split jacobians and lower bounds on heights

Martin Djukanovic

Split Jacobians and Lower Bounds on Heights

Proefschrift

ter verkrijging van

de graad van Doctor aan de Universiteit Leiden

op gezag van Rector Magnificus prof. mr. C. J. J. M. Stolker,

volgens besluit van het College voor Promoties

te verdedigen op woensdag 1 november 2017

klokke 16:15 uur

door

Martin Djukanović

geboren te Nikšić, Joegoslavië

in 1988

Samenstelling van de promotiecommissie:

Promotor: Prof. dr. Sebastiaan J. Edixhoven

Copromotores:

Dr. Robin S. de Jong

Dr. Fabien M. Pazuki (Université de Bordeaux & Københavns Universitet)

Overige leden:

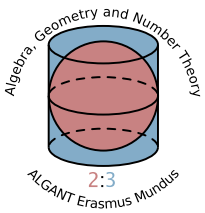
Prof. dr. Adrianus W. van der Vaart

Prof. dr. Bart de Smit

Prof. dr. Marc Hindry (Université Paris Diderot (Paris VII))

Prof. dr. Evelina Viada (Georg-August Universität Göttingen)

This work was funded by the Algant-Doc Erasmus Action and was carried out at Universiteit Leiden and Université de Bordeaux.



THÈSE

présentée à

L'UNIVERSITÉ DE BORDEAUX

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE

par Martin DJUKANOVIĆ

POUR OBTENIR LE GRADE DE

DOCTEUR

SPECIALITÉ : Mathématiques Pures

Jacobiennes Décomposées et Minoration de Hauteurs

Soutenue le 1er novembre 2017 à Leyde

Devant la commission d'examen formée de :

Marc HINDRY	Professeur	Université Paris VII	Rapporteur
Evelina VIADA	Professeur	Université de Göttingen	Rapporteur
Nils BRUIN	Professeur	Université Simon Fraser	Président
Robin DE JONG	Docteur	Université de Leyde	Directeur
Fabien PAZUKI	Professeur associé	Université de Bordeaux et Université de Copenhague	Directeur

Preface

This thesis deals with properties of Jacobians of genus two curves that cover elliptic curves, over number fields.

If C is a genus two curve and $C \to E$ is an optimal covering of degree n, i.e. a covering that does not factor through a non-trivial isogeny, then, possibly after extending the base field, there exist an elliptic curve $\widetilde{E}$ and an optimal covering $C \to \widetilde{E}$ of degree n, such that both curves can be embedded into the Jacobian $\mathrm{Jac}(C)$ of C so that they have precisely their n-torsion points in common. Moreover, the abelian surface $\mathrm{Jac}(C)$ is isogenous to $E \times \widetilde{E}$ via an isogeny whose kernel is precisely the image of $E[n]$ under the embedding into the Jacobian. The curves E and $\widetilde{E}$ are said to be glued along their n-torsion, while $\mathrm{Jac}(C)$ is said to be (n,n)-split.

The thesis is organized into two chapters, each of which contains an introduction into the topics discussed, making the chapters relatively self-contained.

Chapter 1 contains a detailed exposition of different approaches to constructing (n,n)-split Jacobians. A geometric description of the case $n = 2$ is a classical result, attributed to Jacobi. A modern approach to the topic can be found in [**Kuhn**], where a parametrization of the curves is given for $n = 3$. This description omits exactly one isomorphism class, which we find. The case $n = 4$ is treated in [**Br-Do**]. We build upon these ideas and give a general description of the procedure that yields the modular invariants of the two elliptic curves, at least in principle. We also revisit the cases $n = 2$ and $n = 3$ from a different perspective, starting with two elliptic curves E_1 and E_2, and an isomorphism $\alpha\colon E_1[n] \to E_2[n]$ whose graph we denote by Γ_α. The divisor $\Theta := E_1 \times \{0_{E_2}\} + \{0_{E_1}\} \times E_2$ induces a principal polarization of $E_1 \times E_2$. For some isomorphisms α, this polarization will descend to a

principal polarization on the quotient $J := (E_1 \times E_2)/\Gamma_\alpha$. We ask when the surface J is defined over K and when it is a Jacobian of a genus two curve, as above. For $n = 2$, we obtain several simple results (Propositions 1.4 – 1.8). Our analysis of the case $n = 3$ is focused on the Hesse pencil and yields a criterion that, for odd n, distinguishes between the cases where J is a Jacobian and the cases where it is a product of two elliptic curves (Proposition 1.9). This criterion is practical if one can explicitly find the divisor D on $E_1 \times E_2$ that is linearly equivalent to $n\Theta$ and whose image in J defines the principal polarization. We find this divisor in all cases when $n = 3$. The Appendix contains details concerning the computations involved.

Chapter 2 deals with canonical heights on abelian varieties. Historically, height functions have played a very important role in the study of rational points on abelian varieties, most notably in the proof of the famed Mordell-Weil theorem that establishes that the group of rational points of an abelian variety defined over a number field is finitely generated. A major inspiration for the thesis is a paper by Frey and Kani [**Fr-Ka**], where several conjectures concerning heights are compared for $\mathrm{Jac}(C)$ and $E \times \tilde{E}$ in the scenario described in Chapter 1, one notable exception being the Lang-Silverman conjecture. This conjecture estimates the height of a non-torsion point on an abelian variety in terms of an invariant of the variety, namely its Faltings height. Some recent results by Pazuki towards the Lang-Silverman conjecture in the case of abelian surfaces can be found in [**Paz2**]. We overview the theory of heights in the modern setting in great detail and the chapter concludes with a result that compares this conjecture for $\mathrm{Jac}(C)$ and $E \times \tilde{E}$, adding it to the list found in [**Fr-Ka**] (Theorems 2.38 and 2.39).

Contents

Partial list of notations

$\mathbf{Z}$	the integers
$\mathbf{Q}$	the rationals
$\mathbf{R}$	the reals
$\mathbf{C}$	the complex numbers
$\mathbf{H}$	the upper half-plane $\{x+iy \mid x,y \in \mathbf{R} \text{ and } y>0\}$
$\mathfrak{H}_g$	the Siegel upper half-space of $g \times g$ symmetric complex matrices with positive definite imaginary part
$\#S$	the cardinality of a set S
$\mathrm{char}(K)$	the characteristic of a field K
$\mathbb{1}$	the identity map or the identity element
$\otimes$	the tensor product
$\rtimes$	the semidirect product
$\mathbb{A}^n$	the n-dimensional affine space
$\mathbb{P}^n$	the n-dimensional projective space
$\mathcal{O}_X$	the structure sheaf of X (with X often omitted)
$\mathcal{O}(n)$	the twisting sheaves of Serre
Ω^r_X	the sheaf of differential forms of order r on X
ω_X	the dualizing (or canonical) sheaf
$\mathcal{F}(n)$	$\mathcal{F} \otimes \mathcal{O}(n)$
R_f	the ramification divisor of a morphism f
$K(X)$	the function field of X
$X(K)$	the K-rational points of a variety X

$\mathrm{Div}(X)$	the group of Weil divisors of X
$\mathrm{Div}^0(X)$	the subgroup of Weil divisors of degree 0
$\mathrm{Ca}(X)$	the group of Cartier divisors of X
$\mathrm{Pic}(X)$	the Picard group of X i.e. the group of isomorphism classes of invertible sheaves on X
$D \geq 0$	divisor D is effective
$D_1 \sim D_2$	two linearly equivalent divisors
$[D]$	the (linear) equivalence class of a divisor
$D_1 \cdot D_2$	the intersection of two divisors
$\mathscr{L}(D)$	the invertible sheaf associated to a Cartier divisor D
$L(D)$	the K-vector space of global sections of $\mathscr{L}(D)$, given as $\{0\} \cup \{f \in K(X)^\times \mid (f) + D \geq 0\}$
$p_a(X)$	the arithmetic genus of X
$p_g(X)$	the geometric genus X
$\ell(D)$	the dimension of $L(D)$
A/K	an abelian variety A defined over a field K
0_A	the identity element of the group structure of an abelian variety A (with A sometimes omitted)
$j(E)$	the modular invariant j of an elliptic curve E
$[n]\colon A \to A$	multiplication by $n \in \mathbf{Z}$ on an abelian variety A
$A[n]$	the kernel of $[n]$ (usually with the base extended to an algebraic closure)
e_n	the Weil pairing on $A[n]$
$\varphi^\vee\colon B^\vee \to A^\vee$	the isogeny dual to $\varphi\colon A \to B$
μ_n	the group scheme of n-th roots of unity
$\mathbf{G}_m$	the multiplicative group scheme

$t_P \colon A \to A$	translation by P on an abelian variety A
Γ_f	the graph of a morphism $f \colon X \to Y$
$H^i(X, \mathcal{F})$	the i-th sheaf cohomology group of $\mathcal{F}$
$h^i(X)$	the dimension of $H^i(X, \mathcal{O}_X)$
S_n	the group of permutations of n elements
$[L : K]$	the degree of a field extension L/K
$\mathrm{Frac}(R)$	the field of fractions of an integral domain R
$N_{L/K}$	the ideal norm in a field extension L/K
O_K	the ring of integers of a number field K
Δ_E	the minimal discriminant of an elliptic curve E
$\mathfrak{F}_E$	the conductor of an elliptic curve E
$x \gg y$	$x \geq c_1 y + c_2$ for some $c_1, c_2 \in \mathbf{R}_{>0}$

Chapter 1

Genus two curves with split Jacobians

Throughout the thesis, by a *variety* over a field K we mean a K-scheme of finite type, separated, and geometrically integral. By a *curve* we mean a variety of dimension one and by a *surface* we mean a variety of dimension two. By an abelian variety, we mean a complete group variety. In this chapter, unless stated otherwise, by K we mean a field of $\mathrm{char}(K) \neq 2$, by $\overline{K}$ we mean an algebraic closure of K, and we assume that all varieties and morphisms are defined over K. By a *model* of a curve, we mean a birational plane model. This is in contrast with the second chapter, where a model of a curve is a type of a fibred surface whose generic fibre is isomorphic to the curve.

1.1 Hyperelliptic curves

We recall some definitions and facts, referring to Chapter IV of [**HAG**] and Chapter 7 of [**Liu**].

A *hyperelliptic curve* C is a smooth projective curve of genus $g \geq 2$ that is equipped with a finite separable morphism $\pi\colon C \to \mathbb{P}^1$ of degree 2. In other words, the curve C is a *double cover* of $\mathbb{P}^1$ and π is a 2-to-1 covering map; this means that the corresponding function fields satisfy

$$[K(C)\colon \pi^* K(\mathbb{P}^1)] = 2.$$

Hence $K(C)$ is of the form $K(x, y)$, where $y^2 = h(x)y + f(x)$ and $f, h \in K[x]$. Since $\mathrm{char}(K) \neq 2$, we can complete the square and therefore assume, without loss of generality, that $y^2 = f(x)$. Hence C admits an affine planar model given by $y^2 = f(x)$. We can and do assume that this model is regular, i.e. that f has distinct roots, because if $y^2 = g(x)^2 f(x)$, we can change the variables by putting $y = g(x)y'$. In the affine model, the map π corresponds to $(x, y) \mapsto x$ and induces an involution ι on C, which is given by $\iota\colon (x, y) \mapsto (x, -y)$ and is called the *hyperelliptic involution*. It is the unique involution, up to automorphisms, with a quotient of genus zero and it corresponds to the generator of $\mathrm{Gal}(K(C)/K(x)) \cong \mathbf{Z}/2\mathbf{Z}$.

The fixed (geometric) points of ι are the ramification points of π and are called the *Weierstraß points*[1] of C. They lie above the roots of f and possibly also above ∞. Under our assumptions, the Hurwitz formula holds, i.e. the canonical divisors K_C and $K_{\mathbb{P}^1}$ of C and $\mathbb{P}^1$, respectively, are related by the linear equivalence

$$K_C \sim \pi^*(K_{\mathbb{P}^1}) + R$$

where R is the ramification divisor of π. Note that every ramification index e_P such that $e_P > 1$ necessarily equals 2 and, since $\mathrm{char}(K) \neq 2$, all ramification is tame. Therefore $R = \sum_{P \in C} (e_P - 1)P$ is the sum of the Weierstraß points. Recall that $K_{\mathbb{P}^1} \sim -2\infty$ so that $K_C \sim -2\pi^*(\infty) + R$. In case π does not ramify above ∞, applying Riemann-Roch yields

$$\deg K_C = 2g - 2 = -4 + \deg R = -4 + \deg f$$

which means $\deg f = 2g + 2$. If, on the other hand, π ramifies above ∞, then Riemann-Roch yields

$$\deg K_C = 2g - 2 = -4 + \deg R = -4 + \deg f + 1$$

which means $\deg f = 2g + 1$. To simplify, we introduce $d = \deg f$ if $\deg f$ is even and $d = \deg f + 1$ if $\deg f$ is odd so that Riemann-Roch yields $d = 2g + 2$. In either case, the ramification divisor R consists of $2g + 2$ distinct geometric points. We will always assume that the degree of f is even so that ∞ is not a branch point of π. If ∞ is a branch point, it is K-rational and we can apply an automorphism of $\mathbb{P}^1$ to make sure that it is not a branch point in the new coordinates.

[1] More generally, a Weierstraß point of a smooth projective curve X of genus g (over an algebraically closed field) is defined to be a point $P \in X$ s.t. $\ell(gP) \geq 2$.

So far, we have only mentioned an affine model of a hyperelliptic curve C. To build the actual curve C, it will not suffice to take the projective closure of the affine model $y^2 = f(x)$ because it is not smooth at infinity. Instead, we first observe that $v^2 = u^d f(u^{-1})$ is also a smooth affine model of C and we glue the two affine models via $(x, y) = (u^{-1}, u^{-d/2}v)$. Another way is to use the functions $x, y \in K(C)$ and embed C into $\mathbb{P}^{g+1}$ via

$$P \mapsto [1 \colon x(P) \colon x^2(P) \colon \cdots \colon x^g(P) \colon y(P)].$$

Every smooth projective curve of genus two is hyperelliptic. This follows from Riemann-Roch because $\deg K_C = 2 = \ell(K_C)$ implies that the *canonical map*, defined by the linear system $|K_C|$, is a 2-to-1 map from C to $\mathbb{P}^1$ (given by $P \mapsto [1 : x(P)]$ for a non-constant $x \in L(K_C)$). Curves of higher genera are "generically" not hyperelliptic. One can see this by an argument based on dimensions of moduli spaces. See also the remark below.

Remark 1.1 Most of the notions mentioned above are just as valid for curves of genus 0 or 1 and some authors include them in the definition of hyperelliptic curves. For a curve of genus 0 (resp. 1) in this context, we usually also assume that it has at least one K-rational point so that it is isomorphic to $\mathbb{P}^1$ (resp. an elliptic curve), whereas for curves of higher genera we make no such assumption. Some authors define a hyperelliptic curve to be a smooth projective curve that is a double cover of a smooth conic. Over an algebraically closed field, this coincides with our definition for $g \geq 2$. Under this definition, a smooth projective curve C of genus $g \geq 2$ is hyperelliptic if and only if the canonical map to $\mathbb{P}^{g-1}$ is not an embedding, in which case its image is a rational normal curve. In other words, among smooth projective curves, hyperelliptic curves of genus $g \geq 2$ are characterized by the fact that their canonical divisor K_C is ample, but *not* very ample. Its ampleness is a consequence of Riemann-Roch, since $\deg K_C = 2g - 2 > 0$ under our assumptions. To see that it is not very ample, we first note that, by Riemann-Roch and Proposition IV.3.1 of [**HAG**], the divisor K_C is very ample if and only if $\ell(P + Q) = 1$ for any two points P and Q. However, on hyperelliptic curves we have $\ell(P + Q) = 2$ for any two points P and Q in the same fibre of the 2-to-1 covering map. If the canonical map sends two different points P and Q to the same image, then by Riemann-Roch

$$\ell(P + Q) = \ell(K_C - P - Q) - g + 3 = \ell(K_C - P) - g + 3 = 2$$

and $|P + Q|$ defines the 2-to-1 map. This map is unique up to actions of automorphisms of $\mathbb{P}^1$ and C. When the canonical map is injective, it is also

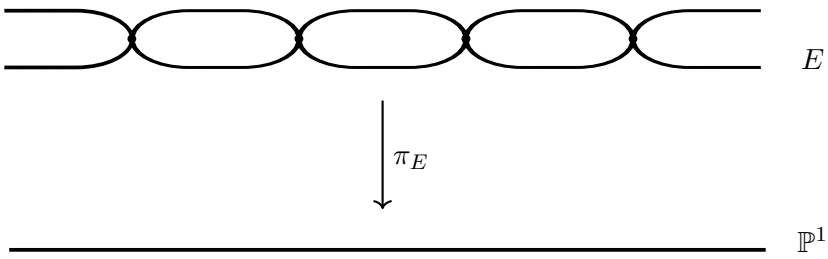


Figure 1.1: A genus one curve as a double cover of the projective line with the ramification points marked.

an embedding because we can take $P = Q$ just as well. Moreover, $2K_C$ is very ample if and only if $g \geq 3$ and $3K_C$ is very ample if and only if $g \geq 2$. See IV.3 and IV.5 in [**HAG**] and 7.4 in [**Liu**].

We depict finite separable coverings between curves with a diagram of the kind that is shown in Fig. 1.1 above. In case the degree of the covering is greater than 2, we depict only the fibres containing the ramification points, denoting unramified points by —, doubly ramified points by $\times$, triply ramified points by $\divideontimes$ etc.

Remark 1.2 The case of $\mathrm{char}(K) = 2$ is excluded from the very beginning because it allows for wild ramification of the covering map. That is to say that $\mathrm{char}(K)$ divides the ramification indices of the Weierstraß points and the multiplicity of each ramification point in the ramification divisor is $\geq e_P$. In this setting, hyperelliptic curves are a special case of the so-called *Artin-Schreier curves*, which are curves in characteristic p that are covers of $\mathbb{P}^1$ of degree p. Such a curve C admits an affine model of the form $y^p - y = f(x)$ where $f \in K(x)$ is not of the form $g(x)^p - g(x)$ for any $g \in K(x)$ and $\deg f$ is coprime to p. Here $\deg f = \deg f_1 - \deg f_2$ if $f = f_1/f_2$, with $f_1, f_2 \in K[x]$, in lowest terms. If $(x, y) \in \mathbb{A}^2$ satisfies $y^p - y = f(x)$, then so does $(x, y + 1)$ because $(y+1)^p - y - 1 = y^p - y = f(x)$. We therefore have an automorphism σ of the curve, defined by $\sigma(y) = y + 1$, which is of order p. This implies that $\mathrm{Gal}(K(C)/K(x))$ is cyclic of order p. It also implies that the ramification points can only occur above ∞ and the poles of f. The relation between f and the genus of the curve is more complicated in this case and we omit it here (see Lemma 2.2.3 in [**Farn**]).

1.2 Curves of genus two covering curves of genus one

Let C be a curve of genus two that covers a curve E of genus one via $\phi\colon C \to E$ of degree n. Let ι denote the hyperelliptic involution on C. Recall that we had assumed that the curves and the maps are defined over a field K of characteristic $\mathrm{char}(K) \neq 2$.

Lemma 1.1 *The hyperelliptic involution ι of C induces an involution of E, also denoted by ι, such that ϕ commutes with the involutions and such that the quotient E/ι is of genus zero. In particular, the map ϕ sends fixed points on C to fixed points on E (under ι).*

Proof Naturally, we make an argument over $\overline{K}$. Let $W \in C(\overline{K})$ be a Weierstraß point. We embed C into its Jacobian via $P \mapsto [P - W]$ and E into its Jacobian via $P \mapsto [P - \phi(W)]$. The choice of the embedding guarantees that ι on C is compatible with $-\mathbb{1} \in \mathrm{Aut}(\mathrm{Jac}(C))$, i.e. $\iota = -\mathbb{1}$ when restricted to the image of C inside its Jacobian. The morphism ϕ induces a morphism ϕ_* between the Jacobians of the two curves and we have the following commutative diagram:

$$\begin{array}{ccc} C & \hookrightarrow & \mathrm{Jac}(C) \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi_*} \\ E & \overset{\sim}{\hookrightarrow} & \mathrm{Jac}(E) \end{array} \tag{1.1}$$

Since $-\mathbb{1}_E \circ \phi_* = \phi_* \circ (-\mathbb{1}_C)$ (ϕ_* is a group morphism) and $E \cong \mathrm{Jac}(E)$ (geometrically), the involution on C induces an involution on E, that we also denote by ι. The morphism ϕ clearly respects the involutions, therefore it sends fixed points to fixed points, under ι. Furthermore, it induces a morphism $\mathrm{Jac}(C)/_{-\mathbb{1}} \to \mathrm{Jac}(E)/_{-\mathbb{1}}$ that, when restricted to C, gives a morphism $f\colon C/_\iota \to E/_\iota$. Since $C/_\iota$ is of genus zero, so is $E/_\iota$, and from the construction it follows that f and the involutions are defined over K. □

In view of the lemma, we have the following commutative diagram:

$$\begin{array}{ccc} C & \xrightarrow{\phi} & E \\ \downarrow{\scriptstyle \pi_C} & & \downarrow{\scriptstyle \pi_E} \\ C/\iota & \xrightarrow{f} & E/\iota \end{array} \tag{1.2}$$

Remark 1.3 By our definition, we have $C/_\iota \cong \mathbb{P}^1$ and since f is K-rational, we also have $E/_\iota \cong \mathbb{P}^1$. Some authors define a hyperelliptic curve more generally by requiring only that $C/_\iota$ is of genus zero.

We now consider, over $\overline{K}$, the ramification of each map in diagram (1.2). Let $W_1, \ldots, W_6$ denote the ramification points of π_C and let $T_1, \ldots, T_4$ denote the ramification points of π_E, i.e. the points fixed by ι. Let $w_1, \ldots, w_6$ and $t_1, \ldots, t_4$ denote their respective images under the corresponding projection maps π_C and π_E. Lemma 1.1 tells us that $\phi(\{W_i\}) \subseteq \{T_j\}$. From the commutativity of the diagram, we have $\deg f = \deg \phi = n$ and $f(\{w_i\}) \subseteq \{t_j\}$.

Lemma 1.2 ([**Kuhn**]) *With the notations as above, for every $i \in \{1, 2, \ldots, 6\}$ the divisor $f^*(\sum_{j=1}^4 t_j)$ contains w_i with odd multiplicity and any other points with even multiplicity.*

Proof We assume, without loss of generality, that

$$\overline{K}(C) = \overline{K}(x)[y]/(y^2 - P(x))$$

for some $P \in K[x]$ of degree 6, which is an extension of degree two of $\overline{K}(x)$, the function field of the underlying projective line. Similarly, we assume

$$\overline{K}(E) = \overline{K}(t)[s]/(s^2 - Q(t))$$

for some $Q \in K[t]$ of degree 4, which is an extension of degree two of $\overline{K}(t)$, the function field of the other underlying projective line, where $t = f(x)$. We may view all these fields as subfields of $\overline{K}(C)$. That being said, we observe that the hyperelliptic involution ι fixes $\overline{K}(x)$ and $\overline{K}(t)$. Furthermore, we have $\iota(y) = -y$ and $\iota(s) = -s$, whence $\iota(s/y) = s/y$. Being fixed by the involution, s/y must be an element of $\overline{K}(x)$, say $s/y = A(x)/B(x)$ for some coprime $A, B \in \overline{K}[x]$. This implies

$$Q(t) = s^2 = y^2 \frac{A(x)^2}{B(x)^2} = P(x) \frac{A(x)^2}{B(x)^2}.$$

The roots of the right-hand side are exactly the points that lie above the t_j, i.e. they are the roots of $Q(t)$. Since P is square-free with w_i as roots, we are done. □

Applying Riemann-Hurwitz to ϕ yields $\deg R_\phi = 2$, therefore either ϕ doubly ramifies at two distinct points or it has one triple ramification point.

We distinguish two cases – either this ramification occurs above some T_j (the "special" case) or it does not (the "generic" case). As ι acts on R_ϕ, if there are two distinct ramification points, they cannot lie above two distinct T_j.

In the generic case, the map $\pi_E \circ \phi = f \circ \pi_C$ ramifies at $4n$ double points that lie above the T_j. Since π_C ramifies at six double points, we have that f ramifies at

$$\frac{1}{2}(4n-6) = 2n-3$$

double points above the t_j, none of which is any of the w_i. Applying Riemann-Hurwitz to f yields $\deg R_f = 2n-2$ which means that there is one more doubly ramified point that does not lie above the t_j. In the special case, all of the ramification lies above the t_j.

Since f is finite and between smooth varieties, it is flat and every fibre of f has exactly $n = \deg f$ points over $\overline{K}$, counting with multiplicities. More precisely, we have that $f_*\mathcal{O}_{C/\iota}$ is a locally free $\mathcal{O}_{E/\iota}$-module of rank n. Lemma 1.2 implies that above each t_j there is an odd number of the w_i if n is odd and an even number of the w_i if n is even, thus limiting the ramification of f above the t_j to four cases. This is by virtue of the simple fact that 6 has a unique decomposition as a sum of four odd non-negative integers and exactly three decompositions as a sum of four even non-negative integers. The four cases are depicted in Fig. 1.2, where the unramified points, i.e. the w_i, are denoted by — and doubly ramified points are denoted by $\times$.

Remark 1.4 From now on, we will assume that the points are indexed as in Fig. 1.2. In the generic case, we will denote by t_0 the image under f of the ramification point that does not lie above $\{t_1, t_2, t_3, t_4\}$, and we will call *special* the ramification point above t_0 (in the generic case) and the ramification point with ramification index ≥ 3 (in the special case).

Theorem 1.3 ([**Kuhn**]) *Let i and j run through $\{1, \ldots, 6\}$ and $\{1, \ldots, 4\}$, respectively. If $\phi\colon C \to E$ is unramified above the T_j, then the ramification of $f\colon C/\iota \to E/\iota$ consists of $2n-3$ doubly ramified points above the t_j that are distributed as in Fig. 1.2 and one other doubly ramified point that does not lie above any of the t_j. If ϕ ramifies above the T_j, then the entire ramification of f occurs above the t_j and its distribution is the same except that either:*

(1) One of the w_i has ramification index 3; or

(2) There is a unique point, not one of the w_i, with ramification index 4.

Corollary 1.4 *The point t_4 is K-rational. Consequently, so is T_4.*

Proof We again assume, without loss of generality, that even degree models are given for both curves. First we observe that the divisors $w_1 + \cdots + w_6$ and $t_1 + \cdots + t_4$ are K-rational because they correspond to roots of polynomials with K-rational coefficients. That is to say that the absolute Galois action permutes $\{w_1, \ldots, w_6\}$ and it also permutes $\{t_1, t_2, t_3, t_4\}$. Moreover, the absolute Galois action permutes the fibres of f because this map is K-rational and therefore commutes with $\mathrm{Gal}(\overline{K}/K)$. In particular, the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ permutes the four fibres of f above $\{t_1, t_2, t_3, t_4\}$.

Suppose n is odd. Let w_1, w_2, w_3 be the three points above t_4. Since the fibre $f^{-1}(t_4)$ is the only fibre with three of the w_i, it must be that the absolute Galois action permutes $\{w_1, w_2, w_3\}$, i.e. $w_1 + w_2 + w_3$ is K-rational. Hence its image under f, namely t_4, is K-rational.

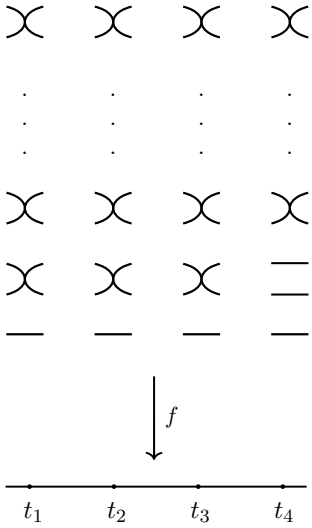
Suppose n is even. We consider each case separately. In case (1), we have that $t_1+t_2+t_3$ is the image of $w_1+\cdots+w_6$ under f and is therefore K-rational, which implies that t_4 is K-rational. In case (2), the argument is analogous to the one above, for odd n, and shows that t_4 and t_3 are K-rational. In case (3), the K-rationality of t_4 is immediate as t_4 is the image of $w_1+\cdots+w_6$ under f. □

Corollary 1.5 *The special ramification point of the map f is K-rational. Consequently, so is its image under f.*

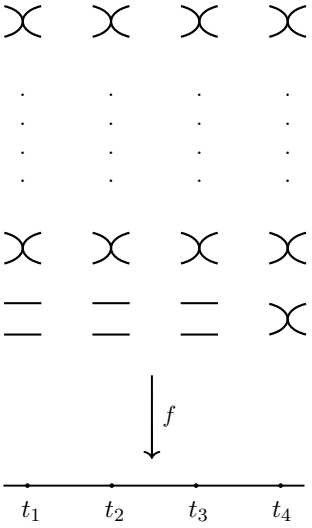
Proof In the generic case, the fibre $f^{-1}(t_0)$ is the unique one containing a single ramification point and none of the w_i. In the special case, the special point is the unique point with ramification index ≥ 3. Thus the absolute Galois action fixes the special point in both cases. □

Remark 1.5 Given that the highest possible ramification index is 4, wild ramification of f can only occur if $\mathrm{char}(K) \in \{2, 3\}$. We always assume that this is not the case so that the ramification is tame.

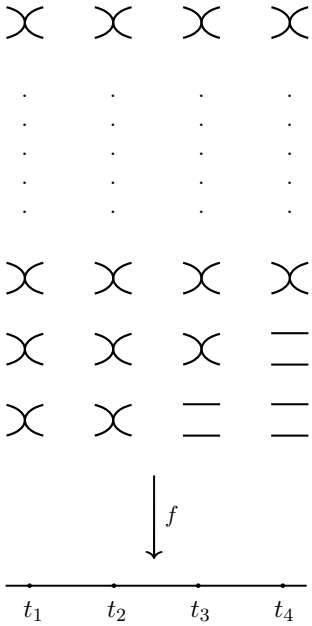
Remark 1.6 Corollary 1.4 shows that the covering $\phi\colon C \to E$ induces a structure of an elliptic curve on E where T_4 is the identity element of the group structure.



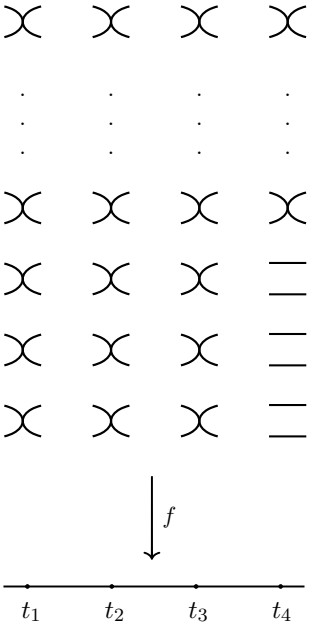
odd degree



even degree, case (1)



even degree, case (2)



even degree, case (3)

Figure 1.2: Generic picture of the possible ramification of f above the t_j.

Example 1.1 If $\deg f = 2$, only case (1) can occur (Fig. 1.3).

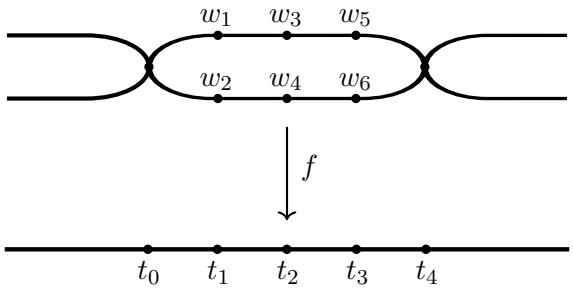


Figure 1.3: Ramification of f when $\deg f = 2$.

Example 1.2 If $\deg f = 3$, there are two possible cases (Fig. 1.4).

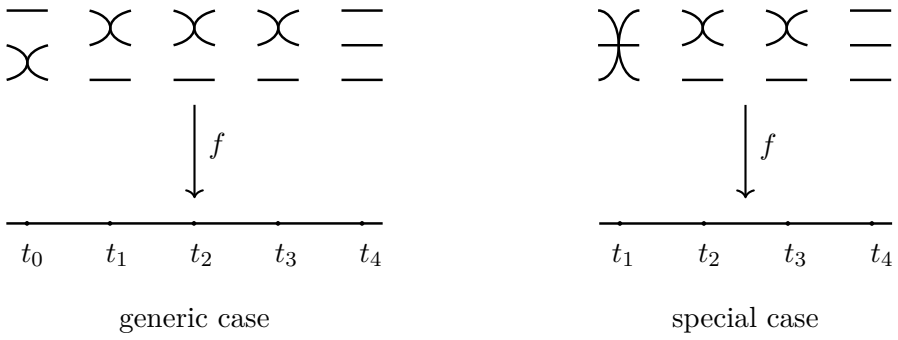


Figure 1.4: Ramification of f when $\deg f = 3$.

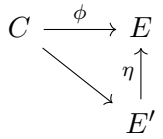
Proposition 1.1 *A given finite separable map $f\colon \mathbb{P}^1 \to \mathbb{P}^1$ with ramification as described in Theorem 1.3 lifts to a finite separable map $\phi\colon C \to E$ that makes the diagram* (1.2) *commute. Moreover, the curves C and E are unique up to isomorphisms and the map ϕ is unique up to compositions with automorphisms.*

Proof Let $w_1, \ldots, w_6$ and $t_1, \ldots, t_4$ be the geometric points defined by ramification of f as in Fig. 1.2 (with the analogous definition for the special case). Let $B_1 = w_1 + \cdots + w_6$ and let $B_2 = t_1 + \cdots + t_4$. By the above argument, the ramification behaviour of f implies K-rationality of B_1 and B_2. Therefore B_1 corresponds to $\mathcal{O}(6) \in \mathrm{Pic}(\mathbb{P}^1) \cong \mathbf{Z}$ and B_2 corresponds to $\mathcal{O}(4) \in \mathrm{Pic}(\mathbb{P}^1)$. Both are uniquely divisible by two and are therefore respectively branch divisors of 2-to-1 separable coverings $\pi_C \colon C \to \mathbb{P}^1$ and $\pi_E \colon E \to \mathbb{P}^1$ (see §I.17 in [**B-H-P-V**], for example), where C is a curve of genus two and E is a curve of genus one, by Riemann-Hurwitz. Since B_1 is contained in f^*B_2, we have an injection $\mathcal{O}(B_1) \hookrightarrow \mathcal{O}(f^*B_2)$ and, by the functoriality of the constructions, this gives the desired covering $\phi \colon C \to E$. □

Remark 1.7 Note that, in the previous proposition, if $\deg f \notin \{2, 5\}$, then the ramification of f implies that t_4 is K-rational and therefore E is elliptic with T_4 as the identity, where T_4 is the point whose image is t_4 under π_E. If $\deg f \in \{2, 5\}$, then $f^*(t_4)$ and $f^*(t_0)$ have the same ramification indices for their points.

1.3 Optimal coverings

Definition 1.1 Let C be a curve of genus two and let E be an elliptic curve. We say that a covering map $\phi \colon C \to E$ is *optimal*[2] if whenever there exists another elliptic curve E' such that ϕ decomposes (over $\overline{K}$) as



then $\eta \colon E' \to E$ is an isomorphism. In other words, if ϕ factors through an isogeny, then the isogeny is trivial.

Definition 1.2 Let $\lambda_A \colon A \to A^\vee$ and $\lambda_B \colon B \to B^\vee$ be polarizations of abelian varieties. Let $\varphi \colon A \to B$ be an isogeny and let $\varphi^\vee$ denote the dual isogeny.

[2] Some authors use the term *maximal* or *minimal*.

We say that the isogeny φ is *polarized* with respect to λ_A and λ_B if the following diagram commutes:

$$\begin{array}{ccc} A & \xrightarrow{\lambda_A} & A^\vee \\ \downarrow{\scriptstyle \varphi} & & \uparrow{\scriptstyle \varphi^\vee} \\ B & \xrightarrow{\lambda_B} & B^\vee \end{array}$$

The central claim of the following lemma is well known, but here we give a complete formal proof.

Lemma 1.6 *Let C be a curve of genus two and let $\phi\colon C \to E$ be an optimal covering of an elliptic curve E with $\deg\phi = n$. Then there exists an elliptic curve $\widetilde{E}$, an optimal covering $\widetilde{\phi}\colon C \to \widetilde{E}$, and an isogeny $\varphi\colon E \times \widetilde{E} \to \mathrm{Jac}(C)$, possibly after extending the base field, such that:*

(1) $\deg\widetilde{\phi} = n$;

(2) $\varphi = \phi^* + \widetilde{\phi}^*$;

(3) $\deg\varphi = n^2$;

(4) $\mathrm{Ker}(\varphi) \cong E[n] \cong \widetilde{E}[n]$;

(5) *φ is polarized with respect to the polarizations $[n]\circ\lambda_\Theta$ of $E\times\widetilde{E}$ and λ_C of $\mathrm{Jac}(C)$, where λ_Θ and λ_C denote the usual principal polarizations, respectively induced by $\mathscr{L}(\Theta)$ and $\mathscr{L}(C)$, and $\Theta := \{0_E\}\times\widetilde{E} + E\times\{0_{\widetilde{E}}\}$.*

Proof Let D be a geometric divisor of degree 1 on C that is invariant under the hyperelliptic involution. We embed C into $\mathrm{Jac}(C)$ via $\varepsilon\colon P \mapsto [P - D]$. We consider all schemes over the extended base $\overline{K}$. Recalling that $E \cong \mathrm{Jac}(E)$ and denoting $\mathcal{K} := \mathrm{Ker}(\phi_*)$, we consider the following exact sequence of commutative group schemes:

$$0 \longrightarrow \mathcal{K} \longrightarrow \mathrm{Jac}(C) \xrightarrow{\phi_*} E \longrightarrow 0\,. \tag{1.3}$$

Note that $\dim\mathcal{K} = 1$ because ϕ_* is surjective, but not an isogeny. Let $\mathcal{K}_0$ denote the connected component of the identity of $\mathcal{K}$. We claim that $\mathcal{K} = \mathcal{K}_0$, i.e. $\mathcal{K}$ is connected.

To see this, consider the following commutative exact diagram in the category of commutative finite type group schemes over K:

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & 0 & & 0 & & \mathrm{Ker}(\gamma) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathcal{K}_0 & \longrightarrow & \mathrm{Jac}(C) & \longrightarrow & F & \longrightarrow & 0 \\
 & & \downarrow & & \| & & \downarrow{\scriptstyle \gamma} & & \\
0 & \longrightarrow & \mathcal{K} & \longrightarrow & \mathrm{Jac}(C) & \xrightarrow{\phi_*} & E & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & G & & 0 & & 0 & & \\
 & & \downarrow & & & & & & \\
 & & 0 & & & & & &
\end{array} \tag{1.4}$$

where $F := \mathrm{Jac}(C)/\mathcal{K}_0$ and $G := \mathcal{K}/\mathcal{K}_0$. The map $\gamma\colon F \to E$ is the induced map and the unlabeled arrows denote the canonical inclusions and quotients. Note that G is finite and that F is connected, being a quotient of the connected $\mathrm{Jac}(C)$. Since our category is abelian (see [**SGA3**] exposé $\mathrm{VI_A}$, Thm 5.4.2), the Snake Lemma gives an isomorphism $\mathrm{Ker}(\gamma) \cong G$. Since γ is surjective and has a finite kernel, it is an isogeny (see 8.1. in [**Miln1**]). Restricting to $\varepsilon(C) \subset \mathrm{Jac}(C)$, we see that ϕ factors as

$$\begin{array}{ccc}
C & \xrightarrow{\phi} & E \\
 & \searrow & \uparrow{\scriptstyle \gamma} \\
 & & F
\end{array}$$

However, by our optimality assumption, it must be that γ is an isomorphism. Therefore G is trivial and $\mathcal{K} = \mathcal{K}_0$, making $\mathcal{K}$ an elliptic curve. We accordingly adopt a new notation for it, namely $\widetilde{E}$.

Consider now, in the category of abelian varieties, the exact sequence

$$0 \longleftarrow \widetilde{E}^\vee \xleftarrow{\eta} \mathrm{Jac}(C)^\vee \xleftarrow{\phi^*} E^\vee \longleftarrow 0\,, \tag{1.5}$$

that is dual to the sequence (1.3). Using the fact that elliptic curves are canonically isomorphic to their Jacobians and that Jacobians are canonically self-dual (see §6 in [**Miln2**]), we can write

$$\begin{array}{ccc} \widetilde{E} & \xleftarrow{\eta} & \mathrm{Jac}(C) \\ & \nwarrow & \uparrow{\scriptstyle \varepsilon} \\ & & C \end{array}$$

and define $\widetilde{\phi}\colon C \to \widetilde{E}$ as the composition $\eta \circ \varepsilon$. Since $\mathrm{Ker}(\widetilde{\phi}_*) = E$ is connected, it follows that $\widetilde{\phi}$ is likewise optimal. Thus the curve C is a degree n cover of both E and $\widetilde{E}$, and the latter two are complementary in the sense that one is the quotient of $\mathrm{Jac}(C)$ by the other. That is to say that the following two sequences

$$0 \longrightarrow E \xrightarrow{\phi^*} \mathrm{Jac}(C) \xrightarrow{\widetilde{\phi}_*} \widetilde{E} \longrightarrow 0 \tag{1.6}$$

$$0 \longrightarrow \widetilde{E} \xrightarrow{\widetilde{\phi}^*} \mathrm{Jac}(C) \xrightarrow{\phi_*} E \longrightarrow 0 \tag{1.7}$$

are exact.

