Split Jacobians and Lower Bounds on Heights

Djukanovic, M.

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

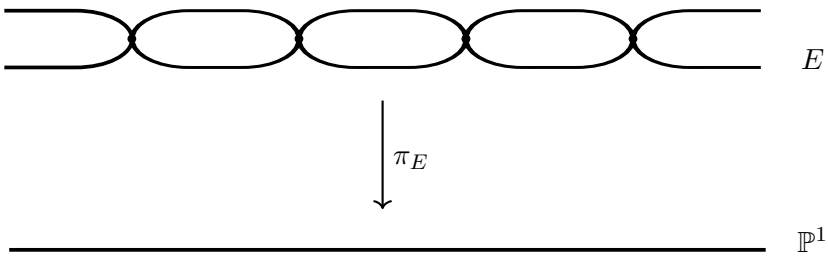


Figure 1.1: A genus one curve as a double cover of the projective line with the ramification points marked.

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.

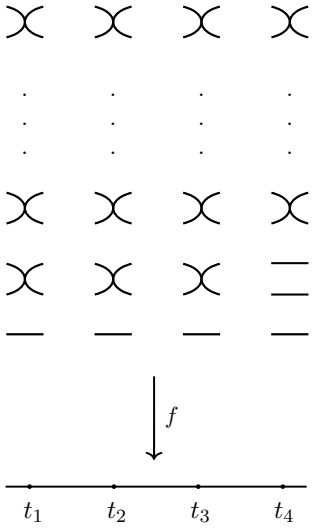
Suppose n is even. We consider each case separately. In case (1), we have that $t_1+t_2+t_3$ is the image of $w_1+\cdots+w_6$ under f and is therefore K-rational, which implies that t_4 is K-rational. In case (2), the argument is analogous to the one above, for odd n, and shows that t_4 and t_3 are K-rational.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

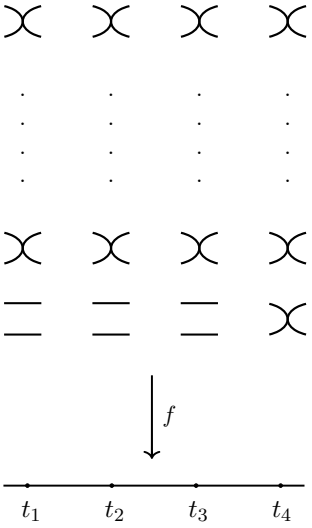
Proof In the generic case, the fibre $f^{-1}(t_0)$ is the unique one containing a single ramification point and none of the w_i. In the special case, the special point is the unique point with ramification index ≥ 3. Thus the absolute Galois action fixes the special point in both cases. □

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.

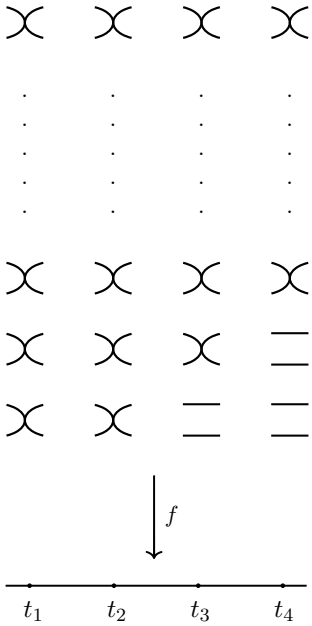
Remark 1.6 Corollary 1.4 shows that the covering $\phi\colon C \to E$ induces a structure of an elliptic curve on E where T_4 is the identity element of the group structure.



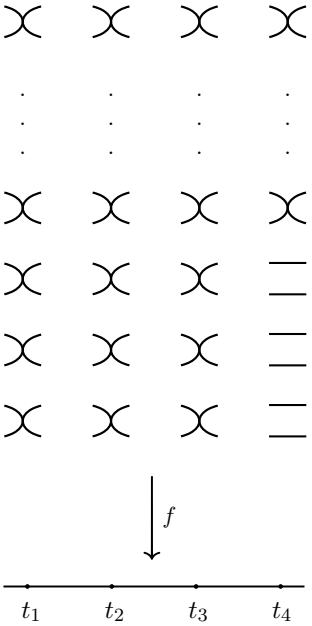
odd degree



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).

