ETH Zürich

Master Thesis

Hyperelliptic curves with many automorphisms

by

Nicolas David Müller

supervised by

Prof. Dr. Richard Pink

April 2017

Introduction

A smooth projective complex algebraic curve X of genus $g \geq 2$ is said to have *many automorphisms* if every deformation of X together with its automorphism group is trivial. Previous work on curves with many automorphisms includes papers by Rauch [Rau70], Popp [Pop72], Wolfart [Wol97], [Wol00], and Streit [Str01]. In [Wol00], among other results, the curves with many automorphisms up to genus four are classified. Furthermore, for each of these curves X of genus up to four, Wolfart determines if the Jacobian variety $\mathrm{Jac}(X)$ has complex multiplication. Related work also includes papers by Shaska [Sha04], [Sha06], and Sevilla and Shaska [SS07]. In [Sha06], Shaska determines equations of hyperelliptic curves with a given automorphism group and branching type.

In this thesis, with Theorem 5.4, we give a classification, up to isomorphism, of the curves with many automorphisms that are hyperelliptic. There are three infinite families, two of which have one curve each for each genus $g \geq 2$, and one of which has one curve for each genus $g \geq 3$. Furthermore, there are 15 hyperelliptic curves with many automorphisms which do not belong to the infinite families. For each hyperelliptic curve with many automorphisms, we try to determine whether its Jacobian variety $\mathrm{Jac}(X)$ has complex multiplication. This is achieved for all but five of the curves.

Furthermore, with Theorem 10.25, we give a necessary and sufficient criterion, based on the construction of an n-pointed stable curve of genus zero, to decide whether the Jacobian of a hyperelliptic curve defined over a number field has potential good reduction at a given prime with residue characteristic > 2. The proof is based on the characterization of a semi-stable model of the curve presented in a paper by Bosch [Bos80].

This thesis is organized as follows: In Section 1, we review parts of equivariant deformation theory that are needed in Section 2. In Section 2, we give several equivalent characterizations of curves with many automorphisms. In Section 3, we review some results about hyperelliptic curves that are needed in the remainder of the thesis. In Section 4, we give a necessary and sufficient criterion for a hyperelliptic curve to have many automorphisms. In Section 5, we apply this criterion to find, up to isomorphism, all hyperelliptic curves with many automorphisms. In Section 6, we introduce a method for finding genus one curves that are quotients of a given hyperelliptic curve, which we use in Section 9. In Section 7, we review some results from the theory of abelian and semi-abelian varieties and complex multiplication. In Section 8, we mostly determine the characters of the representations of the automorphism groups of the curves found in Section 5 on their spaces of global holomorphic 1-forms. In Section 9, we apply the methods from Section 6 and the results from Section 8 to determine, for most of the hyperelliptic curves with many automorphisms, whether the Jacobian variety has complex multiplication. Finally, in Section 10, we give a criterion to determine if the Jacobian variety of a hyperelliptic curve over a number field has potential good reduction in characteristic > 2.

Acknowledgments First and foremost, I would like to thank Professor Richard Pink for dedicating many hours to supervise me and making many helpful suggestions. I feel that, with his help, I have learned much about algebraic geometry and mathematical writing in the last months. I also would like to thank the ETH Zürich and the German Academic Scholarship Foundation for supporting me financially.

Contents

1. Equivariant deformations

Notation 1.1. For an algebraic curve X over a field K, we denote by $\mathrm{Aut}_K(X)$ the automorphism group of X over K. If the field K is clear from the context, we sometimes write $\mathrm{Aut}(X)$ instead of $\mathrm{Aut}_K(X)$. For a smooth projective complex algebraic curve X, we denote by Ω_X the sheaf of holomorphic 1-forms on X, and by Θ_X the tangent sheaf. Because Ω_X and Θ_X are invertible, they are coherent. For $n \in \mathbb{Z}_{\geq 1}$, we denote by C_n the cyclic group of order n, by D_n the dihedral group of order $2n$, by S_n the symmetric group on n points and by A_n the alternating group on n points. For a scheme S over a ring R and some ring R' with a morphism $\mathrm{Spec}(R') \to \mathrm{Spec}(R)$, we define $S_{R'} := S \times_{\mathrm{Spec}(R)} \mathrm{Spec}(R')$. For a number field K, we denote by $\mathcal{O}_K$ its ring of integers. For any field K, we denote by $K^\times$ its multiplicative group. Suppose that R is a discrete valuation ring (DVR) with fraction field K and corresponding discrete valuation $v : K \to \mathbb{Z} \cup \{\infty\}$. Then we denote by $\hat{K}$ the completion of K with respect to v and by $\hat{R}$ the corresponding DVR of $\hat{K}$. For a graph G, we denote by $V(G)$ and $E(G)$ the vertex set and the edge set, respectively.

Definition 1.2. Let G be a group, let X_1, X_2 be sets and suppose that G acts on X_1 and X_2. A map $f : X_1 \to X_2$ is called *G-equivariant* if

$$\forall x \in X_1\, \forall g \in G : f(gx) = gf(x).$$

We follow Chapter 3.2.b of [Bys09]. For an introduction to deformation theory see also [Ser06]. Let K be an algebraically closed field, let $\mathcal{C}$ denote the category of local Artinian rings with residue field K. The morphisms of $\mathcal{C}$ are the local ring homomorphisms between the objects of $\mathcal{C}$. Let Set denote the category of sets. Let X be a smooth scheme over K, let G be a finite group and let $\rho : G \to \mathrm{Aut}_K(X)$ be a faithful action of G on X.

Definition 1.3 (Definition 3.2.5 in [Bys09])**.** A *lift* of the pair (X, ρ) to an object A of $\mathcal{C}$ is a triple (X_A, ρ_A, i), where X_A is a flat scheme over $\mathrm{Spec}(A)$ and $\rho_A : G \to \mathrm{Aut}_A(X_A)$ is a homomorphism and $i : X \to X_A$ is a G-equivariant K-morphism inducing an isomorphism $X \to X_A \times_{\mathrm{Spec}(A)} \mathrm{Spec}(K)$.

Two lifts (X_A, ρ_A, i) and (X'_A, ρ'_A, i') are called *equivalent* if there exists a G-equivariant isomorphism $\varphi : X_A \to X'_A$ over A such that $\varphi \circ i = i'$.

The following definition partly follows Definition 3.2.6 in [Bys09] and page 21 in [Ser06].

Definition 1.4. The covariant *infinitesimal deformation functor* of the pair (X, ρ) is defined by

$$\begin{aligned} D_{X,G} : \mathcal{C} &\to \mathrm{Set} \\ A &\mapsto \{\text{lifts of } (X, \rho) \text{ to } A\} / \sim, \end{aligned}$$

where $\sim$ denotes the equivalence relation on lifts. On the morphisms of $\mathcal{C}$, the functor is defined as follows: Let $f : A \to B$ be a morphism of $\mathcal{C}$ and let (X_A, ρ_A, i) be a lift of (X, ρ) to A.

$$\begin{array}{ccc} X & \xrightarrow{\;i\;} & X_A \\ \downarrow & & \downarrow \\ \operatorname{Spec}(K) & \longrightarrow & \operatorname{Spec}(A) \end{array}$$

Then, there is an induced lift (X_B, ρ_B, j) of (X, ρ) to B given as follows:

$$\begin{array}{ccc} X & \xrightarrow{\;j\;} & X_A \times_{\operatorname{Spec}(A)} \operatorname{Spec}(B) =: X_B \\ \downarrow & & \downarrow \\ \operatorname{Spec}(K) & \longrightarrow & \operatorname{Spec}(B) \end{array}$$

We define $X_B := X_A \times_{\operatorname{Spec}(A)} \operatorname{Spec}(B)$. The morphism j is the unique morphism induced by the universal property of the fiber product $X_A \times_{\operatorname{Spec}(A)} \operatorname{Spec}(B)$. The map ρ_B is constructed as follows: The universal property of the fiber product induces a homomorphism $\psi : \operatorname{Aut}_A(X_A) \to \operatorname{Aut}_B(X_B)$. We define $\rho_B := \psi \circ \rho_A$. It is G-equivariant. The image of the morphism $f : A \to B$ under $D_{X,G}$ is now defined as the map

$$\begin{aligned} \{\text{lifts of } (X,\rho) \text{ to } A\} / \sim &\to \{\text{lifts of } (X,\rho) \text{ to } B\} / \sim \\ (X_A, \rho_A, i) &\mapsto (X_A \times_{\operatorname{Spec}(A)} \operatorname{Spec}(B), \rho_B, j), \end{aligned}$$

where ρ_B and j are as constructed above. This is well-defined since equivalent lifts to A induce equivalent lifts to B. Since the identity morphism $\operatorname{id} : A \to A$ induces the identity map on the equivalence classes of lifts and the construction respects compositions of morphisms of $\mathcal{C}$, we see that $D_{X,G}$ is a covariant functor.

Definition 1.5. The *tangent space* of $D_{X,G}$ is $t_{D_{X,G}} := D_{X,G}(K[\epsilon]/\epsilon^2)$.

Remark 1.6. By Proposition 1.2.2 in [Bys09], the tangent space $t_{D_{X,G}}$ can be endowed with a canonical K-vector space structure.

Remark 1.7. Let X' be a smooth scheme over K and let $\rho' : G' \to \operatorname{Aut}_K(X')$ be a faithful action of a finite group G' on X'. Suppose that $\eta : D_{X,G} \to D_{X',G'}$ is a natural transformation. By Theorem 3.2.4 in [Bys09] and Remark 1.2.3 in [Bys09], the natural transformation η induces a K-linear map

$$\eta_{K[\epsilon]/\epsilon^2} : t_{D_{X,G}} \to t_{D_{X',G'}}$$

on the tangent spaces.

Proposition 1.8. *Suppose that X is a smooth curve over K of genus $g \geq 2$. Then $D_{X,G}$ is pro-representable.*

Proof. The proof is analogue to the proof of Théorème 2.1 in [BM00], where it is proved in positive characteristic. □

Definition 1.9 (see page 9 in Section 1.1.1 and Definition 1.1.3 in [Ser06])**.** Let A be a ring, let R be an A-algebra and let I be an R-module. An *A-extension of R by I* is a short exact sequence

$$(R', \varphi): \quad 0 \to I \to R' \xrightarrow{\varphi} R \to 0,$$

where R' is an A-algebra and φ is a homomorphism of A-algebras whose kernel I is an ideal of R' satisfying $I^2 = (0)$. For every A-algebra R and for every R-module I we let $\mathrm{Ex}_A(R, I)$ denote the set of A-extensions of R by I.

Fact 1.10. *We can define an R-module structure on $\mathrm{Ex}_A(R, I)$. For the construction see Section 1.1.2 in [Ser06].*

Definition 1.11 (see Section 2.1 in [Ser06])**.** For any object A of $\mathcal{C}$, we call $\mathrm{Ex}_K(A, K)$ the *obstruction space* of A.

Definition 1.12 (see Definition 2.2.9 in [Ser06])**.** Suppose that V is a K-vector space such that for every object A of $\mathcal{C}$ and for every $\xi \in D_{X,G}(A)$ there is a K-linear map

$$\xi_V : \mathrm{Ex}_K(A, K) \to V$$

with the following property: The kernel $\ker(\xi_V)$ consists of isomorphism classes of extensions $(\tilde{A}, \varphi) \in \mathrm{Ex}_K(A, K)$ such that

$$\xi \in \mathrm{Im}[D_{X,G}(\tilde{A}) \to D_{X,G}(A)].$$

Then V is called an *obstruction space* for the functor $D_{X,G}$. If $D_{X,G}$ has 0 as an obstruction space, then it is called *unobstructed*.

To compute the tangent space and an obstruction space of $D_{X,G}$, we need equivariant sheaf cohomology, which was introduced by Grothendieck in Section 5.2 in [Gro57].

Proposition 1.13.

1. *The equivariant sheaf cohomology $H^1(X; G, \Theta_X)$ is the tangent space to $D_{X,G}$.*
2. *The equivariant sheaf cohomology $H^2(X; G, \Theta_X)$ is an obstruction space to $D_{X,G}$.*

Proof. See Proposition 3.2.7 in [Bys09]. □

Proposition 1.14. *Suppose that $D_{X,G}$ is unobstructed. Let A^{univ} be the ring underlying the universal formal deformation given by Proposition 1.8 and let $d = \dim t_{D_{X,G}}$. Then*

$$A^{\mathrm{univ}} \cong K[x_1, \ldots, x_d].$$

Proof. It follows from the paragraph after Definition 2.2.9 in [Ser06] that the obstruction space to A^{univ}, as in Definition 1.11, is isomorphic to the obstruction space of $D_{X,G}$. Because the tangent spaces of A^{univ} and $D_{X,G}$ are isomorphic, Corollary 2.2.11 in [Ser06] now tells us that $\dim A^{\mathrm{univ}} = d$. Because $D_{X,G}$ is unobstructed, we have

$$A^{\mathrm{univ}} \cong K[x_1, \ldots, x_d]$$

by Proposition 2.1.1.(ii) in [Ser06]. □

2. Curves with many automorphisms

Let X be a smooth projective complex algebraic curve of genus $g \geq 2$.

Definition 2.1. The curve X is said to have *many automorphisms* if $D_{X,\mathrm{Aut}(X)}(A)$ is trivial for all $A \in \mathcal{C}$.

Theorem 2.2. *The following categories are equivalent:*

1. *The category of smooth projective complex algebraic curves.*

2. *The category of compact Riemann surfaces.*

3. *The category of field extensions of transcendence degree one over $\mathbb{C}$, with arrows reversed.*

Proof. See Theorem 4.2.9 in [Nam84]. □

Theorem 2.3 (Serre)**.** *Let X^{an} denote the compact Riemann surface associated to X by Theorem 2.2. Then the category of coherent schemes on X is equivalent to the category of coherent analytic schemes on X^{an}.*

Proof. This is an instance of Serre's GAGA principle. See for example Theorem 2.1 in Appendix B in [Har77]. □

Lemma 2.4. *Let $G < \mathrm{Aut}(X)$. Then, for any $n \geq 0$, we have $H^n(X; G, \Theta_X) \cong H^n(X, \Theta_X)^G$.*

Proof. We transfer the problem to the category of compact Riemann surfaces by Theorem 2.2 and Theorem 2.3. Then, the group G acts discontinuously on X by homeomorphisms. Therefore, we obtain from the first corollary to Théorème 5.3.1 in [Gro57] and the following paragraph that $H^q(G, \Theta_X) = 0$ for $q > 0$. Because G is finite and we are working in characteristic 0, the conclusion is obtained from the corollary to Proposition 5.2.3 in [Gro57]. □

Definition 2.5. A branched covering $\beta : X \to \mathbb{P}^1_{\mathbb{C}}$ with at most three branch points is called a *Belyĭ function*.

Proposition 2.6. *The following are equivalent:*

(i) The curve X has many automorphisms.

(ii) We have $H^1(X, \Theta_X)^{\mathrm{Aut}(X)} = 0$.

(iii) We have $H^0(X, \Omega_X^{\otimes 2})^{\mathrm{Aut}(X)} = 0$.

(iv) There exists a Belyĭ function $\beta : X \to \mathbb{P}^1_{\mathbb{C}}$ that defines a normal cover.

Proof. (i)$\Longleftrightarrow$(ii): Let $G := \mathrm{Aut}(X)$. By Lemma 2.4, we have $H^1(X; G, \Theta_X) \cong H^1(X, \Theta_X)^G$ and $H^2(X; G, \Theta_X) \cong H^2(X, \Theta_X)^G$. But $H^2(X, \Theta_X) = 0$, because the dimension of X is one. Therefore, by Proposition 1.13, it follows that $D_{X,G}$ is unobstructed and of dimension $d := \dim t_{D_{X,G}} = \dim H^1(X, \Theta_X)^G$. By Proposition 1.14, we have $A^{\mathrm{univ}} \cong \mathbb{C}[x_1, \dots, x_d]$, where A^{univ} is the universal deformation of $D_{X,G}$. Since for every $A \in \mathcal{C}$ we have

$$D_{X,G}(A) \cong \mathrm{Mor}_{\mathbb{C}\text{-alg.}}(A^{\mathrm{univ}}, A),$$

it follows that $\dim D_{X,G}(A) = 0 \Leftrightarrow d = 0$.

(ii)$\Longleftrightarrow$(iii): Since $\Theta_X^\vee = \Omega_X$, by Serre duality we have

$$H^1(X, \Theta_X) \cong H^0(X, \Omega_X^{\otimes 2})^\vee$$

and this isomorphism is $\mathrm{Aut}(X)$-equivariant. The representation of $\mathrm{Aut}(X)$ on $H^0(X, \Omega_X^{\otimes 2})^\vee$ has nonzero fixed points if and only if the dual representation on $H^0(X, \Omega_X^{\otimes 2})$ has nonzero fixed points.

(i)$\Longleftrightarrow$(iv): See Theorem 6 in [Wol97]. □

Remark 2.7. Belyĭ's Theorem 4 in [Bel83] states that X can be defined over a number field if and only if X admits a Belyĭ function. Therefore, by Proposition 2.6, every curve with many automorphisms can be defined over a number field.

3. Hyperelliptic curves

Definition 3.1. A smooth projective algebraic curve $X$of genus $g \geq 2$ over a field K of characteristic 0 is called *hyperelliptic* if there is a finite morphism $\pi : X \to \mathbb{P}^1_K$ of degree 2, called the *hyperelliptic double cover.*

Let X be a complex hyperelliptic curve of genus g.

Proposition 3.2. *The morphism $\pi : X \to \mathbb{P}^1_{\mathbb{C}}$ of degree 2 is unique up to automorphisms of $\mathbb{P}^1_{\mathbb{C}}$.*

Proof. See Theorem III.7.3 in [FK92]. □

Proposition 3.3. *A complex algebraic curve is hyperelliptic if and only if it is the projective completion of an affine curve of the form*

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

where f is a separable polynomial of degree $\deg f \geq 5$.