Now let $\varphi\colon E \times \widetilde{E} \to \mathrm{Jac}(C)$ denote the map $\phi^* + \widetilde{\phi}^*$. By the exactness of the sequences and the fact that ϕ^* and $\widetilde{\phi}^*$ are embeddings into $\mathrm{Jac}(C)$, we have

$$\begin{aligned} \mathrm{Ker}(\varphi) &\cong \phi^*(E) \cap \widetilde{\phi}^*(\widetilde{E}) \\ &= \mathrm{Im}(\phi^*) \cap \mathrm{Ker}(\phi_*) \\ &\cong \mathrm{Ker}(\phi_* \circ \phi^*) \\ &= \mathrm{Ker}([n]) \\ &= E[n]. \end{aligned}$$

In particular, we have that $\deg \varphi = n^2$. The same argument also shows that $\mathrm{Ker}(\varphi) \cong \widetilde{E}[n]$. Since $\mathrm{Ker}(\varphi)$ is finite, we have that φ is an isogeny of abelian surfaces and we have the following exact sequence:

$$0 \longrightarrow \mathrm{Ker}(\varphi) \longrightarrow E \times \widetilde{E} \xrightarrow{\varphi} \mathrm{Jac}(C) \longrightarrow 0.$$

It is now clear that the two diagrams

$$\begin{array}{ccc} E \times \widetilde{E} & \xrightarrow{[n] \circ \lambda_\Theta} & (E \times \widetilde{E})^\vee \\ \Big\downarrow{\scriptstyle \phi^* + \widetilde{\phi}^*} & & \Big\uparrow{\scriptstyle \lambda_\Theta \circ (\phi_*, \widetilde{\phi}_*) \circ \lambda_C^{-1}} \\ \mathrm{Jac}(C) & \xrightarrow[\sim]{\lambda_C} & \mathrm{Jac}(C)^\vee \end{array} \tag{1.8}$$

$$\begin{array}{ccc} \mathrm{Jac}(C) & \xrightarrow{[n] \circ \lambda_C} & \mathrm{Jac}(C)^\vee \\ \Big\downarrow{\scriptstyle (\phi_*, \widetilde{\phi}_*)} & & \Big\uparrow{\scriptstyle \lambda_C \circ (\phi^* + \widetilde{\phi}^*) \circ \lambda_\Theta^{-1}} \\ E \times \widetilde{E} & \xrightarrow[\sim]{\lambda_\Theta} & (E \times \widetilde{E})^\vee \end{array} \tag{1.9}$$

are commutative, so that φ and its dual $\varphi^\vee$ are polarized. This completes the proof. □

By abuse of notation, we also denote by ι the involution on $\widetilde{E}$ induced by the hyperelliptic involution on C.

Definition 1.3 We say that $\widetilde{E}$, $\widetilde{\phi}$, and $\widetilde{f}$ are *complementary* to E, ϕ, and f, respectively.

Definition 1.4 A Jacobian $\mathrm{Jac}(C)$ of a genus two curve C is said to be *split* if it is isogenous to a product $E \times \widetilde{E}$ of two elliptic curves; more specifically, if the isogeny is induced by an optimal covering $C \to E$ of degree n, then $\mathrm{Jac}(C)$ is said to be (n, n)-*split*.

Remark 1.8 The curve $\widetilde{E}$ is defined over K, given that C, E, and ϕ are. The extension of the base field is only required to define the divisor D. If D is rational over the base field, then so are all the constructions that follow. In view of Lemma 1.6, we say that $\mathrm{Jac}(C)$ can be obtained by "gluing together" the two elliptic curves along their n-torsion. Moreover, as we shall see later, the induced isomorphism $E[n] \cong \widetilde{E}[n]$ inverts the Weil pairing (Lemma 1.14).

1.3.1 The Weil pairing on the 2-torsion

The cases of odd and even degree of an optimal covering $\phi\colon C \to E$ differ in one other important aspect. Since $T_1, T_2, T_3, T_4 \in E(\overline{K})$ are the 2-torsion points on E, they are in the kernel $\mathrm{Ker}(\varphi) \cong E[n]$ of the isogeny $\varphi\colon E \times \widetilde{E} \to \mathrm{Jac}(C)$ if and only if the degree n is even.

Let $(i,j) := [W_i - W_j] = [W_j - W_i]$ for $1 \leq i < j \leq 6$, denote the 15 distinct linear equivalence classes that are the points of order two on $\mathrm{Jac}(C)$. Then for distinct indices i,j,k,l,m,n, in the group structure of $\mathrm{Jac}(C)$ we have

$$(i,j)+(i,j)=0, \qquad (i,j)+(k,l)=(m,n), \qquad (i,j)+(i,k)=(j,k),$$

and the Weil pairing on $\mathrm{Jac}(C)[2]$ is given by (see [**Tata1**] and [**Tata2**]):

$$e_2((i,j),(i,j))=1, \qquad e_2((i,j),(k,l))=1, \qquad e_2((i,j),(i,k))=-1. \quad (1.10)$$

1.3.2 Optimal coverings of odd degree

We have established that when the degree of $\phi\colon C \to E$ is odd, there is a unique ramification point on E denoted by T_4 such that exactly three of the W_i, that we index as W_1, W_2, W_3, lie above it. Moreover, the point T_4 is K-rational. Likewise, the points w_1, w_2, w_3 map to the K-rational $t_4 \in \mathbb{P}^1$ under the induced f. Both $w_1+w_2+w_3$ and $W_1+W_2+W_3$ are K-rational. Thus we can and do assume that C is given by a model $y^2 = P(x)Q(x)$, where $P, Q \in K[x]$ are cubics with roots $\{w_1,w_2,w_3\}$ and $\{w_4,w_5,w_6\}$, respectively. Since the canonical divisor $K_C \sim 2W_i$ is K-rational, so is the divisor $W_1 - W_2 + W_3$. Moreover, the latter determines a unique linear equivalence class $[W_i - W_j + W_k]$ for $\{i,j,k\} = \{1,2,3\}$ or $\{4,5,6\}$. Thus ϕ induces a canonical K-rational embedding $C \hookrightarrow \mathrm{Jac}(C)$, given by

$$P \mapsto [P - W_1 + W_2 - W_3], \quad (1.11)$$

which is compatible with the canonical isomorphism $E \cong \mathrm{Jac}(E)$, that is given by $P \mapsto [P - T_4]$, and the involutions. Therefore we still have (1.1) and we could have assumed this embedding a priori.

Theorem 1.7 ([**Kuhn**]) *In the case of optimal coverings of odd degree, the roles of the divisors $w_1+w_2+w_3$ and $w_4+w_5+w_6$ are exchanged between the two complementary maps f and $\widetilde{f}$. We have $f_*(w_1+w_2+w_3) = \pi_{E*}(0_E)$ and $\widetilde{f}_*(w_4+w_5+w_6) = \pi_{\widetilde{E}*}(0_{\widetilde{E}})$, and hence also $f_*(w_4+w_5+w_6) = \pi_{E*}(E[2]\backslash\{0_E\})$ and $\widetilde{f}_*(w_1+w_2+w_3) = \pi_{\widetilde{E}*}(\widetilde{E}[2] \setminus \{0_{\widetilde{E}}\})$, where the identity element 0_E is given by T_4.*

Proof Note that under the canonical embedding (1.11), a Weierstraß point W_i maps to (j,k) for $\{i,j,k\} = \{1,2,3\}$ or $\{4,5,6\}$. Since the degree is odd, the isogeny $\varphi = \phi^* + \widetilde{\phi}^*$ induces an isomorphism of the 2-torsion subgroups, with inverse $\varphi^{-1} = (\phi_*, \widetilde{\phi}_*)$. The fact that $\phi(\{W_1, W_2, W_3\}) = T_4$ implies

$$\mathrm{Ker}(\phi_*) \cap \mathrm{Jac}(C)[2] = \{0, (1,2), (1,3), (2,3)\}.$$

We are done if we show that

$$\mathrm{Ker}(\widetilde{\phi}_*) \cap \mathrm{Jac}(C)[2] = \{0, (4,5), (4,6), (5,6)\}.$$

Suppose $(i,j) \in \mathrm{Ker}(\phi_*)$ and $(k,l) \in \mathrm{Ker}(\widetilde{\phi}_*)$ are two points of order two. Applying the isomorphism φ^{-1} between the 2-torsion subgroups of the two abelian surfaces and comparing the Weil pairings, which are preserved under polarized isogenies (Lemma 16.2(c) in [**Miln1**]), we obtain

$$\begin{aligned} e_2((i,j),(k,l)) &= e_2((\phi_*(i,j), \widetilde{\phi}_*(i,j)) \,,\, (\phi_*(k,l), \widetilde{\phi}_*(k,l))) \\ &= e_2(\phi_*(i,j), \phi_*(k,l)) \,\cdot\, e_2(\widetilde{\phi}_*(i,j), \widetilde{\phi}_*(k,l)) \\ &= e_2(0_E, \cdot) \,\cdot\, e_2(\cdot, 0_{\widetilde{E}}) \\ &= 1 \cdot 1 = 1. \end{aligned}$$

This, together with (1.10), implies

$$(k,l) \in \{(4,5),(4,6),(5,6)\} \cup \{(1,2),(1,3),(2,3)\}.$$

However, there can be no point of order two in $\mathrm{Ker}(\phi_*) \cap \mathrm{Ker}(\widetilde{\phi}_*)$ because φ^{-1} would map such a point to $0 \in (E \times \widetilde{E})[2]$, which is impossible since φ induces a group isomorphism on $\mathrm{Jac}(C)[2]$. □

1.3.3 Optimal coverings of even degree

The case of even degree is quite different because we do not necessarily have a K-rational embedding $C \hookrightarrow \mathrm{Jac}(C)$ that would be compatible with the canonical elliptic curve structure of E (with T_4 as the identity element). In this case, we have $(E \times \widetilde{E})[2] \subset \mathrm{Ker}(\varphi)$. The map $\phi_* \circ \phi^* \colon E \to E$ is multiplication by the even n and therefore identically zero on $E[2]$. Therefore we have $\mathrm{Im}(\phi^*) \cap \mathrm{Jac}(C)[2] = \mathrm{Ker}(\phi_*) \cap \mathrm{Jac}(C)[2] = \widetilde{E}[2]$ so that $\widetilde{E}[2]$ is a subgroup of $\mathrm{Jac}(C)[2]$ of order 4.

Let $(i,j) \in \mathrm{Ker}(\phi_*)$. Suppose that also $(i,k) \in \mathrm{Ker}(\phi_*)$. Then the equality $(i,j)+(i,k)=(j,k)$ implies that $\mathrm{Ker}(\phi_*)=\{0,(i,j),(i,k),(j,k)\}$, and under the embedding of C into $\mathrm{Jac}(C)$, given by $P \mapsto [P-W_i]$, we have $\{W_i,W_j,W_k\} \subseteq \phi^{-1}(0)$, which contradicts Theorem 1.3, given the optimality of ϕ. Indeed, in cases (2) and (3) of Fig. 1.2, there are more than four points in $\mathrm{Ker}(\phi_*) \cap \mathrm{Jac}(C)[2]$, so that $\mathrm{Ker}(\phi_*)$ is not connected.

Hence we can assume, reindexing the points if necessary, that

$$\mathrm{Ker}(\phi_*) \cap \mathrm{Jac}(C)[2] = \{0,(1,2),(3,4),(5,6)\}.$$

Thus for each choice of the embedding $P \mapsto [P-W_i]$ of C into its Jacobian (and the induced isomorphism $P \mapsto [P-\phi(W_i)]$ of E and its Jacobian), we have precisely two Weierstraß points of C mapped to $0 \in \mathrm{Jac}(E) \cong E$. Since

$$\widetilde{E}[2] \cong \mathrm{Ker}(\phi_*) \cap \mathrm{Jac}(C)[2] \quad \text{and} \quad E[2] \cong \mathrm{Ker}(\widetilde{\phi}_*) \cap \mathrm{Jac}(C)[2],$$

we have the following theorem.

Theorem 1.8 ([**Kuhn**]) *Let $\phi\colon C \to E$ be an optimal covering of even degree. Then the ramification diagram of $f\colon C/\iota \to E/\iota$ is the one depicted in case (1) of Fig. 1.2 and the complementary $\widetilde{\phi}\colon C \to \widetilde{E}$ induces a map $\widetilde{f}\colon C/\iota \to \widetilde{E}/\iota$ with the same ramification diagram and the same indexing of the Weierstraß points.*

1.4 Characterization of split Jacobians

Given an optimal covering $\phi\colon C \to E$, Theorems 1.7 and 1.8 may allow us to algorithmically determine the complementary optimal covering $\widetilde{\phi}\colon C \to \widetilde{E}$. Before delving into specifics, we will state several useful lemmas, starting with an important result of elimination theory.

Let K be any field and $\overline{K}$ an algebraic closure of K. For any non-negative integer m, let $K[x,y]_m$ denote the K-vector space of all homogeneous polynomials in $K[x,y]$ of degree m. We fix a basis for this space that is given by the monomials $x^m, x^{m-1}y, \ldots, x^{m-i}y^i, \ldots, xy^{m-1}, y^m$. Let $F \in K[x,y]_m$ and $G \in K[x,y]_n$ with $m,n \geq 1$ and consider the map

$$\mu_{F,G}\colon K[x,y]_{n-1} \oplus K[x,y]_{m-1} \to K[x,y]_{m+n-1}, \qquad (A,B) \mapsto AF+BG.$$

This is a linear map between two K-vector spaces, both of dimension $m+n$. The *resultant* $\mathrm{Res}(F,G) \in K$ of F and G is defined to be the determinant of $\mu_{F,G}$ with respect to the monomial bases. We recall some well known properties of resultants, that will be of use to us.

Lemma 1.9 $\mathrm{Res}(F,G) = 0$ *if and only if the polynomials* F *and* G *have a common root in* $\mathbb{P}^1(\overline{K})$.

Proof If F and G have a common root in $\mathbb{P}^1(\overline{K})$, then they must have a common linear factor $L \in \overline{K}[x,y]$. Suppose $F = LF_1$ and $G = LG_1$. Then it is clear that $(-G_1, F_1) \in \overline{K}[x,y]_{n-1} \oplus \overline{K}[x,y]_{m-1}$ is a non-trivial element of $\mathrm{Ker}(\mu_{F,G})$, i.e. $\mu_{F,G}$ is not injective, whence $\mathrm{Res}(F,G) = 0$.

Suppose $\mathrm{Res}(F,G) = 0$. Then $\mu_{F,G}$ is not injective and there exists a non-trivial $(A,B) \in \overline{K}[x,y]_{n-1} \oplus \overline{K}[x,y]_{m-1}$ such that $AF + BG = 0$. Now suppose, without loss of generality, that $A \neq 0$. Then G divides AF in $\overline{K}[x,y]$. Since $\deg A < \deg G$, it must be that F and G have a common factor. □

Remark 1.9 $\mathrm{Res}(F,G)$ is a polynomial in the coefficients of F and G. More precisely, if $F(x,y) = \sum_{i=0}^{m} a_i x^{m-i} y^i$ and $G(x,y) = \sum_{j=0}^{n} b_j x^{n-j} y^j$, then the resultant of F and G is the determinant of their *Sylvester matrix*

$$\mathrm{Res}(F,G) = \det \begin{bmatrix} a_0 & a_1 & \dots & \dots & a_m & 0 & \dots & \dots & \dots & \dots & 0 \\ 0 & a_0 & a_1 & \dots & \dots & a_m & 0 & \dots & \dots & \dots & 0 \\ 0 & 0 & a_0 & a_1 & \dots & \dots & a_m & 0 & \dots & \dots & 0 \\ & & & & & \vdots & & & & & \\ 0 & 0 & \dots & \dots & \dots & 0 & a_0 & a_1 & \dots & \dots & a_m \\ b_0 & b_1 & \dots & b_n & 0 & \dots & \dots & \dots & \dots & \dots & 0 \\ 0 & b_0 & b_1 & \dots & b_n & 0 & \dots & \dots & \dots & \dots & 0 \\ 0 & 0 & b_0 & b_1 & \dots & b_n & 0 & \dots & \dots & \dots & 0 \\ & & & & & \vdots & & & & & \\ 0 & 0 & \dots & \dots & \dots & \dots & 0 & b_0 & b_1 & \dots & b_n \end{bmatrix}.$$

We denote this matrix by $\mathscr{S}_{F,G}$. It has n rows with the coefficients of F and m rows with the coefficients of G. Given two polynomials $f, g \in K[x]$, we define their resultant to be the resultant of their homogenizations $y^{\deg f} f(\frac{x}{y})$ and $y^{\deg g} g(\frac{x}{y})$. The resultant $\mathrm{Res}(f, \frac{\mathrm{d}}{\mathrm{d}x} f(x))$ is denoted by $\mathrm{Disc}(f)$ and is called the *discriminant* of f. By Lemma 1.9, the discriminant $\mathrm{Disc}(f)$ vanishes if and only if f has a double root in $\overline{K}$.

Given $F, G \in K[x_0, x_1, \ldots, x_r]$ for some integer $r \geq 1$, we index their resultant with the appropriate variable(s) in order to clarify in which polynomial ring we consider them to be, e.g. $\mathrm{Res}_{x_0}(F, G)$ for $F, G \in K(x_1, \ldots, x_r)[x_0]$.

Lemma 1.10 *Let $F \in K[x, y]_m$, let $G \in K[x, y]_n$, let $H \in K[x, y]_k$, and let F^* and G^* denote $F(y, x)$ and $G(y, x)$, respectively. Then the following hold:*

(1) $\mathrm{Res}(F, G) = (-1)^{mn}\mathrm{Res}(G, F)$;

(2) $\mathrm{Res}(F^*, G^*) = \mathrm{Res}(G, F)$;

(3) $\mathrm{Res}(xF, G) = b_n\mathrm{Res}(F, G)$;

(4) $\mathrm{Res}(yF, G) = b_0\mathrm{Res}(F, G)$;

(5) $\mathrm{Res}(F, GH) = \mathrm{Res}(F, G)\mathrm{Res}(F, H)$.

Before proceeding with the proof of each claim, we note that *(1)* implies analogous results when the two polynomials, whose resultant is under consideration, have their roles reversed.

Proof $\mathscr{S}_{G,F}$ can be obtained from $\mathscr{S}_{F,G}$ by a permutation of rows that is of parity $(-1)^{mn}$, therefore $\det \mathscr{S}_{F,G} = (-1)^{mn} \det \mathscr{S}_{G,F}$. This implies *(1)*. We can obtain $\mathscr{S}_{F^*,G^*}$ by reversing the order of the rows and the columns of $\mathscr{S}_{G,F}$. Hence $\det \mathscr{S}_{F^*,G^*} = \det \mathscr{S}_{G,F}$, which implies *(2)*. Laplacian expansion of $\det \mathscr{S}_{xF,G}$ along the $(m + n + 1)$-th column gives *(3)*, while *(4)* follows from *(3)* by applying *(2)*.

To prove *(5)*, we first note that, by *(4)* and *(1)*, we can and do assume that y does not divide F, G, or H. Under this assumption, we will infer the claim by proving that

$$\mathrm{Res}(F, G) = a_0^n b_0^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j),$$

where $\alpha_1, \ldots, \alpha_m \in \overline{K}$ and $\beta_1, \ldots, \beta_n \in \overline{K}$ are the roots, not necessarily distinct, of $F(x, 1)$ and $G(x, 1)$, respectively. Since

$$F(x, 1) = a_0 \prod_{i=1}^{m} (x - \alpha_i),$$

$$G(x, 1) = b_0 \prod_{j=1}^{n} (x - \beta_j),$$

this is equivalent to

$$\mathrm{Res}(F,G) = a_0^n \prod_{i=1}^{m} G(\alpha_i, 1) = (-1)^{mn} b_0^m \prod_{j=1}^{n} F(\beta_i, 1). \tag{1.12}$$

We prove this by induction on $m+n$. If $m = n = 1$, we have

$$\mathrm{Res}(a_0x+a_1y, b_0x+b_1y) = \det \begin{bmatrix} a_0 & a_1 \\ b_0 & b_1 \end{bmatrix} = a_0b_1 - a_1b_0 = a_0b_0 \left(-\frac{a_1}{a_0} + \frac{b_1}{b_0} \right),$$

where $a_0b_0 \neq 0$, so (1.12) holds in this case. Now suppose that it holds for any two polynomials whose sum of degrees is smaller than $m+n$. By *(1)*, we can and do suppose that $m \leq n$. By the Euclidean algorithm, there exist Q, R such that $G = FQ + R$ and either $R = 0$ or $\deg R < \deg F = m$. If $R = 0$, then $F(x,1)$ and $G(x,1)$ have a common root, whence $\mathrm{Res}(F,G) = 0$ and (1.12) holds. If $R \neq 0$, let $l = \deg R$ and note that $l < n$.

Also note that $\mathrm{Res}(F,G) = \mathrm{Res}(F, y^{n-l}R)$. The reason is that $\mathscr{S}_{F,y^{n-l}R}$ can be obtained from $\mathscr{S}_{F,G}$ by elementary row operations that do not change the determinant. Namely, if $Q = \sum_{j=0}^{n-m} c_j x^{n-m-j} y^j$, then for each $i \in \{1, \ldots, m\}$ and each $j \in \{0, 1, \ldots, n-m\}$, we multiply the $(i+j)$-th row by $-c_j$ and add it to the $(n+i)$-th row.

By *(4)* and *(1)*, we have $\mathrm{Res}(F,G) = \mathrm{Res}(F, y^{n-l}R) = a_0^{n-l}\mathrm{Res}(F,R)$ and, by the induction hypothesis, we have

$$\mathrm{Res}(F,R) = a_0^l \prod_{i=1}^{m} R(\alpha_i, 1).$$

Together, this gives

$$\mathrm{Res}(F,G) = a_0^n \prod_{i=1}^{m} G(\alpha_i, 1)$$

since $G = FQ + R$ and $F(\alpha_i, 1) = 0$ for each $i \in \{1, \ldots, m\}$. This product formula, along with *(1)* and *(4)*, finally implies

$$\begin{aligned} \mathrm{Res}(F, GH) &= \mathrm{Res}(F,G)\mathrm{Res}(F,H), \\ \mathrm{Res}(FH, G) &= \mathrm{Res}(F,G)\mathrm{Res}(H,G) \end{aligned}$$

for any three homogeneous polynomials in $K[x,y]$. □

Suppose that $f\colon \mathbb{P}^1 \to \mathbb{P}^1$ is a finite K-morphism given as

$$[x\colon y] \mapsto [F(x,y)\colon G(x,y)]$$

and let D be a K-rational divisor on $\mathbb{P}^1$ that is given as the zero locus of a polynomial $P \in K[x,y]$. We have the following two corollaries of the preceding two lemmas.

Corollary 1.11 *The K-rational divisor f_*D is given as the zero locus of*

$$\operatorname{Res}\left(zG(x,y) - wF(x,y), P(x,y)\right) \in K[z,w],$$

where the two polynomials are considered as elements of $K(z,w)[x,y]$.

Corollary 1.12 *The K-rational divisor $f^*f_*D - D$ is given as the zero locus of*

$$\operatorname{Res}\left(\frac{F(x,y)G(z,w) - F(z,w)G(x,y)}{xw - yz}, P(z,w)\right) \in K[x,y],$$

where the two polynomials are considered as elements of $K(x,y)[z,w]$.

Proof The case when D is a point follows easily by Lemma 1.9 and the general case follows by induction, by applying Lemma 1.10. □

These two corollaries play an important role in the following subsections. Another tool we shall use is Gröbner bases, for which [**IVA**] is a useful reference. We now revert back to the notations of the previous sections.

1.4.1 (2,2)-split Jacobians

Let $\phi\colon C \to E$ be an optimal covering of degree 2. The two ramification points of f lie above the K-rational points t_0 and t_4. It follows that the ramification points of f (and hence those of ϕ) are likewise both K-rational. We assume, without loss of generality, that $t_0 = 0$, $t_4 = \infty$, $f(0) = 0$, and $f(\infty) = \infty$, by applying an automorphism of $\mathbb{P}^1$ if necessary. In other words, we may assume that f is given as $x \mapsto x^2 = t$ where t is the local parameter on $E/\iota \cong \mathbb{P}^1$, implying the ramification picture for f that is shown in Fig. 1.5, where $t_i = w_i^2$.

Therefore the curve C is given by a model of the form

$$y^2 = x^6 + ax^4 + bx^2 + c \in K[x].$$

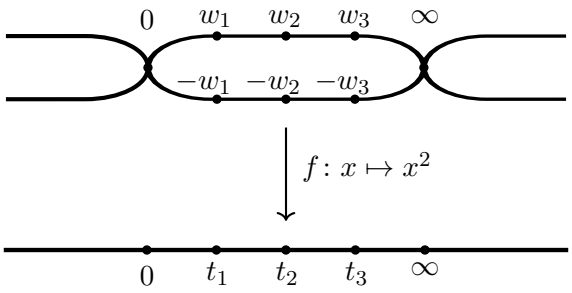


Figure 1.5: Ramification of $f\colon \mathbb{P}^1 \to \mathbb{P}^1$

The elliptic curve E is determined by the branch points $\{t_1, t_2, t_3, \infty\}$, from which we immediately obtain a model, namely

$$s^2 = t^3 + at^2 + bt + c \in K[t].$$

By Theorem 1.8, we know that $\widetilde{f}(\pm w_1), \widetilde{f}(\pm w_2), \widetilde{f}(\pm w_3)$ are three pairwise distinct points. Moreover, we know that $\widetilde{f}$ doubly ramifies above 0 and ∞. Given that we fixed $f(x) = x^2$, there is exactly one choice for $\widetilde{f}$, up to multiplication by a nonzero scalar, namely $\widetilde{f}(x) = 1/x^2$. Thus the elliptic curve $\widetilde{E}$ is determined by the branch points $\{1/t_1, 1/t_2, 1/t_3, \infty\}$ and we obtain a model of $\widetilde{E}$ as $s^2 = \mathrm{Res}_z(1 - tz, t^3 + at^2 + bt + c) = ct^3 + bt^2 + at + 1 \in K[t]$. From this, we can directly calculate

$$j(E) = \frac{2^8(a^2 - 3b)^3}{a^2b^2 - 4b^3 - 4a^3c + 18abc - 27c^2}, \tag{1.13}$$

$$j(\widetilde{E}) = \frac{2^8(b^2 - 3ac)^3}{c^2(a^2b^2 - 4b^3 - 4a^3c + 18abc - 27c^2)}. \tag{1.14}$$

The symmetry between the two is perhaps better appreciated if one homogenizes and views them as functions on $\mathbb{P}^3$. We also note that the denominators do not vanish. Indeed, the fact that the t_j are pairwise distinct is equivalent to the nonvanishing of

$$\mathrm{Disc}_x(x^3 + ax^2 + bx + c) = a^2b^2 - 4b^3 - 4a^3c + 18abc - 27c^2,$$

while the fact that none of the w_i is zero is equivalent to $c \neq 0$.

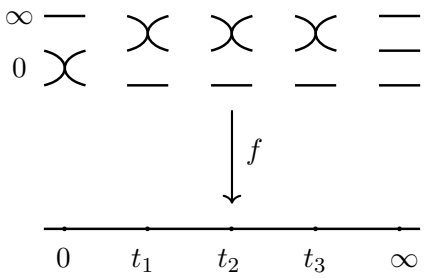
The curve C has an extra automorphism $\sigma\colon (x, y) \mapsto (-x, y)$, which, along with the hyperelliptic involution ι, generates a Klein four-group. Then, taking quotients, we have $C/_{\sigma} \cong E$ and $C/_{\sigma \circ \iota} \cong \widetilde{E}$.

Remark 1.10 The two j-invariants are algebraically independent, meaning that there is no Zariski closed subset of $\mathbb{A}^1 \times \mathbb{A}^1$ that contains the j-invariants of all pairs $(E, \widetilde{E})$ of elliptic curves that admit an optimal covering of degree 2 by the same curve C of genus two. We will come back to this later and see that it is expected.

Remark 1.11 The case of $(2, 2)$-split Jacobians is classically known. Kuhn attributes the solution to Legendre and Jacobi.

1.4.2 (3,3)-split Jacobians

Let $\phi\colon C \to E$ be an optimal covering of degree 3. We treat the generic case first (recall Fig. 1.4). Once more, we have that t_0 and t_4 are K-rational. Also, in view of Corollary 1.5, both points in $f^{-1}(t_0)$ are K-rational. Hence we can and do assume that $t_0 = 0$, $t_4 = \infty$, and $f^*(0) = 2 \cdot 0 + \infty$. This yields the following ramification picture for f:



That is to say that we assume, without loss of generality, that

$$f(x) = \frac{x^2}{x^3 + ax^2 + bx + c},$$

where the denominator, denoted by $P(x)$, has roots w_1, w_2, w_3. Moreover, the w_i are pairwise distinct and none of them equals zero. We can express this

fact as

$$\mathrm{Res}_x(x^2, P(x)) = c^2 \neq 0, \tag{1.15}$$

$$\mathrm{Disc}_x(P(x)) = a^2b^2 - 4b^3 - 4a^3c + 18abc - 27c^2 \neq 0. \tag{1.16}$$

The pullback of $t_1 + t_2 + t_3$ corresponds to roots of $D(x)^2Q(x)$ for some two cubics $D(x), Q(x) \in K[x]$, where the roots of $D(x)$ are the ramification points distinct from 0, and the roots of $Q(x)$ are w_4, w_5, w_6. Now

$$\frac{\mathrm{d}f}{\mathrm{d}x}(x) = -\frac{x(x^3 - bx - 2c)}{P(x)^2}$$

so we can take $D(x) = x^3 - bx - 2c$ because the roots of the numerator are precisely the doubly ramified points of f. These are again pairwise distinct points so we have

$$\mathrm{Disc}_x(D(x)) = 4(b^3 - 27c^2) \neq 0. \tag{1.17}$$

From this we calculate, again via resultants, the nonic $D(x)^2Q(x)$ whose roots are $f^*f_*(d_1 + d_2 + d_3)$, where the d_i are the roots of $D(x)$. We have

$$\mathrm{Res}_y(x^2P(y) - y^2P(x), D(y)) = c(x^3 - bx - 2c)^2(4cx^3 + b^2x^2 + 2bcx + c^2),$$

whence $Q(x) = 4cx^3 + b^2x^2 + 2bcx + c^2$. Therefore the genus two curve C admits a model

$$y^2 = P(x)Q(x) = (x^3 + ax^2 + bx + c)(4cx^3 + b^2x^2 + 2bcx + c^2).$$

In view of Theorem 1.7, we have

$$\widetilde{f}(x) = \frac{(x + d)^2(x + e)}{4cx^3 + b^2x^2 + 2bcx + c^2}$$

for some $d, e \in K$ such that $d \neq e$ and $Q(-d), Q(-e) \neq 0$, i.e.

$$\mathrm{Res}_x(x + d, x + e) \neq 0, \quad \mathrm{Res}_x(x + d, Q(x)) \neq 0, \quad \mathrm{Res}_x(x + e, Q(x)) \neq 0.$$

Condition $\mathrm{Disc}_x(Q(x)) = 16c^4(b^3 - 27c^2) \neq 0$ is superfluous because of (1.15) and (1.17). It remains to find d and e. To this end, we repeat the argument

used to obtain $Q(x)$ from f to the map $\widetilde{f}$. In doing so, we must obtain a multiple of $P(x)$ and this imposes algebraic conditions from which we determine d and e. We have

$$\frac{\mathrm{d}\widetilde{f}}{\mathrm{d}x}(x) = \frac{(x+d)\widetilde{D}(x)}{Q(x)^2},$$

where

$$\begin{aligned}\widetilde{D}(x) \ &= (b^2 - 8cd - 4ce)x^3 + (4bc - b^2d - 12cde)x^2 \\ &\quad + (3c^2 + 2bce - 2b^2de)x + c^2d + 2c^2e - 2bcde.\end{aligned}$$

Now we calculate that

$$\mathrm{Res}_y\left((x+d)^2(x+e)Q(y) - (y+d)^2(y+e)Q(x), \widetilde{D}(y)\right)$$

equals $Q(-d)Q(-e)\widetilde{D}(x)^2R(x)$, where $R(x)$ is the polynomial

$$\begin{aligned}&16c(2c^2d - bcd^2 + cd^4 + c^2e - 2bcde + b^2d^2e - 4cd^3e)x^3 \\ &+ 4(-bc^3 + 2b^2c^2d - b^3cd^2 + 18c^3d^2 - 8bc^2d^3 + 2b^2cd^4 \\ &+ b^2c^2e - 2b^3cde + 12c^3de + b^4d^2e - 12bc^2d^2e - 12c^2d^4e)x^2 \\ &+ (-3c^4 + 10b^2c^2d^2 - 8b^3cd^3 + 48c^3d^3 + b^4d^4 + 4bc^3e - 4b^2c^2de \\ &- 4b^3cd^2e + 72c^3d^2e + 4b^4d^3e - 64bc^2d^3e - 8b^2cd^4e)x - 4c^4d + 8bc^3d^2 \\ &- 4b^2c^2d^3 + 16c^3d^4 + c^4e - 2b^2c^2d^2e + 32c^3d^3e + b^4d^4e - 32bc^2d^4e.\end{aligned}$$

Dividing $R(x)$ by $P(x)$, we obtain the remainder

$$\begin{aligned}&(-4bc^3 + 8b^2c^2d - 32ac^3d - 4b^3cd^2 + 16abc^2d^2 + 72c^3d^2 - 32bc^2d^3 + 8b^2cd^4 \\ &- 16ac^2d^4 + 4b^2c^2e - 16ac^3e - 8b^3cde + 32abc^2de + 48c^3de + 4b^4d^2e \\ &- 16ab^2cd^2e - 48bc^2d^2e + 64ac^2d^3e - 48c^2d^4e)x^2 + (-3c^4 - 32bc^3d \\ &+ 26b^2c^2d^2 - 8b^3cd^3 + 48c^3d^3 + b^4d^4 - 16bc^2d^4 - 12bc^3e + 28b^2c^2de \\ &+ 4b^4d^3e - 8b^2cd^4e)x - 36c^4d + 24bc^3d^2 - 4b^2c^2d^3 - 15c^4e + 32bc^3de \\ &- 20b^3cd^2e + 72c^3d^2e - 18b^2c^2d^2e + 96c^3d^3e + b^4d^4e - 32bc^2d^4e.\end{aligned}$$

Equating it with zero, we obtain three polynomial equations from which we determine

$$d = \frac{3c}{b}, \qquad e = \frac{b^2c - 3ac^2}{b^3 - 4abc + 9c^2}, \tag{1.18}$$

by a Gröbner basis computation. More precisely, we consider d and e as unknowns and solve over the field $K(a,b,c)$, by computing a Gröbner basis for the ideal $I \subset K(a,b,c)[d,e]$ that is generated by the three polynomials that define our three equations. Alternatively, we can factor the polynomials, note that $3c - db$ is a factor in two of them (making one equation superfluous), and then show that there are no other solutions than the one above. Either way, this finally gives

$$\widetilde{f}(x) = \frac{(bx+3c)^2((b^3 - 4abc + 9c^2)x + b^2c - 3ac^2)}{4cx^3 + b^2x^2 + 2bcx + c^2}.$$

A model for E can be determined by requiring that the set of branch points of the quotient map π_E is $\{t_1, t_2, t_3, \infty\}$, i.e. ∞ and the image under f of the three roots of $Q(x)$. A model for $\widetilde{E}$ is similarly determined by requiring that $\pi_{\widetilde{E}}$ ramifies above ∞ and the image under $\widetilde{f}$ of the three roots of $P(x)$. We can find the corresponding cubics from $\mathrm{Res}_x(tP(x) - x^2, Q(x))$ and $\mathrm{Res}_x(tQ(x) - (x+d)^2(x+e), P(x))$, but we omit them here. The modular invariants of the two elliptic curves can be obtained from the two cubics by a direct calculation. We find that

$$j(E) = \frac{2^4(a^2b^4 + 12b^5 - 126ab^3c + 216a^2bc^2 + 405b^2c^2 - 972ac^3)^3}{(b^3 - 27c^2)^3(a^2b^2 - 4b^3 - 4a^3c + 18abc - 27c^2)^2},$$

$$j(\widetilde{E}) = \frac{2^8(a^2 - 3b)^3}{a^2b^2 - 4b^3 - 4a^3c + 18abc - 27c^2}.$$

If $b = 0$, then ∞ is the doubly ramified point of $\widetilde{f}$ above 0. In this case, we obtain, by the same argument, the following:

$$f(x) = \frac{x^2}{x^3 + ax^2 + c}, \qquad \widetilde{f}(x) = \frac{3x - a}{4x^3 + c},$$

$$j(E) = \frac{2^{10}3^6a^3c}{(4a^3 + 27c)^2}, \qquad j(\widetilde{E}) = -\frac{2^8a^6}{c(4a^3 + 27c)}.$$

If $b^3 - 4abc + 9c^2 = 0$, then ∞ is the unramified point of $\widetilde{f}$ above 0. In this case, we obtain:

$$f(x) = \frac{x^2}{4bx^3 + (b^3+9)x^2 + 4b^2x + 4b}, \qquad \widetilde{f}(x) = \frac{(bx+3)^2}{4x^3 + b^2x^2 + 2bx + 1},$$

$$j(E) = \frac{b^3(b^3-24)^3}{b^3-27}, \qquad j(\widetilde{E}) = -\frac{(b^3-27)(b^3-3)^3}{b^3}.$$

Remark 1.12 This is what [**Kuhn**] obtains. It is, at least in part, also classically known, albeit not in a modern setting (see [**Kraz**]).

Remark 1.13 The factors in the numerator and the denominator of f and $\widetilde{f}$ are unique up to multiplication by non-zero constants. Recall that we have assumed (Remark 1.5) that $\mathrm{char}(K) \notin \{2, 3\}$ so that our resultants, including the leading and the tailing terms of the polynomials etc, are not identically zero.

1.4.3 Special cases of $(3,3)$-split Jacobians

Unlike with $(2,2)$-split Jacobians, the $(3,3)$-split case allows for special cases (recall Fig. 1.4). There are two possibilities, namely either one map is special and the other is not, or they are both special. Suppose that f is special and $\widetilde{f}$ is not. Then we can and do assume that 0 is the special, triply ramified point of f so that, by the same arguments as in the previous subsection, we have

$$f(x) = \frac{x^3}{x^3 + ax^2 + bx + c}, \qquad \widetilde{f}(x) = \frac{(x+d)^2(x+e)}{(-b^2+4ac)x^3 + 2bcx^2 + 3c^2x}.$$

Solving for d and e, by imposing the generic ramification picture on $\widetilde{f}$ and using Theorem 1.7, we again obtain

$$d = \frac{3c}{b}, \qquad e = \frac{b^2c - 3ac^2}{b^3 - 4abc + 9c^2},$$

whence

$$\widetilde{f}(x) = \frac{(bx+3c)^2((b^3-4abc+9c^2)x + b^2c - 3ac^2)}{(-b^2+4ac)x^3 + 2bcx^2 + 3c^2x}.$$

We ultimately obtain

$$j(E) = \frac{16(-16b^6 + 144ab^4c - 405a^2b^2c^2 - 108b^3c^2 + 324a^3c^3 + 486abc^3 - 729c^4)^3}{729c^4(-b^2 + 3ac)^3(-a^2b^2 + 4b^3 + 4a^3c - 18abc + 27c^2)^2},$$

$$j(\widetilde{E}) = \frac{2^8(b^2 - 3ac)^3}{c^2(a^2b^2 - 4b^3 - 4a^3c + 18abc - 27c^2)}.$$

Now suppose that both f and $\widetilde{f}$ are special. We assume that 0 is the triply ramified point of f above 0 and that ∞ is the unramified point of f above ∞, that is

$$f(x) = \frac{x^3}{x^2 + ax + b}, \tag{1.19}$$

with $b \neq 0$ and $a^2 - 4b \neq 0$. The argument above, applied to (1.19), implies that ∞ is the triply ramified point of $\widetilde{f}$ above 0, which gives $\widetilde{f}(x) = 1/Q(x)$. We find $Q(x) = (-a^2 + 4b)x^3 + 2abx^2 + 3b^2x$, using Corollary 1.12 and Theorem 1.7. Applying the same argument to $\widetilde{f}(x)$ yields

$$(3a^4 - 24a^2b + 48b^2)x^2 + (-4a^3b + 16ab^2)x - 16a^2b^2 + 48b^3,$$

that must be divisible by $x^2 + ax + b$. Dividing the two, we obtain

$$-a(3a^2 - 8b)(a^2 - 4b)x - a^2b(3a^2 - 8b) \tag{1.20}$$

as remainder. Given that $b \neq 0$ and $a^2 - 4b \neq 0$, equating (1.20) with zero yields two possible solutions, namely $a = 0$ and $b = 3a^2/8$. The first solution gives

$$f(x) = \frac{x^3}{x^2 + b}, \qquad \widetilde{f}(x) = \frac{1}{4x^3 + 3bx}, \qquad j(E) = j(\widetilde{E}) = 1728.$$

Kuhn obtained this solution with $b = 4/3$. However, it would seem that he missed the second solution, namely $a \neq 0, b = 3a^2/8$, which gives

$$f(x) = \frac{x^3}{8x^2 + 8ax + 3a^2}, \qquad \widetilde{f}(x) = \frac{1}{32x^3 + 48ax^2 + 27a^2x},$$

$$j(E) = j(\widetilde{E}) = -\frac{873722816}{59049} = -\frac{2^6 \cdot 239^3}{3^{10}}.$$

Before dealing with the cases of higher degree split Jacobians and generalizing the above, we introduce some prerequisites in the next subsection.

1.4.4 Powers of polynomials

Lemma 1.13 *Let F be a field, let m, n be two positive integers with m coprime to $\mathrm{char}(F)$, and let $A(x) = \sum_{i=0}^{mn} a_i x^i \in F[x]$ be a polynomial of degree mn that is an m-th power of a polynomial $B(x) = \sum_{j=0}^{n} b_j x^j \in \overline{F}[x]$ of degree n. Then $B(x)$ is uniquely determined, up to multiplication by m-th roots of unity, by coefficients $a_{mn}, a_{mn-1}, \ldots, a_{mn-n}$. Consequently, these coefficients uniquely determine $A(x)$.*

Proof It is clear that $b_n^m = a_{mn}$ so the claim is true for the leading coefficient of $B(x)$. Expanding $B(x)^m$, we note that for each $j \in \{0, \ldots, n-1\}$ we have

$$a_{mn-n+j} = m b_j b_n^{m-1} + (\text{terms independent of } b_j). \tag{1.21}$$

To see this, note that if $b_j x^j$ is one of the contributing factors to a summand of $a_{mn-n+j} x^{mn-n+j}$ in the expansion, then the other $m-1$ factors are all $b_n x^n$ because their product is the only possible one of the required degree. Moreover, no coefficient of $B(x)$ of index lower than j can appear in a_{mn-n+j}. Since we assumed that m is not zero in F, we can divide equation (1.21) for each j by m and, starting with $j = n-1$, recursively express the b_j in terms of $a_{mn-1}, a_{mn-2}, \ldots, a_{mn-n}$ and b_n. □

Remark 1.14 With notations as in the preceding lemma, let $\mathrm{char}(F) = p$. Then if $m = p^r m'$ for some $r, m' \in \mathbf{Z}_{>0}$ such that $\gcd(p, m') = 1$, we can reduce this to the case in the lemma by introducing a new variable $X = x^{p^r}$.