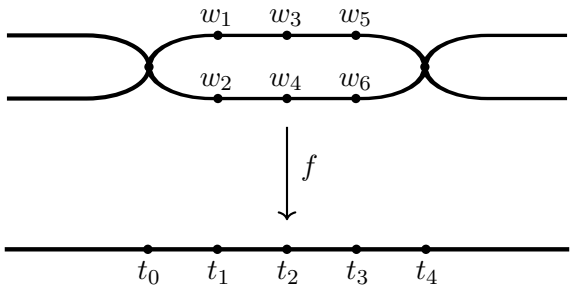


Figure 1.3: Ramification of f when $\deg f = 2$.

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

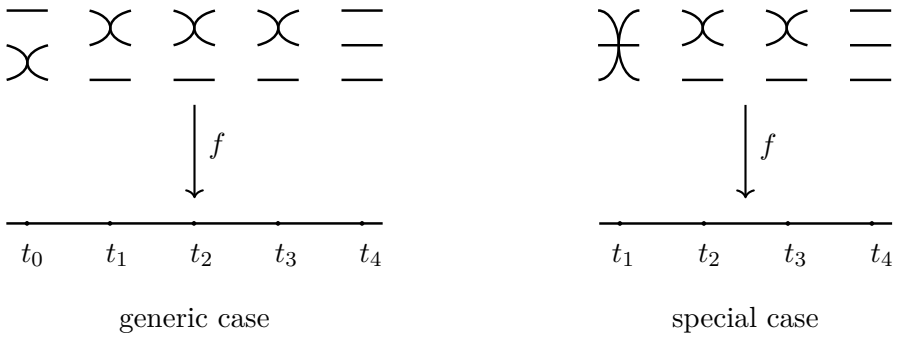


Figure 1.4: Ramification of f when $\deg f = 3$.

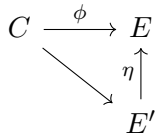
Proposition 1.1 *A given finite separable map $f\colon \mathbb{P}^1 \to \mathbb{P}^1$ with ramification as described in Theorem 1.3 lifts to a finite separable map $\phi\colon C \to E$ that makes the diagram* (1.2) *commute. Moreover, the curves C and E are unique up to isomorphisms and the map ϕ is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

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

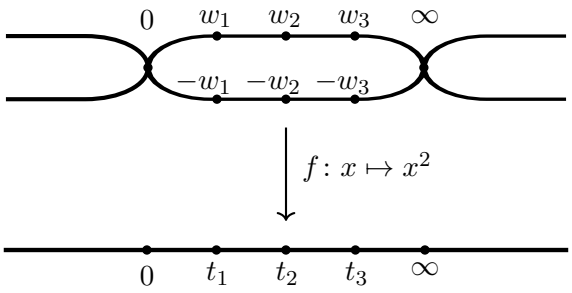


Figure 1.5: Ramification of $f\colon \mathbb{P}^1 \to \mathbb{P}^1$

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 $c \neq 0$.

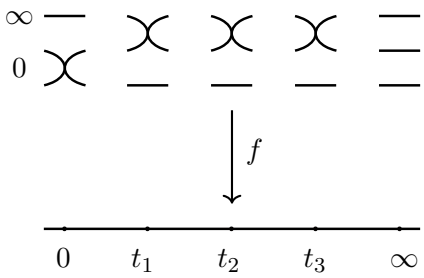
The curve C has an extra automorphism $\sigma\colon (x, y) \mapsto (-x, y)$, which, along with the hyperelliptic involution ι, generates a Klein four-group. Then, taking quotients, we have $C/_{\sigma} \cong E$ and $C/_{\sigma \circ \iota} \cong \widetilde{E}$.

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 $P(x) = x^3 + ax^2 + bx + c$.

