This is Chapter 5 by Gerhard Frey and Tanja Lange of the Handbook of Elliptic and Hyperelliptic Curve Cryptography, Henri Cohen, Christophe Doche, and Gerhard Frey, Editors, CRC Press 2006.

Chapter 5

Varieties over Special Fields

Gerhard Frey and Tanja Lange

Contents in Brief

In the previous chapter we dealt with algebraic and geometric objects over arbitrary fields. In this chapter we explain additional properties of these objects when considered over special fields. We concentrate on varieties over the complex numbers and finite fields.

5.1 Varieties over the field of complex numbers

In the whole section we take ground field K as the field of complex numbers $\mathbb{C}$. Since $\mathbb{C}$ is algebraically closed we can identify the affine space $\mathbb{A}^n$ (respectively the projective space $\mathbb{P}^n$) with the set of points in $\mathbb{C}^n$ (respectively the homogeneous classes of $(n+1)$-tuples in $\mathbb{C}^{n+1}$) together with the topological structure induced by the Zariski topology. Recall that closed sets are given as zeroes of polynomial equations.

The absolute value $|\cdot|$ makes $\mathbb{C}^n$ to a metric space and hence induces a "natural" topology. Since polynomial functions are continuous in this topology it follows that Zariski closed sets are also closed in this topology.

5.1.1 Analytic varieties

First we shall describe very briefly the *analytic structure* on $\mathbb{A}^n$ (respectively $\mathbb{P}^n$): the key notions are *holomorphic functions*. Locally, holomorphic functions are given by power series converging in an open ball.

For open sets $U \subset \mathbb{P}^n$ one can globalize to get holomorphic functions by gluing together the local "germs." So a holomorphic function f on U is a complex valued function defined on U such that for all $P \in U$ there is an open ball around P on which f is given by a convergent power series. Examples for holomorphic functions are polynomials (for $U = \mathbb{A}^n$) and rational functions (for U equal to the set of definition).

Meromorphic functions on U are defined as quotients of holomorphic functions. Locally they are given by Laurent series with finite negative part. To a meromorphic function f on U and to any point $P \in U$ we can associate the order of vanishing $n_P(f)$ of f at P. It is negative if f has a pole of order $|n_P(f)|$ at P, and positive if f has a zero of order $n_P(f)$ at P. If $n_P(f) = 0$ there is a neighborhood of P in U such that the restriction of f is invertible in this neighborhood as a holomorphic function. In particular, it follows that the set of zeroes and poles of meromorphic functions on U does not have a limit point in U. The (analytic) divisor $\mathrm{div}_{\mathrm{an}}(f)$ is equal to the formal sum $\mathrm{div}_{\mathrm{an}}(f) = \sum_{P \in U} n_P(f)P$.

One can differentiate and integrate holomorphic and meromorphic functions and as usual one has meromorphic differentials ω on U. Locally at a point $P \in U$ they are of the form $f_P(x)dx_1 \cdots dx_n$ with f_P meromorphic and $(x_1, \ldots, x_n)$ a local system of coordinates (mapping the chosen neighborhood to an open ball in $\mathbb{C}^n$ with 0 as image of P). Their divisor is $\mathrm{div}_{\mathrm{an}}(\omega) = \sum_{P \in U} n_P(f_P)P$. One sees that ω is holomorphic on U if and only if the divisor of ω has only nonnegative coefficients.

In the sequel we shall need a further concept, namely *analytic varieties*. For the notion of analytic varieties (without boundary) in projective spaces we refer to [GRHA 1978].

One essential property of analytic varieties $V_{\mathrm{an}} \subseteq \mathbb{P}^n$ is that there exists a number $d \leqslant n$ such that V_{an} is locally isomorphic to a ball in an affine space $\mathbb{A}^d$, or equivalently: every point $P \in V_{\mathrm{an}}$ has an open neighborhood U_P (with respect to the topology on V_{an} induced by the restriction of the topology on $\mathbb{P}^n$ to V_{an}) and local coordinate functions (holomorphic in U_P) which map U_P bijectively to a ball in $\mathbb{C}^d$ with 0 as image of P.

Using this local analytic structure one defines holomorphic functions on open subsets of V_{an}, meromorphic functions on V_{an}, holomorphic (respectively meromorphic) differentials and holomorphic (respectively meromorphic) maps between two analytic varieties. The number d is the *dimension of V_{an}*.

Now assume that V is an (affine or projective) algebraic variety of algebraic dimension d embedded in $\mathbb{P}^n$. First of all the underlying set is closed. Next, all points of V are nonsingular, and the Jacobi criterion (cf. Lemma 4.94) for the local (algebraic) coordinate functions together with the implicit function theorem ensures that this set satisfies the conditions of analytic varieties being locally isomorphic to $\mathbb{C}^d$. So we can give V the structure of an analytic variety of dimension d denoted by V_{an}. Note that rational functions on V are meromorphic functions on V_{an}. Of course, the converse does not have to hold true.

But there is a very important special case. Assume that V is a projective algebraic variety. Then the underlying set is *compact* in $\mathbb{P}^n$. It follows that meromorphic functions on V_{an} have only finitely many zeroes and poles. Therefore, they are rational functions on V. So the field of meromorphic functions on V_{an} is equal to $K(V)$ and has transcendental degree d over $\mathbb{C}$.

The converse of this remark is true, too. So we can state the following fundamental result.

Theorem 5.1 Let V_{an} be a compact analytic variety in $\mathbb{P}^n$ of dimension d. There is an algebraic projective variety $V \subset \mathbb{P}^n$ such that the induced analytic variety is equal to V_{an}, and the field of meromorphic functions on V_{an} has transcendence degree d over $\mathbb{C}$ and hence is equal to $K(V)$.

The next lemma gives a slight generalization of the above facts about functions on varieties.

Lemma 5.2 Let V, W be projective algebraic varieties. Then the set of holomorphic maps from V_{an} to W_{an} is (in a natural way) identical with $\mathrm{Hom}_{\mathbb{C}}(V, W)$.

As a consequence of these comparison results, we can use the full power of complex analysis to get purely algebraic properties of objects related to varieties defined over the complex numbers.

Before discussing the two examples that are the most important for us we will conclude this section with a remark.

Remark 5.3 It is well-known in number theory that the interpretation of number fields K as subfields of $\mathbb{C}$ is in a most fruitful way generalized to the study of number fields as subfields of p-adic fields. The same is true if we want to study objects of algebraic geometry by analytic methods. As counterpart of $\mathbb{C}$ one uses the completion of the algebraic closure of $\mathbb{Q}_p$. Over these fields we have the highly developed machinery of rigid analytic geometry. In Chapter 17 we shall have to use parts of this theory as *background* for discussing p-adic point counting methods on curves over finite fields, which have become important in recent years.

5.1.2 Curves over $\mathbb{C}$

Analytic curves C_{an} are one-dimensional analytic varieties embedded into a projective space over $\mathbb{C}$. From now on we shall assume that C_{an} is compact. Then there is a nonsingular projective irreducible curve C such that C_{an} is the corresponding analytic curve. Hence, from an abstract point of view the rational functions on C cannot be distinguished from the meromorphic functions on C_{an}.

One uses this to produce functions on C by analytic methods: locally there are many more meromorphic functions given by converging Laurent series, and by the gluing process we can hope to get global meromorphic functions that turn out to be *algebraic*.

In the previous section we introduced the notion of divisors on analytic curves C_{an} in a way analogous to the algebraic case. The finiteness condition for coefficients not equal to 0 is replaced by the condition that poles and zeroes have no limit point. But since we have assumed that C_{an} is compact this is exactly the same condition as in the algebraic case. Therefore, analytic divisors can be identified with algebraic divisors in a canonical way. The same is true for divisor class groups. (Note again that the situation changes totally if we go to affine parts of C.)

We introduced differentials for algebraic curves in Section 4.4.2.c. We now look at them from the analytic point of view. Here the usual calculus methods are used to construct the meromorphic differentials. Again we get:

Proposition 5.4 Meromorphic (respectively holomorphic) differentials on C_{an} can be identified with meromorphic (respectively holomorphic) differentials on C.

We have defined the genus g of C with the help of the theorem of Riemann–Roch (cf. Theorem 4.106). This theorem also holds for the divisor theory of C_{an}. (In fact its original version was proved in this context.) One of its consequences is that the holomorphic differentials Ω_C on C_{an} (or on C) form a g-dimensional vector space over $\mathbb{C}$ and that these differentials can be identified with algebraic differentials with effective divisors. Let us choose a basis $\{\omega_1, \ldots, \omega_g\}$. To get the full power of analytic methods we have to go one step further and go to real surfaces.

Digression: the easiest example of Weil descent

Next we use an additional special property of $\mathbb{C}$: it is a two-dimensional vector space over the field of real numbers $\mathbb{R}$ with basis $\{1, i\}$ where as usual $i^2 = -1$.

Replacing a complex variable z by two real variables x, y using $z = x + iy$ identifies the metric vector space $\mathbb{C}^n$ with the usual Euclidean space $\mathbb{R}^{2n}$. By this process we lose the analytic structure but have a *differentiable structure* from usual real calculus again compatible with the Zariski topology. Applying this to algebraic varieties V of dimension d in $\mathbb{A}^n_{\mathbb{C}}$ we find in a natural way an affine variety $W_{\mathbb{R}} \subset \mathbb{A}^{2n}_{\mathbb{R}}$ of dimension $2d$ with $W(\mathbb{R}) = V(\mathbb{C})$: we replace the n complex affine

coordinates $(X_1, \ldots, X_n)$ by the real coordinates $(U_1, V_1, \ldots, U_n, V_n)$ with $X_j = U_j + iV_j$, plug them into the equations $\big(f_1(X), \ldots, f_m(X)\big)$ defining V and separate the resulting polynomials into their real and imaginary part $f_k(U,V) = g_k(U,V) + ih_k(U,V)$, where g_k and h_k are defined over $\mathbb{R}$. Then W is the variety defined by (g_k, h_k).

By a gluing process we can apply this procedure to *projective* algebraic varieties. So we attach to every affine or projective variety V of dimension d defined over $\mathbb{C}$ an affine (respectively projective) algebraic variety W_V of dimension $2d$ defined over $\mathbb{R}$ with $W_V(\mathbb{R}) = V(\mathbb{C})$. It is a nice exercise to show that $W_V \cdot \mathbb{C}$ is isomorphic to $V \times V$ as algebraic variety over $\mathbb{C}$.

What we have sketched above is the most simple example of scalar (or Weil-) restriction of varieties defined over a finite algebraic extension field L of a field K to varieties over K. This construction will play an important role later (cf. Chapter 7 on Weil descent).

Riemann surfaces

We apply Weil descent to irreducible nonsingular projective curves C defined over $\mathbb{C}$ and get an irreducible two-dimensional projective variety W_C defined over $\mathbb{R}$. The analytic structure of C induces a differentiable real structure that makes W_C locally isomorphic to a unit ball in $\mathbb{R}^2$. That means that for every $P \in W_C(\mathbb{R})$ there is an open neighborhood $U_P \in W_C$ and real differentiable functions f_1, f_2 defined on U_P mapping U_P to the open unit disc in $\mathbb{R}^2$ and sending P to $(0,0)$.

Since $C(\mathbb{C})$ is compact, it follows that W_C is compact in the real topology.

As result we get that the projective curve C carries in a natural way the structure of a *compact Riemann surface.* We remark that the converse is true, too: every compact Riemann surface is the Weil descent of a projective nonsingular irreducible curve defined over $\mathbb{C}$.

Riemann surfaces R are classical and very well studied objects in geometry. One key ingredient is the study of paths on them up to homology (cf. [GRHA 1978]). They can be used to define the topological genus g_{top} of R. Namely fixing a base point P_0 and composing closed paths in a natural way we turn the set of points $\mathcal{P}$ into a group. By identifying homologous paths we get the *fundamental group* Π_R of R as quotient of $\mathcal{P}$. It is generated by $2g_{\text{top}}$ paths satisfying one relation which lies in the commutator subgroup of the fundamental group. This implies that the maximal abelian factor group of Π_R, the first homology group $H_1(R, \mathbb{Z})$, is a free abelian group with $2g_{\text{top}}$ generators $(\alpha_1, \ldots, \alpha_{2g_{\text{top}}})$.

We come back to the case that $R = W_C$ with C a projective curve over $\mathbb{C}$.

