(X)$ we must have for $v(X)$:

$$\left(\frac{d}{dx}\right)^j \left[v(x)^2 + v(x)\, h(x) - f(x)\right]_{x = x_i} = 0,$$

and one determines $v(X)$ by solving this system of equations.

Addition: Take the divisor classes represented by $[(u_1, v_1]$ and $[u_2, v_2]$ and "in general position". Then the product is represented by the ideal $I \in \mathcal{O}$ given by $< u_1u_2, u_1(y - v_2), u_2(y - v_1), (y - v_1)(y - v_2) >$. We have to determine a base, and this is done by Hermite reduction. The resulting ideal is of the form $< u_3'(X), v_3'(X) + w_3'(X)Y >$ but not necessarily reduced. To reduce it one uses recursively the fact that $u|(v^2 - hv - f)$. The formalization of this procedure and the treatment of special cases are the content of the algorithm of **Cantor**, which will be given in detail in the interesting cases $g = 2, 3$.

For another approach using approximation by rational functions see [37]. We give his algorithm in the next subsection.

4.3.1. *Genus 2.* Let $\mathcal{C}$ be a genus 2 curve defined over a field k. If char $k \neq 2, 3$ the $\mathcal{C}$ is isomorphic to a curve with equation

$$y^2 = a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0. \tag{3}$$

Thus, infinity is a Weierstrass point of $\mathcal{C}$. Let $\mathcal{O} = \infty$ and $D \in \operatorname{Jac}(\mathcal{C})$. Then, in the equivalence class of D we find a **reduced divisor** which is given by

$$D = P_1 + P_2 - 2\mathcal{O}$$

where $P_1(x_1, y_1)$, $P_2(x_2, y_2)$ are points in the curve. For any two divisors $D_1 = P_1 + P_2 - 2\mathcal{O}$ and $D_2 = Q_1 + Q_2 - 2\mathcal{O}$ in the reduced form, we determine the cubic polynomial

$$y = g(x) = b_0x^3 + b_1x^2 + b_2x + b_3, \tag{4}$$

going through the points $P_1(x_1, y_1)$, $P_2(x_2, y_2)$, $Q_1(x_3, y_3)$, and $Q_2(x_4, y_4)$. This cubic will intersect the curve $\mathcal{C}$ at exactly two other points R_1 and R_2 with coordinates

$$R_1 = (x_5, g(x_5)) \quad \text{and} \quad R_2 = (x_6, g(x_6))\,, \tag{5}$$

where x_5, x_6 are roots of the quadratic

$$x^2 + \left(\sum_{i=1}^{4} x_i\right) x + \frac{b_3^2 - a_5}{b_0^2 \prod_{i=1}^{4} x_i} = 0. \tag{6}$$

Let us denote by $\overline{R}_1 = (x_5, -g(x_5))$ and $\overline{R}_2 = (x_6, -g(x_6))$. Then,

$$D_1 + D_2 = \overline{R}_1 + \overline{R}_2 - 2\mathcal{O}. \tag{7}$$

4.4. Division Polynomials. An elliptic curve E over a field K is a one-dimensional Abelian variety over K or equivalently a genus one irreducible, projective curve over K with a specified point $\mathcal{O}$.

When char $K \neq 2, 3$ then we can take the affine equation of E as

$$E: \quad y^2 = x^3 + ax + b,$$

for $a, b \in K$. Usually we take the point $\mathcal{O}$ to be the point at infinity. Since our focus is on isogenies and torsion subgroups of $E(K)$ let us first recall a few basic results:

LEMMA 13. *For any integer m and point $P(x, y) \neq \mathcal{O}$ in E, the point $[m]P$ has coordinates*

$$[m]P = \left(\frac{\phi_m(x, y)}{\psi_m(x, y)^2}, \frac{\omega_m(x, y)}{\psi_m(x, y)^3}\right)$$

where are given by the recurrence

$$\begin{aligned}
\psi_1 &= 1,\\
\psi_2 &= 2y^2,\\
\psi_3 &= 3x^4 + 6ax^2 + 12bx - a^2,\\
\psi_4 &= (2x^6 + 10ax^4 + 40bx^3 - 10a^2x^2 - 8abx - 2a^3 - 16b^2)2y^2, \qquad (8)\\
&\dots\\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad \textit{for } m \geq 2,\\
\psi_2\psi_{2m} &= (\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)\psi_m \quad \textit{for } m \geq 3.
\end{aligned}$$

and ϕ_m and ω_m are

$$\begin{aligned}
\phi_m &= x\psi_m^2 - \psi_{m+1}\psi_{m-1},\\
\omega_m &= \psi_{m-1}^2\psi_{m+2} + \psi_{m-2}\psi_{m+1}^2.
\end{aligned} \tag{9}$$

The proof is considered part of the folklore of elliptic curves and we will skip it here. The polynomial ψ_m is called the **m-th division polynomial** and it vanishes in $E[m]$

Corollary 7. *All m-torsion points $P(x,y)$ of E have coordinates satisfying $\psi_m(x,y)=0$*

This provides a computational approach on how to determine the m-torsion points for any given $m \geq 2$.

4.4.1. *Division polynomials for genus 2 Jacobians.* Now that we have defined explicitly the addition in $\operatorname{Jac} \mathcal{X}$ it is a natural problem that given a reduced divisor $D \in \operatorname{Jac} \mathcal{X}$, determine explicitly the formulas for $[n]D$, similarly as in the case of elliptic curves. Hence, we want to determine explicitly division polynomials which would help us determine the torsion points. There has been a lot of activity on this area lately; see [49], [32], [33]. We describe briefly below.

Let $P \in \operatorname{Jac} \mathcal{X}$. Define $\phi_1, \dots, \phi_4$ as

$$\phi_1 = 1, \ \phi_2 = \dots, \phi_3 = \dots, \phi_4 = \dots.$$

Then, for m and n be integers with $m > n \geq 1$. Then,

$$\phi_{m+n}\phi_{m-n} = \phi_n^2 \phi_{m+1}\phi_{m-1} - \phi_m^2 \phi_{n+1}\phi_{n-1} + \frac{h_n^1 h_m^2 - h_n^2 h_m^1}{m^2 n^2}$$

where

$$h_n^{(i)} = \left(\frac{\partial}{\partial u_i} \phi_n \right) \left(\frac{\partial}{\partial u_2} \phi_n \right) - \phi_n \left(\frac{\partial}{\partial u_i} \frac{\partial}{\partial u_2} \phi_n \right)$$

In particular,

$$\phi_{2m+1} = \phi_m^3 \phi_{m+2} - \phi_{m+1}^3 \phi_{m-1} + \frac{h_m^{(1)} h_{m+1}^{(2)} - h_m^{(2)} h_{m+1}^{(1)}}{m^2 (m+1)^2}, \text{ for } \ m \geq 2$$

$$\phi_2 \phi_{2m} = \phi_{m-1}^2 \phi_m \phi_{m+2} - \phi_{m+1}^2 \phi_m \phi_{m-2} + \frac{h_{m-1}^{(1)} h_{m+1}^{(2)} - h_{m-1}^{(2)} h_{m+1}^{(1)}}{(m-1)^2}, \text{ for } \ m \geq 3$$

see [33, Theorem 9]. If char $k = 0$ or char k is prime to n and all the coefficients of $\phi_1, \dots, \phi_n$ then

$$[n]P = \left(s_{n,0} : s_{n,11} : s_{n,12} : s_{n,22} : s_{n,111} : s_{n,112} : s_{n,122} : s_{n,222} : s_n \right),$$

where $s_{n,0}, \dots, s_n$ are as in [33, pg. 192]. Such formulas are generalized in [63] for all hyperelliptic Jacobians.

4.5. Endomorphism rings. Not every algebraic curve of genus $g \geq 3$ is hyperelliptic. Hence, the first task is to distinguish which Jacobian varieties are hyperelliptic. We have the following:

Theorem 29. *Let $\mathcal{X}$ be an algebraic curve and $\mathcal{A} := \operatorname{Jac}(\mathcal{X})$ with canonical principal polarization ι. Then,*

$$\operatorname{Aut} \mathcal{X} \cong \begin{cases} \operatorname{Aut}(\mathcal{A}, \iota), & \textit{if } \mathcal{X} \textit{is hyperelliptic} \\ \operatorname{Aut}(\mathcal{A}, \iota)/\{\pm 1\}, & \textit{if } \mathcal{X} \textit{is non-hyperelliptic} \end{cases}$$

See [47] for a proof. The above result can be used to find Jacobians of genus 3 hyperelliptic curves; see [65].

There is a nice result on endomorphism rings when restricted to hyperelliptic Jacobians.

Theorem 30 (Zarhin). *Let $\mathcal{X}$ be a hyperelliptic curves with affine equation $y^2 = f(x)$, $n = \deg f$, and $f \in \mathbb{Q}[x]$. If $\operatorname{Gal}(f)$ is isomorphic to A_n or S_n then $\operatorname{End}_{\overline{\mathbb{Q}}}(\operatorname{Jac} \mathcal{X}) \cong \mathbb{Z}$.*

The theorem is actually true over any number field K.

4.6. Hyperelliptic curves over finite fields. Let $\mathcal{X}$ be a hyperelliptic curve of genus $g \geq 2$ defined over $\mathbb{F}_q$. The Hasse-Weil bound gives

$$(q^{1/2}-1)^{2g} \leq |\operatorname{Pic}^0(\mathcal{X})| \leq (q^{1/2}+1)^{2g} \tag{10}$$

The characteristic polynomial of the Frobenius as defined in eq. (1) is a degree $2g$ polynomial given as follows:

(11)
$$\chi_{\mathcal{X},q}(T) = T^{2g}+a_1T^{2g-1}+\cdots+a_gT^g+a_{g-1}q\,T^{g-1}+\cdots+a_{g-i}q^i\,T^{g-i}+\cdots a_1q^{g-1}\,T+q^g,$$

where $a_i \in \mathbb{Z}$ and $1 \leq i \leq g$. We denote by

$$M_k = \#\mathcal{X}(\bar{\mathbb{F}}_q) \quad \text{and} \quad N_k = |\operatorname{Pic}^0_{\mathcal{X}/\mathbb{F}_{q^k}}|.$$

Let us assume that $\chi_{\mathcal{A},q}(T)$ factors over $\mathbb{C}$ as

$$\chi_{\mathcal{X},q}(T) = \prod_{i=1}^{2g}(T-\alpha_i).$$

Next we have the following:

Proposition 6. *The following are true:*

i) *The roots of $\chi_{\mathcal{X},q}(T)$ have magnitude $|\alpha_i| = \sqrt{q}$, for $1 \leq i \leq g$.*

ii) *$\chi_{\mathcal{X},q}(T)$ is quasi-palindromic. In other words, $\alpha_{i+g} = \bar{\alpha}_i$, hence $\alpha_i\alpha_{i+g} = q$, for $1 \leq i \leq g$.*

iii) *For any integer j we have,*

$$N_j = \prod_{i+1}^{2g}(1-\alpha_i^j), \quad M_j = q^j+1-\sum_{i=1}^{2g}\alpha_i^j$$

and

$$\left|M_j-(q^j+1)\right| \leq g\left\lfloor 2q^{j/2}\right\rfloor$$

iv) *For $1 \leq i \leq g$ and $a_0 := 1$ we have*

$$i\,a_i = \sum_{s=1}^{i}\left(M_s-(q^s+1)a_{i-s}\right).$$

We refer the reader to [7, pg. 311] for more details. We will revisit hyperelliptic curves over finite fields again in the next chapters when we consider cryptographic applications.

5. Modular curves

Let $\mathbb{P}^1 := \mathbb{C} \cup \{\infty\}$ be the Riemann sphere and $\mathrm{GL}_2(\mathbb{C})$ the group of 2×2 matrices with entries in $\mathbb{C}$. The group $\mathrm{GL}_2(\mathbb{C})$ acts on $\mathbb{P}^1$ by linear fractional transformations as follows

$$\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} z = \frac{\alpha z+\beta}{\gamma z+\delta} \tag{12}$$

where $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in \mathrm{GL}_2(\mathbb{C})$ and $z \in \mathbb{P}^1$. The $\mathrm{GL}_2(\mathbb{C})$ action on $\mathbb{P}^1$ is a transitive action, i.e. has only one orbit. Moreover, the action of $\mathrm{SL}_2(\mathbb{C})$ on $\mathbb{P}^1$ is also transitive.

Consider now the induced action of $\mathrm{SL}_2(\mathbb{R})$ on the Riemann sphere. Notice that this action is not transitive. Let $\mathbb{H}_2$ be the *complex upper half plane*, i.e.

$$\mathbb{H}_2 = \left\{ z = x + iy \in \mathbb{C} \;\middle|\; y > 0 \right\} \subset \mathbb{C}.$$

Lemma 14. *i) The action of* $\mathrm{SL}_2(\mathbb{R})$ *on* $\mathbb{P}^1$ *has three orbits, namely* $\mathbb{R} \cup \infty$*, the upper half plane* $\eqsim_2$*, and the lower-half plane.*

ii) The group $\mathrm{SL}_2(\mathbb{R})$ *acts transitively on* $\mathbb{H}_2$ *and for every* $g \in \mathrm{SL}_2(\mathbb{R})$ *and* $z \in \mathcal{H}_2$ *we have*

$$\mathrm{Im}(gz) = \frac{\mathrm{Im}\, z}{|\gamma z + \delta|^2}$$

Recall that a group action $G \times X \to X$ is called **faithful** if there are no group elements g, except the identity element, such that $gx = x$ for all $x \in X$. The group $\mathrm{SL}_2(\mathbb{R})$ does not act faithfully on $\mathbb{H}_2$ since the elements $\pm I$ act trivially on $\mathbb{H}_2$. Hence, consider the above action as $\mathrm{PSL}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})/\{\pm I\}$ action. This group acts faithfully on $\mathbb{H}_2$.

5.1. The modular group and the fundamental domain. Let S be a set and G a group acting on it. Two points s_1, s_2 are said to be G**-equivalent** if $s_2 = gs_1$ for some $g \in G$. For any group G acting on a set S we call a **fundamental domain** $\mathcal{F}_S$, if one exists, a subset of S such that any point in S is G-equivalent to some point in $\mathcal{F}$, and no two points in the interior of $\mathcal{F}$ are G-equivalent.

The group $\Gamma = \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$ is called the **modular group**. The following theorem determines the generator of the modular group and their relations.

Theorem 31. *The modular group* Γ *is generated by* $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ *and* $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$*, where* $S^2 = 1$ *and* $(ST)^3 = 1$.

Note that $S^2 = 1$, so S has order 2, while $T^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ for any $k \in \mathbb{Z}$, so T has infinite order. It is easy to prove that the Γ action on $\mathbb{H}_2$ via linear fractional transformations is a group action. This action has a fundamental domain $\mathcal{F}$ as follows;

$$\mathcal{F} = \left\{ \; z \in \mathbb{H}_2 \;\middle|\; |z|^2 \geq 1 \;\text{ and }\; |\Re(z)| \leq 1/2 \right\}$$

as stated in the following theorem.