Proof. See Proposition 4.11 in Chapter III of [Mir95]. □

Remark 3.4. If, in affine coordinates, the curve X is given by $y^2 = f(x)$, the double cover $\pi : X \to \mathbb{P}^1_{\mathbb{C}}$, in affine coordinates, is given by

$$(x, y) \mapsto x.$$

Proposition 3.5. *Suppose that X is given by $y^2 = f(x)$. Then $\deg f = 2g + 2$ or $\deg f = 2g + 1$. If $\deg f = 2g + 2$, the branch points of the double cover π are the roots of f. If $\deg f = 2g + 1$, then the branch points of π are the roots of f and the point $\infty \in \mathbb{P}^1_{\mathbb{C}}$.*

Proof. See Lemma 1.7 in Chapter III of [Mir95]. □

Definition 3.6. The ramification points $P_1, \dots, P_{2g+2} \in X$ of the double cover π are called the *Weierstrass points* of X. We denote the set of the images of the Weierstrass points under π by

$$W(X) := \{\pi(P_1), \dots, \pi(P_{2g+2})\}.$$

Proposition 3.7. *There is a unique involution in $\mathrm{Aut}(X)$, denoted by σ and called the hyperelliptic involution, that fixes exactly the Weierstrass points of X. It is the unique involution of X with $2g + 2$ fixed points. Furthermore, the hyperelliptic involution is in the center of $\mathrm{Aut}(X)$.*

Proof. Corollary 1 and 2 and 3 in III.7.9. in [FK92]. □

Corollary 3.8. *The hyperelliptic double cover $\pi : X \to \mathbb{P}^1_{\mathbb{C}}$ is the quotient map $X \to X/\langle\sigma\rangle \cong \mathbb{P}^1_{\mathbb{C}}$, up to a change of coordinates of $\mathbb{P}^1_{\mathbb{C}}$.*

Proof. The quotient map $f : X \to X/\langle\sigma\rangle$ is of degree 2, because σ has order 2. The ramification points of f are exactly the fixed points of σ. Therefore, by Proposition 3.7 and Proposition 3.2, the maps f and π are equal up to an automorphism of $\mathbb{P}^1_{\mathbb{C}}$. $\square$

Definition 3.9. We call $\overline{\mathrm{Aut}}(X) := \mathrm{Aut}(X)/\langle\sigma\rangle$ the *reduced automorphism group* of X.

In the following, we will identify $\overline{\mathrm{Aut}}(X)$ with its image in $\mathrm{Aut}(\mathbb{P}^1_{\mathbb{C}})$. This is possible by Corollary 3.8.

Proposition 3.10. *Each finite subgroup of* $\mathrm{Aut}(\mathbb{P}^1_{\mathbb{C}}) \cong \mathrm{PGL}_2(\mathbb{C})$ *is isomorphic to one of* C_n, D_n, A_4, S_4 *and* A_5 *for some* $n \in \mathbb{Z}_{\geq 1}$, *and any two finite isomorphic subgroups of* $\mathrm{Aut}(\mathbb{P}^1_{\mathbb{C}})$ *are conjugate to each other.*

Proof. See Chapter III in [Bli17]. $\square$

Because $g \geq 2$, the groups $\mathrm{Aut}(X)$ and $\overline{\mathrm{Aut}}(X)$ are finite. Therefore we have:

Corollary 3.11. *The reduced automorphism group* $\overline{\mathrm{Aut}}(X)$ *is isomorphic to one of the groups listed in Proposition 3.10.*

Proposition 3.12. *The reduced automorphism group* $\overline{\mathrm{Aut}}(X)$ *is the maximal subgroup of* $\mathrm{Aut}(\mathbb{P}^1_{\mathbb{C}})$ *that acts on* $W(X)$. *That is:*

$$\overline{\mathrm{Aut}}(X) = \left\{\overline{T} \in \mathrm{Aut}(\mathbb{P}^1_{\mathbb{C}}) \;\middle|\; \overline{T}W(X) = W(X)\right\}.$$

Proof. Let T be an automorphism of X. Then T permutes the ramification points of the hyperelliptic double cover π. Therefore, the image $\overline{T}$ of T in $\overline{\mathrm{Aut}}(X)$ acts as a permutation on $W(X)$. Conversely, by Lemma 2 in [Tsu58], any automorphism $\overline{S}$ of $\mathrm{Aut}(\mathbb{P}^1_{\mathbb{C}})$, which permutes $W(X)$, can be lifted to an automorphism of X. $\square$

Finally, we will also use the following:

Proposition 3.13. *Let* Y *be a smooth projective complex algebraic curve of genus* g'. *Then*

$$\dim H^0(Y, \Omega_Y) = g'.$$

Proof. See Proposition III.5.2 in [FK92]. $\square$

4. A criterion for finding the hyperelliptic curves with many automorphisms

Let X be a complex hyperelliptic curve of genus $g \geq 2$.

Theorem 4.1. *If $\overline{\mathrm{Aut}}(X)$ is not cyclic, then X has many automorphisms if and only if the action of $\overline{\mathrm{Aut}}(X)$ on $W(X)$ does not have a free orbit. If $\overline{\mathrm{Aut}}(X)$ is cyclic, then X has many automorphisms if and only if the action of $\overline{\mathrm{Aut}}(X)$ on $W(X)$ has exactly one free orbit.*

We will need the following lemma:

Lemma 4.2. *If $w \in W(X)$, then $|\overline{\mathrm{Aut}}(X)w| = |\overline{\mathrm{Aut}}(X)|$ if and only if w is not a ramification point of $\phi : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}/\overline{\mathrm{Aut}}(X) \cong \mathbb{P}^1_{\mathbb{C}}$.*

Proof. Let $p := \phi(w)$. Then $\overline{\mathrm{Aut}}(X)w = \phi^{-1}(p)$ by the definition of ϕ. Because p is a branch point of ϕ if and only if $|\phi^{-1}(p)| < |\overline{\mathrm{Aut}}(X)|$, the result follows. □

Proposition 4.3. *Let $H < \mathrm{Aut}(X)$, let $\phi : X \to X/H$ be the quotient map and let g_H be the genus of X/H. Let n be the number of branch points of ϕ in X/H. Then*

$$\dim H^0(X, \Omega_X^{\otimes 2})^H = 3g_H - 3 + n.$$

Proof. A point $y \in X/H$ is a branch point of ϕ if and only if its preimages are ramification points of ϕ. The ramification points of ϕ are exactly those for which the point stabilizer in H is nontrivial. The conclusion then follows from Remark in V.2.2 in [FK92]. □

In our case, we will use $H = \mathrm{Aut}(X)$ and therefore $X/H \cong \mathbb{P}^1_{\mathbb{C}}$ and $g_{\mathrm{Aut}(X)} = 0$.

Lemma 4.4. *Let $\phi : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}/\overline{\mathrm{Aut}}(X) \cong \mathbb{P}^1_{\mathbb{C}}$ denote the quotient map. If $\overline{\mathrm{Aut}}(X)$ is not cyclic, then ϕ has exactly three branch points. If $\overline{\mathrm{Aut}}(X)$ is cyclic and nontrivial, then ϕ has exactly two branch points.*

Proof. See for example §2 in [BS86]. □

Lemma 4.5. *If $\overline{\mathrm{Aut}}(X)$ is trivial, then X does not have many automorphisms.*

Proof. If $\overline{\mathrm{Aut}}(X)$ is trivial, then $\mathrm{Aut}(X)$ is generated by the hyperelliptic involution and the quotient map $X \to X/\mathrm{Aut}(X)$ has $2g + 2$ branch points. Then X cannot have many automorphisms, because by Proposition 4.3 we would need

$$0 = \dim H^0(X, \Omega_X^{\otimes 2})^{\mathrm{Aut}(X)} = -3 + 2g + 2,$$

which is impossible because $g \in \mathbb{Z}_{\geq 1}$. □

Proof of Theorem 4.1. Denote by $\pi : X \to \mathbb{P}^1_{\mathbb{C}}$ the hyperelliptic double cover and denote by $\phi : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}/\overline{\mathrm{Aut}}(X)$ the quotient map and let

$$\psi := \phi \circ \pi : X \to X/\mathrm{Aut}(X) \cong \mathbb{P}^1_{\mathbb{C}}.$$

We want to use condition (iii) in Proposition 2.6 to determine the hyperelliptic curves that have many automorphisms.

By Lemma 4.5, we may assume that $\overline{\mathrm{Aut}}(X)$ is nontrivial. Let n denote the number of branch points of ψ and let m denote the number of branch points of ϕ.
Claim: Let k be the number of free orbits of $\overline{\mathrm{Aut}}(X)$ in $W(X)$. Then $n = m + k$.

Proof. A point $p \in \mathbb{P}^1_{\mathbb{C}}$ is a branch point of ψ if and only if $|\psi^{-1}(p)| < |\operatorname{Aut}(X)|$. Therefore, the point p is a branch point of ψ if and only if p is a branch point of ϕ or $\phi^{-1}(p) \subseteq W(X)$. We want to show that the branch points of ψ that are not branch points of ϕ correspond precisely to the free orbits of $\overline{\mathrm{Aut}}(X)$ in $W(X)$. If p is not a branch point of ϕ then $\phi^{-1}(p)$ is a free orbit of the action of $\overline{\mathrm{Aut}}(X)$ on $\mathbb{P}^1_{\mathbb{C}}$. Therefore, if p is a branch point of ψ that is not a branch point of ϕ, then $\phi^{-1}(p)$ is a free orbit of $\overline{\mathrm{Aut}}(X)$ in $W(X)$. Conversely, if $\phi^{-1}(p)$ is a free orbit in $W(X)$, then p is a branch point of ψ and p is not a branch point of ϕ, because $|\phi^{-1}(p)| = |\overline{\mathrm{Aut}}(X)|$. □

By Proposition 4.3, we have $\dim H^0(X, \Omega_X^{\otimes 2})^{\operatorname{Aut}(X)} = 0$ if and only if $n = 3$. If $\overline{\mathrm{Aut}}(X)$ is not cyclic, then, by Lemma 4.4, the map ϕ has exactly three branch points. Therefore, by the Claim, we have $n = 3$ if and only if $\overline{\mathrm{Aut}}(X)$ has no free orbits in $W(X)$. If $\overline{\mathrm{Aut}}(X)$ is cyclic, then by Lemma 4.4, the map ϕ has exactly two branch points. Therefore, by the Claim, we have $n = 3$ if and only if $\overline{\mathrm{Aut}}(X)$ has exactly one free orbit in $W(X)$. □

Remark 4.6. For a hyperelliptic curve X of genus g given by

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

a basis of $H^0(X, \Omega_X^{\otimes 2})$ is $\mathcal{B}_1 \cup \mathcal{B}_2$, where $\mathcal{B}_1$ and $\mathcal{B}_2$ are defined by

$$\mathcal{B}_1 := \left\{ \frac{x^k (dx)^2}{y} \;\middle|\; 0 \leq k \leq g-3 \right\},$$
$$\mathcal{B}_2 := \left\{ \frac{x^k (dx)^2}{y^2} \;\middle|\; 0 \leq k \leq 2g-2 \right\}.$$

Furthermore, we have $H^0(X, \Omega_X^{\otimes 2})^{\langle \sigma \rangle} = \operatorname{span}(\mathcal{B}_2)$. For a reference see Section 7 in [Løn80]. Therefore, if $\operatorname{Aut}(X)$ is known, one can compute $H^0(X, \Omega_X^{\otimes 2})^{\operatorname{Aut}(X)}$ by a direct calculation by using the given basis.

5. Calculating the hyperelliptic curves with many automorphisms

To compute equations for the hyperelliptic curves with many automorphisms, we have to choose a conjugacy class for each of the finite subgroups of $\operatorname{Aut}(\mathbb{P}^1_{\mathbb{C}})$ listed in Proposition 3.10.

Definition 5.1. We choose the following coordinates, as in [Sha06], where ξ_n is a primitive nth root of unity and $\omega = \frac{1-\sqrt{5}}{2}$ and ϵ is a primitive fifth root of unity:

$$
\begin{aligned}
C_n &:= \langle x \mapsto \xi_n x \rangle \\
D_n &:= \left\langle x \mapsto \xi_n x,\ x \mapsto x^{-1} \right\rangle \\
A_4 &:= \left\langle x \mapsto -x,\ x \mapsto \frac{x+i}{x-i} \right\rangle \\
S_4 &:= \left\langle x \mapsto ix,\ x \mapsto -\frac{x-1}{x+1} \right\rangle \\
A_5 &:= \left\langle x \mapsto \frac{\omega x + 1}{x - \omega},\ x \mapsto \epsilon x \right\rangle
\end{aligned}
$$

Proposition 5.2. *For each finite subgroup $G < \operatorname{Aut}(\mathbb{P}^1_{\mathbb{C}})$ in the coordinates given in the previous definition and for each non-free orbit A of G in $\mathbb{P}^1_{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$, Table 1 lists a separable polynomial p with $A \cap \mathbb{C}$ as its roots.*

G	Polynomial p	$\infty \in A$
$C_n,\ n > 1$	1	yes
	x	no
$D_n,\ n > 1$	x	yes
	$x^n - 1$	no
	$x^n + 1$	no
A_4	$t_4 := x(x^4 - 1)$	yes
	$p_4 := x^4 + 2i\sqrt{3}x^2 + 1$	no
	$q_4 := x^4 - 2i\sqrt{3}x^2 + 1$	no
S_4	$r_4 := x^{12} - 33x^8 - 33x^4 + 1$	no
	$s_4 := x^8 + 14x^4 + 1$	no
	t_4	yes
A_5	$r_5 := x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1$	no
	$s_5 := x(x^{10} + 11x^5 - 1)$	yes
	$t_5 := x^{30} + 522x^{25} - 10005x^{20} - 10005x^{10} - 522x^5 + 1$	no

Table 1: Non-free orbits of the finite subgroups of $\operatorname{Aut}(\mathbb{P}^1_{\mathbb{C}})$

Proof. Because the non-free orbits of G in $\mathbb{P}^1_{\mathbb{C}}$ are exactly the preimages of the branch points of the quotient map $\phi : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}/G \cong \mathbb{P}^1_{\mathbb{C}}$, we know by Lemma 4.4 that there are two non-free orbits if G is cyclic and three non-free orbits otherwise. To find the points in these orbits, note that a point $P \in \mathbb{P}^1_{\mathbb{C}}$ is in a non-free orbit of G if and only if the stabilizer G_P of P is nontrivial. Therefore, it suffices to calculate fixed points of elements of G and their orbits under the action of G until we have found enough non-free orbits.

1. For the case $G = C_n$, for $n \in \mathbb{Z}_{\geq 1}$, clearly the points 0 and ∞ are fixed points of the whole group. Therefore, we already found all non-free orbits of G.

2. For the case $G = D_n$, we see by a direct calculation that $\{0, \infty\}$ and $\left\{\xi_n^1, \ldots, \xi_n^n\right\}$ and $\left\{\zeta\xi_n^1, \ldots, \zeta\xi_n^n\right\}$, where $\zeta \in \mathbb{C}$ is chosen such that such that $\zeta^n = -1$, are three distinct non-free orbits.

3. If $G \in \{A_4, S_4, A_5\}$, see the calculation in GAP [GAP17] in Appendix B.1.

□

Lemma 5.3. *Let $G < \operatorname{Aut}(\mathbb{P}^1_{\mathbb{C}})$ be finite. If G fixes a point $p \in \mathbb{P}^1_{\mathbb{C}}$, then G is cyclic.*

Proof. After a change of coordinates, we may assume that $p = \infty$. Then we can embed $G \hookrightarrow \operatorname{Aut}(\mathbb{C})$ by restricting the action of G, where $\operatorname{Aut}(\mathbb{C})$ denotes the automorphism group of $\mathbb{C}$ viewed as an affine algebraic variety. Because all finite subgroups of $\operatorname{Aut}(\mathbb{C})$ are cyclic, the conclusion follows. □

Theorem 5.4. *A complex hyperelliptic curve has many automorphisms if and only if it is isomorphic to a curve in Table 2.*

Proof. Let X be a complex hyperelliptic curve with many automorphisms of genus g. Then $\overline{G} := \overline{\operatorname{Aut}}(X)$ is not trivial by Lemma 4.5. By Corollary 3.11, the group $\overline{G}$ is isomorphic to one of C_n, D_n, A_4, S_4 and A_5 for some $n \geq 2$. We choose coordinates on $\mathbb{P}^1_{\mathbb{C}}$, such that $\overline{G}$ acts on $\mathbb{P}^1_{\mathbb{C}}$ as specified in Definition 5.1. We proceed by a case distinction on the different possibilities for $\overline{G}$ and list, for each choice of $\overline{G}$, the possible sets $W(X)$ and use the fact that X is uniquely determined by $W(X)$. View $W(X)$ as the union of the orbits of the action of $\overline{G}$ on it. We construct all possibilities for $W(X)$ by using Theorem 4.1 and Proposition 5.2 and exclude possible sets of branch points when the curve associated to these already has a reduced automorphism group strictly containing $\overline{G}$.

1. Case $\overline{G} = C_n$: By Theorem 4.1, the action of $\overline{G}$ on $W(X)$ has exactly one free orbit. By Proposition 5.2, the non-free orbits of $\overline{G}$ on $\mathbb{P}^1_{\mathbb{C}}$ are $\{0\}$ and $\{\infty\}$. Let $p \in W(X)$ be in the free orbit of $\overline{G}$. After a change of coordinates in $\mathbb{P}^1_{\mathbb{C}}$ by multiplication with p^{-1}, we may assume without loss of generality that $p = 1$. Because multiplication with a constant commutes with the action of $\overline{G}$, the coordinates of the action of $\overline{G}$ do not change. The free orbit is now the set of roots of $x^n - 1$.
   Claim: n is odd.

   Proof. Assume, for contradiction, that n is even. Then, because $|W(X)|$ is even, either none or both of $\{0\}$ and $\{\infty\}$ have to be subsets of $W(X)$. In either case, the dihedral group D_n acts on $W(X)$. Therefore, by Proposition 3.12, we have $D_n < \overline{\operatorname{Aut}}(X)$, which is a contradiction. □

Because n is odd and $|W(X)|$ is even, either $0 \in W(X)$ or $\infty \in W(X)$. But the curves given by $y^2 = x^{2g+1} - 1$ and $y^2 = x^{2g+2} - x$ are isomorphic. Therefore, if X exists, we may assume that X is given by $y^2 = x^{2g+1} - 1$ and $n = 2g + 1$. By Lemma 5.3, it follows that C_{2g+1} is indeed the full reduced automorphism group of the hyperelliptic curve defined by $y^2 = x^{2g+1} - 1$. Therefore, a hyperelliptic curve X with many automorphisms and $\overline{\mathrm{Aut}}(X) = C_n$ exists and is defined by

$$y^2 = x^n - 1.$$

2. Case $\overline{G} = D_n$: By Theorem 4.1, the action of $\overline{G}$ on $W(X)$ has no free orbits. By Proposition 5.2, the non-free orbits of $\overline{G}$ on $\mathbb{P}^1_{\mathbb{C}}$ are $\{0, \infty\}$, the set of roots of $x^n - 1$ and the set of roots of $x^n + 1$. Therefore, the curve X is given by

$$y^2 = x^{\epsilon_1}(x^n - 1)^{\epsilon_2}(x^n + 1)^{\epsilon_3}$$

for some $\epsilon_1, \epsilon_2, \epsilon_3 \in \{0, 1\}$.
Claim: $\epsilon_2 + \epsilon_3 = 1$.