Proposition 5.5 The genus g of C is equal to the topological genus g_{top} of W_C.

Using well-known results from (real and complex) calculus we do integration on W_C using holomorphic differentials ω on C and closed paths α on W_C. As above we choose a base point P_0 on W_C and get the group $\mathcal{P}$ by composing closed (continuous) paths beginning in P_0.

Lemma 5.6 We have a map

$$\langle \cdot\,, \cdot \rangle_0 : \mathcal{P} \times \Omega_C \to \mathbb{C}$$

defined by $\langle \alpha, \omega \rangle_0 := \int_\alpha \omega$ where $\int_\alpha$ is the line integral along the path α.

Moreover, $\langle \cdot\,, \cdot \rangle_0$ is independent of the homology class of α and vanishes when restricted to the commutator subgroup of $\mathcal{P}$ in the first component.

Corollary 5.7 The map $\langle \cdot\,, \cdot \rangle_0$ induces a pairing, that is denoted by $\langle \cdot\,, \cdot \rangle$, between the $\mathbb{Z}$-module $H_1(W_C, \mathbb{Z})$ and the $\mathbb{C}$-vector space Ω_C.

Recall that we have chosen a basis $(\omega_1, \ldots, \omega_g)$ of the space of holomorphic differentials on C. We define the map

$$\begin{aligned} \phi: H_1(W_C, \mathbb{Z}) &\longrightarrow \mathbb{C}^g \\ \tau &\longmapsto \left(\int_\alpha \omega_1, \ldots, \int_\alpha \omega_g\right) \end{aligned}$$

where α is a path in the class of τ.

Proposition 5.8 The image Λ_C of ϕ is a full lattice in $\mathbb{C}^g$, i.e., a discrete free $\mathbb{Z}$-module of rank $2g$ in $\mathbb{C}^g$.

By this proposition we can associate a full rank lattice to each curve over $\mathbb{C}$. The following lemma describes what quotients of lattices look like.

Lemma 5.9 Let Λ be a lattice of full rank in $\mathbb{C}^g$ and let $\mathbb{C}^g/\Lambda$ be the quotient group with quotient topology. Then $\mathbb{C}^g/\Lambda$ is compact and locally isomorphic (as topological space) to the unit ball in $\mathbb{C}^g$.

Corollary 5.10 The set $\mathbb{C}^g/\Lambda_C$ is a compact topological space with respect to the quotient topology inherited from $\mathbb{C}^g$. It is locally homeomorphic to the unit ball in $\mathbb{C}^g$.

Definition 5.11 The lattice Λ_C is called the *period lattice of* C (with respect to the basis $\{\omega_1, \ldots, \omega_g\}$ of the holomorphic differentials).

We are now ready to define the Abel–Jacobi map. We fix the base point $P_0 \in C(\mathbb{C})$. For $P \in C(\mathbb{C})$ choose a path γ from P_0 to P and define $J_\gamma(P) := \left(\int_\gamma \omega_1, \ldots, \int_\gamma \omega_n\right) \in \mathbb{C}^g$. The tuple $J_\gamma(P)$ will — in general — depend on the choice of γ. If γ' is another path from P_0 to P then γ and γ' differ by a closed path beginning in P_0 and so $J_\gamma(P) - J_{\gamma'}(P)$ is an element of Λ_C.

Definition 5.12 The *Abel–Jacobi map* is defined by

$$\begin{aligned} J: C(\mathbb{C}) &\to \mathbb{C}^g/\Lambda_C \\ P &\mapsto J_\gamma(P) + \Lambda_C. \end{aligned}$$

We can generalize this definition to divisors on C by linear extension. We denote the corresponding map again by J.

Theorem 5.13 (Abel–Jacobi)

(i) Let D be a principal divisor of C. Then $J(D) = 0$. So J induces a map $\bar{J}$ from Pic_C^0 to $\mathbb{C}^g/\Lambda_C$.
(ii) The map $\bar{J}$ is a group isomorphism.

By Lemma 5.9 the group $\mathbb{C}^g/\Lambda_C$ carries an analytic structure since it is locally homeomorphic to the unit ball in $\mathbb{C}^g$. The group Pic_C^0 carries the structure of an abelian variety, namely the Jacobian variety J_C of C (see Definition 4.134). Hence, it has an analytic structure, too. The theorem of Abel–Jacobi includes that $\bar{J}$ is an *analytic isomorphism.*

So the structure of J_C as analytic variety is rather simple and described by $\mathbb{C}^g/\Lambda$.

5.1.3 Complex tori and abelian varieties

An important part of the introduction to the objects relevant for cryptography were the connected *projective* algebraic groups called abelian varieties (cf. Section 4.3). The analytic counterpart are connected *compact* complex Lie groups (cf. e.g., Lang [LAN 2002a]).

We give the most simple example of a complex Lie group: take $\mathbb{C}^d$ with the usual complex structure and with vector addition $+$ as group composition. It is obvious that the addition $+$ as well as the inversion $-$ are holomorphic. The group $\mathbb{C}^d$ is not compact but we can easily find quotients that are compact.

For this we choose a lattice (always assumed to be of full rank) $\Lambda \subset \mathbb{C}^d$, i.e., there is a basis $\{\mu_1, \ldots, \mu_{2d}\}$ of $\mathbb{C}^d$ as real vector space such that

$$\Lambda = \left\{ \sum_{j=1}^{2d} z_j \mu_j \mid z_j \in \mathbb{Z} \right\}.$$

Equivalently we have: Λ is a $\mathbb{Z}$-submodule of $\mathbb{C}^d$ of rank $2d$ which is discrete, i.e., in every bounded subset of $\mathbb{C}^d$ there are only finitely many elements of Λ.

We can endow $\mathbb{C}^d/\Lambda$ with an analytic structure in a natural way. Let the U_j be open sets covering $\mathbb{C}^d/\Lambda$ such that each U_j is homeomorphic via bijective continuous maps φ_j to balls B_j in $\mathbb{C}^d$. The maps φ_j are assumed to be compatible with restrictions to intersections of the sets U_j. We define holomorphic functions on U_j as functions $f_j : U_j \to \mathbb{C}$ such that $f_j \circ \varphi_j^{-1}$ are holomorphic on B_j and come to global functions by gluing local holomorphic functions. Meromorphic functions are defined as quotients of holomorphic functions. It is an immediate consequence from these definitions that $\mathbb{C}^d/\Lambda$ carries the structure of a complex connected Lie group that is a quotient (as Lie group) of $\mathbb{C}^d/\Lambda$.

Definition 5.14 A complex Lie group isomorphic to $\mathbb{C}^d/\Lambda$ is called a *complex d-dimensional torus*.

A fundamental result is:

Proposition 5.15 Let X be a connected compact complex Lie group of dimension d. Then X is isomorphic to a torus $T := \mathbb{C}^d/\Lambda$.

For the proof see [MUM 1974, p. 2].

We apply this to an abelian variety $\mathcal{A}$ of dimension d defined over $\mathbb{C}$. The associated analytic variety $\mathcal{A}_{\text{an}}$ is connected and compact. Since addition and inversion on $\mathcal{A}$ are given by polynomials, $\mathcal{A}_{\text{an}}$ is a torus and, hence, is isomorphic to the Lie group $\mathbb{C}^d/\Lambda$ for some lattice Λ. Note that by this isomorphism the addition on $\mathcal{A}$ is transferred into a very easy form. It is just the vector addition in $\mathbb{C}^d$ modulo Λ.

Next we shall study the converse. We want to decide whether T is the analytic companion of an algebraic variety. By Chow's theorem this is equivalent to the question whether we can embed T into a projective space such that the analytic structures are compatible.

If this is possible we shall find d algebraically independent meromorphic functions on T. By standard methods of algebraic theory (the key word is "ample line bundle") one sees that the converse is true, too. So one has to *construct* meromorphic functions on T, or equivalently, meromorphic functions on $\mathbb{C}^d$ which are *periodic* with respect to Λ. There are well-known methods for this (for $d = 1$ one uses results like the Weierstraß product theorem or the Mittag–Leffler theorem). In general the main ingredients are theta functions attached to Λ. We shall need them later on (cf. Chapter 18) and then deal explicitly with the case that is most interesting for us, and so we do not give a formal definition here.

In [MUM 1974, pp. 24-35] one finds the discussion what additional properties Λ has to have in order to have enough periodic functions.

First recall that a Hermitian form H on $\mathbb{C}^d \times \mathbb{C}^d$ can be decomposed as

$$H(x,y) = E(ix,y) + iE(x,y)$$

where E is a skew symmetric real form on $\mathbb{C}^d$ satisfying $E(ix,iy) = E(x,y)$. The form E is called the imaginary part $\Im m(H)$ of H. (Since these notations are rather standard we find it convenient not to change them though the letter E is used for elliptic curves in most cases. We hope that this does not give rise to confusion.)

Theorem 5.16 The torus $T = \mathbb{C}^d/\Lambda$ can be embedded into a projective space and, hence, equals *the analytic variety attached to an abelian variety* if and only if there exists a positive definite Hermitian form H on $\mathbb{C}^d$ with $E = \Im m(H)$ such that E restricted to $\Lambda \times \Lambda$ has values in $\mathbb{Z}$.

We use the structure theorems for Hermitian forms and get

Corollary 5.17 Let $T = \mathbb{C}^d/\Lambda$ 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 the $(d \times d)$-matrix Ω is symmetric and has a positive definite imaginary part, i.e., lies in the Siegel upper half plane $\mathbb{H}_g$.

Corollary 5.18 Assume that $d = 1$, i.e., $\mathcal{A}$ is an elliptic curve E. Then the torus associated to E is isomorphic to $\mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ where τ is a complex number with positive imaginary part.

Definition 5.19 We call Ω the *period matrix of* $\mathcal{A}$.

We continue to assume that $T = \mathcal{A}_{\text{an}}$ with Hermitian form H and $E = \Im m(H)$.

With the help of E we can define a dual lattice $\widehat{\Lambda}$ given by

$$\widehat{\Lambda} := \big\{x \in \mathbb{C}^d \mid E(x,y) \in \mathbb{Z}, \text{ for all } y \in \Lambda\big\}.$$

The lattice $\widehat{\Lambda}$ contains Λ and $\widehat{\Lambda}/\Lambda$ is finite. Furthermore, $\widehat{\Lambda}$ belongs to a torus $\widehat{T}$, which is attached to an abelian variety $\hat{\mathcal{A}}$. In fact we have just constructed the *dual abelian variety* to $\mathcal{A}$ by analytic methods over the complex numbers (see [MUM 1974], 82-86). There it is also shown how this dual abelian variety can be constructed by purely algebraic methods over any ground field.

For us a special case is most important. Assume that $\widehat{\Lambda} = \Lambda$ and so $\mathcal{A}$ is equal to its dual.

Definition 5.20 If $\widehat{\Lambda} = \Lambda$ then $\mathcal{A}$ is called *principally polarized*.

Corollary 5.21 Let $\mathcal{A}$ be a principally polarized abelian variety over $\mathbb{C}$ with lattice Λ, Hermitian form H and $E = \Im m(H)$. Then there exists a basis $\{\mu_1, \ldots, \mu_{2d}\}$ of Λ such that

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

Now we come back to the theme of this book, namely projective irreducible nonsingular curves C and their Jacobians J_C.

By the theorem of Abel–Jacobi (cf. Theorem 5.13) we have found an isomorphism from $\mathrm{Pic}^{\,0}_C$, the divisor class group of degree 0 of C to $\mathbb{C}^g/\Lambda_C$ by integrating a basis of holomorphic differentials along paths that form a basis of the first homology group of C. So the period lattice of C is attached to the isomorphism class of $(J_C)_{\text{an}}$.

Definition 5.22 The period matrix Ω_C of Λ_C is called the *period matrix of* C. The form $E(x,y)$ is called the *Riemann form*.

Lemma 5.23 The period matrix Ω_C can be computed by integrating a basis of holomorphic differentials along paths on the Riemann surface corresponding to C.

By duality theorems about differentials and paths on Riemann surfaces one sees:

Proposition 5.24 The Jacobian of a projective irreducible nonsingular curve is a *principally polarized* abelian variety.

5.1.4 Isogenies of abelian varieties over $\mathbb{C}$

We can use the torus representation of abelian varieties to find the algebraic results about torsion points, isogenies and endomorphisms. So assume that $\mathcal{A}$ is analytically given by $T = \mathbb{C}^d/\Lambda$.