Theorem 32. *i) Every* $z \in \mathbb{H}_2$ *is* Γ*-equivalent to a point in* $\mathcal{F}$.

ii) No two points in the interior of $\mathcal{F}$ *are equivalent under* Γ*. If two distinct points* z_1, z_2 *of* $\mathcal{F}$ *are equivalent under* Γ *then* $\Re(z_1) = \pm 1/2$ *and* $z_1 = z_2 \pm 1$ *or* $|z_1| = 1$ *and* $z_2 = -1/z_1$.

iii) Let $z \in \mathcal{F}$ *and* $I(z) = \{g \,|\, g \in \Gamma,\, gz = z\}$ *the stabilizer of* $z \in \Gamma$*. One has* $I(z) = \{1\}$ *except in the following cases:*

$z = i$*, in which case* $I(z)$ *is the group of order 2 generated by* S*;*

$z = \rho = e^{2\pi i/3}$*, in which case* $I(z)$ *is the group of order 3 generated by* ST*;*

$z = -\overline{\rho} = e^{\pi i/3}$*, in which case* $I(z)$ *is the group of order 3 generated by* TS*.*

The following corollary is obvious.

Corollary 8. *The canonical map* $\mathcal{F} \to \mathbb{H}_2/\Gamma$ *is surjective and its restriction to the interior of* $\mathcal{F}$ *is injective.*

Consider again the action of Γ on $\mathbb{H}_2$. Take the space $\mathbb{H}_2/\Gamma$ which is indeed the interior of $\mathcal{F}$. This is denoted by $Y(1)$, which is a Riemann surface. Its compactification is denoted by $X(1)$. Obviously, $X(1)$ is the Riemann sphere.

Let us now consider some subgroups of the modular group,

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid a \equiv 0 \mod N \right\}$$
$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid c \equiv 0 \mod N \right\}$$

Such groups also act on $\mathbb{H}_2$. The quotient spaces $\mathbb{H}_2/\Gamma(N)$ and $\mathbb{H}_2/\Gamma_0(N)$ are denoted by $Y(N)$ and $Y_0(N)$ respectively. They are Riemann surfaces since $\Gamma(N)$ and $\Gamma_0(N)$ are discrete subgroups.

The compactification of $Y(N)$ and $Y_0(N)$ are denoted by $X(N)$ and $X_0(N)$ respectively. They are smooth, projective curves defined over $\mathbb{Q}$. The genus of $X_0(p)$ is given below when p is prime:

$$g = \begin{cases} 0 \quad if \quad p = 2, 3 \\ \dfrac{(p-13)}{12} \quad if \quad p \equiv 1 \mod 12 \\ \dfrac{(p-5)}{12} \quad if \quad p \equiv 5 \mod 12 \\ \dfrac{(p-7)}{12} \quad if \quad p \equiv 7 \mod 12 \\ \dfrac{(p-11)}{12} \quad if \quad p \equiv 11 \mod 12 \end{cases}$$

Next we see how we can compute the equations of

5.2. Modular Polynomials. Modular polynomials play an important role in the theory of elliptic curves.

We denote by $\phi_N(x, y)$ the N-th modular polynomial. Two elliptic curves with j-invariants j_1 and j_2 are n-isogenous if and only if $\phi_N(j_1, j_2) = 0$. The equation $\phi_N(x, y) = 0$ is the canonical equation of the modular curve $X_0(N)$. We display $\phi_N(x, y)$ for $N = 2, 3$.

$$\begin{aligned} \phi_2 &= x^3 - x^2y^2 + y^3 + 1488xy(x+y) + 40773375xy - 162000(x^2+y^2) \\ &+ 8748000000(x+y) - 157464000000000 \\ \phi_3 &= -x^3y^3 + 2232x^3y^2 + 2232y^3x^2 + x^4 - 1069956x^3y + 2587918086x^2y^2 \\ &- 1069956y^3x + y^4 + 36864000x^3 + 8900222976000x^2y + 8900222976000y^2x \\ &+ 36864000y^3 + 452984832000000x^2 - 770845966336000000xy + 452984832000000y^2 \\ &+ 1855425871872000000000x + 1855425871872000000000y \end{aligned}$$

Modular polynomials are computed for large N.

Lemma 15. *Two elliptic curves E and E' are isogenous, with an isogeny of degree n if and only if their j-invariants satisfy the n-th modular polynomial.*

There have been some attempts in the last decade to generalize modular polynomials for higher dimensional varieties. The interested reader should consult [4] for abelian surfaces.

Part 2. Cryptography

Next we will focus on applications of abelian varieties to cryptography. Our main goal is to give a brief description of current methods used in cryptography including recent developments. Throughout this part we leave the reader with open questions and challenges which we hope will get the interested reader involved.

6. Diffie-Hellman Key Exchange

6.1. The Classical Case. The task to solve is: Find a protocol such that two partners P_1, P_2 can agree on a common secret by using public channels and algorithms.

A groundbreaking solution was found by W. Diffie and H. E. Hellman in [17] with the idea to use (computational) one-way functions. They suggest to use the multiplicative group of finite fields $\mathbb{F}_q$ and, for a prime number $\ell | q-1$ choose a primitive root ζ_ℓ, private keys $k_i \in \mathbb{Z}$ and public keys $p_i = \zeta_\ell^{k_i}$. The common secret is

$$s_{1,2} = \zeta_\ell^{k_1 \cdot k_2}.$$

All computations are very fast (polynomial in $\log(q)$. The security is measured by the hardness of the **Diffie-Hellman** computational problem (CDH):

$$\text{For random elements } a, b \in \{0, \ell - 1\} \text{ and given } \zeta_\ell^a,\ \zeta_\ell^b \text{ compute } \zeta_\ell^{a \cdot b}.$$

Let ζ be a primitive root of unity in $\mathbb{F}_q^*$. Define the (classical) discrete logarithm (DL) of an element $x \in \mathbb{F}_q^*$ with respect to the base ζ by

$$\log_\zeta(x) = \mathrm{Min}\{n \in \mathbb{N} \text{ such that } \zeta^n = x.$$

It is obvious that an algorithm that computes discrete logarithms (e.g. in ζ_ℓ) solves (CDH). This problem is rather old (going back at least to the 19-th century). C.F. Gauss introduced the term "index" in the Disquisitiones Arithmeticae (1801) for the discrete logarithm modulo p, and there are tables for primes up to 1000 by C.G. Jacobi(1839).

A systematic algorithm is given in the book of Kraichik (1922) [35]; in fact this is the index-calculus algorithm reinvented and refined in cryptography from 1980 till today [31]. As result one gets algorithms of subexponential complexity (with relatively small constants, see [31]), which are even dramatically faster if q is not a prime. The reason for these fast algorithms is the fact that it is easy to lift elements in $\mathbb{F}_q$ to elements in rings of integers of number fields.

6.2. A First Abstraction. Obviously we can use the Diffie-Hellman key exchange scheme if we have

- a finite cyclic group $(C, \circ)$ with a generator g_0,
- a numeration, i.e. an injective map

$$f : C \to \mathbb{N},$$

- an addition law $\oplus$ on $f(C)$ with

$$f(f^{-1}(a) \circ f^{-1}(b)) = a \oplus b \text{ for all } a, b \in f(C).$$

$f(C)$ becomes a $\mathbb{Z}$-module in the usual scalar multiplication: $0 \cdot a = f(0_C)$, $n \cdot a =$ $(n-1)$-fold addition of a to itself, $(-n) \cdot a = n \cdot (\ominus a)$ for $a \in f(C)$, $n \in \mathbb{N}$.

The private keys are again $k_i \in \mathbb{Z}$, the public keys are $k_i \cdot f(g_0)$, and the common secret is $k_1 \cdot (k_2 \cdot f(g_0))$. The CDH problem is: For random $a_1, a_2 \in f(C)$ with (publicly unknown k_1, k_2 such that $k_i \cdot f(g_0) = a_i$ compute $c = (k_1 \cdot k_2) \cdot f(g_0)$.

Define the discrete logarithm (DL) by

$$\log_{g_0}(a) := \mathrm{Min}\{n \in \mathbb{N} \text{ such that } n \cdot f(g_0) = a.$$

Again, the computation of the (DL) solves CDH. By elementary number theory (CRT and p-adic expansion) one sees immediately that the computation of (DL) is reduced to the computation of the discrete logarithms in all $f(C_\ell)$ with C_ℓ the subgroup of C of elements of order dividing ℓ and ℓ dividing $|C|$. Hence we can and will assume from now on that C is cyclic of prime order ℓ.

6.2.1. *Black Box Groups.* A "generic" object of the situation above is given by a black box group C of prime order ℓ.

(1) There are algorithms that compute (DL) (probabilistically) with $\mathcal{O}(\sqrt(\ell)$ group operations in C (e.g. Shank's bay-step giant step algorithm, Pollard ρ algorithm et.al.), and these algorithms are applicable for all finite cyclic groups, and one cannot do better.

(2) Up to algorithms with subexponential complexity, the computation of (DL) in C is equivalent with (CDH)(Maurer-Wolf).

6.3. Mathematical Task. In order that we can use (a family of) groups C for crypto systems based on discrete logarithms they have to satisfy three crucial conditions:

(1) C has a known large prime order ℓ and a numeration $f : C \to \mathbb{N}$.

(2) Condition for the numeration: The elements in C can be stored in a computer in a compact way (e.g. $\mathcal{O}(\log \ell)$ bits needed)).

(3) The group composition $\oplus$ induced by f is given by an algorithm that is easily and efficiently implemented and very fast.

(4) The computation of the DL in $f(C)$ (for random elements) is very hard and so infeasible in practice (ideally the bit-complexity should be exponential in $\log \ell$).

It is surprisingly hard to construct such groups. All known examples today are related with subgroups of Picard groups of hyperelliptic curves of genus ≤ 3 over prime fields $\mathbb{F}_p$. It will be one of the main aims of the paper to explain this statement.

6.4. Q-bit Security. As said, we shall describe below DL-systems for which we have good reasons to believe that the bit-complexity is exponential and so the task in Subsection 6.3 is solved. But the possibility that quantum computing may be realizable in foreseeable time yields new aspects for the discussion of security of crypto systems. By Shor's algorithm it follows that the q-bit complexity of discrete logarithms in **all** finite groups is polynomial!. So it is challenging to find key exchange systems that are not based on discrete logarithms in groups but still are near to the original idea of Diffie and Hellman. In the quantum world new relations between crypto primitives arise, and it seems that hidden subgroup problem and connected to it, the hidden shift problem related to groups G are central ([51] and [36]). Here the state of the art is that for abelian G the problems can be solved in subexponential time and space, for dihedral groups there is "hope".

6.5. Key Exchange with G-sets. The DL-system in Subsection 6.3 can be seen in the following way: By scalar multiplication the set of generators $A \subset \mathbb{N}$ of the group $f(C)$ becomes a $\mathbb{Z}$-set, and so elements of $\mathbb{Z}$ induce commuting translations on A.

A next step to generalize the Diffie-Hellman key exchange is to replace $\mathbb{Z}$ by a (semi-) group G and the set of generators by a G-set $A \subset \mathbb{N}$ on which G operates transitive. For $g \in G$, define $t_g \in \mathrm{End}_{set}(A)$ by

$$a \mapsto t_g(a) := g \cdot a.$$

Let G_1 be a semi-subgroup of G and $G_2 = Z(G_1)$ the centralizer of G_1 in G. (If G is abelian then $G = G_1 = G_2$.) Because of

$$g_1 \cdot (g_2 \cdot a_0) = (t_{g_1} \circ t_{g_2}) \cdot a_0 = (t_{g_2} \circ t_{g_1}) \cdot a_0$$

for $g_1 \in G_1$ and $g_2 \in G_2$ we can use (A, a_0, G_1, G_2) for key exchange by defining an obvious analogue of the scheme in Subsection 6.3.

The security of this exchange depends on the difficulty to find the translations t_{g_i}. We remark that though the security of such systems is, in general, not related to discrete logarithms, it may happen that the generic algorithms from 6.3 can still be applied.

What about quantum security? One breaks the system if one can determine t_{g_1}. This is a typical problem for the hidden shift: Take the maps

$$f_0 : B_1 \to A \text{ with } f_0(g) = t_g \cdot a_0$$

and

$$f_1 : B_1 \to A \text{ with } f_1(g) = t_g \cdot (t_{g_1} \cdot a_0)$$

and find the shift.

For B_1 abelian and finite there is an algorithm of Kuperberg [36], which solves this task in subexponential time. In particular we see that every Diffie-Hellman key exchange based on $\mathbb{Z}$-sets has at best subexponential security.

6.6. Abstract Setting of Key Exchange. On our way to generalization we get rid of the algebraic structures. Assume $A \subset \mathbb{N}$ and let $B_1, B_2 \subset \mathrm{End}_{set}(A)$. Choose $a_0 \in A$. We need the **Centralizing Condition**:

The elements of B_1 commute with the elements of B_2 on $B_i\{a_0\}$. Then

$$\{b_1(b_2(a_0)) = b_2(b_1(a_0))\}$$

and this is all we need for key exchange.

The effectiveness of this exchange is given if for $b_i \in B_i, b_j \in B_j$ the value $b_i(b_j(a_0))$ can be quickly evaluated (i.e., calculated and represented). The analogue of the Computational Diffie-Hellman problem is

CDH: For randomly given $a_1, a_2 \in A$compute (if existing)a_3 with $a_3 = b_{a_1} \cdot (b_{a_2} \cdot a_0)$

where $b_{a_i} \in B_i$ such that $b_{a_i} \cdot a_0 = a_i$. It is clear that CDH can be solved if one can calculate for random $a \in B_i \cdot \{a_0\}$ an endomorphism $b_a \in B_i$ with $b_a(a_0) = a$. We remark that b_a may be not uniquely determined by a.

Problem:

(1) Find a "genuine" usable instance for the abstract setting!
(2) What can one say about quantum computing security?

6.7. Key Exchange in Categories. We make a final step of abstraction (and leave it to the reader to check that the schemes above are special cases). As always we assume that we have two partners P_1 and P_2 who want to have a common secret.

Let $\mathbb{C}_i$; $i = 1, 2$ be two categories whose objects are the same sets A_j; $j \in I$ and with morphisms $B^i_{j,k} = \mathrm{Mor}^i(A_j, A_k)$. We fix a "base" object A_0. We assume that $\mathbb{C}^1, \mathbb{C}^2, A_0$ satisfies the following conditions:

(1) For every $\varphi \in B^1(A_0, A_j)$ and every $\psi \in B^2(A_0, A_k)$ the pushout exists, i.e. there is a uniquely (up to isomorphisms) determined triple
$$(A_l,\ \gamma_1 \in B^1(A_k, A_l),\ \gamma_2 \in B^2(A_j, A_l))$$
with
$$\gamma_2 \circ \varphi = \gamma_1 \circ \psi$$
and this triple is minimal.