Remark 1.15 For any polynomial of degree mn with a fixed non-zero leading coefficient, Lemma 1.13 provides $(m-1)d$ equations that the coefficients of the polynomial satisfy if and only if it is an m-th power. One can take $B(t)$ defined over F if and only if F contains an m-th root of a_{mn}. Another way of obtaining the same equations is computing a Gröbner basis of the ideal $I \subset F[a_0, \ldots, a_{mn}, b_0, \ldots, b_n, u]$ generated by $u a_{mn} - 1$ and the coefficients of $A(t) - B(t)^m$, and then eliminating the variables $b_0, \ldots, b_n$.

Example 1.3 ($n = 3$) Let $a, b, c, d \in F$, where $a \neq 0$, and let $m \geq 2$ be an integer coprime to $\mathrm{char}(F)$. Let $A(x) \in F[x]$ be a polynomial given as

$$A(x) = a^m x^{3m} + b x^{3m-1} + c x^{3m-2} + d x^{3m-3} + \ldots.$$

If $A(x)$ is an m-th power of a cubic $B(x) = \alpha x^3 + \beta x^2 + \gamma x + \delta \in \overline{F}[x]$, then we have

$$\begin{aligned} \alpha &= a \ \text{ (up to mult. by } m\text{-th roots of unity)}, \\ \beta &= \frac{b}{m\alpha^{m-1}}, \\ \gamma &= \frac{c - \binom{m}{2}\alpha^{m-2}\beta^2}{m\alpha^{m-1}}, \\ \delta &= \frac{d - 2\binom{m}{2}\alpha^{m-2}\beta\gamma - \binom{m}{3}\alpha m - 3\beta^3}{m\alpha^{m-1}} \end{aligned} \tag{1.22}$$

whence, up to multiplication by an m-th root of unity, $B(x)$ equals

$$ax^3 + \frac{b}{ma^{m-1}}x^2 + \frac{m^2a^mc - \binom{m}{2}b^2}{m^3a^{2m-1}}x + \frac{m^4a^{2m}d - 2m^2\binom{m}{2}a^mbc + \left(2\binom{m}{2}^2 - m\binom{m}{3}\right)b^3}{m^5a^{3m-1}}.$$

For each $m \in \mathbf{Z}_{>0}$, by expanding $B(x)^m$, we can obtain the remaining coefficients of $A(x)$ in terms of the leading four, which gives us the form of any polynomial of degree $3m$ that is an m-th power of a cubic.

Example 1.4 Over a field F with $\mathrm{char}(F) \neq 2$, every sextic in $F[x]$ that is a square has the form

$$\begin{aligned} ax^6 + bx^5 + cx^4 + dx^3 + \frac{5b^4 - 24ab^2c + 16a^2c^2 + 32a^2bd}{64a^3}x^2 \\ + \frac{(-b^2 + 4ac)(b^3 - 4abc + 8a^2d)}{64a^4}x + \frac{(b^3 - 4abc + 8a^2d)^2}{256a^5} \end{aligned}$$

for some $a, b, c, d \in F$ with $a \neq 0$.

The goal of the following two subsections is to generalize Subsections 1.4.1 and 1.4.2 and describe how one could obtain a parametrization of the modular invariants of the two complementary elliptic curves in the general case.

1.4.5 The odd degree generic case of split Jacobians

Let, as before, $f\colon C/\iota \to E/\iota$ be the map induced by an optimal covering. If $n = \deg f > 3$ is odd, we suppose that the curve C of genus two is given by a model $y^2 = P(x)Q(x)$, where $P(x), Q(x) \in K[x]$ are cubics and $P(x) = x^3 + ax^2 + bx + c$.

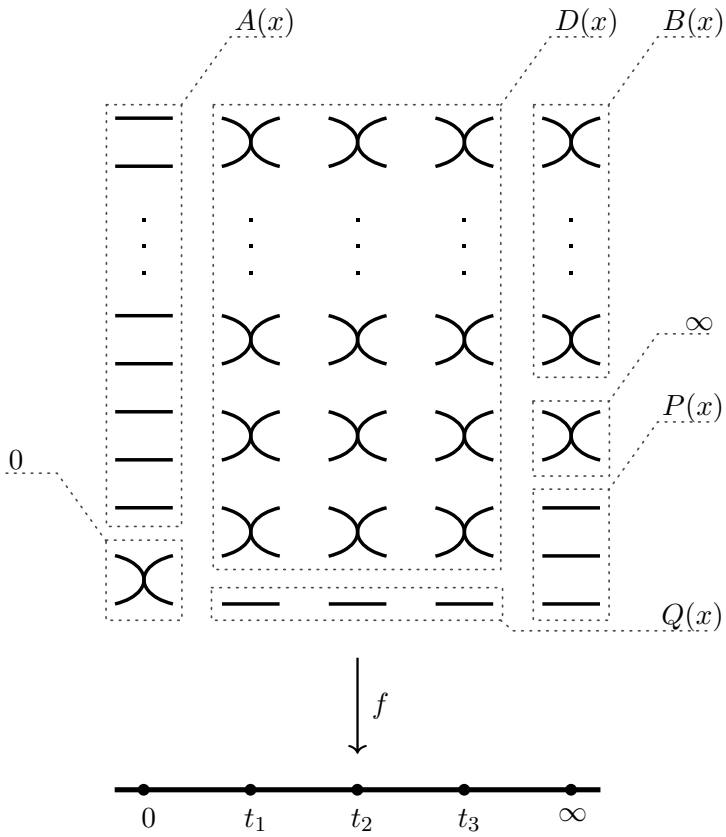


Figure 1.6: Ramification of f in the case of odd degree.

In view of Theorem 1.3, we also suppose that the induced map is given as

$$f(x) = \frac{x^2 A(x)}{P(x)B(x)^2}, \tag{1.23}$$

where

$$A(x) = x^{n-2} + \sum_{i=0}^{n-3} a_i x^i \in K[x],$$
$$B(x) = x^{(n-5)/2} + \sum_{j=0}^{(n-7)/2} b_j x^j \in K[x].$$

In doing so, we assume that 0 and ∞ are points of ramification index 2 in the fibres $f^*(0)$ and $f^*(\infty)$, respectively. To make the ramification of f fit Fig. 1.6, we also must have

$$\begin{aligned} r_1 &:= \mathrm{Res}_x(x, P(x)) \neq 0, & r_2 &:= \mathrm{Res}_x(x, B(x)) \neq 0, \\ r_3 &:= \mathrm{Res}_x(A(x), P(x)) \neq 0, & r_4 &:= \mathrm{Res}_x(A(x), B(x)) \neq 0, \\ r_5 &:= \mathrm{Res}_x(x, A(x)) \neq 0, & r_6 &:= \mathrm{Res}_x(P(x), B(x)) \neq 0, \\ d_1 &:= \mathrm{Disc}_x(P(x)) \neq 0, & d_2 &:= \mathrm{Disc}_x(A(x)) \neq 0, \\ d_3 &:= \mathrm{Disc}_x(B(x)) \neq 0. \end{aligned}$$

The coefficients a, b, c, a_i, b_j are not all free; not all maps of the form (1.23) fit the ramification picture of Fig. 1.6. The imposed distribution of the double points in the fibres above t_1, t_2, t_3 means that we must have

$$f^*(t_1 + t_2 + t_3) = Z(Q) + 2Z(D),$$

where $Z(\cdot)$ denotes the zero locus and

$$\begin{aligned} D(x) \ &= 2A(x)B(x)P(x) + x\frac{\mathrm{d}A}{\mathrm{d}x}(x)B(x)P(x) \\ &\quad - 2xA(x)\frac{\mathrm{d}B}{\mathrm{d}x}(x)P(x) - xA(x)B(x)\frac{\mathrm{d}P}{\mathrm{d}x}(x), \end{aligned}$$

which is a polynomial of degree $\frac{3}{2}(n-1)$. This follows from computing the derivative of f with respect to x. The ramification picture imposes an additional restriction, namely that

$$f_*(Z(D)) = \frac{n-1}{2}Z(U)$$

for some cubic U. By Corollary 1.11, we have that the divisor $f_*(Z(D))$ is the zero locus of

$$M(t) := \frac{1}{r_1 r_2^2 r_3 r_4}\mathrm{Res}_x\left(tP(x)B(x)^2 - x^2A(x), D(x)\right). \tag{1.24}$$

In view of Lemma 1.9, the resultant in (1.24) is divisible by $r_1 r_2^2 r_3 r_4$ because $P(x)B(x)^2$, $x^2A(x)$ and $D(x)$ have a common factor whenever any of the r_i vanish. Note that r_2 appears with an exponent 2 because if it vanishes, the common factor is x^2. It is also worth noting that the factors of the leading (resp. tailing) coefficient of $M(t)$ are d_1, d_3, r_4, r_6 (resp. r_1, r_5, d_2). Indeed,

by Lemma 1.9, the vanishing of any of these resultants corresponds to common factors of $P(x)B(x)^2$ (resp. $x^2A(x)$) and $D(x)$, and a common root of the two is clearly mapped to ∞ (resp. 0) under f, so the claim follows by Corollary 1.11.

In order to determine the unknowns $\{a_i, b_j\}_{i,j}$, of which there are $\frac{3}{2}(n-3)$, in terms of a, b, c, we impose the condition that the polynomial $M(t)$ divided by its leading coefficient equals a $\frac{1}{2}(n-1)$-th power of a cubic $U(t)$ that, up to multiplication by a non-zero constant, equals $(t-t_1)(t-t_2)(t-t_3)$. Equivalently, $M(t)$ is divisible by $U(t)^{\frac{n-1}{2}}$. By Subsection 1.4.4, we get precisely $\frac{3}{2}(n-3)$ equations by imposing the said condition. We obtain the a_i and the b_j in terms of a, b, c, by computing a Gröbner basis of the ideal

$$I \subset K(a,b,c)[a_i, b_j]_{i,j}$$

that is generated by the $\frac{3}{2}(n-3)$ corresponding polynomials. Having determined the form of f in terms of parameters a, b, c, we compute the expression

$$R(x) := \frac{1}{r_1 r_2^2 r_3 r_4} \mathrm{Res}_y \left(\frac{f_1(x)f_2(y) - f_1(y)f_2(x)}{x-y}, D(y) \right) \in K(a,b,c)[x],$$

where $f_1 = x^2A(x)$ and $f_2 = P(x)B(x)^2$. This resultant is a polynomial of degree $\frac{3}{2}(n-1)^2$ and, by Corollary 1.12, it determines the divisor

$$f^*(f_*(Z(D))) - Z(D) = f^*\left(\frac{n-1}{2}Z(U)\right) - Z(D) = \frac{n-1}{2}Z(Q) + (n-2)Z(D).$$

Therefore $R(x)$ must be divisible by $Q(x)^{\frac{n-1}{2}}D(x)^{n-2}$. Let $T(x)$ denote the result of Euclidean division of $R(x)$ by $D(x)^{n-2}$. To obtain $Q(x)$ from $T(x)$, we first divide $T(x)$ by its leading coefficient, which is not zero under our restrictions, and then we use (1.22). Since $Q(x)$ is only unique up to multiplication by a non-zero constant, we can clear the denominators and choose that form for $Q(x)$. Having determined $Q(x)$, Theorem 1.7 implies that we can write

$$\widetilde{f}(x) = \frac{(x+u)^2\widetilde{A}(x)}{Q(x)\widetilde{B}(x)^2}, \tag{1.25}$$

with

$$A(x) = x^{n-2} + \sum_{i=0}^{n-3} \widetilde{a}_i x^i \in K[x],$$

$$B(x) = x^{(n-3)/2} + \sum_{j=0}^{(n-5)/2} \widetilde{b}_j x^j \in K[x],$$

where $u, \widetilde{a}_i, \widetilde{b}_j \in K$ are all to be determined. Note that the number of the unknowns is now increased by two. We repeat the exact same procedure as above, this time starting with (1.25), and obtain the $\frac{3}{2}(n-3)$ equations that must be satisfied by its coefficients because this map has the same ramification picture as f. In the process, we obtain a polynomial $\widetilde{D}(x)$ of degree $\frac{3}{2}(n-1)$, that is a factor of $\mathrm{d}\widetilde{f}/\mathrm{d}x(x)$ and whose zero locus consists of the doubly ramified points of $\widetilde{f}$ above t_1, t_2, t_3. We also obtain a polynomial $\widetilde{M}(t)$ that corresponds to $\widetilde{f}_*(Z(\widetilde{D}))$, that must be divisible by $V(t)^{\frac{n-1}{2}}$, where $V(t) \in K[t]$ is a cubic. We find the corresponding resultant

$$\mathrm{Res}_y\left(\frac{\widetilde{f}_1(x)\widetilde{f}_d(y) - \widetilde{f}_2(y)\widetilde{f}_d(x)}{x-y}, \widetilde{D}(y)\right) \in K(a,b,c)[u, \widetilde{a}_i, \widetilde{b}_j][x],$$

that must be divisible by $\widetilde{r_1}\widetilde{r_2}^2\widetilde{r_3}\widetilde{r_4}\widetilde{P}(x)^{\frac{1}{2}(n-1)}\widetilde{D}(x)^{n-2}$, where

$$\begin{aligned} \widetilde{r_1} &= \mathrm{Res}_x(x+u, Q(x)), & \widetilde{r_2} &= \mathrm{Res}_x(x+u, \widetilde{B}(x)), \\ \widetilde{r_3} &= \mathrm{Res}_x(\widetilde{A}, Q(x)), & \widetilde{r_4} &= \mathrm{Res}_x(\widetilde{A}, \widetilde{B}(x)), \end{aligned}$$

and $\widetilde{P}(x) \in K(a,b,c)[u, \widetilde{a}_i, \widetilde{b}_j][x]$ is a cubic. We divide by $\widetilde{r_1}\widetilde{r_2}^2\widetilde{r_3}\widetilde{r_4}\widetilde{D}(x)^{n-2}$ and express $\widetilde{P}(x)$ using (1.22) again. Three additional equations are obtained by imposing the condition that $P(x) \in K[x]$ is divisible by $\widetilde{P}(x)$. Finally, we solve for $u, \widetilde{a}_i, \widetilde{b}_j$ in terms of a, b, c, by computing a Gröbner basis of the ideal $J \subset K(a,b,c)[u, \widetilde{a}_i, \widetilde{b}_j]_{i,j}$ that is generated by these three equations and the $\frac{3}{2}(n-3)$ equations we had already obtained.

With all the coefficients in f and $\widetilde{f}$ known, we determine $U(t)$ and $V(t)$ using (1.22) and we directly determine the j-invariants of E and $\widetilde{E}$, in terms of the parameters a, b, c, from the models $s^2 = U(t)$ and $s^2 = V(t)$, respectively.

1.4.6 The even degree generic case of split Jacobians

If $\deg f = n > 3$ is even, virtually nothing changes in the approach so we go through it briefly. We suppose that the curve C of genus two is given by a model $y^2 = P(x)$, where $P(x) \in K[x]$ is a sextic, and we suppose that the map $f\colon C/_\iota \to E/_\iota$ is given as

$$f(x) = \frac{x^2 A(x)}{B(x)^2},$$

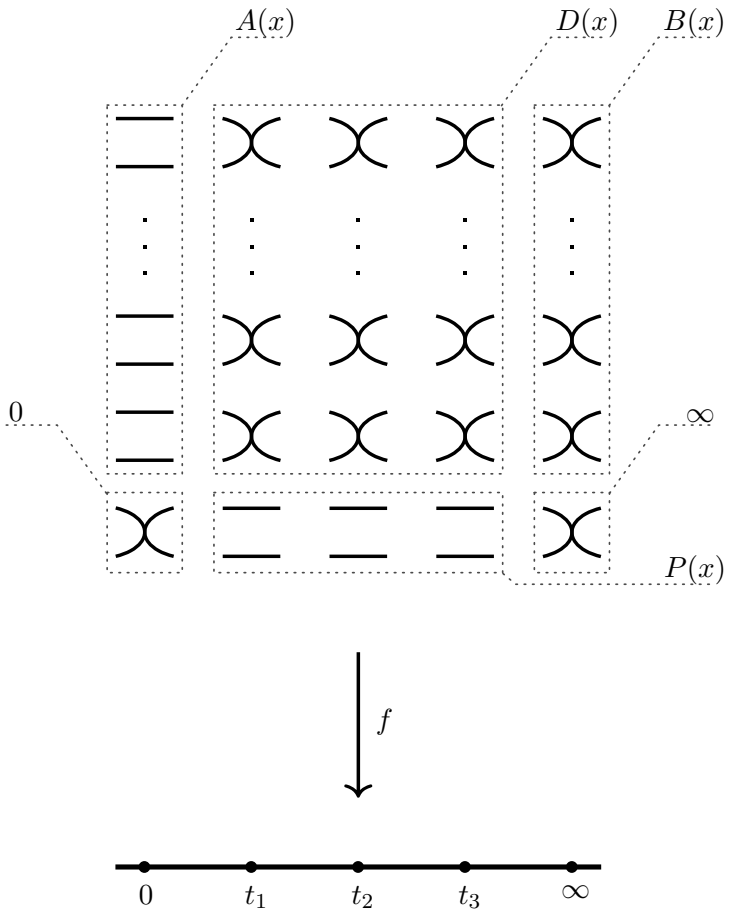


Figure 1.7: Ramification of f in the case of even degree.

where

$$A(x) = x^{n-2} + \sum_{i=0}^{n-3} a_i x^i \in K[x],$$
$$B(x) = x^{(n-2)/2} + \sum_{j=0}^{(n-4)/2} b_j x^j \in K[x].$$

It follows from the ramification picture of f in Fig. 1.7 that we must have

$$r_1 := \mathrm{Res}_x(x, A(x)) \neq 0, \qquad r_2 := \mathrm{Res}_x(x, B(x)) \neq 0,$$
$$r_3 := \mathrm{Res}_x(A(x), B(x)) \neq 0, \qquad r_4 := \mathrm{Res}_x(x(x), A(x)) \neq 0,$$
$$d_1 := \mathrm{Disc}_x(A(x)) \neq 0, \qquad d_2 := \mathrm{Disc}_x(B(x)) \neq 0.$$

As opposed to the case of odd n, we use a different set of three parameters, namely a_1, a_0, b_0. We are left with $\frac{3}{2}(n-4)$ unknowns. The ramification behaviour of f also forces $f^*(t_1+t_2+t_3) = Z(P) + 2Z(D)$, where

$$D(x) = -2A(x)B(x) - x\frac{\mathrm{d}A}{\mathrm{d}x}(x)B(x) + 2xA(x)\frac{\mathrm{d}B}{\mathrm{d}x}(x) \in K[x],$$

which is of degree $\frac{3}{2}(n-2)$ and is a factor of $\mathrm{d}f(x)/\mathrm{d}x$. As before, we calculate

$$M(t) := \frac{1}{r_1 r_2^2}\mathrm{Res}_x\left(tB(x)^2 - x^2A(x), D(x)\right)$$

and impose the conditions on its coefficients that make it divisible by $U(t)^{\frac{n-2}{2}}$, where $U(t) \in K[t]$ is a cubic. In view of Example 1.3, this provides us with $\frac{3}{2}(n-4)$ equations that we solve for a_i, b_j in terms of a_1, a_0, b_0, by computing a Gröbner basis of the ideal $I \subset K(a_1, a_0, b_0)[a_i, b_j]_{i\neq 0,1,\, j\neq 0}$ that is generated by the equations.

The defining equation $y^2 = P(x)$ of C is found by calculating

$$\frac{1}{r_1 r_2^2}\mathrm{Res}_y\left(\frac{f_1(x)f_2(y) - f_1(y)f_2(x)}{x-y}, D(y)\right) \in K[x], \tag{1.26}$$

where $f_1(x) = x^2A(x)$ and $f_2(x) = B(x)^2$. We obtain a polynomial of degree $\frac{3}{2}(n-1)(n-2)$ that must be divisible by $P(x)^{\frac{n-2}{2}}D(x)^{n-3}$. Performing Euclidean division of (1.26) by $D(x)^{n-3}$, we obtain some polynomial $T(x)$. We obtain $P(x)$ from $T(x)$, up to multiplication by a non-zero constant, by using the same principle from Subsection 1.4.4 that we applied in the case of odd degree, only this time for a sextic.

By Theorem 1.8, the map $\widetilde{f}$ must have the same ramification picture as f and therefore it must be of the form

$$\widetilde{f}(x) = \frac{(x+u)^2\widetilde{A}(x)}{\widetilde{B}(x)^2},$$

where

$$\widetilde{A}(x) = x^{n-2} + \sum_{i=0}^{n-3}\widetilde{a}_i x^i \in K[x],$$

$$B(x) = x^{n/2} + \sum_{j=0}^{(n-2)/2}\widetilde{b}_j x^j \in K[x].$$

Again, we find $\widetilde{D}(x) = 2A(x)B(x) + (x+u)\frac{\mathrm{d}A}{\mathrm{d}x}(x)B(x) - 2(x+u)A(x)\frac{\mathrm{d}B}{\mathrm{d}x}(x)$, the factor of $\mathrm{d}\widetilde{f}(x)/\mathrm{d}x$ whose zero locus consists of the double ramification points of $\widetilde{f}$ above t_1, t_2, t_3, whence we also obtain the polynomial $\widetilde{M}(t)$ that corresponds to $\widetilde{f}_*(Z(\widetilde{D}))$. We obtain $\frac{3}{2}(n-4)$ polynomial equations that the coefficients of $\widetilde{M}(t)$ must satisfy, by imposing that $\widetilde{M}(t)$ is divisible by $V(t)^{\frac{n-2}{2}}$ where $V(t) \in K[t]$ is a cubic. To obtain additional equations, we compute the resultant analogous to (1.26), that corresponds to $\widetilde{f}^*(\widetilde{f}_*(Z(\widetilde{D}))) - Z(\widetilde{D})$. This yields a polynomial of degree $\frac{3}{2}(n-1)(n-2)$ that must be divisible by $Q(x)^{\frac{n-2}{2}}\widetilde{D}(x)^{n-3}$. From this we determine $Q(x)$. Theorem 1.8 implies that $Q(x)$ divides $P(x)$, and imposing this condition on the coefficients gives six additional equations. Finally, we solve all the equations in terms of a_1, a_0, b_0 for the remaining coefficients, by computing a Gröbner basis of the ideal

$$J \subset K(a_1, a_0, b_0)[u, \widetilde{a}_i, \widetilde{b}_j]$$

that they generate.

Remark 1.16 If $n = \deg\phi = \deg f$ is a prime, then ϕ and $\widetilde{\phi}$ are necessarily optimal because if they factor through an isogeny, the isogeny must be of degree 1. However, for composite n, one must also impose additional conditions on the final forms of f and $\widetilde{f}$ in order to make sure that the corresponding coverings do not factor through non-trivial isogenies. Moreover, the choice of the parameters is not canonical. While in the case of odd n it might seem logical to begin with $P(x) = x^3 + ax^2 + bx + c$ just as in the case of $n = 3$, the choice is less clear in the case of even n, except when $n = 4$ when there is only one choice. Unfortunately, the suggested computations are unfeasible in practice, even for small degrees, due to the complexity of Gröbner bases algorithms over the field $F(a, b, c)$, even for F finite. Computing symbolic determinants also becomes unfeasible as the dimension increases.

1.5 A different point of view

In Section 1.3 we started with an optimal covering map $C \to E_1$ of degree n and constructed the complementary curve E_2. In this section, we present an alternative point of view. We start instead with two elliptic curves and a particular kind of K-isomorphism between their n-torsions, and construct the curve C of genus two from this data. This approach can be found in [**Fr-Ka**]. We begin by recalling some definitions and an important lemma.

Let A be an abelian variety over K and $\lambda\colon A \to A^\vee$ a polarization. Suppose that $m \in \mathbf{Z}$ is coprime to $\mathrm{char}(K)$ and such that $\mathrm{Ker}(\lambda) \subset A[m]$, and let

$$e_m\colon A[m](\overline{K}) \times A^\vee[m](\overline{K}) \to \mu_m$$

be the Weil pairing. Then we can associate to λ a skew-symmetric pairing

$$e_\lambda\colon \mathrm{Ker}(\lambda) \times \mathrm{Ker}(\lambda) \to \mu_m$$

that is defined for geometric points P, Q as $e_\lambda(P,Q) = e_m(P, \lambda(R))$, for any R such that $[m]R = Q$. This does not depend on R or m (see §16 in [**Miln1**]).

Lemma 1.14 (Mumford) *Let $\varphi\colon A \to B$ be an isogeny whose degree is coprime to $\mathrm{char}(K)$ and let $\lambda\colon A \to A^\vee$ be a polarization. Then $\lambda = \varphi^*(\lambda')$ for some polarization $\lambda'\colon B \to B^\vee$ if and only if $\mathrm{Ker}(\varphi) \subset \mathrm{Ker}(\lambda)$ and e_λ is trivial on $\mathrm{Ker}(\varphi) \times \mathrm{Ker}(\varphi)$.*

Proof See Proposition 16.8 in [**Miln1**] or Theorem 2 and its Corollary in §23 in [**MumAV**]. □

Corollary 1.15 *Let $\phi\colon C \to E_1$ be an optimal covering of an elliptic curve by a curve of genus two, such that $\deg \phi = n$ is coprime to $\mathrm{char}(K)$, and let E_2 be the complementary elliptic curve. Let $\alpha\colon E_1[n] \xrightarrow{\sim} E_2[n]$ be the induced canonical isomorphism (with respect to an embedding of C; recall Lemma 1.6). Then α inverts the Weil pairing, i.e.*

$$e_n(P,Q) = e_n\left(\alpha(P), \alpha(Q)\right)^{-1}$$

for any $P, Q \in E_1[n](\overline{K})$.

Proof By Lemma 1.6, we have an isogeny $\varphi\colon E_1 \times E_2 \to \mathrm{Jac}(C)$ that is polarized with respect to $[n] \circ \lambda_\Theta$ and λ_C, i.e. $\varphi^*(\mathscr{L}(C)) = \mathscr{L}(n\Theta)$. Moreover, we have $\mathrm{Ker}(\varphi) \cong \Gamma_\alpha$. Lemma 1.14 implies $\mathrm{Ker}(\varphi) \subset (E_1 \times E_2)[n]$. It follows that for any geometric point of $\mathrm{Ker}(\varphi) \times \mathrm{Ker}(\varphi)$ that corresponds to a point of the form $((P,Q),\ (\alpha(P), \alpha(Q)))$, we have

$$1 = e_n\left((P,Q),\ (\alpha(P), \alpha(Q))\right) = e_n(P,Q) \cdot e_n(\alpha(P), \alpha(Q)).$$

This completes the proof. □

In view of Lemma 1.14, we begin with two elliptic curves E_1 and E_2. Let $n \geq 2$ be an integer coprime to $\mathrm{char}(K)$ and let $\alpha\colon\ E_1[n] \xrightarrow{\sim} E_2[n]$ be an isomorphism of K-group schemes between the n-torsion subgroups of the two curves, such that

$$e_n(\alpha(P), \alpha(Q)) = e_n(P, Q)^{-1} \tag{1.27}$$

for any $P, Q \in E_1[n](\overline{K})$. In other words, the isomorphism α is *anti-symplectic* with respect to the Weil pairing.

Let λ_Θ be the usual principal polarization of $E_1 \times E_2$, namely the one induced by the divisor $\Theta = \{0_{E_1}\} \times E_2 + E_1 \times \{0_{E_2}\}$, let $\Gamma_\alpha \subset (E_1 \times E_2)[n]$ denote the graph of α, and let

$$\varphi\colon E_1 \times E_2 \to (E_1 \times E_2)/\Gamma_\alpha =: J$$

be the canonical map. The map φ is an isogeny, being surjective and of finite kernel. We also let $\eta_i\colon E_i \to E_1 \times E_2$ denote the canonical embeddings and we let $p_i\colon E_1 \times E_2 \to E_i$ denote the canonical projections.

Lemma 1.16 *The isogeny $\varphi\colon E_1 \times E_2 \to J$ induces a principal polarization of J.*

Proof By Lemma 1.14, the condition (1.27) implies that there exists a line bundle $\mathscr{M} \in \mathrm{Pic}(J)$ such that $\varphi^*(\mathscr{M}) = \mathscr{L}(n\Theta)$. This bundle naturally induces a polarization $\lambda_{\mathscr{M}}\colon J \to J^\vee$ given by

$$\lambda_{\mathscr{M}}\colon P \mapsto t_P^*\mathscr{M} \otimes \mathscr{M}^{-1}.$$

Now let $D \in \mathrm{Div}(J \otimes \overline{K})$ be any divisor such that $\mathscr{M} \cong \mathscr{L}(D)$ and let $D_1 := E_1 \times \{0_{E_2}\}$ and $D_2 := \{0_{E_1}\} \times E_2$, so that $\Theta = D_1 + D_2$. Both D_1 and D_2 are fibres of projections, namely $D_i = p_j^*(0_{E_j})$. Since any two fibres of p_i are algebraically equivalent, it follows that they are also numerically equivalent (see [**HAG**], see pp. 364–367) and we have

$$D_1 \cdot D_1 = D_2 \cdot D_2 = 0. \tag{1.28}$$

Since D_1 and D_2 meet transversally with $D_1 \cap D_2 = \{(0_{E_1}, 0_{E_2})\}$, we also have

$$D_1 \cdot D_2 = 1 \tag{1.29}$$

(see V.1.3 and V.1.5 in [**HAG**]). Equalities (1.28) and (1.29) together give

$$\Theta \cdot \Theta = D_1 \cdot D_1 + 2D_1 \cdot D_2 + D_2 \cdot D_2 = 2.$$

Now the Projection Formula gives

$$n^2\Theta \cdot \Theta = n\Theta \cdot n\Theta = \varphi^*(D) \cdot \varphi^*(D) = \deg \varphi D \cdot D = n^2 D \cdot D$$

whence $D \cdot D = 2$. Therefore, by Riemann-Roch (see §16 in [**MumAV**]), we have

$$\deg \lambda_{\mathscr{M}} = \frac{D \cdot D}{2} = 1,$$

i.e. the polarization $\lambda_{\mathscr{M}} \colon J \to J^\vee$ is principal. □

Remark 1.17 The polarization $\lambda_{\mathscr{M}}$ is defined over K and does not depend on D.

Lemma 1.16 implies that we have the following commutative diagrams, analogous to (1.8) and (1.9):

$$\begin{array}{ccc} E_1 \times E_2 & \xrightarrow{[n] \circ \lambda_\Theta} & (E_1 \times E_2)^\vee \\ \downarrow{\scriptstyle \varphi} & & \uparrow{\scriptstyle \varphi^\vee} \\ J & \xrightarrow[\sim]{\lambda_{\mathscr{M}}} & J^\vee \end{array} \tag{1.30}$$

$$\begin{array}{ccc} J & \xrightarrow{[n] \circ \lambda_{\mathscr{M}}} & J^\vee \\ {\scriptstyle \lambda_\Theta^{-1} \circ \varphi^\vee \circ \lambda_{\mathscr{M}}}\downarrow & & \uparrow{\scriptstyle \lambda_{\mathscr{M}} \circ \varphi \circ \lambda_\Theta^{-1}} \\ E_1 \times E_2 & \xrightarrow[\sim]{\lambda_\Theta} & (E_1 \times E_2)^\vee \end{array} \tag{1.31}$$

Let $\psi := \lambda_\Theta^{-1} \circ \varphi^\vee \circ \lambda_{\mathscr{M}}$, for convenience. Then we have the following two exact sequences:

$$0 \longrightarrow E_1 \xrightarrow{\varphi \circ \eta_1} J \xrightarrow{p_1 \circ \psi} E_2 \longrightarrow 0, \tag{1.32}$$

$$0 \longrightarrow E_2 \xrightarrow{\varphi \circ \eta_2} J \xrightarrow{p_2 \circ \psi} E_1 \longrightarrow 0, \tag{1.33}$$

that are analogous to (1.6) and (1.7).

Let $\mathcal{S}$ be the set containing the effective divisors $D \in \mathrm{Div}(J \otimes \overline{K})$ such that $\varphi^*(D) \sim n\Theta$. For any $D_1, D_2 \in \mathcal{S}$, we have $\mathscr{L}(D_1 - D_2) \in \mathrm{Ker}(\varphi^\vee)$. The polarization $\lambda_{\mathscr{M}}$ induces an isomorphism $\mathrm{Ker}(\varphi^\vee) \cong \mathrm{Ker}(\lambda_\Theta^{-1} \circ \varphi^\vee \circ \lambda_{\mathscr{M}})$ and therefore $\mathrm{Ker}(\varphi^\vee)(\overline{K})$ acts freely and transitively on $\mathcal{S}$ via translation, whence

$$\#S = \#\mathrm{Ker}(\varphi^\vee) = \#\mathrm{Ker}(\varphi) = n^2.$$

Lemma 1.17 *If n is odd, then there exists a unique divisor $C \in \mathcal{S}$ such that $-\mathbb{1}_J(C) = C$. This divisor is K-rational and $\varphi^*(C)$ is the unique divisor in $\varphi^*(\mathrm{Div}(J))$ that is both linearly equivalent to $n\Theta$ and fixed by $-\mathbb{1}_{E_1 \times E_2}$.*

Proof For any $D \in \mathcal{S}$, we have

$$\varphi^*(-\mathbb{1}_J(D)) = -\mathbb{1}_{E_1 \times E_2}(\varphi^*(D)) \sim -\mathbb{1}_{E_1 \times E_2}(n\Theta) = n\Theta$$

so that $-\mathbb{1}_J$ acts on $\mathcal{S}$. Since $\#S = n^2$ is odd, the action of $-\mathbb{1}_J$ must fix some $C \in \mathcal{S}$. Suppose that some $C' \in \mathcal{S}$ is also fixed. Then $C' = t_P(C)$ for some $P \in \mathrm{Ker}(\psi)$, which means that $C' = t_P(C) = t_{-P}(C)$ and therefore $2P = 0$. This implies that $P = 0$ since $\#\mathrm{Ker}(\psi) = n^2$ is odd. □

By Riemann-Roch, we have

$$p_a(C) = \frac{C \cdot C}{2} + 1 = 2$$

and therefore $(p_i \circ \psi)_{|C} \colon C \to E_i$ are both coverings of degree n. However, we are not necessarily in the situation described in Section 1.2 because C, although of arithmetic genus 2, need not be irreducible.

Remark 1.18 The elements of $\mathcal{S}$ are either all irreducible or all reducible, since they are translates of each other.

With Lemmas 1.16 and 1.17 in mind, we recall the following classical result.

Theorem 1.18 (Weil) *Let A be a polarized abelian surface with a polarization induced by $\mathscr{L}(D)$ such that $D \cdot D = 2$. Then exactly one of the following two holds:*

(1) D is a curve of genus two and A is the canonically polarized Jacobian of D, with D embedded into A;

(2) A is the product $E_1 \times E_2$ of two elliptic curves E_1 and E_2, and D is of the form $\{a_1\} \times E_2 + E_1 \times \{a_2\}$ for some $a_1 \in E_1$ and $a_2 \in E_2$.

Proof This is Satz 2 in [**Weil**]. □

Corollary 1.19 *If an element $D \in \mathcal{S}$ is reducible, then we have $D = F_1 + F_2$ and $J \cong F_1 \times F_2$, where F_1 and F_2 are elliptic curves. Moreover, the elliptic curves E_1, E_2, F_1, F_2 are all isogenous.*

Proof The first claim follows directly from Theorem 1.18. Let

$$\varepsilon_i := \varphi \circ \eta_i \colon E_i \to J$$

be the induced embeddings, by (1.32) and (1.33). By the same argument as in the proof of Lemma 1.16, the self-intersection numbers of E_1, E_2, F_1, F_2 are all zero. It is also true that

$$\begin{aligned} &\varepsilon_1(E_1) \cdot F_1 \neq 0, \qquad &&\varepsilon_2(E_2) \cdot F_1 \neq 0, \\ &\varepsilon_1(E_1) \cdot F_2 \neq 0, \qquad &&\varepsilon_2(E_2) \cdot F_2 \neq 0. \end{aligned} \tag{1.34}$$

Indeed, suppose that for some i we have $\varepsilon_i(E_i) \cdot F_1 = 0$. Then $F_1 = t_P(\varepsilon_i(E_i))$ for some point P, and for $j \neq i$ we have

$$\varepsilon_j(E_j) \cdot F_1 = \varepsilon_j(E_j) \cdot \varepsilon_i(E_i) = \#\mathrm{Ker}(\varphi) = n^2,$$

which implies

$$n = E_j \cdot n\Theta = \varepsilon_j(E_j) \cdot D = \varepsilon_j(E_j) \cdot (F_1 + F_2) \geq n^2,$$

which is a contradiction. The same argument shows that $\varepsilon_i(E_i) \cdot F_2 \neq 0$. It now follows that $\varepsilon_1(E_1)$ and $\varepsilon_2(E_2)$ are not translates of F_1 and F_2 in J and since $\varphi \colon E_1 \times E_2 \to F_1 \times F_2$ is an isogeny, all four curves are isogenous. □

Proposition 1.2 ([**Fr-Ka**]) *There exist examples where the elements of $\mathcal{S}$ are reducible.*

Proof Let $\gamma \colon E_1 \longrightarrow E_2$ be an isogeny of two elliptic curves, of degree $n - 1$. Let $\alpha \colon E_1[n] \xrightarrow{\sim} E_2[n]$ be the anti-symplectic isomorphism that is the restriction of γ to the n-torsion and let Γ_α denote its graph. Then the map

$$\phi \colon E_1 \times E_2 \to E_1 \times E_2, \quad (P, Q) \mapsto (nP, Q - \gamma(P))$$

is an isogeny with kernel $\mathrm{Ker}(\phi) = \Gamma_\alpha$ and therefore

$$J := (E_1 \times E_2)/\Gamma_\alpha \cong E_1 \times E_2.$$ □

Frey and Kani (see §2 in [**Fr-Ka**]) also give the following "irreducibility criterion".

Proposition 1.3 *Let $n \in \mathbf{Z}_{>0}$ be odd, let E_1 and E_2 be two elliptic curves without K-rational points of order two, and let $\alpha\colon E_1[n] \xrightarrow{\sim} E_2[n]$ be an anti-symplectic isomorphism. Then the induced curve C, that polarizes the quotient $J := (E_1 \times E_2)/\Gamma_\alpha$, is irreducible if and only if $0_J \notin C$.*

Proof First suppose that C is reducible, say $C = F_1 + F_2$. Then we have $F_1 \cap F_2 = \{P\}$ for some point $P \in J[2](K)$. Since φ induces an isomorphism between $J[2]$ and $(E_1 \times E_2)[2]$, we have $J[2](K) = \{0_J\}$ and therefore $P = 0_J$. On the other hand, if C is irreducible, the configuration of the Weierstraß points of C when $\deg \varphi = n$ is odd (Theorem 1.3) implies that $0_J \notin C(K)$, having embedded C into J via $P \mapsto [P - W_1 + W_2 - W_3]$ (or $P \mapsto [P - W_4 + W_5 - W_6]$). □

1.5.1 Gluing two elliptic curves along their 2-torsion

In this subsection, we will consider in more detail the special case of $n = 2$.

Example 1.5 Let E_1 and E_2 be elliptic curves and let $\alpha\colon E_1[2] \xrightarrow{\sim} E_2[2]$ be an isomorphism. Then α is necessarily anti-symplectic because the Weil pairing takes values in $\{-1, 1\}$, meaning that the two curves can always be glued (over K) along their 2-torsion to form a (principally polarized) abelian surface.