First we find a result given previously.

Proposition 5.25 Let n be a natural number. The points of order dividing n of $\mathcal{A}$, $\mathcal{A}[n]$, are isomorphic to the subgroup $\frac{1}{n}\Lambda/\Lambda \subset \mathbb{C}^d/\Lambda$ and hence isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2d}$.

Let G be a subgroup of $\frac{1}{n}\Lambda/\Lambda$. The inverse image of G in $\mathbb{C}^d$ is a lattice Λ_G that contains Λ, and hence we get a quotient map from T to $\mathbb{C}^d/\Lambda_G = T/G$ with kernel isomorphic to G. This quotient map is, by definition of the analytic structure on tori, an analytic map. The Hermitian structure on T induces one on T_G that satisfies the condition from Theorem 5.16 and hence T_G corresponds to an abelian variety $\mathcal{A}_G$.

By Lemma 5.2 the quotient map comes from an algebraic morphism that is an isogeny from $\mathcal{A}$ to $\mathcal{A}_G$ with kernel corresponding to G.

Proposition 5.26 Let $\mathcal{A}$ be an abelian variety defined over $\mathbb{C}$ with lattice $\Lambda \subset \mathbb{C}^d$. The isogenies η of degree n of $\mathcal{A}$ are, up to isomorphisms, in one-to-one correspondence with lattices Λ_η which contain Λ and satisfying $[\Lambda_\eta : \Lambda] = n$. The kernel of η is isomorphic to Λ_η/Λ.

Of special interest are isogenies with image isomorphic to $\mathcal{A}$. For simplicity and since it is in the center of our interest we restrict the discussion to *simple abelian varieties*.

We know that in this case the ring $\mathrm{End}_{\mathbb{C}}(\mathcal{A})$ of endomorphisms of $\mathcal{A}$ is a skew field and that all endomorphisms different from the zero map are isogenies.

We want to use the results of Proposition 5.26 but look at them from a slightly different point of view. In the proposition we interpreted isogenies as quotient maps of the identity map on $\mathbb{C}^d$ with changing lattices. Now we shall *fix the lattice* Λ and study holomorphic additive maps $\alpha : \mathbb{C}^d \to \mathbb{C}^d$. Such a map α induces an endomorphism of $\mathcal{A}$ if and only if it is well defined modulo Λ, i.e., $\alpha(\Lambda) \subset \Lambda$.

Example 5.27 We give the most simple example to explain this. Look at the endomorphism $[n]$ obtained by scalar multiplication with n.

In the first interpretation we take as lattice of the image the lattice $\frac{1}{n}\Lambda$ and take the quotient map from $\mathbb{C}^d/\Lambda$ to $\mathbb{C}^d/\left(\frac{1}{n}\Lambda\right)$.

In the second interpretation we multiply elements in $\mathbb{C}^d$ by n and so the subset $\frac{1}{n}\Lambda$ is mapped to Λ and hence to the zero element of the torus associated to $\mathcal{A}$.

From the condition imposed on α (it has to be continuous) it follows that α is a linear invertible map on the real vector space of dimension $2d$ attached to $\mathbb{C}^d$. Hence (after having chosen a basis $\{\mu_1, \ldots, \mu_{2d}\}$ of Λ) we can describe α by a real invertible $(2d \times 2d)$-matrix B with the additional condition that α maps Λ into itself. But this is equivalent to the condition that B has integers as coefficients. Hence the characteristic polynomial $\chi(\alpha)_{\mathcal{A}}(T)$ of α is a monic polynomial of degree $2d$ with integers as coefficients.

Remark 5.28 The reader should recall that we have described endomorphisms α in the algebraic setting by using Tate modules to produce ℓ-adic representations. One of the crucial results due to Weil is that the characteristic polynomials do not depend on the prime ℓ.

Here we use the period lattice to produce an integral representation again of dimension $2d$. It plays the role of Tate modules in the analytic setting. The resulting characteristic polynomial $\chi_\alpha(T)$ is *the same* as the corresponding ℓ-adic polynomial. This remark will become important for point counting algorithms.

Until now we have only looked at linear algebra and continuity. But we have to take into account the analytic structure that yields holomorphy conditions for α.

We shall explain this in the simplest case.

Example 5.29 Let $\mathcal{A} =: E$ be an elliptic curve. The associated analytic variety is isomorphic to $\mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ with $\tau \notin \mathbb{R}$. A holomorphic additive map α is given by a matrix

$$B = \begin{bmatrix} n_1 & n_2 \\ n_3 & n_4 \end{bmatrix}$$

over $\mathbb{Z}$ if we take $\{1, \tau\}$ as basis, it also represents a multiplication by a complex number β that is determined by $\alpha(1) =: \beta = n_1 + n_2\tau$. Hence it maps τ to $\beta\tau = n_1\tau + n_2\tau^2 = n_3 + n_4\tau$.

Now assume that $n_2 \neq 0$ or, equivalently, that $\beta \notin \mathbb{Z}$. Then τ satisfies the equation

$$n_2\tau^2 + (n_1 - n_4)\tau - n_3 = 0$$

and, hence, $\mathbb{Q}(\tau)$ is an imaginary quadratic field K.

The lattice $\mathbb{Z} + \tau\mathbb{Z}$ is an ideal A_τ of an order of K, and the isogenies correspond to numbers $n_1 + n_2\mathbb{Z}$ that map A_τ into itself. But this means that $\mathrm{End}_{\mathbb{C}}(E)$ is an order (cf. Definition 2.81) in K and that E has complex multiplication.

For higher dimensional abelian varieties $\mathcal{A}$, analogous but more complicated considerations lead to the CM-theory mentioned already in the algebraic part. Again one gets that the lattice of abelian varieties with complex multiplication is very special and that the period matrix has an algebraic structure. This combined with class field theory is the key of the CM method used to construct abelian varieties over finite fields with known number of points. We shall be more precise in the next sections in the case of elliptic and hyperelliptic curves and come to algorithmic details in Chapter 18.

5.1.5 Elliptic curves over $\mathbb{C}$

In this section we shall apply the theory of curves and their Jacobians over $\mathbb{C}$ for elliptic curves E.

5.1.5.a The complex theory of elliptic curves

We recall Corollary 5.18 that the Jacobian variety of E and hence E itself is analytically isomorphic to $\mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ where τ is a complex number with a positive imaginary part.

Let E be given by an affine Weierstraß equation

$$E : y^2 = x^3 + a_4x + a_6 \text{ with } a_4, a_6 \in \mathbb{C}.$$

As a consequence of the theorem of Abel–Jacobi 5.13 we get: there is an analytic isomorphism between the groups $E(\mathbb{C})$ and $\mathbb{C}/\Lambda_E$ where Λ_E is a lattice $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ in $\mathbb{C}$.

We want to describe explicitly this isomorphism. For this we *begin* with the lattice $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ and then construct the elliptic curve corresponding to it. We shall follow closely [COH 2000, Chapter 7] and [SIL 1986, Chapter VI, section 3]. The first step is to find the meromorphic functions.

Definition 5.30 Let $\omega_1, \omega_2 \in \mathbb{C}$ be linearly independent over $\mathbb{R}$. An *elliptic function with periods* $\{\omega_1, \omega_2\}$ is a meromorphic function $f(x)$ on $\mathbb{C}$ such that for all $x \in \mathbb{C}$ one has $f(x + \omega_1) = f(x + \omega_2) = f(x)$.

We shall fix ω_1, ω_2 as well as the lattice Λ spanned by them in the following. Elliptic functions will always be periodic with respect to Λ.

The task is to construct nonconstant elliptic functions. It was solved by Weierstraß.

Definition 5.31 The Weierstraß $\wp$-function is defined by the series

$$\wp(z,\Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \smallsetminus \{0\}} \left(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2} \right). \tag{5.1}$$

This series converges uniformly on every compact subset of $\mathbb{C} \smallsetminus \Lambda$. The function $\wp := \wp(z,\Lambda)$ defined by (5.1) is a meromorphic function on $\mathbb{C}$ with poles (of order 2) in Λ. It is an even function, i.e., $\wp(z,\Lambda) = \wp(-z,\Lambda)$ for all $z \in \mathbb{C} \smallsetminus \Lambda$.

The proofs are straightforward applications of the basics of complex analysis, see e.g., [SIL 1986, Chapter VI, Theorem 3.1].

As usual we denote by $\wp' := \wp'(z,\Lambda)$ the derivative of $\wp$. Again it is an elliptic function. It can be computed easily by using the series defining $\wp$; the result is again a series whose first term is $-\frac{2}{z^3}$. It follows immediately that $\wp'$ is an odd function, i.e., $\wp'(z) = -\wp'(-z)$.

Define the *Eisenstein series* $G_n := G_n(\Lambda)$ of weight n for Λ by

$$G_n(\Lambda) := \sum_{\omega \in \Lambda \smallsetminus \{0\}} \omega^{-n}.$$

The fundamental observation is:

Theorem 5.32 The elliptic functions $\wp$ an $\wp'$ satisfy the equation

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6.$$

This is the affine equation for an elliptic curve E_Λ with function field $\mathbb{C}(\wp, \wp')$. The map

$$\begin{array}{rcl} \Phi : \mathbb{C}/\Lambda & \to & E_\Lambda \subset \mathbb{P}^2 \\ z & \mapsto & \begin{cases} \big(\wp(z) : \wp'(z) : 1\big) & \text{for } z \notin \Lambda \\ \Phi(\Lambda) = (0:1:0) \end{cases} \end{array}$$

is an isomorphism of Riemann surfaces, which is a group homomorphism (using the induced natural additive group structure on $\mathbb{C}/\Lambda$ and the elliptic curve group structure on E_Λ).

Hence E_Λ is the abelian variety attached to the torus $\mathbb{C}/\Lambda$, and we can interpret the map Φ as the inverse of the Abel–Jacobi map from E_Λ as curve to its Jacobian variety which is isomorphic to E_Λ.

Remark 5.33 The equation defining E_Λ is not quite in the standard Weierstraß form. We obtain it if we replace $\wp'$ by $y = 1/2\wp'$ and set $x = \wp$, $g_2 := g_2(\Lambda) := 15G_4(\Lambda)$ and $g_3 := g_3(\Lambda) := 35G_6(\Lambda)$. The resulting equation is

$$E_\Lambda : y^2 = x^3 - g_2 x - g_3.$$

We have seen that for every lattice Λ we can use $g_2(\Lambda)$ and $g_3(\Lambda)$ to obtain the equation of the corresponding elliptic curve E_Λ. The first question is now to describe in terms of the two lattices Λ, Λ' what it means that E_Λ is isomorphic to $E_{\Lambda'}$.

As we have seen in Lemma 5.2 this is equivalent to the question under which conditions $\mathbb{C}/\Lambda$ is analytically isomorphic to $\mathbb{C}_{\Lambda'}$.

Example 5.34 Take $\alpha \in \mathbb{C}^*$ and define the map t_α from $\mathbb{C}$ to $\mathbb{C}$ by $z \mapsto \alpha z$. Define $\Lambda' := \alpha\Lambda$.
Then t_α induces an analytic isomorphism

$$h_\alpha : \mathbb{C}/\Lambda \to \mathbb{C}/\alpha\Lambda.$$

Motivated by the example we define that two lattices Λ_1 and Λ_2 are *homothetic* if there is an $\alpha \in \mathbb{C}^*$ such that $\alpha\Lambda_1 = \Lambda_2$.

Theorem 5.35 There is a canonical isomorphism between the set of $\mathbb{C}$-isomorphism classes of elliptic curves and the set of homothety classes of lattices in $\mathbb{C}$.

Corollary 5.36 Let Λ be a lattice in $\mathbb{C}$ with basis $\{\omega_1, \omega_2\}$. We can assume (by replacing ω_1 by $-\omega_1$ if necessary) that $\tau := \omega_2/\omega_1$ is a complex number with positive imaginary part. Let Λ_τ be the lattice $\mathbb{Z} + \tau\mathbb{Z}$. Then the elliptic curve E_Λ is isomorphic to E_{Λ_τ}.

By this result we have attached to every (isomorphism class of) elliptic curves over $\mathbb{C}$ a unique lattice $\Lambda_\tau := \mathbb{Z} + \tau\mathbb{Z}$ such that E is isomorphic to $E_{\mathbb{Z}+\tau\mathbb{Z}} =: E_\tau$ with $\tau \in \mathbb{C}$ with imaginary part $\Im m(\tau) > 0$. But τ is not uniquely determined by Λ_τ.