Proof. If $\epsilon_2 = \epsilon_3 = 0$, the curve X is not hyperelliptic. If $\epsilon_2 = \epsilon_3 = 1$, the curve X is given by $y^2 = x^{\epsilon_1}(x^{2n} - 1)$ and D_{2n} acts on X. Then, by Proposition 3.12, we have $D_{2n} < \overline{G}$, which is a contradiction. □

Therefore, the curve X is of the form $y^2 = x^{\epsilon_1}(x^n \pm 1)$.
Claim: n is even.

Proof. Suppose that n is odd. If $\epsilon_1 = 0$, then $0 \notin W(X)$ and $\infty \in W(X)$, because $|W(X)|$ is even, which is a contradiction. If $\epsilon_1 = 1$, then $0 \in W(X)$ and $\infty \notin W(X)$, which is also a contradiction. □

Because the curves given by $y^2 = x^{\epsilon_1}(x^n - 1)$ and $y^2 = x^{\epsilon_1}(x^n + 1)$ are isomorphic, we may assume that X is given by

$$y^2 = x^{\epsilon_1}(x^{2g+2-2\epsilon_1} - 1)$$

and $n = 2g + 2 - 2\epsilon_1$. Note that, for even $n > 4$ we have $D_n \not< S_4$ and for even $n > 2$ we have $D_n \not< A_5$. If $g \geq 2$ and $\epsilon_1 = 0$ the curve X is given by $y^2 = x^{2g+2} - 1$ and its full automorphism is indeed D_{2g+2}. If $g \geq 3$ and $\epsilon_1 = 1$ the curve X is given by $y^2 = x^{2g+1} - x$ and its full automorphism group is indeed D_{2g}. The remaining case, if $g = 2$ and $\epsilon_1 = 1$, is given by $y^2 = x(x^4 - 1)$ and has reduced automorphism group S_4 as is shown below.

3. Case $\overline{G} = A_4$: By Theorem 4.1, the action of $\overline{G}$ on $W(X)$ has no free orbits. By Proposition 5.2, the curve X is given by

$$y^2 = t_4^{\epsilon_1} p_4^{\epsilon_2} q_4^{\epsilon_3}$$

for some $\epsilon_1, \epsilon_2, \epsilon_3 \in \{0,1\}$. Note that $p_4 q_4 = s_4$, where the roots of s_4 are a non-free orbit of the action of S_4. Also the roots of t_4, together with ∞, form a non-free orbit of the action of S_4. Therefore, if ϵ_1 is arbitrary and $\epsilon_2 = \epsilon_3 = 1$, the group S_4 acts on $W(X)$ and therefore, by Proposition 3.12, we have $S_4 < \overline{G}$, which is a contradiction.

Claim: $\epsilon_1 = 1$.

Proof. If $\epsilon_1 = 0$, then $\epsilon_2 = \epsilon_3 = 1$, because otherwise the genus of X would be one. This is a contradiction. □

Claim: $\epsilon_2 + \epsilon_3 = 1$.

Proof. The case $\epsilon_2 = \epsilon_3 = 1$ has been treated above. If $\epsilon_2 = \epsilon_3 = 0$, the curve X is defined by $y^2 = t_4$, which implies $S_4 < \overline{G}$, which is also a contradiction. □

It follows that X, if it exists, is defined by $y^2 = t_4 p_4$ or $y^2 = t_4 q_4$. But the two possibilities are isomorphic. Therefore, we may assume that X is defined by $y^2 = t_4 p_4$. It remains to show that the reduced automorphism group of the projective curve Y defined by $y^2 = t_4 p_4$ is indeed A_4 and not S_4. Suppose that S_4 acts on $W(Y)$. Then all orbits of S_4 on $W(Y)$ are non-free, because all points in $W(Y)$ already have non-trivial point stabilizers in $A_4 < S_4$. Therefore, the curve Y would be a curve with many automorphisms and appear in the next case. Since it does not do that, the group S_4 does not act on $W(Y)$ and therefore X exists and is equal to Y.

4. Case $\overline{G} = S_4$ or $\overline{G} = A_5$: By Theorem 4.1, the action of $\overline{G}$ on $W(X)$ has no free orbits. Since S_4 and A_5 are not proper subgroups of any finite subgroups of $\mathrm{Aut}(\mathbb{P}^1_{\mathbb{C}})$ and all nontrivial products of the polynomials for S_4, respectively A_5, listed in Table 1 define hyperelliptic curves, the hyperelliptic curves with many automorphisms with reduced automorphism group S_4, respectively A_5, are exactly given by the nontrivial products of the polynomials listed for the respective groups in Table 1.

□

Definition 5.5. The groups V_n, U_n, W_2 and W_3 in Table 2 are defined by

$$\begin{aligned} U_n &:= \langle a, b \mid a^2, b^{2n}, abab^{n+1} \rangle, \\ V_n &:= \langle a, b \mid a^4, b^n, (ab)^2, (a^{-1}b)^2 \rangle, \\ W_2 &:= \langle a, b \mid a^4, b^3, ba^2b^{-1}a^2, (ab)^4 \rangle, \\ W_3 &:= \langle a, b \mid a^4, b^3, (ab)^8, a^2(ab)^4 \rangle \end{aligned}$$

as defined in Theorem 2.1 in [BGG93].

Theorem 5.6. *The automorphism groups of the hyperelliptic curves with many automorphisms are as given in Table 2.*

Proof. To determine the (not reduced) automorphism groups of the curves in Table 2, we use the classification of the automorphism groups of hyperelliptic curves in Satz 5.1 in [BS86]. Let X by a hyperelliptic curve and let $\psi : X \to X/\operatorname{Aut}(X) \cong \mathbb{P}^1_{\mathbb{C}}$ and $\phi : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}/\overline{\operatorname{Aut}}(X)$ be the quotient maps. Then the isomorphism class of $\operatorname{Aut}(X)$ is completely determined by $\overline{\operatorname{Aut}}(X)$ and the ramification orders of the map ψ of the branch points of ϕ. Each branch point of ϕ corresponds to a non-free orbit of the action of $\overline{\operatorname{Aut}}(X)$ on $\mathbb{P}^1_{\mathbb{C}}$. Let $p \in \mathbb{P}^1_{\mathbb{C}}$ be a branch point of ϕ and let

$$e_p = \frac{|\operatorname{Aut}(X)|}{|\psi^{-1}(p)|}$$

denote its ramification order with respect to ψ. If $\phi^{-1}(p) \subseteq W(X)$, then

$$|\psi^{-1}(p)| = |\phi^{-1}(p)|$$

and

$$e_p = \frac{|\operatorname{Aut}(X)|}{|\phi^{-1}(p)|}.$$

Otherwise, we have $|\psi^{-1}(p)| = 2|\phi^{-1}(p)|$ and therefore,

$$e_p = \frac{|\operatorname{Aut}(X)|}{2\,|\phi^{-1}(p)|}.$$

Thus, for each curve X in Table 2, we can determine the needed ramification orders by looking at which non-free orbits of $\overline{\operatorname{Aut}}(X)$ on $\mathbb{P}^1_{\mathbb{C}}$ are in $W(X)$.

Alternatively, the automorphism groups can be obtained from Table 1 in [Sha06]. □

6. Quotient curves

Let X be a smooth projective complex algebraic curve of genus $g \geq 0$ and let $G < \operatorname{Aut}(X)$ be a finite group. Recall that the quotient X/G also has the structure of a smooth projective complex algebraic curve.

Proposition 6.1. *Suppose that $g \geq 2$ and let $\tilde{g}$ be the genus of X/G. Then*

$$\tilde{g} = \dim H^0(X, \Omega_X)^G.$$

Proof. See Corollary V.2.2 in [FK92]. □

Suppose that $g \geq 2$. The dimension of the space of invariants in the space of holomorphic differentials can be computed using character theory:

	$\mathrm{Aut}(X)$	$\overline{\mathrm{Aut}}(X)$	Affine eq. of X is $y^2 - f(x)$	Genus	$\mathrm{Jac}(X)$ has CM
X_1	C_{4g+2}	C_{2g+1}	$f = x^{2g+1} - 1$	$g \geq 2$	yes
X_2	V_{2g+2}	D_{2g+2}	$f = x^{2g+2} - 1$	$g \geq 2$	yes
X_3	U_{2g}	D_{2g}	$f = x^{2g+1} - x$	$g \geq 3$	yes
X_4	$\mathrm{SL}_2(3)$	A_4	$f = t_4 p_4$	4	yes
X_5	$\mathrm{GL}_2(3)$	S_4	$f = t_4$	2	yes
X_6	$C_2 \times S_4$	S_4	$f = s_4$	3	no
X_7	W_2	S_4	$f = r_4$	5	yes
X_8	$\mathrm{GL}_2(3)$	S_4	$f = s_4 t_4$	6	no
X_9	W_3	S_4	$f = r_4 t_4$	8	yes
X_{10}	W_2	S_4	$f = r_4 s_4$	9	?
X_{11}	W_3	S_4	$f = r_4 s_4 t_4$	12	?
X_{12}	$C_2 \times A_5$	A_5	$f = s_5$	5	no
X_{13}	$C_2 \times A_5$	A_5	$f = r_5$	9	no
X_{14}	$\mathrm{SL}_2(5)$	A_5	$f = t_5$	14	yes
X_{15}	$C_2 \times A_5$	A_5	$f = r_5 s_5$	15	no
X_{16}	$\mathrm{SL}_2(5)$	A_5	$f = s_5 t_5$	20	?
X_{17}	$\mathrm{SL}_2(5)$	A_5	$f = r_5 t_5$	24	?
X_{18}	$\mathrm{SL}_2(5)$	A_5	$f = r_5 s_5 t_5$	30	?

Table 2: Hyperelliptic curves with many automorphisms

Definition 6.2. We denote by χ_{hol} the character of the canonical representation of $\mathrm{Aut}(X)$ on the space of holomorphic differentials $H^0(X, \Omega_X)$ and by χ_{triv} the trivial character of $\mathrm{Aut}(X)$.

Lemma 6.3. *For a character χ of $\mathrm{Aut}(X)$, denote by $\chi|_G$ the restriction of χ to G. We have*

$$\dim H^0(X, \Omega_X)^G = \langle \chi_{\mathrm{hol}}|_G, \chi_{\mathrm{triv}}|_G \rangle.$$

Proof. This follows from basic character theory. □

Proposition 6.4. *Let E be a complex elliptic curve with identity $P \in E$. Then, the group of automorphisms of E that fixes P is cyclic of order 2, 4 or 6.*

Proof. See Corollary III.10.2 in [Sil09]. □

Proposition 6.5. *Let X be a complex hyperelliptic curve and let $G < \mathrm{Aut}(X)$ be such that $Y := X/G$ has genus one. Denote by $\overline{G}$ the image of G in $\overline{\mathrm{Aut}}(X)$ and denote by $\phi : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}/\overline{G} \cong \mathbb{P}^1_{\mathbb{C}}$ the quotient map. Let $V_1 := \phi(W(X))$ and let V_2 be* *the set of branch points of* ϕ *and let* $V := V_1 \cup V_2$*. Then, there are distinct points* $P_1, \ldots, P_4 \in V$ *such that* $\infty \notin \{P_1, P_2, P_3\}$ *and* Y *is isomorphic to the projective completion of*

$$y^2 = (x - P_1)(x - P_2)(x - P_3)(x - P_4)$$

if $P_4 \neq \infty$*, and*

$$y^2 = (x - P_1)(x - P_2)(x - P_3),$$

if $P_4 = \infty$*.*

Proof. First note that the hyperelliptic involution σ of X is not contained in G, because if it was, the quotient Y would have genus 0. Since σ is in the center of $\mathrm{Aut}(X)$ and the quotient $\pi_2 : X \to Y$ is categorical, the involution σ acts on Y. Let $w \in X$ be a Weierstrass point and denote the hyperelliptic double cover by $\pi_1 : X \to \mathbb{P}^1_{\mathbb{C}}$. Then w is fixed by σ, and therefore $\pi_2(w)$ is fixed by the action of σ on Y. It follows that σ induces an involution on Y, again called σ, that fixes $\pi_2(w)$. It follows directly from Proposition 6.4 that σ is the unique involution on Y that fixes $\pi_2(w)$. Let $g : Y \to Y/\langle\sigma\rangle \cong \mathbb{P}^1_{\mathbb{C}}$ denote the quotient map. Then $g \circ \pi_2 = \phi \circ \pi_1$, since in the case of $g \circ \pi_2$, we first take the quotient by G and then by σ, and in the case of $\phi \circ \pi_1$, we first take the quotient by σ and then by $\overline{G}$. Let $P_1, \ldots, P_4$ denote the branch points of g in $\mathbb{P}^1_{\mathbb{C}}$ and suppose, without loss of generality, that $\infty \notin \{P_1, P_2, P_3\}$. If $P_4 \neq \infty$, an equation for Y is given by

$$y^2 = (x - P_1)(x - P_2)(x - P_3)(x - P_4).$$

Otherwise, an equation for Y is given by

$$y^2 = (x - P_1)(x - P_2)(x - P_3).$$

Because $P_1, \ldots, P_4$ are branch points of g and π_2 is a branched covering of degree $|G|$, the points $P_1, \ldots, P_4$ are also branch points of $g \circ \pi_2$. Then $P_1, \ldots, P_4$ are also branch points of $\phi \circ \pi_1$. The branch points of $\phi \circ \pi_1$ are given by V. □

Theorem 6.6 (Constructive version of Lüroth's theorem)**.** *Let* K *and* L *be fields such that* $K \subsetneq L \subseteq K(x)$*. Then, the field extension* $K(x)/L$ *is finite and any coefficient of the minimal polynomial of* x *over* L *that is not in* K *generates* $K(x)$ *over* L*.*

Proof. See the proof of Theorem 1.3 in [Oja90]. □

Remark 6.7. At least one of the coefficients of the minimal polynomial of x over L is not in K since x is transcendental over K.

The following Lemma is stated without a detailed proof in [Sha06].

Lemma 6.8. *Let* G *be a finite subgroup of* $\mathrm{Aut}(\mathbb{P}^1_{\mathbb{C}})$ *and let* $h_1, \ldots, h_{|G|} \in \mathbb{C}(x)$ *be the Möbius transformations associated to the elements of* G*. Then, up to an* *automorphism of the image, the morphism $f : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}/G \cong \mathbb{P}^1_{\mathbb{C}}$ is given by any nonconstant elementary symmetric polynomial in $h_1, \ldots, h_{|G|}$.*

Proof. In terms of function fields, the morphism f is given by the inclusion $\mathbb{C}(x)^G \hookrightarrow \mathbb{C}(x)$. It remains to show that $\mathbb{C}(x)^G$ is generated by any nonconstant elementary symmetric polynomial in $h_1, \ldots, h_{|G|}$. Because G is finite, the extension $\mathbb{C}(x)/\mathbb{C}(x)^G$ is Galois with $\operatorname{Gal}\left(\mathbb{C}(x)/\mathbb{C}(x)^G\right) = G$. Let $f \in \left(\mathbb{C}(x)^G\right)[y]$ be the minimal polynomial of x over $\mathbb{C}(x)^G$. Then $f(x) = 0$ and therefore $f(h_k(x)) = 0$ for $1 \leq k \leq |G|$, because $Gx = \left\{h_1(x), \ldots, h_{|G|}(x)\right\}$. Because $\left[\mathbb{C}(x)/\mathbb{C}(x)^G\right] = |G|$, we have $\deg_y f = |G|$. Therefore,

$$f(y) = \prod_{k=1}^{|G|} (y - h_k(x))$$

and the coefficients of $f(y)$ are the elementary symmetric polynomials in $h_1, \ldots, h_{|G|}$. The conclusion follows from Theorem 6.6. □

7. Abelian varieties and semi-abelian varieties

7.1. Abelian varieties

For more information on abelian varieties see for example [Lan83], [BL04] and [Mil08]. Let K be a field.

Definition 7.1. An *abelian variety over K* is a smooth geometrically connected projective commutative group scheme over K.

Definition 7.2. An *abelian scheme $\mathcal{A}$ over a scheme S* is a proper smooth commutative group scheme over S whose fibers are abelian varieties.

Remark 7.3. Not all commutative group schemes are abelian varieties. For example the multiplicative group $\mathbb{G}_{m,K} := \mathrm{GL}_{1,K}$ is an affine algebraic group.

Let A be an abelian variety over K.

Definition 7.4. We say that A is *simple* if $A \neq 0$ and the only abelian subvarieties of A, i.e. the subschemes of A that are also abelian varieties with the group structure induced by A, are 0 and A.

Remark 7.5. For every abelian variety A over $\mathbb{C}$ the underlying complex analytic manifold is isomorphic to a complex torus $\mathbb{C}^{\dim A}/\Lambda$, where Λ is a real lattice of rank $2\dim A$. For further information see for example Chapter I of [Mum74] or Theorem 4.5.4 in [BL04].

Example 7.6. The complex abelian varieties of dimension one are precisely the complex elliptic curves. See Example 4.1.3 in [BL04].

Definition 7.7. Let B be an abelian varieties over K. A *morphism* $\varphi : A \to B$ is a morphism $A \to B$ of schemes. A *homomorphism* $\psi : A \to B$ is a morphism that is also a group homomorphism for the group structures on A and B. A homomorphism is called an *isogeny* if φ is surjective and $\ker \varphi$ is finite. If there exists an isogeny $\varphi : A \to B$, we call A and B *isogenous* and write $A \sim B$.