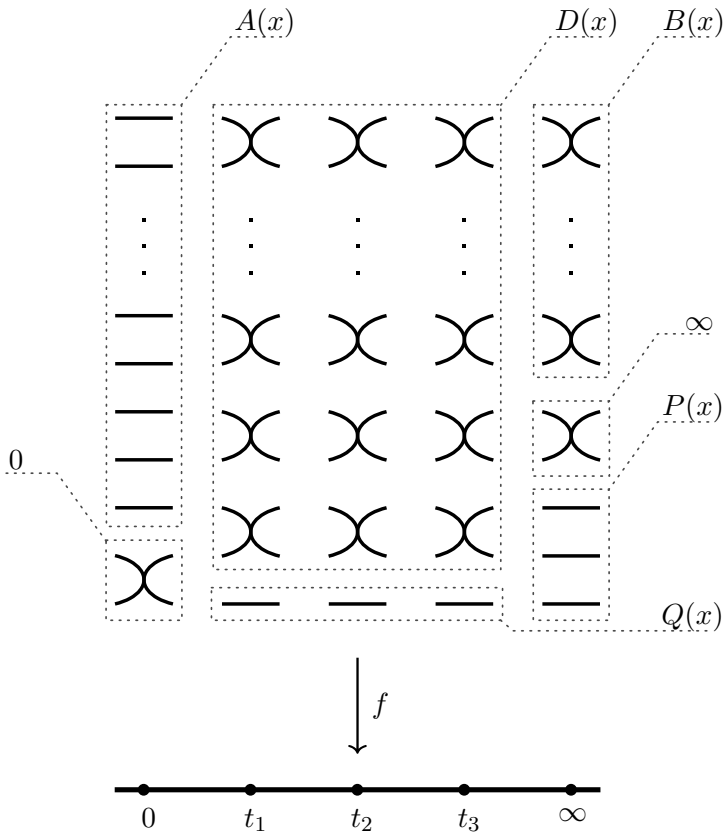


Figure 1.6: Ramification of f in the case of odd degree.

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

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

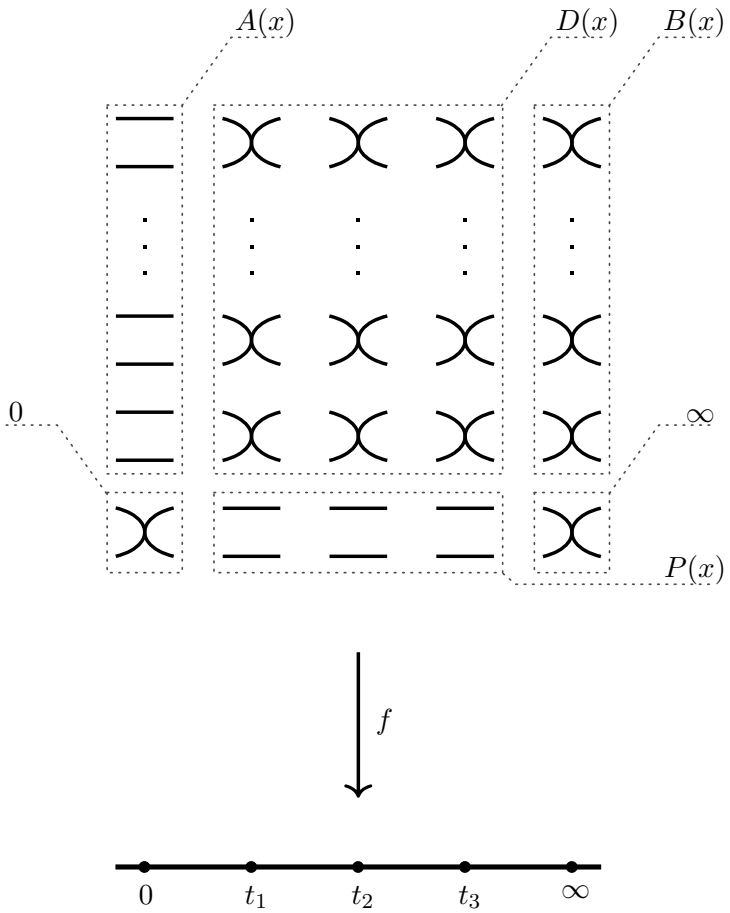


Figure 1.7: Ramification of f in the case of even degree.