Lemma 5.37 Let τ, τ' be complex numbers with positive imaginary part. Then $\Lambda_\tau = \Lambda_{\tau'}$ if and only if there exist integers a, b, c, d with $ad - bc = 1$ and $\tau' = \frac{a\tau+b}{c\tau+d}$.

Definition 5.38 A complex function f which is holomorphic on the upper half plane

$$\mathcal{H} := \{\tau \in \mathbb{C} \mid \Im m(\tau) > 0)\}$$

and which satisfies

$$f(\tau) = f\left(\frac{a\tau + b}{c\tau + d}\right)$$

for all integers a, b, c, d with $ad - bc = 1$ is called a *modular function*.

The set of modular functions forms a field F_1.

Example 5.39 Define

$$\begin{aligned} j : \mathcal{H} &\to \mathbb{C} \\ \tau &\mapsto j(\tau) := 1728\frac{g_2(\Lambda_\tau)^3}{4g_2(\Lambda_\tau)^3 - 27g_3(\Lambda_\tau)^2}. \end{aligned}$$

Then $j \in F_1$.

Theorem 5.40

(i) The field of modular functions is equal to $\mathbb{C}(j)$.
(ii) The elliptic curve E_τ is isomorphic to $E_{\tau'}$ if and only if $j(\tau) = j(\tau')$.
(iii) Let E be an elliptic curve defined over $\mathbb{C}$ with absolute invariant j_E (cf. Corollary 4.118) Then there is a $\tau \in \mathcal{H}$ with $j(\tau) = j_E$ and E is isomorphic to E_τ.

Since $j \in F_1$ we have $j(\tau + 1) = j(\tau)$. (Take $a = 1, b = 1, c = 0, d = 1$.) We can use this identity to develop j into a Laurent series "at ∞."

Define $q := e^{2\pi i\tau}$ and $j^*(q) := j(\tau)$. Observe that q approaches 0 when $\Im m(\tau)$ becomes large. It turns out that j^* can be extended to a meromorphic function with a pole in 0 of order 1. Its Laurent series has integer coefficients. It is called the *q-expansion of the j-function.*

Proposition 5.41 The q-expansion of the j-function is given by

$$j(q) = \frac{(1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n)^3}{q \prod_{n \in \mathbb{N}} (1 - q^n)^{24}}.$$

For a proof we refer to [SIL 1994, Chapter I, Remark 7.4.2].

After having an explicit description of isomorphism classes of elliptic curves over $\mathbb{C}$ we now determine the *isogeny classes* again by using the theory of complex tori (see Section 5.26) applied to elliptic curves and get:

Proposition 5.42 Let E and E' be two elliptic curves defined over $\mathbb{C}$ with lattices Λ (respectively Λ').

Then E is isogenous to E' if and only if there exists an $\alpha \in \mathbb{C}^*$ with $\alpha\Lambda \subset \Lambda'$. If so denote by η_α the isogeny from E to E'. Then the kernel of η_α is canonically isomorphic to $\alpha^{-1}\Lambda'/\Lambda$.

Corollary 5.43 Assume that E is an elliptic curve over $\mathbb{C}$ with $j_E = j(\tau)$. Then

$$\mathrm{End}_{\mathbb{C}}(E) = \{\alpha \in \mathbb{C} \mid \alpha\Lambda_\tau \subset \Lambda_\tau\}.$$

5.1.5.b Elliptic curves with complex multiplication

The ring

$$\mathrm{End}_{\mathbb{C}}(E) = \{\alpha \in \mathbb{C} \mid \alpha\Lambda_\tau \subset \Lambda_\tau\}$$

always contains and in general will be equal to $\mathbb{Z}$.

We reformulate the definition of complex multiplication (cf. Definition 4.88) applied to elliptic curves E over $\mathbb{C}$.

Definition 5.44 The elliptic curve E has complex multiplication if and only if $\mathrm{End}_{\mathbb{C}}(E)$ is larger than $\mathbb{Z}$.

In Example 4.90 we have already discussed that this implies:

Corollary 5.45 Let E be an elliptic curve defined over $\mathbb{C}$ with period τ. Then τ is a *nonrational integer in an imaginary quadratic field* K_τ and $\mathrm{End}_{\mathbb{C}}(E)$ is the *order corresponding to* $\mathbb{Z} + \tau\mathbb{Z}$ in K_τ.

The converse is true as well.

Proposition 5.46 Let K be an imaginary quadratic field, let $\mathcal{O}$ be an order of K, and let A be an ideal of $\mathcal{O}$. Then $A \subset \mathbb{C}$ is a lattice, the elliptic curve $E_A := \mathbb{C}/A$ is an elliptic curve with complex multiplication and $\mathrm{End}_{\mathbb{C}}(E_A) = \mathcal{O}$. For two ideals A, A' of $\mathcal{O}$ we get: E_A is isomorphic to $E_{A'}$ over $\mathbb{C}$ (i.e., the absolute j-invariants are equal) if and only if A and A' are in the same ideal class.

So elliptic curves with complex multiplication have *algebraic* periods τ. But even more important we get that the absolute invariant $j(\tau)$ is a very special algebraic integer, i.e., it is the zero of a monic polynomial over $\mathbb{Z}$, and is obtained as j-invariant of an ideal in an imaginary quadratic field. The exact statement is the key result of class field theory of imaginary quadratic fields.

Theorem 5.47 Assume that E is defined over $\mathbb{C}$ and has complex multiplication. Let τ be its period. Then $\mathbb{Q}(\tau)$ is an imaginary quadratic field, $\mathrm{End}_{\mathbb{Q}(\tau)}(E) = \mathrm{End}_{\mathbb{C}}(E)$ is an order $\mathcal{O}_E$ in $\mathbb{Q}(\tau)$ and the absolute invariant $j(\tau)$ is an algebraic integer that lies in the ring class field $H_{\mathcal{O}_E}$ over $\mathbb{Q}(\tau)$. The invariant $j(\tau)$ is the j-function evaluated at an ideal of $\mathcal{O}_E$.

Recall that the ring class field of $\mathcal{O}_E$ is an abelian extension of $\mathbb{Q}(\tau)$ whose Galois group is isomorphic in a canonical way to the ideal class group of $\mathcal{O}_E$. The most important case for us will be that $\mathcal{O}_E$ is the ring of integers $\mathcal{O}$ of $\mathbb{Q}(\tau)$. Then $H_{\mathcal{O}_E}$ is the *Hilbert class field* H of $\mathbb{Q}(\tau)$, the maximal Galois extension of $\mathbb{Q}(\tau)$, which is unramified and has an abelian Galois group. In particular, we get that the degree of H over $\mathbb{Q}(\tau)$ is equal to the order of $\mathrm{Cl}(\mathcal{O})$, which is called the class number of $\mathbb{Q}(\tau)$.

On the other side it follows easily from Theorem 5.35 that j_{E_A} depends only on the ideal class group of A in $\mathrm{Cl}(\mathcal{O})$ and class field theory tells us that all the algebraic numbers j_{E_A} are conjugates under the action of the Galois group of H over $\mathbb{Q}(\tau)$. From this we get:

Corollary 5.48 Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field with ring of integers $\mathcal{O}$. Let E be an elliptic curve with $\mathrm{End}_{\mathbb{C}}(E) = \mathcal{O}$. Then the minimal polynomial of j_E is the *Hilbert class polynomial*

$$H_d(x) := \prod_{i=1}^{h_d} \big(x - j(A_i)\big)$$

where $j(A_i)$ is the j-invariant of the elliptic curve corresponding to A_i, the number h_d is the order of the ideal class group of K and A_i are representatives of elements of the class group of $\mathcal{O}$. The coefficients of the Hilbert class polynomial are rational numbers. As j_E is an algebraic integer, they are integers.

For the proof of Theorem 5.47 and Corollary 5.48, see for example [SIL 1986, Appendix C, Theorem 11.2], or [LAN 1973, Chapter 10, Theorem 1].

Reduction of elliptic curves with complex multiplication

In Section 5.2 below we shall discuss elliptic curves over finite fields. The determination of the order of the rational points will be one of the most important topics in this part. Here we can give a bridge from elliptic curves over number fields to elliptic curves over finite fields.

The class polynomial

$$H_d(x) := \prod_{i=1}^{h_d} \big(x - j(A_i)\big)$$

can be reduced modulo a prime p to a polynomial $H_d(x)_p$ defined over $\mathbb{F}_p$, and it has simple roots if p does not divide d.

Let $\mathbb{F}_{p^r}$ be the smallest field that contains a root j_p of $H_d(x)_p$. It is the reduction modulo p of one of the invariants $j(A_i)$. As the elements $j(A_i)$ are conjugate it follows that all roots of $H_d(x)_p$ are in this field.

By the algebraic theory of elliptic curves we know that there are elliptic curves E_p defined over $\mathbb{F}_{p^r}$ with absolute invariant j_p. The curve E_p is determined up to twists, and if $j_p \neq 0, 12^3$ there is exactly one twist of E_p.

For the sake of simplicity we shall assume now that $r = 1$ and that the prime number p is decomposed in $\mathbb{Q}(\sqrt{-d})$. Class field theory of imaginary quadratic fields gives the following remarkable result.

Theorem 5.49 There is an integer $\pi \in \mathbb{Q}(\sqrt{-d})$ such that $\pi\overline{\pi} = p$ and $|p + 1 - (\pi + \overline{\pi})|$ is the number of $\mathbb{F}_p$-rational points on either E_p or one of its twists.

To understand this theorem one needs the theory of elliptic curves over finite fields and in particular of the Frobenius endomorphism and its related characteristic polynomial (cf. Example 4.87) made explicit in Example 5.83. The theorem then states that the algebraic integer π, interpreted

as endomorphism of $E_{j(A_i)}$ operates modulo p on E_p or one of its twists as Frobenius endomorphism, and so the characteristic polynomial of π, interpreted as an algebraic number, is equal to the characteristic polynomial of the Frobenius endomorphism.

5.1.6 Hyperelliptic curves over $\mathbb{C}$

5.1.6.a Periods and invariants

Let C be a hyperelliptic curve of genus g defined over $\mathbb{C}$ with Jacobian variety J_C. As we know J_C is as analytic variety isomorphic to a torus $\mathbb{C}^g/\Lambda_C$. Since J_C is principally polarized Λ_C can be chosen in the form $\mathbb{Z}^d \oplus \Omega \cdot \mathbb{Z}^d$, where the $(g \times g)$-matrix Ω is symmetric and has a positive definite imaginary part, i.e., lies in the Siegel upper half plane $\mathbb{H}_g$.

The matrix Ω is the *period matrix of* C. It can be computed by integrating a basis of holomorphic differentials along paths on the Riemann surface corresponding to C. Since such a basis is explicitly known for hyperelliptic curves (see Chapter 17) it is in principle possible to compute it. For elliptic curves E this gives the period τ, a complex number with a positive imaginary part.

The next step for elliptic curves was to determine the isomorphism class when the period is known. This task was solved by the j-function whose value at τ is the absolute invariant of E. To construct j we used Eisenstein series as special functions on lattices, i.e., modular forms.

Analogous to the elliptic curve case we define values of complex functions to lattices that are now *Siegel modular forms*: let $\Omega \in \mathbb{H}_g$ the period matrix of a principally polarized abelian variety and let $z \in \mathbb{C}^g$ be a column vector. The Riemann theta function is given by

$$\theta(z,\Omega) = \sum_{\mathbf{n}\in\mathbb{Z}^g} \exp\bigl(\pi i(\mathbf{n}^t\Omega\mathbf{n} + 2\mathbf{n}^t z)\bigr).$$

This function is $\mathbb{C}$-valued, holomorphic and symmetric, i.e., $\theta(z,\Omega) = \theta(-z,\Omega)$.

For fixed $\Omega \in \mathbb{H}_g$ we get a function from $\mathbb{C}^g$ to $\mathbb{C}$ and we define the *Riemann theta divisor* by

$$\Theta^{(\Omega)} := \bigl\{ z \bmod \Lambda \mid \theta(z,\Omega) = 0 \bigr\}.$$

Recall that τ and τ' define isomorphic elliptic curves if and only if $\tau' = \frac{a\tau+b}{c\tau+d}$ with $a,b,c,d \in \mathbb{Z}$ and $ad - bc = 1$, i.e., if τ and τ' are equivalent under the action of $\mathrm{SL}_2(\mathbb{Z})$, the group of invertible (2×2)-matrices over $\mathbb{Z}$ with determinant 1.