Proposition 7.8. *Being isogenous defines an equivalence relation on the category of abelian varieties over K.*

Proof. See Remark 8.6 in [Mil08] and Section 10 in [Mil08]. □

Theorem 7.9 (Poincaré's complete reducibility theorem)**.** *If B is an abelian subvariety of A, then there is an abelian subvariety C of A such that $B \cap C$ is finite and $A = B + C$. In particular, we have $A \sim B \times C$. If A and B are defined over K, then we can also take C to be defined over K.*

Proof. See Theorem 6 in §1 in Chapter II in [Lan83]. □

Corollary 7.10. *The abelian variety A is isogenous to a product $X_1^{n_1} \times \cdots \times X_k^{n_k}$, where the X_i are simple and not isogenous to each other. Up to permutation of the factors, the isogeny types of $X_1, \ldots, X_n$ and the integers $n_1, \ldots, n_k$ are uniquely determined.*

Proof. See the Corollary to Theorem 6 in §1 in Chapter II in [Lan83]. □

Corollary 7.11. *Suppose that $\varphi : A \to B$ is a surjective homomorphism of abelian varieties. Then, there is an abelian subvariety C of A such that $A \sim B \times C$.*

Proof. Let $C = \ker \varphi$. By Theorem 7.9, there is an abelian subvariety B' of A such that $A \sim B' \times C$ and $A = B' + C$ and $B' \cap C$ is finite. We get a homomorphism $\tilde{\varphi} : B' \times C \to B$ that factors through A. Because $C = \ker \varphi$ the map $\tilde{\varphi}|_{B'}$ is still surjective, and because $B' \cap \ker \varphi$ is finite, the kernel $\ker \tilde{\varphi}|_{B'}$ is also finite. Therefore, we have $B' \sim B$ and the conclusion follows. □

7.2. Semi-abelian varieties

Let K be a perfect field and let $\overline{K}$ be an algebraic closure of K.

Definition 7.12. An *algebraic torus* over K of rank $r \in \mathbb{Z}_{\geq 0}$ is an algebraic group that is isomorphic over $\overline{K}$ to $\mathbb{G}_{m,\overline{K}}^r$.

Definition 7.13. A *semi-abelian variety over K* is a commutative group scheme G over K for which there exists an exact sequence

$$1 \to T \to G \to A \to 1,$$

where T is an algebraic torus and A is an abelian variety.

Definition 7.14. A *semi-abelian scheme over a scheme S* is a separated smooth commutative group scheme over S whose fibers are semi-abelian varieties.

Theorem 7.15 (Chevalley's Theorem)**.** *Let G be an algebraic group over K. Then, there is a unique short exact sequence of algebraic groups*

$$1 \to H \to G \to A \to 1,$$

where H is a linear algebraic group and A is an abelian variety. The formation of H commutes with base change to an arbitrary perfect field extension of K.

Proof. See Theorem 1.1 in [Con02]. □

Definition 7.16. Let G be a semi-abelian variety over K. Let T be an algebraic torus over K and let A be an abelian variety over K such that G is an extension of A by T. The rank of T is called the *toric rank* of G.

Corollary 7.17. *The toric rank of a semi-abelian variety G over K is well-defined.*

Proof. This follows from the uniqueness in Theorem 7.15, because algebraic tori are linear algebraic groups. □

Corollary 7.18. *Let G be a semi-abelian variety over K and let K' be a perfect field extension of K. Then G and $G_{K'}$ have the same toric rank.*

Proof. This follows from Theorem 7.15, because the formation of the linear algebraic group commutes with base change to K'. □

Let R be a DVR with fraction field K and perfect residue field k of characteristic $\operatorname{char} k \neq 2$ and let $S = \operatorname{Spec}(R)$.

Definition 7.19. Let $\mathcal{X}$ be a scheme over S. We define the *generic fiber* of $\mathcal{X}$ to be $\mathcal{X}_\eta := X_K$. The *special fiber* of $\mathcal{X}$ is defined as $\mathcal{X}_0 := X_k$.

Let A be an abelian variety over K.

Definition 7.20. We say that A has *good reduction over R* if it is the generic fiber of an abelian scheme $\mathcal{A}$ over R. We say that A has *potential good reduction over R* if there is a finite extension K' of K and an extension of R to a DVR R' of K' such that $A_{K'}$ has good reduction over R'.

The abelian variety A is said to have *semi-stable reduction of toric rank r over R* if there is a semi-abelian group scheme $\mathcal{A}$ over S such that $\mathcal{A}_\eta \cong A$ and $\mathcal{A}_0$ is a semi-abelian group scheme of toric rank r.

For a number field F, a prime ideal $\mathfrak{p} \subset \mathcal{O}_F$ and an abelian variety A' over F we say that A' *has good reduction*, respectively *potential good reduction*, respectively *semi-stable reduction at $\mathfrak{p}$* if A' has good reduction, respectively potential good reduction, respectively semi-stable reduction over the DVR $\mathcal{O}_{F,\mathfrak{p}} := (\mathcal{O}_F)_{\mathfrak{p}}$.

An important result about semi-stable reduction due to Grothendieck and Mumford is the following:

Theorem 7.21 (Stable Reduction Theorem for abelian varieties)**.** *There is a finite extension K' of K such that A has semi-stable reduction over the integral closure of R in K'.*

Proof. See Theorem 1 in Section 7.4 of [BLR90] □

For a reference about good reduction of abelian varieties see [ST68] and Section 6 in [Mil06]. For a reference about semi-stable reduction see Section 7.4 in [BLR90].

Proposition 7.22. *Suppose that K' is a perfect extension of K and let R' be a DVR that extends R in K'. Denote by k' the residue field of R' and suppose that k' is perfect. Let A be an abelian variety over K. Suppose that A has semi-stable reduction of toric rank r over R and that $A_{K'}$ has semi-stable reduction of toric rank r' over R'. Then $r = r'$.*

Proof. Suppose first that $K' = K$ and $R' = R$. Let $\mathcal{A}$ be the Néron model of A over R. The Néron model exists by Corollary 2 in Section 1.3 in [BLR90]. Let $\mathcal{A}_1$ and $\mathcal{A}_2$ be semi-abelian schemes over R such that the special fiber A_1 of $\mathcal{A}_1$ has toric rank r and the special fiber A_2 of $\mathcal{A}_2$ has toric rank r'. Then, since $\mathcal{A}_1$ and $\mathcal{A}_2$ are smooth and separated, Proposition 3 in Section 7.4 in [BLR90] states that the identity components A_1^0 and A_2^0 of A_1 and A_2 are both isomorphic to the identity component $\mathcal{A}^0$ of $\mathcal{A}$. In particular, they have the same toric rank, since the toric rank of a semi-abelian variety is only determined by its identity component.

For the general case, let $\mathcal{A}_R$ be a semi-abelian scheme over R such that the special fiber $A_{0,R}$ of $\mathcal{A}_R$ has toric rank r. Then, the general fiber of $\mathcal{A}_{R'}$ is $A_{K'}$ and the special fiber $A_{0,R'}$ of $\mathcal{A}_{R'}$ is given by $A_{0,R'} = A_{0,R} \times_{\mathrm{Spec}(k)} \mathrm{Spec}(k')$. Then, the semi-abelian schemes $A_{0,R}$ and $A_{0,R'}$ have the same toric rank by Corollary 7.18. Therefore, the scheme $\mathcal{A}_{R'}$ is a semi-abelian model of $A_{K'}$ over R', the special fiber of which has toric rank r'. The conclusion now follows from the first part of the proof. □

Proposition 7.23. *Suppose that A has semi-stable reduction of toric rank r over R. Then A has potential good reduction over R if and only if $r = 0$.*

Proof. If $r = 0$, then there is a model $\mathcal{A}$ of A over R such that the special fiber is an abelian variety. Then, by Theorem 5 in Section 7.4 in [BLR90], the abelian variety A has good reduction over R. Conversely, suppose that $r > 0$. Assume, for contradiction, that A has potential good reduction. Let R' be an extension of R and K' be the fraction field of R' such that there is an abelian scheme $\mathcal{A}$ that is a model of the extension $A_{K'}$ of A to K'. Then, by Theorem 5 in Section 7.4 in [BLR90] the abelian variety $A_{K'}$ has semi-stable reduction of toric rank 0. By applying Proposition 7.22, we obtain the desired contradiction. □

Proposition 7.24. *Let $\hat{K}$ and $\hat{R}$ be the completions of K and R with respect to the discrete valuation on K that induces R. Then A has potential good reduction over R if and only if $A_{\hat{K}}$ has potential good reduction over $\hat{R}$.*

Proof. Suppose that $A_{\hat{K}}$ has potential good reduction. Then $A_{\hat{K}}$ has semi-stable reduction of rank zero over a finite extension $\hat{L}$ of $\hat{K}$. By Theorem 7.21, the abelian variety A has semi-stable reduction of reduction of rank r over some finite extension F of K for some $r \geq 0$. Denote by $\hat{F}$ the corresponding completion of F and let $\hat{M}$ be a finite extension of $\hat{K}$ that contains $\hat{L}$ and $\hat{F}$. Then $A_{\hat{M}}$ has semi-stable reduction of rank zero over the corresponding extension $R_{\hat{M}}$ of R. Since $\hat{M}$ is a perfect extension of F, by Proposition 7.22 it follows that $r = 0$.

Conversely, suppose that A has potential good reduction over R. Let F be a finite extension of K such that A_F has good reduction over the corresponding extension of R. Then, by Proposition 7.23 and Corollary 7.18, the abelian variety $A_{\hat{F}}$ has good reduction over the corresponding extension of $\hat{R}$. The conclusion follows since $\hat{F}/\hat{K}$ is finite. □

7.3. Jacobian varieties

We follow Section 11.1 in [BL04] for the construction of the Jacobian variety for a complex smooth projective curve X of genus $g > 0$:

Lemma 7.25. *A canonical embedding of $H_1(X, \mathbb{Z})$ into $H^0(X, \Omega_X)^\vee$ is given by*

$$\begin{aligned} H_1(X, \mathbb{Z}) &\to H^0(X, \Omega_X)^\vee \\ \gamma &\mapsto \left(\omega \mapsto \int_\gamma \omega \right). \end{aligned}$$

Proof. See Lemma 11.1.1 in [BL04]. □

We identify $H_1(X, \mathbb{Z})$ with its image in $H^0(X, \Omega_X)^\vee$ and define

Definition 7.26. The *Jacobian variety* or *Jacobian* of X is

$$\operatorname{Jac}(X) := H^0(X, \Omega_X)^\vee / H_1(X, \mathbb{Z}).$$

Proposition 7.27. *The complex torus* $\operatorname{Jac}(X)$ *can be endowed with a canonical structure of an abelian variety.*

Proof. See the definition of a complex abelian variety in Section 4.1 in [BL04] and Proposition 11.1.2 in [BL04]. □

Proposition 7.28. *The dimension of* $\operatorname{Jac}(X)$ *is* g.

Proof. We have $\dim \operatorname{Jac}(X) = \dim H^0(X, \Omega_X)^\vee = \dim H^0(X, \Omega_X) = g$ by Proposition 3.13. □

Proposition 7.29 (Universal property of the Jacobian)**.** *Let $p \in X$. Then there is a canonical morphism $\alpha_p : X \to \mathrm{Jac}(X)$ called the Abel-Jacobi map for p with $\alpha_p(p) = 0$ such that the following holds: Suppose that A is an abelian variety and $\varphi : X \to A$ is a rational map. For $q \in A$, let t_q denote the translation map of A by q. Then there exists a unique homomorphism $\tilde{\varphi} : \mathrm{Jac}(X) \to A$ such that for every $p \in X$ the following diagram commutes:*

$$\begin{array}{ccc} X & \xrightarrow{\varphi} & A \\ {\scriptstyle \alpha_p}\big\downarrow & & \big\downarrow{\scriptstyle t_{-\varphi(p)}} \\ \mathrm{Jac}(X) & \xrightarrow[\tilde{\varphi}]{} & A \end{array}$$

Proof. See the Universal Property of the Jacobian 11.4.1 in [BL04]. □

7.4. The Picard scheme

Definition 7.30. For a scheme X we denote by $\mathrm{Pic}(X)$ the *Picard group* of X, that is the group of isomorphism classes of invertible sheaves on X with the tensor product as the group operation.

Remark 7.31. By Remark 6.12.1 in [Har77], the Picard group $\mathrm{Pic}(X)$ can be expressed as the sheaf cohomology group $H^1(X, \mathcal{O}_X^*)$.

The following definitions follow Chapter 9 in [FGI+05].

Definition 7.32. Let S be a locally Noetherian scheme and let $f : X \to S$ be a separated morphism of finite type. For an S-scheme T we write $X_T := X \times_S T$. The *relative Picard functor* $\mathrm{Pic}_{X/S}$ from the category of schemes over S to the category of abelian groups is defined by

$$\mathrm{Pic}_{X/S}(T) = \mathrm{Pic}(X_T)/f_T^* \,\mathrm{Pic}(T),$$

where $f_T : X_T \to T$ denotes the projection map. It is a contravariant functor, because the functor $X \mapsto \mathrm{Pic}(X) \cong H^1(X, \mathcal{O}_X^*)$ is contravariant. We denote its associated sheaves in the étale and fppf Grothendieck topologies by $\mathrm{Pic}_{(X/S)(\text{ét})}$ and $\mathrm{Pic}_{(X/S)(\text{fppf})}$ respectively. If $\mathrm{Pic}_{X/S}$ or $\mathrm{Pic}_{(X/S)(\text{ét})}$ or $\mathrm{Pic}_{(X/S)(\text{fppf})}$ is representable, the representing scheme is called the *Picard scheme* and is denoted by $\mathbf{Pic}_{X/S}$. In this case, we say that the Picard scheme $\mathbf{Pic}_{X/S}$ exists.

For more information on Grothendieck topologies and sheaves in this context, see Section 2.3 in Part 1 of [FGI+05].

Remark 7.33. If $\mathbf{Pic}_{X/S}$ exists, it is unique up to unique isomorphism and represents all of the relative Picard functors $\mathrm{Pic}_{X/S}$, $\mathrm{Pic}_{(X/S)(\text{ét})}$ and $\mathrm{Pic}_{(X/S)(\text{fppf})}$ that are representable. See page 262 in [FGI+05]. Furthermore $\mathbf{Pic}_{X/S}$ commutes with base change: Let S' be an S-scheme. Then $\mathbf{Pic}_{X_{S'}/S'}$ exists, too, and is given by $\mathbf{Pic}_{X_{S'}/S'} = \mathbf{Pic}_{X/S} \times_S S'$. This is a formal consequence of the definition. For a reference, see page 305 in [FGI+05].

Proposition 7.34. *For a smooth proper curve C over a field K, the Picard scheme $\mathbf{Pic}_{C/K}$ exists and is a group scheme and the identity component $\mathbf{Pic}^0_{C/K}$ is an abelian variety.*

Proof. See Proposition 3 in Section 9.2 in [BLR90]. □

Proposition 7.35. *Let C be a proper smooth curve over a field K. Then the formation of $\mathbf{Pic}^0_{X/K}$ commutes with base extension: For a field K' containing K we have*

$$\mathbf{Pic}^0_{X_{K'}/K'} = \mathbf{Pic}^0_{X/K} \times_{\mathrm{Spec}(K)} \mathrm{Spec}(K').$$

Proof. See Proposition 9.5.3 in Part 5 in [FGI+05]. □

Definition 7.36. Let C be a smooth proper curve over a field K. Then we call $\mathbf{Pic}^0_{C/K}$ its *Jacobian.*

By the following proposition, this definition agrees with our earlier definition of the Jacobian:

Proposition 7.37. *There is a canonical isomorphism of abelian varieties* $\mathrm{Jac}(X) \xrightarrow{\sim} \mathbf{Pic}^0_{X/\mathbb{C}}$.

Proof. By Theorem 2.5 in Chapter VII in [CS86], there is a canonical isomorphism between $\mathrm{Jac}(X)$ and the identity component $\mathrm{Pic}^0(X)$ of the Picard group $\mathrm{Pic}(X)$. We can identify $\mathrm{Pic}^0(X)$ and $(\mathbf{Pic}^0_{X/\mathbb{C}})_{\mathrm{red}}$, but by the main Theorem in [Oor66], the scheme $\mathbf{Pic}^0_{X/\mathbb{C}}$ is already reduced. □

7.5. Complex multiplication

For an introduction to the theory of complex multiplication for abelian varieties see [Mil06]. Let A be an abelian variety over a field F of characteristic 0.

Definition 7.38. We define the *endomorphism algebra over* $\mathbb{Q}$ of A as

$$\mathrm{End}_{\mathbb{Q}}(A) := \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Definition 7.39. Suppose that A is simple. Then we say that A has *complex multiplication (CM)* if $\mathrm{End}_{\mathbb{Q}}(A)$ contains a field K with $[K : \mathbb{Q}] = 2 \dim A$. For A not necessarily simple, we say that A has CM if every simple abelian subvariety in the isogenous decomposition in Corollary 7.10 has CM.

Remark 7.40. The abelian variety A has CM if and only if $\mathrm{End}_{\mathbb{Q}}(A)$ contains a commutative semisimple algebra Λ of dimension $2 \dim A$ over $\mathbb{Q}$.

Proposition 7.41. *Suppose that an abelian variety B is isogenous to A. Then A has CM if and only if B has CM.*

Proof. It suffices to prove the claim for the case in which A and B are simple. In this case $\mathrm{End}_{\mathbb{Q}}(A) \cong \mathrm{End}_{\mathbb{Q}}(B)$, as stated on page 43 in Section I.10 in [Mil08]. □

Corollary 7.42. *Let X be a smooth projective complex algebraic curve and suppose that there is a non-constant morphism $\varphi : X \to E$, where E is an elliptic curve. If E does not have CM, then* $\mathrm{Jac}(X)$ *does not have CM.*

Proof. By Proposition 7.29, there is a surjective homomorphism $\tilde{\varphi} : \mathrm{Jac}(X) \to E$. By Corollary 7.11, we obtain a decomposition $\mathrm{Jac}(X) \sim E \times B$ for some abelian subvariety B of $\mathrm{Jac}(X)$. Because E is simple, it must be isogenous to one of the components in the decomposition of $\mathrm{Jac}(X)$ into simple abelian varieties. The claim then follows from Proposition 7.41. □

To find curves in Table 2 that have Jacobians that have CM, we apply the following criterion:

Proposition 7.43. *Let X be a smooth projective complex algebraic curve of genus $g \geq 2$. If*

$$\langle \mathrm{Sym}^2 \chi_{\mathrm{hol}}, \chi_{\mathrm{triv}} \rangle = 0,$$

then $\mathrm{Jac}(X)$ *has CM.*

Proof. This is the statement of the second part of Proposition 5 in [Str01]. □

Remark 7.44. The condition in Proposition 7.43 can only be satisfied by curves with many automorphisms. For a reference, see the Remark on page 287 in [Str01].