(2) P^1 can determine A_l if he knows φ, A_k and an additional (publicly known) information $P(\psi)$ (which is often a subset of A_k), and an analogue fact holds for P^2.

Key Exchange. Given such categories $\mathbb{C}^1, \mathbb{C}^2$ the partners can chose φ, , ψ, send A_j, A_k and $P(\psi)$ respectively $P(\varphi)$ and compute the ***common secret*** A_l.

Effectiveness. We assume that all the objects concerning $\mathbb{C}^i$ can be handled by computers in a fast and compact way, in particular, for chosen φ, ψ the objects A_j, A_k as well as the additional information can be computed rapidly. Moreover, using the given information, P^i can compute of A_l quickly.

Security. The scheme is broken if (CDH) is weak: For randomly given A_j, A_k determine A_l, which is the pushout of
$$A_0 \overset{\varphi}{\to} A_j$$
and
$$A_0 \overset{\psi}{\to} A_k.$$
For this, it is allowed to use the additional information. We shall see an example for this categorial key exchange in section 9.4.2, and till now all algorithms for breaking this system have exponential complexity.

7. Index calculus for hyperelliptic Jacobians

The method of index calculus shows that for some special groups we can get subexponential time algorithms for the DLP. We will briefly describe the idea of index calculus and then see how it applies to Jacobians of hyperelliptic curves.

7.1. Introduction to index calculus. Let G be a group of order N generated by an element g. If the following holds

$$\oplus_{i=1}^{r}\,[n_i]g_i = 1, \tag{13}$$

then

$$\sum_{i=1}^{r} n_i \log_g(g_i) \equiv 0 \mod N. \tag{14}$$

If we can find many equations as in Eq. (13) such that then we can solve the system in Eq. (14) via linear algebra for $\log_g g_i$, $i = 1, \dots, r$. The set $\{g_1, g_2, \dots, g_r\}$ is called the **factor base**.

Finding enough equations of the form (13) is equivalent is knowing the structure of the group G as a $\mathbb{Z}$-module. A free Abelian group $\mathbb{Z}^r$ generated by $\{X_1, \dots, X_r\}$ and a lattice L in $\mathbb{Z}^r$ generated by relations $\prod_{i=1}^r X_i^{n_i} = 1$ we have a homomorphism

$$\begin{aligned} \phi : \ Z^k &\to G \\ (n_1, \dots, n_k) &\to [n_1]g_1 \oplus \cdots \oplus [n_k]g_k \end{aligned}$$

with kernel L such that $\mathbb{Z}^k/L \cong G$.

Let $\mathcal{P}$ be a countable set of elements in G. A free Abelian monoid M over $\mathcal{P}$ together with an equivalence relation $\sim$ such that $G \cong M/\sim$ is called an **additive semigroup**. The *representation map*

$$\iota : G \hookrightarrow M$$

gives $G \cong M/\sim$. Hence, every element $g \in G$ corresponds uniquely to $\iota(g)/\sim$.

A **size map** is a homomorphism of the monoids norm

$$| \cdot | : (M, \oplus) \mapsto (\mathbb{R}, +).$$

Hence, it is determined by the values of elements of $\mathcal{P}$. We assume that all elements of $\mathcal{P}$ have positive size. The size of an element $g \in G$ is denoted by $|g|$.

The group G together with the monoid M, the equivalence relation $\sim$, the representation map ι, and a size map $| \cdot |$, forms an **arithmetic formation** or simply a formation

$$(G, (M, \cdot), \sim, \iota, | \cdot |) .$$

Let B be a positive integer. Denote by M_B (resp. $\mathcal{P}_B$) the set of elements of M (resp. $\mathcal{P}$) of size not larger than B. In the literature B is referred as a **smoothness bound**. An element of G is called B-smooth if the decomposition of its representation in M involves only elements in $\mathcal{P}_B$.

Example 5 (Prime fields). *Take $G = \mathbb{F}_p^*$ and $M = (\mathbb{Z}, \times)$. Let $\sim$ be the equivalence relation $(\mod p)$ in $\mathbb{Z}$ and $\mathcal{P}$ the set of rational prime numbers. The size map*

$$\log : (\mathbb{Z}, \times) \mapsto (\mathbb{R}, +).$$

is the logarithm of the corresponding positive integer.

7.2. Finite fields. Let $\mathbb{F}_q$ be a finite field, where $q = p^n$ for some prime p. Let $f(x)$ be a monic, irreducible polynomial over $\mathbb{F}_p$ of degree n. Then, there is an isomorphism

$$\psi : \mathbb{F}_q \mapsto \mathbb{F}_p[x]/\langle f(x) \rangle.$$

We take $G = \mathbb{F}_q^*$ and M as the multiplicative monoid of the ring of polynomials over $\mathfrak{f} - p$ under the composition of polynomials. For each element $g \in G$, there is a unique $u \in \mathbb{F}_p[x]$ of degree less than n with $\psi(g) = U + (f)$. Define $\iota(g) = U$. Thus the equivalence relation on M is $U_1 \sim U_2$ if and only if $U_1 \equiv U_2 (\mod f)$. The set $\mathcal{P}$ of primes consists of the set of monic irreducible polynomials over $\mathbb{F}_p$ together with a generator of $\mathbb{F}_p^*$. The size of an element $g \in \mathbb{F}_q$ is defined as $\deg \iota(g)$.

Remark 5. *If the group G has non-trivial automorphisms, say there exists $\tau \in \mathrm{Aut}(G)$ of order m then, under certain conditions, index calculus can search for relations m times faster and perform the linear algebra steps m^2 faster. We will explore this in more details when discussing index calculus for hyperelliptic Jacobians.*

7.3. Index calculus for hyperelliptic Jacobians. Index calculus can be applied to a discrete logarithm in Jacobians of hyperelliptic curves.

Let $\mathcal{X}$ be a hyperelliptic curve of genus $g \geq 2$ over a finite field $\mathbb{F}_q$ of characteristic p and $G := \mathrm{Pic}^0_{\mathbb{F}_q}(\mathcal{X})$. Every element of G can be represented by a $\mathbb{F}_q$-rational divisor of degree at most g. We take the set of *primes* as the set of principal divisors whose effective divisors are irreducible over $\mathbb{F}_q$ or as they are also called *prime divisors*. In terms of the ideal class group they are the *prime ideals*.

Hence, a divisor D with Mumford representation $[u(x), v(x)]$ is *prime* if and only if the polynomial $u(x)$ is irreducible over $\mathbb{F}_q$. The degree of the polynomial $u(x)$ is the degree of the divisor D.

By the above remark, using group automorphisms can have a significant on the speed of the index calculus algorithm. In the case of the hyperelliptic curves the hyperelliptic involution is used to speed up the algorithm.

Let $\mathcal{X}$ have equation

$$y^2 + h(x)\, y = f(x),$$

for $h(x), f(x) \in \mathbb{F}_q[x]$. Let $\tau \in \mathrm{Aut}(\mathcal{X})$ be the hyperelliptic involution. Then τ lifts to an involution in $\mathrm{Jac}(\mathcal{X})$ as follows:

$$\bar{\tau}\left([u(x), v(x)]\right) = [u(x),\, -v(x) - h(x) \mod u(x)]$$

The image of a divisor D under $\bar{\tau}$ is denoted by $-D$.

For a given smoothness bound B the factor base will be composed by all the prime divisors of degree at most B, where as noted above the degree of a prime divisor is the degree of its polynomial $u(x)$ in the Mumford representation $[u(x), v(x)]$.

A divisor is said to be *B-smooth* if all the prime divisors in its decomposition have degree at most B. Then we have the following simple algorithm to compute a set $\mathcal{P}_B$ of B-smooth prime divisors.

Due to work of Adleman, Demarrais, and Huang we have now an algorithm which performs the discrete logarithm in $\mathrm{Jac}_{\mathbb{F}_q}(\mathcal{X})$ in reasonable time. We describe the result below, for an explicit description of the algorithm see [7, pg. 525].

Theorem 33. *If $\ln q \leq (2g+1)^{1-\epsilon}$, then there exists a constant $c \leq 2.18$ such that the discrete logarithms in $\mathrm{Jac}_{\mathbb{F}_q}(\mathcal{X})$ can be computed in expected time $L_{q^{2g+1}}(1/2, c)$.*

The above theorem gives an efficient algorithm for $g > \log_g q$. However, something has to be worked out for curves of "small" genus, namely $g < \log_g q$. This was done by Gaudry and his collaborators.

Theorem 34 (Gaudry). *Let $\mathcal{X}$ be a genus $g \geq 2$ hyperelliptic curve defined over a finite field $\mathbb{F}_q$. If $q > g!$ then discrete logarithms in $\mathrm{Jac}_{\mathbb{F}_q}(\mathcal{X})$ can be computed in expected time $O(g^3 q^{2+\epsilon})$.*

8. Isogenies of Jacobians via Correspondences

We describe a general construction of isogenies between abelian varieties closely attached to Jacobians of curves. As always, K is assumed to be a perfect field. Let

L be a finite algebraic extension field of K. Let $\mathcal{D}_1$ be a regular projective curve over L and $\mathcal{D}_2$ a regular projective curve defined over K. Let $\mathcal{H}$ be a curve over L and

$$\varphi_1 : \mathcal{H} \to \mathcal{D}_1,$$

respectively

$$\varphi_2 : \mathcal{H} \to \mathcal{D}_2 \times_{\mathrm{Spec}(K)} \mathrm{Spec}(L) =: \mathcal{D}_{2,L},$$

be L-rational morphisms. The morphism φ_1 induces the L-rational **conorm morphism**

$$\varphi_1^* : \mathcal{J}_{\mathcal{D}_1} \to \mathcal{J}_{\mathcal{H}}$$

and the morphism φ_1 induces the **norm morphism**

$$\varphi_{2,*} : \mathcal{J}_{\mathcal{H}} \to \mathcal{J}_{\mathcal{D}_{2,L}}.$$

By composition we get a homomorphism

$$\eta_L : \mathcal{J}_{\mathcal{D}_1} \to \mathcal{J}_{\mathcal{D}_{2,L}}$$

defined over L.

Let $\mathcal{W}_{L/K}$ be the Weil restriction of the Jacobian of $\mathcal{D}_1$ to K. This is an abelian variety defined over K with $\mathcal{W}_{L/K}(K) = \mathrm{Pic}^0_{\mathcal{D}_1}$. Applying the norm map from L to K and using the functorial properties of the Weil restriction we get a homomorphism

$$\eta : \mathcal{W}_{L/K} \to \mathcal{J}_{\mathcal{D}_2}.$$

In general, neither the kernel nor the cokernel of η will be finite. But under, usually mild, conditions one can assure that that η has a finite kernel, and so it induces an isogeny of $\mathcal{W}_{L/K}$ to an abelian subvariety of $\mathcal{J}_{\mathcal{D}_2}$.

As application we get a transfer of the discrete logarithm problem from $\mathrm{Pic}^0_{\mathcal{D}_1}$ (defined over L) to the DL-problem in a subvariety of $\mathcal{J}_{\mathcal{D}_2}$ (defined over K). Of course, the efficiency of this transfer depends on the complexity of the algorithms computing the norm- and conorm maps(hence φ_i and $[L : K]$ must have reasonably small degrees), and it makes sense only if the DL-problem after the transfer is easier than before.

8.1. Weil Descent. Take $K = \mathbb{F}_q$ and $L = \mathbb{F}_{q^d}$ with $d > 1$ and $\mathcal{H} = \mathcal{D}_{2,L}$, i.e. a given curve $\mathcal{X}$ defined over $\mathbb{F}_{q^d}$ is covered by a curve $\mathcal{D}_{\mathbb{F}_{q^d}}$, which is the scalar extension of a curve $\mathcal{D}$ defined over K.

This yields a K-rational homomorphism from the Weil restriction $\mathcal{W}_{L/K}$ of $\mathcal{J}_{\mathcal{X}}$ to $\mathcal{J}_{\mathcal{D}}$. $\mathcal{D}$ will (in all non-trivial cases) be a curve of a genus larger than the genus of $\mathcal{X}$ but since it is defined over the smaller field $\mathbb{F}_q$ one can hope that one can apply fast algorithms to compute the discrete logarithm in $\mathcal{J}_{\mathcal{D}}(\mathbb{F}_q)$, e.g. by methods of index-calculus in Sect. 7. Indeed, if $\mathcal{X}$ is not defined of a proper subfield of $\mathbb{F}_{q^d}$ this is the principle of the so-called GHS-attack in (see [26] and [7], 22.3.2), which is successful in remarkably many cases.

If $\mathcal{X}$ is already defined over $\mathbb{F}_q$ one is lead to the so-called trace-zero varieties in $\mathcal{J}_{\mathcal{X}}(\mathbb{F}_{q^d})$ ([7], 7.4.2), and again correspondences induced by covers of curves can be used for attacks on crypto systems based on discrete logarithms on these varieties by work of Diem [7, 22.3.4]. These results already indicate that the use of Picard groups of curves (e.g. elliptic curves) over non-prime fields $\mathbb{F}_{q^d}$ with $d \geq 4$ is not advisable for cryptographic use.

By more recent work of C. Diem this "feeling" is reinforced for instance for families of elliptic curves in towers of finite fields. The methods used in these papers use the Weil restriction method explained above only as a "guideline" and sometimes as tools for proof. The real heart of the methods of Diem is the use of Semaev' s summation polynomials. In this context and in particularly because of suggestions of pairing based cryptography using (supersingular) elliptic curves it is important to mention the enormous progress made in the computation of discrete logarithm in the multiplicative group of finite non-prime fields [31].

8.2. Modular Correspondences. We recall from Section 5 that for N prime to char (K) the modular curve $X_0(N)$ is a regular projective curve, defined over $\mathbb{Z}[1/N]$, and so in particular over $\mathbb{Q}$ and over $\mathbb{F}_p$ with p prime to N.

There is an affine part $Y_0(N)$, which is a (coarse) moduli scheme for the the isomorphism classes of pairs (E, η_N) of elliptic curves with cyclic isogeny of degree N. This means that for every point $P = (j_E, j_\eta)$ in $Y_0(N)(K)$ there is an elliptic curve E defined over K and an isogeny $\eta_N : E \to E'$ with $\ker(\eta_N)$ invariant under the action of G_K and as abelian group isomorphic to $\mathbb{Z}/N$ such that the invariants of E and E' are (j_E, j_η).

The points in $X_0(N) \setminus Y_0(N)$ are the cusps, and it is important that these points have a modular interpretation, too. For example, if N is squarefree, then there is one cusp point at ∞ (in the upper half plane) which corresponds to the pair (Néron polygon with N vertices $,< \zeta_N >$) where ζ_N is a primitive N-th root of unity.