An analogous result holds for arbitrary dimension. We define $\mathrm{Sp}(2g,\mathbb{Z})$ to be the *symplectic group* of dimension g over $\mathbb{Z}$. (For $g = 1$ this is $\mathrm{SL}_2(\mathbb{Z})$.) It acts on $\mathbb{H}_g$ in a natural way (cf. [LAN 1982]).

Theorem 5.50 Two period matrices Ω, Ω' define isomorphic principally polarized abelian varieties if and only if they lie on the same orbit under the operation of the symplectic group $\mathrm{Sp}(g,\mathbb{Z})$ on $\mathbb{H}_g$.

For a proof see [LAN 1982].

The theta divisors of two equivalent period matrices Ω, Ω' do not have to be equal. But if they are equivalent then there exists an $a \in \Omega\bigl(\frac{1}{2}\mathbb{Z}^g\bigr) + \frac{1}{2}\mathbb{Z}^g$ such that $\Theta^{(\Omega')} = \Theta_a^{(\Omega)}$ where $\Theta_a^{(\Omega)}$ denotes the translation of $\Theta^{(\Omega)}$ by a.

This motivates the introduction of *theta characteristics*

$$\theta\begin{bmatrix}\delta\\ \epsilon\end{bmatrix}(z,\Omega) = \sum_{\mathbf{n}\in\mathbb{Z}^g} \exp\left(\pi i\left(\mathbf{n}+\frac{1}{2}\delta\right)^t \Omega\left(\mathbf{n}+\frac{1}{2}\delta\right) + 2\left(\mathbf{n}+\frac{1}{2}\delta\right)^t\left(z+\frac{1}{2}\epsilon\right)\right) \qquad (5.2)$$

with column vectors δ and $\epsilon \in (\mathbb{Z}/2\mathbb{Z})^g$. If we fix δ, ϵ and set $z = 0$, we obtain functions on $\mathbb{H}_g$, called the *theta constants*. A theta constant is even, if $\delta^t\epsilon \equiv 0 \pmod 2$, and odd otherwise. All

odd theta constants vanish for principally polarized varieties. There are $2^{g-1}(2^g+1)$ even theta constants.

Theorem 5.51 The complete set of theta constants uniquely determines the isomorphism class of a principally polarized abelian variety of dimension g.

The proof is given in [IGU 1960].

Example 5.52 For $g=2$ there are 10 even theta constants. A list of the vectors $\delta,\epsilon \in (\mathbb{Z}/2\mathbb{Z})^2$ used to get them is found in [WEN 2003]. For $g=3$ there are 32 even theta constants.

By the theta constants we have found a complete system of invariants for isomorphism classes of principally polarized abelian varieties of dimension $g \geqslant 2$. But two things are disturbing. First these invariants are not "independent." Secondly and worse they are defined analytically. But they define points in an algebraic variety, the *moduli space of isomorphism classes of principally polarized abelian varieties of dimension g*. So we would like to have algebraically defined invariants.

For $g=2,3$ we can make this precise. Due to results of Weil [WEI 1957] we know that every principally polarized abelian variety $\mathcal{A}$ of dimension $g \leqslant 3$ is the Jacobian variety of a curve C. Because of the famous theorem of Torelli, the isomorphism class of $\mathcal{A}$ *with its polarization* is determined uniquely by the isomorphism class of C. So the invariants have to be algebraic expressions in the coefficients of the equation defining C. Recall that for elliptic curves E we can express j_E by the coefficients g_2, g_3 of a Weierstraß equation.

In fact we can find these algebraic invariants for hyperelliptic curves of genus 2 and 3 using work of Igusa [IGU 1960] and Shioda [SHI 1967].

5.1.6.b Hyperelliptic curves of genus 2

For every principally polarized abelian variety $\mathcal{A}$ of dimension two there exist three absolute invariants j_1, j_2, and j_3 called *Igusa invariants*, which determine its isomorphism class. They can be expressed in terms of the theta constants. The explicit formulas can be found in [WEN 2003, Section 5].

Let $C: y^2 = x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$ be the curve with $J_C = \mathcal{A}$. Then the invariants j_i of the Jacobian of C can be expressed by

$$j_1 = I_2^5/I_{10},\ j_2 = I_2^3 I_4/I_{10} \text{ and } j_3 = I_2^2 I_6/I_{10}, \tag{5.3}$$

where the I_i's are given below expressed in the coefficients of the curve.

By Spallek [SPA 1994, p. 71] the absolute invariants I_i are given in terms of the coefficients f_j as

$$\begin{aligned}
I_2 &= 6f_3^2 - 16f_4f_2 + 40f_1,\\
I_4 &= 4\big(f_4^2f_2^2 - 3f_3f_2^2 - 3f_4^2f_3f_1 + 9f_3^2f_1 + f_4f_2f_1 - 20f_1^4 + 12f_4^3f_0 - 45f_4f_3f_0 + 75f_2f_0\big),\\
I_6 &= -2\big(-4f_4^2f_3^2f_2^2 + 12f_3^3f_2^2 + 12f_4^3f_2^3 - 38f_4f_3f_2^3 + 18f_2^4 + 12f_4^2f_3^3f_1 - 36f_3^4f_1\\
&\quad - 38f_4^3f_3f_2f_1 + 119f_4f_3^2f_2f_1 - 14f_4^2f_2^2f_1 - 13f_3f_2^2f_1 + 18f_4^4f_1^2 - 13f_4^2f_3f_1^2 - 88f_3^2f_1^2\\
&\quad - 32f_4f_2f_1^2 + 160f_1^4 - 30f_4^3f_3^2f_0 + 99f_4f_3^3f_0 + 80f_4^4f_2f_0 - 246f_4^2f_3f_2f_0 - 165f_3^2f_2f_0\\
&\quad + 320f_4f_2^2f_0 - 308f_4^3f_1f_0 + 930f_4f_3f_1f_0 - 800f_2f_1f_0 + 450f_4^2f_0^2 - 1125f_3f_0^2\big),\\
I_{10} &= f_4^2f_3^2f_2^2f_1^2 - 4f_3^3f_2^2f_1^2 - 4f_4^3f_2^3f_1^2 + 18f_4f_3f_2^3f_1^2 - 27f_2^4f_1^2 - 4f_4^2f_3^3f_1^3 + 16f_3^4f_1^3\\
&\quad + 18f_4^3f_3f_2f_1^3 - 80f_4f_3^2f_2f_1^3 - 6f_4^2f_2^2f_1^3 + 144f_3f_2^2f_1^3 - 27f_4^4f_1^4 + 144f_4^2f_3f_1^4\\
&\quad - 128f_3^2f_1^4 - 192f_4f_2f_1^4 + 256f_1^5 - 4f_4^2f_3^2f_2^3f_0 + 16f_3^3f_2^3f_0 + 16f_4^3f_2^4f_0 - 72f_4f_3f_2^4f_0\\
&\quad + 108f_2^5f_0 + 18f_4^2f_3^3f_2f_1f_0 - 72f_3^4f_2f_1f_0 - 80f_4^3f_3f_2^2f_1f_0 + 356f_4f_3^2f_2^2f_1f_0\\
&\quad + 24f_4^2f_2^3f_1f_0 - 630f_3f_2^3f_1f_0 - 6f_4^3f_3^2f_1^2f_0 + 24f_4f_3^3f_1^2f_0 + 144f_4^4f_2f_1^2f_0\\
&\quad - 746f_4^2f_3f_2f_1^2f_0 + 560f_3^2f_2f_1^2f_0 + 1020f_4f_2^2f_1^2f_0 - 36f_4^3f_1^3f_0 + 160f_4f_3f_1^3f_0
\end{aligned}$$

$$
\begin{aligned}
&- 1600 f_2 f_1^3 f_0 - 27 f_4^2 f_3^4 f_0^2 + 108 f_3^5 f_0^2 + 144 f_4^3 f_3^2 f_2 f_0^2 - 630 f_4 f_3^3 f_2 f_0^2 - 128 f_4^4 f_2^3 f_0^2 \\
&+ 560 f_4^2 f_3 f_2^2 f_0^2 + 825 f_3^2 f_2^2 f_0^2 - 900 f_4 f_2^3 f_0^2 - 192 f_4^4 f_3 f_1 f_0^2 + 1020 f_4^2 f_3^2 f_1 f_0^2 \\
&- 900 f_3^3 f_1 f_0^2 + 160 f_4^3 f_2 f_1 f_0^2 - 2050 f_4 f_3 f_2 f_1 f_0^2 + 2250 f_2^2 f_1 f_0^2 - 50 f_4^2 f_1^2 f_0^2 \\
&+ 2000 f_3 f_1^2 f_0^2 + 256 f_4^5 f_0^3 - 1600 f_4^3 f_3 f_0^3 + 2250 f_4 f_3^2 f_0^3 + 2000 f_4^2 f_2 f_0^3 - 3750 f_3 f_2 f_0^3 \\
&- 2500 f_4 f_1 f_0^3 + 3125 f_0^4.
\end{aligned}
$$

Hence we can compute the invariants j_i of the curve C if we know either its period matrix or the curve equation. Conversely, from the invariants we get a system of polynomial equations for the coefficients of an equation defining C and we can solve this system in principle, e.g., by applying Buchberger's algorithm.

But there is a much more efficient way due to Mestre [MES 1991].

To use it we have to define new invariants, which we call *Mestre's invariants*. In his paper, Mestre introduces the invariants A, B, C, D [MES 1991] and invariants j_1', j_2', j_3' with

$$j_1' = A^5/D,\ j_2' = A^3 B/D \text{ and } j_3' = A^2 C/D$$

which satisfy

$$j_1' = \frac{-j_1}{120^5}, j_2' = \frac{720 j_1'}{6750} - \frac{j_2}{(120^3 \times 6750)}, j_3' = \frac{j_3}{120^2 \times 2025100} + \frac{1080 j_2'}{2025} - \frac{16 j_1'}{375}.$$

In addition we need

$$\alpha = \frac{-1}{4556250}\left(\frac{1}{j_1'} + 62208\right) + \frac{16 j_2'}{75 j_1'} + \frac{16 j_3'}{45 j_1'} - 2\frac{{j_2'}^2}{3 j_1' 2} - \frac{4 j_2' j_3'}{3 {j_1'}^2}$$

which relates Mestre's invariant D with Igusa's discriminant Δ by $\alpha = \frac{D}{\Delta}$.