Proposition 7.45. *Let E be an elliptic curve over $\mathbb{C}$ with CM. Then $j(E)$ is an algebraic integer.*

Proof. See Theorem 6.1 in II.6 of [Sil94]. □

Proposition 7.46. *Let A be an abelian variety over a number field $K \subset \mathbb{C}$ such that $A_{\mathbb{C}}$ has CM. Then A has potential good reduction at all primes of $\mathcal{O}_K$.*

Proof. Denote by $\overline{K}$ the algebraic closure of K in $\mathbb{C}$. Then, by Corollary II.7.10 in [Mil06], the abelian variety $A_{\overline{K}}$ has CM over $\overline{K}$, because $A_{\mathbb{C}}$ has CM. Let $e_1, \ldots, e_n$ for some $n \in \mathbb{Z}_{\geq 1}$ be generators of a semisimple commutative $\mathbb{Q}$-algebra Λ in $\mathrm{End}_{\mathbb{Q}}(A_{\overline{K}})$ with of degree $2 \dim A_{\overline{K}}$ over $\mathbb{Q}$. Let $K' \subset \overline{K}$ be a finite extension of K such that for $1 \leq l \leq n$ we have $e_l \in \mathrm{End}_{\mathbb{Q}}(A_{K'})$, where we identify $\mathrm{End}_{\mathbb{Q}}(A_{K'})$ with its image in $\mathrm{End}_{\mathbb{Q}}(A_{\overline{K}})$. Such an extension exists, because each morphism between projective varieties over $\overline{K}$ can be defined by a finite set of polynomials with coefficients in $\overline{K}$. Since $e_1, \ldots, e_n \in \mathrm{End}_{\mathbb{Q}}(A_{K'})$, we have $\Lambda \subseteq \mathrm{End}_{\mathbb{Q}}(A_{K'})$ and $A_{K'}$ has CM. If $A_{K'}$ has potential good reduction at all primes of K', then A_K has potential good reduction at all primes of K. The abelian variety $A_{K'}$ has potential good reduction at all primes of K' by Proposition II.7.12 in [Mil06]. $\square$

Remark 7.47. Let X be a smooth projective curve defined over a number field K. If $\mathrm{Jac}(X_{\mathbb{C}})$ has CM, then we can apply Proposition 7.46, because the formation of $\mathbf{Pic}^0$ commutes with extending the base field by Proposition 7.35, and therefore,

$$\mathrm{Jac}(X_{\mathbb{C}}) \cong \mathbf{Pic}^0_{X/K} \times_{\mathrm{Spec}(K)} \mathrm{Spec}(\mathbb{C}).$$

Below, in Theorem 10.25, we will give a criterion to decide whether $\mathbf{Pic}^0_{X/K}$ has potential good reduction at a given prime ideal $\mathfrak{p}$ with $2 \notin \mathfrak{p}$ in the case that X is hyperelliptic.

8. Computing the representation on the space of holomorphic differentials

To get information about whether the Jacobians of the curves in Table 2 have CM, we determine χ_{hol} for each of the curves in Table 2 that does not belong to one of the infinite families X_1, X_2 or X_3. Let X be a smooth projective complex algebraic curve X of genus $g \geq 2$.

Theorem 8.1 (Eichler trace formula)**.** *Let $T \in \mathrm{Aut}(X)$ be an automorphism of order $n > 1$. Let $\xi = e^{2\pi i/n}$ and let t be the number of fixed points of T on X. Then there are integers $\nu_1, \ldots, \nu_t$ such that $1 \leq \nu_k < n$ and ν_k and n are coprime for all $k \in \{1, \ldots, t\}$ such that*

$$\chi_{\mathrm{hol}}(T) = 1 + \sum_{k=1}^{t} \frac{\xi^{\nu_k}}{1 - \xi^{\nu_k}}.$$

Proof. This is a special case of the Eichler trace formula in V.2.9 in [FK92]. $\square$

Corollary 8.2 (Lefschetz Fixed Point Formula)**.** *Let $T \in \mathrm{Aut}(X)$ be a nontrivial automorphism and let t be the number of fixed points of T. Then*

$$2\,\mathrm{Re}\,(\chi_{\mathrm{hol}}(T)) = 2 - t.$$

Proof. We follow the proof of Corollary in V.2.9 in [FK92]: Note that for any $\theta \in \mathbb{C}$ with $|\theta| = 1$ and $\theta \neq 1$ we have $2\,\mathrm{Re}(\theta/(1-\theta)) = -1$ and apply Theorem 8.1. $\square$

Proposition 8.3. *Let $T \in \mathrm{Aut}(X)$ be nontrivial. If T is the hyperelliptic involution, then T has $2g + 2$ fixed points. Otherwise T has at most four fixed points.*

Proof. See Corollary 2 in III.7.9 and Proposition III.7.11 in [FK92]. $\square$

Corollary 8.4. *Let $T \in \operatorname{Aut}(X)$ be nontrivial. If T is the hyperelliptic involution, then*

$$\chi_{\text{hol}}(T) = -g.$$

Otherwise, we have

$$\operatorname{Re}\left(\chi_{\text{hol}}(T)\right) \in \left\{1, \frac{1}{2}, 0, -\frac{1}{2}, -1\right\}.$$

Proof. This follows directly from the combination of Corollary 8.2 and Proposition 8.3. □

Proposition 8.5. *For $4 \leq k \leq 18$ the character χ_{hol} of the curve X_k in Table 2 has the decomposition into irreducible characters as stated in Table 3. When several alternatives are given, the character χ_{hol} is sufficiently determined to know the degrees of the constituents, their fields of definition and to apply Proposition 7.43.*

Proof. Let X be one of the curves in Table 3 and let g be the genus of X. We proceed as follows to find χ_{hol}:

1. We determine which conjugacy class of $\operatorname{Aut}(X)$ contains the hyperelliptic involution σ. By Proposition 3.7, the involution σ is in the center. In all cases, there is a single conjugacy class which contains elements of order 2 and is in the center of $\operatorname{Aut}(X)$.

2. Let $\chi_1, \ldots, \chi_n$ be the irreducible characters of $\operatorname{Aut}(X)$. For $1 \leq k \leq n$, if $\chi_k(\sigma) \neq -\deg \chi_k$, then χ_k cannot be a constituent of χ_{hol}. This is because $\chi_{\text{hol}}(\sigma) = -g = -\deg \chi_{\text{hol}}$ by Corollary 8.4 and $|\chi_k(\sigma)| \leq \deg \chi_k$ by basic character theory. Using this observation, we can cut down on the set of possible constituents of χ_{hol}.

3. Enumerate all possible characters of $\operatorname{Aut}(X)$ with degree g that have only constituents that satisfy the observation in step 2. Remove from this list all characters which do not satisfy the condition in Corollary 8.4. If $X \notin \{X_4, X_{10}\}$, this determines χ_{hol} sufficiently.

If $X = X_4$, after step 3, we have

$$\chi_{\text{hol}} \in \{\chi_4 + \chi_5, \chi_4 + \chi_6, \chi_5 + \chi_6\}.$$

Consider the element $\overline{T} \in S_4 = \overline{\operatorname{Aut}}(X_4)$ with

$$\overline{T}(x) = \frac{x - i}{x + i}$$

of order 3. By a direct calculation, we see that $\overline{T}$ has exactly one fixed point in $W(X_4)$. Therefore, a lift T of $\overline{T}$ to $\operatorname{Aut}(X)$ has either one or three fixed points.

Then, by Corollary 8.2, we have $\mathrm{Re}(\chi_{\mathrm{hol}}(\overline{T})) = \pm\frac{1}{2}$. By looking at the character table of $\mathrm{SL}_2(3) \cong \mathrm{Aut}(X)$ in Appendix A, we see that

$$\chi_{\mathrm{hol}} \in \{\chi_4 + \chi_5, \chi_4 + \chi_6\}\,,$$

and the two possibilities are complex conjugate to each other.

If $X = X_{10}$, after step 3, we have

$$\chi_{\mathrm{hol}} \in \{\chi_j + \chi_5 + \chi_k + \chi_l \mid j \in \{3,4\} \text{ and } k,l \in \{9,10\}\}\,.$$

By looking at the character table of $W_2 \cong \mathrm{Aut}(X)$ in Appendix A, we see that if $T \in \mathrm{Aut}(X)$ has order 4, then $\mathrm{Re}(\chi_{\mathrm{hol}}(T)) = 0$ and therefore, by Corollary 8.2, the automorphism T has two fixed points. Then, by Theorem 8.1, we have

$$\chi_{\mathrm{hol}}(T) = 1 + \frac{i^{m_1}}{1 - i^{m_1}} + \frac{i^{m_2}}{1 - i^{m_2}},$$

for some $m_1, m_2 \in \{1,3\}$. It follows that $\chi_{\mathrm{hol}}(T) \in \{-i, 0, i\}$. By a direct calculation, this implies that $\{k,l\} = \{9,10\}$. $\square$

Curve X	$\mathrm{Aut}(X)$	χ_{hol}	Degrees
X_4	$\mathrm{SL}_2(3)$	$\chi_4+\chi_5$ or $\chi_4+\chi_6$	$\deg\chi_4=\deg\chi_5=\deg\chi_6=2$
X_5	$\mathrm{GL}_2(3)$	χ_4 or χ_5	$\deg\chi_4=\deg\chi_5=2$
X_6	$C_2\times S_4$	χ_7 or χ_8	$\deg\chi_7=\deg\chi_8=3$
X_7	W_2	$\chi_5+\chi_9$ or $\chi_5+\chi_{10}$	$\deg\chi_5=2$ $\deg\chi_9=\deg\chi_{10}=3$
X_8	$\mathrm{GL}_2(3)$	$\chi_4+\chi_8$ or $\chi_5+\chi_8$	$\deg\chi_4=\deg\chi_5=2$ $\deg\chi_8=4$
X_9	W_3	$\chi_4+\chi_5+\chi_8$	$\deg\chi_4=\deg\chi_5=2$ $\deg\chi_8=4$
X_{10}	W_2	$\chi_3+\chi_5+\chi_9+\chi_{10}$ or $\chi_4+\chi_5+\chi_9+\chi_{10}$	$\deg\chi_3=\deg\chi_4=1$ $\deg\chi_5=2$ $\deg\chi_9=\deg\chi_{10}=3$
X_{11}	W_3	$\chi_4+\chi_5+2\chi_8$	$\deg\chi_4=\deg\chi_5=2$ $\deg\chi_8=4$
X_{12}	$C_2\times A_5$	χ_{10}	$\deg\chi_{10}=5$
X_{13}	$C_2\times A_5$	$\chi_8+\chi_{10}$	$\deg\chi_8=4$ $\deg\chi_{10}=5$
X_{14}	$\mathrm{SL}_2(5)$	$\chi_2+\chi_3+\chi_7+\chi_9$	$\deg\chi_2=\deg\chi_3=2$ $\deg\chi_7=4$ $\deg\chi_9=6$
X_{15}	$C_2\times A_5$	$\chi_3+\chi_4+\chi_8+\chi_{10}$	$\deg\chi_3=\deg\chi_4=3$ $\deg\chi_8=4$ $\deg\chi_{10}=5$
X_{16}	$\mathrm{SL}_2(5)$	$\chi_2+\chi_3+\chi_7+2\chi_9$	See X_{14}
X_{17}	$\mathrm{SL}_2(5)$	$\chi_2+\chi_3+2\chi_7+2\chi_9$	See X_{14}
X_{18}	$\mathrm{SL}_2(5)$	$\chi_2+\chi_3+2\chi_7+3\chi_9$	See X_{14}

Table 3: The character χ_{hol} for the hyperelliptic curves with many automorphisms. The names of the irreducible characters for each group are taken from the character tables in Appendix A. The automorphism groups were determined in Theorem 5.6.

9. Determining which Jacobians have CM

Theorem 9.1. *For each curve X in Table 2 the Jacobian* $\mathrm{Jac}(X)$ *has CM or does not have CM as indicated in the table, unless the curve is marked with a "?".*

Proof. If X is of type X_1, X_2 or X_3, it is shown in Theorem 2.4.4 in [Roh09] that

Jac(X) has CM. Otherwise, the character χ_{hol} is sufficiently determined in Proposition 8.5 to determine whether Proposition 7.43 is applicable. If the criterion Proposition 7.43 is applicable, i.e. if

$$\langle \operatorname{Sym}^2 \chi_{\text{hol}}, \chi_{\text{triv}} \rangle = 0,$$

the Jacobian Jac(X) has CM. This supplies the "yes" entries in Table 2. For the "no" entries, we want to apply Corollary 7.42.

If $X = X_6$, then X is defined by $y^2 = s_4$ and it is shown on page 20 in Section 6.3 of [Wol00] that a simple factor of Jac(X) is isogenous to the genus one curve given by

$$y^2 = x^4 - 14x^2 + 1.$$

which has the non-integral j-invariant $\frac{2^4 \cdot 13}{3^2}$. Therefore, by Proposition 7.45, this elliptic curve does not have CM. Therefore, by Corollary 7.42, the abelian variety Jac(X) does not have CM.

If $X = X_{12}$, by Theorem 2 in [Pau13], we have Jac(X) $\sim E^5$, where E is the genus one curve defined by the affine equation

$$y^2 = x(x^2 + 11x - 1).$$

The elliptic curve E has the non-integral j-invariant $\frac{2^{14} \cdot 31^3}{5^3}$. Therefore, by Proposition 7.45, this elliptic curve does not have CM. Therefore, by Corollary 7.42, the abelian variety Jac(X) does not have CM.

Suppose that $X = X_{13}$. Then, as stated in Table 2, the curve X is defined by the affine equation

$$y^2 = r_5(x) = x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1.$$

Let

$$p(x) := x^4 - 228x^3 + 494x^2 + 228x + 1$$

and consider the morphism of function fields

$$\begin{aligned} \phi : \mathbb{C}(x, y)/(y^2 - p(x)) &\to \mathbb{C}(x, y)/(y^2 - r_5(x)) \\ x &\mapsto x^5 \\ y &\mapsto y. \end{aligned}$$

This induces a surjective morphism from X to the elliptic curve defined by the affine equation

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

The j-invariant of this elliptic curve is $\frac{2^{17}}{3^2}$. Therefore, by Proposition 7.45, it does not have CM. By Corollary 7.42, the abelian variety Jac(X) does not have CM.

Suppose that $X = X_8$. Then, by a computation in GAP in Appendix B.2, the automorphism group $\mathrm{Aut}(X)$ has a subgroup $G \cong S_3$ such that

$$\langle \mathrm{Res}_G(\chi_{\mathrm{hol}}), \mathrm{Res}_G(\chi_{\mathrm{triv}}) \rangle = 1.$$

By Lemma 6.3, we have

$$\dim H^0(X, \Omega_X)^G = \langle \mathrm{Res}_G(\chi_{\mathrm{hol}}), \mathrm{Res}_G(\chi_{\mathrm{triv}}) \rangle = 1$$

and therefore, by Proposition 6.1, the quotient curve $Y := X/G$ has genus one. Let $\overline{G}$ be the image of G in $\overline{\mathrm{Aut}}(X)$ and denote by $\phi : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}/\overline{G} \cong \mathbb{P}^1_{\mathbb{C}}$ the quotient map. In Appendix B.2, using Sage [S+17] and GAP [GAP17], we calculate $V_1 := \phi(W(x))$, using Lemma 6.8, and the branch points V_2 of ϕ in $\mathbb{P}^1_{\mathbb{C}}/\overline{G}$. Then, we iterate through the possible equations of Y given by Proposition 6.5. By a calculation in Sage [S+17] in Appendix B.2, we find that the j-invariant of Y is one of the following, where $\xi_8 = e^{2\pi i/8}$:

$$j_{8,1} := \frac{467888 + 855712\xi_8 + 855712\xi_8^3}{729},$$
$$j_{8,2} := \overline{j_{8,1}},$$
$$\frac{207646}{6561},$$
$$\frac{4000}{9},$$
$$\frac{-219488}{729}$$

By $\overline{j_{8,1}}$, we denote the complex conjugate of $j_{8,1}$. Because $j_{8,1}$ and $j_{8,2}$ are complex conjugates, either both or none of them is an algebraic integer. If both were algebraic integers, then $j_{8,1} + j_{8,2} = \frac{935776}{729}$ would be an algebraic case. Therefore, none of the possible j-invariants is an algebraic integer. Hence, the elliptic curve Y does not have CM by Proposition 7.45. Therefore, by Corollary 7.42, the abelian variety $\mathrm{Jac}(X)$ does not have CM.

Suppose that $X = X_{15}$. Analogously to the case where $X = X_8$, we find a group $G < \mathrm{Aut}(X)$ such that X/G has genus one. In this case, we have $G \cong A_4$. We proceed analogously to the case of $X = X_8$ and find that the j-invariant of $Y := X/G$ is one of the following, where $\xi_{15} = e^{2\pi i/15}$:

$$j_{15,1} := -\frac{149017}{240}\xi_{15}^7 + \frac{149017}{240}\xi_{15}^5 - \frac{149017}{120}\xi_{15}^4 + \frac{149017}{240}\xi_{15}^3 - \frac{149017}{240}\xi_{15}^2 - \frac{149017}{120}\xi_{15} + \frac{771047}{720},$$
$$j_{15,2} := \overline{j_{15,1}},$$
$$\frac{27436}{27},$$
$$\frac{-19465109}{248832},$$
$$\frac{357911}{2160}$$

We have $j_{15,1} + j_{15,2} = \frac{200941}{720}$. Therefore, as in the case of X_8, none of the possible j-invariants is an algebraic integer. It follows that the abelian variety $\mathrm{Jac}(X_{15})$ does not have CM. For the calculation of the j-invariants see Appendix B.2. □

10. Models of curves

10.1. Semi-stable models

Definition 10.1 (see page 246 in [BLR90]). Let X be a curve over an algebraically closed field K. A point x of X is an *ordinary double point* if the completion $\hat{\mathcal{O}}_{X,x}$ of the local ring $\mathcal{O}_{X,x}$ is isomorphic to $K[[s,t]]/(st)$.

Definition 10.2 (Definition 9.2.6 in [BLR90]). Let S be any scheme, and let g be an integer. A *semi-stable curve of genus g over S* is a proper and flat morphism $f : X \to S$ whose fibers $X_{\bar{s}}$ over geometric points $\bar{s}$ of S are reduced, connected, one-dimensional, and satisfy the following conditions:

(i) The scheme $X_{\bar{s}}$ has only ordinary double points as singularities.

(ii) We have $\dim_{k(\bar{s})} H^1(X_{\bar{s}}, \mathcal{O}_{X_{\bar{s}}}) = g$.

Definition 10.3 (see page 246 in [BLR90]). Let X be a semi-stable curve over an algebraically closed field K. We define the *dual graph* of X to be an undirected multigraph $\Gamma(X)$ as follows: The vertex set of $\Gamma(X)$ is the set of irreducible components of X. The edges correspond to the ordinary double points of X: Each singular point x of X which lies on some irreducible components X_1 and X_2 defines an edge connecting the vertices corresponding to X_1 and X_2.