Denote the Jacobian variety of $X_0(N)$ by $J_0(N)$. Let ℓ be a prime not dividing char(K) $\cdot$ N. By the splitting $\mathbb{C}/\ell \cdot N \cong \mathbb{Z}/\ell \times \mathbb{Z}/N$ and an analogous splitting of the kernel of a cyclic isogeny of degree $\ell \cdot N$ in $C_\ell \times C_N$ we get a natural morphism

$$\varphi_\ell : X_0(\ell \cdot N) \to X_0(N).$$

Let ω_ℓ be the involution of $X_0(\ell \cdot N)$ induced by the map that sends the pair (E, η) with $\ker(\eta) = C_\ell \times C_N$ to the pair (E, η') where the kernel of η' is $E[\ell]/C_\ell \times C_N$. Define

$$\psi_\ell := \varphi_\ell \circ \omega_\ell : X_0(\ell \cdot N) \to X_0(N).$$

We are in the situation described above (with $K = L$) and can define the Hecke correspondence

$$T_\ell : J_0(N) \to J_0(N),$$

by

$$T_\ell := \varphi_{\ell *} \circ \psi_\ell^*.$$

The Hecke ring of $X_0(N)$ is $\mathcal{T}_N =< T_\ell$ with ℓ prime to $N >$, the ring generated by the endomorphisms T_ℓ. It is a commutative ring, which is very near to End$(J_0(N)$ as in [46]. It acts on the vector space of holomorphic differentials of $X_0(N)$ which can be identified with cusp forms of level N (and trivial nebentype). By classical theory one knows that $\mathcal{T}_N$ is endowed with an hermitian structure due to the Peterson scalar product, and so the eigenvalues of the operators T_ℓ are totally real numbers.

Remark 6. *Assume that A is a simple factor of $J_0(N)$. Then* $\mathrm{End}^0(A)$ *is a totally real field of degree* $\dim(A)$.

This means that factors of $J_0(N)$ have very special and large endomorphism rings. As consequence there is a splitting of Galois representations of $G_{\mathbb{Q}}$ into a sum of two-dimensional representations with real eigenvalues, and these "modular representations" play a most important role in number theory, e.g. for the proof of Fermat's Last Theorem. The narrow relation to arithmetic is reflected by the **Eichler-Shimura** congruence

$$T_\ell = \mathrm{Frob}_\ell + \ell/\mathrm{Frob}_\ell,$$

where Frob is the Frobenius endomorphism on $\mathcal{J}_0(N)\bigotimes\mathbb{F}_\ell$. In particular, Frob_ℓ satisfies the **Eichler-Shimura** equation

$$X^2 - T_\ell \cdot X + \ell = 0.$$

A curve $\mathcal{X}$ whose Jacobian is a factor of $\mathcal{J}_0(N)$ is called **modular of level** N.

Using cusps forms it is possible to determine its period matrix, decide whether it is hyperelliptic, and then compute its Weierstrass equation (see [65], [64]). The fact that Frob satisfies the quadratic Eichler-Shimura equation over a totally real number field can be used for point counting for curves of genus ≥ 2 as in [27].

8.3. Correspondences via Monodromy Groups.

We assume that we have a cover morphism

$$f : \mathcal{X} \to \mathbb{P}^1$$

defined over K of degree n, satisfying some fixed ramification conditions and having a fixed monodromy group $G_f := \mathrm{Mon}\ (f)$. We have morphisms

$$\tilde{f} : \tilde{\mathcal{H}} \xrightarrow{h} \mathcal{X} \xrightarrow{f} \mathbb{P}^1$$

with $\tilde{f}$ a Galois cover of f with Galois group G_f. For simplicity, we assume that the field of constants of $\tilde{\mathcal{H}}$ is K. This setting is motivated by the theory of *Hurwitz spaces* and it is hoped that one can exploit their rich and, over $\mathbb{C}$, well understood theory ([23] and [24]).

Next we choose subgroups $H_1 \subset G_f$ fixing $\mathcal{X}$ and H_2 containing H_1. Let $\mathcal{H}$ be the curve fixed by H_1 and $\mathcal{D}$ the fixed curve under H_2. So $\mathcal{H}$ covers both $\mathcal{X}$ and $\mathcal{D}$. Let

$$h : \mathcal{H} \to \mathcal{X}$$

and

$$g : \mathcal{H} \to \mathcal{D}$$

with morphisms induced by the Galois action. Hence the degree of h is equal to $\deg(h) = \frac{|G_f|}{|H_1|\cdot n}$ and the degree of g is equal to $\deg(g) = \frac{|H_2|}{|H_1|}$. We get a correspondence

$$\eta : \mathcal{J}_{\mathcal{X}} \to \mathcal{J}_{\mathcal{D}}$$

by applying $g_* \circ h^*$ to the Picard groups. In general, η will be neither injective nor surjective.

Lemma 16. *In the above situation, assume in addition that $\mathcal{J}_{\mathcal{D}}$ is a simple abelian variety of dimension equal to the genus of $\mathcal{X}$, that there is a prime divisor $\mathfrak{p}_\infty$ of $\mathcal{X}$ which is totally ramified under h, i.e. there is exactly one prime divisor $\mathfrak{P}_\infty$ of $\mathcal{H}$ with norm $\mathfrak{p}$, and that there is no non-constant morphism of degree $\leq \deg(h)$ from $\mathcal{D}$ to the projective line. Then η is an isogeny.*

PROOF. Since $J_{\mathcal{D}}$ is simple, it is enough to show that η is not the zero map. Let $\mathfrak{p}'_\infty$ be the norm of $\mathfrak{P}_\infty$ under g. Without loss of generality we can assume that K is algebraically closed.

So we find a prime divisor $\mathfrak{P}$ of $\mathcal{H}$ which is different from all prime divisors in $g^{-1}(\mathfrak{p}'\infty)$.

Let c be the class of $\mathfrak{p} - \mathfrak{p}_\infty$, where $\mathfrak{p} = h_*(\mathfrak{P})$. Then $\eta(c)$ is the class of the divisor

$$D_{\mathfrak{p}} := \sum_{\mathfrak{P} \in h^{-1}(\mathfrak{p})} g_*(\mathfrak{P}) - \deg(h) \cdot g_*(\mathfrak{P}_\infty).$$

Note that $D_{\mathfrak{p}} \neq 0$ (as divisor). If the class of $D_{\mathfrak{p}}$ would be trivial, then there would be a non-constant function on $\mathcal{D}$ with pole order $\leq \deg(h)$ and hence a non-constant map of $\mathcal{D}$ to the projective line of degree $\leq \deg(h)$, which is a contradiction. □

We shall see in Section 11 that we can realize the situation (over K_s) of the lemma for hyperelliptic curves of genus 3 with non-decomposable Jacobian, f a polynomial of degree 6, $G_f = S_4$, H_1 a subgroup of order 2 and H_2 a subgroup of order 6. This leads to isogenies of degree 8 discussed by B. Smith.

It is an open and challenging problem to find other interesting correspondences of low degree between Jacobian varieties induced by correspondences between curves and (possibly) attached to Hurwitz spaces.

9. Elliptic curve cryptography

In Section 4.4.1 we described a way of determining m-torsion points for any given m. Finite subgroups G of E correspond to isogenies $E \to E/G$. Velu's formula describes such isogeny map explicitly.

PROPOSITION 7 (Velu's formula). *Let E be an elliptic curve, defined over a field k, with equation*

$$E : y^2 = x^3 + ax + b$$

and $G \subset E(\bar{k})$ be a finite subgroup. The separable isogeny $\phi : E \to E/G$, of kernel G, can be written as follows for any $P(x, y)$

$$\phi(P) = \left(x + \sum_{Q \in G \setminus \{\mathcal{O}\}} x(P+Q) - x(Q),\ y + \sum_{Q \in G \setminus \{\mathcal{O}\}} y(P+Q) - y(Q) \right) \tag{15}$$

and the curve E/G has equation $y^2 = x^3 + a'x + b'$, where

$$a' = a - 5 \sum_{Q \in G \setminus \{\mathcal{O}\}} (3x(Q)^2 + a),$$

$$b' = b - 7 \sum_{Q \in G \setminus \{\mathcal{O}\}} (5x(Q)^3 + 3ax(Q) + b).$$

Thus, knowing a finite subgroup G of E we can explicitly construct the corresponding isogeny $E \to E' := E/G$. What if we are given two elliptic curves E and E', how do we check if they are isogenous?

In order to explain the isogeny based cryptography we need to understand the endomorphism rings of elliptic curves and the difference between ordinary and supersingular elliptic curves.

9.1. Endomorphism ring of E.

The definitions from the Abelian varieties apply here. In the case of elliptic curves we have the following:

Definition 35. If char $(K) = 0$, then we say that an elliptic curve E/K has complex multiplication or (historically) that E is singular, if $\mathrm{End}(E) \neq \mathbb{Z}$. If char $(K) > 0$, we say that E/K is **supersingular** if $\mathrm{End}(E)$ is an order in a rational quaternion algebra, otherwise we say that E is **ordinary**.

9.2. Elliptic curves over finite fields.

Let E be an elliptic curve over $\mathbb{F}_q$, where $q = p^n$ for some prime p and an integer n. Its characteristic polynomial of the Frobenius π is

$$\chi_{E,q}(T) = T^2 - \mathrm{tr}(\pi)\,T + q = (T - \lambda_1)(T - \lambda_1).$$

where the eigenvalues λ_1, λ_2 are in some quadratic extension of $\mathbb{Q}$. Let $K_E = \mathbb{Q}(\lambda_1)$ and $\mathcal{O}_{K_E}$ its ring of integers. An elliptic curve E defined over $\mathbb{F}_q$ is called **ordinary** if the separable degree of $[p]$ is p.

The following results are mostly due to M. Deuring and mainly contained in the beautiful paper [14].

THEOREM 36 (Deuring). *Let E be an elliptic curve defined over a field K. The following hold:*

i) If $\mathrm{char(K)} = 0$*, then E is ordinary and*

- $\mathrm{End}_{\overline{K}}(\mathcal{E}) = \mathbb{Z}$ *(generic case) or* $\mathrm{End}_{\overline{K}}(\mathcal{E})$ *is an order* $O_{\mathcal{E}} \subset \mathbb{Q}(\sqrt{-d_{\mathcal{E}}})$, $d_{\mathcal{E}} > 0$ *(CM-case).*
- *Take $\mathcal{E}$ with CM with order $O_{\mathcal{E}}$. Let $\mathcal{S}_{\mathcal{E}}$ be the set of $\mathbb{C}$-isomorphy classes of elliptic curves with endomorphism ring $O_{\mathcal{E}}$. Then* $\mathrm{Pic}(O_{\mathcal{E}})$ *acts in a natural and simply transitive way on $\mathcal{S}_{\mathcal{E}}$, hence $\mathcal{S}_{\mathcal{E}}$ is a principally homogeneous space with translation group* $\mathrm{Pic}(O_{\mathcal{E}})$*: For* $c \in \mathrm{Pic}(O_{\mathcal{E}})$, $\mathfrak{A} \in c$ *and* $\mathbb{C}/O_{\mathcal{E}} = \mathcal{E}_0$ *we get* $c \cdot [\mathcal{E}_0]$ *is the class of* $\mathbb{C}/\mathfrak{A}$.

*ii) (**Deuring's Lifting Theorem**) Let $\mathcal{E}$ be an elliptic curve over $\mathbb{F}_q$ which is ordinary over $\overline{\mathbb{F}_q}$. Then there is, up to $\mathbb{C}$-isomorphisms, exactly one elliptic curve $\mathcal{E}$ with CM over a number field K such that*

- *there is a prime $\mathfrak{p}$ of K with $\mathcal{E}_{\mathfrak{p}} \cong \mathcal{E}$, and*
- $\mathrm{End}(\mathcal{E}) = \mathrm{End}(\mathcal{E})_{\mathfrak{p}} = O_{\mathcal{E}}$*, with $O_{\mathcal{E}}$ an order in an imaginary quadratic field.*

iii) If $\mathcal{E}$ is supersingular, then

- *Up to twists, all supersingular elliptic curves in characteristic p are defined over $\mathbb{F}_{p^2}$, i.e. their j-invariant lies in $\mathbb{F}_{p^2}$.*
- $|\mathcal{E}(\mathbb{F}_{p^2}| = (p \pm 1)^2$*, and the sign depends on the twist class of $\mathcal{E}$.*
- $\mathrm{End}_{\overline{\mathbb{F}_p}}(\mathcal{E})$ *is a maximal order in the quaternion algebra $\mathbb{Q}_p$, which is unramified outside of ∞ and p.*

We remark that the endomorphism rings of elliptic curves over finite fields $\mathbb{F}_q$ is never equal to $\mathbb{Z}$ since there is the Frobenius endomorphism $\phi_{\mathbb{F}_q,\mathcal{E}}$ induced by the Frobenius automorphism of $\mathbb{F}_q$ which has degree q. We give a first application of the lifting theorem.

COROLLARY 9 (Hasse). *Let $\mathcal{E}$ be an ordinary elliptic curve over $\mathbb{F}_q$. Then the Frobenius endomorphism $\phi_{\mathbb{F}_q,\mathcal{E}}$ is an integer in an imaginary quadratic fields with norm q, and hence has a minimal polynomial*

$$\chi_{\mathcal{E},q}(T) = T^2 - \mathrm{tr}(\phi_{\mathbb{F}_q,\mathcal{E}}) \cdot T + q$$

with

$$|(\mathrm{tr}(\phi_{\mathbb{F}_q,\mathcal{E}})^2 - 4q| < 0.$$

Recall that the number of $\mathbb{F}_q$-rational points of $\mathcal{E}$ is

$$|\mathcal{E}(\mathbb{F}_q)| =: n_{\mathbb{F}_q,\mathcal{E}} = \chi_{\mathcal{E},q}(1).$$

Corollary 10. $|n_{\mathbb{F}_q,\mathcal{E}} - q - 1| < 2\sqrt{q}$.

Using the result iii) in Theorem 36 and the observation that the eigenvalues of $\phi_{\mathbb{F}_{q^d},\mathcal{E}}$ are the d-th power of the eigenvalues of $\phi_{\mathbb{F}_q,\mathcal{E}}$ we get that

$$|n_{\mathbb{F}_q,\mathcal{E}} - q - 1| \le 2\sqrt{q}$$

for all elliptic curves of $\mathbb{F}_q$. This is the *Hasse bound* for elliptic curves, a special case of the Weil bound for points on curves over finite fields; see Eq. 10.

9.3. Point Counting. Corollary 10 is the key fact for a polynomial time algorithm for computing the order of $\mathcal{E}(\mathbb{F}_q)$ for elliptic curves $\mathcal{E}$ defined over the field $\mathbb{F}_q$, which is called **Schoof's Algorithm** and we briefly explain below.

The idea is to compute $\chi_{\mathcal{E},q}(T) \mod n$ for small numbers n by computing the action of $\phi_{\mathbb{F}_q,\mathcal{E}}$ on $\mathcal{E}[n]$ (take for instance $n = \ell$ as small prime number or $n = 2^k$ with k small) and then to use CRT and the Hasse bound for trace of $\phi_{\mathbb{F}_q,\mathcal{E}}$ to determine $\chi_{\mathcal{E},q}(T)$. To do this use the classical n-division polynomials Ψ_n and then use *CRT*. The disadvantage is that $\deg(\Psi_n) \sim n^2/2$ and therefore the Schoof algorithm is too slow.