Next one defines a conic $\mathcal{Q}(j_1, j_2, j_3)$ by the equation

$$\sum_{1 \leqslant i,k \leqslant 3} Q_{ik} x_i x_k = 0$$

with

$$
\begin{aligned}
Q_{11} &= \frac{6 {j'}_3 + {j'}_2}{3 {j'}_1}, \\
Q_{12} &= Q_{21} = \frac{2\left({j_2'}^2 + j_1' j_3'\right)}{3 {j_1'}^2}, \\
Q_{13} &= Q_{31} = Q_{22}\alpha \\
Q_{23} &= Q_{32}\frac{1}{{j_1'}^2}\left(\frac{{j_2'}^3}{3 j_1'} + \frac{4 j_2' j_3'}{9} + \frac{2 {j_3'}^2}{3}\right), \\
Q_{33} &= \frac{1}{{j_1'}^2}\left(\frac{j_1' j_2' \alpha}{2} + \frac{2 {j_2'}^2 j_3'}{9 {j'}_1} + \frac{2 {j_3'}^2}{9}\right).
\end{aligned}
$$

This conic is intersected with a cubic $\mathcal{H}(j_1, j_2, j_3)$ given by the equation

$$\sum_{1 \leqslant i,k,l \leqslant 3} H_{ikl} x_i x_k x_l$$

where

$$
\begin{aligned}
H_{111} &= \frac{2\left(j_1'j_3' - 6j_2'j_3' + 9{j_1'}^2\alpha\right)}{9{j_1'}^2},\\
H_{112} &= H_{211} = \frac{2{j_2'}^3 + 4j_1'j_2'j_3' + 12j_1'{j_3'}^2 + {j_1'}^3\alpha}{9{j_1'}^3},\\
H_{113} &= H_{311} = H_{131} = H_{122} = \frac{{j_2'}^3 + 4/3j_1'j_2'j_3' + 4{j_2'}^2j_3' + 6j_1'{j_3'}^2 + 3{j_1'}^2j_2'\alpha}{9{j_1'}^3},\\
H_{123} &= \frac{1}{18{j_1'}^3}\left(\frac{2{j_2'}^4}{j_1'} + 4{j_2'}^2j_3' + \frac{4j_1'{j_3'}^2}{3} + 4j_2'{j_3'}^2 + 3{j_1'}^2j_2'\alpha + 12{j_1'}^2j_3'\alpha\right),\\
H_{133} &= H_{313} = H_{331} = \frac{1}{18{j_1'}^3}\left(\frac{{j_2'}^4}{j_1'} + \frac{4{j_2'}^2j_3'}{3} + \frac{16{j_2'}^3j_3'}{3j_1'} + \frac{26j_2'{j_3'}^2}{3} + 8{j_3'}^3 + 3j_1'{j_2'}^2\alpha + 2{j_1'}^2j_3'\alpha\right),\\
H_{222} &= \frac{1}{9{j_1'}^3}\left(\frac{3{j_2'}^4}{j_1'} + 6{j_2'}^2j_3' + \frac{8j_1'{j_3'}^2}{3} + 2j_2'{j_3'}^2 - 3{j_1'}^2j_3'\alpha\right),\\
H_{223} &= H_{232} = H_{322} = \frac{1}{18{j_1'}^3}\left(-\frac{2{j_2'}^3j_3'}{3j_1'} - \frac{4j_2'{j_3'}^2}{3} - 4{j_3'}^3 + 9j_1'{j_2'}^2\alpha + 8{j_1'}^2j_3'\alpha\right),\\
H_{233} &= H_{323} = H_{332} = \frac{1}{18{j_1'}^3}\left(\frac{{j_2'}^5}{{j_1'}^2} + \frac{2{j_2'}^3j_3'}{j_1'} + \frac{8j_2'{j_3'}^3}{9} + \frac{2{j_2'}^2{j_3'}^2}{3j_1'} - j_1'j_2'j_3'\alpha + 9{j_1'}^3\alpha^2\right),\\
H_{333} &= \frac{1}{36{j_1'}^3}\left(-\frac{2{j_2'}^4j_3'}{{j_1'}^2} - \frac{4{j_2'}^2{j_3'}^2}{j_1'} - \frac{16{j_3'}^3}{9} - \frac{4j_2'{j_3'}^3}{j_1'} + 9{j_2'}^3\alpha + 12j_1'j_2'j_3'\alpha + 20j_1'{j_3'}^2\alpha\right).
\end{aligned}
$$

Note that this is easily done if the conic has a rational point. Then the set of points on the conic can be parameterized by a parameter t. So in the worst case we have to go to a quadratic extension of K to perform this step. The intersection consists of six points that are the zeroes of a polynomial $f(t)$ of degree 6 in the parameter t.

Lemma 5.53 (Mestre) The curve C with Igusa invariants $\{j_1, j_2, j_3\}$ can be given by the equation

$$y^2 = f(x).$$

where f is the polynomial of degree 6 constructed above.

We note that this is not the standard form for an equation of genus 2. But we can transform one of the zeroes of $f(x)$ to be the infinite point on C and then find an equation

$$y^2 = \bar{f}(x)$$

with $\bar{f}$ a polynomial of degree 5 for the curve C.

Until now we have done all computations over $\mathbb{C}$. But Mestre's result is a purely algebraic one, and so we get:

Theorem 5.54 Let $\mathcal{A}$ be a principally polarized abelian variety defined over $\mathbb{C}$ with Igusa invariants $\{j_1, j_2, j_3\}$. Let $K_0 \subset \mathbb{C}$ be a field containing these invariants and such that the conic $\mathcal{Q}(j_1, j_2, j_3)$ has a K_0-rational point. Then $\mathcal{A}$ is the Jacobian variety of a curve C of genus 2 defined over K_0. Its equation is

$$y^2 = f(x),$$

where $f(x)$ is the polynomial of degree 6 from Lemma 5.53.

Let K be an extension field of K_0 such that $f(x)$ has a zero x_0 in K. Then C as curve over K can be given by the equation

$$y^2 = \bar{f}(x)$$

which is obtained by transforming the point $(x_0, 0)$ to infinity.

5.1.6.c Hyperelliptic curves of genus 3

Let $\mathcal{A}$ be a principally polarized abelian variety of dimension 3. We assume that we know its period matrix. So we know the theta constants and, by using a theorem of Mumford–Poor, we can decide whether it is the Jacobian of a hyperelliptic curve (cf. [WEN 2001a, Theorem 4.3]. If so we want to find the equation of the corresponding curve given in the form

$$C : y^2 = f(x)$$

where $f(x)$ is a polynomial of degree 7.

In principle we can proceed as in the case of genus 2. Only things become more complicated. One way proposed in [WEB 1997] is as follows. First one computes the *Rosenhain model*

$$y^2 = x(x - \lambda_1) \cdots (x - \lambda_7)$$

of C where the complex numbers λ_i are rational expressions in theta constants. Having this equation one computes the *Shioda invariants* j_1, j_3, j_5, j_7, j_9, which determine the isomorphism class of C as curve over $\mathbb{C}$.

Then a variant of Mestre's method allows us to find an equation for C that is defined over field of degree $\leqslant 2$ over $\mathbb{Q}(j_1, j_3, j_5, j_7, j_9)$. For details we refer to [WEB 1997] and [WEN 2001a].

Remarks 5.55

(i) In [WEB 1997] the theoretical results and the algorithms to compute curves are given for hyperelliptic curves of genus $\leqslant 5$.

(ii) In the elliptic case we went further. By using the Weierstraß $\wp$ function and its derivative we were able to make (the inverse of) the Abel–Jacobi map explicit. In [KAM 1991] it is shown that an analogous definition of Weierstraß functions and its higher derivatives can be used to achieve this for hyperelliptic curves of any genus.

5.1.6.d Hyperelliptic curves of genus 2 and 3 with CM

In the last section we have seen that the knowledge of the period matrix of a hyperelliptic curve C of genus 2 or 3 makes it possible to compute its invariants and then to determine its equation in an algebraic way.

We shall discuss now how the theory of CM-fields makes it possible to determine the invariants in an algebraic way if J_C has complex multiplication. Though the ideas are quite analogous to those that occurred in the case of complex multiplication of elliptic curves we need considerably more technical details. The key ingredients were developed in the important book of Taniyama–Shimura [SHTA 1961]. The reader who is interested in this deep and beautiful theory is encouraged to use this book as reference for the whole section.

We shall begin by giving a very rough sketch of the general CM theory and then we shall apply it to the special case of Jacobian varieties of hyperelliptic curves of genus 2 and 3.

Abelian varieties to CM-types

A number field K with $[K:\mathbb{Q}] = 2g$ is called *CM-field* if K is an imaginary quadratic extension of a totally real number field K_0.

Let $\varphi_i, 1 \leqslant i \leqslant 2g$ be the $2g$ distinct embeddings from K into $\mathbb{C}$. A tuple

$$(K, \Phi) := \big(K, \{\varphi_1, \varphi_2, \ldots, \varphi_g\}\big)$$

is called CM-type, if all embeddings φ_i are distinct and no two of them are complex conjugate to each other.

Let $\mathcal{A} \simeq \mathbb{C}^g/\Lambda_{\mathcal{A}}$ be an abelian variety over $\mathbb{C}$ with $\mathrm{End}(\mathcal{A}) \otimes \mathbb{Q} \simeq K$. Hence $\mathcal{A}$ has complex multiplication with ring of endomorphisms being an order $\mathcal{O} \subset K$. We have to make the identification of $\mathcal{O}$ with $\mathrm{End}(\mathcal{A})$ more explicit.

Definition 5.56 Assume that the operation of $\alpha \in \mathcal{O}$ on $\mathcal{A}$ is given by the action of

$$\begin{bmatrix} \varphi_1(\alpha) & & \\ & \ddots & \\ & & \varphi_g(\alpha) \end{bmatrix}.$$

on $\mathbb{C}^g$. Then $\mathcal{A}$ is an abelian variety of CM-type $(K, \Phi) = \big(K, \{\varphi_1, \cdots, \varphi_g\}\big)$.

Proposition 5.57 For every abelian variety $\mathcal{A}$ with $\mathrm{End}(\mathcal{A}) \otimes \mathbb{Q} \simeq K$ there exists a CM-type $(K, \Phi) = \big(K, \{\varphi_1, \cdots, \varphi_g\}\big)$.

To ease things we restrict ourselves (as in the case of elliptic curves) to the case that $\mathrm{End}(\mathcal{A}) = \mathcal{O}_K$, the ring of integers in K.

Theorem 5.58 Let $\mathfrak{A}$ be an ideal in $\mathcal{O}_K$ and let (K, Φ) be a CM-type. Take

$$\Phi(\mathfrak{A}) := \Big\{ \big(\varphi_1(\alpha), \ldots, \varphi_g(\alpha)\big)^t \mid \alpha \in \mathfrak{A} \Big\}$$

in $\mathbb{C}^g$.

Then $\Phi(\mathfrak{A})$ is a lattice in $\mathbb{C}^g$ and the torus $\mathbb{C}^g/\Phi(\mathfrak{A})$ is an abelian variety $\mathcal{A}_{\mathfrak{A},\Phi}$ which has complex multiplication by $\mathcal{O}_K$.

The action of $\mathcal{O}_K$ on $\mathbb{C}^g/\Phi(\mathfrak{A})$ is given by the action of the g-tuple

$$\begin{bmatrix} \varphi_1(\gamma) & & \\ & \ddots & \\ & & \varphi_g(\gamma) \end{bmatrix} \text{ with } \gamma \in \mathcal{O}_K$$

on $\mathbb{C}^g$. Conversely every abelian variety $\mathcal{A}$ of CM-type (K, Φ) with complex multiplication by $\mathcal{O}_K$ is isomorphic to an abelian variety $\mathcal{A}_{\mathfrak{A},\Phi}$.

The proof of this theorem can be found in [SHTA 1961].

Principal polarizations

We are interested in Jacobian varieties and corresponding curves with complex multiplications and so we need a finer structure: we want to construct principally polarized abelian varieties and we have to determine isomorphism classes of abelian varieties *with principal polarizations*. For this it is convenient to make an *additional assumption* that is very often satisfied: the maximal real subfield K_0 of K has class number 1, i.e., the ring of integers $\mathcal{O}_{K_0}$ is principal.

Lemma 5.59 Assume that the maximal real subfield K_0 in the CM-field K has class number 1. Let (K, Φ) be a CM-type, $\mathfrak{A}$ an ideal of $\mathcal{O}_K$ and $\mathcal{A}_{\mathfrak{A},\Phi}$ the abelian variety attached to these data.

There exists a basis $\{\alpha_1, \ldots, \alpha_{2g}\}$ of $\Phi(\mathfrak{A})$ such that the Riemann form 5.22 is

$$\big[E(\alpha_i, \alpha_j)\big]_{1 \leqslant i,j \leqslant 2n} = \begin{bmatrix} 0 & I_g \\ -I_g & 0 \end{bmatrix}.$$

Hence the period matrix of $\mathcal{A}_{\mathfrak{A},\Phi}$ lies in the Siegel upper half plane $\mathbb{H}_g$ and we can endow $\mathcal{A}_{\mathfrak{A},\Phi}$ with a principal polarization determined by an element γ in K (cf. [LAN 1982]).

For a proof see [WEN 2001b].

Definition 5.60 We take the notations as in the Lemma 5.59. We shall write $(\mathcal{A}_{\mathfrak{A},\Phi}, \gamma)$ for the abelian variety corresponding to the ideal $\mathfrak{A}$, the CM-type Φ and the polarization attached to γ.

As in the case of elliptic curves, we now need a characterization of *isomorphism classes* of abelian varieties with principal polarization that correspond to a given CM-type (K, Φ).

For this we need some notation. Let K be a CM-field with CM-type Φ. We assume that the maximal totally real subfield has class number 1.