Remark 10.4. Note that in this definition $X_1 = X_2$ is allowed.

Let R be a DVR, let K be its field of fractions and let $S = \mathrm{Spec}(R)$.

Definition 10.5. Let X be a smooth projective algebraic curve of genus g over K. A *semi-stable model of X over S* is a semi-stable curve $\mathcal{X}$ of genus g over S such that $\mathcal{X}_K \cong X$.

Remark 10.6. The semi-stable reduction theorem, Theorem 9.2.7 in [BLR90], asserts that every proper smooth geometrically connected curve X over K has a semi-stable model $\mathcal{X}$ after replacing K with some finite extension K' of K and R with the integral closure R' of R in K'.

10.2. Stable n-pointed curves of genus zero

For more information about n-pointed stable curves see [Knu83], [GHvdP88], [Kee92] and [Pin13]. The following definition is a special case of Definition 1.1 in [Knu83].

Definition 10.7. Let S be a scheme and let $n \in \mathbb{Z}_{\geq 3}$. An *$n$-pointed stable curve of genus zero over S* is a flat and proper morphism $f : X \to S$ together with n distinct sections $s_1, \dots, s_n : S \to X$ such that for each geometric fiber $X_{\bar{s}}$ of f

(i) the geometric fiber $X_{\bar{s}}$ is a reduced and connected curve such that each irreducible component is isomorphic to $\mathbb{P}^1_{k(\bar{s})}$ and any singularities are ordinary double points.

(ii) for all $i \in \{1, \dots, n\}$ the geometric fiber $X_{\bar{s}}$ is smooth at $s_i(\bar{s})$.

(iii) for all $i, j \in \{1, \dots, n\}$ we have $s_i(\bar{s}) \neq s_j(\bar{s})$ whenever $i \neq j$.

(iv) for every irreducible component E of $X_{\bar{s}}$ we have

$$|\{s_i(\bar{s}) \mid s_i(\bar{s}) \in E\} \cup \{\text{singularities on } E\}| \geq 3.$$

(v) we have $H^1(X_{\bar{s}}, \mathcal{O}_{X_{\bar{s}}}) = 0$.

Fact 10.8. *Conditions (i) and (v) imply together that the dual graph $\Gamma(X_{\bar{s}})$ is a tree.*

Let R be a DVR with fraction field K, a uniformizer $\pi \in R$ and residue field $k = R/(\pi)$ with $\operatorname{char} k > 2$. We set $S = \operatorname{Spec}(R)$.

Definition 10.9. Let $\mathcal{X}$ be an n-pointed stable curve of genus zero over S. We call $\Gamma(\mathcal{X}_{\bar{k}})$ the *dual tree of $\mathcal{X}$*, where $\bar{k}$ is an algebraic closure of k. The sections $s_1(k), \dots, s_n(k)$ of $\mathcal{X}_0$ induce markings $s_1^\Gamma, \dots, s_n^\Gamma \in V(\Gamma(\mathcal{X}_{\bar{k}}))$ such that $s_i^\Gamma = v$ if and only if $s_i(k)$ is in the irreducible component of $\mathcal{X}_{\bar{k}}$ that corresponds to v. We define

$$\begin{aligned} m_{\mathcal{X}} : V(\Gamma(\mathcal{X}_{\bar{k}})) &\to \mathbb{Z}_{\geq 0} \\ v &\mapsto \left|\left\{i \in \{1, \dots, n\} \mid s_i^\Gamma = v\right\}\right| \end{aligned}$$

to be the function that assigns the number of markings on a vertex v to the vertex.

Proposition 10.10. *Let $\lambda_1, \dots, \lambda_n \in K \cup \{\infty\}$ be n distinct points. Then there is, up to isomorphism, a unique n-pointed stable curve $\mathcal{X}$ of genus zero over S with $\mathcal{X}_\eta \cong \mathbb{P}^1_K$ and $\lambda_1, \dots, \lambda_n$ as sections in $\mathcal{X}_\eta$.*

Proof. This follows from the uniqueness of the stabilization and contraction operations. For more information on stabilization and contraction of n-pointed stable curves see Section 2 in [Knu83]. □

Lemma 10.11. *Let $\lambda_1, \dots, \lambda_n \in K$ be distinct elements. Then, there is a K-affine linear transformation $\mu : K \to K$ such that $\mu(\lambda_1), \dots, \mu(\lambda_n)$ lie in R and have at least two distinct equivalence classes* $\operatorname{mod} \pi$.

Proof. After multiplication with a sufficient power of π, we may assume without loss of generality that $\lambda_1, \dots, \lambda_n \in R$. Let $\mu_1(x) := x - \lambda_1$ and let $r \in \mathbb{Z}_{\geq 0}$ be such that $\pi^r | \mu(\lambda_i)$ and $\pi^{r+1} \nmid \mu(\lambda_i)$ for all $i \in \{1, \dots, n\}$. Let $\mu_2(x) := x/\pi^r$, then $\mu := \mu_2 \circ \mu_1$ has the desired property. $\square$

Let $\Lambda = \{\lambda_1, \dots, \lambda_n\} \subset K \cup \{\infty\}$ be a set of n distinct points with $n \geq 3$. After an application of Lemma 10.11, we may assume without loss of generality that $\Lambda \subset R \cup \{\infty\}$ and at least two of the elements of $\Lambda \cap R$ have different reductions $\operatorname{mod} \pi$. We want to construct the n-pointed stable curve of genus zero $\mathcal{C}$ over S with $\mathcal{X}_\eta \cong \mathbb{P}^1_K$ and the markings $\Lambda \subset \mathbb{P}^1_K$ in the generic fiber. We proceed iteratively to construct $\mathcal{C}$:

Let $\mathcal{C}^1 := \mathbb{P}^1_R$. We define the sections $s_i(K) := \lambda_i$ for $i \in \{1, \dots, n\}$. Then the sections $s_1(K), \dots, s_n(K)$ of $\mathbb{P}^1_K$ extend to sections $s_1(k), \dots, s_n(k) \in \mathbb{P}^1_k$ of the special fiber of $\mathbb{P}^1_R$, because Λ is a set of R-rational points in $\mathbb{P}^1_K$. Now $\mathbb{P}^1_R$ is "almost" an n-pointed stable curve of genus zero over S: Conditions (iii) and (iv) might be violated, since there might be $i, j \in \{1, \dots, n\}$ with $i \neq j$ such that $\lambda_i \equiv \lambda_j \pmod{\pi}$ and there might be only two distinct equivalence classes $\operatorname{mod} \pi$. If the stability condition (iv) is indeed violated, we add an auxiliary section $\delta : S \to \mathbb{P}^1_R$ that does not collide with any other sections in the special fiber. Then condition (iv) is not violated anymore, because there are at least two equivalence classes of the $\lambda_1, \dots, \lambda_n \pmod{\pi}$.

Suppose we are given a model $\mathcal{C}^l$ of $\mathbb{P}^1_K$ over S with sections $s_1, \dots, s_n$, such that $\mathcal{C}^l$ is "almost" an n-pointed stable curve of genus zero over S, in the sense that only condition (iii) possibly fails in the special fiber. For $i \in \{1, \dots, n\}$, we denote by

$$A_i := \{j \in \{1, \dots, n\} \mid s_i(k) = s_j(k)\}$$

the set indices of the sections which collide with $s_i(k)$ in the special fiber. If all of the A_i contain only one element each, the model $\mathcal{C}^l$ is already stable. Otherwise, we want to construct a model $\mathcal{C}^{l+1}$ with strictly fewer collisions. Pick some i_0 such that $|A_{i_0}| \geq 2$ and let $x : \mathbb{P}^1_K \to K$ denote a coordinate on $\mathbb{P}^1_K$ such that

$$x\left(\{\lambda_i \mid i \in A_{i_0}\}\right) \subset R$$

and

$$\{i \in \{1, \dots, n\} \mid x(\lambda_i) + (\pi) = x(\lambda_{i_0}) + (\pi)\} = A_{i_0}.$$

Let $r \in \mathbb{Z}_{\geq 1}$ be the largest integer such that for all $i, j \in A_{i_0}$ we have

$$\pi^r | (x(\lambda_i) - x(\lambda_j)).$$

Now, let $\mathcal{C}^{l+1}$ be the scheme obtained from $\mathcal{C}^l$ by blowing up the ideal

$$(x - x(\lambda_{i_0}), \pi^r) \subset R[x]$$

centered at the section $s_{i_0}(k) \in \mathcal{C}_0^l$. By doing this, a new irreducible component isomorphic to $\mathbb{P}_k^1$ is attached at $s_{i_0}(k)$ in $\mathcal{C}_0^l$ and affine coordinates for this new component on $\mathbb{P}_K^1$ are given by

$$x' = \frac{x - x(\lambda_{i_0})}{\pi^r} \quad \text{and} \quad y' = \frac{1}{x'}.$$

Then the sections $\{s_i \mid i \in A_{i_0}\}$ do not all collide in the same point of $\mathcal{C}_0^{l+1}$, since, by the definition of r, there are $i', j' \in A_{i_0}$ such that $x(\lambda_{i'}) \not\equiv x(\lambda_{j'}) \pmod{\pi^r}$. Also, we have

$$\{x'(\lambda_i) \mid i \in A_{i_0}\} \subset R$$

and therefore, for all $j \in A_{i_0}$, the section $s_j(k)$ lands in the smooth locus of the new irreducible component. The other sections in the special fiber, that is $\{s_i(k) \mid i \in \{1, \ldots, n\} \setminus A_{i_0}\}$, do not change, since the blow-up induces an isomorphism away from the closed point that we blow up. Also, the generic fiber $\mathbb{P}_K^1$ of $\mathcal{C}^l$ does not change when we blow up.

The scheme $\mathcal{C}^{l+1}$ is again "almost" an n-pointed stable curve of genus zero over S in the sense that only condition (iii) may be violated. Indeed, the new irreducible component of $\mathcal{C}_0^{l+1}$ has at least two distinct points with markings and is connected by a double point to the component in which the sections associated to A_{i_0} previously collided.

After finitely many steps of blowing up, we finally arrive at some scheme $\mathcal{C}'$ over S, where no sections collide in the special fiber. Let $\mathcal{C}$ be the model obtained from $\mathcal{C}'$ after possibly removing the auxiliary section δ and collapsing the corresponding component in the special fiber which becomes unstable, i.e. violating condition (iv), by using the contraction defined in Section 2 in [Knu83]. Then $\mathcal{C}$ is an n-pointed stable curve over S with markings $\lambda_1, \ldots, \lambda_n$ in the generic fiber $\mathbb{P}_K^1$ of $\mathcal{C}$.

10.3. The relative Picard functor

Definition 10.12 (see Theorem 2.13 in [Hat02])**.** If A is a topological space and B is a nonempty closed subspace that is a deformation retract of some neighborhood of B in A, we call (A, B) a *good pair*.

Lemma 10.13. *For a connected finite multi-graph G with n vertices and m edges, we have $H_0(G) \cong \mathbb{Z}$ and $H_1(G) \cong \mathbb{Z}^{m-n+1}$ and $H_l(G) = 0$ for $l > 1$.*

Proof. Let e be an edge in G which is not a loop. Then (G, e) is a good pair and the graph G' obtained from G by collapsing e has the same homology groups by Theorem 2.13 in [Hat02]. The graph G' has $n-1$ vertices and $m-1$ edges. The claim then follows by induction on the number of vertices, because if $n > 1$ there is at least one edge in G which is not a loop. The base case is the wedge sum of $m-n+1$ circles. □

Proposition 10.14. *Let X be a semi-stable curve over a field K. Then $\mathbf{Pic}^0_{X/K}$ is uniquely an extension of an abelian variety by an algebraic torus T. The rank of* *the torus part T is the rank of $H^1(\Gamma(X_{\overline{K}}), \mathbb{Z})$. In particular, the semi-abelian variety $\mathbf{Pic}^0_{X/K}$ is an abelian variety if and only if $\Gamma(X_{\overline{K}})$ is a tree.*

Proof. Let $G := \Gamma(X_{\overline{K}})$. By Example 8 in Chapter 9.2 of [BLR90], the scheme $\mathbf{Pic}^0_{X/K}$ is a semi-abelian variety of toric rank $\operatorname{rk} H^1(G, \mathbb{Z})$. To prove the last statement of the proposition, let $n := |V(G)|$ and $m := |E(G)|$. Because G is connected, it is a tree if and only if $n - m = 1$. The conclusion follows with Lemma 10.13 and the universal coefficients theorem for cohomology. □

Let R be a DVR, let K be its field of fractions, let π be a uniformizer of R, and let $k = R/(\pi)$ be the residue field. Suppose that $\operatorname{char} k > 2$ and let $S = \operatorname{Spec}(R)$.

Proposition 10.15. *Let X be a geometrically irreducible projective algebraic curve over K and let $\mathcal{X}$ be a projective semi-stable model of X over S such that the irreducible components of $\mathcal{X}_k$ are geometrically irreducible. Then $\mathbf{Pic}_{\mathcal{X}/S}$ exists and has an open group subscheme $\mathbf{Pic}^0_{\mathcal{X}/S}$ of finite type whose fibers are $\mathbf{Pic}^0_{X/K}$ and $\mathbf{Pic}^0_{\mathcal{X}_k/k}$. Furthermore, the scheme $\mathbf{Pic}^0_{\mathcal{X}/S}$ is smooth over S.*

Proof. By Theorem 9.4.18.1 in Part 5 of [FGI+05], the scheme $\mathbf{Pic}_{\mathcal{X}/S}$ exists and represents $\operatorname{Pic}_{(\mathcal{X}/S)(\text{ét})}$. By Remark 7.33, the scheme $\mathbf{Pic}_{\mathcal{X}/S}$ also represents $\operatorname{Pic}_{(\mathcal{X}/S)(\text{fppf})}$. By Example 8 in Section 9.2 in [BLR90], the schemes $\mathbf{Pic}_{X/K}$ and $\mathbf{Pic}_{\mathcal{X}_k/k}$ exist and by Proposition 9.5.19 in Part 5 of [FGI+05] they are smooth. By Corollary 9.5.13 in Part 5 of [FGI+05], we have $\dim_K \mathbf{Pic}_{X/K} = \dim_K(X, \mathcal{O}_X)$ and $\dim_k \mathbf{Pic}_{\mathcal{X}_k/k} = \dim_k(\mathcal{X}_k, \mathcal{O}_{\mathcal{X}_k})$. By the definition of a semi-stable curve, it follows that $\dim_K \mathbf{Pic}_{X/K} = \dim_k \mathbf{Pic}_{\mathcal{X}_k/k}$. Now we can apply Proposition 9.5.20 in Part 5 of [FGI+05]: There is an open group subscheme $\mathbf{Pic}^0_{\mathcal{X}/S}$ of $\mathbf{Pic}_{\mathcal{X}/S}$ with generic fiber $\mathbf{Pic}^0_{\mathcal{X}/S} \times_S \operatorname{Spec}(K) \cong \mathbf{Pic}^0_{X/K}$ and special fiber $\mathbf{Pic}^0_{\mathcal{X}/S} \times_S \operatorname{Spec}(k) \cong \mathbf{Pic}^0_{\mathcal{X}_k/k}$. Furthermore, because S is reduced, it follows from the same Proposition that $\mathbf{Pic}^0_{\mathcal{X}/S}$ is smooth over S. □

10.4. Associated trees

We fix some conventions on graphs that we use throughout the remainder of this Section.

Definition 10.16. Let T be a rooted tree with root r. Let $v_1, v_2 \in V(T)$ be adjacent vertices. Then v_1 is called the *parent* of v_2 and v_2 is called a *child* of v_1 if the unique path from r to v_2 contains v_1. The set of *descendants of* v for $v \in V(T)$ is defined as

$$D_T(v) := \{w \in V(T) \mid \text{the (unique) path from } r \text{ to } w \text{ contains } v\}.$$

The subtree T_v is defined to be the full subgraph of T induced by $D_T(v)$. We define

$$\ell_T(v) := |D_T(v) \cap \{\text{leaves of } T\}|$$

to be the number of descendants v which are leaves of T.

For a graph G and an edge $e \in E(G)$, we denote by $G - e$ the graph which is obtained from G by deleting the edge e (but not its incident vertices).

Example 10.17. For a rooted tree T with root r, we have $T_r = T$. For every leaf $l \in V(T)$, the graph T_l consists only of the vertex l.

Let R and K and k and π be as in the previous Subsection and denote by $v : K \to \mathbb{Z} \cup \{\infty\}$ the discrete valuation on K that induces R. For some $n \geq 3$, let $\lambda_1, \ldots, \lambda_n \in R$ be distinct elements. We set $\Lambda := \{\lambda_1, \ldots, \lambda_n\}$. Following Section 5 in [Bos80], we construct a tree T_A associated to $\lambda_1, \ldots, \lambda_n$. The subscript A stands for *associated*. Let $s \in \mathbb{R}_{>1}$ and denote by $|\cdot|_v$ the non-archimedean norm induced on K by v defined by $|\lambda|_v := s^{-v(\lambda)}$ for all $\lambda \in K$. We define the vertex set of T_A by

$$V(T_A) := \{B \cap \Lambda \mid B \subset K \text{ is a closed ball in the } |\cdot|_v\text{-norm such that } B \cap \Lambda \neq \emptyset\}.$$

The edges are given by

$$E(T_A) := \{\{v_1, v_2\} \mid v_1, v_2 \in V(T_A) \text{ such that } v_1 \subsetneq v_2 \text{ and } \nexists w \in V(T_A) : v_1 \subsetneq w \subsetneq v_2\}.$$

Definition 10.18. The graph T_A is called the *associated tree* of $\lambda_1, \ldots, \lambda_n$. We call $\Lambda = \{\lambda_1, \ldots, \lambda_n\}$ the *root* of T_A.

Remark 10.19. The construction is independent of the parameter $s > 1$, since the norms are equivalent for different choices of s.