Proposition 1.4 *If $n = 2$, then the elements of $\mathcal{S}$ are reducible if and only if α is induced by an isomorphism $\gamma\colon E_1 \xrightarrow{\sim} E_2$. Moreover, with notations as above, if $n = 2$ and $J \cong F_1 \times F_2$, then $E_1 \cong E_2 \cong F_1 \cong F_2$.*

Proof Let $D \in \mathcal{S}$ and suppose $D = F_1 + F_2$, where F_1 and F_2 are elliptic curves. Let $\varphi\colon E_1 \times E_2 \to F_1 \times F_2$ be the isogeny with kernel $\mathrm{Ker}(\varphi) = \Gamma_\alpha$. We denote by η_i the canonical embeddings $E_i \hookrightarrow E_1 \times E_2$ and $F_i \hookrightarrow F_1 \times F_2$, and we denote by p_i the canonical projections $E_1 \times E_2 \to E_i$ and $F_1 \times F_2 \to F_i$. Slightly abusing notation, we also denote by E_i and F_i the images of the corresponding curves under η_i. We claim that the composition

$$\gamma_{ij}\colon E_i \xrightarrow{\eta_i} E_1 \times E_2 \xrightarrow{\varphi} F_1 \times F_2 \xrightarrow{p_j} F_j$$

is an isomorphism, where $i, j \in \{1, 2\}$. With $\varepsilon_i = \varphi \circ \eta_i$, we have

$$n = 2 = \varepsilon_i(E_i) \cdot D = \varepsilon_i(E_i) \cdot (F_1 + F_2)$$

and $\varepsilon_i(E_i) \cdot F_j \neq 0$, whence $\varepsilon_i(E_i) \cdot F_j = 1$. Therefore $\varepsilon_i(E_i)$ has precisely one point in common with F_j and all its translates (in J) and it follows that the projection of $\varepsilon_i(E_i)$ to F_j is an isomorphism. It remains to show that the isomorphisms

$$\gamma_{1i} \circ \gamma_{2i}^{-1} \colon E_1 \to E_2, \quad i \in \{1, 2\}$$

agree with α on the 2-torsion. Let $P \in E_1[2]$ and note that

$$\begin{aligned}(P, 0) + \Gamma_\alpha &= \{(P + T, \alpha(T)) \mid T \in E_1[2]\} \\ &= \{(T, \alpha(T - P)) \mid T \in E_1[2]\} \\ &= (0, -\alpha(P)) + \Gamma_\alpha \\ &= (0, \alpha(P)) + \Gamma_\alpha,\end{aligned}$$

where the last equality follows from the fact that $\alpha(P)$ is a 2-torsion point. It follows that $\varepsilon_1(P) = \varepsilon_2(\alpha(P)) \in J$ and therefore $\gamma_{1i} \circ \gamma_{2i}^{-1}(P) = \alpha(P)$. The other direction follows from Proposition 1.2. □

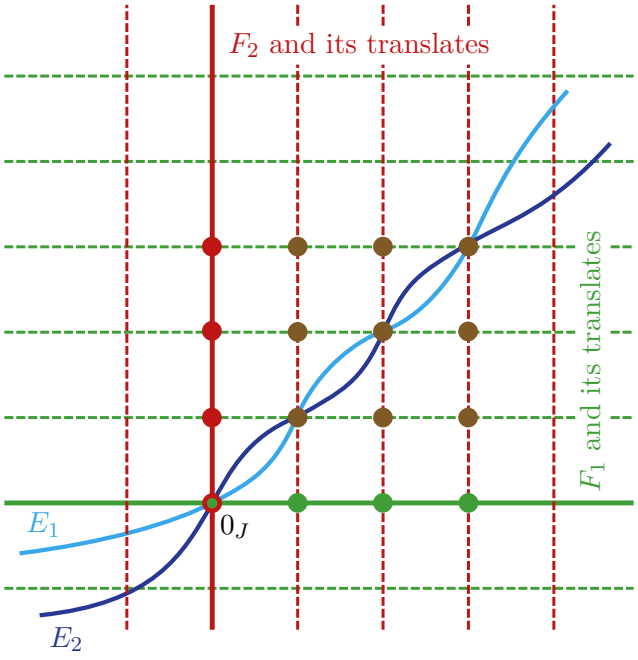


Figure 1.8: An illustration of E_1 and E_2 glued along 2-torsion inside $J \cong F_1 \times F_2$; the marked points denote $J[2]$.

Proposition 1.5 *Let E_1 and E_2 be two isomorphic elliptic curves with a modular invariant $j(E_i) \notin \{0, 1728\}$. Then they can be glued over K along the 2-torsion if and only if at least one of the following two conditions holds:*

(1) E_1 (and therefore E_2) has a K-rational point of order two;

(2) The minimal discriminant of E_1 (and E_2) is a square in K.

Proof Note that $j(E_i) \notin \{0, 1728\}$ implies that $\mathrm{Aut}(E_i) = \{\pm\mathbb{1}\}$ and that both automorphisms fix the 2-torsion pointwise. We choose a model

$$E\colon y^2z = x^3 + ax^2z + bxz^2 + cz^3$$

for both curves, where $a, b, c \in K$. In particular, we have $0_E = [0 : 1 : 0]$. In addition to this point, the 2-torsion consists of three more geometric points, namely

$$[r : 0 : 1], \quad [s : 0 : 1], \quad [t : 0 : 1],$$

where $r, s, t \in \overline{K}$ are the three distinct roots of $x^3 + ax^2 + bx + c \in K[x]$. Since any isomorphism $\alpha\colon E_1[2] \xrightarrow{\sim} E_2[2]$ is necessarily anti-symplectic, we only need to show precisely when the possible automorphisms $\alpha\colon E[2] \xrightarrow{\sim} E[2]$ are K-rational (the identity map being excluded, by Proposition 1.4). It is readily seen that α can be realized as

$$\alpha\colon [x : y : z] \mapsto [ux^2 + vxz + wz^2 : y^2 : z^2]$$

for some $u, v, w \in \overline{K}$. We distinguish two cases:

(1) α is an odd permutation of the points of order two, i.e. it fixes exactly one point of order two;

(2) α is an even permutation of the points of order two, i.e. it fixes none of the points of order two.

We deal with case (1) first. Suppose, without loss of generality, that $[r : 0 : 1]$ is fixed by α. Then under α we have

$$[s : 0 : 1] \mapsto [t : 0 : 1], \quad [t : 0 : 1] \mapsto [s : 0 : 1],$$

which implies that $ux^2 + vx + w \in \overline{K}[x]$ must equal the Lagrange polynomial

$$r\frac{x-s}{r-s}\frac{x-t}{r-t} + t\frac{x-r}{s-r}\frac{x-t}{s-t} + s\frac{x-r}{t-r}\frac{x-s}{t-s} = \frac{2r-s-t}{(r-s)(r-t)}x^2 + \frac{-r^2+s^2+t^2-rs-rt+st}{(r-s)(r-t)}x + \frac{r^2s-rs^2+r^2t-rt^2}{(r-s)(r-t)}.$$

Treating $u, v, w, a, b, c, r, s, t$ as variables, let $I_q \subset K[q, a, b, c, r, s, t]$ denote the ideal generated by four elements, namely the three polynomials

$$a + r + s + t, \quad -b + rs + rt + st, \quad c + rst,$$

and the fourth polynomial

$$\begin{aligned} &- u(r-s)(r-t) + 2r - s - t && \text{for } q = u, \\ &- v(r-s)(r-t) - r^2 + s^2 + t^2 - rs - rt + st && \text{for } q = v, \\ &- w(r-s)(r-t) + r^2s - rs^2 + r^2t - rt^2 && \text{for } q = w. \end{aligned}$$

Eliminating the variables s and t from each I_q, we obtain

$$u = \frac{3r+a}{3r^2+2ra+b}, \quad v = \frac{2ra+a^2-b}{3r^2+2ra+b}, \quad w = \frac{r^3-ra^2+3rb+c}{3r^2+2ra+b}. \tag{1.35}$$

It follows that $u, v, w \in K$ whenever $r \in K$. On the other hand, we verify easily that

$$r = \frac{1-au+v}{u}$$

if $u \neq 0$. If $u = 0$ and $\operatorname{char}(K) \neq 3$, then $v = -1$ and $r = -a/3$, and if $u = 0$ and $\operatorname{char}(K) = 3$, then $v = -1$ and $r = -a$. Hence it also follows that $r \in K$ whenever $u, v, w \in K$. We conclude that an automorphism $\alpha\colon E[2] \xrightarrow{\sim} E[2]$ that fixes a point of order two is K-rational if and only if the said point is K-rational.

To deal with case (2), suppose that $\alpha([r : 0 : 1]) = [t : 0 : 1]$, for example. Then $ux^2 + vx + w \in \overline{K}[x]$ must equal the Lagrange polynomial

$$t\frac{x-s}{r-s}\frac{x-t}{r-t} + r\frac{x-r}{s-r}\frac{x-t}{s-t} + s\frac{x-r}{t-r}\frac{x-s}{t-s} = \frac{r^2-rs+s^2-rt-st+t^2}{(r-s)(s-t)(t-r)}x^2 + \frac{-r^3+r^2s-s^3+s^2t+rt^2-t^3}{(r-s)(s-t)(t-r)}x + \frac{-r^2s^2+rs^3+r^3t-r^2t^2-s^2t^2+st^3}{(r-s)(s-t)(t-r)}.$$

In the same manner as before, let $I_q \subset K[q,a,b,c,d,r,s,t]$ denote the ideal generated by five elements, namely the four polynomials

$$a+r+s+t, \quad -b+rs+rt+st, \quad c+rst, \quad d-(r-s)(s-t)(t-r),$$

and the fifth polynomial

$$\begin{aligned}
&-u(r-s)(s-t)(t-r)+r^2+s^2+t^2-rs-rt-st && \text{for } q=u,\\
&-v(r-s)(s-t)(t-r)-r^3-s^3-t^3+r^2s+rt^2+s^2t && \text{for } q=v,\\
&-w(r-s)(s-t)(t-r)+r^3t+rs^3+st^3-r^2t^2-r^2s^2-s^2t^2 && \text{for } q=w.
\end{aligned}$$

Eliminating r,s,t gives

$$u=\frac{a^2-3b}{d}, \quad v=\frac{2a^3-7ab+9c-d}{2d}, \quad w=\frac{a^2b-4b^2+3ac-ad}{2d}, \quad (1.36)$$

where $d=(r-s)(s-t)(t-r)$. Therefore we have $u \in K$ if and only if $d \in K$ and, since $\Delta_E=(d^2)$ modulo twelfth powers, the claim follows. □

Remark 1.19 Proposition 1.5 also follows by equating (1.13) and (1.14). Factoring the difference of the two expressions and equating it with zero gives

$$(b^3-a^3c)(b^3+a^3c-9abc+27c^2)=0.$$

Equating the first term with zero gives $c=b^3/a^3$. As one of the curves was given by $s^2=f(t)$, where $f(t)=t^3+at^2+bt+c$, this corresponds to case (1) because $f(-b/a)=0$. If the second term is zero, then we obtain case (2) since

$$\mathrm{Disc}(f)=\mathrm{Disc}(f)+4(b^3+a^3c-9abc+27c^2)=(ab-9c)^2.$$

We deal separately with the remaining two cases.

Proposition 1.6 *Let E_1 and E_2 be two elliptic curves with $j(E_1)=j(E_2)=0$. Then they can be glued along the 2-torsion if and only if every $P \in E_i[2]$ is K-rational.*

Proof We fix a model

$$E\colon y^2z=x(x^2-Bz^2)$$

for both curves, where $B = b^2 \in K$ for some $b \in \overline{K} \setminus \{0\}$. Then the two automorphisms (over $\overline{K}$) of $E[2]$ given by

$$[x : y : z] \mapsto \left[\frac{3}{2b}x^2 \mp \frac{1}{2}xz - bz^2 : y^2 : z^2\right]$$

fix no points of order two and fix $[b : 0 : 1]$, respectively. They are defined over K if and only if $b \in K$. The automorphism that fixes $[0 : 0 : 1]$ is given by

$$[x : y : z] \mapsto [-x : y : z]$$

and is induced by automorphisms $[x : y : z] \mapsto [-x : \pm iy : z]$, where $i^2 = -1$. Therefore the claim follows. □

Proposition 1.7 *Let E_1 and E_2 be two elliptic curves whose j-invariants satisfy $j(E_1) = j(E_2) = 1728 \neq 0$. Then they can be glued along the 2-torsion if and only if E_i has at least one K-rational point of order two.*

Proof We fix a model

$$E\colon y^2z = x^3 - Cz^3$$

for both curves, where $C = c^3 \in K$ for some $c \in \overline{K} \setminus \{0\}$. Let ζ be a primitive third root of unity. Then the automorphisms of $E[2]$ given by

$$[x : y : z] \mapsto \left[\zeta^i x : y : z\right], \quad i \in \{0, 1, 2\}$$

fix no points of order two and are induced by automorphisms of E, whereas automorphisms

$$[x : y : z] \mapsto \left[\frac{1}{\zeta^i c}x^2 : y^2 : z^2\right], \quad i \in \{0, 1, 2\}$$

fix a single point of order two and are defined over K if and only if $\zeta^i c \in K$. □

Proposition 1.8 *Let E_1 and E_2 be two elliptic curves with $j(E_1) \neq j(E_2)$. Suppose that:*

(1) Both curves have a K-rational point of order two;

(2) The product of their minimal discriminants is a square in K.

Then E_1 and E_2 can be glued over K along the 2-torsion.

Proof First of all, suppose $\mathrm{char}(K) \neq 3$ and choose two models

$$E_1 \colon y^2z = x^3 + B_1xz^2 + C_1z^3,$$
$$E_2 \colon y^2z = x^3 + B_2xz^2 + C_2z^3.$$

Let $r_i, s_i, t_i \in \overline{K}$ be the roots of $x^3 + B_ix + C_i \in K[x]$, for $i \in \{1, 2\}$. Then $\alpha \colon E_1[2] \xrightarrow{\sim} E_2[2]$ such that

$$[r_1 : 0 : 1] \mapsto [r_2 : 0 : 1], \quad [s_1 : 0 : 1] \mapsto [s_2 : 0 : 1], \quad [t_1 : 0 : 1] \mapsto [t_2 : 0 : 1]$$

may be given as $[x : y : z] \mapsto [Ux^2 + Vxz + Wz^2 : y^2 : z^2]$, where $U, V, W \in \overline{K}$ are such that $Ux^2 + Vx + W$ equals the polynomial

$$r_2\frac{x - s_1}{r_1 - s_1}\frac{x - t_1}{r_1 - t_1} + s_2\frac{x - r_1}{s_1 - r_1}\frac{x - t_1}{s_1 - t_1} + t_2\frac{x - r_1}{t_1 - r_1}\frac{x - s_1}{t_1 - s_1}.$$

Let $D_i = (r_i - s_i)(s_i - t_i)(t_i - r_i)$ and note that the assumption *(2)* is equivalent to $D = D_1D_2 \in K$. A simple calculation gives

$$\begin{aligned}
D_1U &= -r_2s_1 + r_1s_2 + r_2t_1 - s_2t_1 - r_1t_2 + s_1t_2,\\
D_1V &= r_2s_1^2 - r_1^2s_2 - r_2t_1^2 + s_2t_1^2 + r_1^2t_2 - s_1^2t_2,\\
D_1W &= -r_2s_1^2t_1 + r_1^2s_2t_1 + r_2s_1t_1^2 - r_1s_2t_1^2 - r_1^2s_1t_2 + r_1s_1^2t_2.
\end{aligned}$$

The same elimination procedure from the previous proofs gives, among others, the following equations

$$\begin{aligned}
2D(3r_1^2 + B_1)U &= 3(-12r_1^3r_2^4 + 8r_1^3B_2^2 + 6r_2^4C_1 - 4B_2^2C_1 - 30r_1^3r_2C_2\\
&\quad + 15r_2C_1C_2 + r_2D),\\
2D(3r_1^2 + B_1)V &= 12r_2^4B_1^2 - 8B_1^2B1^2 - 54r_1r_2^4C_1 + 36r_1B_2^2C_1 + 30r_2B_1^2C_2\\
&\quad - 135r_1r_2C_1C_2 + 3r_1r_2D,\\
D(3r_1^2 + B_1)W &= 12r_1^5r_2^4 - 8r_1^5B_2^2 + 12r_1^2r_2^4C_1 + 6r_2^4B_1C_1\\
&\quad - 8r_1^2B_2^2C_1 - 4B_1B_2^2C_1 + 30r_1^5r_2C_2 + 30r_1^2r_2C_1C_2\\
&\quad + 15r_2B_1C_1C_2 + r_2B_1D.
\end{aligned}$$

Therefore $U, V, W \in K$ if $r_1, r_2, D \in K$. An analogous argument yields the same result for $\mathrm{char}(K) = 3$. □

1.5.2 The Hesse pencil and the (3,3)-split case

In this subsection, we will assume that K satisfies $\mathrm{char}(K) \neq 3$ and $K = K(\zeta)$, where $\zeta \in \overline{K}$ denotes a primitive third root of unity, i.e. $1 + \zeta + \zeta^2 = 0$. The one dimensional family of curves given by

$$E_{[\lambda:\mu]} \,:\, \mu(x^3 + y^3 + z^3) + \lambda xyz = 0$$

for $[\lambda : \mu] \in \mathbb{P}^1$ is called the *Hesse pencil*. Exactly four members of the pencil are singular, namely the curves corresponding to $[-3 : 1]$, $[-3\zeta : 1]$, $[-3\zeta^2 : 1]$, and $[1 : 0]$. We will also consider the family $\mathcal{H}$, given by

$$E_\lambda \,:\, x^3 + y^3 + z^3 + 3\lambda xyz = 0, \tag{1.37}$$

that we will refer to by the same name.

Any elliptic curve over K with K-rational 3-torsion admits a model of the form (1.37) (see Lemma 1 in [**Ar-Do**], for example). With the exception of $\lambda^3 = -1$, each $\lambda \in K$ defines an elliptic curve E_λ, with the identity element $[1 : -1 : 0]$, that is isomorphic to the elliptic curve given by

$$Y^2Z = X^3 - 3\lambda(\lambda^3 - 8)XZ^2 - 2(\lambda^6 + 20\lambda^3 - 8)Z^3, \tag{1.38}$$

via the following linear transformation:

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = \begin{bmatrix} 3\lambda^2 & 3\lambda^2 & \lambda^3 + 4 \\ 4(\lambda^3 + 1)(\zeta - \zeta^2) & -4(\lambda^3 + 1)(\zeta - \zeta^2) & 0 \\ 1 & 1 & -\lambda \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix}. \tag{1.39}$$

Each of the four singular elements of $\mathcal{H}$ is a union of three lines, namely:

$$\begin{aligned} E_\infty &\,:\, xyz = 0, \\ E_{-1} &\,:\, (x + y + z)(\zeta x + \zeta^2 y + z)(\zeta^2 x + \zeta y + z) = 0, \\ E_{-\zeta} &\,:\, (x + \zeta y + z)(\zeta x + y + z)(\zeta^2 x + \zeta^2 y + z) = 0, \\ E_{-\zeta^2} &\,:\, (x + \zeta^2 y + z)(\zeta^2 x + y + z)(\zeta x + \zeta y + z) = 0. \end{aligned}$$

Let $F = \mu(x^3 + y^3 + z^3) + \lambda xyz$. Then the Hessian of $E_{[\lambda:\mu]}$ is given by

$$\det \begin{bmatrix} \frac{\partial F}{\partial^2 x} & \frac{\partial F}{\partial x \partial y} & \frac{\partial F}{\partial x \partial z} \\ \frac{\partial F}{\partial y \partial x} & \frac{\partial F}{\partial^2 y} & \frac{\partial F}{\partial y \partial z} \\ \frac{\partial F}{\partial z \partial x} & \frac{\partial F}{\partial z \partial y} & \frac{\partial F}{\partial^2 z} \end{bmatrix} = 3\mu\lambda^2(x^3 + y^3 + z^3) - (108\mu^3 + \lambda^3)xyz.$$

We note that this gives another element of $\mathcal{H}$. Restricting to (1.37), the Hessian of E_λ corresponds to the curve given by

$$x^3 + y^3 + z^3 - \frac{\lambda^3 + 4}{\lambda^2} xyz = 0 \quad \text{if } \lambda \neq 0.$$

In case $\lambda = 0$, the Hessian corresponds to the three lines $xyz = 0$.

We assume from now on that $\lambda^3 \neq -1$ so that $E = E_\lambda$ is an elliptic curve with $0_E = [1 : -1 : 0]$. For $P = [x : y : z] \in E$ one has

$$\begin{aligned} -P &= [y : x : z], \\ 2P &= [y(x^3 - z^3) : x(z^3 - y^3) : z(y^3 - x^3)], \\ 3P &= [F_1 : F_2 : F_3], \end{aligned} \tag{1.40}$$

where

$$\begin{aligned} F_1 &= x^6y^3 + y^6z^3 + z^6x^3 - 3x^3y^3z^3, \\ F_2 &= x^6z^3 + y^6x^3 + y^3z^6 - 3x^3y^3z^3, \\ F_3 &= xyz(x^6 + y^6 + z^6 - x^3y^3 - y^3z^3 - z^3x^3). \end{aligned}$$

Also, for $P_1, P_2 \in E$ with $P_i = [x_i : y_i : z_i]$ one has

$$P_1 + P_2 = [y_1^2x_2z_2 - y_2^2x_1z_1 : x_1^2y_2z_2 - x_2^2y_1z_1 : z_1^2x_2y_2 - z_2^2x_1y_1]. \tag{1.41}$$

The curve E and its Hessian meet at nine points that are the flexes of E and satisfy $xyz = 0$. These are the points of $E[3]$ for every elliptic curve in the pencil and the pencil consists precisely of the cubic curves that pass through these nine points. It is easy to see that these nine points are given in the following table.

$[1 : 0 : -\zeta]$	$[1 : -\zeta^2 : 0]$	$[0 : 1 : -\zeta^2]$
$[1 : 0 : -1]$	$[1 : -1 : 0]$	$[0 : 1 : -1]$
$[1 : 0 : -\zeta^2]$	$[1 : -\zeta : 0]$	$[0 : 1 : -\zeta]$

Table 1.1: points of $E[3]$ in the Hessian model

Letting $S = [1 : 0 : -1]$, $T = [-\zeta : 1 : 0]$, and $O = 0_E$, we choose a particular isomorphism $\eta\colon E[3] \xrightarrow{\sim} (\mathbf{Z}/3\mathbf{Z})^2$, setting $S \mapsto (1, 0)$ and $T \mapsto (0, 1)$.

Hence Table 1.1 can be rewritten as:

$S+T$	T	$2S+T$		$(1,1)$	$(0,1)$	$(2,1)$
S	O	$2S$	$\cong$	$(1,0)$	$(0,0)$	$(2,0)$
$S+2T$	$2T$	$2S+2T$		$(1,2)$	$(0,2)$	$(2,2)$

Table 1.2: Table 1.1 under the chosen isomorphism $E[3] \cong (\mathbf{Z}/3\mathbf{Z})^2$

The Weil pairing on $E[3]$ is completely determined by $\langle S, T\rangle$, which we find directly. Let $P \in E(\overline{K})$ be any point such that $3P = S$. By a direct computation for a specific curve (e.g. $P = [-\sqrt[3]{2}\zeta : \sqrt[3]{4}\zeta^2 : 1]$ for $\lambda = 1/2$) or by a Gröbner basis computation for the ideal $(F_1 + F_3, F_2) \subset K[x, y, z]$, combined with the fact that $[3][x : y : z] = [1 : 0 : -1]$ implies $xyz \neq 0$ and $y \neq z$, we obtain that $x^2z + y^2x + z^2y$ vanishes on $\{P + R \mid R \in E[3]\}$. Since we already know that $E[3]$ is determined by lines $xyz = 0$, we conclude that

$$g = \frac{x^2z + y^2x + z^2y}{xyz} \in K(E)$$

is such that

$$\operatorname{div}(g) = \sum_{R \in E[3]} (P + R) - R,$$

and therefore

$$\langle S, T\rangle = \frac{g(X + T)}{g(X)} = \zeta$$

regardless of the choice of $X \in E(\overline{K}) \setminus (E[3] \cup t_P(E[3]))$ (see III §8 in [**AEC**]). It follows that

$$\langle P_1, P_2\rangle = \zeta^{\det(\eta(P_1), \eta(P_2))} \quad \text{for any } P_1, P_2 \in E[3],$$

and we can interpret the Weil pairing on $E[3]$ as the determinant map

$$\det \colon \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \to \mathbf{Z}/3\mathbf{Z}.$$

This correspondence is unique up to sign, i.e. up to multiplication by units of $\mathbf{Z}/3\mathbf{Z}$; it could also be given as $-\det$ for a different choice of S and T.

We note that $\operatorname{Aut}(E[3]) \cong \mathrm{GL}_2(\mathbf{Z}/3\mathbf{Z})$, which is a group of order 48. Its action on $E[3]$, with respect to Table 1.1, is depicted in Figures 1.9 and 1.10.

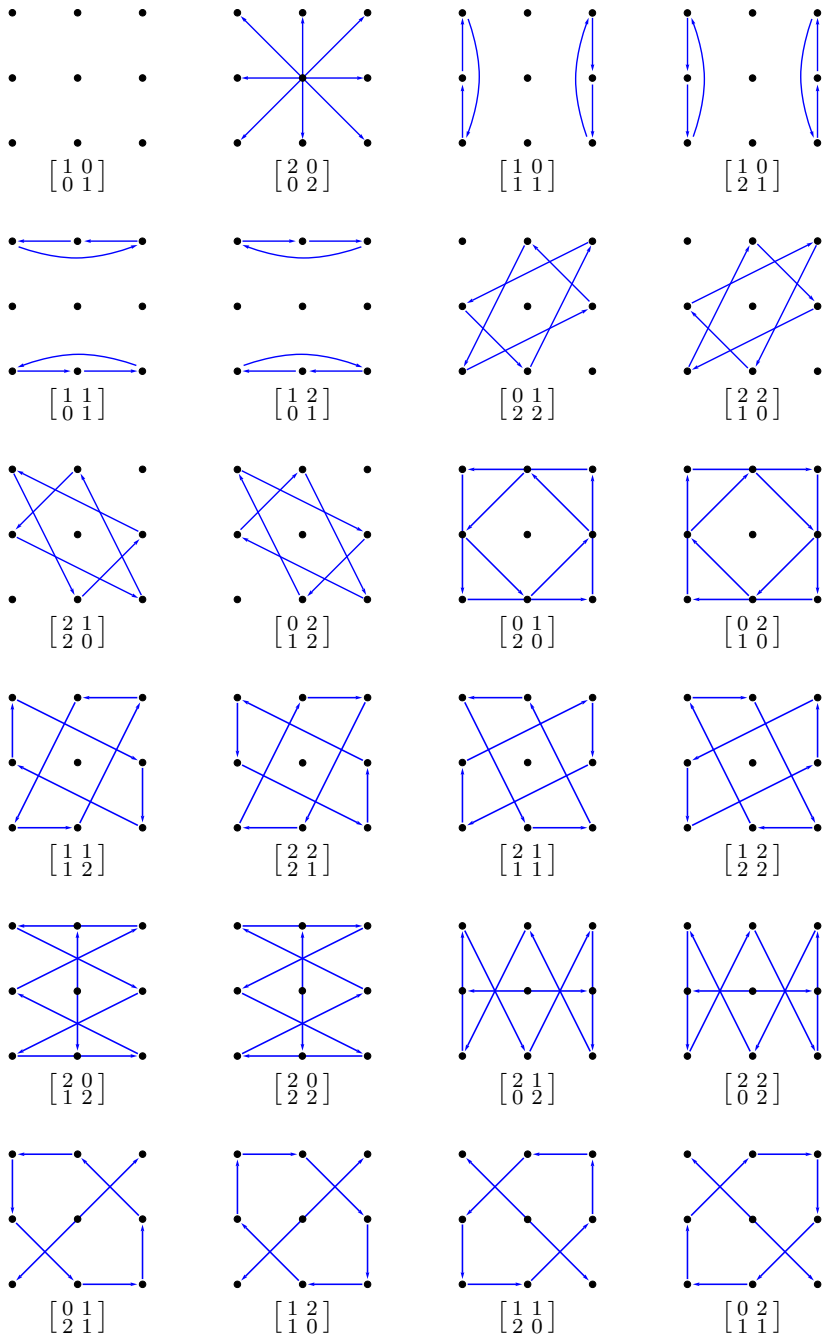


Figure 1.9: Normal subgroup $\mathrm{SL}_2(\mathbf{Z}/3\mathbf{Z})$

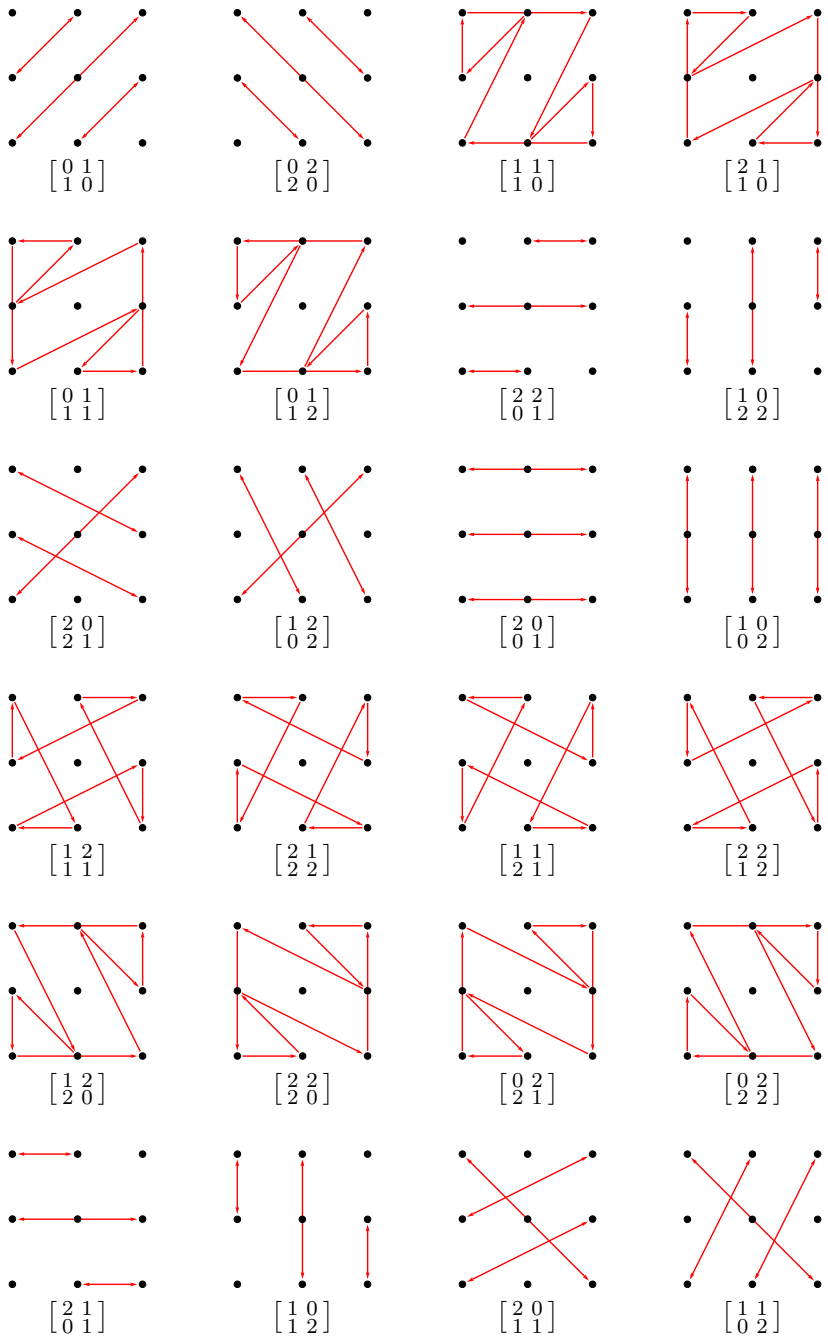


Figure 1.10: Coset $\left[\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right]\mathrm{SL}_2(\mathbf{Z}/3\mathbf{Z})$

We recall some basic properties of these groups. We have $\mathrm{SL}_2(\mathbf{Z}/3\mathbf{Z}) \cong Q_8 \rtimes C_3$ with

$$Q_8 = \langle -\mathbb{1}, I, J \mid (-\mathbb{1})^2 = \mathbb{1},\, I^2 = J^2 = (IJ)^2 = -\mathbb{1} \rangle,$$
$$C_3 = \langle G \mid G^3 = \mathbb{1} \rangle.$$

Here $-\mathbb{1} = \left[\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right]$ and we can take, for example,

$$I = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}, \quad J = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}, \quad G = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

Moreover, the group $\mathrm{SL}_2(\mathbf{Z}/3\mathbf{Z})$ is generated by I and G. The corresponding isomorphisms are given by

$$\begin{aligned} -\mathbb{1} &\mapsto [y : x : z] \\ I &\mapsto [\zeta^2 x + \zeta y + z : \zeta x + \zeta^2 y + z : x + y + z] \\ J &\mapsto [\zeta x + y + z : x + \zeta y + z : \zeta x + \zeta y + \zeta^2 z] \\ G &\mapsto [x : y : \zeta z]. \end{aligned}$$

Therefore the elements of $\mathrm{SL}_2(\mathbf{Z}/3\mathbf{Z})$ correspond to automorphisms of $E[3]$, each of which is induced by an isomorphism (of elliptic curves) between E and another element of $\mathcal{H}$. This defines an action of $\mathrm{SL}_2(\mathbf{Z}/3\mathbf{Z})$ on $\mathcal{H}$. Since we have $\mathrm{Aut}(E) = \{\pm\mathbb{1}\}$ for a generic $E_\lambda \in \mathcal{H}$, each element of

$$\mathrm{PSL}_2(\mathbf{Z}/3\mathbf{Z}) = \mathrm{SL}_2(\mathbf{Z}/3\mathbf{Z})/\{\pm\mathbb{1}\} \cong A_4$$

corresponds to a pair of isomorphisms between E and a unique element of $\mathcal{H}$ (exceptions being $\lambda(\lambda^3 - 8) = 0$ and $\lambda^6 + 20\lambda^3 - 8 = 0$).

One can easily determine from (1.38) that the j-invariant of E_λ is

$$j(E_\lambda) = -\frac{27\lambda^3(\lambda^3 - 8)^3}{(\lambda^3 + 1)^3}. \tag{1.42}$$

We can therefore conclude that $j\colon \mathcal{H} \to \mathbb{P}^1$ is 12-to-1, except above $j = 0$ and $j = 1728$, where it is 4-to-1 and 6-to-1, respectively. Every element of

$$\left\{\lambda, \lambda\zeta, \lambda\zeta^2, \frac{-\lambda+2}{\lambda+1}, \frac{-\lambda+2}{\lambda+1}\zeta, \frac{-\lambda+2}{\lambda+1}\zeta^2, \frac{-\lambda+2\zeta}{\lambda+\zeta}, \frac{-\lambda+2\zeta^2}{\lambda+\zeta^2}, \frac{-\zeta\lambda+2}{\lambda+\zeta^2}, \frac{-\zeta^2\lambda+2}{\lambda+\zeta}, \frac{-\lambda+2\zeta}{\zeta^2\lambda+1}, \frac{-\lambda+2\zeta^2}{\zeta\lambda+1}\right\}$$

defines the same isomorphism class.

The set $\{-\mathbb{1}, I, J, G, H\}$, where $H = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$, generates $\mathrm{GL}_2(\mathbf{Z}/3\mathbf{Z})$. It is readily checked that H corresponds to the 3-torsion isomorphism $[h_1 : h_2 : h_3]$, where

$$\begin{aligned} h_1 &= x(y^2+z^2)\zeta^2 + y(x^2+z^2)\zeta + z(x^2+y^2), \\ h_2 &= x(y^2+z^2)\zeta + y(x^2+z^2)\zeta^2 + z(x^2+y^2), \\ h_3 &= x(y^2+z^2) + y(x^2+z^2) + z(x^2+y^2). \end{aligned}$$

Therefore the anti-symplectic 3-torsion isomorphisms for curves in $\mathcal{H}$ are precisely those corresponding to the coset $H\mathrm{SL}_2(\mathbf{Z}/3\mathbf{Z})$ and they can be written down explicitly.

We conclude by analysing a specific example.

Example 1.6 Suppose that we have $1 + 3\lambda t^2 + 2t^3 = 0$ for some $t \in K$, such that $(t^3-1)(8t^3+1) \neq 0$. Then the elliptic curve

$$E_\lambda \colon x^3 + y^3 + z^3 - \frac{1+2t^3}{t^2}xyz = 0$$

has a rational point $[t : t : 1]$ of order two. Applying the isomorphism (1.39), Vélu's formula for 2-isogenies (and applying a suitable isomorphism), we obtain as the image a curve that is given by a model of type (1.38) with the parameter $\mu = (1-4t^3)/(3t)$. We omit the details and give only the final map

$$\gamma \colon E_\lambda \to E_\mu, \quad [x : y : z] \mapsto [f_1(x,y,z) : f_2(x,y,z) : f_3(x,y,z)],$$

where

$$\begin{aligned} f_1 &= x(-2t^2y^2 - t^2xy + t^2x^2 - yz + 2t^3xz + tz^2), \\ f_2 &= y(-2t^2x^2 - t^2xy + t^2y^2 - xz + 2t^3yz + tz^2), \\ f_3 &= tz(x+y+tz)(x+y-2tz). \end{aligned}$$

Thus γ is an isogeny whose kernel is the cyclic group of order two that is generated by the point $[t : t : 1]$. Restricting γ to the 3-torsion, we obtain the isomorphism $\alpha \colon E_\lambda[3] \to E_\mu[3]$ that corresponds to $\left[\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right] \in \mathrm{GL}_2(\mathbf{Z}/3\mathbf{Z})$. It follows from the proof of Proposition 1.2 that $J := (E_\lambda \times E_\mu)/\Gamma_\alpha$ is isomorphic to $E_\lambda \times E_\mu$.

Suppose that $E_\lambda \cong E_\mu$ and suppose that $\sqrt{-2} \in K$, extending K if necessary. To determine the isomorphism classes of such curves, we may suppose, without loss of generality, that $\lambda = \mu$. This implies

$$0 = 4t^4 - 2t^3 - t - 1 = (t-1)(2t+1)(2t^2+1).$$

Hence $t = \pm\frac{\sqrt{-2}}{2}$ and $\lambda = \frac{2\pm\sqrt{-2}}{3}$. Both values of λ correspond to the same isomorphism class since for each one, the other is given by $\frac{-\lambda+2}{\lambda+1}$. Hence E_λ is an elliptic curve defined over $K = K(\zeta, \sqrt{-2})$, with j-invariant $j(E_\lambda) = 8000$ and with complex multiplication by $\mathbf{Z}[\sqrt{-2}]$.

We note that λ and μ satisfy

$$3\lambda^2\mu^2 + \lambda^3 + \mu^3 - 3\lambda\mu + 2 = 0, \tag{1.43}$$

describing a singular curve of genus zero.

We now consider the case $\alpha = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right]$ in more generality. Let E_λ and E_μ be two elliptic curves in $\mathcal{H}$ and let A and G respectively denote the images of $E_\lambda \times E_\mu$ and Γ_α in $\mathbb{P}^8$ under the Segre embedding

$$\sigma\colon ([x : y : z], [u : v : w]) \mapsto [xu : xv : xw : yu : yv : yw : zu : zv : zw].$$

The identity element of A is $O_A = [1 : -1 : 0 : -1 : 1 : 0 : 0 : 0 : 0]$ and the inversion morphism $-\mathbb{1}_A$ is given as

$$[X_1 : X_2 : \cdots : X_9] \mapsto [X_5 : X_4 : X_6 : X_2 : X_1 : X_3 : X_8 : X_7 : X_9]. \tag{1.44}$$

Lemma 1.20 *Let $\mathcal{W}_1$ and $\mathcal{W}_2$ denote the set of (geometric) points of order two on $\sigma(E_\lambda \times \{0_{E_\mu}\})$ and the set of points of order two on $\sigma(\{0_{E_\lambda}\} \times E_\mu)$, respectively. Then any hyperplane section on A that is invariant under $-\mathbb{1}_A$ contains either $\mathcal{W}_1 \cup \mathcal{W}_2$ or its complement in $A[2](\overline{K})$.*

Proof The two eigenspaces of (1.44) are respectively generated by the sets

$$S_1 = \{X_1 + X_5, X_2 + X_4, X_3 + X_6, X_7 + X_8, X_9\},$$
$$S_2 = \{X_1 - X_5, X_2 - X_4, X_3 - X_6, X_7 - X_8\}.$$

We find that $A[2](\overline{K})$ consists of six points that are in the zero locus of the ideal generated by S_1 and ten points that are in the zero locus of the ideal generated by S_2. Since any linear form that is fixed by $-\mathbb{1}_A$ is a linear combination of the elements of exactly one of these two sets, we are done. □

It is a fact that the translations by points of $A[3]$ can be extended to automorphisms of $\mathbb{P}^8$ and this is crucial to our analysis because there exist algorithms (see [**Ke-St**]) that compute invariants of $K[X_1, \ldots, X_9]$, of a given

degree, under an action by a finite matrix group. The computations involved were done in MAGMA. The details are given in the Appendix.

We find that the vector space of degree 3 invariants (under the action of G) is of dimension 21, with an explicitly given basis, while there are no invariants of degree 1 or 2. We then use a Gröbner basis computation to reduce the elements of this basis to elements of the coordinate ring of A and we find that there are exactly 9 linearly independent ones, say $F_1, \ldots, F_9$. Using another Gröbner basis computation, we solve the equation

$$d_1F_1 + \cdots + d_9F_9 - (c_1X_1 + \cdots + c_9X_9)^3 = 0$$

for $c_1, \ldots, c_9$. The solution set has exactly nine points and they give us linear forms that are invariant under the translations by points of G. In particular, we find that the linear form $X_1 + X_5 + X_9$ is the one that is also invariant under $-\mathbb{1}_A$. Therefore we find the divisor $D := \varphi^*(C)$ from Lemma 1.17 explicitly. Moreover, the divisor D does not contain O_A and, as expected, the remaining 8 divisors are obtained as translates of D by the points of $A[3]/G$. Analogous results can be obtained for all choices of anti-symplectic α. We summarize with the following proposition.

Proposition 1.9 *Let $n \geq 3$ be an odd integer, let E_1 and E_2 be two elliptic curves, let $\Theta := E_1 \times \{0_{E_2}\} + \{0_{E_1}\} \times E_2$, and let $\alpha\colon E_1[n] \to E_2[n]$ be an anti-symplectic isomorphism. Let D be the unique divisor on $E_1 \times E_2$ that is linearly equivalent to $n\Theta$, invariant under the translations by points of Γ_α, and invariant under $-\mathbb{1}_{E_1\times E_2}$. Then $(E_1 \times E_2)/\Gamma_\alpha$ is not a Jacobian if and only if D contains a 2-torsion point of $E_1 \times E_2$ that is not a point of order two on $E_1 \times \{0_{E_2}\}$ or a point of order two on $\{0_{E_1}\} \times E_2$.*

Proof As before, let J and C respectively denote the images of $E_1 \times E_2$ and D under the isogeny $\varphi\colon E_1 \times E_2 \to (E_1 \times E_2)/\Gamma_\alpha$. By Theorem 1.18, the divisor C is either a curve of genus two or a sum of two elliptic curves that meet in a rational 2-torsion point. Since $-\mathbb{1}_J$ induces an involution ι on C, we conclude that $C(\overline{K})$ contains exactly six points fixed by ι if and only if it is irreducible and that it contains exactly seven points fixed by ι if and only if it is reducible. Since n is odd, the restriction of φ to the 2-torsion is an isomorphism and there is exactly one geometric point of $(E_1 \times E_2)[2]$ above each point of $C(\overline{K})$ that is fixed by ι. Therefore $D(\overline{K})$ cannot contain more than seven 2-torsion points. Lemma 1.20 shows that $D(\overline{K})$ contains at least the six points of $(E_1[2] \times \{0_{E_2}\} \cup \{0_{E_1}\} \times E_2[2]) \setminus \{0_{E_1\times E_2}\}$ and the claim follows. □

Remark 1.20 If the divisor D can be given explicitly, the condition in Proposition 1.9 is not difficult to check. For $n = 3$, we can compute this divisor, given the datum $(E_\lambda, E_\mu, \alpha)$ as above. In particular, if α is given by $\left[\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right]$ with respect to our choice of bases for $E_\lambda[3]$ and $E_\mu[3]$, we find that $(E_\lambda \times E_\mu)/\Gamma_\alpha$ is not a Jacobian if and only if (1.43) holds (see the Appendix for more details).