Let U^+ denote the totally positive units of K_0 (i.e., units u in $\mathcal{O}_K$ such that for all $1 \leqslant j \leqslant g$ we have $\varphi_i(u)$ is a positive real number). Let U_1 be the image of the norm map from K to K_0 applied to the units in $\mathcal{O}_K$. We denote by $\epsilon_1, \ldots, \epsilon_d$ a system of representatives for U^+/U_1. Note that the complex conjugation $\overline{\ }$ generates the Galois group of K over K_0. Using our assumption that the class number of K_0 is 1 we get that for any ideal $\mathfrak{A}$ of K the ideal $\mathfrak{A}\overline{\mathfrak{A}}$ can be interpreted as a principal ideal (α) of K_0.

Definition 5.61 The subgroup $\mathrm{Cl}'(\mathcal{O}_K)$ of the class group $\mathrm{Cl}(\mathcal{O}_K)$ consists of the ideal classes c that contain an ideal $\mathfrak{A}$ with $\mathfrak{A}\overline{\mathfrak{A}} = \alpha\mathcal{O}_K$ with $\varphi_i(\alpha)$ totally positive, i.e., $\varphi_i(\alpha)$ is a real positive number for every $1 \leqslant i \leqslant g$. The order of $\mathrm{Cl}(\mathcal{O}_K)'$ is denoted by h'_K.

We have the following theorem:

Theorem 5.62 Let $(\mathcal{A}_{\mathcal{O}_K,\Phi}, \gamma)$ be a principally polarized abelian variety attached to $\mathcal{O}_K$. Let $\mathfrak{A}_1, \ldots,$
$\mathfrak{A}_{h'_K}$ be a system of representatives for $\mathrm{Cl}(\mathcal{O}_K)'$ with $\mathfrak{A}_i\overline{\mathfrak{A}_i} = (\alpha_i)$ and α_i totally positive. There are $h'_k d$ isomorphism classes of principally polarized abelian varieties with complex multiplication by $\mathcal{O}_K$ of CM-type (K, Φ).

Let $K_\Phi = \bigcup_{l=1}^{d} K_\Phi^l$ with

$$K_\Phi^l = \big\{(\mathcal{A}_{\mathfrak{A}_i}, \epsilon_l(\alpha_i\gamma)^{-1}) \mid i = 1, \ldots, h'_k\big\}.$$

The set K_Φ is a set of representatives of the isomorphism classes of principally polarized abelian varieties of CM-type (K, Φ).

Warning: principally polarized abelian varieties of different CM-types can be isomorphic.

Example 5.63 Consider the case where the principally polarized abelian variety has dimension two. Here, the CM-field is an imaginary quadratic extension of a real quadratic field K_0.

If K is Galois, we get all isomorphism classes of principally polarized abelian varieties with complex multiplication with $\mathcal{O}_K$ by choosing one CM-type.

If K is non-normal, we need two CM-types to get all isomorphism classes of principally polarized abelian varieties.

Class polynomials for hyperelliptic curves of genus 2 and 3

Recall from the previous paragraph that for elliptic curves with complex multiplication by $\mathcal{O}_K$ the j-invariant lies in the Hilbert class field of the imaginary quadratic field K. Again the situation is analogous but more complicated in the higher dimensional case.

We need the notion of the *reflex CM-field* $\widehat{K}$ ([SHI 1998]), which for $g = 1$ is equal to K and in general different from K. We shall not need the explicit definition of the reflex CM-field but use the arithmetic information from class field theory to determine minimal polynomials for invariants.

Theorem 5.64 Let K be a CM-field of degree 4 over $\mathbb{Q}$.

(i) The *Igusa invariants* $j_1(C), j_2(C), j_3(C)$ for hyperelliptic curves C of genus 2 with complex multiplication with the ring of integers $\mathcal{O}_K$ of K are algebraic numbers that lie in a class field over the reflex CM-field $\widehat{K}$.

(ii) For hyperelliptic curves C and C' with complex multiplication with $\mathcal{O}_K$ we get that for $k \in \{1, 2, 3\}$ the invariants $j_k(C)$ and $j_k(C')$ are Galois conjugates.

(iii) Let $\{C_1, \ldots, C_s\}$ be a set of representatives of isomorphism classes of curves of genus 2 whose Jacobian varieties have complex multiplication with endomorphism ring $\mathcal{O}_K$. We denote by $j_k(i)$ the k-th Igusa invariant belonging to the curve C_i.
The three *class polynomials*

$$H_{K,k}(X) = \prod_{i=1}^{s} \big(X - j_k^{(i)}\big), k = 1, \ldots, 3.$$

have coefficients in $\mathbb{Q}$.

For hyperelliptic curves of genus 3 we get a completely analogous result.

Theorem 5.65 Let K be a CM-field of degree 6 over $\mathbb{Q}$.

(i) The *Shioda invariants* $j_1(C), j_3(C), j_5(C), j_7(C), j_9(C)$ for hyperelliptic curves C of genus 3 with complex multiplication with the ring of integers $\mathcal{O}_K$ of K are algebraic numbers that lie in a class field over the reflex CM-field $\widehat{K}$.

(ii) For hyperelliptic curves C and C' with complex multiplication with $\mathcal{O}_K$ we get that for $k \in \{1, 3, 5, 7, 9\}$ the invariants $j_k(C)$ and $j_k(C')$ are Galois conjugate.

(iii) Let $\{C_1, \ldots, C_s\}$ be a set of representatives of isomorphism classes of curves of genus 3 whose Jacobian varieties have complex multiplication with endomorphism ring $\mathcal{O}_K$. We denote by $j_k(i)$ the k-th Igusa invariant belonging to the curve C_i.
The five *class polynomials*

$$H_{K,k}(X) = \prod_{i=1}^{s} \big(X - j_k^{(i)}\big), \quad k \in \{1, 3, 5, 7, 9\}.$$

have coefficients in $\mathbb{Q}$.

Denominators in the class polynomials

The careful reader will have remarked that — contrary to the elliptic case — we did not claim in Theorems 5.64 and 5.65 that the class polynomials have integer coefficients. In fact this is wrong.

There are two reasons for this. First, small primes occur (for $g = 2$ up to 5 and for $g = 3$ up to 7) because we did not normalize the invariants in a careful enough way. But much more serious is the second reason: it may happen that the Jacobian of a curve has good reduction modulo a place

$\mathfrak{p}$ of the field over which it is defined but the curve does not have good reduction. The curve may become reducible modulo $\mathfrak{p}$.

There are famous conjectures about the arithmetic of curves over number fields related to the ABC-conjecture that this should occur only for places with moderate norm.

In practice this is confirmed. So to compute the coefficients of the class polynomial one computes a real approximation with high precision and then determines the denominator using the continued fraction algorithm.

Reduction of hyperelliptic curves of genus 2 and 3 with complex multiplication

The invariants of a hyperelliptic curves of genus 2 or 3 with complex multiplication with a CM-field K are zeroes of polynomials over $\mathbb{Q}$. Let us choose a prime p that does not divide the denominator of the coefficients of these polynomials. Then we can reduce the class polynomials modulo p.

We can factor the resulting polynomials over $\mathbb{F}_p$ and find zeroes in an extension field $\mathbb{F}_q$. By Galois theory we see that the class polynomials will split in linear factors over $\mathbb{F}_q$. Combining "related" zeroes we get systems of invariants for which the resulting curves C_q have a Jacobian variety with ring of endomorphisms containing an isomorphic copy of $\mathcal{O}_K$.

So, we have very explicit information about the endomorphisms of the Jacobian variety of C_q, which are defined over (possibly a quadratic extension of) $\mathbb{F}_q$. Class field theory of CM-fields can be used to identify the Frobenius endomorphism.

We explain the easiest case, which is the most important one for practical use: we assume that the genus of C_q is equal to 2 and that $q = p$.

Theorem 5.66 Let K be a CM-field of degree 4 and assume that p is a prime $\geqslant 7$, which does not divide the denominator of the class polynomials $H_{K,k}(X) =: H_k(X)$.

- For every $w \in \mathcal{O}_K$ with $w\overline{w} = p$ the polynomials $H_k(X)$ have a linear factor over $\mathbb{F}_p$ corresponding to w.
- Let $\overline{j_k}$ be a zero of $H_k(X)$ modulo p. There are two $\mathbb{F}_p$-isomorphism classes $\mathcal{A}_{p,1}$ and $\mathcal{A}_{p,2}$ of principally polarized abelian varieties over $\mathbb{F}_p$ with Igusa invariants $\overline{j_k}$.
- The principally polarized abelian varieties $\mathcal{A}_{p,1}$ and $\mathcal{A}_{p,2}$ have complex multiplication by $\mathcal{O}_K$.
- The number of $\mathbb{F}_p$-rational points of $\mathcal{A}_{p,m}, m = 1, 2$ is given by

$$\prod_{i=1}^{4}(1 + (-1)^m w_i)$$

  where $w = w_1$ and w_i are conjugates of w.
- The equation $w\overline{w} = p$ with $w \in \mathcal{O}_K$ has (up to conjugacy and sign) at most two different solutions, i.e., for every CM-field of degree 4 there are at most four different possible orders of groups of $\mathbb{F}_p$-rational points of principally polarized abelian varieties, defined over $\mathbb{F}_p$ with complex multiplication by $\mathcal{O}_K$.

For genus 3 an analogous result holds. We refer the interested reader to Weng [WEN 2001a].

5.2 Varieties over finite fields

In this section we shall deal with varieties defined over finite fields. We assume that the ground field K is equal to $\mathbb{F}_q$ with $q = p^d$.

5.2.1 The Frobenius morphism

In this section, we consider two extension fields of $\mathbb{F}_p$. We assume $K = \mathbb{F}_q$ with $q = p^d$, and consider an arbitrary power ϕ_p^k of the absolute Frobenius automorphism, which fixes the elements of $\mathbb{F}_{p^k} \subset \overline{\mathbb{F}}_p$. We recall the definition of the Frobenius endomorphism and its action on varieties over $\mathbb{F}_q$ given in Example 4.39, which we shall need in a slightly more general way.

Take $k \in \mathbb{N}$ and let ϕ_{p^k} be the Frobenius automorphism of the field $\mathbb{F}_{p^k}$, sending $\alpha \in \mathbb{F}_{p^k}$ to $\pi_k(\alpha) = \alpha^{p^k}$. We can extend ϕ_{p^k} to points of projective spaces over $\mathbb{F}_{q^k}$ by sending points $(X_0, \ldots, X_n)$ to $(X_0^{p^k}, \ldots X_n^{p^k})$. We apply ϕ_{p^k} to polynomials with coefficients in the algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$ by applying it to the coefficients.

If V is a projective variety over $\mathbb{F}_q$ with ideal I we can apply ϕ_{p^k} to I and get a variety $\phi_{p^k}(V)$ with ideal $\phi_{p^k}(I)$. The points of V are mapped to points on $\phi_{p^k}(V)$.

The corresponding morphism from V to $\phi_{p^k}(V)$ is called the *Frobenius morphism* with respect to the field $\mathbb{F}_{p^k}$ and is again denoted by ϕ_{p^k}. It is the k-th power of the *absolute Frobenius* ϕ_p.

We note that though ϕ_{p^k} is by definition a Galois group element it induces a *morphism* from V to $\phi_{p^k}(V)$. We recall that in the language of function fields the corresponding rational map $\phi_{p^k}^*$ from $K(\phi_{p^k}(V))$ is given as follows: choose an open affine part of V and affine coordinate functions $x_1, \ldots, x_n$; then the image of $\phi_{p^k}^*$ in $K(V)$ is generated by $x_1^{p^k}, \ldots, x_n^{p^k}$.

It follows that this rational map is purely inseparable of degree $p^{k \dim(V)}$.

In general $\phi_{p^k}(V)$ will not be isomorphic to V. But if d divides k then $V = \phi_{p^k}(V)$ since then $\phi_{p^k}(I) = I$.

Proposition 5.67 Let s be a natural number such that ks is divisible by d. Put $V_0 := V$ and for $i = 1, \ldots, s-1$ define $V_i := \phi_{p^k}(V_{i-1})$.

Then we get the chain of morphisms

$$V = V_0 \stackrel{\phi_{p^k}}{\to} V_1 \stackrel{\phi_{p^k}}{\to} \cdots \stackrel{\phi_{p^k}}{\to} V_{s-1} \stackrel{\phi_{p^k}}{\to} V_s = V$$

each being purely inseparable of degree $p^{k \dim(V)}$.

The composite of the morphisms is $\phi_{p^{ks}}$.

Hence for $k = 1$ we get a decomposition of ϕ_q into a chain in which the absolute Frobenius endomorphism occurs.