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. □

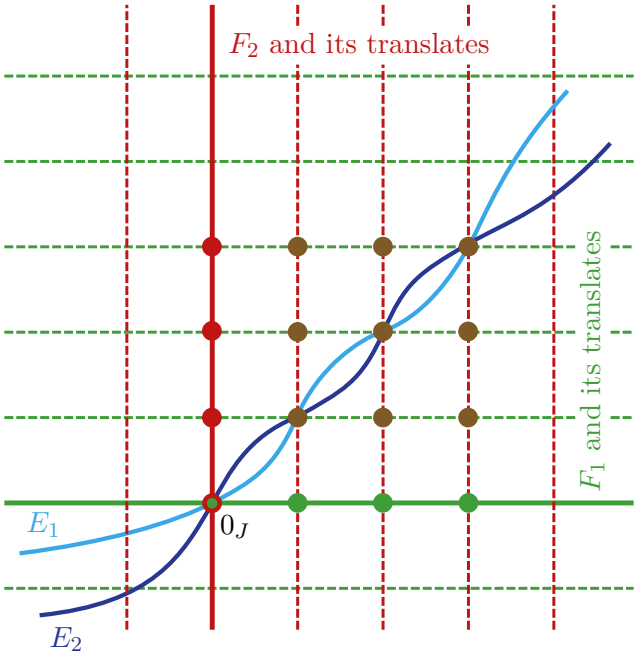


Figure 1.8: An illustration of E_1 and E_2 glued along 2-torsion inside $J \cong F_1 \times F_2$; the marked points denote $J[2]$.

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.