Chapter 2

Heights on abelian varieties

In this chapter, we deal with the theory of heights on abelian varieties, using mostly [**Liu**] and [**DG**] as references. Height functions lie at the heart of some well known finiteness results in Diophantine geometry, some of which are mentioned below. We begin by giving a short overview of the theory of heights and recalling some prerequisites, without going into full detail.

From now on, unless stated otherwise, the base field K is assumed to be a number field, although there are analogues for most of the statements when K is the function field $k(C)$ of a smooth curve C defined over a finite field k. As before, we let $\overline{K}$ be an algebraic closure of K and we suppose that all varieties and morphisms are defined over K unless stated otherwise. The ring of integers of K will be denoted by O_K.

Given a variety X, we are interested in functions

$$h\colon X(K) \to \mathbf{R}_{\geq 0}$$

that satisfy certain finiteness properties. In particular, given a bound $B \in \mathbf{R}$,

$$\#\{P \in X(K) \mid h(P) < B\} \tag{2.1}$$

should be finite. This finiteness property is a key component in proving, for example, the Thue-Siegel-Roth theorem(s), the Mordell-Weil theorem, and the Faltings's theorem.

2.1 Naive height in a projective space

Let $P \in \mathbb{P}^n(\mathbf{Q})$ and choose $x_0, x_1, \ldots, x_n \in \mathbf{Z}$ such that $\gcd(x_0, x_1, \ldots x_n) = 1$ and $P = [x_0 : x_1 : \cdots : x_n]$. We define the *naive height* of the point P as

$$H(P) := \max\{|x_0|, |x_1|, |x_2|, \ldots, |x_n|\}. \tag{2.2}$$

For any $a/b \in \mathbf{Q}$ with $\gcd(a, b) = 1$, we define $H(a/b) := H([a : b])$. The finiteness condition (2.1) is obviously satisfied for H. This simple function features in the classical Diophantine theorems, e.g. the approximation theorems of Dirichlet and Liouville, and Roth's theorem (see [**DA**]). When the number of points in a subset of $\mathbb{P}^n(\mathbf{Q})$ is not known to be finite, the asymptotic behaviour of a point counting function is an arithmetic datum that is of interest. For example, the behaviour of the point counting function of $\mathbb{P}^n$ is well understood (see Schanuel's Theorem, [III, §5] in [**Lang1**] for a general statement and proof).

As a motivation for the general theory of this chapter, we consider an explicit example. Let $E/\mathbf{Q}$ be an elliptic curve given by

$$y^2z = x^3 - xz^2 + z^3$$

and let $P = [1 : -1 : 1]$. The points $[n]P$ for $n \in \{1, 2, \ldots, 26\}$ are listed in Figure 2.1. The parabolic shape formed by the digits would seem to suggest that *the number of digits required to write* $[n]P$ *increases quadratically with* n. This is formalized in the following sections.

2.2 More general height functions

It is natural to extend the notion of a height to all number fields. Let K be a number field of degree $[K : \mathbf{Q}] = d = r_1 + 2r_2$ and let M_K denote the set of places of K. Recall that $M_K = M_K^0 \cup M_K^\infty$, where

$$M_K^0 = \{\text{maximal ideals of } O_K\},$$
$$M_K^\infty = \{\sigma_1, \ldots, \sigma_{r_1}, \tau_1, \ldots, \tau_{r_2}\},$$

and $\sigma_i \colon K \hookrightarrow \mathbf{R}$ and $\tau_j, \overline{\tau}_j \colon K \hookrightarrow \mathbf{C}$ are the real and the complex embeddings of K, respectively.

$[1 : -1 : 1]$

$[1 : 1 : -1]$

$[0 : 1 : 1]$

$[3 : 5 : 1]$

$[5 : -11 : 1]$

$[2 : -7 : 8]$

$[-33 : 17 : 27]$

$[95 : 103 : 125]$

$[56 : 419 : 1]$

$[1749 : -1861 : 1331]$

$[-4845 : -7981 : 6859]$

$[-6244 : 24655 : 21952]$

$[300245 : 399083 : 148877]$

$[1338189 : -4231459 : 132651]$

$[5232472 : -8824453 : 11089567]$

$[-180611015 : 13919407 : 136590875]$

$[1441793001 : 2068194649 : 2633789341]$

$[8246188998 : 30795303833 : 588480472]$

$[516748560445 : -640700244397 : 289723287113]$

$[-3375972447067 : -9902960463475 : 8578614947111]$

$[-51055373209680 : 101098481076377 : 85923747076383]$

$[5084973401787721 : 5668823512883159 : 3486845747330119]$

$[51706401333034393 : -284766785698664807 : 1702936561884713]$

$[1796402375990961480 : -2098030206970736191 : 2631958890650432000]$

$[-165839455909553978217 : -589894998303060345 83 : 130151721705221306663]$

$[3141659240481142325561 : 7943031662998736010841 : 9462748411719641574199]$

Figure 2.1: Positive integer multiples of $[1 : -1 : 0]$ on $E\colon y^2 = x^3 - x + 1$

For $v \in M_K$, one defines the corresponding absolute value as

$$|\cdot|_v \colon K \to \mathbf{R}_{\geq 0}, \quad |x|_v = \begin{cases} p^{-\mathrm{ord}_{\mathfrak{p}}(x)/e_{\mathfrak{p}}} & \text{if } v \text{ is a maximal ideal } \mathfrak{p} \subset O_K, \\ |\sigma(x)| & \text{if } v \text{ is an embedding } \sigma \in M_K^{\infty}, \end{cases}$$

where $e_{\mathfrak{p}} = \mathrm{ord}_{\mathfrak{p}}(p)$ is the ramification index of $\mathfrak{p}$ in K and $|\ \cdot\ |$ is the usual archimedean absolute value on $\mathbf{C}$. By convention, we set $|0|_v = 0$. These absolute values are extensions of the usual (p-adic and archimedean) absolute values on $\mathbf{Q}$ and they are unique, up to equivalence[1], as is the case with the absolute values on $\mathbf{Q}$ (a theorem of Ostrowski). If L/K is a field extension and $w \in M_L$ and $v \in M_K$ are such that the restriction of $|\cdot|_w$ to K equals $|\cdot|_v$, we say that w *divides* v (or *lies above* v) and write $w|v$.

To extend our definition of a height, it is necessary to first *normalize* the absolute values so that the Product Formula holds. To that end, for any $v \in M_K$, let K_v denote the completion of K with respect to $|\cdot|_v$. We define the *local degree of* v to be $n_v := [K_v : \mathbf{Q}_v]$ and we define the *normalized absolute value* associated to v as

$$||x||_v := |x|_v^{n_v}.$$

Equivalently, for a prime ideal $\mathfrak{p} \subset O_K$ above $p \in \mathbf{Z}$, we have

$$||x||_{\mathfrak{p}} = (N_{K/\mathbf{Q}}(\mathfrak{p}))^{-\mathrm{ord}_{\mathfrak{p}}(x)} = p^{-\mathrm{ord}_{\mathfrak{p}}(x) f_{\mathfrak{p}}} \quad (\text{for } x \neq 0),$$

where $f_{\mathfrak{p}}$ is the residue degree of $\mathfrak{p}$, and for an embedding $\sigma \in M_K^{\infty}$ we have

$$||x||_{\sigma} = \begin{cases} |\sigma(x)| & \text{if } \sigma \text{ is real,} \\ |\sigma(x)|^2 & \text{if } \sigma \text{ is complex.} \end{cases}$$

Definition 2.1 Let $P = [x_0 : x_1 : \cdots : x_n] \in \mathbb{P}^n(K)$ with $x_i \in K$. The *relative height function* $H_K \colon \mathbb{P}^n(K) \to \mathbf{R}_{\geq 1}$ is given by

$$H_K(P) = \prod_{v \in M_K} \max\{||x_0||_v, ||x_1||_v, \ldots, ||x_n||_v\}.$$

That this is well defined (independent of the choice of homogeneous coordinates for P) follows from the following theorem.

[1] Two norms are called *equivalent* if they define the same topology.

Theorem 2.1 (Product Formula) *Let K be a number field and let $x \in K \setminus \{0\}$. Then*

$$\prod_{v \in M_K} ||x||_v = 1.$$

Proof This is obvious for $K = \mathbf{Q}$. The general case follows from the so called Degree Formula for number field extensions L/K:

$$[L : K] = \sum_{\substack{w \in M_L \\ w|v}} [L_w : K_v] \quad \text{for every } v \in M_K \tag{2.3}$$

(see Theorem 2 and its Corollaries in Chapter II of [**Lang2**]). □

One can show, using the Degree Formula (2.3), that if L/K is an extension of number fields and $P \in \mathbb{P}^n(K)$, then

$$H_L(P) = H_K(P)^{[L:K]}.$$

This leads to a new definition of a height function that is independent of the underlying field.

Definition 2.2 Let $P = [x_0 : x_1 : \cdots : x_n] \in \mathbb{P}^n(\overline{\mathbf{Q}})$. The *absolute height function* is the function

$$H \colon \mathbb{P}^n(\overline{\mathbf{Q}}) \to \mathbf{R}_{\geq 1}, \quad H(P) := H_K(P)^{1/[K:\mathbf{Q}]}$$

for any K such that $P \in \mathbb{P}^n(K)$. As before, one defines the relative (resp. absolute) height of $a \in K$ to be the relative (resp. absolute) height of the point $[a : 1] \in \mathbb{P}^1(K)$.

Note that this definition of H is reduced to (2.2) when $K = \mathbf{Q}$. Being independent of the field, the absolute height is Galois invariant.

Proposition 2.1 *For every $P \in \mathbb{P}^n(\overline{\mathbf{Q}})$ and every $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, one has*

$$H(P) = H(\sigma(P)).$$

Proof Let $K = \mathbf{Q}(P)$. Since σ restricts to an isomorphism $K \xrightarrow{\sim} \sigma(K)$, it induces a bijection between M_K and $M_{\sigma(K)}$, where $\sigma(v)$ is defined by the

equality $|x|_v = |\sigma(v)|_{\sigma(v)}$. Moreover, one has $[k_v : \mathbf{Q}_v] = [\sigma(K)_{\sigma(v)} : \mathbf{Q}_v]$ since σ induces an isomorphism on completions, and therefore

$$\prod_{v \in M_K} \max_i \{|x_i|_v^{n_v}\} = \prod_{w \in M_{\sigma(K)}} \max_i \{|\sigma(x_i)|_w^{n_w}\}$$

and the claim follows. □

The absolute height satisfies several very useful properties that are outlined in the remaining statements of this subsection.

Theorem 2.2 (Northcott) *For any $D, B > 0$, the set*

$$\{P \in \mathbb{P}^n(\overline{\mathbf{Q}}) \mid H(P) \leq B \text{ and } [\mathbf{Q}(P) : \mathbf{Q}] \leq D\}$$

is finite.

Proof For $P = [x_0 : x_1 : \cdots : x_n] \in \mathbb{P}^n(\overline{\mathbf{Q}})$ one has $H(P) \geq H(x_i) \geq 1$, so it suffices to prove the case $n = 1$ for all $1 \leq d \leq D$. For any $x \in \overline{\mathbf{Q}}$ of degree d, the Galois conjugates of x have the same height as x, by Proposition 2.1. Therefore the bound $H(x) \leq B$ implies a bound, in terms of B and d, on the height of the coefficients of the minimal polynomial $F_x \in \mathbf{Q}[T]$ of x. Since there are finitely many points of bounded height in $\mathbb{P}^d(\mathbf{Q})$ and F_x has rational coefficients, there are finitely many possibilities for F_x and therefore for x. See the proof of Theorem B.2.3 in [**DG**] for the precise bound. □

Let X be a projective variety over the number field K. If $\phi\colon X \hookrightarrow \mathbb{P}^n$ is an embedding, one is tempted to define the height of a point $P \in X$ as $H(\phi(P))$. However, height functions defined so far are not stable under embeddings; composing ϕ with an automorphism of $\mathbb{P}^n$ or an embedding $\mathbb{P}^n \hookrightarrow \mathbb{P}^m$ may give different values for H. For example, we have the following

Lemma 2.3 *Let $P \in \mathbb{P}^n(K)$ and $Q \in \mathbb{P}^m(K)$. Let $d \in \mathbf{N}$ and let $N = \binom{d+n}{n}$. Let ϕ_d denote the d-uple embedding, given as*

$$\phi_d\colon \mathbb{P}^n \to \mathbb{P}^N, \quad [x_0 : \cdots : x_n] \mapsto [M_1 : \cdots : M_N],$$

where the M_i are the monomials of degree d in $x_0, \ldots, x_n$, and let $S_{m,n}$ denote the Segre embedding, given as

$$S_{m,n}\colon \mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^{(m+1)(n+1)-1}, \quad ([x_i], [y_j]) \mapsto [x_i y_j].$$

Then the following two equalities hold:

$$\begin{aligned} H(\phi_d(P)) &= H(P)^d, \\ H(S_{m,n}(P,Q)) &= H(P)H(Q). \end{aligned} \tag{2.4}$$

Proof This follows immediately from the definitions. □

In general, the absolute height does not behave as nicely under morphisms (or, more generally, rational maps). However, its "bad behaviour" is bounded and this is the key property that allows us to proceed in our endeavor.

Theorem 2.4 *Let $\phi\colon \mathbb{P}^n \to \mathbb{P}^m$ be a rational map of degree d, given as*

$$x = [x_0 : x_1 : \cdots : x_n] \mapsto [F_0(x) : F_1(x) : \cdots : F_m(x)],$$

where $\deg F_i = d$ for every $i = 0, \ldots, m$. Let $Z = \cap_{i=0}^m Z(F_i)$ be the zero locus of the F_i. Then the following hold:

(1) There is a constant $c_1 = c_1(\phi) > 0$ such that for all $P \in \mathbb{P}^n(\overline{\mathbf{Q}}) \setminus Z$, we have

$$H(\phi(P)) \leq c_1 H(P)^d;$$

(2) If X is a subvariety of $\mathbb{P}^n$ such that $X \cap Z = \emptyset$, so that $\phi\colon X \to \mathbb{P}^m$ is a morphism, then there exists a constant $c_2 = c_2(\phi) > 0$ such that for all $P \in X(\overline{\mathbf{Q}})$, we have

$$H(\phi(P)) \geq c_2 H(P)^d.$$

Proof See Theorem B.2.5 in [**DG**]. □

Remark 2.1 The constants do not depend on the point P and are effective. The constant c is obtained directly by the triangle inequality, while obtaining the constant c' requires an application of an effective version of the Nullstellensatz. In general, the opposite inequality does not hold in *(1)*.

2.3 Heights on varieties

For convenience, we introduce the (absolute) *logarithmic height*

$$h\colon \mathbb{P}^n(\overline{\mathbf{Q}}) \to \mathbf{R}_{\geq 0}, \quad h(P) = \log H(P).$$

We call H the *multiplicative height*. We will omit these adjectives and refer to them simply as heights when the context makes it clear what we are referring to.

Let X be a projective variety and let $\phi\colon X \to \mathbb{P}^n$ be a morphism (not necessarily an embedding), all defined over $\overline{\mathbf{Q}}$. We refer to the function

$$h_\phi\colon X(\overline{\mathbf{Q}}) \to \mathbf{R}_{\geq 0}, \quad h_\phi(P) = h(\phi(P))$$

as the *height on X relative to ϕ*.

If $\phi\colon \mathbb{P}^n \to \mathbb{P}^m$ is a morphism of degree d, Theorem 2.4 gives

$$h_\phi(P) = dh(P) + O(1).$$

Since $\deg \phi = d$, one has $\phi^*\mathcal{O}(1) = \mathcal{O}(d)$, which leads to the following generalization of Theorem 2.4.

Theorem 2.5 *Let X be a projective variety over $\overline{\mathbf{Q}}$ and let $\phi\colon X \to \mathbb{P}^n$ and $\psi\colon X \to \mathbb{P}^m$ be morphisms (over $\overline{\mathbf{Q}}$) such that $\phi^*\mathcal{O}(1) = \psi^*\mathcal{O}(1)$. Then*

$$h_\phi(P) = h_\psi(P) + O(1)$$

holds for every $P \in X(\overline{\mathbf{Q}})$. The constant depends on X, ϕ, and ψ, but not on P.

Proof Let $\mathscr{L} = \phi^*\mathcal{O}(1) = \psi^*\mathcal{O}(1)$ and choose a basis $\{s_0, \dots, s_N\}$ for the $\overline{\mathbf{Q}}$-vector space $H^0(X, \mathscr{L})$. There are linear combinations

$$f_i = \sum_{j=0}^{N} a_{ij} s_j \text{ for } i = 0, \dots, n$$

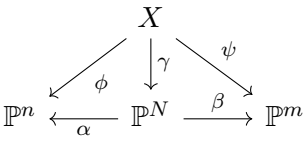
$$g_i = \sum_{j=0}^{N} b_{ij} s_j \text{ for } i = 0, \dots, m$$

such that $\phi = [f_0 : f_1 : \cdots : f_n]$ and $\psi = [g_0 : g_1 : \cdots : g_m]$. Let

$$\gamma = [s_0 : s_1 : \cdots : s_N]\colon X \to \mathbb{P}^N$$

be a morphism associated to $\mathscr{L}$ and let $\alpha\colon \mathbb{P}^N \to \mathbb{P}^n$ and $\beta\colon \mathbb{P}^N \to \mathbb{P}^m$ be the linear maps determined by the matrices (a_{ij}) and (b_{ij}), respectively. Then the

following diagram is commutative:



Applying Theorem 2.4 to α and β gives

$$h(\alpha(Q)) = h(Q) + O(1),$$
$$h(\beta(Q)) = h(Q) + O(1)$$

for every $Q \in \gamma(X(\overline{\mathbf{Q}}))$. Hence for every $P \in X(\overline{\mathbf{Q}})$ we have

$$\begin{aligned} h(\phi(P)) &= h(\alpha(\gamma(P))) = h(\gamma(P)) + O(1) \\ &= h(\beta(\gamma(P))) + O(1) = h(\psi(P)) + O(1) \end{aligned}$$

and we are done. □

The preceding theorem is the first step in constructing the so-called *Weil Height Machine*.

Let X be a projective variety over K and let $\phi\colon X \hookrightarrow \mathbb{P}^n$ be an embedding. Then $\mathscr{L} = \phi^*\mathcal{O}(1) \in \operatorname{Pic}(X)$ is a very ample line bundle. Conversely, if $\mathscr{L} \in \operatorname{Pic}(X)$ is a very ample line bundle, we can choose a basis $\{s_0, \dots, s_n\}$ of the space $H^0(X, \mathscr{L})$ of the global sections and define

$$\phi_{\mathscr{L}, s_0, \dots, s_n}\colon X \to \mathbb{P}^n, \quad x \mapsto [s_0(x) : \cdots : s_n(x)].$$

This map depends on the choice of the basis and is uniquely defined up to $\operatorname{Aut}(\mathbb{P}^n)$. Theorem 2.5 implies that, modulo a bounded function, we may define a height function associated to $\mathscr{L}$, namely $h_{\mathscr{L}} = h \circ \phi_{\mathscr{L}}$, because it does not depend on the choice of a morphism (that is, the choice of sections), up to $O(1)$. If $\mathscr{L}_1, \mathscr{L}_2 \in \operatorname{Pic}(X)$ are two very ample line bundles and $\phi_{\mathscr{L}_i}\colon X \to \mathbb{P}^{n_i}$ for $i = 1, 2$ are two associated morphisms, we can compose their product with the Segre embedding and obtain a morphism

$$\phi_{\mathscr{L}_1} \otimes \phi_{\mathscr{L}_2}\colon P \mapsto S_{n_1,n_2}(\phi_{\mathscr{L}_1}(P), \phi_{\mathscr{L}_2}(P)) \tag{2.5}$$

that corresponds to the line bundle $\mathscr{L}_1 \otimes \mathscr{L}_2$, since $S^*_{n_1,n_2}(\mathcal{O}(1)) = \mathcal{O}(1,1)$. The following classical result of algebraic geometry allows us to extend this definition of a height to arbitrary line bundles.

Lemma 2.6 *Let X be a projective Noetherian scheme. Then for every line bundle $\mathscr{L}$ there exist very ample line bundles $\mathscr{L}_1, \mathscr{L}_2$ such that $\mathscr{L} = \mathscr{L}_1 \otimes \mathscr{L}_2^{-1}$.*

Proof Recall that, by a theorem of Serre (see II.5.17 in [**HAG**]), there exists a positive integer n such that $\mathscr{L}(n) = \mathscr{L} \otimes \mathcal{O}(n)$ is ample. Therefore, for all sufficiently large integers m, the line bundle $\mathscr{L}^{\otimes m} \otimes \mathcal{O}(mn)$ is very ample. Since $\mathcal{O}(n)$ is very ample, we have

$$\mathscr{L} = (\mathscr{L} \otimes \mathcal{O}(n))^{m+1} \otimes (\mathscr{L}^m \otimes \mathcal{O}(mn+n))^{-1}$$

and we are done. □

We may now associate a height to any line bundle.

Definition 2.3 Let X be a projective variety over K and let $\mathscr{L} = \mathscr{L}_1 \otimes \mathscr{L}_2^{-1}$, with $\mathscr{L}_1, \mathscr{L}_2 \in \mathrm{Pic}(X)$ very ample. The *Weil height associated to* $\mathscr{L}$ is the function

$$h_{\mathscr{L}} \colon X(\overline{K}) \to \mathbf{R}, \quad h_{\mathscr{L}} = h_1 \circ \phi_{\mathscr{L}_1} - h_2 \circ \phi_{\mathscr{L}_2}, \tag{2.6}$$

where h_1 and h_2 are the logarithmic heights on the corresponding projective spaces.

The height $h_{\mathscr{L}}$ is well defined up to a bounded function (by Theorem 2.5); it does not depend on the decomposition of $\mathscr{L}$. The Weil height has some very useful properties, all up to a bounded function, as summarized in the following theorem (see Theorem B.3.2 in [**DG**], where the statement is given in terms of divisors).

Theorem 2.7 *Let X be a projective variety over the number field K. For any line bundle $\mathscr{L} \in \mathrm{Pic}(X)$, the Weil height function $h_{\mathscr{L}}$ has the following properties:*

(1) For $X = \mathbb{P}^n$, the function $h_{\mathcal{O}(1)} \colon \mathbb{P}^n(\overline{K}) \to \mathbf{R}$ "extends" the absolute logarithmic height, that is

$$h_{\mathcal{O}(1)}(P) = h(P) + O(1) \quad \textit{for all } P \in \mathbb{P}^n(\overline{K})$$

(2) (additivity) Let $\mathscr{L}, \mathscr{M} \in \mathrm{Pic}(X)$. Then

$$h_{\mathscr{L} \otimes \mathscr{M}}(P) = h_{\mathscr{L}}(P) + h_{\mathscr{M}}(P) + O(1) \quad \textit{for all } P \in X(\overline{K}).$$

(3) (functoriality) Let $\varphi\colon X \to Y$ be a morphism of projective varieties over K and let $\mathscr{L} \in \mathrm{Pic}(Y)$. Then

$$h_{\varphi^*\mathscr{L}}(P) = h_{\mathscr{L}}(\varphi(P)) + O(1).$$

(4) (positivity) Suppose $\mathscr{L} \in \mathrm{Pic}(X)$ is effective, i.e. $h^0(X, \mathscr{L}) > 0$, and let $\mathcal{B} = \cap_{s \in H^0(X,\mathscr{L})} Z(s)$ be the base locus of $\mathscr{L}$. Then

$$h_{\mathscr{L}}(P) \geq O(1) \quad \textit{for all } P \in (X \setminus \mathcal{B})(\overline{K}).$$

(5) (finiteness) Let $\mathscr{L} \in \mathrm{Pic}(X)$ be an ample line bundle and let L/K be a finite number field extension. Then for every $B > 0$, the set

$$\{P \in X(L) \mid h_{\mathscr{L}}(P) \leq B\}$$

is finite.

Proof Property *(1)* follows immediately from the definition, using the height function $h_{\mathcal{O}(1)} = h \circ \phi_{\mathcal{O}(1)}$, where $\phi_{\mathcal{O}(1)}$ is taken to be the identity morphism.

Let $\mathscr{L}, \mathscr{M} \in \mathrm{Pic}(X)$ be such that $\mathscr{L} = \mathscr{L}_1 \otimes \mathscr{L}_2^{-1}$ and $\mathscr{M} = \mathscr{M}_1 \otimes \mathscr{M}_2^{-1}$ for some very ample $\mathscr{L}_i, \mathscr{M}_j \in \mathrm{Pic}(X)$. Then $\mathscr{L}_1 \otimes \mathscr{M}_1$ and $\mathscr{L}_2 \otimes \mathscr{M}_2$ are very ample and therefore for every $P \in X(\overline{K})$ we have

$$\begin{aligned} h_{\mathscr{L}\otimes\mathscr{M}}(P) &= h_{\mathscr{L}_1\otimes\mathscr{M}_2\otimes(\mathscr{L}_2\otimes\mathscr{M}_2)^{-1}}(P) \\ &= h_{\mathscr{L}_1\otimes\mathscr{M}_2}(P) - h_{\mathscr{L}_2\otimes\mathscr{M}_2}(P) + O(1) \\ &= h_{\mathscr{L}_1}(P) + h_{\mathscr{M}_1}(P) - h_{\mathscr{L}_2}(P) - h_{\mathscr{M}_2}(P) + O(1) \\ &= h_{\mathscr{L}}(P) + h_{\mathscr{M}}(P) + O(1) \end{aligned}$$

The third equality follows by using (2.5) and Lemma 2.3, that together imply additivity for very ample line bundles. We therefore have *(2)*.

To prove functoriality *(3)*, suppose that $\mathscr{L} = \mathscr{L}_1 \otimes \mathscr{L}_2^{-1} \in \mathrm{Pic}(X)$, where the line bundles $\mathscr{L}_1, \mathscr{L}_2$ are very ample. Let $\phi_1 \circ \varphi$ and $\phi_2 \circ \varphi$ be two morphisms that are associated to $\varphi^*\mathscr{L}_1$ and $\varphi^*\mathscr{L}_2$, respectively. Then we have

$$\begin{aligned} h_{\varphi^*\mathscr{L}}(P) &= h_{\varphi^*\mathscr{L}_1}(P) - h_{\varphi^*\mathscr{L}_2}(P) + O(1) \\ &= (h \circ \phi_1 \circ \varphi)(P) - (h \circ \phi_2 \circ \varphi)(P) + O(1) \\ &= (h_{\mathscr{L}_1} \circ \varphi)(P) - (h_{\mathscr{L}_2} \circ \varphi)(P) + O(1) \\ &= (h_{\mathscr{L}} \circ \varphi)(P) + O(1) \end{aligned}$$

for every $P \in X(\overline{K})$ and *(3)* follows.

Now suppose that $\mathscr{L} = \mathscr{L}_1 \otimes \mathscr{L}_2^{-1}$ is effective with $\mathscr{L}_1, \mathscr{L}_2$ very ample. Let $\{s_0, \ldots, s_n\}$ be a basis for $H^0(X, \mathscr{L}_2)$. Since $\mathscr{L}$ is effective, it follows that

$$s_i \in H^0(X, \mathscr{L}_2 \otimes \mathscr{L}) = H^0(X, \mathscr{L}_1) \quad \text{for each } i.$$

We then extend this basis to a basis $\{s_0, \ldots, s_n, s_{n+1}, \ldots s_m\}$ of $H^0(X, \mathscr{L}_1)$ and define morphisms

$$\begin{aligned} \phi_{\mathscr{L}_1} &= [s_0 : \cdots : s_m] \colon X \to \mathbb{P}^m, \\ \phi_{\mathscr{L}_2} &= [s_0 : \cdots : s_n] \colon X \to \mathbb{P}^n. \end{aligned}$$

Now, since $\mathscr{L}_2$ is base-point free, the base locus of $\mathscr{L}_1$ coincides with the base locus $\mathcal{B}$ of $\mathscr{L}$ and for every $P \in X(\overline{K}) \setminus \mathcal{B}$, we have

$$\begin{aligned} h_{\mathscr{L}}(P) &= h_{\mathscr{L}_1}(P) - h_{\mathscr{L}_2}(P) + O(1) \\ &= h(\phi_{\mathscr{L}_1}(P)) - h(\phi_{\mathscr{L}_1}(P)) + O(1) \\ &= h([s_0(P) : \cdots : s_m(P)]) - h([s_0(P) : \cdots : s_n(P)]) + O(1) \\ &\geq O(1) \quad (\text{since } m \geq n). \end{aligned}$$

This establishes positivity *(4)*.

To show finiteness *(5)*, it suffices to consider the case of a very ample $\mathscr{L}$ because if $\mathscr{L}$ is ample, then $\mathscr{L}^{\otimes m}$ is very ample for some positive integer n and, by additivity, we have $h_{\mathscr{L}^{\otimes m}} = m h_{\mathscr{L}} + O(1)$. Suppose that $\mathscr{L}$ is very ample so that $\phi_{\mathscr{L}} \colon X \hookrightarrow \mathbb{P}^n$ is an embedding. Then we have $h_{\mathscr{L}}(P) = h(\phi_{\mathscr{L}}(P)) + O(1)$, and property *(5)* follows by Theorem 2.2. □

Remark 2.2 For each $\mathscr{L} \in \mathrm{Pic}(X)$, the Weil height function $h_{\mathscr{L}}$ is uniquely determined, up to $O(1)$, by properties *(1)*, *(2)* and *(3)*. In fact, it suffices to restrict *(3)* to embeddings $\varphi \colon X \hookrightarrow \mathbb{P}^n$.

2.4 Canonical heights on abelian varieties

It is possible to further refine the Weil height. Under certain assumptions, there exists a function in the same equivalence class (modulo bounded functions) as a given Weil height function $h_{\mathscr{L}}$, that satisfies very nice properties, as we will see below.

Theorem 2.8 (Néron & Tate) *Let X be a projective variety over K and let $\mathscr{L} \in \mathrm{Pic}(X)$. Suppose that $\phi\colon X \to X$ is an endomorphism such that*

$$\phi^*\mathscr{L} = \mathscr{L}^{\otimes d} \qquad \text{for some } d \in \mathbf{Z}_{\geq 2}.$$

Let $\phi^n = \phi \circ \phi \circ \cdots \circ \phi$ denote the n-th self-composition of ϕ. Then the function $\hat{h}_{\phi,\mathscr{L}}\colon X(\overline{K}) \to \mathbf{R}$ given by

$$\hat{h}_{\phi,\mathscr{L}}\colon P \mapsto \lim_{n\to\infty} \frac{h_{\mathscr{L}}(\phi^n(P))}{d^n} \tag{2.7}$$

is well defined and it is the unique function satisfying:

(1) $\hat{h}_{\phi,\mathscr{L}}(P) = h_{\mathscr{L}}(P) + O(1)$;

(2) $\hat{h}_{\phi,\mathscr{L}}(\phi(P)) = dh_{\mathscr{L}}(P)$.

We refer to $\hat{h}_{\phi,\mathscr{L}}$ as the *canonical height associated to $\mathscr{L}$ and ϕ*.

Proof We show that the sequence

$$n \mapsto h_{\mathscr{L}}(\phi^n(P))d^{-n} \tag{2.8}$$

is Cauchy and therefore convergent. Since $\phi^*\mathscr{L} = \mathscr{L}^{\otimes d}$, by assumption, linearity of the Weil height implies

$$h_{\mathscr{L}}(\phi(P)) = dh_{\mathscr{L}}(P) + O(1) \quad \text{for every } P \in X(\overline{K}).$$

More precisely, there exists a constant $C \geq 0$, independent of P, such that

$$|h_{\mathscr{L}}(\phi(P)) - dh_{\mathscr{L}}(P)| \leq C \quad \text{for every } P \in X(\overline{K}). \tag{2.9}$$

Hence for any two positive integers $m \geq n$, we have

$$\begin{aligned}
\left|\frac{h_{\mathscr{L}}(\phi^m(P))}{d^m} - \frac{h_{\mathscr{L}}(\phi^n(P))}{d^n}\right| &= \left|\sum_{i=n}^{m-1} \frac{1}{d^{i+1}}\left(h_{\mathscr{L}}(\phi^{i+1}(P)) - dh_{\mathscr{L}}(\phi^i(P))\right)\right| \\
&\leq \sum_{i=n}^{m-1} \frac{1}{d^{i+1}}\left|h_{\mathscr{L}}(\phi^{i+1}(P)) - dh_{\mathscr{L}}(\phi^i(P))\right| \\
&\leq \sum_{i=n}^{m-1} \frac{1}{d^{i+1}} C \quad \text{(applying (2.9))} \\
&= \frac{d^{-n} - d^{-m}}{d-1} C.
\end{aligned} \tag{2.10}$$

The last expression converges to zero as $m, n \to \infty$ and therefore (2.8) converges and $\hat{h}_{\phi,\mathscr{L}}$ is well defined. Now putting $n = 0$ and $m \to \infty$ in (2.10) gives *(1)*, while property *(2)* follows directly from the definition (2.7). Given two functions that satisfy both said properties, it follows that their difference is bounded and satisfies property *(2)* and is therefore zero. □

Theorem 2.8 allows us to associate a height function to a pair $(A, \mathscr{L})$ in a canonical way. We first recall the following lemma.

Lemma 2.9 (Mumford's Formula) *Let A be an abelian variety over any field and let $n \in \mathbf{Z}$. Then for any $\mathscr{L} \in \mathrm{Pic}(A)$, the map $[n]\colon A \to A$ satisfies*

$$[n]^*\mathscr{L} = \mathscr{L}^{\frac{n^2+n}{2}} \otimes ([-1]^*\mathscr{L})^{\frac{n^2-n}{2}}.$$

In particular,

$$[n]^*\mathscr{L} = \mathscr{L}^{n^2} \quad \text{if } \mathscr{L} \text{ is symmetric, i.e. if } [-1]^*\mathscr{L} = \mathscr{L};$$
$$[n]^*\mathscr{L} = \mathscr{L}^{n} \quad \text{if } \mathscr{L} \text{ is anti-symmetric, i.e. if } [-1]^*\mathscr{L}^{-1} = \mathscr{L}.$$

Proof This ultimately follows from the Theorem of the Cube for abelian varieties. See Corollary 6.6 in [**Miln1**]. □

The following statements describe the corresponding relations for heights.

Corollary 2.10 *Let A be an abelian variety over the number field K and let $\mathscr{L} \in \mathrm{Pic}(A)$ be a symmetric line bundle on A. Then there is a unique function $\hat{h}_{\mathscr{L}}\colon A(\overline{K}) \to \mathbf{R}$ in the equivalence class of $h_{\mathscr{L}}$ (modulo bounded functions) that satisfies*

$$\hat{h}_{\mathscr{L}}([m]P) = m^2\hat{h}_{\mathscr{L}}(P) \quad \text{for all } m \in \mathbf{Z} \text{ and all } P \in A(\overline{K}) \tag{2.11}$$

Moreover, the function $\hat{h}_{\mathscr{L}}$ satisfies the parallelogram law. That is to say that for all $P, Q \in A(\overline{K})$ we have

$$\hat{h}_{\mathscr{L}}(P+Q) + \hat{h}_{\mathscr{L}}(P-Q) = 2\hat{h}_{\mathscr{L}}(P) + 2\hat{h}_{\mathscr{L}}(Q). \tag{2.12}$$

Proof Let $\hat{h}_{\mathscr{L}}\colon A(\overline{K}) \to \mathbf{R}$ be the function

$$\hat{h}_{\mathscr{L}}\colon P \mapsto \lim_{n\to\infty} \frac{1}{4^n} h_{\mathscr{L}}([2^n]P).$$

Then equality in (2.11) follows immediately from the equality $[m]^*\mathscr{L} = \mathscr{L}^{m^2}$ and Theorem 2.8. The same two also imply that for any integer $m \geq 2$, we have

$$\hat{h}_{\mathscr{L}}([m]P) = m^2\hat{h}_{\mathscr{L}}(P) + O(1) \quad \text{for any } P \in A(\overline{K}).$$

Note that the definition of $\hat{h}_{\mathscr{L}}$ uses the doubling map and does not depend on m. Hence when dealing with $\hat{h}_{\mathscr{L}}(P)$, we can always replace P by $[2^n]P$ and divide by 4^n. This gives

$$\begin{aligned}\hat{h}_{\mathscr{L}}([m]P) &= \lim_{n\to\infty} \frac{1}{4^n} h_{\mathscr{L}}([2^n m]P) \\ &= \lim_{n\to\infty} \frac{1}{4^n} h_{\mathscr{L}}([m2^n]P) \\ &= \lim_{n\to\infty} \frac{1}{4^n} (m^2 h_{\mathscr{L}}([2^n]P) + O(1)) \\ &= m^2 \hat{h}_{\mathscr{L}}(P)\end{aligned} \tag{2.13}$$

and (2.11) follows for any m. By Theorem 2.8, the function $\hat{h}_{\mathscr{L}}$ is unique and independent of our initial choice of $m = 2$.

We recall that, again, it follows ultimately from the Theorem of the Cube that $[-1]^*\mathscr{L} = \mathscr{L}$ if and only if

$$s^*\mathscr{L} \otimes d^*\mathscr{L} = (\pi_1^*\mathscr{L})^2 \otimes (\pi_2^*\mathscr{L})^2, \tag{2.14}$$

where $s, d, \pi_1, \pi_2 \colon A \times A \to A$ are the sum, the difference, and the projection morphisms, respectively. Equation (2.14) implies the parallelogram law up to $O(1)$ for $h_{\mathscr{L}}$, and hence also for $\hat{h}_{\mathscr{L}}$ because they are in the same equivalence class modulo bounded functions. Indeed, we have

$$\hat{h}_{\mathscr{L}}(P+Q) + \hat{h}_{\mathscr{L}}(P-Q) = 2\hat{h}_{\mathscr{L}}(P) + 2\hat{h}_{\mathscr{L}}(Q) + O(1) \quad \text{for all } P, Q \in A(\overline{K}).$$

We can now replace P and Q by $[2^n]P$ and $[2^n]Q$, respectively, divide by 4^n and let $n \to \infty$. This yields (2.12) because the $O(1)$ does not depend on P and Q. □

Remark 2.3 The parallelogram law implies that we can associate to $\hat{h}_{\mathscr{L}}$ a bilinear pairing $A(\overline{K}) \times A(\overline{K}) \to \mathbf{R}$, called the *canonical height pairing*, defined as

$$\langle P, Q\rangle = \frac{1}{2}\left(\hat{h}_{\mathscr{L}}(P+Q) - \hat{h}_{\mathscr{L}}(P) - \hat{h}_{\mathscr{L}}(Q)\right), \tag{2.15}$$

which together with (2.11), makes $\hat{h}_{\mathscr{L}}$ a *quadratic form* on $A(\overline{K})$.

Remark 2.4 It is possible to choose $\mathscr{L} \in \mathrm{Pic}(A)$ that is ample and symmetric and this is usually sufficient for applications. In this case, the canonical height $\hat{h}_{\mathscr{L}}$ has the nice property that $\hat{h}_{\mathscr{L}}(P) = 0$ if and only if $P \in A(\overline{K})$ is a torsion point. Indeed, it is clear from (2.11) that $\hat{h}_{\mathscr{L}}$ sends torsion points on $A(\overline{K})$ to zero. On the other hand, suppose that $\hat{h}_{\mathscr{L}}(P) = 0$ for some $P \in A(\overline{K})$. Then for every $n \in \mathbf{Z}$, we have

$$h_{\mathscr{L}}(nP) = \hat{h}_{\mathscr{L}}(nP) + O(1) = n^2 \hat{h}_{\mathscr{L}}(P) + O(1) = O(1).$$

It follows that the Weil height is bounded on the set $\{P, 2P, 3P, \dots\}$ and therefore the set must be finite by Northcott's Theorem.

There is an analogous result for anti-symmetric line bundles. In this case, the canonical height is linear.

Corollary 2.11 *Let A be an abelian variety over the number field K and let $\mathscr{L} \in \mathrm{Pic}(A)$ be an anti-symmetric line bundle on A. Then there is a unique function $\hat{h}_{\mathscr{L}} \colon A(\overline{K}) \to \mathbf{R}$ in the equivalence class of $h_{\mathscr{L}}$ (modulo bounded functions) that satisfies*

$$\hat{h}_{\mathscr{L}}(P+Q) = \hat{h}_{\mathscr{L}}(P) + \hat{h}_{\mathscr{L}}(Q) \quad \text{for all } P, Q \in A(\overline{K}), \tag{2.16}$$

and it is therefore a group homomorphism.

Proof Define $\hat{h}_{\mathscr{L}} \colon A(\overline{K}) \to \mathbf{R}$ to be the function

$$\hat{h}_{\mathscr{L}} \colon P \mapsto \lim_{n\to\infty} \frac{1}{2^n} h_{\mathscr{L}}([2^n]P).$$

The proof of linearity is now analogous to the proof of Corollary 2.10. Any two homomorphisms $A(\overline{K}) \to \mathbf{R}$ whose difference is bounded must be equal because the image of their difference is a bounded and therefore trivial subgroup of $\mathbf{R}$. Hence (2.16) uniquely determines $\hat{h}_{\mathscr{L}}$ within its class. □

Now we can extend the canonical height to arbitrary line bundles, but first we recall a useful definition. Let G and H be two abelian groups, written additively, and suppose that H is such that $[2] \colon H \to H$ is invertible. We say that a function $f \colon G \to H$ is *quadratic* if for all $P, Q, R \in G$, we have

$$f(P+Q+R) - f(P+Q) - f(P+R) - f(Q+R) + f(P) + f(Q) + f(R) - f(0) = 0.$$

Theorem 2.12 *Let A be an abelian variety and let $\mathscr{L} \in \mathrm{Pic}(A)$ be a line bundle on A. Then the following hold:*

(1) There is a unique quadratic function $\hat{h}_{\mathscr{L}} \colon A(\overline{K}) \to \mathbf{R}$ in the equivalence class of $h_{\mathscr{L}}$ (modulo bounded functions) such that $\hat{h}_{\mathscr{L}}(0) = 0$;

(2) For all $\mathscr{L}, \mathscr{M} \in \mathrm{Pic}(A)$, we have $\hat{h}_{\mathscr{L}\otimes\mathscr{M}} = \hat{h}_{\mathscr{L}} + \hat{h}_{\mathscr{M}}$;

(3) For any morphism $\phi \colon B \to A$ of abelian varieties, we have

$$\hat{h}_{\phi^*\mathscr{L}} = \hat{h}_{\mathscr{L}} \circ \phi - \hat{h}_{\mathscr{L}}(\phi(0)).$$

We call $\hat{h}_{\mathscr{L}}$ the *canonical height associated* to $\mathscr{L}$ or the *Néron-Tate height* associated to $\mathscr{L}$.