5.2.2 The characteristic polynomial of the Frobenius endomorphism

We assume now that C is a projective absolutely irreducible nonsingular curve over $\mathbb{F}_q$ of genus $g \geqslant 1$. As seen above the Frobenius endomorphism operates on the rational functions on C, on the points of C and — by linear continuation — on the divisors of C. It maps principal divisors to principal divisors and preserves the degree of divisors. So it operates in a natural way on $\mathrm{Pic}^0_{C_{\overline{\mathbb{F}}_q}}$, the divisor class group of degree 0 of the curve C over $\overline{\mathbb{F}}_q$.

From the results in the last paragraph and from the fact that the Galois group of $\mathbb{F}_q$ is (topologically) generated by ϕ_q we get:

Proposition 5.68 The Frobenius morphism induces a homomorphism of $\mathrm{Pic}^0_{C_{\overline{\mathbb{F}}_q}}$ and hence an endomorphism, also denoted by ϕ_q, of the Jacobian variety J_C defined over $\mathbb{F}_q$.

This endomorphism is an isogeny that is purely inseparable of degree q^g.

The elements fixed by ϕ_q in $J_{C(\overline{\mathbb{F}}_q)}$ are $J_C(\mathbb{F}_q) = \mathrm{Pic}^0_C$. Hence $J_C(\mathbb{F}_q)$ is the kernel of $\mathrm{Id}_{J_C} - \phi_q$ and $|\mathrm{Pic}^0_C| = \deg(\mathrm{Id}_{J_C} - \phi_q)$.

Now recall that for primes ℓ different from p we have attached a Galois ℓ-adic representation $\tilde{\rho}_{J_C,\ell}$ induced by the action of $G_{\mathbb{F}_q}$ on points of order ℓ^k of J_C Theorem 4.82. In fact, we have to replace the field $\mathbb{F}_p$ by $\mathbb{F}_q$ and the absolute Frobenius endomorphism by the relative one ϕ_q but all the results about ℓ-adic representations of Galois elements and endomorphisms remain true after this change.

We associate to ϕ_q the characteristic polynomial $\chi\big(T_\ell(\phi_q)\big)_{J_C}(T)$ of $\tilde{\rho}_{J_C,\ell}(\phi_q)$, which is a monic polynomial of degree $2g$ with coefficients in $\mathbb{Z}$ and it is *independent* of the choice of ℓ.

Definition 5.69 The polynomial $\chi(\phi_q)_{J_C}(T) := \chi\big(T_\ell(\phi_q)\big)_{J_C}(T)$ is the *characteristic polynomial of the Frobenius endomorphism* ϕ_q on C and of J_C. To simplify notation we also use $\chi(\phi_q)_{\overline{C}}(T)$ to denote it.

Since we know that $\deg([1]-\phi_q) = \chi(\phi_q)_C(1)$ we get:

Corollary 5.70 The order of Pic^0_C, or equivalently, of $J_C(\mathbb{F}_q)$ is equal to $\chi(\phi_q)_C(1)$.

Hence the determination of the number of elements in Pic^0_C is easy if we can compute the characteristic polynomial of the Frobenius endomorphism on C.

The following remark is very useful if we want to compute this polynomial.

Lemma 5.71 For n prime to p the restriction of ϕ_q to $J_C[n]$ has the characteristic polynomial $\chi(\phi_q)_C(T) \pmod n$.

Corollary 5.72 The endomorphism $\chi(\phi_q)_C(\phi_q)$ is equal to the zero map on J_C.

There are two distinguished coefficients of the characteristic polynomial of a linear map: the absolute coefficient, which is (up to a sign) the determinant of the map, and the second highest coefficient, which is the negative of the sum of the eigenvalues and is called the trace of the map.

In our case we know that $\chi(\phi_q)_C(0) = q^g$ since the degree of ϕ_q as endomorphism on J_C is $q^{\dim(J_C)}$.

The trace of $\chi(\phi_q)_C(T)$ is called the *trace of the Frobenius endomorphism on* C and denoted by $\mathrm{Tr}(\phi_q)$.

Example 5.73 Let E be an elliptic curve over $\mathbb{F}_q$. Then $\chi(\phi_q)_E(T) = T^2 - \mathrm{Tr}(\phi_q)T + q$, and so

$$|E(\mathbb{F}_q)| = q + 1 - \mathrm{Tr}(\phi_q).$$

5.2.3 The theorem of Hasse–Weil for Jacobians

The following results are true for arbitrary abelian varieties over finite fields. We shall state them only for Jacobians of curves C of genus $g > 0$.

Definition 5.74 The zeroes $\lambda_1, \ldots, \lambda_{2g}$ of $\chi(\phi_q)_C(T)$ are called the *eigenvalues of the Frobenius* ϕ_q on C and on J_C.

By definition the eigenvalues of ϕ_q are algebraic integers lying in a number field of degree $\leqslant g$.

The product is equal to

$$\prod_{i=1}^{2g} \lambda_i = q^g.$$

Because of the duality on Jacobian varieties (or as a consequence of the theorem of Riemann–Roch [STI 1993]) one can make a finer statement.

Proposition 5.75 We can arrange the eigenvalues of ϕ_q on C such that

$$\text{for all } \; i = 1, \ldots, g \quad \text{we have } \; \lambda_i \lambda_{i+g} = q.$$

But there is a much deeper result. It is the analogue of the famous *Riemann hypothesis* for the Riemann ζ-function and it says that *the absolute value of each eigenvalue λ_i interpreted as a complex number is, for every curve C of arbitrary positive genus g, equal to $\sqrt{q}$.*

This result was proved by Hasse for elliptic curves and by Weil for abelian varieties. A generalization for arbitrary varieties over finite fields was formulated by Weil. One of the greatest achievements of mathematics in the twentieth century was the proof of these Weil conjectures by Deligne.

The general philosophy is that the number of rational points on varieties over finite fields should not differ "too much" from the number of points of the projective spaces of the same dimension, and the difference is expressed in terms of the size of the trace of the Frobenius endomorphism acting on attached vector spaces like Tate modules, or more generally, cohomology groups.

Let us come back to our situation and resume what we know.

Theorem 5.76 Let C be a projective absolutely irreducible nonsingular curve of genus $g > 0$ over $\mathbb{F}_q$. Let $\lambda_1, \ldots, \lambda_{2g}$ be the eigenvalues of the Frobenius endomorphism on C.

(i) Each λ_i is an algebraic integer of degree $\leqslant 2g$.

(ii) We can numerate the eigenvalues such that for $1 \leqslant i \leqslant g$ we have

$$\lambda_i \lambda_{i+g} = q.$$

(iii) For $1 \leqslant i \leqslant 2g$ take any embedding of λ_i into $\mathbb{C}$. Then the complex absolute value $|\lambda_i|$ is equal to $\sqrt{q}$.

For the proof of these fundamental results about the arithmetic of curves and abelian varieties we refer to [STI 1993] or, in a more general frame, to [MUM 1974, pp. 203–207].

Corollary 5.77 Let $C/\mathbb{F}_q$ be a curve of genus g. If

$$J_C(\mathbb{F}_q)[n] \supseteq (\mathbb{Z}/n\mathbb{Z})^t$$

for some $t > g$ then

$$n \mid q - 1.$$

Proof. We find t linear independent $\overline{D}_1, \ldots, \overline{D}_t$ elements in $J_C(\mathbb{F}_q)[n]$, which lie in the eigenspace $\rho_{J_C,n}(\phi_q)$ with eigenvalue $1 \pmod n$. Hence, there is a $1 \leqslant i \leqslant g$ such that λ_i and λ_{i+g} are both equivalent to 1 modulo n. Since $\lambda_i \lambda_{i+g} = q$ we have $q \equiv 1 \pmod n$. □

We can combine this corollary with Theorem 4.73 to get the following proposition.

Proposition 5.78 Let $C/\mathbb{F}_q$ be a curve of genus g. For the structure of the group of $\mathbb{F}_q$-rational points on the Jacobian we have

$$J_C(\mathbb{F}_q)[n] \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_{2g}\mathbb{Z},$$

where $n_i \mid n_{i+1}$ for $1 \leqslant i < 2g$ and for all $1 \leqslant i \leqslant g$ one has $n_i \mid q - 1$.

From the Theorem 5.76 we obtain bounds on the number of points on the curve and its Jacobian.

Corollary 5.79 Let C be as in Theorem 5.76.
Then

$$\left| |\mathrm{Pic}^0_C| - q^g \right| = \left| \prod_{i=1}^{2g} (1-\lambda_i) - q^g \right| = O\left(q^{g-1/2}\right).$$

Take $k \in \mathbb{N}$. Since $\phi_{q^k} = \phi_q^k$ we can extend this result:

Corollary 5.80 The number N_k of $\mathbb{F}_{q^k}$-rational points of J_C, or equivalently, the number of elements in $\mathrm{Pic}^0_{C\cdot\mathbb{F}_{q^k}}$ is estimated by

$$\left| N_k - q^{gk} \right| = \left| \prod_{i=1}^{2g} (1-\lambda_i^k) - q^{gk} \right| = O\left(q^{k(g-1/2)}\right).$$

This corollary can be used to compute the ζ-function of the curve C [STI 1993] and to get a bound for the number of rational points on C.

Corollary 5.81 Let C be as above.
Then

$$| |C(\mathbb{F}_q)| - q - 1| \leqslant 2g\sqrt{q}.$$

The estimates for the number of elements of Pic^0_C and of $C(\mathbb{F}_q)$ are called the *Hasse–Weil bounds*.
In fact the Serre bound gives the sharper estimate

$$| |C(\mathbb{F}_q)| - q - 1| \leqslant g\lfloor 2\sqrt{q} \rfloor.$$

When one wants to compute the characteristic polynomial of the Frobenius endomorphism it is very important that one has *ad hoc* estimates for the size of the coefficients of this polynomial. Again Theorem 5.76 can be used in an obvious way to get

Corollary 5.82 The characteristic polynomial of ϕ_q has a very symmetric shape given by

$$\chi(\phi_q)_C(T) = T^{2g} + a_1 T^{2g-1} + \cdots + a_g T^g + \cdots + a_1 q^{g-1} T + q^g,$$

where $a_i \in \mathbb{Z}, 1 \leqslant i \leqslant g$.
The absolute value of the i-th coefficient of $\chi(\phi_q)_C(T)$ is bounded by $\binom{2g}{i} q^{(2g-i)/2}$.

Example 5.83 Let E be an elliptic curve over $\mathbb{F}_q$. The eigenvalues λ_1 and λ_2 of ϕ_q on E are algebraic integers of degree $\leqslant 2$ with absolute value $|\lambda_i| = \sqrt{q}$ and $\lambda_1\lambda_2 = q$. The number of points in $E(\mathbb{F}_q)$ is estimated by

$$| |E(\mathbb{F}_q)| - q - 1| \leqslant 2\sqrt{q}.$$

The interval $[-2\sqrt{q} + q + 1, 2\sqrt{q} + q + 1]$ is called the *Hasse–Weil interval*. All elliptic curves defined over $\mathbb{F}_q$ are forced to have their number of rational points lying in this interval.

5.2.4 Tate's isogeny theorem

We end this section by stating deep results due to Tate and Tate–Honda [TAT 1966], which demonstrate the importance of characteristic polynomials of Frobenius endomorphisms.

Theorem 5.84

(i) Let $\mathcal{A}$ and $\mathcal{A}'$ be abelian varieties over $\mathbb{F}_q$. Then $\mathcal{A}$ is isogenous to $\mathcal{A}'$ over $\mathbb{F}_q$ if and only if $\chi(\phi_q)_{\mathcal{A}}(T) = \chi(\phi_q)_{\mathcal{A}'}(T)$.

(ii) Assume that $\lambda_1, \ldots, \lambda_{2g}$ are algebraic integers lying in a number field of degree $\leqslant 2g$ and satisfying the properties of eigenvalues of Frobenius endomorphism as stated in Corollary 4.118. Then there is an abelian variety $\mathcal{A}$ over $\mathbb{F}_q$ such that $\lambda_1, \ldots, \lambda_{2g}$ are the eigenvalues of the Frobenius endomorphism on $\mathcal{A}$.

Note that this abelian variety need not be principally polarized, and if it is, it need not to be a Jacobian of a curve.

Maisner and Nart [MANA 2002] study the problem to decide whether $\lambda_1, \ldots, \lambda_{2g}$ belong to a hyperelliptic curve.