The way out of this problem is to use étale isogenies with cyclic kernel of order n and the fact (see Section 5) that we can interpret these isogenies with the help of points on an explicitly known curve, namely the modular curve $X_0(n)$. An explicit equation for an affine model of $X_0(N)$ is given by the classical modular polynomial $\phi(j, j_N)$. It allows an effective computation of isogenies (as functions including the determination of the image curve) at least if n is of moderate size).

Theorem 37 (Vélu, Couveignes, Lercier, Elkies, Kohel, and many other contributors:). *The cost for the computation of an isogeny of degree ℓ of an elliptic curve $\mathcal{E}$ over $\mathbb{F}_q$ is*

$$\mathcal{O}(\ell^2 + \ell \log(\ell) \log(q)).$$

The **Idea of Atkin-Elkies** is: Use *étale isogenies* of small degree of E instead of points, and use the modular polynomial ϕ_n of degree $\sim n$. The resulting *Schoof-Atkin-Elkies algorithm* is very fast, in particular if one assumes as "standard conjecture" the generalized Riemann hypothesis (GRH).

Corollary 11 (SAE). *$|E(\mathbb{F}_q)|$ can be computed (probabilistically, with GRH) with complexity $\mathcal{O}((\log q)^4)$. Therefore we can construct, for primes p sufficiently large, (many) elliptic curves with $|\mathcal{E}(\mathbb{F})| = k \cdot \ell$ with k small (e.g. $k = 1$ if we want) and ℓ a prime so large that (using classical computers and according to our best knowledge) the security level of the discrete logarithm in $\mathcal{E}(\mathbb{F}_p)$ is matching AES 128 (or larger).*

9.4. Looking for Post-Quantum Security. As we have seen in Subsection 9.3 we can construct elliptic curves over prime fields such that the resulting DL-systems are secure under the known attacks. But the situation changes totally if we allow algorithms based on quantum computers. One of the first algorithms of this kind is due to **Shor** and compute the DL in any group in polynomial time. Hence it seems to be wise to look for totally different methods for key exchange.

We shall discuss now how we can use isogenies of elliptic curves (and maybe, of curves of larger genus with convenient endomorphism rings) to find key exchange schemes staying in the frame of Diffie-Hellman type protocols as described in 6.

9.4.1. *The System of Couveignes-Stolbunov.* We sketch in the following work of Stolbunov [61] and Couveignes [9]. We use the results of Theorem 36 for an ordinary elliptic curve $\mathcal{E}_0$ over $\mathbb{F}_q$ with ring of endomorphism $\mathrm{End}(\mathcal{E}_0) = O$, which is an order in a quadratic imaginary field.

In analogy to the notation in Theorem 36 define $\mathcal{S}_{E_0}$ as set of isomorphism classes of elliptic curves over $\overline{\mathbb{F}_q}$ with ring of endomorphisms O. Then $\mathcal{S}_{E_0}$ is a $\mathrm{Pic}(O)$-set. Hence, we can use it for *Key Exchange protocols:*

The partner P choses $c \in \mathrm{Pic}(O)$ and publishes the j-invariant of $c \cdot E_0$.

The exchange is not as fast as DL-systems since we cannot use a *double-and add*-algorithm but it is feasible since one finds enough isogenies that are composites of isogenies of small degree (smoothness); for an example see [61]. The **security** depends on the hardness of the following problem:

PROBLEM 1. *Find an isogeny between two given isogenous elliptic curves.*

The following gives an idea of the running time for the solution to this problem.

PROPOSITION 8 (Kohel, Galbraith, Hess, Smart et al.). *The expected number of* ***bit****-operations for the computation of an isogeny between ordinary elliptic curves over* $\mathbb{F}_q$ *with endomorphism ring* O_{K_E} *is*

$$\mathcal{O}(q^{1/4+o(1)} \log^2(q) \log\log(q)).$$

But recall: We are in the situation where an abelian group is acting on a set, and so there is a subexponential algorithm to solve the hidden-shift problem. This means that we can only expect *subexponential* security for the key exchange scheme; see results of Childs, Jao, Soukharev in [6]. Comparing this with the situation we have nowadays with respect to the widely tolerated RSA-system this may be not so disastrous.

9.4.2. *The Key Exchange System of De Feo.* The suggestion is now to use supersingular elliptic curves over $\mathbb{F}_{p^2}$ and their properties also stated in Theorem 36. Take

$$p = r^a \cdot s^b \cdot f - 1$$

with $p \equiv 1 \mod 4$. Then

$$E_0 : Y^Z = X^3 + XZ^2$$

is a supersingular elliptic curve over $\mathbb{F}_{p^2}$. We describe the key exchange scheme invented and implemented by De Feo, Jao and Plût [12] in the frame we have introduced in Section 6.

As categories $\mathcal{C}_i$; $(i = 1, 2)$ are given by the **objects** are isomorphism classes of supersingular curves E over $\mathbb{F}_{p^2}$ isogenous to $\mathcal{E}_0$ and hence with

$$|E(\mathbb{F}_{p^2})| = (r^a \cdot s^b \cdot f)^2.$$

Recall that:

i) The **morphisms in** $\mathcal{C}_1$ are isogenies φ with $|\ker(\varphi)|$ dividing r^a.
ii) The **morphisms in** $\mathcal{C}_2$ are isogenies ψ with $|\ker(\psi)|$ dividing s^b.

For these categories pushouts exist. For additional information choose P_1, P_2 of order r^a and Q_1, Q_2 of order s^b in $\mathcal{E}_0(\mathbb{F}_{p^2})$.
Key Exchange:

- The Partner P_1 chooses $n_1, n_2 \in \mathbb{Z}/r^a$ and the isogeny
$$\eta : E_0 \to E_0/\langle n_1 P_1 + n_2 P_2 \rangle =: E_1.$$
- P_2 chooses $m_1, m_2 \in \mathbb{Z}/s^b$ and computes the isogeny
$$\psi : E_0/\langle m_1 Q_1 + m_2 Q_2 \rangle =: E_2.$$
- P_2 sends $(\mathcal{E}_2, \psi(P_1), \psi(P_2))$.
- P_1 can compute the common secret, the pushout of η and ψ as
$$\mathcal{E}_3 := E_2/\langle n_1 \psi(P_1) + n_2 \psi(P_2) \rangle.$$

Again **security** depends on the hardness to compute an isogeny of two elliptic curves, but now the two elliptic curves are supersingular.

State of the art: The best known algorithms have exponential complexity $p^{1/4}$ (bit-computer) resp. $p^{1/6}$ (quantum computer), and so one can hope that a prime p with 768 bit yields AES128 security level. So we have, compared with other post-quantum suggestions for key exchange schemes, a very small key size.

In contrast to the ordinary case the groups around like the class groups of left ideals in maximal orders **are not abelian**, and so the hidden shift problem is not solved till now in subexponential time.

9.5. Isogeny graphs. In cryptographic applications of isogenies of elliptic curves and important role play the isogeny graphs, which we will briefly describe here.

Definition 38. An **isogeny graph** is a graph where nodes are j-invariants of isogenous curves and edges the isogenies between the curves.

One of the first questions is to check whether there are any differences between isogeny graphs of ordinary curves and isogeny graphs of supersingular curves.

9.5.1. *Supersingular isogeny graphs.* An elliptic curve supersingular $E/\mathbb{F}_q$, for $q = p^n$, is supersingular if and only if $E[p] = \{\infty\}$. All supersingular curves can be defined over $\mathbb{F}_{p^2}$. Set S_{p^2} be the set of supersingular j-invariants. Then we have the following:

Theorem 39. *The cardinality of S_{p^2} is given by*
$$\# S_{p^2} = \left\lfloor \frac{p}{12} \right\rfloor + b, \quad \textit{where } \; b \in \{0, 1, 2\}$$

From theorem 36 we know that all supersingular curves over $\mathbb{F}_{p^2}$ are in the same isogeny class and we get $(l+1)$ directed regular graph $X(S_{p^2}, l)$. Supersingular isogeny graphs are Ramanujan graphs. The following is [12, Prop. 2.1].

PROPOSITION 9. *Let G be a regular graph of degree k on h vertices. Suppose that the eigenvalue λ of any non-constant eigenvector satisfies the bound $|\lambda| \leq c$, for some $c \leq k$. Let S be any subset of the vertices of G and x any vertex on G. Then a random walk of length at least $\frac{\log 2h/|S|^{1/2}}{\log k/c}$ starting from x will land in S with probability at least $\frac{|S|}{2h} = \frac{|S|}{2G}$.*

10. Genus 2 curves and cryptography

We assume some familiarity with the computational aspects of genus 2 curves. Let $\mathcal{X}$ be a genus 2 curve defined over a field k. We assume that char $k \neq 2$. Then $\mathcal{X}$ has Weierstrass equation

$$y^2 = f(x) = a_6 x^6 + \dots a_1 x + a_0, \tag{16}$$

for discriminant $\Delta_f \neq 0$. We denote Igusa arithmetic invariants by J_2, J_4, J_6, J_{10}, see [45] for explicit formulas.

The moduli space $\mathcal{M}_2$ of genus 2 curves, via the Torelli morphism, can be identified with the moduli space of the principally polarized abelian surfaces A_2 which are not products of elliptic curves. Its compactification $A_2^\star$ is the weighted projective space $\mathbb{P}^3_{(2,4,6,10)}(\bar{\mathbb{Q}})$ via the Igusa invariants J_2, J_4, J_6, J_{10}. Hence,

$$A_2 \cong \mathbb{P}^3_{(2,4,6,10)}(\bar{\mathbb{Q}}) \setminus \{J_{10} = 0\}.$$

In [54], for any number field K, a height on $\mathbb{P}^3_{(2,4,6,10)}(K)$ is introduced and in [2] a database of all genus 2 curves with such small height is constructed. Once a point $\mathfrak{p} \in \mathbb{P}^3_{(2,4,6,10)}(K)$ is given, one can determine the equation of the genus two curve defined over a minimal field of definition via the algorithm in [45].

10.1. Decomposable Jacobians.

Let $\psi : \mathcal{X} \to E_1$ be a maximal degree n covering which does not factor through an isogeny. Then, there is another elliptic curve $E_2 := \operatorname{Jac} \mathcal{X}/E_1$ such that $\operatorname{Jac} \mathcal{X}$ is isogenous via a degree n^2 isogeny to the product $E_1 \times E_2$. We say that $\operatorname{Jac} \mathcal{X}$ is (n, n)-decomposable. Such curves were studied in [23]. The locus of curves with (n, n)-decomposable Jacobians is a 2-dimensional irreducible locus in $\mathcal{M}_2$. Such loci for small $n = 2, 3, 5$ are computed in [57], [52], and [44].

10.2. Endomorphism ring of an abelian surface.

Jacobians with non-trivial endomorphisms are parametrized by proper subvarieties of $A_2^\star$ as follows:

i) Points on the Humbert space $\mathcal{H}_{n^2}$, where $\mathcal{H}_1$ denotes the locus of abelian surfaces which are the product of two elliptic curves.

ii) For each quaternion ring R there are $S_{R,1}, \dots, S_{R,k}$ Shimura curves contained in $A_2^\star$ that parametrize genus 2 curves whose Jacobians admit an optimal action of R.

iii) Curves whose jacobians admit complex multiplication correspond to isolated points in the moduli space.

Thus we have the following:

PROPOSITION 10. $\operatorname{Jac}(\mathcal{X})$ *is a geometrically simple Abelian variety if and only if it is not (n, n)-decomposable for some n.*

The endomorphism rings of Abelian surfaces can be determined by the Albert's classification and results in [50]. We summarize in the following:

Proposition 11. *The endomorphism ring* $\mathrm{End}^0_{\overline{\mathbb{Q}}}(\mathrm{Jac}\,\mathcal{X})$ *of an abelian surface is either* $\mathbb{Q}$*, a real quadratic field, a CM field of degree 4, a non-split quaternion algebra over* $\mathbb{Q}$*,* $F_1 \oplus F_2$ *where each* F_i *is either* $\mathbb{Q}$ *or an imaginary quadratic field, the Mumford-Tate group where* F *is either* $\mathbb{Q}$ *or an imaginary quadratic field.*

Remark 7. *Most genus 2 curves with extra involutions have endomorphism ring larger than* $\mathbb{Z}$*. Let* $\mathcal{X}$ *be a genus 2 curve defined over* $\mathbb{Q}$*. If* $\mathrm{Aut}(\mathcal{X}) \cong V_4$*, then* $\mathcal{X}$ *is isomorphic to a curve* $\mathcal{X}'$ *with equation*

$$y^2 = f(x) = x^6 - ax^4 + bx^2 - 1.$$

Moreover, if $a, b \in \mathbb{Q}$ *then* $\mathcal{X}'$ *has minimal naive height as shown in* [1]*. We denote* $u = a^3 + b^3$ *and* $v = ab$*. The discriminant* $\Delta_f = -2^6 \cdot \left(27 - 18v + 4u - u^2\right)^2$*, is not a complete square in* $\mathbb{Q}$ *for any values of* $a, b \in \mathbb{Q}$*. In this case* $\mathrm{Gal}_{\mathbb{Q}}(f)$ *has order 24. There is a twist of this curve, namely* $y^2 = f(x) = x^6 + a'x^4 + b'x^2 + 1$*, in which case* Δ_f *is a complete square in* $\mathbb{Q}$ *and* $\mathrm{Gal}_{\mathbb{Q}}(f)$ *has order 48. In both cases, from theorem 30 we have that* $\mathrm{End}_{\overline{\mathbb{Q}}}(\mathrm{Jac}\,\mathcal{X}') \neq \mathbb{Z}$*.*

Next we turn our attention to determining the endomorphism ring of abelian surfaces. Let us first recall a few facts on characteristic polynomials of Frobenius for abelian surfaces. The Weil q-polynomial arising in genus 2 have the form

$$f(T) = T^4 - aT^3 + (b + 2q)T^2 - aqT + q^2, \tag{17}$$

for $a, b \in \mathbb{Z}$ satisfying the inequalities

$$2|a|\sqrt{q} - 4q \leq b \leq \frac{1}{4}a^2 \leq 4q.$$

We follow the terminology from [3]. Let $\mathcal{X}$ be a curve of genus 2 over $\mathbb{F}_q$ and $J = \mathrm{Jac}\,\mathcal{X}$. Let f be the Weil polynomial of J as in eq. (17). We have that $\#\mathcal{X}(\mathbb{F}_q) = q + 1 - a$, $\#J(\mathbb{F}_q) = f(1)$ and it lies in the genus-2 Hasse interval

$$\mathcal{H}_q^{(2)} = \left[(\sqrt{q} - 1)^4, (\sqrt{q} + 1)^4\right]$$

In [3] are constructed decomposable $(3,3)$-jacobians with a given number of rational points by glueing two elliptic curves together.