Proof Let $\mathscr{L}_1 = \mathscr{L} \otimes [-1]^*\mathscr{L}$ and $\mathscr{L}_2 = \mathscr{L} \otimes ([-1]^*\mathscr{L})^{-1}$. Then $\mathscr{L}_1$ is symmetric and $\mathscr{L}_2$ is anti-symmetric. We can therefore define

$$\hat{h}_{\mathscr{L}} := \frac{1}{2}\left(\hat{h}_{\mathscr{L}_1} + \hat{h}_{\mathscr{L}_2}\right).$$

Most of the properties follow by arguments analogous to the ones in Corollaries 2.10 and 2.11. That $\hat{h}_{\mathscr{L}} = h_{\mathscr{L}} + O(1)$ is quadratic and $\hat{h}_{\mathscr{L}}(0) = 0$ is clear from the construction. Let h_1 and h_2 be two quadratic functions in the class of $h_{\mathscr{L}}$ that satisfy $h_1(0) = h_2(0) = 0$. Then $f = h_1 - h_2$ is a bounded quadratic function and $f(0) = 0$. This implies that the associated bilinear pairing $A(\overline{K}) \times A(\overline{K}) \to \mathbf{R}$ given by

$$\langle P, Q\rangle = \frac{1}{2}\left(f(P+Q) - f(P) - f(Q) + f(0)\right)$$

is also bounded and therefore identically zero, whence $f(P+Q) = f(P)+f(Q)$. This, along with the fact that f is bounded, implies that f is identically zero, proving *(1)*. Applying *(1)* to the function $\hat{h}_{\mathscr{L}} + \hat{h}_{\mathscr{M}} = \hat{h}_{\mathscr{L}\otimes\mathscr{M}} + O(1)$ proves *(2)*, while *(3)* follows from the fact that every morphism of abelian varieties is a group homomorphism composed with a translation (see Corollary 2.2 in [**Miln1**]). □

2.5 Relation to intersection theory on arithmetic surfaces

Let S be a Dedekind scheme, i.e. a normal, irreducible, locally Noetherian scheme of dimension 0 or 1. Following the notations in [**Liu**], let η denote the generic point of S and let s denote a closed point of S, with residue field $k(s)$. Let C be a smooth, projective, geometrically connected curve of genus $g > 0$ over the function field $K(S)$ of S.

Definition 2.4 A *model of C over S* is a pair $(\mathcal{C}, f)$, where $\phi\colon \mathcal{C} \to S$ is an integral, normal, projective, flat, Noetherian S-scheme of dimension 2 with generic fibre $\mathcal{C}_\eta$, and $f\colon C \xrightarrow{\sim} \mathcal{C}_\eta$ is an isomorphism.

We usually omit the isomorphism f from the notation and talk about a model $\mathcal{C}$, with the understanding that a particular isomorphism is fixed.

Definition 2.5 A fibre $\mathcal{C}_s$ is called the *reduction of C at s*. If C has a smooth model over $\operatorname{Spec}(\mathcal{O}_{S,s})$, it is said to have *good reduction at s*, otherwise it is said to have *bad reduction*.

A morphism $\mathcal{C} \to \mathcal{C}'$ of models is a morphism of S-schemes that respects the isomorphisms $\mathcal{C}_\eta \cong C$ and ${\mathcal{C}'}_\eta \cong C$. We are particularly interested in regular models. A regular model $\mathcal{C} \to S$, with S one-dimensional, is usually called an *arithmetic surface*.

A regular model $\mathcal{C}$ is called *relatively minimal* if every proper birational morphism $\mathcal{C} \to \mathcal{C}'$ (as S-schemes), where $\mathcal{C}' \to S$ is a regular model of C, is an isomorphism. It is called *minimal* if every birational map $\mathcal{C}' \dashrightarrow \mathcal{C}$ is a birational morphism. A minimal model is relatively minimal.

Theorem 2.13 *With S and $C/K(S)$ defined as above and with $\dim S = 1$, there exists a minimal regular model $\mathcal{C} \to S$ of C.*

Proof See 9.3.3 and its preceding sections in [**Liu**]. □

Concrete cases that we have in mind are $S = \operatorname{Spec}(R)$, where R is the ring of integers of a valuated field k with a discrete valuation v, that is

$$R = \{x \in k \mid v(x) \geq 0\}.$$

Therefore, let k denote a field with a discrete valuation, let C denote a smooth, projective, geometrically connected curve of genus $g > 0$ over k, and let $\mathcal{C}$ denote the minimal regular model of C (over the corresponding Dedekind scheme).

2.5.1 The non-archimedean case

Suppose k is a local non-archimedean field with a discrete valuation v. Let O_v denote the ring of integers of k and let $S = \mathrm{Spec}(O_v)$. The residue field $k(s)$ at s will also be denoted by the conventional $k(v)$.

For a prime divisor $D \in \mathrm{Div}(C)$, let $\overline{D} \in \mathrm{Div}(\mathcal{C})$ denote the prime divisor that is the Zariski closure of D in $\mathcal{C}$ and extend the association $D \mapsto \overline{D}$ by linearity. For any closed point $x \in \mathcal{C}_v$ and any two distinct prime divisors D, E, respectively defined locally at x by $f, g \in \mathcal{O}_{\mathcal{C},x}$, we define their *intersection multiplicity at* x as

$$i_x(D, E) := \mathrm{length}(\mathcal{O}_{\mathcal{C},x}/(f, g)) \quad (\text{as an } \mathcal{O}_{\mathcal{C},x} - \text{module}). \tag{2.17}$$

This definition extends by linearity to all divisors D, E with no common component. The *total intersection multiplicity* of D, E is defined as

$$i_v(D, E) := \sum_x i_x(D, E)[k(x) : k(v)],$$

where the sum is over closed points $x \in \mathcal{C}_v$. We refer to the divisor

$$D \cdot E := \sum_x i_x(D, E)[x]$$

as the intersection of D and E. If $D \cdot E$ is a single point with some multiplicity, the multiplicity is sometimes also denoted by $D \cdot E$.

We denote by $\mathrm{Div}_v(\mathcal{C})$ the group freely generated by the (finitely many) irreducible components of $\mathcal{C}_v$.

Theorem 2.14 (Hriljac [**Hri**]) *For every $D \in \mathrm{Div}^0(C)$, there exists a divisor $\Phi_v(D) \in \mathrm{Div}_v(\mathcal{C}) \otimes \mathbf{Q}$ such that $\overline{D} + \Phi_v(D)$ is orthogonal to, i.e. it has trivial intersection with, all elements of $\mathrm{Div}_v(\mathcal{C})$.*

This theorem provides justification for the following definition.

Definition 2.6 Let $D, E \in \mathrm{Div}^0(C)$ be two divisors with disjoint supports. Then their *local Néron symbol* is defined as

$$\langle D, E\rangle_v := i_v(\overline{D} + \Phi_v(D), \overline{E}) \log(\#k(v)).$$

Proposition 2.2 *The local Néron symbol is well defined and does not depend on the choice of the regular model $\mathcal{C}$ or on the choice of the divisor $\Phi_v(D)$.*

Proof See Theorem III.5.2 in [**Lang2**]. □

Let $f \in k(C)^\times$ and let $D = \sum_i n_i P_i \in \mathrm{Div}^0(C)$ be coprime to (f). Then we define

$$f(D) := \prod_i f(P_i)^{n_i}.$$

Theorem 2.15 *Suppose $C(k)$ is Zariski dense in C. Then for any pair of divisors $D, E \in \mathrm{Div}^0(C)$ with disjoint supports, one can define in a unique way a real number $\langle D, E\rangle_v$ such that:*

(1) The pairing is bilinear;

(2) The pairing is symmetric;

(3) If $D = (f)$, then $\langle D, E\rangle_v = v \circ f(E)$, where $v(z) = -\log ||z||_v$;

(4) Fix any $P_0 \in C(k) \setminus \mathrm{supp}(D)$. Then the map $C(k) \setminus \mathrm{supp}(D) \to \mathbf{R}$ given by

$$P \mapsto \langle D, P - P_0\rangle_v$$

is continuous and locally bounded.

Proof See Theorem III.5.1 in [**Lang2**]. □

Remark 2.5 Let k'/k be a field extension and let $w \in M_{k'}$ be an absolute value dividing v. Then restricting $\langle D, E\rangle_w$ to k gives the symbol $\langle D, E\rangle_v$ if $D, E \in \mathrm{Div}^0(C(k))$. Therefore, by taking an appropriate field extension, one can drop the assumptions of k-rationality and Zariski density.

Lemma 2.16 *Let $\varphi\colon X \to Y$ be a projective surjective morphism of arithmetic surfaces. Let $D \in \mathrm{Div}(X)$ be a prime divisor and let $E \in \mathrm{Div}(Y)$, such that D is not contained in $\varphi^{-1}(\mathrm{supp}(E))$. Then*

$$\sum_x i_x(D, \varphi^* E)[k(x) : k(y)] = \begin{cases} 0 & \text{if } \varphi(D) \text{ is a point,} \\ [k(D) : k(\varphi(D))] i_y(\varphi(D), E) & \text{otherwise.} \end{cases}$$

Proof See Theorem III.4.1 in [**Lang2**] or Theorem 9.2.12 and its succeeding remark in [**Liu**]. □

Corollary 2.17 (Projection Formula) *With notations as in the preceding lemma, we have*

$$\varphi_*(D \cdot \varphi^* E) = (\varphi_* D) \cdot E.$$

2.5.2 The archimedean case

We will now deal with the local archimedean case and modify the definitions accordingly. Since $\bar{k}_v = \mathbf{C}$, we have that $\mathcal{X} := C(\bar{k}_v)$ is a compact connected Riemann surface of genus $g \geq 1$. In the archimedean setting, the definitions are complex-analytic and it is the Arakelov-Green function that plays the role of the intersection multiplicity defined by (2.17). We recall some necessary prerequisites first.

Let $\Omega^1_{\mathcal{X}}$ denote the sheaf of holomorphic 1-forms on $\mathcal{X}$. The holomorphic differentials $H^0(\mathcal{X}, \Omega^1_{\mathcal{X}})$ are a g-dimensional vector space, equipped with a hermitian inner product:

$$\langle \omega, \eta \rangle = \frac{i}{(2\pi)^2} \int_{\mathcal{X}} \omega \wedge \bar{\eta}. \tag{2.18}$$

Let $\{\omega_1, \ldots, \omega_n\}$ be an orthonormal basis of $H^0(\mathcal{X}, \Omega^1_{\mathcal{X}})$ with respect to (2.18). Then one defines a *canonical fundamental (1,1)-form* μ as

$$\mu := \frac{i}{(2\pi)^2 g} \sum_{j=1}^{g} \omega_j \wedge \bar{\omega}_j, \tag{2.19}$$

which does not depend on the choice of the basis.

Theorem 2.18 (Arakelov [**Ara**]) *There exists a unique function*

$$G \colon \mathcal{X} \times \mathcal{X} \to \mathbf{R}_{\geq 0},$$

called the Arakelov-Green function, such that the following hold for all $P \in \mathcal{X}$:

(1) For all $Q \in \mathcal{X}$, the function $\log G(P, Q)$ is C^∞ if $Q \neq P$;

(2) Locally at $P \in \mathcal{X}$, we have $\log G(P, Q) = \log |z(Q)| + f(Q)$, where z is a local coordinate at P with $z(P) = 0$ and $f \in C^\infty(P)$;

(3) For all $Q \in \mathcal{X}$, we have $\partial_Q \bar{\partial}_Q \log G^2(P,Q) = 2\pi i \mu(Q)$ if $Q \neq P$;

(4) For all $Q \in \mathcal{X}$, we have $\int_{\mathcal{X}} \log G(P,Q)\mu(Q) = 0$.

It follows from the Theorem of Stokes that the Arakelov-Green function is symmetric, i.e. for all $P, Q \in \mathcal{X}$, we have $G(P,Q) = G(Q,P)$ if $P \neq Q$ (see [**Falt1**] for example).

For every $D \in \mathrm{Div}(\mathcal{X})$, the Arakelov-Green function induces a Hermitian metric on $\mathscr{L}(D)$. It suffices to consider the case of points $P \in \mathcal{X}$ as the general case then follows by taking tensor products of line bundles. If $P \in \mathcal{X}$, then we define a smooth Hermitian metric on $\mathscr{L}(P)$ as

$$||1||_P \colon Q \mapsto G(P,Q),$$

where 1 denotes the constant section of $\mathscr{L}(P)$. We refer to a line bundle with a smooth Hermitian metric as a *metrized line bundle*.

Let f be a non-zero meromorphic function on $\mathcal{X}$ and assume the standard Hermitian metric on $\mathbf{C}$. For a local coordinate z, we have

$$\begin{aligned} \partial\bar{\partial} \log ||f(z)||^2 &= \partial\bar{\partial} \log(f(z)\overline{f(z)}) \\ &= \partial\bar{\partial}(\log f(z) + \log \overline{f(z)}) = 0 \end{aligned}$$

away from the zero-poles of f. Therefore if $\mathscr{L}$ is a metrized line bundle on $\mathcal{X}$, with a metric $||\cdot||$, we can define its *curvature*, that is the following (1,1)-form:

$$\mathrm{curv}_{\mathscr{L}} = \frac{1}{2\pi i}\partial\bar{\partial} \log(||s||^2) = \frac{1}{2\pi i}\frac{\partial^2 \log(||s||^2)}{\partial z \partial \bar{z}} \mathrm{d}z \wedge \mathrm{d}\bar{z},$$

where s is a local generating section of $\mathscr{L}$ and z is a local coordinate. For a line bundle $\mathscr{L}$, a metric is called *admissible* if $\mathrm{curv}_{\mathscr{L}}$ with respect to the metric is a multiple of the canonical fundamental form μ (recall (2.19)).

Example 2.1 The holomorphic cotangent bundle $\Omega^1_{\mathcal{X}}$ is metrizable with an admissible metric. Let Δ denote the diagonal on $\mathcal{X} \times \mathcal{X}$. By the Adjunction Formula (cf. [**PAG**] pp. 146–148), there is a canonical isomorphism

$$\mathscr{L}(-\Delta)|_{\Delta} \xrightarrow{\sim} \Omega^1_{\mathcal{X}}. \tag{2.20}$$

The line bundle $\mathscr{L}(\Delta)$ is metrizable by $||1||(P,Q) := G(P,Q)$. The *Arakelov metric* $||\cdot||_{\mathrm{Ar}}$ is the unique metric on $\Omega^1_{\mathcal{X}}$ that makes the isomorphism (2.20) an isometry. It was proved by Arakelov in [**Ara**] that $||\cdot||_{\mathrm{Ar}}$ is admissible.

For $D \in \mathrm{Div}(\mathcal{X})$ and $P \in \mathcal{X}$, let $G(D,P) := \prod_{Q \in D} G(P,Q)$, taking multiplicities in D into account.

Theorem 2.19 (Analytic projection formula) *Let $\mathcal{X}$ and $\mathcal{X}'$ be Riemann surfaces of genus one and let $G_{\mathcal{X}}$ and $G_{\mathcal{X}'}$ denote their Arakelov-Green functions, respectively. Let $\varphi\colon \mathcal{X} \to \mathcal{X}'$ be a non-constant holomorphic map and let $D \in \mathrm{Div}(\mathcal{X}')$. Then the canonical isomorphism*

$$\varphi^* \mathscr{L}(D) \xrightarrow{\sim} \mathscr{L}(\varphi^* D)$$

is an isometry and for any $P \in \mathcal{X}$, we have

$$G_{\mathcal{X}}(\varphi^* D, P) = G_{\mathcal{X}'}(D, \varphi(P)).$$

Proof See Propositions 3.1 and 3.2 in [**dJ**]. □

Definition 2.7 Let $D, E \in \mathrm{Div}(\mathcal{X})$ be two divisors with disjoint supports. Then their *local Néron symbol* is defined as

$$\langle D, E \rangle_v := -\varepsilon_v \log G(D,E),$$

where

$$\varepsilon_v = \begin{cases} 1 & \text{if } k_v = \mathbf{R}, \\ 2 & \text{if } k_v = \mathbf{C}. \end{cases}$$

Remark 2.6 Let f be a non-zero meromorphic function on the Riemann surface $\mathcal{X}$. Then for any point $P \notin \mathrm{div}(f)$, we have

$$\partial_P \bar{\partial}_P \log G^2(\mathrm{div}(f), P) = 0$$

because $\mathrm{div}(f) \in \mathrm{Div}^0(\mathcal{X})$. Outside $\mathrm{div}(f)$, we have $\partial\bar{\partial} \log |f|^2 = 0$ since f is holomorphic there. It follows that

$$G(\mathrm{div}(f), P) = e^a |f(P)|$$

for some real number a, independent of P. Taking the logarithm and integrating over $\mathcal{X}$ (with respect to μ), and using the fact $\int_{\mathcal{X}} \log G(P,Q) \mu(Q) = 0$, one finds that

$$a = -\int_{\mathcal{X}} \log |f| \, \mu.$$

2.5.3 Adding the infinite places

Let K be a number field and let M_K be its set of places. We denote by K_v the v-adic completion of K at v and we denote by O_v the ring of integers at v if v is a prime. Let $X \to \mathrm{Spec}(O_K)$ be an arithmetic surface whose generic fibre is isomorphic to a smooth, projective, geometrically connected curve over K, of positive genus.

Definition 2.8 An *Arakelov divisor* on X is a formal sum of a divisor in $\mathrm{Div}(X)$ and a sum $\sum_\sigma \alpha_\sigma X_\sigma$, where $\sigma\colon K \hookrightarrow \mathbf{C}$ are the archimedean places, $\alpha_\sigma \in \mathbf{R}$, and $X_\sigma = X_\eta \otimes_\sigma \mathbf{C}$ is a Riemann surface with the corresponding complex structure. Arakelov divisors form a group, denoted by $\widehat{\mathrm{Div}}(X)$. The X_σ are referred to as the *fibres of X at infinity*.

For $D \in \widehat{\mathrm{Div}}(X)$ we usually write $D = D_{\mathrm{fin}} + D_{\mathrm{inf}}$, where $D_{\mathrm{fin}} \in \mathrm{Div}(X)$ and $D_{\mathrm{inf}} = \sum_\sigma \alpha_\sigma X_\sigma$.

Now let f be a non-zero rational function on X. We define the principal Arakelov divisor associated to f as the sum

$$(f) = \mathrm{div}(f) + \sum_\sigma a_\sigma(f) X_\sigma, \tag{2.21}$$

where $\mathrm{div}(f)$ is the usual principal divisor of f and $a_\sigma(f) := -\int_{X_\sigma} \log|f|_\sigma \, \mu_\sigma$, where μ_σ denotes the canonical form on X_σ, as defined above. We define two divisors in $\widehat{\mathrm{Div}}(X)$ to be linearly equivalent if their difference is a principal Arakelov divisor and we denote the group of Arakelov divisors modulo linear equivalence by $\widehat{\mathrm{Cl}}(X)$.

We are now ready to extend the definition of intersections and the Néron pairing. Recall that a divisor $D \in \mathrm{Div}(X)$ is called *vertical* if its support is contained in a fibre of the structure morphism $X \to \mathrm{Spec}(O_K)$, and that it is called *horizontal* if the restriction of the structure morphism to D is surjective. For $D, E \in \widehat{\mathrm{Div}}(X)$ and $v, v' \in M_K^\infty$ we define:

(1) If D is vertical and $E = X_v$, then $\langle D, E\rangle_v = 0$;

(2) If D is horizontal and $E = X_v$, then $\langle D, E\rangle_v = \varepsilon_v [K(D) : K]$;

(3) If $D = X_v$ and $E = X_{v'}$, then $\langle D, E\rangle_v = 0$;

(4) If D, E are horizontal, then $\langle D, E\rangle_v = -\varepsilon_v \log G_\sigma(D^\sigma, E^\sigma)$.

By linearity, this extends to a pairing $\widehat{\mathrm{Div}}(X) \times \widehat{\mathrm{Div}}(X) \to \mathbf{R}$ as

$$\langle D, E \rangle = \sum_{v \in M_K} \langle D, E \rangle_v. \tag{2.22}$$

Proposition 2.3 *Let $(f) \in \widehat{\mathrm{Div}}(X)$ be a principal divisor. Then for any divisor $D \in \widehat{\mathrm{Div}}(X)$, we have $\langle (f), D \rangle = 0$.*

Proof The only interesting case to prove is when D is a horizontal divisor because the other cases follow directly from the definitions. We have

$$\begin{aligned}\langle (f), D \rangle &= \langle \mathrm{div}(f) + \sum_\sigma a_\sigma X_\sigma \rangle \\ &= \sum_{v \in M_K^0} \langle \mathrm{div}(f), D \rangle_v + \sum_{v \in M_K^\infty} \varepsilon_v \langle \mathrm{div}(f), D \rangle_v + \sum_{v \in M_K^\infty} \varepsilon_v a_v \\ &- \sum_{v \in M_K^0} \log ||f(D)||_v - \sum_{v \in M_K^\infty} \log(e^{\varepsilon_v a_v} ||f(D^v)||_v) + \sum_{v \in M_K^\infty} \varepsilon_v a_v.\end{aligned}$$

The middle sum follows from Remark 2.6. Now all the terms with a_v cancel out and the remaining sum is zero by the product formula. □

Theorem 2.20 ([**Ara**]) *The pairing defined by* (2.22) *respects linear equivalence and therefore induces a canonical pairing $\widehat{\mathrm{Cl}}(X) \times \widehat{\mathrm{Cl}}(X) \to \mathbf{R}$.*

A line bundle $\mathscr{L}$ on X is called admissible if its restrictions to X_σ are metrized line bundles equipped with admissible metrics, as defined above. The group of admissible line bundles modulo isomorphisms is denoted by $\widehat{\mathrm{Pic}}(X)$.

To every Arakelov divisor $D = D_{\mathrm{fin}} + D_{\mathrm{inf}}$, we associate the metrized line bundle $\mathscr{L}(D_{\mathrm{fin}})$, equipped with $e^{-a_v/\varepsilon_v} || \cdot ||$, where $|| \cdot ||$ is the canonical Hermitian metric, induced by (2.18). In fact, this association induces an isomorphism on divisor classes.

Theorem 2.21 ([**Ara**]) *There exists a canonical group isomorphism*

$$\widehat{\mathrm{Cl}}(X) \xrightarrow{\sim} \widehat{\mathrm{Pic}}(X).$$

As we have already indicated, this allows one to define intersections of (admissible) line bundles, which is an essential part of intersection theory (see the papers of Arakelov and Faltings). Likewise, it allows us to define a new notion of a degree of a (metrized) line bundle. We will return to these notions and deal with specific cases in a slightly more general setting.

2.5.4 Global Néron symbol

Recall the definition of C/K from the beginning of the section. For $v \in M_K$ and $D \in \mathrm{Div}(C)$, we let $D_v := D \otimes_K K_v$. If $D, E \in \mathrm{Div}^0(C)$ are two divisors with disjoint supports, then we define their local Néron symbol as

$$\langle D, E \rangle_v := \langle D_v, E_v \rangle_v$$

and we define their *global Néron symbol* as the sum of the local symbols over all places, i.e.

$$\langle D, E \rangle := \sum_{v \in M_K} \langle D_v, E_v \rangle_v. \tag{2.23}$$

Remark 2.7 The sum (2.23) has only finitely many non-zero terms. Recall that $\mathcal{C}$ has only finitely many places of bad reduction (see 10.1.2 in [**Liu**]). For any place $v \in M_K^0$ of good reduction, the curve C extends to a smooth proper model over $\mathrm{Spec}(O_v)$, for which $\Phi_v(D_v) = 0$.

Remark 2.8 It follows from the previous subsection that the global Néron pairing depends only on linear equivalence classes of the divisors. We can therefore define the bilinear, symmetric *Néron pairing*

$$\langle \cdot, \cdot \rangle \colon \mathrm{Pic}^0(C)(\overline{K}) \times \mathrm{Pic}^0(C)(\overline{K}) \to \mathbf{R}. \tag{2.24}$$

Since $\mathrm{Pic}^0(C) \cong \mathrm{Jac}(C)$ can be equipped with the structure of an abelian variety, the following theorem, although not obvious, is not entirely surprising.

Theorem 2.22 ([**Falt1**], [**Hri**]) *Let Θ be a symmetric theta divisor on $\mathrm{Jac}(C)$ and let $\mathscr{M} = \mathscr{L}(\Theta)$. Let $D, E \in \mathrm{Div}^0(C)$ and let $[D], [E] \in \mathrm{Pic}^0(C)$ denote their linear equivalence classes, respectively. Then*

$$\frac{1}{[K : \mathbf{Q}]} \langle D, E \rangle = -\frac{1}{2} \left(\hat{h}_{\mathscr{M}}([D] + [E]) - \hat{h}_{\mathscr{M}}([D]) - \hat{h}_{\mathscr{M}}([E]) \right).$$

Proof See §5 in [**Lang2**]. □

Remark 2.9 This result has been successfully used in computing and estimating heights of points on Jacobians of curves (see, for example, [**Holm**] and [**Müll**] and references therein).

2.6 The Mordell-Weil group

Let A/K be an abelian variety (over the number field K). The following theorem is a classical result, first proved for elliptic curves over $\mathbf{Q}$ by Mordell and later generalized by Weil to Jacobians over number fields.

Theorem 2.23 (Mordell-Weil) *The group $A(K)$ of K-rational points of A is a finitely generated abelian group.*

Proof See Part C of [**DG**]. □

The proof is based on first proving the so-called Weak Mordell-Weil Theorem, i.e. that for an integer $m \geq 2$, the quotient $A(K)/mA(K)$ is finite, and then applying the following lemma (see Lemma C.0.3 in [**DG**]).

Lemma 2.24 *Let G be an abelian group that is equipped with a quadratic form $q\colon G \to \mathbf{R}$ such that for any $c > 0$, the set $\{x \in G \mid q(x) < c\}$ is finite. Suppose that for some integer $m \geq 2$, the group G/mG is finite and let $\{y_1, \ldots, y_n\} \subseteq G$ be a set of representatives of the cosets in G/mG. Then the group G is finitely generated by the finite set $\{x \in G \mid q(x) < \max_i q(y_i)\}$.*

The lemma is applied to $A(K)$ with the quadratic form $\hat{h}_{\mathscr{L}}$ for some symmetric ample line bundle $\mathscr{L}$. Establishing that $A(K)/mA(K)$ is finite involves constructing a short exact sequence of groups

$$0 \to A(K)/mA(K) \to \mathrm{Sel}^{(m)}(A/K) \to Ш(A/K)[m] \to 0, \tag{2.25}$$

where the group $\mathrm{Sel}^{(m)}(A/K)$ is shown to be finite. We will discuss these groups in more detail in the next section.

It follows from Theorem 2.23 that $A(K) = \mathbf{Z}P_1 \oplus \cdots \oplus \mathbf{Z}P_r \oplus A(K)_{\mathrm{tors}}$ for some non-zero $P_1, \ldots P_r \in A(K)$, where $A(K)_{\mathrm{tors}}$ is a finite abelian group. The integer r is called the *rank* of A over K. It is a relatively easy task to determine $A(K)_{\mathrm{tors}}$ for a particular variety A. For example, if $v \in M_K^0$ is a place of good reduction and $m \geq 1$ is an integer that is not divisible by $\mathrm{char}(k(v))$, then the reduction morphism $A[m](K) \to A(k(v))$ is injective (see Theorem C.1.4 in [**DG**]). Then choosing two places v, w of good reduction such that the characteristics of the residue fields $k(v), k(w)$ are coprime, yields an embedding

$$A(K)_{\mathrm{tors}} \hookrightarrow A(k(v)) \times A(k(w)).$$

In particular, the torsion subgroup of $A(K)$ is finite and it can be determined. There are also general results for elliptic curves (theorems of Mazur, Kamienny, and Merel; see Theorem F.4.1.1 in [**DG**]). It is conjectured[2] that for all abelian varieties of dimension $g \geq 1$ over K, there exists a constant $c = c(g, K)$ such that $\#A(K)_{\mathrm{tors}} \leq c$. However, computing the rank of $A(K)$ or a set of generators is considerably more difficult, to say the least. Only finitely many cases are known, over $\mathbf{Q}$ and some number fields, with results achieved using algorithms based on modularity (see Cremona [**Cre**] and the [**LMFDB**] database).

If one could a priori bound the projective height of a set of generators, one could obtain the generators by an exhaustive search of points of bounded height. In view of Lemma 2.24, one could find a set of generators for the group $A(K)/A(K)_{\mathrm{tors}}$ if one could find a set of representatives for cosets of $A(K)/mA(K)$ for some $m \geq 2$. However, there is currently no known algorithm that accomplishes the latter. We sketch briefly the only known approach.

Let $\mathscr{L}$ be a symmetric ample line bundle on A. Then $A(K)$ is equipped with a positive definite quadratic form $\hat{h} = \hat{h}_{\mathscr{L}} \colon A(K) \to \mathbf{R}$, and a corresponding bilinear symmetric pairing $\langle \cdot, \cdot \rangle \colon A(K) \times A(K) \to \mathbf{R}$ (recall (2.15)). Tensoring with $\mathbf{R}$, we obtain an induced pairing which makes $A(K) \otimes \mathbf{R} \cong \mathbf{R}^r$ a euclidean space. For $P \in A(K) \otimes \mathbf{R}$, let $|P| := \sqrt{\langle P, P \rangle}$. We now have a lattice in a euclidean space and we can use the following classical result of Hermite.

Theorem 2.25 *Let V be a real vector space of dimension r, equipped with a euclidean norm $|\cdot|$, and let $\Lambda \subset V$ be a lattice. Let* $\mathrm{Vol}(\Lambda)$ *denote the volume of a fundamental domain of Λ. Then there exists a basis $u_1, \ldots, u_r$ of Λ such that*

$$\mathrm{Vol}(\Lambda) \leq |u_1| \cdots |u_r| \leq \left(\frac{4}{3}\right)^{r(r-1)/2} \mathrm{Vol}(\Lambda), \tag{2.26}$$

where $|u_1| \leq |u_2| \leq \cdots \leq |u_r|$ with $|u_1| = \min\limits_{x \in \Lambda, x \neq 0} |x|$.

Proof The first inequality is a classical result in linear algebra, known as Hadamard's inequality. For the proof of the second inequality, see Theorem 7.7 and its corollary in [**Lang1**]. □

[2] This is known as the (Weak) Torsion Conjecture.

If $\{P_1, \ldots, P_r\}$ is a $\mathbf{Z}$-basis of $A(K)/A(K)_{\text{tors}}$, the real number

$$\text{Reg}(A/K) := |\det(\langle P_i, P_j \rangle)|, \quad 1 \leq i, j \leq r$$

is called the *regulator of A over K*. In view of the preceding theorem, there exists a constant $c > 0$ and a basis $P_1, \ldots, P_r$ for $A(K)/A(K)_{\text{tors}}$ such that

$$\text{Reg}(A/K) \leq \hat{h}(P_1) \cdots \hat{h}(P_r) \leq c^{r^2} \text{Reg}(A/K),$$

where $P_1 \in A(K)$ is a non-torsion point of minimal height and the P_i are indexed so that $\hat{h}(P_1) \leq \cdots \leq \hat{h}(P_r)$. It therefore follows that

$$\hat{h}(P_r) \leq c^{r^2} \frac{\text{Reg}(A/K)}{\hat{h}(P_1)^{r-1}}.$$

Therefore, an upper bound for the height of the P_i can be obtained by first obtaining a lower bound for the minimal height of non-torsion points and an upper bound for the regulator. There are some results known about the former, but the latter is conjectural; it is based on the famous Birch and Swinnerton-Dyer Conjecture, that links the regulator (and the size of the Tate-Šafarevič group) to coefficients in the expansion of a certain L-series.

Remark 2.10 As we mentioned in Chapter 1, discussing a specific case, if $\mathscr{L}$ is an ample line bundle on an abelian variety A, we can associate to it a polarization

$$\lambda_{\mathscr{L}} \colon A \to A^\vee, \quad P \mapsto t_P^* \mathscr{L} \otimes \mathscr{L}^{-1}.$$

If $(A, \lambda_{\mathscr{L}})$ is an abelian variety with a fixed polarization $\lambda_{\mathscr{L}}$, we sometimes omit the $\mathscr{L}$ from the notation and write $\hat{h}$ for $\hat{h}_{\mathscr{L}}$. However, if (A, λ) is a principally polarized abelian variety, there is what may be called a canonical way of choosing a line bundle for the purpose of introducing heights, the regulator, etc, namely via the *Poincaré line bundle* $\mathcal{P}$ on $A \times A^\vee$ (see Remark 9.3 in [**Miln1**]). Then all heights on A can be obtained from the canonical height $\hat{h}_{\mathcal{P}}$ on $A \times A^\vee$. In particular, if $\mathscr{L}$ is symmetric, then

$$2\hat{h}_{\mathscr{L}}(P) = \hat{h}_{\mathcal{P}}(P, \lambda_{\mathscr{L}}(P)).$$

In general we need not have a principal polarization on A. However, a trick of Zarhin (see Remark 16.12 in loc. cit.) guarantees that $(A \times A^\vee)^4$ is principally polarized.

2.7 The Selmer group and the Tate-Šafarevič group

In this section, we give only a brief overview of the Galois cohomology definitions required to introduce these groups and we sketch a proof of the finiteness of the Selmer group. For the full proof of the Mordell-Weil theorem, see Part C of [**DG**]. A simple introduction to group cohomology can be found in Appendix B of [**AEC**] and more details can be found in [**At-Wa**].

Let G be a profinite group acting on an abelian group M, with action denoted by $\sigma\colon x \mapsto x^\sigma$ for $\sigma \in G$ and $x \in M$. We call M a *G-module* if

$$x^{\mathbb{1}} = x, \quad (x+y)^\sigma = x^\sigma + y^\sigma, \quad (x^\sigma)^\tau = x^{\sigma\tau}$$

for every $x, y \in M$ and $\sigma, \tau \in G$. A homomorphism of G-modules is a group homomorphism that commutes with the action of G.

The *0-th cohomology group* associated to the action of G on M is the subgroup of G-invariant elements of M, that is

$$H^0(G, M) := \{x \in M \mid x^\sigma = x \text{ for all } \sigma \in G\}.$$

A map $\phi\colon G \to M$ is called a *cocycle* if it satisfies

$$\phi(\sigma\tau) = \phi(\sigma)^\tau + \phi(\tau) \quad \text{for all } \sigma, \tau \in G.$$

Note how this differs from a homomorphism (unless the action of G is trivial). We define the sum of two cocycles ϕ_1, ϕ_2 to be the map given by

$$(\phi_1 + \phi_2)(\sigma) = \phi_1(\sigma) + \phi_2(\sigma),$$

which is also a cocycle since M is abelian. Thus cocycles form a group, denoted by $Z^1(G, M)$.

A map $\delta\colon G \to M$ is called a *coboundary* if it satisfies

$$\delta(\sigma) = x^\sigma - x \quad \text{for some } x \in M.$$

Every coboundary is a cocycle and the sum of two coboundaries is again a coboundary so they form a subgroup $B^1(G, M) \subset Z^1(G, M)$. The *first cohomology group* associated to the action of G on M is then defined as the quotient

$$H^1(G, M) := Z^1(G, M)/B^1(G, M).$$

Remark 2.11 The first cohomology group is functorial. A continuous homomorphism $f\colon G \to G'$ induces a homomorphism $H^1(G', M) \to H^1(G, M)$ via $[\phi] \mapsto [\phi \circ f]$. Likewise, if $\mathfrak{f}\colon M \to M'$ is a G-homomorphism, it induces a homomorphism $H^1(G, M) \to H^1(G, M')$ via $[\phi] \mapsto [\mathfrak{f} \circ \phi]$.

The case of particular interest to us is that of absolute Galois action on a subgroup M of an abelian variety, with the additional condition that all cocycles are continuous maps if M is equipped with the discrete topology.

Let $m \geq 2$ be an integer, let $G_K := \mathrm{Gal}(\overline{K}/K)$, and let A/K be an abelian variety. Let $x \in A(K)$ be a K-rational point and let $y \in A(\overline{K})$ be any point such that $[m]y = x$. The map

$$\kappa_y\colon G \to A[m], \quad \sigma \mapsto y^\sigma - y$$

is a cocycle in $H^1(G_K, A[m])$, satisfying $\kappa_y(\sigma\tau) = \kappa_y(\sigma)^\tau + \kappa_y(\tau)$. If $z \in A(\overline{K})$ is also a point such that $[m]z = x$, then let $w = z - y$. For every $\sigma \in G_K$ we have

$$\kappa_y(\sigma) - \kappa_z(\sigma) = (z^\sigma - z) - (y^\sigma - y) = (z - y)^\sigma - (z - y) = w^\sigma - w.$$

Noting that $w \in A[m]$, we conclude that $\kappa_y - \kappa_z$ is a coboundary. It follows that we can associate a well-defined class in $H^1(G_K, A[m])$ to every $x \in A(K)$.

Remark 2.12 If $A[m]$ is fully K-rational, then the map defined above gives rise to what is called the *Kummer pairing*

$$\kappa\colon G_K \times A(K) \to A[m], \quad (\sigma, x) \mapsto y^\sigma - y,$$

where $y \in A(\overline{K})$ is such that $[m]y = x$. It is analogous to the classical Kummer pairing for number fields (cf. [**ANT1**]), namely

$$\kappa\colon G_K \times K^\times \to \mu_m, \quad (\sigma, x) \mapsto \sigma(y)/y,$$

where $y = \sqrt[m]{x}$ and a primitive m-th root of unity ζ_m is assumed to be in K.

More generally, we have the following theorem for any isogeny.

Theorem 2.26 *Let $\varphi\colon A \to B$ be an isogeny of abelian varieties over K. Then the short exact sequence*

$$0 \longrightarrow \mathrm{Ker}(\varphi) \hookrightarrow A(\overline{K}) \xrightarrow{\varphi} B(\overline{K}) \longrightarrow 0$$

induces a long exact sequence

$$0 \longrightarrow \mathrm{Ker}(\varphi)(K) \hookrightarrow A(K) \xrightarrow{\varphi} B(K) \xrightarrow{\delta} H^1(G_K, \mathrm{Ker}(\varphi)) \longrightarrow H^1(G_K, A(\overline{K})) \xrightarrow{\varphi_\circ} H^1(G_K, B(\overline{K})),$$

where the homomorphism $\delta\colon B(K) \to H^1(G_K, \mathrm{Ker}(\varphi))$ *is defined as follows. Let* $x \in B(K)$ *and let* $y \in A(\overline{K})$ *be such that* $\varphi(y) = x$*. Then the cocycle* $\delta(x)$ *is defined as*

$$\delta(x)\colon \sigma \mapsto y^\sigma - y.$$

This long exact sequence induces the short exact sequence

$$0 \to B(K)/\varphi(A(K)) \xrightarrow{\delta} H^1(G_K, \mathrm{Ker}(\varphi)) \longrightarrow H^1(G_K, A(\overline{K}))[\varphi] \to 0, \tag{2.27}$$

where $H^1(G_K, A(\overline{K}))[\varphi] := \mathrm{Ker}\left(H^1(G_K, A(\overline{K})) \xrightarrow{\varphi_\circ} H^1(G_K, B(\overline{K}))\right)$.

Now let $v \in M_K$ be a place of K and let $G_v := \mathrm{Gal}(\overline{K}_v/K_v)$. We can view G_v as a subgroup of G_K in a natural way and therefore we have a natural restriction homomorphism $H^1(G_K, \cdot) \to H^1(G_v, \cdot)$. This induces a local short exact sequence, analogous to (2.27), and we have the following commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & B(K)/\varphi(A(K)) & \xrightarrow{\delta} & H^1(G_K, \mathrm{Ker}(\varphi)) & \longrightarrow & H^1(G_K, A(\overline{K}))[\varphi] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & B(K_v)/\varphi(A(K_v)) & \xrightarrow{\delta_v} & H^1(G_v, \mathrm{Ker}(\varphi)) & \longrightarrow & H^1(G_v, A(\overline{K}_v))[\varphi] & \longrightarrow & 0
\end{array}$$

Finally, we are able to define the two groups in the subsection title.

Definition 2.9 Let $\varphi\colon A \to B$ be an isogeny of abelian varieties over K. Then the *Selmer group of* A*, with respect to* φ, is the group

$$\mathrm{Sel}^{(\varphi)}(A/K) := \bigcap_{v \in M_K} \mathrm{Ker}\left(H^1(G_K, \mathrm{Ker}(\varphi)) \to H^1(G_v, A(\overline{K}_v))[\varphi]\right),$$

whereas the *Tate-Šafarevič group of* A is the group defined as

$$Ш(A/K) := \bigcap_{v \in M_K} \mathrm{Ker}\left(H^1(G_K, A(\overline{K})) \to H^1(G_v, A(\overline{K}_v))\right).$$

From the preceding definition and theorem one deduces the following short exact sequence (recall (2.25)):

$$0 \to B(K)/\varphi(A(K)) \to \mathrm{Sel}^{(\varphi)}(A/K) \to Ш(A/K)[\varphi] \to 0. \tag{2.28}$$

Now the finiteness of $\mathrm{Sel}^{(\varphi)}(A/K)$ implies the finiteness of $B(K)/\varphi(A(K))$ and $Ш(A/K)[\varphi]$, which in turn implies the Mordell-Weil theorem. That the Selmer group is finite follows from the fact that it can be embedded in a finite subgroup of $H^1(G_K, \mathrm{Ker}(\varphi))$ (which itself is not finite). Before stating the theorem, we need some definitions.