Proposition 10.20. *The graph T_A is a rooted tree.*

Proof. Since $\Lambda \in V(T_A)$ and every $v \in V(T_A)$ is a subset of Λ and there are only finitely many vertices, it follows that there is a path from v to Λ in T_A. Therefore, the graph T_A is connected. Assume, for contradiction, that T_A is not a tree. Then, there is a cycle $(v_1, \ldots, v_l)$ for some pairwise different $v_1, \ldots, v_l \in V(T_A)$. The graph T_A induces a directed graph T' as follows: We set $V(T') := V(T_A)$ and for each edge $\{v_1, v_2\} \in E(T_A)$ we add the directed edge (v_1, v_2) to $E(T')$ if $v_2 \subset v_1$. Otherwise, we have $v_1 \subset v_2$ and add the directed edge (v_2, v_1) to T'. Then $(v_1, \ldots, v_l)$ is not a cycle in T', because the inclusions of the vertices in each other are strict. Therefore, there exists some $i \in \{1, \ldots, l\}$ such that $(v_{i-1}, v_i) \in E(T')$ and $(v_{i+1}, v_i) \in E(T')$, where we set $v_0 := v_l$ and $v_{l+1} := v_1$. Then, we have $v_{i-1} \supsetneq v_i \subsetneq v_{i+1}$ and it follows that $v_{i-1} \cap v_{i+1} \neq \emptyset$. Since the metric on K that is induced by $|\cdot|_v$ is an ultrametric, it follows that either $v_i \subsetneq v_{i-1} \subsetneq v_{i+1}$ or $v_i \subsetneq v_{i+1} \subsetneq v_{i-1}$. But this is a contradiction to the fact that $\{v_i, v_{i+1}\} \in E(T_A)$ and $\{v_i, v_{i-1}\} \in E(T_A)$. □

If n is odd, let $T_A^{(1)}$ be the tree obtained from T_A by adding one extra leaf $\{\infty\}$ to the root vertex $\Lambda = \{\lambda_1, \ldots, \lambda_n\} \in V(T_A)$. Otherwise, let $T_A^{(1)} := T_A$. Let $T_A^{(2)}$ be the tree obtained from $T_A^{(1)}$ in the following way: If the root $\Lambda \in V(T_A^{(1)})$ has more than two children in $T_A^{(1)}$, let $T_A^{(2)} := T_A^{(1)}$. Otherwise, by the construction of $T_A^{(1)}$ and T_A, the root Λ has exactly two children in $T_A^{(1)}$. In this case, we let $T_A^{(2)}$ be the tree obtained from $T_A^{(1)}$ by "collapsing" the root node. More precisely, we add an edge $\{v_1, v_2\}$ connecting the two children of Λ in $T_A^{(1)}$ and remove Λ and the edges incident to Λ in $T_A^{(1)}$ and call the resulting tree $T_A^{(2)}$. We do this, so that the tree $T_A^{(2)}$ is stable in the sense that every non-leaf vertex has degree at least 3.

Let T'_A be the tree obtained from $T_A^{(2)}$ by removing all vertices that are leaves in $T_A^{(2)}$. We define the map

$$\begin{aligned} m_A : V(T'_A) &\to \mathbb{Z}_{\geq 0} \\ v &\mapsto \left| \left\{ \text{leaves adjacent to } v \text{ in } T_A^{(2)} \right\} \right| \end{aligned}$$

that counts the leaves in $T_A^{(2)}$ adjacent to each non-leaf vertex $v \in T_A^{(2)}$.

Lemma 10.21. *If n is even, let $\Lambda' := \{\lambda_1, \ldots, \lambda_n\}$. Otherwise, let $\Lambda' := \{\lambda_1, \ldots, \lambda_n, \infty\}$. Let $\mathcal{C}$ be the n-pointed stable curve of genus zero over S with markings $\Lambda' \subset \mathbb{P}^1_K$ in the generic fiber constructed in Section 10.2. Denote by T the dual tree of $\mathcal{C}$. Then, there is a canonical isomorphism $f : T'_A \to T$ such that $m_A(v) = m_{\mathcal{C}}(f(v))$ for all $v \in V(T'_A)$.*

Proof. Both T'_A and $\mathcal{C}_0$ can be constructed by iteratively adding new vertices, respectively, irreducible components, to distinguish the markings that are the same up to some power of π, and contracting at most one vertex, respectively at most one irreducible component that is unstable.

More precisely, let $v \in V(T_A)$ be a vertex and let $v_1, \ldots, v_l$ be the children of v. The elements of v cannot be further distinguished $\bmod \pi^r$ for some $r \in \mathbb{Z}_{>0}$. Let $r' > r$ be the smallest integer such that $\bmod \pi^{r'}$ not all of the elements of v are equivalent. Then $v_1, \ldots, v_l$ are the subsets of v whose elements are equivalent $\bmod \pi^{r'}$.

For $\mathcal{C}_0$ the situation is analogous: As described in Section 10.2, we repeatedly blow up points in the special fiber where several sections collide. Also in this case, we blow up with the smallest possible power of π such that not all of the sections which previously collided, collide in the blow-up. The final contraction in the construction of $\mathcal{C}_0$ in Section 10.2 corresponds to "collapsing" the root node to go from $T_A^{(1)}$ to $T_A^{(2)}$ in the construction of T'_A above. □

Let $n \geq 5$ and let X be the projective hyperelliptic curve given by the affine equation

$$y^2 = \prod_{i=1}^{n} (x - \lambda_i).$$

Let $\hat{K}$ be the completion of K with respect to $|\cdot|_v$ and let $\hat{R}$ be the corresponding completion of R. In Theorem 4.2 in [Bos80], a semi-stable model $\mathcal{X}$ of $X_{\hat{F}}$ is constructed for some finite extension $\hat{F}$ of $\hat{K}$ over the corresponding extension $\hat{R}'$ of $\hat{R}$. Denote by k' the residue field of $\hat{R}'$ and let $\overline{k'}$ be an algebraic closure of k'. Furthermore, the irreducible components of the special fiber $\mathcal{X}_0$ are geometrically irreducible. The special fiber $\mathcal{X}_0$ is described in the following two lemmas.

Lemma 10.22. *The non-leaf vertices of the associated tree T_A of $\lambda_1, \dots, \lambda_n$ correspond to the irreducible components of $\mathcal{X}_0$ as follows: Let $v \in V(T_A)$ be a non-leaf and let $v_1, \dots, v_r$ be the children of v. If*

$$\ell_{T_A}(v_1) \equiv \cdots \equiv \ell_{T_A}(v_r) \equiv 0 \pmod 2$$

then v corresponds to two disjoint irreducible components $C_{v,1}$ and $C_{v,2}$ of $\mathcal{X}_0$ with $C_{v,1} \cong C_{v,2} \cong \mathbb{P}^1_{k'}$. Otherwise, the vertex v corresponds to a single irreducible component $C_{v,1}$ of $\mathcal{X}_0$.

Proof. See paragraph A) on page 38 in Section 5 in [Bos80]. □

Lemma 10.23. *The singularities of $\mathcal{X}_{\overline{k'}}$ are characterized as follows: Let C_{u,i_1} and C_{w,i_2} be irreducible components of $\mathcal{X}_0$ corresponding to non-leaf vertices $u, w \in V(T_A)$. They are disjoint if and only if u and w are not neighbors in T_A. Suppose that u and w are neighbors and that $w \subset u$. Then C_{u,i_1} and C_{w,i_2} intersect in exactly two points if and only if $\ell_{T_A}(w)$ is even and neither u nor w have two disjoint irreducible components corresponding to them. Otherwise, that is if $\ell_{T_A}(w)$ is odd or at least one of u and w has two irreducible components corresponding to it, the components C_{u,i_1} and C_{w,i_2} intersect in exactly one point.*

Proof. See paragraph B) on page 38 in Section 5 in [Bos80]. □

Lemma 10.24. *The graph $\Gamma(\mathcal{X}_{\overline{k'}})$ is a tree if and only if for every non-root vertex $v \in V(T_A)$ the number of descendant leaves $\ell_{T_A}(v)$ is odd.*

Proof. If $\ell_{T_A}(v)$ is odd for all non-root vertices $v \in V(T_A)$, then by Lemma 10.22, each non-leaf vertex $w \in V(T_A)$ corresponds to a unique vertex of $\Gamma(\mathcal{X}_{\overline{k'}})$. By Lemma 10.22, because for each child w of a vertex v in $V(T_A)$ the number $\ell_{T_A}(w)$ is odd, there are no multiple edges in T_A. Two vertices of $\Gamma(\mathcal{X}_{\overline{k'}})$ are connected by an edge, if and only if the corresponding vertices in T_A are neighbors. Then $\Gamma(\mathcal{X}_{\overline{k'}})$ is a tree, because T_A is a tree.

Conversely, suppose that $\Gamma(\mathcal{X}_{\overline{k'}})$ is a tree.

Claim: No vertex in $v \in V(T_A)$ corresponds to two irreducible components in $\mathcal{X}_{\overline{k'}}$.

Proof. Assume, for contradiction, that there is a (non-leaf) vertex $v \in V(T_A)$ that corresponds to two irreducible components in $\mathcal{X}_{\overline{k'}}$. Denote by w_1 and w_2 the vertices in $\Gamma(\mathcal{X}_{\overline{k'}})$ that correspond to the two irreducible components in $\mathcal{X}_{\overline{k'}}$ that correspond to v. Let $v_1, \dots, v_l \in V(T_A)$ be the children of v in T_A. We have $l \geq 2$, because every non-leaf vertex of T_A has at least two children by the construction of T_A. Note that $v_1, \dots, v_l$ are not leaves in T_A, because $\ell_{T_A}(t)$ is odd for any leaf $t \in V(T_A)$. Let w_1' and w_2' be vertices in $\Gamma(\mathcal{X}_{\overline{k'}})$ that correspond to v_1 and v_2, respectively. Then by Lemma 10.23, we have $\{w_1, w_1'\}, \{w_2, w_1'\}, \{w_1, w_2'\}, \{w_2, w_2'\} \in E(T_A)$. We have found the cycle $(w_1, w_1', w_2, w_2', w_1)$ in $\Gamma(\mathcal{X}_{\overline{k'}})$ and therefore, thee graph $\Gamma(\mathcal{X}_{\overline{k'}})$ is not a tree. □

Assume, for contradiction, that there is a non-root vertex $v \in V(T_A)$ with $\ell_{T_A}(v) \equiv 0 \pmod 2$. Let $w \in V(T_A)$ be the parent of v. Then, by the Claim and Lemma 10.22, the vertices v and w both correspond to unique vertices v' and w' in $\Gamma(\mathcal{X}_{\overline{k}})$. Because $\ell_{T_A}(v)$ is even, by Lemma 10.23, the vertices v' and w' are connected by two edges which gives the desired contradiction. □

10.5. A criterion for potential good reduction of $\mathbf{Pic}^0_{X/K}$

Theorem 10.25. *Let X be a hyperelliptic curve with branch points $\lambda_1, \dots, \lambda_n \in \mathbb{P}^1_K$ for some number field K and let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal such that $2 \notin \mathfrak{p}$. Let $\mathcal{Y}$ denote the n-pointed stable curve of of genus zero over* $\operatorname{Spec}(\mathcal{O}_{K,\mathfrak{p}})$ *with the markings $\lambda_1, \dots, \lambda_n$ in the generic fiber. Then $\mathbf{Pic}^0_{X/K}$ has potential good reduction at $\mathfrak{p}$ if and only if the following condition holds for every edge e of the dual tree T of $\mathcal{Y}$: Let T_1 and T_2 be the two connected components of $T - e$. Then, the marked trees T_1 and T_2 each have an odd number of markings, i.e.*

$$\sum_{v \in V(T_1)} m_{\mathcal{Y}}(v) \equiv \sum_{v \in V(T_2)} m_{\mathcal{Y}}(v) \equiv 1 \pmod 2.$$

Proof. After multiplication of $\lambda_1, \dots, \lambda_n$ with a suitable power of a generator of $\mathfrak{p}$, we may assume that $\lambda_1, \dots, \lambda_n \in \mathcal{O}_{K,\mathfrak{p}} \cup \{\infty\}$. Let $\mathcal{X}$ be the semi-stable model of $X_{\hat{F}}$, constructed in [Bos80] and mentioned in the previous Subsection, for some finite extension $\hat{F}$ of $\hat{K}$. By Proposition 7.24 and Proposition 7.35, the abelian variety $\mathbf{Pic}^0_{X_{\hat{F}}/\hat{F}}$ has potential good reduction over the extension $\hat{R}$ of $\mathcal{O}_{K,\mathfrak{p}}$ to $\hat{F}$ if and only if $\mathbf{Pic}^0_{X_K/K}$ has potential good reduction over $\mathcal{O}_{K,\mathfrak{p}}$. Let $S = \operatorname{Spec}(\hat{R})$ and denote by k the residue field of $\hat{R}$. By Proposition 10.15, the generic fiber of $\mathbf{Pic}^0_{\mathcal{X}/S}$ is $\mathbf{Pic}^0_{X_{\hat{F}}/\hat{F}}$ and the special fiber is $\mathbf{Pic}^0_{\mathcal{X}_0/k}$. By Proposition 10.14, the special fiber $\mathbf{Pic}^0_{\mathcal{X}_0/k}$ is a semi-abelian variety with toric rank $r := \operatorname{rk} H^1(\Gamma(\mathcal{X}_{\overline{k}}), \mathbb{Z})$. Therefore, the abelian variety $\mathbf{Pic}^0_{X_{\hat{F}}/\hat{F}}$ has semi-stable reduction of toric rank r over $\hat{R}$. By Proposition 7.23, the abelian variety $\mathbf{Pic}^0_{X_{\hat{F}}/\hat{F}}$ has potential good reduction over $\hat{R}$ if and only if $r = 0$. By Proposition 10.14, this is the case if and only if $\Gamma(\mathcal{X}_{\overline{k}})$ is a tree. Let T_A be the associated tree of $\{\lambda_1, \dots, \lambda_n\} \setminus \{\infty\}$. By Lemma 10.24, the dual graph $\Gamma(\mathcal{X}_{\overline{k}})$ is a tree if and only if for every non-root vertex of $v \in V(T_A)$ the number $\ell(v)$ is odd. Let T_A' and $m_A : V(T_A') \to \mathbb{Z}_{\geq 0}$ be as constructed in Section 10.4. Let T_v'

denote the subtree of T'_A with root v. Then

$$\sum_{w \in T'_v} m_A(w) = \ell_{T_A}(v).$$

By Lemma 10.21, there is an isomorphism $f : T'_A \to T$ such that $m_{\mathcal{Y}}(f(w)) = m_A(w)$ for all $w \in V(T'_A)$. Let $e \in E(T'_A)$ be the edge connecting v and its parent in T'_A. The subtree T'_v of T'_A then corresponds to one of the connected components C of $T - f(e)$. It follows that

$$\sum_{w \in V(T'_v)} m_A(w) = \sum_{w \in V(T - f(e))} m_{\mathcal{Y}}(w)$$

and therefore, the component C contains an odd number of markings if and only if $\ell_{T_A}(v)$ is odd. Because the total number of markings n is even, the other component C' of $T - f(e)$ contains the same parity of markings as C. The conclusion follows, because every edge of T is in the image of f. $\square$

Corollary 10.26. *Suppose that the hyperelliptic curve X is defined by the affine equation*

$$y^2 = f(x) := \prod_{i=1}^{n} (x - \lambda_i)$$

for some $\lambda_1, \ldots, \lambda_n \in \mathcal{O}_K$ for some number field K. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal with a generator $p \in \mathcal{O}_K$, such that $\operatorname{char} \mathcal{O}_{K,\mathfrak{p}} > 2$ *and such that p does not divide the discriminant $\Delta(f)$ in $\mathcal{O}_K$. Then $\mathbf{Pic}^0_{X/K}$ has potential good reduction at $\mathfrak{p}$.*

Proof. We have

$$\Delta(f) = \prod_{1 \le i < j \le n} (\lambda_i - \lambda_j)^2.$$

Therefore, for all $i, j \in \{1, \ldots, n\}$ with $i \neq j$, we have $p \nmid (\lambda_i - \lambda_j)$. Let k be the residue field of $\mathcal{O}_{K,\mathfrak{p}}$, then because $\lambda_i \not\equiv \lambda_j \pmod{p}$, the reductions $\overline{\lambda_1} := \lambda_1 + (p), \ldots, \overline{\lambda_n} := \lambda_n + (p) \in k$ are all different. Therefore, the special fiber of the n-pointed stable curve over $\operatorname{Spec}(\mathcal{O}_{K,\mathfrak{p}})$ with markings $\lambda_1, \ldots, \lambda_n$ is isomorphic to $\mathbb{P}^1_k$ and the dual tree is just one vertex without any edges. The conclusion follows from Theorem 10.25. $\square$

Remark 10.27. If we want to check whether $\mathbf{Pic}^0_{X/K}$ for a hyperelliptic curve X given by the affine equation

$$y^2 = f(x) := \prod_{i=1}^{n} (x - \lambda_i)$$

for $\lambda_1, \ldots, \lambda_n \in \mathcal{O}_K$ for some number field K has potential good reduction at all primes of $\mathcal{O}_K$ such that the residue field does not have characteristic two, Corollary 10.26 implies that the condition in Theorem 10.25 only needs to be verified for finitely many primes $p_1, \ldots, p_s$, namely the prime factors of $\Delta(f)$. Since the dual tree of the n-pointed stable model of $\mathbb{P}^1_K$ over a DVR with fraction field K can be algorithmically constructed, for example by using the associated tree defined above, we can algorithmically decide whether $\mathbf{Pic}^0_{X/K}$ has potential good reduction everywhere, except in characteristic two.

10.6. Application to the hyperelliptic curves with many automorphisms

For the hyperelliptic curves with many automorphisms in Table 2, we can now determine whether their Jacobians have potential good reduction in characteristic > 2. Unfortunately, for the curves X_{10}, X_{11}, X_{16}, X_{17} and X_{18} for which we did not determine if their Jacobians have CM in Theorem 9.1, it turns out that their Jacobians have potential good reduction in all characteristics > 2. Therefore, we cannot apply Proposition 7.46 to prove that the Jacobians do not have CM.

In the following examples, for each curve X given by $y^2 = f(x)$ in Table 2 whose Jacobian does not have CM, or where we do not know whether it has CM, we calculate the dual trees of the pointed stable curves of genus zero that are marked with the branch points $W(X)$. We do this at all primes that do not lie above 2 which divide the discriminant of the polynomial $f(x)$ defining the curve. We then know all characteristics > 2 for which $\mathrm{Jac}(X)$ does not have potential good reduction. The calculations were done by constructing the associated trees in Sage [S+17] in Appendix B.3.

In the following examples, the numbers on the vertices of the dual trees are the numbers of markings on the corresponding irreducible components of the pointed stable curves.

Example 10.28.
The Jacobian $\mathrm{Jac}(X_6)$ does not have potential good reduction in characteristic 3, as can be seen from the dual tree of the pointed stable curve and applying Theorem 10.25.