Next we describe some of the results obtained in [39] for $\mathrm{End}_K(\mathcal{A})$ in terms of the characteristic polynomial of the Frobenius. We let K be a number field and M_K the set of norms of K. Let $\mathcal{A}$ be an abelian surface defined over K and f_v the characteristic Frobenius for every norm $v \in M_K$.

Lemma 17. *Let* v *be a place of characteristic* p *such that* $\mathcal{A}$ *has good reduction. Then* $\mathcal{A}_v$ *is ordinary if and only if the characteristic polynomial of the Frobenius*

$$f_v(x) = x^4 + ax^3 + bx^2 + apx + p^2,$$

satisfies $b \not\equiv 0 \mod p$*.*

Then from [39, Lemma 4.3] we have the following.

Lemma 18. *Let* $\mathcal{A}$ *be an absolutely simple abelian surface. The endomorphism algebra* $\mathrm{End}^0_{\overline{K}}(\mathcal{A})$ *is non-commutative (thus a division quaternion algebra) if and only if for every* $v \in M_K$*, the polynomial* $f_v(x^{12})$ *is a square in* $\mathbb{Z}[x]$*.*

The following gives a condition for geometrically reducible abelian surfaces.

Proposition 12. *If* $\mathcal{A}/K$ *is geometrically reducible then for all* $v \in M_k$ *for which* $\mathcal{A}$ *has good reduction the polynomial* $f_v(x^{12})$ *is reducible in* $\mathbb{Z}[x]$*.*

Proposition 13. *If $\mathcal{X}$ is a smooth, irreducible genus 2 curve with affine equation $y^2 = f(x)$ such that $f(x) \in K[x]$ is an irreducible polynomial of degree 5 then* $\operatorname{Jac} \mathcal{X}$ *is absolutely irreducible.*

In [39] is given a detailed account of all the cases and an algorithm how to compute $\operatorname{End}_K \mathcal{A}$.

10.3. Isogenies. Let us now consider the problem of computing isogenies between two Abelian surfaces. As above, we let $\mathcal{X}$ be a curves of genus 2 defined over a perfect field k such that char $k \neq 2$ and $\mathcal{J} = \operatorname{Jac}(\mathcal{X})$ its Jacobian. Fix a prime $\ell \geq 3$ and let S be a maximal ℓ-Weil isotropic subgroup of $\mathcal{J}[n]$. From Theorem **??** we have $S \cong (\mathbb{Z}/\ell\mathbb{Z})^2$. Let $\mathcal{J}' := \mathcal{J}/S$ be the quotient variety and $\mathcal{Y}$ a genus 2 curve such that $\operatorname{Jac}(\mathcal{Y}) = \mathcal{J}'$. Hence, the classical isogeny problem becomes to compute $\mathcal{Y}$ when given $\mathcal{X}$ and S.

If $\ell = 2$ this problem is done with the Richelot construction. Over finite fields this is done by Lubicz and Robert in [41] using theta-functions.

In general, if $\phi : \mathcal{J}(\mathcal{X}) \to \mathcal{J}(\mathcal{Y})$ is the isogeny and $\Theta_{\mathcal{X}}$, Θ_Y the corresponding theta divisors, then $\phi(\Theta_{\mathcal{X}})$ is in $|\ell\Theta_{\mathcal{Y}}|$. Thus, the image of $\phi(\Theta_{\mathcal{X}})$ in the Kummer surface $\mathcal{K}_{\mathcal{Y}} = \mathcal{J}(\mathcal{Y})/\langle \pm 1 \rangle$ is a degree 2ℓ genus zero curve in $\mathbb{P}^3$ of arithmetic genus $\frac{1}{2}(\ell^2 - 1)$. This curve can be computed without knowing ϕ; see [19] for details.

For $\mathcal{X}$ given as in Eq. (16), we have the divisor at infinity

$$D_\infty := (1 : \sqrt{f(x)} : 0) + (1 : -\sqrt{f(x)} : 0)$$

The Weierstrass points of $\mathcal{X}$ are the projective roots of $f(x)$, namely $w_i := (x_i, z_i)$, for $i = 1, \dots, 6$ and the Weierstrass divisor $W_{\mathcal{X}}$ is

$$W_{\mathcal{X}} := \sum_{i=1}^{6} (x_i, 0, z_i).$$

A canonical divisor on $\mathcal{X}$ is

$$\mathcal{K}_{\mathcal{X}} = W_{\mathcal{X}} - 2D_\infty.$$

Let $D \in \operatorname{Jac} \mathcal{X}$, be a divisor expressed as $D = P + Q - D_\infty$. The effective divisor $P + Q$ is determined by an ideal of the form $(a(x), b(x)$ such that $a(x) = y - b(x))$, where $b(x)$ is a cubic and $a(x)$ a monic polynomial of degree $d \leq 2$.

We can define the ℓ-tuple embedding $\rho_{2\ell} : \mathbb{P}^2 \to \mathbb{P}^{2\ell}$ by

$$(x, y, z) \to (z^{2\ell}, \dots, x^i z^{2\ell - i}, x^{2\ell})$$

and denote the image of this map by $\mathcal{R}_{2\ell}$. It is a rational normal curve of degree 2ℓ in $\mathbb{P}^{2\ell}$. Hence, any $2\ell+1$ distinct points on $\mathcal{R}_{2\ell}$ are linearly independent. Therefore, the images under $\rho_{2\ell}$ of the Weierstrass points of $\mathcal{X}$ are linearly independent for $\ell \geq 3$. Thus, the subspace

$$W := \langle \rho_{2\ell}(W_{\mathcal{X}}) \rangle \subset \mathbb{P}^{2\ell}$$

is 5-dimensional. For any pair of points P, Q in $\mathcal{X}$, the secant line $\mathcal{L}_{P,Q}$ is defined to be the line in $\mathbb{P}^{2\ell}$ intersecting $\mathcal{R}_{2\ell}$ in $\rho_{2\ell}(P) + \rho_{2\ell}(Q)$. In other words,

$$\mathcal{L}_{P,Q} = \begin{cases} \langle \rho_{2\ell}(P), \rho_{2\ell}(Q) \rangle & \text{if } P \notin \{Q, \tau(Q)\} \\ T_{\rho_{2\ell}(P)}(\mathcal{R}_{2\ell}) & \text{otherwise} . \end{cases}$$

The following is proved in [19].

Theorem 40 (Dolgachev-Lehavi). *There exists a hyperplane $H \subset \mathbb{P}^{2\ell}$ such that:*

1) H contains W and

2) the intersection of H with the secants $\mathcal{L}_e$ for each nonzero $e \in S$ are contained in a subspace N of codimension 3 in H.

The image of the Weierstrass divisor under the map $\mathbb{P}^{2\ell} \to \mathbb{P}^3$ with centre N lies on a conic $\mathcal{C}$, and the double cover of $\mathcal{C}$ ramified over this divisor is a stable curve $\mathcal{Y}$ of genus 2 such that $\operatorname{Jac} \mathcal{Y} \cong \operatorname{Jac} \mathcal{X}/S$.

This was used by Smith [59] to devise an algorithm for determining $\mathcal{Y}$ and determining ϕ. The algorithm works well for $\ell = 3$.

11. Genus 3 curves and cryptography

We continue the discussion of generic curves from section 3. For $g = 3$ a generic cover has degree three and 9 branch points. The signature is $\sigma = (\sigma_1, \dots, \sigma_9)$ where $\sigma_i \in S_3$ is an transposition for $i = 1, \dots, 8$ and σ_9 is the 3-cycle. For a generic curve of genus $g = 3$ defined over a field k we have the following:

Lemma 19 ([56]). *Let $\mathcal{X}$ be a generic curve of genus 3 defined over a field k of characteristic $\operatorname{char} k \neq 2, 3$. Then, there is a degree 3 covering $\psi : \mathcal{X} \to \mathbb{P}^1$ of full moduli dimension. Moreover, $\mathcal{X}$ is isomorphic to a curve with affine equation*

$$Y^3(X + a) + Y^2(bX + c) + Y(dX^2 + eX) + X^3 + fX^2 + X = 0$$

for $a, b, c, d, e, f \in \bar{k}$ such that $\Delta \neq 0$, where Δ is the discriminant of the quartic.

All the degenerations of the cover $\pi : \mathcal{X} \to \mathbb{P}^1$, including their monodromy groups and the moduli dimension are given in [56, Table 1]. Such curves are non-hyperelliptic. Their isomorphism classes are determined by Diximier invariants of ternary quartics as defined in [18]. The discriminant of curve with respect to Y is given by

$$\Delta(X) = -X(27X^7 + A_6X^6 + A_5X^5 + A_4X^4 + A_3X^3 + A_2X^2 + A_1X + 4c^3)$$

where $A_1, \dots A_6 \in k[a, b, c, d, e, f]$. The branch points of the cover $\psi : \mathcal{X} \to \mathbb{P}^1$ coalesce when $\Delta(X)$ has multiple roots. Thus, its discriminant Δ in X is $\Delta = 0$. There are four factors of the discriminant

$$\Delta = \Delta_1 \cdot \Delta_2 \cdot \Delta_3 \cdot \Delta_4 = 0,$$

each corresponding to one of the degenerate cases, which are obtained when the branch points of ψ coalesce,

$$(3, 3, 2, 2, 2, 2, 2, 2), \quad (3, 3, 3, 2, 2, 2, 2), \quad (3, 3, 3, 3, 2, 2), \quad (3, 3, 3, 3, 3).$$

The information for the corresponding Hurwitz spaces is given in [56, Table 1].

The generic curve has no automorphisms. In [43] among other papers, parametric equations are determined for all non-hyperelliptic genus 3 curves with non-trivial automorphism group.

11.1. Hyperelliptic Curves. Let $\mathcal{X}$ be a hyperelliptic curve of genus 3 over the field k, such that char(k) $\neq 2$. As shown in **??**, $\mathcal{X}$ is hyperelliptic if and only if there is a degree 2 cover map $\pi : \mathcal{X} \to \mathbb{P}^1$, which is uniquely determined up to automorphisms of $\mathbb{P}^1$. This cover is Galois, and the non-trivial automorphism on $\mathcal{X}$ fixing $\mathbb{P}^1$ is the the hyperbolic involution ω. Hence, we can give $\mathcal{X}$ by a plane projective Weierstrass equation, which has an affine part

$$\mathcal{X}_a : y^2 = f(x)$$

invariant under ω and

$$\mathbb{P}^1 \setminus \pi(\mathcal{X}_a) =: \{P_\infty\} \subset \mathbb{P}^1(k).$$

Moreover, $\deg(f) = 7$ if the fiber $\pi^{-1}(P_\infty) = \mathcal{X}(k) \setminus \mathcal{X}_a(k)$ has a unique point (i.e. P_∞ is a k- rational Weierstraß point of $\mathcal{X}$) and $\deg(f) = 8$ otherwise.

Since X is determined up to automorphisms of $\mathbb{P}^1$ we get that the hyperelliptic locus of curves of genus 3 is a 5-dimensional subspace of the moduli space $\mathcal{M}_3$ of curves of genus 3. In fact, there is a system of invariants that describes this locus, namely the Shioda invariants $J_2, \dots, J_8$ as described in [58], [53].

Remark 8. *This explains why it is very hard to use constructions of curves of genus* 3*, for instance as modular curves (*[65]*) or by CM-methods (*[65]*) to find hyperelliptic curves. A rough and heuristic argument is that (for large q) the probability to find a point in $\mathcal{M}_3(\mathbb{F}_q)$ that corresponds to a hyperelliptic curve is $1/q$.*

11.2. Plane Equations. Let $D_{\mathcal{X}}$ be a canonical divisor of $\mathcal{X}$, i.e. the divisor of a holomorphic differential $\omega_{\mathcal{X}}$ of $\mathcal{X}$. Then, $D_{\mathcal{X}}$ has degree 4. Let $\mathcal{L}_{D_{\mathcal{X}}}$ be the k-space of functions f on $\mathcal{X}$ such that $(f) + D_{\mathcal{X}}$ is an effective divisor. It is a classical and well-known fact that $\mathcal{X}$ is non-hyperelliptic if and only if f the k-vector space $\mathcal{L}_{D_{\mathcal{X}}} = \langle f_0, f_1, f_2 \rangle$ has dimension three and the map $\varphi : \mathcal{X} \to \mathbb{P}^2$, where $P \mapsto (f_0 : f_1 : f_2)$ is a projective embedding of $\mathcal{X}$ into the projective plane. Hence if $\mathcal{X}$ is non-hyperelliptic then it has a plane projective regular model of degree 4, as already noted in Lemma 19. Obviously, this is the minimal degree, for curves of degree ≤ 3 have genus ≤ 1.

What about hyperelliptic curves? As discussed already, we find a plane projective curve of degree ≤ 8 (with regular affine part given by a Weierstraß equation) defining $\mathcal{X}$.

Question 1. *Is $\mathcal{X}$ birational equivalent to a plane curve of smaller degree?*

Indeed, we shall see below that, at least if k is algebraically closed, we find a plane equation of degree 5 for $\mathcal{X}$. But this is the *lowest possible degree*, as follows from Proposition 2.2 in [8]. Since the degree of plane curves is crucial for the hardness of discrete logarithms we formulate these results as

Corollary 12. *Let $\mathcal{X}$ be a curve of genus* 3*. If $\mathcal{X}$ is not hyperelliptic then $\mathcal{X}$ has a plane regular projective curves of degree* 4 *as model. If $\mathcal{X}$ is hyperelliptic then the degree of every plane curve birationally equivalent to $\mathcal{X}$ has degree ≥ 5.*

There is a long discussion on equations of genus 3 hyperelliptic curves, their automorphisms, invariants, and minimal fields of definition in [55] and [38].

11.3. Picard Groups of Curves of Genus 3 in Cryptography. The following is the natural question when considering genus $g = 3$ cryptography.

Question 2. *Can one use Picard groups of curves of genus* 3 *for DL-systems?*

11.3.1. *Addition.* As pointed out above, there are relatively fast algorithms which allow addition in Picard groups of curves of any genus (at least if one knows a relatively simple plane model found after a pre-computation).

We recall the general procedure: We assume that there is a point $P_\infty \in \mathcal{X}(k)$ with corresponding prime divisor $\mathfrak{p}_\infty$. In the divisor classes $c_1, c_2 \in \mathrm{Pic}^0_k \mathcal{X}$ we choose convenient divisors D_i, e.g.

$$D_i = E_i - d \cdot \mathfrak{p}_\infty,$$

with E_i an effective divisor of degree $d \leq g$. Then $c_1 + c_2$ is the divisor class of

$$E_1 + E_2 - (d_1 + d_2)\mathfrak{p}_\infty,$$

and the "reduction algorithm" has to compute a divisor

$$E_3 - d_3\mathfrak{p}_0 \sim E_1 + E_2 - (d_1 + d_2)\mathfrak{p}_\infty$$

with $d_3 \leq g$. This is an interpolation problem solved by Hess by the computation of Riemann-Roch spaces; see [30] for details.