We recall some facts from number theory. Details can be found in §9 of Chapters I and II in [**ANT2**], for example. Let L/K be a finite Galois extension of number fields with Galois group $G = \mathrm{Gal}(L/K)$, let $\mathfrak{p}$ be a prime of O_K, and let $\mathfrak{q}$ be a prime of O_L that lies above $\mathfrak{p}$. We associate to $\mathfrak{q}$ the subgroup

$$D_\mathfrak{q} := \{\sigma \in G \mid \sigma(\mathfrak{q}) = \mathfrak{q}\},$$

called the *decomposition group of* $\mathfrak{q}$. Note that G acts transitively on primes of O_L that extend $\mathfrak{p}$. If $\mathfrak{q}'$ is another prime dividing $\mathfrak{p}$, then we have $\mathfrak{q}' = \sigma(\mathfrak{q})$ for some $\sigma \in G$ and therefore $D_{\mathfrak{q}'} = \sigma D_\mathfrak{q} \sigma^{-1}$. In other words, all decomposition groups associated to primes above $\mathfrak{p}$ are conjugates (in G). Since every automorphism $\sigma \in D_\mathfrak{q}$ fixes $\mathfrak{q}$, it descends to an automorphism of the residue field $l_\mathfrak{q} := O_L/\mathfrak{q}$ that fixes $k := O_K/\mathfrak{p}$. We therefore have a surjective homomorphism

$$D_\mathfrak{q} \to \mathrm{Gal}(l_\mathfrak{q}/k),$$

whose kernel $I_\mathfrak{q}$ is called the *inertia group of* $\mathfrak{q}$. In fact, the inertia group $I_\mathfrak{q}$ is normal in $D_\mathfrak{q}$ and we have the following exact sequence

$$0 \longrightarrow I_\mathfrak{q} \longrightarrow D_\mathfrak{q} \longrightarrow \mathrm{Gal}(l_\mathfrak{q}/k) \longrightarrow 0.$$

Let $e_\mathfrak{q}$ denote the ramification index of $\mathfrak{q}$ and let $f_\mathfrak{q} = [l_\mathfrak{q} : k]$ denote the residue degree. We therefore have a group $D_\mathfrak{q}$ of order $e_\mathfrak{q} f_\mathfrak{q}$ and a normal subgroup $I_\mathfrak{q} \subset D_\mathfrak{q}$ of order $e_\mathfrak{q}$, with the quotient $D_\mathfrak{q}/I_\mathfrak{q}$ being a cyclic group of order $f_\mathfrak{q}$. By a slight abuse of language and notation, we set $D_\mathfrak{p} := D_\mathfrak{q}$ and $I_\mathfrak{p} := I_\mathfrak{q}$ and refer to them as the decomposition group of $\mathfrak{p}$ and the inertia group of $\mathfrak{p}$, with the understanding that the two groups are defined up to conjugation.

If L/K is an infinite Galois extension, then the inertia group of a prime ideal $\mathfrak{p} \subset O_K$ is taken to be the inverse limit of the inertia groups taken

over K', for every finite Galois subextension $L/K'/K$. An equivalent, valuative definition states that for a Galois extension L/K and a place $v \in M_K$, the inertia group I_v of v (with respect to L) is the subgroup that consists precisely of those $\sigma \in \mathrm{Gal}(L/K)$ for which the implication

$$v(x) \geq 0 \Rightarrow w(\sigma(x) - x) > 0$$

holds for all $x \in L$ and all $w|v$.

Definition 2.10 Let M be a G_K-module. A class $\phi \in H^1(G_K, M)$ is called *unramified at* $v \in M_K$ if its restriction to $H^1(I_v, M)$ is trivial.

Note that this definition is independent of the choice of the conjugate of I_v. We are now ready to state the theorems that establish the finiteness of the Selmer group.

Theorem 2.27 *Let M be a G_K-module, let $S \subset M_K$ be a finite set of places, and let $H^1_S(G_K, M) \subset H^1(G_K, M)$ denote the subgroup of cohomology classes that are unramified at places outside S. Then the group $H^1_S(G_K, M)$ is finite.*

Theorem 2.28 *Let $\varphi\colon A \to B$ be an isogeny of abelian varieties over K. Let S be a set of places that includes:*

- *the infinite places $v \in M_K^\infty$,*
- *the places of bad reduction of A and B (these are the same places, in fact),*
- *the places that divide* $\deg(\varphi)$.

Then $\mathrm{Sel}^{(\varphi)}(A/K)$ *is a subgroup of* $H^1_S(G_K, \mathrm{Ker}(\varphi))$.

The proof is based on the functorial properties of H^1 and a classical result (Hermite-Minkowski) about the finiteness of the number of number field extensions of bounded degree, unramified outside a finite set of places. See Theorem C.4.2 in [**DG**] for details.

The Selmer group and the Tate-Šafarevič group have an interesting geometric interpretation. Namely, the elements of $H^1(G_K, A(\overline{K}))$ correspond to principal homogeneous spaces of A (see [**La-Ta**]). Recall that a *principal homogeneous space of* A is a K-variety X on which A acts[3] freely and transitively.

[3] Since A is abelian, we make no distinction between left-action and right-action.

More precisely, the variety X is equipped with a K-morphism $X \times A \to X$, denoted by $(x, a) \mapsto x \cdot a$, such that for all $x \in X$ and all $a, b \in A$, we have:

(1) $x \cdot 0_A = x$;

(2) $x \cdot (a + b) = (x \cdot a) \cdot b$;

(3) $a \mapsto x \cdot a$ defines a $K(x)$-isomorphism $A \xrightarrow{\sim} X$.

In particular, the variety X is a *twist* of A, i.e. a variety that is isomorphic to A over $\overline{K}$. However, we do not have a marked identity point for X. One can show (see Chapter X, §3 in [**AEC**]) that there is a bijection (a group isomorphism, in fact) between $H^1(G_K, A(\overline{K}))$ and the set of principal homogeneous spaces of A, modulo K-isomorphisms compatible with the action of A. The latter is usually denoted by $WC(A/K)$ and called the *Weil-Châtelet* group[4]. The class of X in $WC(A/K)$ is trivial if and only if X contains a K-rational point. Note that A is in the trivial class, acting on itself via translation. Therefore the elements of $\mathrm{Sel}^{(\varphi)}(A/K)$ correspond to principal homogeneous spaces that have K_v-rational points for every $v \in M_K$. Since this definition is entirely local, the Selmer group can be computed (using Hensel's Lemma and estimates for number of points of abelian varieties over finite fields). Likewise, the (non-trivial) elements of $Ш(A/K)$ correspond to principal homogeneous spaces that have K_v-rational points, but do not have any K-rational points, i.e. they fail the Hasse principle. In contrast, there is no known algorithm that computes the Tate-Šafarevič group. We have seen above that $Ш(A/K)[n]$ is finite for any $n \in \mathbf{N}$. It is conjectured that $Ш(A/K)$ itself is finite, but there are very few proven cases.

2.8 Néron models and the Faltings height

We mentioned regular models of curves of positive genus in Section 2.5, whose explicit construction is given in Chapter 9 of [**Liu**]. No analogous construction is known for varieties of higher dimensions. However, abelian varieties admit a different kind of model, with very useful properties.

[4] Historically, the group $WC(A/K)$ was described before the group $H^1(G_K, A(\overline{K}))$.

Definition 2.11 Let S be a one-dimensional Dedekind scheme with function field $K = K(S)$ and let V be a variety over K. A *Néron model of V over S* is a smooth, separated scheme $\mathcal{V} \to S$ of finite type, whose generic fibre is isomorphic to V, satisfying the following universal property – for every smooth scheme $\mathcal{X} \to S$ with generic fibre isomorphic to X, a morphism $f\colon X \to V$ extends to a morphism of S-schemes $\mathcal{X} \to \mathcal{V}$.

The universal property guarantees that if a Néron model exists, it is unique up to unique isomorphism. Existence of Néron models for abelian varieties was first proved by Néron in [**Nér**]. For an overview of the subject, see [**Art**]. A more complete treatment can be found in [**B-L-R**]. The relation between the minimal regular model and the Néron model for curves of positive genus can be found in [**Li-To**].

Let A/K be an abelian variety (over the number field K) of dimension g and let $\mathcal{A}$ be its Néron model (over $S = \mathrm{Spec}(O_K)$). Then the addition morphism $A \times A \to A$ lifts to a morphism $\mathcal{A} \times \mathcal{A} \to \mathcal{A}$, making $\mathcal{A}$ an S-group scheme. Every point $P \in A(K)$, seen as a K-rational morphism $\mathrm{Spec}(K) \to A$, lifts to a section $S \to \mathcal{A}$.

As in Subsection 2.5.2, the line bundle $\Omega^g_{A(\overline{K}_v)}$ of holomorphic g-forms is equipped with a hermitian inner product with a corresponding hermitian metric

$$||\eta||_v^2 = \frac{i^{g^2}}{(2\pi)^{2g}} \int_{A(\overline{K}_v)} \eta \wedge \bar{\eta}. \tag{2.29}$$

Remark 2.13 The choice of normalization in (2.29) is not canonical and differs from other choices that appear in literature. Caution is advised in this regard.

This allows for an analogous construction of Arakelov divisors and metrized line bundles. Now let $\mathscr{L}$ be a metrized line bundle on $S = \mathrm{Spec}(\mathcal{O}_K)$ and let $s \in \mathscr{L}$ be a non-zero section. One defines the *Arakelov degree of $\mathscr{L}$* as

$$\widehat{\deg}(\mathscr{L}) := \log \#(\mathscr{L}/O_K \cdot s) - \sum_{v \in M_K^\infty} \varepsilon_v \log ||s||_v.$$

The product formula guarantees that the definition does not depend on the choice of s.

Let $\epsilon\colon S \to \mathcal{A}$ denote the zero-section, i.e. the section corresponding to the identity element $0_A \in A(K)$. Pulling back, via ϵ, the g-forms on $\mathcal{A}$ and the canonical metrics at the archimedean places, we obtain a metrized line bundle $\omega_A := \epsilon^*\Omega^g_{\mathcal{A}}$ on S. Now we can define the *Faltings height of* A as

$$h_{\mathrm{Falt}}(A/K) := \frac{1}{[K:\mathbf{Q}]}\widehat{\deg}(\omega_A).$$

It was introduced by Faltings over number fields (see [**Falt2**]), whereas the function field case had been previously defined by Parshin. We list some of the properties of h_{Falt} below.

(1) If L/K is a finite field extension, then $h_{\mathrm{Falt}}(A/L) \leq h_{\mathrm{Falt}}(A/K)$. If A/K is semi-stable, then $h_{\mathrm{Falt}}(A/L) = h_{\mathrm{Falt}}(A/K)$. We can therefore define the *stable Faltings height*, denoted by $h_{\mathrm{Falt}}(A/\overline{K})$, by first passing to a finite extension over which A is semi-stable. The existence of such an extension is the subject of Grothendieck's Semi-stable Reduction Theorem for abelian varieties (see [**Abb**]).

(2) $h_{\mathrm{Falt}}(A \times B/K) = h_{\mathrm{Falt}}(A/K) + h_{\mathrm{Falt}}(B/K)$

(3) $h_{\mathrm{Falt}}(A^\vee/K) = h_{\mathrm{Falt}}(A/K)$, where $A^\vee$ denotes the dual of A (a result of Raynaud)

(4) $h_{\mathrm{Falt}}(A/K) \geq 0$ (a result of Bost, see Corollaire 8.4 in [**Ga-Ré**])

(5) For every $g \in \mathbf{N}$ and $C \in \mathbf{R}_{>0}$, the set of isomorphism classes of principally polarized abelian varieties A such that $h_{\mathrm{Falt}}(A/K) < C$ and $\dim A = g$ is finite (see Theorem 1 in [**Falt2**]).

(6) If $\varphi\colon A \to B$ is an isogeny of degree $\deg(\varphi) = m$, then

$$|h_{\mathrm{Falt}}(A/K) - h_{\mathrm{Falt}}(B/K)| \leq \frac{1}{2}\log m \tag{2.30}$$

(see Corollaire 2.1.4 in [**Ray**]).

The Faltings height can be seen as an intrinsic measure of the *arithmetic complexity* of the variety. For Jacobians of dimension $g = 1, 2$, there are explicit formulas. Let E/K be an elliptic curve with minimal discriminant $\Delta_{E/K}$. For each archimedean place v, let $\tau_v \in \mathbf{H}$ be the element of the fundamental domain such that

$$E(\overline{K}_v) \cong \mathbf{C}/(\mathbf{Z} + \tau_v\mathbf{Z}).$$

Then we have (see Proposition 1.1 in [**Sil2**])

$$h_{\mathrm{Falt}}(E/K) = \frac{1}{12[K:\mathbf{Q}]}\left(\log N_{K/\mathbf{Q}}(\Delta_{E/K}) - \sum_{v\in M_K^\infty} \varepsilon_v \log\left(|\Delta(\tau_v)|(\operatorname{Im}\tau_v)^6\right)\right) - \frac{\log 2}{2}. \tag{2.31}$$

Here $\operatorname{Im} z := (z-\bar{z})/2i$ is the imaginary part of z and $N_{K/\mathbf{Q}}$ is the ideal norm, while

$$\Delta(\tau) := q_\tau \prod_{n=1}^{\infty}(1-q_\tau^n)^{24},$$

with $q_\tau := e^{2\pi i\tau}$, is a modular form of weight 12 for $\mathrm{SL}_2(\mathbf{Z})$ (see [**AEC**]).

For $A = \mathrm{Jac}(C)$, where C is a curve of genus two, there is a similar formula (see [**Ueno**]).

2.9 The Lang-Silverman conjecture

With this background in mind, we are interested in implications of the form

$$\hat{h}(P) > 0 \Rightarrow \hat{h}(P) > c_A$$

for some $c_A > 0$, where $P \in A(K)$. In other words, given that $\hat{h}(P) > 0$ for every non-torsion point $P \in A(K)$, what can be said about a positive lower bound and how it changes with A? A conjecture by Lang was first formulated in [**Lang3**] (p. 92) in the following form:

"*It seems a reasonable guess that uniformly for all such models of elliptic curves over* $\mathbf{Z}$*, one has*

$$\hat{h}(P_1) \gg \log|\,\Delta_E\,|."$$

Here P_1 is a point that realizes the minimum of $\hat{h}$ on $A(K)\backslash A(K)_{\mathrm{tors}}$. The conjecture was given a more general form by Silverman. Recall that the j-invariant of an elliptic curve E such that $E(\overline{K}_v) \cong \mathbf{C}/(\mathbf{Z}+\tau\mathbf{Z})$ is given by a Laurent series

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots,$$

where $q := e^{2\pi i\tau}$. Thus $|j(\tau)| \gg\ll |q^{-1}|$ and $\log|j(\tau)| \gg\ll 2\pi\operatorname{Im}\tau$, and from (2.31) we have in particular

$$h_{\mathrm{Falt}}(E/K) \gg\ll \max\{h(j(E)), \log N_{K/\mathbf{Q}}(\Delta_E)\}.$$

Conjecture 2.29 (Lang-Silverman) *Let K be a number field and let A be an abelian variety over K, of dimension g. Let $\mathscr{L}$ be an ample symmetric line bundle on A. Then there exists a constant $C(g,K) > 0$ such that for every $P \in A(K)$ for which $\mathbf{Z} \cdot P$ is Zariski-dense in A, we have*

$$\hat{h}_{\mathscr{L}}(P) \geq C(g,K) \cdot h_{\mathrm{Falt}}(A/K). \tag{2.32}$$

In a manner of speaking, the conjecture states that, for a fixed dimension and a fixed number field, one can uniformly bound the arithmetic complexity of a non-torsion point in terms of the arithmetic complexity of the variety. No proof is currently known for any dimension. Some partial results are known and we will briefly review some of them.

Remark 2.14 If A is an abelian variety, we can embed $A \hookrightarrow A \times B$, for some abelian variety B, via $P \mapsto (P, 0_B)$. Since $h_{\mathrm{Falt}}(A \times B) = h_{\mathrm{Falt}}(A) + h_{\mathrm{Falt}}(B)$ and $\hat{h}(P) = \hat{h}((P, 0_B))$, the assumption $\overline{\mathbf{Z} \cdot P} = A$ is justified. Likewise, if $P = [n]Q$, we have $\hat{h}(Q) = \hat{h}(P)/n^2$, which approaches 0 as $n \to \infty$, so the constant C in (2.32) must depend on the ground field. There are also examples that establish that C must depend on the dimension (viz $\mathrm{Jac}(X_0(N))$, see [**Paz1**]).

Remark 2.15 If we fix the dimension g and consider only a finite set of (isomorphism classes of) abelian varieties, then (2.32) trivially holds on this set for some $C(g,K)$. Whether or not the conjecture is true for all abelian varieties of dimension g, it is certainly of interest to investigate it for infinite families.

Theorem 2.30 *The Lang-Silverman Conjecture holds for elliptic curves E/K whose j-invariant is integral.*

Proof See [**Sil1**]. □

Let E/K be an elliptic curve. We let $\Delta_{E/K}$ and $\mathfrak{F}_{E/K}$ denote its minimal discriminant and its conductor, respectively. These are ideals of O_K, obtained as products of primes of bad reduction of E (with some exponents). See [**AEC**] for the exact definitions. We define the *Szpiro ratio* or the *Szpiro quotient* of E/K to be

$$\sigma_{E/K} := \frac{\log N_{K/\mathbf{Q}}(\Delta_{E/K})}{\log N_{K/\mathbf{Q}}(\mathfrak{F}_{E/K})}.$$

Conjecture 2.31 (Szpiro) *For every $\varepsilon > 0$, there exists a constant $C(\varepsilon, K)$ such that for every elliptic curve E/K, one has*

$$\log N_{K/\mathbf{Q}}(\Delta_{E/K}) \leq (6+\varepsilon)\log N_{K/\mathbf{Q}}(\mathfrak{F}_{E/K}) + C(\varepsilon, K).$$

This conjecture is roughly equivalent to the famous *abc*-conjecture over $\mathbf{Q}$ (Conjecture 2.32); it is implied by it and it implies a weaker version of it, with a modified exponent (see [**Szp**] and references therein).

Recall that for $n \in \mathbf{Z}^\times$ one defines the *radical* of n as

$$\mathrm{rad}(n) := \prod_{p|n} p\,.$$

Conjecture 2.32 (Masser-Oesterlé [**Oes**]) *For every $\varepsilon > 0$ there exists a constant $C_\varepsilon > 0$ such that if $a, b, c \in \mathbf{Z}$ are coprime and $a+b+c = 0$, then*

$$\max\{|a|, |b|, |c|\} \leq C_\varepsilon(\mathrm{rad}(abc))^{1+\varepsilon}.$$

Hindry and Silverman obtained the following result for Conjecture 2.29.

Theorem 2.33 (Hindry-Silverman [**Hi-Si**]) *Let K be a number field of degree d and let E be an elliptic curve over K of Szpiro ratio at most σ. There exists a constant $C = C(d, \sigma) > 0$ such that if $P \in E(K) \setminus E(K)_{\mathrm{tors}}$, then*

$$\hat{h}(P) \geq C \cdot h_{\mathrm{Falt}}(E/K).$$

The constant they obtain depends exponentially on d and $\sigma_{E/K}$, but improvements have been found. For example, one finds in Petsche [**Pet**] that for all $P \in E(K) \setminus E(K)_{\mathrm{tors}}$, the following holds:

$$\hat{h}(P) \geq \left(10^{15} d^3 \sigma_{E/K}^6 \log(104613 \cdot d \cdot \sigma_{E/K})\right)^{-1} \cdot \log N_{K/\mathbf{Q}}(\Delta_E).$$

Therefore it follows that the Szpiro Conjecture implies the Lang-Silverman conjecture for elliptic curves. In fact, Silverman showed that a weaker conjecture (the "prime-depleted" version of the Szpiro Conjecture) also implies the Lang-Silverman Conjecture (see [**Sil3**]).

Remark 2.16 These results imply that the Lang-Silverman conjecture holds for elliptic curves whose j-invariants have a fixed set of primes in the denominator. In particular, Theorem 2.33 implies Theorem 2.30.

A result by David [**Dav**] establishes the conjecture for abelian varieties A for which $h := \max\{1, h_{\mathrm{Falt}}(A/K)\}$ satisfies $h \ll \max_{i,j} |\mathrm{Im}\, \tau_{ij}|$, where τ denotes the element $\tau_v \in \mathfrak{H}_g$ of the fundamental domain that corresponds to $A \otimes_v \bar{k}_v$, for all $v \in M_K^\infty$. That this applies to infinitely many abelian varieties of dimension g follows from the work of Masser [**Mas2**]. We remark here that the opposite relation $h \gg \max_{i,j} |\mathrm{Im}\, \tau_{ij}|$ is a known result of Masser [**Mas1**], known as the *Matrix Lemma* (see also Autissier [**Aut**]).

Another result, for principally polarized abelian surfaces, is due to Pazuki. We introduce some notation first. For $v \in M_K$ let

$$\tau_v = \begin{bmatrix} \tau_{1,v} & \tau_{12,v} \\ \tau_{12,v} & \tau_{2,v} \end{bmatrix} \in \mathfrak{H}_2$$

be the element of the fundamental domain such that

$$A(\overline{K}_v) \cong \mathbf{C}^2/(\mathbf{Z}^2 + \tau_v \cdot \mathbf{Z}^2).$$

Then the *archimedean trace* of A is defined as

$$\mathrm{Tr}_\infty(A) := \sum_{v \in M_K^\infty} \varepsilon_v \,\mathrm{Tr}(\mathrm{Im}\, \tau_v),$$

and the *archimedean simplicity* of A is defined as

$$s_\infty(A) := \prod_{v \in M_K^\infty} ||\tau_{12,v}||_v.$$

One has $s_\infty(A) = 0$ if and only if $A \cong E_1 \times E_2$ as principally polarized abelian surfaces, where E_i are elliptic curves. Recall from Theorem 1.18 that therefore $s_\infty(A) \neq 0$ if and only if $A \cong \mathrm{Jac}(C)$, where C is a smooth curve of genus two.

Theorem 2.34 ([**Paz2**] Théorème 1.8) *Let K be a number field of degree d, let C/K be a curve of genus two, given by an integral model $y^2 = f(x)$, and let $A = \mathrm{Jac}(C)$, principally polarized by Θ. Then there exist positive real constants $c_1(d)$ and $c_2(d)$ such that for every $P \in A(K)$, one of the following two holds:*

(1) $[n]P = 0_A$ *for some* $n \leq c_1(d)$;

(2) $\hat{h}_{2\Theta}(P) \geq c_2(d) \cdot \left(\mathrm{Tr}_\infty(A) - \frac{5}{3} \log \frac{N_{K/\mathbf{Q}}(2^8 \mathrm{Disc}(f))}{s_\infty(A)} \right)$.

Corollary 2.35 *The Lang-Silverman conjecture holds for principally polarized abelian surfaces $A \cong \mathrm{Jac}(C)$ that satisfy $\mathrm{Tr}_\infty(A) > \frac{5}{3}\log\frac{N_{K/\mathbf{Q}}(D)}{s_\infty(A)}$.*

Let E/K be an elliptic curve such that for $v \in M_K^\infty$ and the appropriate τ_v in the fundamental domain of $\mathbf{H}$, we have $E(\overline{K}_v) \cong \mathbf{C}/(\mathbf{Z}+\tau_v\mathbf{Z})$. We similarly define the archimedean trace

$$\mathrm{Tr}_\infty(E) := \sum_{v\in M_K^\infty} \varepsilon_v \mathrm{Im}\,\tau_v.$$

Theorem 2.36 ([**Paz2**] Théorème 7.1) *Let K be a number field of degree d. Then there exists a constant $c = c(d) > 0$ such that for every elliptic curve E over K and every $P \in E(K)\setminus E(K)_{\mathrm{tors}}$ one has*

$$\hat{h}(P) \geq c(d)\left(\mathrm{Tr}_\infty(E) - \frac{1}{7}\log N_{K/\mathbf{Q}}(\Delta_E)\right).$$

Combining this result with Theorem 2.33, we obtain the following.

Corollary 2.37 *The Lang-Silverman conjecture holds for principally polarized abelian surfaces $A \cong E_1 \times E_2$ such that at least one of the following holds for $i = 1, 2$:*

(1) $\mathrm{Tr}_\infty(E_i) > \frac{1}{7}\log N_{K/\mathbf{Q}}(\Delta_{E_i})$*;*

(2) The Szpiro ratio σ_{E_i} is uniformly bounded.

2.9.1 Heights and polarized isogenies

We recall some definitions and facts that will allow us to write more general statements (see VI §2 in [**M-F-C**] or the brief summary in §1 of [**Mum**]). Let $\mathscr{L}$ be an ample line bundle on an abelian variety of dimension g. Then there is an integer $\deg(\mathscr{L})$, called the *degree of* $\mathscr{L}$, such that

$$\dim H^0(A, \mathscr{L}^n) = \deg(\mathscr{L})\cdot n^g \quad \text{for all } n \geq 1.$$

If $\mathscr{L} = \mathscr{L}(D)$ for some $D \in \mathrm{Div}(A)$, then

$$(D^g) = \deg(\mathscr{L})\cdot g!,$$

where (D^g) denotes the self-intersection number of D. The degree of the polarization $\lambda_{\mathscr{L}}$ induced by $\mathscr{L}$ is then $\deg(\lambda_{\mathscr{L}}) = \deg(\mathscr{L})^2$.

Now let $\varphi\colon A \to B$ be an isogeny of polarized abelian varieties of dimension g, where A (resp. B) is equipped with the polarization λ (resp. μ) induced by a line bundle $\mathscr{L}$ (resp. $\mathscr{M}$). Suppose that φ is polarized with respect to λ and μ, that is

$$\lambda = \varphi^\vee \circ \mu \circ \varphi$$

(recall Definition 1.2). Note that:

(1) $\deg(\mathscr{L}) = \deg(\varphi^*\mathscr{M}) = \deg(\varphi)\deg(\mathscr{M})$;

(2) $\deg(\lambda) = \deg(\varphi^\vee \circ \mu \circ \varphi) = \deg(\varphi)^2 \deg(\mu)$.

Suppose that for some $n \in \mathbf{N}$ we have $\lambda = [n] \circ \tilde{\lambda}$, where $\tilde{\lambda}\colon A \to A^\vee$ is a principal polarization, i.e. $\deg(\tilde{\lambda}) = 1$. Then we have

$$\deg(\mathscr{L})^2 = \deg(\lambda) = \deg([n])\deg(\tilde{\lambda}) = n^{2g},$$

whence $\mathscr{L} = \widetilde{\mathscr{L}}^n$, where $\widetilde{\mathscr{L}}$ is the line bundle corresponding to the principal polarization $\tilde{\lambda}$. If we also suppose that $\mu\colon B \to B^\vee$ is principal, then we have

$$n^{2g} = \deg(\mathscr{L})^2 = \deg(\lambda) = \deg(\varphi)^2$$

and therefore $\deg(\varphi) = n^g$.

Remark 2.17 This is precisely the case in the situation that we described in Chapter 1, where $g = 2$ and

$$\varphi\colon E_1 \times E_2 \to \mathrm{Jac}(C)$$

is a polarized isogeny whose kernel is the graph Γ_α of an anti-symplectic isomorphism $\alpha\colon E_1[n] \xrightarrow{\sim} E_2[n]$ and we have $\varphi^*(C) \sim n\Theta$.

Let $\hat{h}_A$ and $\hat{h}_B$ denote the canonical heights corresponding to principal polarizations induced by the line bundles $\widetilde{\mathscr{L}}$ and $\mathscr{M}$, respectively. By Theorem 2.12, for every $P \in A(K)$, we have

$$\begin{aligned}\hat{h}_B(\varphi(P)) &= \hat{h}_{\mathscr{M}}(\varphi(P)) = \hat{h}_{\varphi^*\mathscr{M}}(P)\\ &= \hat{h}_{\mathscr{L}}(P) = \hat{h}_{\widetilde{\mathscr{L}}^n}(P)\\ &= n \cdot \hat{h}_A(P) = \deg(\varphi)^{1/g} \cdot \hat{h}_A(P).\end{aligned}$$

If A and B are elliptic curves, the same result can be obtained by interpreting the Néron-Tate height as an arithmetic intersection number since Corollary 2.17 and Theorem 2.19 give us a projection formula. Viewing points of A and B as sections of the corresponding Néron models, we have

$$\begin{aligned}\hat{h}_B(\varphi(P)) &= \widehat{\deg}(\varphi(P)^*\mathscr{M}) = \widehat{\deg}(P^*\varphi^*\mathscr{M}) \\ &= \widehat{\deg}(P^*\widetilde{\mathscr{L}}^n) = n\cdot\widehat{\deg}(P^*\widetilde{\mathscr{L}}) \\ &= \deg(\varphi)^{1/g}\cdot\hat{h}_A(P)\end{aligned}$$

It follows that $P\in A(K)$ is a point of infinite order if and only if $\varphi(P)\in B(K)$ is one.

Not every point $Q\in B(K)$ need be of the form $\varphi(P)$, that is to say that the cokernel $B(K)/\varphi(A(K))$ need not be trivial. However, any isogeny $A\to B$ induces an isomorphism of real vector spaces

$$A(K)\otimes\mathbf{R}\cong B(K)\otimes\mathbf{R}\cong\mathbf{R}^r \text{ for some } r\in\mathbf{N}.$$

In particular, the lattices $A(K)$ and $B(K)$ are of the same rank. In fact, as we have seen in (2.28), we have

$$B(K)/\varphi(A(K))\leqslant \mathrm{Sel}^{(\varphi)}(A/K),$$

where the latter is a finite group. Let $e_A\in\mathbf{N}$ be the exponent of $\mathrm{Sel}^{(\varphi)}(A/K)$. Then for every $Q\in B(K)$ we have $[e_A]Q\in\varphi(A(K))$. For every $P\in A(K)$ and $Q\in B(K)$ such that $[e_A]Q=\varphi(P)$, we have

$$e_A^2\hat{h}_B(Q)=\hat{h}_B([e_A]Q)=\hat{h}_B(\varphi(P))=n\cdot\hat{h}_A(P),$$

and therefore

$$\hat{h}_B(Q)=\frac{n}{e_A^2}\hat{h}_A(P). \tag{2.33}$$

Since A and B are principally polarized, we may also compare the heights as follows. Let $Q\in B(K)$. Then

$$P:=(\tilde{\lambda}^{-1}\circ\varphi^\vee\circ\mu)(Q)\in A(K)$$

is a point that satisfies $\varphi(P)=[n]Q$ and we have

$$\hat{h}_B(Q)=\frac{1}{n}\hat{h}_A(P). \tag{2.34}$$

Proposition 2.4 *Let $g \in \mathbf{N}$ and let I be an infinite index set. Suppose that*

$$\varphi_i \colon (A_i, \lambda_i) \to (B_i, \mu_i), \quad i \in I$$

is an infinite family of isogenies of g-dimensional principally polarized abelian varieties over a number field K, such that $\deg(\varphi_i) = n_i^g$ for $n_i \in \mathbf{N}$ and φ_i is polarized with respect to $[n_i] \circ \lambda_i$ and μ_i. Suppose that there is a constant $c > 0$ such that $n_i \leq c$ for all $i \in I$. Then if the family $\{A_i\}_{i \in I}$ satisfies the Lang-Silverman conjecture, so does $\{B_i\}_{i \in I}$.

Proof Let $c_1 > 0$ be a constant such that for all $i \in I$, one has

$$\hat{h}_{A_i}(P) \geq c_1 h_{\mathrm{Falt}}(A_i/K) \text{ for all } P \in A_i(K) \setminus A_i(K)_{\mathrm{tors}}.$$

Then we can take $c_2 = c_1/c$ and by (2.34) we have

$$\hat{h}_{B_i}(Q) \geq c_2 h_{\mathrm{Falt}}(A_i/K) \text{ for all } Q \in B_i(K) \setminus B_i(K)_{\mathrm{tors}}.$$

If there exists a constant $c_e > 0$ such that $n_i/e_i^2 \geq c_e$ for all $i \in I$, where e_i denotes the exponent of $\mathrm{Sel}^{(\varphi_i)}(A_i/K)$, then we can take $c_2 = c_1/\min(c, c_e)$.

By the theorem of Raynaud (recall (2.30)), we have

$$|h_{\mathrm{Falt}}(A_i/K) - h_{\mathrm{Falt}}(B_i/K)| \leq \frac{1}{2} \log \deg(\varphi_i) = \frac{g}{2} \log n_i \leq \frac{g}{2} \log c$$

so that for a $c_3 > 0$ and for all $Q \in B_i(K)$, we have

$$\hat{h}_{B_i}(Q) \geq c_2 h_{\mathrm{Falt}}(B_i/K) - c_1 \geq c_3 h_{\mathrm{Falt}}(B_i/K) \tag{2.35}$$

for all but at most finitely many $i \in I$, because for any $c > 0$, there are only finitely many isomorphism classes of abelian varieties A/K of dimension g such that $h_{\mathrm{Falt}}(A/K) < c$. Let $J \subset I$ be the finite index set for which (2.35) fails and for $j \in J$ let $P_j \in B_j(K) \setminus B_j(K)_{\mathrm{tors}}$ denote a point for which $\hat{h}_{B_j}$ achieves its minimum. Let

$$c_4 := \min \left\{ \frac{\hat{h}_{B_j}(P_j)}{h_{\mathrm{Falt}}(B_j/K)} \right\}_{j \in J}.$$

Then for $C := \min\{c_3, c_4\}$ we have

$$\hat{h}_{B_i}(Q) \geq C h_{\mathrm{Falt}}(B_i/K) \text{ for all } Q \in B_i(K)$$

and the claim follows. □

We obtain the following two theorems as corollaries, recalling that we had assumed that all varieties and morphisms are defined over K, a number field.

Theorem 2.38 *For every $n \in \mathbf{N}$, the Lang-Silverman conjecture holds for (n,n)-split Jacobians if and only if it holds for elliptic curves that can be glued along their n-torsion with another elliptic curve to make an (n,n)-split Jacobian. In particular, if the Lang-Silverman conjecture holds for elliptic curves, then it holds for (n,n)-split Jacobians.*

Proof It follows from Lemma 1.6 that Proposition 2.4 applies to (n,n)-split Jacobians. □

Theorem 2.39 *For every $n \in \mathbf{N}$, the Lang-Silverman conjecture holds for Jacobians that are (n,n)-isogenous to a product $E_1 \times E_2$ of elliptic curves such that at least one of the following is satisfied for $i = 1, 2$:*

(1) $\mathrm{Tr}_\infty(E_i) > \frac{1}{7} \log N_{K/\mathbf{Q}}(\Delta_{E_i})$*;*

(2) The Szpiro ratio σ_{E_i} is uniformly bounded.

Proof This follows from Theorem 2.38 and Corollary 2.37. □

Remark 2.18 In the original statement of Theorem 2.34 in [**Paz2**], it is assumed that $\mathrm{Jac}(C)$ is geometrically simple; however, this assumption is not necessary.

Appendix

Computations

This appendix contains the source code for some of the software computations carried out for Chapter 1.

SAGE code that outputs the generic $(2,2)$-case j-invariants (page 23):

```
K.<a,b,c> = Frac(PolynomialRing(QQ,'a,b,c'))
R.<x> = PolynomialRing(K,'x')
S.<y> = PolynomialRing(R,'y')

P = x^3+a*x^2+b*x+c
Q = x^3+(b/c)*x^2+(a/c)*x+1/c

E1 = EllipticCurve([0, P.coefficients()[2], 0,
   P.coefficients()[1],P.coefficients()[0]])
E2 = EllipticCurve([0, Q.coefficients()[2], 0,
   Q.coefficients()[1],Q.coefficients()[0]])

#print the j-invariants
print "j(E1) =",factor(E1.j_invariant()),"\n\n"
print "j(E2) =",factor(E2.j_invariant())
```

SAGE code that outputs the generic $(3,3)$-case j-invariants (page 27):

```
K.<a,b,c,d,e> = Frac(PolynomialRing(QQ,'a,b,c,d,e'))
R.<x> = PolynomialRing(K,'x')
S.<y> = PolynomialRing(R,'y')
L = Frac(PolynomialRing(QQ,'a,b,c'))
L0 = PolynomialRing(QQ,'a,b,c')
M = PolynomialRing(QQ,'a,b,c,d,e')
N = PolynomialRing(L,'d,e',order='lex')

P = x^3+a*x^2+b*x+c
D1 = -2*P + x*P.derivative()
```

```
F1 = S([R(i) for i in
    (x^2*P(y)-y^2*P(x)).quo_rem(x-y)[0].coefficients()])

Res1 = F1.sylvester_matrix(D1(y)).det()
AllmostQ = Res1.quo_rem(D1)[0]
#this polynomial is divisible by Res(P(x),x)=-c
Q = AllmostQ/(-c)

T = (x+d)^2*(x+e)*Q(y)-(y+d)^2*(y+e)*Q(x)
F2 = S([R(i) for i in T.quo_rem(x-y)[0].coefficients()])
D2 = -2*(x+e)*Q - Q*(x+d) + (x+e)*(x+d)*Q.derivative()
Res2 = F2.sylvester_matrix(D2(y)).det()


AllmostP = Res2.quo_rem(D2)[0]
#this polynomial must be divisible by P, i.e.
#the following polynomial is identically zero

RemainderP = AllmostP.quo_rem(P)[1]

Equations = [N(M(RemainderP.coefficients()[0])),
   N(M(RemainderP.coefficients()[1])),
   N(M(RemainderP.coefficients()[2]))]

#the remainder is divisible by Res(Q(x),x+d) and Res(Q(x),x+e)
for i in range(3):
    Equations[i]=Equations[i].quo_rem(N(M(Q(-d)*Q(-e))))[0]

#print the equations
print "C is given by y^2=("+str(P)+")("+str(Q)+")"
print "\nThe two P^1->P^1 maps are"
print "f1: x->x^2/("+str(P)+"),\nf2: x->(x+d)^2*(x+e)/("+str(Q)+")"
print "\nd,e are determined by the following:\n"
for i in range(3):
    print str(i+1)+")",Equations[i],"= 0\n\n"

#print the Groebner basis
I = N.ideal(Equations)
GB = I.groebner_basis()
print "The solution is found by a Groebner basis computation."
print "The lex Groebner basis has",len(GB),"elements:\n"
for i in range(0,len(GB)):
    print "g"+str(i+1)+"=",GB[i],"\n\n"
```

```
#obtain d,e as elements of L
d1 = L(-GB[0]+N(M(d)))
e1 = L(-GB[1]+N(M(e)))
print "Therefore d = "+str(d1)+" and e = "+str(e1)

#the cubic defining E1
U = (x*P(y)-y^2).sylvester_matrix(Q(y)).det()
U = U/U.coefficients()[3]

#the cubic defining E2
V = (x*Q(y)-(y+d1)^2*(y+e1)).sylvester_matrix(P(y)).det()
V = V/V.coefficients()[3]

#print the j-invariants
E1 = EllipticCurve([0, U.coefficients()[2], 0,
   U.coefficients()[1], U.coefficients()[0]])

E2 = EllipticCurve([0, V.coefficients()[2], 0,
   V.coefficients()[1], V.coefficients()[0]])

print "\nThe two curves have modular invariants:\n"
print "j(E1) =",factor(E1.j_invariant()),"\n\n"
print "j(E2) =",factor(E2.j_invariant())
```

SAGE code that outputs (1.35) (page 47):

```
R.<u,v,w,a,b,c,r,s,t> =
    PolynomialRing(QQ,'u,v,w,a,b,c,r,s,t',order='lex')

Iu = R.ideal(a+r+s+t, -b+r*s+r*t+s*t, c+r*s*t,
   -u*(r-s)*(r-t)+2*r-s-t)
Iv = R.ideal(a+r+s+t, -b+r*s+r*t+s*t, c+r*s*t,
   -v*(r-s)*(r-t)-r^2+s^2+t^2-r*s-r*t+s*t)
Iw = R.ideal(a+r+s+t, -b+r*s+r*t+s*t, c+r*s*t,
   -w*(r-s)*(r-t)+r^2*s-r*s^2+r^2*t-r*t^2)

GBu = Iu.groebner_basis('singular:std')._singular_()
Lu = [f.sage_poly(R) for f in GBu.eliminate(prod([s,t]))]
GBv = Iv.groebner_basis('singular:std')._singular_()
Lv = [f.sage_poly(R) for f in GBv.eliminate(prod([s,t]))]
GBw = Iw.groebner_basis('singular:std')._singular_()
Lw = [f.sage_poly(R) for f in GBw.eliminate(prod([s,t]))]
```

```
print "Ideal Iu with s,t eliminated:"
for g in Lu:
    print str(factor(g))

print "\nIdeal Iv with s,t eliminated:"
for g in Lv:
    print str(factor(g))

print "\nIdeal Iw with s,t eliminated:"
for g in Lw:
    print str(factor(g))

print "\nWe solve the following for u,v,w:"
print Lu[2],"= 0"
print Lv[2],"= 0"
print Lw[2],"= 0"
```

SAGE code that outputs (1.36) (page 48):

```
R.<u,v,w,a,b,c,d,r,s,t> =
    PolynomialRing(QQ,'u,v,w,a,b,c,d,r,s,t',order='lex')

Iu = R.ideal(a+r+s+t, -b+r*s+r*t+s*t, c+r*s*t, d-(r-s)*(s-t)*(t-r),
    -u*d+r^2+s^2+t^2-r*s-r*t-s*t )
Iv = R.ideal(a+r+s+t, -b+r*s+r*t+s*t, c+r*s*t, d-(r-s)*(s-t)*(t-r),
    -v*d-r^3-s^3-t^3+r^2*s+r*t^2+s^2*t )
Iw = R.ideal(a+r+s+t, -b+r*s+r*t+s*t, c+r*s*t, d-(r-s)*(s-t)*(t-r),
    -w*d + r^3*t+r*s^3+s*t^3-r^2*t^2-r^2*s^2-s^2*t^2)

GBu = Iu.groebner_basis('singular:std')._singular_()
Lu = [f.sage_poly(R) for f in GBu.eliminate(prod([r,s,t]))]
GBv = Iv.groebner_basis('singular:std')._singular_()
Lv = [f.sage_poly(R) for f in GBv.eliminate(prod([r,s,t]))]
GBw = Iw.groebner_basis('singular:std')._singular_()
Lw = [f.sage_poly(R) for f in GBw.eliminate(prod([r,s,t]))]

print "Ideal Iu with r,s,t eliminated:"
for g in Lu:
    print str(factor(g))

print "\nIdeal Iv with r,s,t eliminated:"
for g in Lv:
    print str(factor(g))
```

```
print "\nIdeal Iw with r,s,t eliminated:"
for g in Lw:
    print str(factor(g))

print "\nWe solve the following for u,v,w:"
print Lu[1],"= 0"
print Lv[1],"= 0"
print Lw[1],"= 0"
```

The following MAGMA codes give the results on page 59.