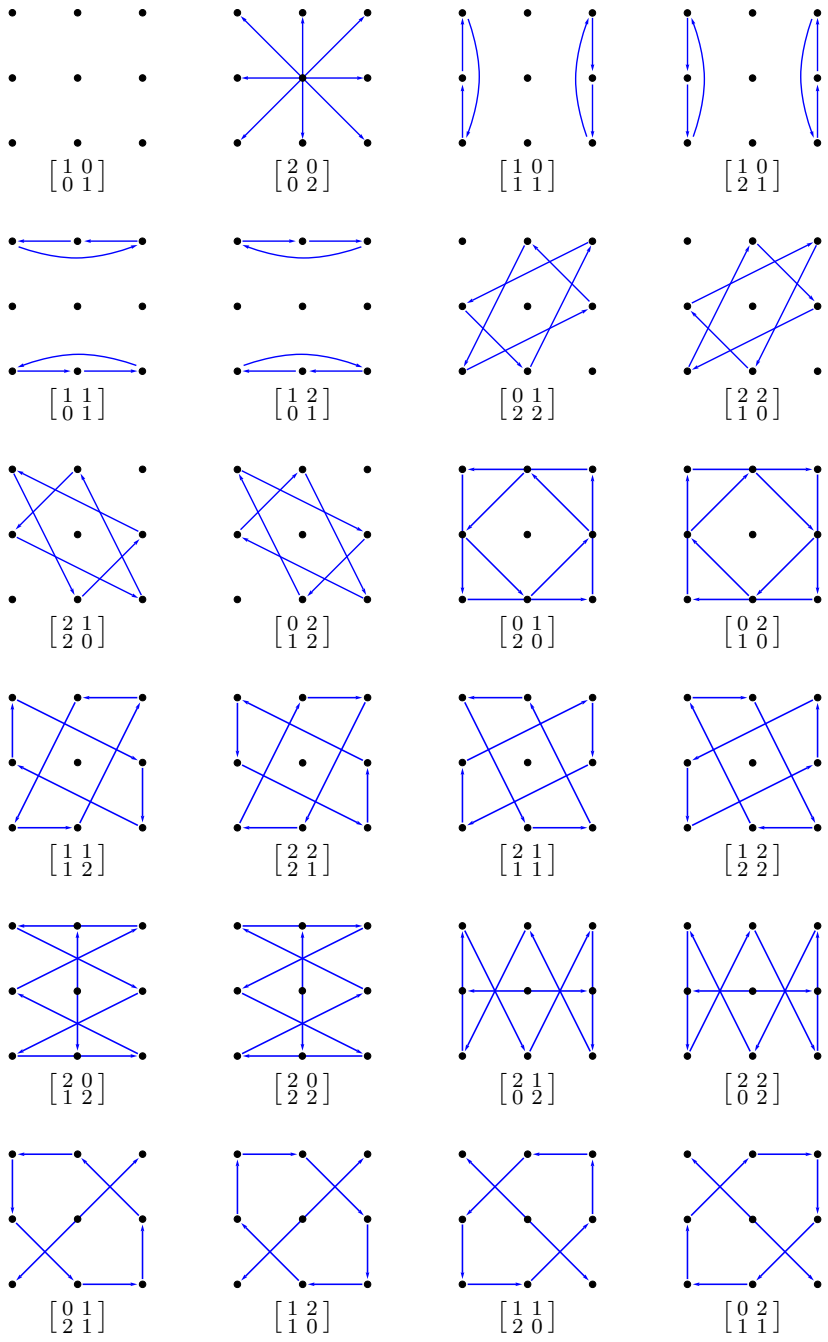


Figure 1.9: Normal subgroup $\mathrm{SL}_2(\mathbf{Z}/3\mathbf{Z})$

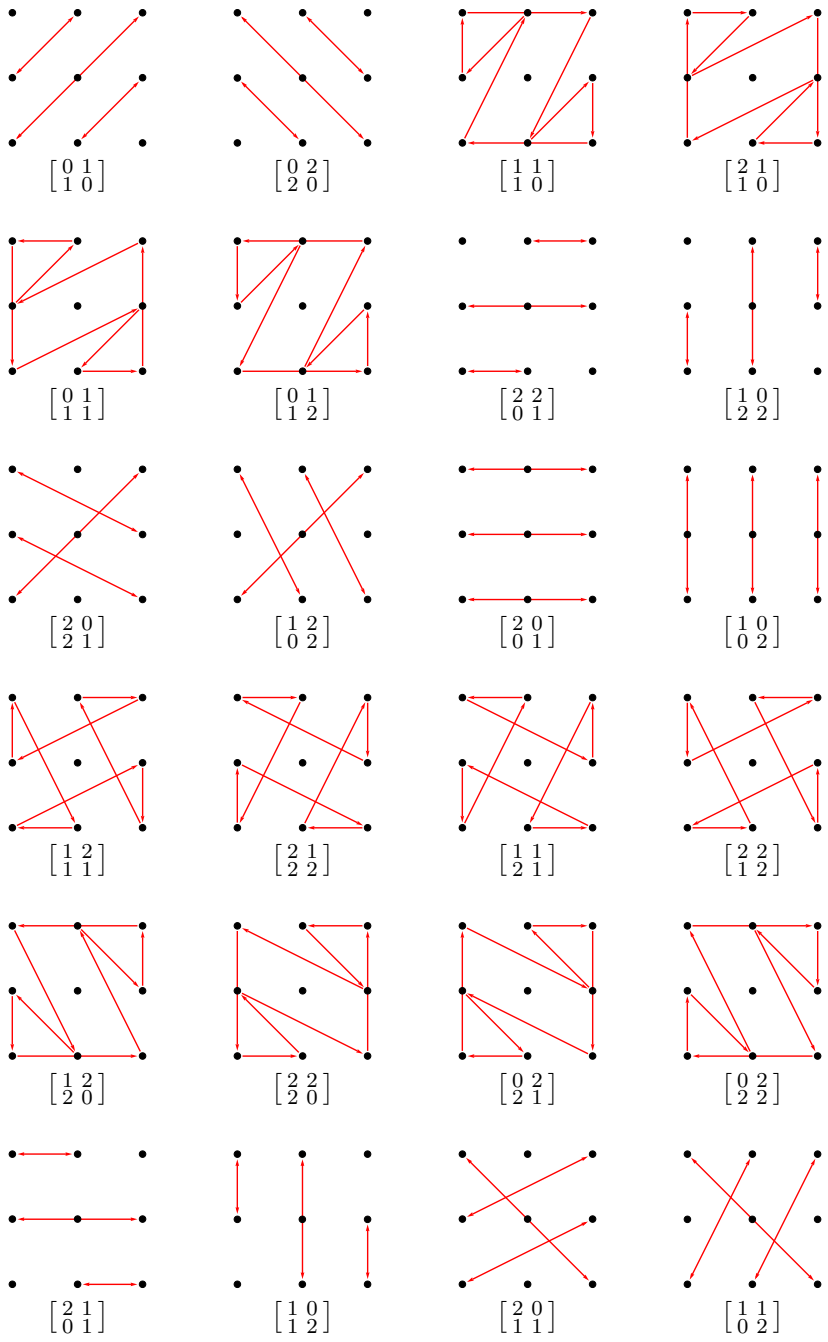


Figure 1.10: Coset $\left[\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right]\mathrm{SL}_2(\mathbf{Z}/3\mathbf{Z})$

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).