Theorem 41 (Diem, Hess). *Let $\mathcal{X}$ be a genus $g \geq 2$ curve defined over $\mathbb{F}_q$. The arithmetic in the degree 0 class group of $\mathcal{X}$ can be performed in the expected time, which is polynomially bounded in g and $\log q$.*

For curves of genus 3 it is convenient to distinguish between non-hyperelliptic and hyperelliptic curves. In the first case one can give $\mathcal{X}$ easily as smooth quartic. Using its geometry one finds, concretely given, fast addition algorithms, which can be found in work of Oyono et al; see [21]. As we shall see below the hardness of the DL is insufficient for cryptographical applications, and so the fast addition is only relevant for attacking systems. So it is enough for us to keep the existence of the addition algorithm in mind.

Next assume that $\mathcal{X}$ is hyperelliptic. We can find rather easily a Weierstrass equation, and the most convenient case is that one of its Weierstrass points is k-rational. We shall restrict to this case (often called "imaginary" because of its analogy to imaginary quadratic fields (E. Artin)) and hence we can give $\mathcal{X}$ by an affine Weierstrass equation

$$\mathcal{X}_a : y^2 = f(x),$$

where $f(x) \in k[x]$ is a monic polynomial of degree 7 without multiple roots. By homogenization we get a plane projective curve with exactly one additional point P_∞, which corresponds to a Weierstraß point of $\mathcal{X}$ and so exactly to one prime divisor $\mathfrak{p}_\infty$ of degree 1 of $\mathcal{X}$. Hence divisors on $\mathcal{X}$ are of the form $D = D_a + z \cdot \mathfrak{p}_\infty$ with D_a a divisor with support on $\mathcal{X}$. Hence we can represent divisor classes in $\mathrm{Pic}^0_k(\mathcal{X})$ by divisors

$$D = E_a - d\,\mathfrak{p}_\infty,$$

with E_a an effective divisor of degree $d \leq 3$ and support in $\mathcal{X}_a$.

Using the special form of $\mathcal{X}_a$ we can give E_i in the so-called "Mumford presentation" as in Theorem 28 and for the reduction step of divisors we can use the very effective Cantor algorithm ([7], Algorithm 14.7). Behind these results is the analogy (developed by E. Artin) between the arithmetic of hyperelliptic function fields and imaginary quadratic fields respectively the arithmetic of quadratic forms due to C.F. Gauß.

This algorithmic approach can be translated into **formulas** (involving, alas, many special cases) that are sometimes more convenient for implementations near to specialized hardware. The generic cases for addition and doubling are explicitly given by Algorithms 14.52 and 14.53 in [7]. These additions are rather fast and not too far away from the timings of additions on elliptic curves (see [7, Table 14.13].

Hence one may well consider to use Picard groups of curves of genus 3 for DL-based cryptographic applications. This will need fast algorithms for point counting, and before that, a security discussion.

11.4. Index-Calculus Attacks. We recall the results from Section 7 based on very refined index-calculus attacks and applied to curves of genus 3:

Corollary 13 (Diem, Gaudry, Thomé, Thériault [28]). *There exists an algorithm which computes, up to* $\log(q)$*-factors, the Discrete Logarithm in the divisor class group of curves* $\mathcal{X}$ *of genus* 3 *in expected time of* $\mathcal{O}(q^{4/3})$*.*

Since the expected size of $\mathrm{Pic}^0\,\mathcal{X}$ is $\sim q^3$ and the generic attacks have complexity $\sim q^{3/2}$ this can be seen as acceptable security. But there is another approach due to C. Diem using factor bases constructed by using plane models of curves; see [16]:

Corollary 14 (Diem). *The following hold:*

- *Let* $\mathcal{X}$ *be be a non-hyperelliptic curve defined over* $\mathbb{F}_q$*. Since* $\mathcal{X}$ *has a plane model of degree* 4 *there exists an algorithm computing the Discrete Logarithm in* $\mathrm{Pic}^0(\mathcal{X})$ *in expected time, up to* $\log(q)$*-factors,* $\mathcal{O}(q)$*.*
- *Let* $\mathcal{X}$ *be a hyperelliptic curve of genus* 3 *then the minimal degree of a plane model of* $\mathcal{X}$ *is* ≥ 5 *and so the degree of Diem's attack has expected complexity* $\mathcal{O}(q^r)$ *with* $r \geq \frac{4}{3}$*.*

This means that the discrete logarithm in Picard groups of non-hyperelliptic curves of genus 3 over finite fields $\mathbb{F}_q$ is too weak for the use in crypto systems (or otherwise expressed, does not yield more security than curves of genus 2 over the same base field), and so they should be avoided. This excludes *randomly chosen* curves of genus 3 over finite fields, but also special curves like the *Picard Curves* with automorphisms of degree 3 ([34]).

But we need more: Let $\mathcal{X}$ be hyperelliptic. Then there must not exist an easily computed isogeny from the Jacobian of $\mathcal{X}$ to the Jacobian of a non-hyperelliptic curve $\mathcal{D}$, for instance induced by a correspondence of small degree between $\mathcal{X}$ and $\mathcal{D}$.

11.5. Isogenies via S_4-Covers. As observed by B. Smith [59] "many" hyperelliptic curves are isogenic to non-hyperelliptic curves via an isogeny with degree dividing 8. This fact is interpreted in terms of Hurwitz spaces and connected modular spaces in [23, 24]. We refer to details and refinements to these papers.

For our purposes it will be enough to look at the case that K is algebraically closed, which we shall assume from now on. For applications in cryptography one has to study rationality problems; see [59] and [24]. The construction relies on the so-called trigonal construction of Donagi-Livné [20].

We begin with a hyperelliptic curve $\mathcal{X}$ of genus 3 and its uniquely determined hyperelliptic projection $f_1 : \mathcal{X} \to \mathbb{P}^1$ with 8 ramification points $P_1, \cdots, P_8$, which extend to the Weierstraß points of $\mathcal{X}$. By linear algebra we show that there is a map

$$f_2 : \mathbb{P}^1 \to \mathbb{P}^1$$

of degree 3 with the following properties:

- f_2 is unramified in $P_1, \cdots P_8$, its ramification points are denoted by $Q_1, \cdots Q_4$ on the base line $\mathbb{P}^1$. The ramification order in Q_i is 2, and so each Q_i has exactly one unramified extension under f_2 denoted by Q_i'.
- $f_2(\{P_1, \cdots P_8\} = \{S_1, \cdots S_4\}$ such that, after a suitable numeration, $f_2(P_i) = f_2(P_{4+i})$ for $1 \leq i \leq 4$.

Now use Galois theory.

11.5.1. *The monodromy group of f_2.* Obviously, the Galois closure $\tilde{f_2} = f_2 \circ h_2$ of f_2 has as Galois group the symmetric group S_3 (since f_2 is not Galois because of the ramification type), and h_2 is degree 2 cover $\mathcal{E}' \stackrel{h_2}{\rightarrow} \mathcal{X}$. From Galois theory we get that $\tilde{f_2} = \pi \circ \eta$, where

$$\eta : \mathcal{E}' \to \mathcal{E}$$

is a cyclic cover of degree 3 with Galois group equal to the alternating subgroup A_3. Then, $\mathcal{E}$ is a quadratic cover of $\mathbb{P}^1$ ramified exactly at the discriminant

$$\Delta_1 = Q_1 + \cdots + Q_4$$

of f_2. Therefore $\mathcal{E}$ is an elliptic curve with cover map π to $\mathbb{P}^1$. From construction and Abhyankar's lemma it follows that η is unramified. Hence $\mathcal{E}'$ is an elliptic curve, too, and η is an isogeny of degree 3 (after applying a suitable translation).

11.5.2. *The monodromy group of $f = f_2 \circ f_1$.* f is a cover of degree 6 and so its Galois group can be embedded into S_6. But a closer analysis using the specific ramification situation shows; see [23, Thm. 3].

Lemma 20. *The monodromy group of f is isomorphic to S_4.*

Let $\tilde{f} : \tilde{\mathcal{X}} \to \mathbb{P}^1$ be the Galois cover of curves factoring over f with Galois group S_4. Let $\mathcal{X}'$ be the subcover of $\tilde{\mathcal{X}}$ with function field equal to the composite of the function fields of $\mathcal{X}$ and $\mathcal{E}'$, i.e. the normalization of the fiber product of $\mathcal{X}$ with $\mathcal{E}'$. Let

$$\pi_{\mathcal{X}} : \mathcal{X}' \to \mathcal{X}$$

the projection to $\mathcal{X}$, which is a cover of degree 2. The Galois group of $\tilde{\mathcal{X}}/\mathcal{X}$ contains 2 transpositions. Let σ be one of them chosen such that with $G_2 = \langle \sigma \rangle$ we get $\mathcal{X}' := \tilde{\mathcal{X}}/G_2$. Hence, σ is contained in precisely two of the stabilizers $T_1, \ldots, T_4$ of the elements $\{1, 2, 3, 4\}$ on which S_4 acts. Let

$$\pi_T : \tilde{\mathcal{X}} \to \mathcal{D} := \tilde{\mathcal{X}}/T$$

be the quotient map. Then $\tilde{f}$ factors over π_T as $\tilde{f} = g \circ \pi_T$, where $g : \mathcal{D} \to \mathbb{P}^1$ has $\deg(g) = 4$. Note that g is primitive (does not factor over a quadratic subcover). We can use the Hurwitz genus formula to compute the genus of $\mathcal{D}$. For this we have to determine the ramification of $\mathcal{D}/\mathbb{P}^1$ under g.

Lemma 21. *The genus of $\mathcal{D}$ is equal to 3, and so is equal to the genus of $\mathcal{X}$.*

We are interested in the case that $\mathcal{J}(\mathcal{X})$ is simple. Then we get from section 8 that:

Proposition 14. *Let $\mathcal{J}_{\mathcal{X}}$ be a simple abelian variety and $\mathcal{D}$ be non-hyperelliptic. The pair of cover maps $(\pi_{\mathcal{X}}, \pi_T)$ from $\mathcal{X}'$ to $(\mathcal{X}, \mathcal{D})$ induces an isogeny*

$$\eta : \mathcal{J}_{\mathcal{X}} \to \mathcal{J}_{\mathcal{D}},$$

whose kernel is elementary-abelian and has degree ≤ 8.

A more detailed analysis due to E. Kani shows that the proposition is true without the assumption that $\mathcal{D}$ is non-hyperelliptic. Then we have the following:

Corollary 15. *The notations are as above. Let K be equal to $\mathbb{F}_q$ and assume that $\mathcal{D}$ is non-hyperelliptic. Then the computation of the Discrete Logarithm in* $\mathrm{Pic}^0_{\mathcal{X}}$ *has complexity $\mathcal{O}(q)$.*

This result motivates the question whether the assumptions of the Corollary are often satisfied. Empirically, B. Smith has given a positive answer. A rigorous answer is given in [24].

We have already explained that by the construction of a $(2,3)$-cover as above we have found a generically finite and dominant morphism from a Hurwitz space $\mathcal{H}_\infty$ to the hyperbolic locus in the moduli space $\mathcal{M}_3$ of curves of genus 3. Hence $\mathcal{H}_\infty$ is a scheme of dimension 5.

Via the trigonal construction we have, to each hyperelliptic curve $\mathcal{X}$, found a curve $\mathcal{D}$ of genus 3 with a cover map

$$g : \mathcal{D} \to \mathbb{P}^1$$

with $\deg(g) = 4$ and the monodromy group of g equal to S_4. Moreover, a detailed study of the construction allows to determine the ramification type of g in the generic case:

There are 8 ramification points of g, exactly 4 points $P_1, \ldots, P_4$ amongst them are of type $(2,2)$ (i.e. $g^*(P_i) = 2(Q_{i,1} + Q_{i,2})$, and the other 4 ramification points are of type $(2,1,1)$. Hence $(\mathcal{D}, g)$ yields a point in a Hurwitz space $\mathcal{H}_2$ of dimension 5.

In [24] one discusses the hyperelliptic locus $\mathcal{H}_{hyp}$ in $\mathcal{H}_2$. The computational part of this discussion determines conditions for the coefficients of Weierstraß equations for curves $\mathcal{D}$ lying in $\mathcal{H}_{hyp}$. This is rather complicated, but one sees that generically these coefficients are parametrized by a 4-dimensional space. Rather deep and involved geometric methods have to be used to transfer these computations into scheme-theoretical results and to get

Theorem 42. *The Hurwitz space $\mathcal{H}_{hyp}$ is a unirational, irreducible variety of dimension 4, provided that char$(K) > 5$. Moreover, the natural forget map*

$$\mu : \mathcal{H}_{hyp} \to \mathcal{M}_3$$

to the moduli space $\mathcal{M}_3$ of genus 3 curves has finite fibers and so its image is also irreducible of dimension 4.

Corollary 16. *We take the notation from above. We assume that K is algebraically closed. There is a one-codimensional subscheme U of $\mathcal{M}_{3,hyp}$ such that for $\mathcal{X} \notin U$ the isogeny η maps $\mathcal{J}_{\mathcal{X}}$ to the Jacobian of a non-hyperelliptic curve $\mathcal{D}$.*

Replacing the algebraically closed field K by a finite field $\mathbb{F}_q$ one has to study rationality conditions for η. This is done in [59] and [24]. As result we get

Corollary 17. *There are $\mathcal{O}(q^5)$ isomorphism classes of hyperelliptic curves of genus 3 defined over $\mathbb{F}_q$ for which the discrete logarithm in the divisor class group of degree 0 has complexity $\mathcal{O}(q)$, up to log-factors. Since $|\mathrm{Pic}^0(C)| \sim q^3$, the DL system of these hyperelliptic curves of genus 3 is weak.*

11.6. Point Counting. In general, not much is known about fast point counting algorithms on curves of genus 3 (aside of the general fact that for all abelian varieties there is a polynomial time algorithm due to Pila). But as we have seen above, for applications in cryptography we have to restrict ourselves to special hyperelliptic curves (where it is not at all clear what "special" means for a concrete curve), and so we do not lose much by restricting to hyperelliptic curves $\mathcal{X}$ whose Jacobian $\mathcal{J}_{\mathcal{X}} =: \mathcal{J}$ has a special endomorphism ring $\mathcal{O}_{\mathcal{J}}$.

11.6.1. *Real Multiplication.* A first possibility is to assume that $\mathcal{J}$ has real multiplication. This means that $\mathcal{O}_{\mathcal{J}}$ contains an order $\mathcal{R}$ of a totally real field of degree 3. An immediate consequence is that there are many isogenies at hand, and in the case of genus 2 this situation has accelerated the point counting dramatically [29]. So there is hope that the same could happen for Jacobians of dimension 3.

So it is interesting to construct hyperelliptic curves $\mathcal{X}$ such that $\mathcal{J}_{\mathcal{X}}$ has real multiplication. In view of the results about Jacobians of the modular curves $X_0(N)$ in section 8.2 it is natural to look for curves whose Jacobian is a quotient of $J_0(N)$ for some N.