Remark A.1 The notations λ, μ, and ζ are replaced by a, b, and z, respectively. The points of G and the corresponding translation morphisms on $\mathbb{P}^8$ can be found easily, using formulas (1.40) and (1.41).

```
RR<x> := PolynomialRing(Integers());
L<z> := NumberField(1+x+x^2);
K<a,b> := FunctionField(L, 2);
/* M is the group of translations by points of the graph of the
   3-torsion isomorphism that is given by S->S and T->-T,
   where S = [1 : 0 : -1], T = [-z : 1 : 0] */
M := MatrixGroup <9, K | [
0,0,0,0,1,0,0,0,0,
0,0,0,0,0,1,0,0,0,
0,0,0,1,0,0,0,0,0,
0,0,0,0,0,0,0,1,0,
0,0,0,0,0,0,0,0,1,
0,0,0,0,0,0,1,0,0,
0,1,0,0,0,0,0,0,0,
0,0,1,0,0,0,0,0,0,
1,0,0,0,0,0,0,0,0
],[
1,0,0,0,0,0,0,0,0,
0,z,0,0,0,0,0,0,0,
0,0,z^2,0,0,0,0,0,0,
0,0,0,z^2,0,0,0,0,0,
0,0,0,0,1,0,0,0,0,
0,0,0,0,0,z,0,0,0,
0,0,0,0,0,0,z,0,0,
0,0,0,0,0,0,0,z^2,0,
0,0,0,0,0,0,0,0,1]>;
```

```
R<X1,X2,X3,X4,X5,X6,X7,X8,X9> := PolynomialRing(K,9);
InvariantsOfDegree(M,R,3);
/* invariants of degree < 3 are no longer invariants if we multiply
   the matrices by z or z^2; one could add these matrices to M,
   but the degree 3 invariants are the same either way */
```

We reduce the obtained invariants $P_1, \ldots, P_{21}$ modulo the ideal $I = I(A)$. This can be done by adding $P_i(X_1, \ldots, X_9) - T_i$ to the ideal and computing a Gröbner basis in $K[T_1, \ldots, T_{21}, X_1, \ldots, X_9]$.

```
I := ideal <R |
    X1^3 + X2^3 + X3^3 + 3*b*X1*X2*X3,
    X1^2*X2 + X4^2*X5 + X7^2*X8 + 3*a*X1*X4*X8,
    X1*X2^2 + X4*X5^2 + X7*X8^2 + 3*a*X1*X5*X8,
    X2^3 + X5^3 + X8^3 + 3*a*X2*X5*X8,
    X1^2*X3 + X4^2*X6 + X7^2*X9 + 3*a*X1*X4*X9,
    X1*X2*X3 + X4*X5*X6 + X7*X8*X9 + 3*a*X1*X5*X9,
    X2^2*X3 + X5^2*X6 + X8^2*X9 + 3*a*X2*X5*X9,
    X1*X3^2 + X4*X6^2 + X7*X9^2 + 3*a*X1*X6*X9,
    X2*X3^2 + X5*X6^2 + X8*X9^2 + 3*a*X2*X6*X9,
    X3^3 + X6^3 + X9^3 + 3*a*X3*X6*X9,
    X1^2*X4 + X2^2*X5 + X3^2*X6 + 3*b*X1*X2*X6,
    X1*X4^2 + X2*X5^2 + X3*X6^2 + 3*b*X1*X5*X6,
    X4^3 + X5^3 + X6^3 + 3*b*X4*X5*X6,
    X1^2*X7 + X2^2*X8 + X3^2*X9 + 3*b*X1*X2*X9,
    X1*X4*X7 + X2*X5*X8 + X3*X6*X9 + 3*b*X1*X5*X9,
    X4^2*X7 + X5^2*X8 + X6^2*X9 + 3*b*X4*X5*X9,
    X1*X7^2 + X2*X8^2 + X3*X9^2 + 3*b*X1*X8*X9,
    X4*X7^2 + X5*X8^2 + X6*X9^2 + 3*b*X4*X8*X9,
    X7^3 + X8^3 + X9^3 + 3*b*X7*X8*X9,
    X2*X4 + -1*X1*X5,
    X3*X4 + -1*X1*X6,
    X3*X5 + -1*X2*X6,
    X2*X7 + -1*X1*X8,
    X3*X7 + -1*X1*X9,
    X5*X7 + -1*X4*X8,
    X6*X7 + -1*X4*X9,
    X3*X8 + -1*X2*X9,
    X6*X8 + -1*X5*X9>;
```

This leaves nine linearly independent invariants $F_1, \ldots, F_9$.

```
F1 := X1*X2*X4 + X3*X7*X9 + X5*X6*X8;
F2 := X1*X3*X7 + X2*X4*X5 + X6*X8*X9;
F3 := X2^2*X7 + X3*X5*X6 + X6*X7^2;
F4 := X3^2*X4 + X3*X8^2 + X4*X5*X7;
F5 := X3^2*X8 + X3*X4^2 + X5*X7*X8;
F6 := X3*X5*X7;
F7 := X2*X3*X5 + X2*X7^2 + X6^2*X7;
F8 := 3*a*X2*X5*X8 + X5^3 + -1*X6^3 + 3*b*X7*X8*X9 + 2*X8^3 + X9^3;
F9 := 3*a*X3*X6*X9 + 3*b*X4*X5*X6 + X5^3 + 2*X6^3 + -1*X8^3 + X9^3;
```

We reduce the polynomial

$$P := d_1F_1 + \cdots + d_9F_9 - (c_1X_1 + \cdots + c_9X_9)^3 \in K(c_i, d_j)[X_1, \ldots, X_9]$$

modulo $I = I(A)$ and we eliminate the variables d_i from the ideal generated by the coefficients of P mod I.

```
R2<d1,d2,d3,d4,d5,d6,d7,d8,d9,c1,c2,c3,c4,c5,c6,c7,c8,c9> :=
   PolynomialRing(K,18);
I2 := ideal<R2 |
   3*c1^2*c5 + 6*c1*c2*c4 - d7,
   3*c1^2*c8 + 6*c1*c2*c7,
   // many generators are omitted here
   -3*c2*c3^2 + 3*c8*c9^2,
   c1^3 - c3^3 - c7^3 + c9^3 + d1 + d2
>;
J := EliminationIdeal(I2,9);
```

Finally, the points of $Z(J)$ are found:

```
P8<c1,c2,c3,c4,c5,c6,c7,c8,c9> := ProjectiveSpace(K,8);
X := Scheme(P8, [
   c8*c9^4,
   c8^2*c9^2,
   c7*c9^4,
   c7*c8*c9^2 + -b*c8^3*c9,
   // many generators are omitted here
   c3^2*c7*c9 + -1/2*c3*c5^2*c9 + -1*c3*c5*c6*c8,
   c1*c3*c6 + 1/2*c3^2*c4 + -1/2*c4^2*c8 + -1*c4*c5*c7
]);
Degree(X) eq 9;
Points(X);
```

These solutions define the following nine linear forms:

```
L1 := z^2*X1 + z*X5 + X9;
L2 := z*X1 + z^2*X5 + X9;
L3 := X3 + X4 + X8;
L4 := z^2*X3 + z*X4 + X8;
L5 := z*X3 + z^2*X4 + X8;
L6 := X2 + X6 + X7;
L7 := z^2*X2 + z*X6 + X7;
L8 := z*X2 + z^2*X6 + X7;
L9 := X1 + X5 + X9;
```

We note that L_9 is the one that is fixed by $-\mathbb{1}_A$, so that it defines the divisor D whose image under $A \to A/G$ principally polarizes A/G. We note that D does not contain O. Finally, we check under which conditions D contains points of $A[2]$ that do not correspond to points of order two on E_λ or E_μ:

```
R3<T,X1,X2,X3,X4,X5,X6,X7,X8,X9,a,b> := PolynomialRing(L,12);
I3 := ideal <R3 |
   X5^3 + -9/4*a*b*X5^2*X9 + -3/4*a*X6^2*X9 + -3/4*b*X8^2*X9 +
       -1/4*X9^3,
   X5^2*X6 + 3/2*a*X5^2*X9 + 1/2*X8^2*X9,
   X5*X6^2 + 3/2*a*X5*X6*X9 + 1/2*X8*X9^2,
   X6^3 + 3/2*a*X6^2*X9 + 1/2*X9^3,
   X5^2*X8 + 3/2*b*X5^2*X9 + 1/2*X6^2*X9,
   X5*X8^2 + 3/2*b*X5*X8*X9 + 1/2*X6*X9^2,
   X8^3 + 3/2*b*X8^2*X9 + 1/2*X9^3,
   X6*X8 + -1*X5*X9,
   X1 + -1*X5,
   X2 + -1*X5,
   X3 + -1*X6,
   X4 + -1*X5,
   X7 + -1*X8,
   X9*T-1,
   L9>;
GroebnerBasis(EliminationIdeal(I3,10))[1];
```

The output is a polynomial that defines a curve of genus zero:

```
A<a,b> := AffineSpace(Rationals(),2);
Genus(Curve(A, 3*a^2*b^2 + a^3 - 3*a*b + b^3 + 2));
```

Bibliography

[**Abb**] Ahmed Abbès, *Réduction semi-stable des courbes d'après Artin, Deligne, Grothendieck, Mumford, Saito, Winters,...*, in *Courbes semi-stables et groupe fondamental en géométrie algébrique (Luminy, 1998)*, Progr. Math. **187**, Birkhäuser, Basel (2000), pp. 59–110

[**Ar-Do**] Michela Artebani and Igor Dolgachev, *The Hesse Pencil of Plane Cubic Curves*, L'Enseignement Mathématique **55** (2009), pp. 235–270
DOI: 10.5169/seals-110104

[**At-Wa**] Michael Atiyah and Charles T. C. Wall, *Cohomology of Groups*, Algebraic Number Theory, University of Sussex, Brighton (1965), pp. 94–115
MR 0219512

[**AEC**] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, New York (1986)
ISBN: 978-0-387-09493-9

[**AEC2**] _____ *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **151**, Springer-Verlag, New York (1994)
ISBN: 978-0-387-94328-2.

[**ANT1**] Serge Lang, *Algebraic Number Theory*, Graduate Texts in Mathematics **110**, Springer-Verlag, New York (1986)
ISBN: 978-0-387-94225-4

[**ANT2**] Jürgen Neukirch, *Algebraic Number Theory*, Grundlehren der mathematischen Wissenschaften **322**, Springer-Verlag Berlin Heidelberg (1999)
ISBN: 978-3-540-65399-8

[**Ara**] Suren Yu. Arakelov, *An Intersection Theory for Divisors on an Arithmetic Surface*, Math. USSR Izv. **8** (1974), pp. 1167–1180
DOI: 10.1070/IM1974v008n06ABEH002141

[**Art**] Michael Artin, *Néron Models*, Ch. VIII in *Arithmetic Geometry* (ed. by G. Cornell and J. H. Silverman), Springer, New York (1986), pp. 213–230
ISBN: 978-0-387-96311-2

[**Aut**] Pascal Autissier, *Un lemme matriciel effectif*, Math. Z. **273**, pp. 355–361
DOI: 10.1007/s00209-012-1008-x

[**Br-Do**] Nils Bruin and Kevin Doerksen, *The Arithmetic of Genus Two Curves with* $(4,4)$*-Split Jacobians*, Canad. J. Math. **63** (2011), pp. 992–1021
DOI: 10.4153/CJM-2011-039-3

[**B-H-P-V**] Wolf P. Barth, Klaus Hulek, Chris A. M. Peters, and Antonius van de Ven*Compact Complex Surfaces (2nd ed.)*, Ergeb. Math. Grenzgeb. **4**, Springer Berlin Heidelberg (2004)
ISBN: 978-3-540-00832-3

[**B-L-R**] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron Models*, Ergeb. Math. Grenz. **21**, Springer-Verlag, Berlin (1990)
ISBN: 978-3-540-50587-7

[**Cre**] John E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press New York, New York (1992)
ISBN: 978-0-521-41813-5

[**Dav**] Sinnou David, *Minorations de hauteurs sur les variétés abéliennes*, Bull. Soc. Math. France **121** (1993), pp. 509–544
ISSN: 0037-9484 EUDML: 87676

[**DA**] Wolfgang M. Schmidt, *Diophantine Approximation*, Lecture Notes in Mathematics **785**, Springer-Verlag, New York (1980)
ISBN: 978-3-540-09762-4

[**dJ**] Robin S. de Jong, *On the Arakelov theory of elliptic curves*, Enseign. Math. **51** (2005), pp. 179–201
arXiv: 0312359

[**DG**] Marc Hindry and Joseph H. Silverman, *Diophantine Geometry: An Introduction*, Graduate Texts in Mathematics **201**, Springer-Verlag, New York (2000)
ISBN: 978-0-387-98975-4

[**Falt1**] Gerd Faltings, *Calculus on Arithmetic Surfaces*, Ann. Math. **119** (1984)
DOI: 10.2307/2007043

[**Falt2**] _____ *Finiteness Theorems for Abelian Varieties*, Ch. II in *Arithmetic Geometry* (ed. by G. Cornell and J. H. Silverman), Springer, New York (1986), pp. 9–27
ISBN: 978-0-387-96311-2

[**Farn**] Shawn Farnell, *Artin-Schreier Curves*, Colorado University, Ph.D. thesis (2010)
http://hdl.handle.net/10217/44957

[**Fr-Ka**] Gerhard Frey and Ernst Kani, *Curves of Genus 2 Covering Elliptic Curves and an Arithmetical Application*, *Arithmetic Algebraic Geometry*, Progress in Mathematics **89**, Birkhäuser Boston (1991), pp. 153–177
ISBN: 978-0-8176-3513-8

[**Ga-Ré**] Eric Gaudron and Gaël Rémond, *Théorème des périodes et degrés minimaux d'isogénies*, Comment. Math. Helv. **89** (2014), pp. 343–403
DOI: 10.4171/CMH/322

[**HAG**] Robin Hartshorne, *Algebraic Geometry*, Springer-Verlag (1977)
ISBN: 978-0-387-90244-9

[**Hi-Si**] Marc Hindry and Joseph H. Silverman, *Canonical heights and integral points on elliptic curves*, Invent. Math. **93** (1988), pp. 419–450
DOI: 10.1007/BF01394340

[**Holm**] David Holmes, *Computing Néron–Tate heights of points on hyperelliptic Jacobians*, J. Number Theor. **132** (2012), pp. 1295–1305
DOI: 10.1016/j.jnt.2012.01.002

[**Hri**] Paul Hriljac, *Heigths and Arakelov's Intersection Theory*, Amer. J. Math. **107** (1985), pp. 23–38
DOI: 10.2307/2374455

[**IVA**] David Cox, John Little, and Donald O'Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer (1997)
ISBN: 978-0-387-94680-1

[**Ke-St**] Gregor Kemper and Allan Steel, *Some Algorithms in Invariant Theory of Finite Groups*, Computational Methods for Representations of Groups and Algebras, Euroconference in Essen, April 1997, Progr. Math. **173**, Birkhäuser, Basel (1997), pp. 267–285 ISBN: 978-3-0348-9740-2

[**Kraz**] Adolf Krazer, *Lehrbuch der Thetafunktionen*, AMS Chelsea Publishing (1970)
ISBN: 978-0-8284-0244-6

[**Kuhn**] Robert M. Kuhn, *Curves of genus 2 with split Jacobian*, Trans. Amer. Math. Soc. **307** (1988)
DOI: 10.2307/2000749

[**Lang1**] Serge Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag New York (1983)
ISBN: 978-1-4419-2818-4

[**Lang2**] _____ *Introduction to Arakelov Theory*, Springer-Verlag New York (1988)
ISBN: 978-0-387-96793-6

[**Lang3**] _____ *Elliptic Curves – Diophantine Analysis*, Springer-Verlag Berlin Heidelberg (1978)
ISBN: 978-3-540-08489-1

[**La-Ta**] Serge Lang and John Tate, *Principal Homogeneous Spaces Over Abelian Varieties*, Am. J. Math. **80** (1958), pp. 659–684
DOI: 10.2307/2372778

[**Liu**] Qing Liu, *Algebraic Geometry and Arithmetic Curves*, Oxford Graduate Texts in Mathematics (2006)
ISBN: 978-0-19-920249-2

[**Li-To**] Qing Liu and Jilong Tong, *Néron models of algebraic curves*, Trans. Amer. Math. Soc. **368** (2016), pp. 7019–7043
DOI: 10.1090/tran/6642

[**LMFDB**] `http://www.lmfdb.org/EllipticCurve/Q`

[**Mas1**] David W. Masser, *Small values of heights on families of abelian varieties*, Lect. Notes Math. **1290** (1987), pp 109–148
DOI: 10.1007/BFb0078706

[**Mas2**] _____ *Large period matrices and a conjecture of Lang*, Séminaire de Théorie des Nombres, Paris, 1991-1992 **116** (1993), pp 153–177
ISBN: 978-0-8176-3741-5

[**Müll**] Jan Steffen Müller, *Computing canonical heights using arithmetic intersection theory*, Math. Comp. **83** (2014), pp. 311–336
DOI: 10.1090/S0025-5718-2013-02719-6

[**Mum**] David Mumford, *On the equations defining abelian varieties I*, Invent. Math. **1** (1966), pp. 287–354
ISSN: 0020-9910 EUDML: 141838

[**MumAV**] _____ *Abelian Varieties (2nd ed.)*, Oxford University Press (1974)
ISBN: 978-81-85931-86-9

[**M-F-C**] David Mumford, John Fogarty, and Frances C. Kirwan, *Geometric Invariant Theory (3rd ed.)*, Ergeb. Math. Grenzgeb. **34**, Springer-Verlag Berlin Heidelberg (1994)
ISBN: 978-3-540-56963-3

[**Miln1**] James S. Milne, *Abelian Varieties*, Ch. V in *Arithmetic Geometry* (ed. by G. Cornell and J. H. Silverman), Springer, New York (1986), pp. 103–150
ISBN: 978-0-387-96311-2

[**Miln2**] _____ *Jacobian Varieties*, Ch. VII in *Arithmetic Geometry* (ed. by G. Cornell and J. H. Silverman), Springer, New York (1986), pp. 167–212
ISBN: 978-0-387-96311-2

[**Nér**] André Néron, *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux*, Publ. IHES Math. **21** (1964), pp. 5–125
DOI: 10.1007/BF02684271

[**Oes**] Joseph Oesterlé, *Nouvelles approches du "théorème" de Fermat*, Séminaire Bourbaki № **694** (1988)
EUDML: 110094

[**PAG**] Phillip Griffiths and Joseph Harris, *Principles of Algebraic Geometry*, John Wiley & Sons (1978)
ISBN: 978-0-471-32792-9

[**Paz1**] Fabien Pazuki, *Remarques sur une conjecture de Lang*, J. Théor. Nombres Bordeaux **22** (2010), pp. 161–179
JSTOR: 43973013

[**Paz2**] _____ *Minoration de la hauteur de Néron-Tate sur les surfaces abéliennes*, Manuscripta Math. **142** (2013), pp. 61–99
DOI: 10.1007/s00229-012-0593-7

[**Paz3**] _____ *Heights, ranks and regulators of abelian varieties*, preprint
arXiv: 1506.05165

[**Pet**] Clayton Petsche, *Small rational points on elliptic curves over number fields*, New York J. Math **12** (2006), 257–268
EUDML: 129992

[**Ray**] Michel Raynaud, *Hauteurs et isogénies*, Seminar on arithmetic bundles: the Mordell conjecture, Astérisque **127** (1985), pp. 199–234.

[**SGA3**] Michel Demazure and Alexandre Grothendieck, *Schemas en Groupes. Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3)*, Lecture Notes in Mathematics **151**, Springer-Verlag Berlin Heidelberg (1970)
ISBN: 978-3-540-05179-4

[**Sil1**] Joseph H. Silverman, *Lower bound for the canonical height on elliptic curves*, Duke Math. J. **48**, (1981), pp. 633–648
MR 630588 DOI: 10.1215/S0012-7094-81-04834-1

[**Sil2**] _____ *Heights and Elliptic Curves*, Ch. X in *Arithmetic Geometry* (ed. by G. Cornell and J.H. Silverman), Springer, New York (1986), pp. 253–265
ISBN: 978-0-387-96311-2

[**Sil3**] _____ *Lang's Height Conjecture and Szpiro's Conjecture*
arXiv: 0908.3895

[**Stich**] Henning Stichtenoth, *Algebraic Function Fields and Codes*, GTM, Springer (2008)
ISBN: 978-3-540-76877-7

[**Szp**] Lucien Szpiro, *Séminaire sur les pinceaux de courbes elliptiques*, Astérisque **183**, SMF (1990)
ISSN: 0303-1179

[**Tata1**] David Mumford, *Tata Lectures on Theta I*, Modern Birkhäuser Classics (1982), pp. 163–170
ISBN: 978-0-8176-4572-4

[**Tata2**] _____ *Tata Lectures on Theta II*, Modern Birkhäuser Classics (1984), pp. 100–106
ISBN: 978-0-8176-4569-4

[**Ueno**] Kenji Ueno, *Discriminants of curves of genus 2 and arithmetic surfaces*, Algebraic Geometry and Commutative Algebra **II**, Kinokuniya, Tokyo (1988), pp. 749–770
MR 977781

[**Weil**] André Weil, *Zum Beweis des Torellischen Satzes*, Oeuvres Scientifiques/Collected Papers: Volume 2 (1951-1964), Springer (2009), pp. 307–329
ISBN: 978-3-662-44322-4

Summary

This thesis deals with properties of Jacobians of genus two curves that cover elliptic curves.

Let E be a curve in the plane, given by an equation $y^2 = F(x)$, where

$$F(x) = x^3 + a_2x^2 + a_1x + a_0$$

is a polynomial with rational coefficients and with three distinct roots. For historical reasons, such a curve is known as an *elliptic curve*. It is known that every elliptic curve E can be equipped with a structure of a commutative group – its points can be added and subtracted. A point O "at infinity", which is contained in all vertical lines (lines of form $x = c$), is the neutral element. This group structure is described by the condition that three points $P, Q, R \in E$ satisfy $P + Q + R = O$ if and only if they are collinear. Surfaces with a commutative group structure are called *abelian*. For example, a product $E_1 \times E_2$ of two elliptic curves is an abelian surface in the obvious way.

Next we consider a planar curve C given by an equation $y^2 = G(x)$, where

$$G(x) = x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$$

is a polynomial with rational coefficients and six distinct roots. The curve C is called *hyperelliptic* and it does not have a group structure. However, we can associate to it, in a natural way, an abelian surface $\mathrm{Jac}(C)$, called the *Jacobian* of C. Moreover, we can embed C into it.

Some hyperelliptic curves, of the form $y^2 = G(x)$ as above, are special because they cover elliptic curves. For example, consider a curve C given by $y^2 = x^6 + ax^4 + bx^2 + c$, so that only even powers of x appear. If (x, y)

is a point on this curve then so is $(-x, y)$ and we can define an algebraic map $f\colon (x, y) \mapsto (x^2, y)$, that is of degree 2, i.e. 2-to-1. Now $(X, Y) = (x^2, y)$ is a point on the elliptic curve E given by $Y^2 = X^3 + aX^2 + bX + c$ and we say that C is a double cover of E.

If E is an elliptic curve, if C is a hyperelliptic curve, and if $C \to E$ is an n-to-1 covering that is not a composition of coverings, then we can embed E into the surface $\mathrm{Jac}(C)$ as a subgroup. Moreover, there exists another elliptic curve $\widetilde{E}$ and an n-to-1 covering $C \to \widetilde{E}$, such that the surface $\mathrm{Jac}(C)$ has a special property – it can be obtained as the quotient of the surface $E \times \widetilde{E}$ by a finite subgroup.

The first chapter of the thesis deals with the geometric aspects of this setup. We investigate which curves can form this special relationship and we focus mostly on the cases $n = 2$ and $n = 3$, which have already been analysed in literature. We also gain some insight into the general case, but a full description proves to be very difficult computationally.

The second chapter deals with the arithmetic aspects of the setup, via the theory of *height functions*, which are a very useful tool in answering questions about rational points on curves and surfaces. To every rational number $x = a/b$, where a and b are coprime integers, one can associate its height $h(x)$, in a very precise way, as a measurement of its arithmetic complexity – the height roughly tells us how many digits are needed to write down the integers a and b. Likewise, the height of a rational point on a curve or surface tells us about the number of digits of the coordinates. For example, $(3, 5)$ and $(1749/1331, -1861/1331)$ are two rational points of rather different complexity on the curve $y^2 = x^3 - x + 1$, while $(2, \sqrt{7})$ is not a rational point. It is also possible to associate a height to an elliptic curve or an abelian surface and measure its arithmetic complexity as a whole. A specific relation between these two heights is conjectured and we investigate it in the context of the setup above. We show that this relation holds for $E \times \widetilde{E}$ if and only if it holds for $\mathrm{Jac}(C)$.

Samenvatting

Dit proefschrift behandelt eigenschappen van Jacobianen van krommen van geslacht twee die elliptische krommen overdekken.

Zij E een kromme in het vlak, gegeven door een vergelijking $y^2 = F(x)$, waarbij $F(x) = x^3 + a_2x^2 + a_1x + a_0$ een polynoom is met rationale coëfficiënten en met drie verschillende nulpunten. Om historische redenen wordt een dergelijke kromme een *elliptische kromme* genoemd. Het is bekend dat elke elliptische kromme kan worden voorzien van een commutatieve groepsstructuur – haar punten kunnen bij elkaar worden opgeteld en van elkaar worden afgetrokken. Een punt O „op oneindig", dat bevat is in alle verticale lijnen (lijnen van de vorm $x = c$), is het neutrale element. De groepsstructuur wordt vastgelegd door de voorwaarde dat drie punten $P, Q, R \in E$ voldoen aan $P + Q + R = O$ dan en slechts dan als zij op één lijn liggen. Oppervlakken met een commutatieve groepsstructuur worden *abels* genoemd. Bijvoorbeeld is een product van twee elliptische krommen $E_1 \times E_2$ op de voor de hand liggende wijze een abels oppervlak.

Vervolgens beschouwen we een vlakke kromme C gegeven door een vergelijking $y^2 = G(x)$, waarbij $G(x) = x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$ een polynoom is met rationale coëfficiënten en zes verschillende nulpunten. De kromme C wordt *hyperelliptisch* genoemd en heeft geen groepsstructuur. Toch kunnen we, op een natuurlijke wijze, eraan een abels oppervlak $\mathrm{Jac}(C)$ toekennen, dat de *Jacobiaan* van C wordt genoemd. Voorts kunnen we C hierin inbedden. Sommige hyperelliptische krommen van de vorm $y^2 = G(x)$ zoals hierboven zijn bijzonder omdat zij elliptische krommen overdekken. Bijvoorbeeld, beschouw een kromme C gegeven door $y^2 = x^6 + ax^4 + bx^2 + c$, zodat alleen even machten van x optreden. Als (x, y) een punt is op deze kromme dan is $(-x, y)$ dat ook en we kunnen een algebraïsche afbeelding $f\colon (x, y) \mapsto (x^2, y)$

definiëren die van graad 2 is, d.w.z. 2-op-1. Het punt $(X, Y) = (x^2, y)$ ligt op de elliptische kromme E gegeven door $Y^2 = X^3 + aX^2 + bX + c$ en we zeggen dat C een dubbele overdekking is van E.

Als E een elliptische kromme is, C een hyperelliptische kromme, en $C \to E$ een n-op-1 overdekking die niet een samenstelling is van overdekkingen, dan kunnen we E inbedden in het oppervlak $\mathrm{Jac}(C)$ als ondergroep. Bovendien bestaat er een andere elliptische kromme $\widetilde{E}$ en een n-op-1 overdekking $C \to \widetilde{E}$. Voorts heeft het oppervlak $\mathrm{Jac}(C)$ een bijzondere eigenschap – het kan worden verkregen als een quotiënt van het oppervlak $E \times \widetilde{E}$ naar een eindige ondergroep.

Het eerste hoofdstuk van dit proefschrift behandelt de meetkundige aspecten van deze situatie. We onderzoeken welke krommen in deze bijzondere verhouding tot elkaar kunnen staan en we concentreren ons hoofdzakelijk op de gevallen $n = 2$ en $n = 3$, die al in de literatuur zijn onderzocht. We verkrijgen ook enig inzicht in het algemene geval, maar een volledige beschrijving blijkt vanuit computationeel oogpunt zeer moeilijk te zijn.

Het tweede hoofdstuk behandelt de aritmetische aspecten van de situatie, met behulp van de theorie van *hoogtes*, die een zeer bruikbaar hulpmiddel vormen bij het beantwoorden van vragen rond rationale punten op krommen en oppervlakken. Voor elk rationaal getal $x = a/b$, waarbij a en b gehele getallen zijn die relatief priem zijn, kan men de hoogte $h(x)$ definiëren, op een heel precieze manier, als een maat voor diens aritmetische complexiteit – de hoogte vertelt ons min of meer hoeveel cijfers er nodig zijn om de gehele getallen a en b op te schrijven. Op eenzelfde manier zegt de hoogte van een rationaal punt op een kromme of oppervlak ons iets over het aantal cijfers van zijn coördinaten. Bijvoorbeeld zijn $(3, 5)$ en $(1749/1331, -1861/1331)$ twee rationale punten van behoorlijk verschillende complexiteit op de kromme $y^2 = x^3 - x + 1$. Anderzijds is $(2, \sqrt{7})$ geen rationaal punt. Het is ook mogelijk om een hoogte toe te kennen aan een elliptische kromme of een abels oppervlak om zodoende diens aritmetische complexiteit als geheel te meten. Er wordt een precies verband tussen de twee hoogtes vermoed, en we onderzoeken dit vermoeden in de context van de situatie zoals boven geschetst. We bewijzen dat het vermoede verband geldt voor $E \times \widetilde{E}$ dan en slechts dan als het geldt voor $\mathrm{Jac}(C)$.

Résumé

Cette thèse concerne des propriétés des variétés jacobiennes de courbes de genre deux qui couvrent des courbes elliptiques.

Soit E une courbe plane, donnée par une équation $y^2 = F(x)$, où

$$F(x) = x^3 + a_2x^2 + a_1x + a_0$$

est un polynôme à coefficients rationnels, qui a trois racines distinctes. Pour des raisons historiques, une telle courbe est appelée *courbe elliptique*. On sait que toute courbe elliptique E peut être équipée d'une structure de groupe commutatif – on peut additionner et soustraire ses points. Un point O « à l'infini », qui est contenu dans toutes les droites verticales (droites de la forme $x = c$), est l'élément neutre. Cette structure de groupe est décrite par la condition que trois points $P, Q, R \in E$ satisfont $P + Q + R = O$ si et seulement s'ils sont alignés. Les surfaces avec une structure de groupe commutatif sont appelées *abéliennes*. Par exemple, un produit $E_1 \times E_2$ de deux courbes elliptiques est une surface abélienne, de façon évidente.

Considérons maintenant une courbe plane C donnée par $y^2 = G(x)$, où

$$G(x) = x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$$

est un polynôme à coefficients rationnels, qui a six racines distinctes. La courbe C est appelée *hyperelliptique* et n'a pas de structure de groupe. Par contre, nous pouvons lui associer, d'une façon naturelle, une surface abélienne $\mathrm{Jac}(C)$, appelée la *jacobienne* de C. En plus, nous pouvons plonger C dans $\mathrm{Jac}(C)$.

Certaines courbes hyperelliptiques sont spéciales car elles couvrent des courbes elliptiques. Par exemple, considérons une courbe C donnée par l'équation $y^2 = x^6 + ax^4 + bx^2 + c$, dans laquelle seulement des puissances paires

de x apparaissent. Si (x, y) est un point de cette courbe alors de même $(-x, y)$, et nous pouvons définir une application algébrique $f\colon (x, y) \mapsto (x^2, y)$ de degré 2, c'est-à-dire, de fibre générale à deux points. Alors $(X, Y) = (x^2, y)$ est un point de la courbe elliptique E donnée par $Y^2 = X^3 + aX^2 + bX + c$ et nous disons que C est un revêtement double de E.

Si E est une courbe elliptique, si C est une courbe hyperelliptique, et si $C \to E$ est un revêtement de degré n qui n'est pas une composition de revêtements, alors nous pouvons plonger E dans la surface $\mathrm{Jac}(C)$ comme un sous-groupe. De plus, il existe une autre courbe elliptique $\widetilde{E}$ et un revêtement $C \to \widetilde{E}$ de degré n, tel que la surface $\mathrm{Jac}(C)$ a une propriété spéciale – elle peut être obtenue comme quotient de la surface $E \times \widetilde{E}$ par un sous-groupe fini.

Le chapitre 1 de cette thèse traite les aspects géométriques de cette situation. Nous cherchons à savoir quelles courbes peuvent avoir une telle relation et nous nous concentrons surtout sur les cas $n = 2$ et $n = 3$, qui ont déjà été analysés dans la littérature. Dans le cas général, nous obtenons quelques résultats, mais une description complète s'avère très difficile de manière explicite.

Le chapitre 2 traite les aspects arithmétiques de la situation, via la théorie des *fonctions hauteurs*, qui sont un outil très utile pour répondre à des questions concernant des points rationnels de courbes et surfaces. Pour tout nombre rationnel $x = a/b$, avec a et b des entiers premiers entre eux, on définit la hauteur $h(x)$ de x, de façon très précise, comme une mesure de sa complexité arithmétique – la hauteur dit approximativement combien de chiffres sont nécessaires pour écrire les entiers a et b. De la même façon, la hauteur d'un point rationnel d'une courbe ou surface nous dit combien de chiffres ont les coordonnées. Par exemple, $(3, 5)$ et $(1749/1331, -1861/1331)$ sont deux points rationnels de complexités plutôt différentes de la courbe $y^2 = x^3 - x + 1$, tandis que $(2, \sqrt{7})$ n'est pas un point rationnel. Il est possible d'attacher une hauteur aux courbes elliptiques et aux surfaces abéliennes qui mesure leur complexité arithmétique totale. Une relation spécifique entre ces deux notions de hauteur est alors conjecturée et nous étudions cette conjecture dans la situation décrite plus haut. Nous montrons que cette relation est vraie pour $E \times \widetilde{E}$ si et seulement si elle est vraie pour $\mathrm{Jac}(C)$.

Sažetak

Predmet ove teze jesu svojstva jakobijana krivih roda dva koje pokrivaju eliptičke krive.

Neka je E kriva u ravni, data jednačinom $y^2 = F(x)$, gdje je

$$F(x) = x^3 + a_2x^2 + a_1x + a_0$$

polinom sa racionalnim koeficijentima i sa tri različita korijena. Iz povijesnih razloga, ovakvu krivu nazivamo *eliptičkom*. Poznato je da svaka eliptička kriva E može biti opremljena strukturom komutativne grupe – njene tačke možemo sabirati i oduzimati. Tačka O „u beskonačnosti", koja leži na svim uspravnim pravama (tj. pravama oblika $x = c$), jeste neutralni element grupe. Ova struktura grupe je opisana uslovom da za svake tri tačke $P, Q, R \in E$ važi $P + Q + R = O$ ako i samo ako one leže na istoj pravoj. Površi sa strukturom komutativne grupe zovemo *Abelovim*. Primjera radi, proizvod dvije eliptičke krive jeste Abelova površ, sa očevidnom strukturom grupe.

Razmotrimo sada krivu C u ravni, zadatu jednačinom $y^2 = G(x)$, gdje je

$$G(x) = x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$$

polinom sa racionalnim koeficijentima i sa šest različitih korijena. Krivu C zovemo *hipereliptičkom*. Ona nema strukturu grupe, ali joj možemo prirodno pridružiti jednu Abelovu površ $\mathrm{Jac}(C)$, koju zovemo *jakobijanom* krive C. Takođe, krivu C možemo uložiti u njen jakobijan.

Neke hipereliptičke krive, oblika $y^2 = G(x)$ kao gore, jesu posebne jer pokrivaju eliptičke krive. Primjera radi, razmotrimo krivu C zadatu jednačinom $y^2 = x^6 + ax^4 + bx^2 + c$, u kojoj se pojavljuju isključivo parni stepeni promjenjive x. Ako je (x, y) tačka na krivoj, onda je to i $(-x, y)$, što znači

da možemo odrediti algebarsko preslikavanje $f\colon (x,y) \mapsto (x^2,y)$, koje je stepena 2, tj. 2-na-1. Imamo da je $(X,Y) = (x^2,y)$ tačka na eliptičkoj krivoj E zadatoj jednačinom $Y^2 = X^3 + aX^2 + bX + c$ i kažemo da kriva C dvostruko pokriva krivu E.

Ako je E eliptička kriva, ako je C hipereliptička kriva, i ako je $C \to E$ pokrivanje stepena n, koje nije razloživo, tj. nije sastavljeno od pokrivanja manjeg stepena, onda krivu E možemo uložiti u površ $\mathrm{Jac}(C)$ kao podgrupu. Štoviše, postoji još jedna eliptička kriva $\widetilde{E}$ i nerazloživo pokrivanje $C \to \widetilde{E}$ stepena n, takvo da površ $\mathrm{Jac}(C)$ ima posebno svojstvo – možemo ju dobiti kao količnik površi $E \times \widetilde{E}$ i jedne njene konačne podgrupe.

Prvo poglavlje teze tiče se geometrijskih strana ove postavke. Istražujemo koje krive se mogu naći u ovoj posebnoj vezi, sa usredsređenjem na slučajeve $n = 2$ i $n = 3$, koji su već razmatrani u literaturi. Takođe izvodimo nekoliko zaključaka o opštem slučaju, ali puni opis nam ostaje nedostupan uslijed velike računske složenosti.

Drugo poglavlje teze tiče se aritmetičkih strana postavke, putem teorije *visinskih funkcija*, koje su veoma korisne u istraživanju pitanja o racionalnim tačkama krivih i površi. Svakom razlomku $x = a/b$, gdje su a i b uzajamno prosti cijeli brojevi, možemo pridružiti njegovu visinu $h(x)$, koja je mjera njegove aritmetičke složenosti – visina nam otprilike govori koliko cifara nam je potrebno da zapišemo brojeve a i b. Slično tome, visina racionalne tačke na krivoj ili površi govori nam o broju cifara potrebnom za zapis njenih koordinata. Primjera radi, $(3,5)$ i $(1749/1331, -1861/1331)$ jesu racionalne tačke veoma različite složenosti na krivoj $y^2 = x^3 - x + 1$, dok $(2,\sqrt{7})$ nije racionalna tačka. Takođe možemo pridružiti visinu svakoj eliptičkoj krivoj ili Abelovoj površi i tako mjeriti njenu aritmetičku složenost u cjelini. Postoji slutnja o određenoj vezi između ovih dvaju visina, koju istražujemo u slučaju gorenavedene postavke. Dokazujemo da spomenuta veza važi za površi $E \times \widetilde{E}$ ako i samo ako važi za površi $\mathrm{Jac}(C)$.

Acknowledgements

I wish to express my deep gratitude to the following people, without whom this work would not be what it is:

Robin de Jong and Fabien Pazuki – for their guidance and their admirable patience;

The reading committee – for their time and their precious comments;

Yuri Bilu and Bas Edixhoven – for looking after me;

The staff at the universities of Leiden, Bordeaux, and Copenhagen – for providing the atmosphere that made this work possible;

Christopher Niesen – for doing an absolutely impeccable job and helping me deal with the complexities of French administration;

Ariyan Javanpeykar, Barinder Banwait and Ronald van Luijk – for the fruitful discussions;

Junjiang and Albert – for their friendship and companionship;

Pınar, Dino, Abtien, Valerio, Iuliana, and Maarten – for all the great times we have had and all the support they have given me;

Milan, Petar, Vuk, Luka, and Ilija – for being my friends and remaining so in spite of the distance;

Anđela – for all the years, happy and sad, and for making me apply to the Algant programme in the first place;

My family – for their love and support.

Curriculum vitae

Martin Djukanović was born in Nikšić, Yugoslavia on 3 March 1988.

In 2006, he graduated from the "Stojan Cerović" gymnasium, Nikšić, and subsequently enrolled in the Faculty of Mathematics and Natural Sciences at the University of Montenegro, Podgorica, where he obtained a B. Sc. degree in mathematics and computer science.

In 2009, he took part in the Algant programme, an Erasmus Mundus master programme that is focused on algebra, geometry and number theory, and spent his time between Universiteit Leiden and Université de Bordeaux. He obtained a M. Sc. degree after defending his master's thesis, titled *Amoebas and Coamoebas in Dimension 2* and completed under the supervision of Prof. Alain Yger.

In 2012, he started his Ph. D. studies within the Algant-Doc programme, which were also completed between the universities of Leiden and Bordeaux. His work on the Ph. D. thesis was carried out under the joint supervision of professors Robin de Jong and Fabien Pazuki.

He currently holds a one year postdoctoral research position at Universität Ulm.

Every August, Martin spends time at the annual Summer School of Science at Ivanova Korita, Montenegro, which is focused on popularizing science among the youth.

Errata

Errata for the officially submitted version, added on 15 November 2017:

Pages 48, 49

The statements of Propositions 1.6 and 1.7 should be swapped.

In the proofs of Propositions 1.6 and 1.7 the two elliptic curves should be assumed more generally to be quadratic twists and not necessarily isomorphic over K. The proofs then require obvious modifications.