This was successfully done by H.J. Weber ([64]. The procedure is: First one computes eigenspaces of dimension 3 of the space of cusp forms of level N under the Hecke operators. Using the attached differentials one can compute (over $\mathbb{C}$) the period matrix of the corresponding factor $\mathcal{J}$ of $J_0(N)$ and decides whether it is principally polarized and hence is the Jacobian of a curve $\mathcal{X}$. Using theta-null values one decides whether $\mathcal{X}$ is hyperelliptic.

If so, one can compute invariants of the curve, and (e.g by a method of Mestre) compute a Weierstrass equation (at the end over $\mathbb{Z}[1/N]$ of $\mathcal{J}$ is a simple factor. Reduction modulo p gives hyperelliptic curves over $\mathbb{Z}/p$ of genus 3 with (known) real multiplication.

The method works quite well but has one disadvantage: Since there are many non-hyperelliptic curves of genus 3 with real multiplication we are not sure whether the constructed curves is isogenous to a non-hyperelliptic curve under the trigonal construction described above.

11.6.2. *Complex Multiplication.* We strengthen the condition on $\mathrm{End}(\mathcal{J})$ and assume that $\mathcal{J}$ has complex multiplication and is defined over a number field. Recall that this means that there is an embedding of $\mathrm{End}(\mathcal{J})$ as order $\mathcal{O}$ into a CM-field K, i.e. K is a totally imaginary quadratic extension of a totally real field K_0 of degree 3 over $\mathbb{Q}$.

The arithmetic of $\mathcal{X}$ and $\mathcal{J}$ is reflected by the arithmetic of orders in K. In particular, one finds the Frobenius endomorphism of reductions of $\mathcal{X}$ modulo prime ideals $\mathfrak{p}$ of K as element in $\mathcal{O}$. This solves the problem of point counting on $\mathcal{X}$ modulo $\mathfrak{p}$ immediately. Moreover, class field theory of K gives both a classification of isomorphy classes of curves $\mathcal{X}$ with CM-field K and methods to find period matrices of $\mathcal{J}$ and so equations of $\mathcal{X}$. Details and more references can be found in [7] sections 5.1 and 18.3.

But trying to find examples for hyperelliptic curves attached to CM fields of degree 6 one runs into trouble since these examples seem to be very rare. This was one of the results of the thesis of A. Weng (Essen 2001). So one has to use some force: If $\mathcal{J}$ has an automorphism of order 4 the curve $\mathcal{X}$ has an automorphism of order at least 2, and if $\mathcal{J}$ is simple the quotient of $\mathcal{X}$ by this automorphism has to be $\mathbb{P}^1$, and so $\mathcal{X}$ is hyperelliptic and has an automorphism of order 4.

The existence of J with automorphism φ of order 4 is obtained by a special choice of the CM-field K: Let K_0 be a totally real field of degree 3 with class number 1 (there are many fields with these properties) and take $K = K_0(\sqrt(-1))$, and for $\mathcal{O}$ take the maximal order of K. In [65] one finds in detail how with these choices lead to many examples of hyperelliptic curves over finite fields suitable for cryptography.

11.6.3. *Resistance against the Trigonal Attack.* We assume now that $\mathcal{X}$ is a hyperelliptic curve with an automorphism φ of order 4. We apply the trigonal construction and take the notation introduced in Section 11.5. First we see that φ induces an automorphism $\varphi_{\mathbb{P}^1}$ of order 2 on $\mathbb{P}^1$, taken as subcover of $\mathcal{X}$ under f_1. Since cross ratios are not changed by automorphisms we see that there is an extension of $\varphi_{\mathbb{P}^1}$ to the elliptic curve $\mathcal{E}'$ having order 4 and so to an automorphism φ' of the curve $\mathcal{X}'$ of order 4. Now we have exactly two choices for the construction of $\mathcal{D}$ as subcover of $\mathcal{X}'$, and this yields that at least two of the curves $\mathcal{D}^{(\varphi')^j}$, $j = 0, 1, 2, 3$, have to be equal, and so $\mathcal{D}$ has an automorphism of order 2 and is, because of the simplicity of $\mathcal{J}$, hyperelliptic.

Conclusion: Hyperelliptic curves with automorphisms of order 4 are resistant against the trigonal attack.

Lemma 22. *Let $\mathcal{X}$ be an hyperelliptic curve with an automorphism of order 4 and with simple Jacobian variety $\mathcal{J}$. Let*

$$\eta : \mathcal{J} \to \mathcal{J}'$$

be an isogeny with $\mathcal{J}'$ principally polarized. Then $\mathcal{J}'$ is the Jacobian variety of a hyperelliptic curve.

Hence, it follows that a "minimal bad" isogeny has to have a two-power and rather large degree.

References

[1] L. Beshaj, *Minimal weierstrass equations for genus 2 curves* (2016), available at 1612.08318.

[2] L. Beshaj and S. Guest, *Weighted projective space of binary sextics*, 2018.

[3] Reinier Bröker, Everett W. Howe, Kristin E. Lauter, and Peter Stevenhagen, *Genus-2 curves and jacobians with a given number of points* (2014), available at 1403.6911.

[4] Reinier Bröker and Kristin Lauter, *Modular polynomials for genus 2*, LMS J. Comput. Math. **12** (2009), 326–339. MR2570930

[5] David G. Cantor, *On the analogue of the division polynomials for hyperelliptic curves*, J. Reine Angew. Math. **447** (1994), 91–145. MR1263171

[6] Andrew Childs, David Jao, and Vladimir Soukharev, *Constructing elliptic curve isogenies in quantum subexponential time*, J. Math. Cryptol. **8** (2014), no. 1, 1–29. MR3163097

[7] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren (eds.), *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2006. MR2162716

[8] Marc Coppens and Gerriet Martens, *Linear series on 4-gonal curves*, Math. Nachr. **213** (2000), 35–55. MR1755245

[9] Jean-Marc Couveignes, *Hard homogeneous spaces*, 2006. Cryptology e-Print Arxive.

[10] Luca De Feo, *Fast algorithms for computing isogenies between ordinary elliptic curves in small characteristic*, J. Number Theory **131** (2011), no. 5, 873–893. MR2772477

[11] Luca De Feo, Cyril Hugounenq, Jérôme Plût, and Éric Schost, *Explicit isogenies in quadratic time in any characteristic*, LMS J. Comput. Math. **19** (2016), no. suppl. A, 267–282. MR3540960

[12] Luca De Feo, David Jao, and Jérôme Plût, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, J. Math. Cryptol. **8** (2014), no. 3, 209–247. MR3259113

[13] P. Deligne and D. Mumford, *The irreducibility of the space of curves of given genus*, Inst. Hautes Études Sci. Publ. Math. **36** (1969), 75–109. MR0262240

[14] Max Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272. MR0005125

[15] C. Diem, *On arithmetic and the discrete logarithm problem in class groups of curves*, Ph.D. Thesis, 2008. Habilitationsschrift.

[16] Claus Diem, *An index calculus algorithm for plane curves of small degree*, Algorithmic number theory, 2006, pp. 543–557. MR2282948

[17] Whitfield Diffie and Martin E. Hellman, *New directions in cryptography*, IEEE Trans. Information Theory **IT-22** (1976), no. 6, 644–654. MR0437208

[18] J. Dixmier, *On the projective invariants of quartic plane curves*, Adv. in Math. **64** (1987), no. 3, 279–304. MR888630

[19] I. Dolgachev and D. Lehavi, *On isogenous principally polarized abelian surfaces*, Curves and abelian varieties, 2008, pp. 51–69. MR2457735

[20] Ron Donagi and Ron Livné, *The arithmetic-geometric mean and isogenies for curves of higher genus*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **28** (1999), no. 2, 323–339. MR1736231

[21] Stéphane Flon, Roger Oyono, and Christophe Ritzenthaler, *Fast addition on non-hyperelliptic genus 3 curves*, Algebraic geometry and its applications, 2008, pp. 1–28. MR2484046

[22] Gerhard Frey, *Isogenies in theory and praxis*, Open problems in mathematics and computational science, 2014, pp. 37–68. MR3330877

[23] Gerhard Frey and Ernst Kani, *Correspondences on hyperelliptic curves and applications to the discrete logarithm*, 2011, pp. 1–19.

[24] ———, *Normal forms of hyperelliptic curves of genus 3*, Des. Codes Cryptogr. **77** (2015), no. 2-3, 677–712. MR3403171

[25] William Fulton, *Algebraic curves*, Advanced Book Classics, Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989. An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original. MR1042981

[26] P. Gaudry, F. Hess, and N. P. Smart, *Constructive and destructive facets of Weil descent on elliptic curves*, J. Cryptology **15** (2002), no. 1, 19–46. MR1880933

[27] P. Gaudry, D. Kohel, B Smith, D. Hoon, and X. Wang, *Counting points on genus 2 curves with real multiplication*, 2011, pp. 504–519.

[28] P. Gaudry, E. Thomé, N. Thériault, and C. Diem, *A double large prime variation for small genus hyperelliptic index calculus*, Math. Comp. **76** (2007), no. 257, 475–492. MR2261032

[29] Pierrick Gaudry, David Kohel, and Benjamin Smith, *Counting points on genus 2 curves with real multiplication*, Advances in cryptology—ASIACRYPT 2011, 2011, pp. 504–519. MR2935020

[30] F. Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics*, J. Symbolic Comput. **33** (2002), no. 4, 425–445. MR1890579

[31] Antoine Joux, Andrew Odlyzko, and Cécile Pierrot, *The past, evolving present, and future of the discrete logarithm*, Open problems in mathematics and computational science, 2014, pp. 5–36. MR3330876

[32] Naoki Kanayama, *Division polynomials and multiplication formulae of Jacobian varieties of dimension 2*, Math. Proc. Cambridge Philos. Soc. **139** (2005), no. 3, 399–409. MR2177167

[33] ———, *Corrections to "Division polynomials and multiplication formulae in dimension 2" [mr2177167]*, Math. Proc. Cambridge Philos. Soc. **149** (2010), no. 1, 189–192. MR2651585

[34] Kenji Koike and Annegret Weng, *Construction of CM Picard curves*, Math. Comp. **74** (2005), no. 249, 499–518. MR2085904

[35] M. Kraichik, *Théorie des nombres*, paris, 1922.

[36] Greg Kuperberg, *A subexponential-time quantum algorithm for the dihedral hidden subgroup problem*, SIAM J. Comput. **35** (2005), no. 1, 170–188. MR2178804

[37] Frank Leitenberger, *About the group law for the Jacobi variety of a hyperelliptic curve*, Beiträge Algebra Geom. **46** (2005), no. 1, 125–130. MR2146447

[38] Reynald Lercier and Christophe Ritzenthaler, *Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects*, J. Algebra **372** (2012), 595–636. MR2990029

[39] Davide Lombardo, *Computing the geometric endomorphism ring of a genus 2 jacobian*, arxiv (2016).

[40] David Lubicz and Damien Robert, *Computing isogenies between abelian varieties*, Compos. Math. **148** (2012), no. 5, 1483–1515. MR2982438

[41] ______, *Computing isogenies between abelian varieties*, Compos. Math. **148** (2012), no. 5, 1483–1515. MR2982438

[42] ______, *Computing separable isogenies in quasi-optimal time*, LMS J. Comput. Math. **18** (2015), no. 1, 198–216. MR3349315

[43] K. Magaard, T. Shaska, S. Shpectorov, and H. Völklein, *The locus of curves with prescribed automorphism group*, Sūrikaisekikenkyūsho Kōkyūroku **1267** (2002), 112–141. Communications in arithmetic fundamental groups (Kyoto, 1999/2001). MR1954371

[44] K. Magaard, T. Shaska, and H. Völklein, *Genus 2 curves that admit a degree 5 map to an elliptic curve*, Forum Math. **21** (2009), no. 3, 547–566. MR2526800

[45] Andreas Malmendier and Tony Shaska, *A universal genus-two curve from Siegel modular forms*, SIGMA Symmetry Integrability Geom. Methods Appl. **13** (2017), 089, 17 pages. MR3731039

[46] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186 (1978). MR488287

[47] J. S. Milne, *Jacobian varieties*, Arithmetic geometry (Storrs, Conn., 1984), 1986, pp. 167–212. MR861976

[48] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition. MR2514037

[49] Yoshihiro Ônishi, *Determinant expressions for hyperelliptic functions*, Proc. Edinb. Math. Soc. (2) **48** (2005), no. 3, 705–742. With an appendix by Shigeki Matsutani. MR2171194

[50] Frans Oort, *Endomorphism algebras of abelian varieties*, Algebraic geometry and commutative algebra, Vol. II, 1988, pp. 469–502. MR977774

[51] Oded Regev, *New lattice-based cryptographic constructions*, J. ACM **51** (2004), no. 6, 899–942. MR2145258

[52] T. Shaska, *Genus 2 fields with degree 3 elliptic subfields*, Forum Math. **16** (2004), no. 2, 263–280. MR2039100

[53] ______, *Some remarks on the hyperelliptic moduli of genus 3*, Comm. Algebra **42** (2014), no. 9, 4110–4130. MR3200084

[54] ______, *Heights on weighted projective spaces* (201801), available at `1801.06250`.

[55] T. Shaska and F. Thompson, *Bielliptic curves of genus 3 in the hyperelliptic moduli*, Appl. Algebra Engrg. Comm. Comput. **24** (2013), no. 5, 387–412. MR3118614

[56] T. Shaska and J. L. Thompson, *On the generic curve of genus 3*, Affine algebraic geometry, 2005, pp. 233–243. MR2126664

[57] T. Shaska and H. Völklein, *Elliptic subfields and automorphisms of genus 2 function fields*, Algebra, arithmetic and geometry with applications (West Lafayette, IN, 2000), 2004, pp. 703–723. MR2037120

[58] Tetsuji Shioda, *On the graded ring of invariants of binary octavics*, Amer. J. Math. **89** (1967), 1022–1046. MR0220738

[59] Benjamin Smith, *Computing low-degree isogenies in genus 2 with the Dolgachev-Lehavi method*, Arithmetic, geometry, cryptography and coding theory, 2012, pp. 159–170. MR2961408

[60] Henning Stichtenoth, *Algebraic function fields and codes*, Second, Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009. MR2464941

[61] Anton Stolbunov, *Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves*, Adv. Math. Commun. **4** (2010), no. 2, 215–235. MR2654134

[62] John Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144. MR0206004

[63] Yukihiro Uchida, *Division polynomials and canonical local heights on hyperelliptic Jacobians*, Manuscripta Math. **134** (2011), no. 3-4, 273–308. MR2765713

[64] Hermann-Josef Weber, *Hyperelliptic simple factors of $J_0(N)$ with dimension at least* 3, Experiment. Math. **6** (1997), no. 4, 273–287. MR1606908

[65] Annegret Weng, *A class of hyperelliptic CM-curves of genus three*, J. Ramanujan Math. Soc. **16** (2001), no. 4, 339–372. MR1877806