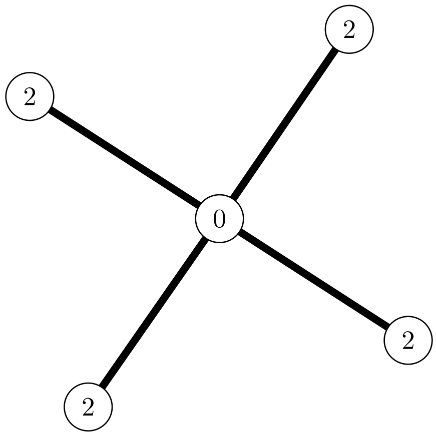

Figure 1: Dual tree of the pointed stable curve of genus zero associated to the curve X_6 and $\operatorname{char} k = 3$

Example 10.29.
The Jacobian $\operatorname{Jac}(X_8)$ does not have potential good reduction in characteristic 3.

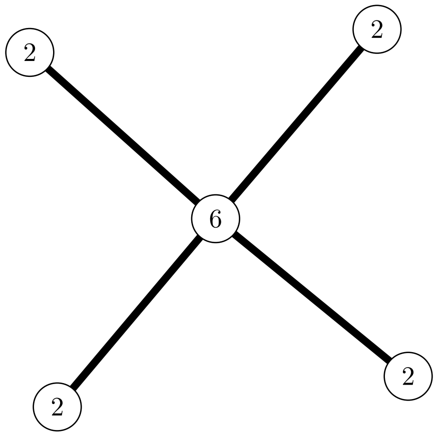

Figure 2: Dual tree of the pointed stable curve of genus zero associated to the curve X_8 and $\operatorname{char} k = 3$

Example 10.30.
The Jacobian $\operatorname{Jac}(X_{10})$ has potential good reduction in all characteristics > 2.

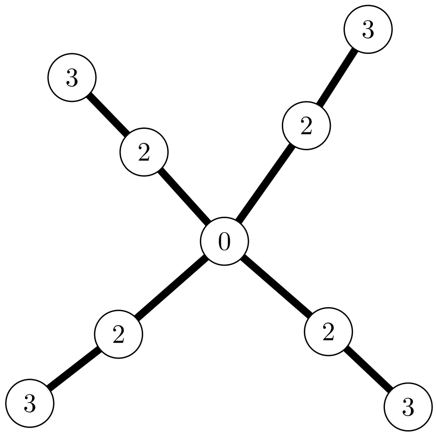

Figure 3: Dual tree of the pointed stable curve of genus zero associated to the curve X_{10} and $\operatorname{char} k = 3$

Example 10.31.
The Jacobian $\mathrm{Jac}(X_{11})$ has potential good reduction in all characteristics > 2.

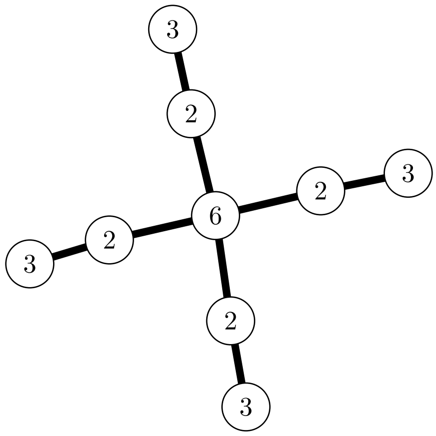

Figure 4: Dual tree of the pointed stable curve of genus zero associated to the curve X_{11} and $\operatorname{char} k = 3$

Example 10.32.
The Jacobian $\mathrm{Jac}(X_{12})$ does not have potential good reduction in characteristic 5.

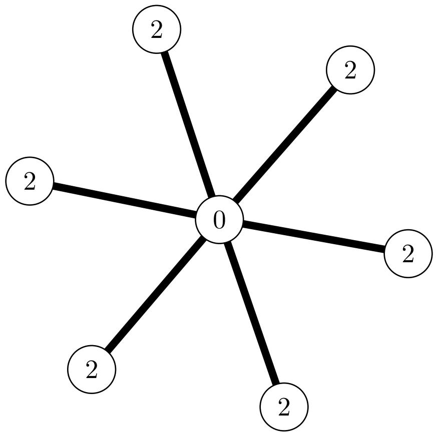

Figure 5: Dual tree of the pointed stable curve of genus zero associated to the curve X_{12} and $\operatorname{char} k = 5$

Example 10.33.
The Jacobian $\operatorname{Jac}(X_{13})$ does not have potential good reduction in characteristic 3.

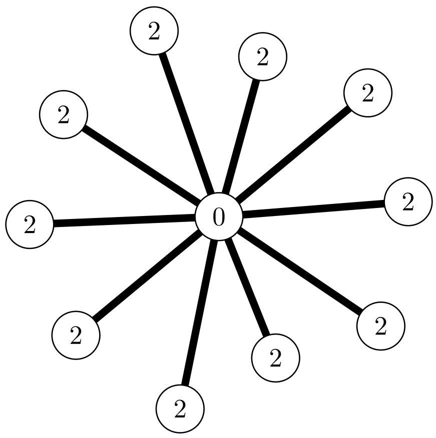

Figure 6: Dual tree of the pointed stable curve of genus zero associated to the curve X_{13} and $\operatorname{char} k = 3$

Figure 7: Dual tree of the pointed stable curve of genus zero associated to the curve X_{13} and $\operatorname{char} k = 5$

Example 10.34.

The Jacobian $\mathrm{Jac}(X_{15})$ does not have potential good reduction in characteristic 3 and 5.

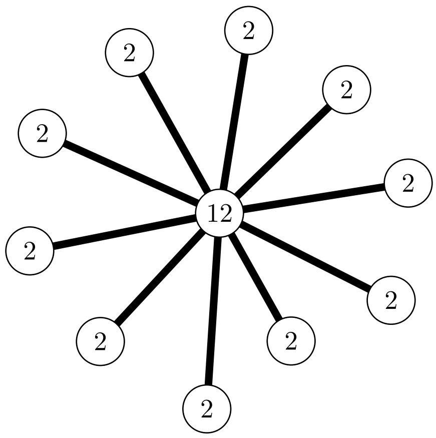

Figure 8: Dual tree of the pointed stable curve of genus zero associated to the curve X_{15} and $\mathrm{char}\, k = 3$

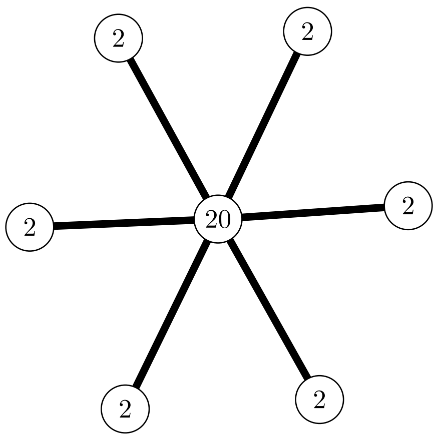

Figure 9: Dual tree of the pointed stable curve of genus zero associated to the curve X_{15} and $\mathrm{char}\, k = 5$

Example 10.35.
The Jacobian $\mathrm{Jac}(X_{16})$ has potential good reduction in all characteristics > 2.

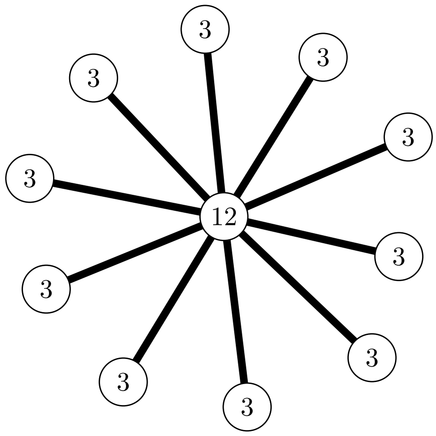

Figure 10: Dual tree of the pointed stable curve of genus zero associated to the curve X_{16} and $\operatorname{char} k = 3$

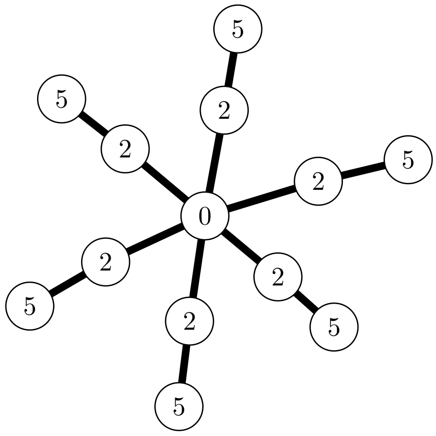

Figure 11: Dual tree of the pointed stable curve of genus zero associated to the curve X_{16} and $\operatorname{char} k = 5$

Example 10.36.
The Jacobian $\mathrm{Jac}(X_{17})$ has potential good reduction in all characteristics > 2.

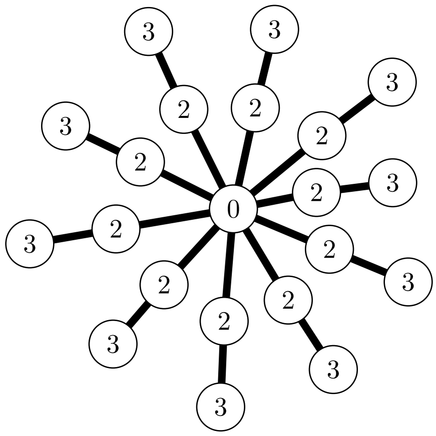

Figure 12: Dual tree of the pointed stable curve of genus zero associated to the curve X_{17} and $\operatorname{char} k = 3$

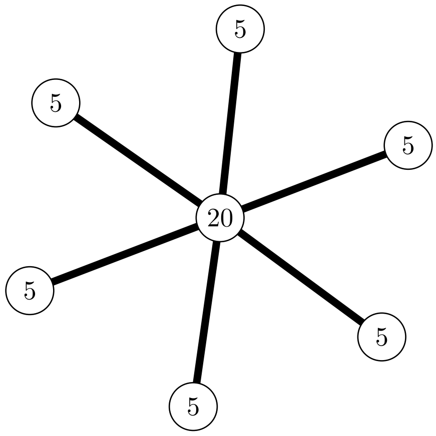

Figure 13: Dual tree of the pointed stable curve of genus zero associated to the curve X_{17} and $\operatorname{char} k = 5$

Example 10.37.
The Jacobian $\mathrm{Jac}(X_{18})$ has potential good reduction in all characteristics > 2.

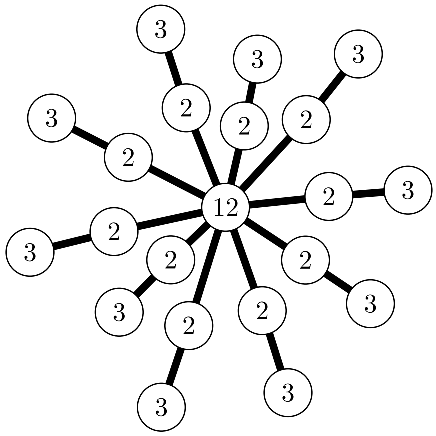

Figure 14: Dual tree of the pointed stable curve of genus zero associated to the curve X_{18} and $\operatorname{char} k = 3$

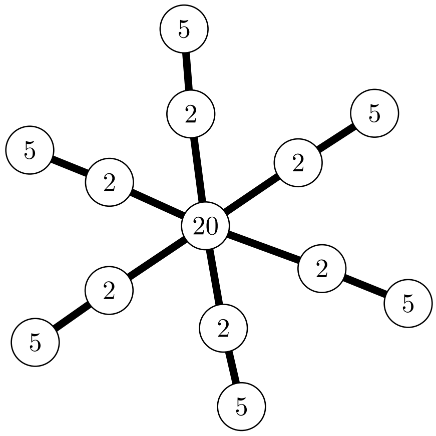

Figure 15: Dual tree of the pointed stable curve of genus zero associated to the curve X_{18} and $\operatorname{char} k = 5$

A. Character tables

The following character tables were computed using GAP [GAP17].

ord(·)	1	6	6	2	3	3	4
Class size	1	4	4	1	4	4	6
χ_1	1	1	1	1	1	1	1
χ_2	1	α^2	α	1	α	α^2	1
χ_3	1	α	α^2	1	α^2	α	1
χ_4	2	1	1	-2	-1	-1	0
χ_5	2	α	α^2	-2	$-\alpha^2$	$-\alpha$	0
χ_6	2	α^2	α	-2	$-\alpha$	$-\alpha^2$	0
χ_7	3	0	0	3	0	0	-1

Table 4: The character table of $\mathrm{SL}_2(3)$, where $\alpha = e^{2\pi i/3}$

ord(·)	1	6	2	3	4	8	8	2
Class size	1	8	1	8	6	6	6	12
χ_1	1	1	1	1	1	1	1	1
χ_2	1	1	1	1	1	-1	-1	-1
χ_3	2	-1	2	-1	2	0	0	0
χ_4	2	1	-2	-1	0	$-\alpha$	α	0
χ_5	2	1	-2	-1	0	α	$-\alpha$	0
χ_6	3	0	3	0	-1	1	1	-1
χ_7	3	0	3	0	-1	-1	-1	1
χ_8	4	-1	-4	1	0	0	0	0

Table 5: The character table of $\mathrm{GL}_2(3)$, where $\alpha = e^{2\pi i/8} + e^{6\pi i/8}$

ord(·)	1	2	2	2	3	6	2	2	4	4
Class size	1	1	6	6	8	8	3	3	6	6
χ_1	1	1	1	1	1	1	1	1	1	1
χ_2	1	-1	-1	1	1	-1	1	-1	-1	1
χ_3	1	-1	1	-1	1	-1	1	-1	1	-1
χ_4	1	1	-1	-1	1	1	1	1	-1	-1
χ_5	2	-2	0	0	-1	1	2	-2	0	0
χ_6	2	2	0	0	-1	-1	2	2	0	0
χ_7	3	-3	-1	1	0	0	-1	1	1	-1
χ_8	3	-3	1	-1	0	0	-1	1	-1	1
χ_9	3	3	-1	-1	0	0	-1	-1	1	1
χ_{10}	3	3	1	1	0	0	-1	-1	-1	-1

Table 6: The character table of $C_2 \times S_4$

ord(·)	1	4	2	3	2	4	4	6	2	4
Class size	1	6	1	8	3	6	6	8	3	6
χ_1	1	1	1	1	1	1	1	1	1	1
χ_2	1	-1	1	1	1	-1	-1	1	1	-1
χ_3	1	$-i$	-1	1	1	i	$-i$	-1	-1	i
χ_4	1	i	-1	1	1	$-i$	i	-1	-1	$-i$
χ_5	2	0	-2	-1	2	0	0	1	-2	0
χ_6	2	0	2	-1	2	0	0	-1	2	0
χ_7	3	-1	3	0	-1	-1	1	0	-1	1
χ_8	3	1	3	0	-1	1	-1	0	-1	-1
χ_9	3	$-i$	-3	0	-1	i	i	0	1	$-i$
χ_{10}	3	i	-3	0	-1	$-i$	$-i$	0	1	i

Table 7: The character table of W_2

ord(·)	1	4	3	4	2	8	6	8
Class size	1	12	8	6	1	6	8	6
χ_1	1	1	1	1	1	1	1	1
χ_2	1	-1	1	1	1	-1	1	-1
χ_3	2	0	-1	2	2	0	-1	0
χ_4	2	0	-1	0	-2	α	1	$-\alpha$
χ_5	2	0	-1	0	-2	$-\alpha$	1	α
χ_6	3	1	0	-1	3	-1	0	-1
χ_7	3	-1	0	-1	3	1	0	1
χ_8	4	0	1	0	-4	0	-1	0

Table 8: The character table of W_3, where $\alpha = -\sqrt{2}$

ord(·)	1	3	2	5	5	2	6	2	10	10
Class size	1	20	15	12	12	1	20	15	12	12
χ_1	1	1	1	1	1	1	1	1	1	1
χ_2	1	1	1	1	1	-1	-1	-1	-1	-1
χ_3	3	0	-1	α	β	-3	0	1	$-\alpha$	$-\beta$
χ_4	3	0	-1	β	α	-3	0	1	$-\beta$	$-\alpha$
χ_5	3	0	-1	α	β	3	0	-1	α	β
χ_6	3	0	-1	β	α	3	0	-1	β	α
χ_7	4	1	0	-1	-1	4	1	0	-1	-1
χ_8	4	1	0	-1	-1	-4	-1	0	1	1
χ_9	5	-1	1	0	0	5	-1	1	0	0
χ_{10}	5	-1	1	0	0	-5	1	-1	0	0

Table 9: The character table of $C_2 \times A_5$, where $\alpha = \frac{1-\sqrt{5}}{2}$ and $\beta = \frac{1+\sqrt{5}}{2}$

ord(·)	1	10	10	2	5	5	3	6	4
Class size	1	12	12	1	12	12	20	20	30
χ_1	1	1	1	1	1	1	1	1	1
χ_2	2	α	β	-2	$-\alpha$	$-\beta$	-1	1	0
χ_3	2	β	α	-2	$-\beta$	$-\alpha$	-1	1	0
χ_4	3	β	α	3	β	α	0	0	-1
χ_5	3	α	β	3	α	β	0	0	-1
χ_6	4	-1	-1	4	-1	-1	1	1	0
χ_7	4	1	1	-4	-1	-1	1	-1	0
χ_8	5	0	0	5	0	0	-1	-1	1
χ_9	6	-1	-1	-6	1	1	0	0	0

Table 10: The character table of $\mathrm{SL}_2(5)$, where $\alpha = \frac{1-\sqrt{5}}{2}$ and $\beta = \frac{1+\sqrt{5}}{2}$

B. Computer algebra code

B.1. Calculating the non-free orbits

The following GAP [GAP17] code calculates the polynomials for the groups A_4, S_4 and A_5 in Table 1.

Listing 1: nonfreeorbitsA4.gap

```
M1 := [[-E(4),0],[0,E(4)]];;
M2 := [[1,E(4)],[1,-E(4)]];;
x  := X(Rationals,"x");;
M2 := M2 / RootsOfPolynomial(CF(4), x^2 - Determinant(M2))[1];;

Gt := Group(M1,M2);;
G  := Gt / Group(-IdentityMat(2));;
f  := NaturalHomomorphism(G);;
elePGL := List(Elements(G), g->PreImagesRepresentative(f,g));;
moeb := List(elePGL, g->(g[1][1]*x+ g[1][2])/(g[2][1]*x+g[2][2]));;

fp := Set(Union(List(moeb,m->RootsOfPolynomial(CF(12),
  NumeratorOfRationalFunction(m) - x*DenominatorOfRationalFunction(m)))));
orbit1 := Set(List(Filtered(moeb,m->Value(DenominatorOfRationalFunction(m),
        [x],[fp[1]])<>0), m->Value(m,[x],[fp[1]])));;
orbit2 := Set(List(moeb,m->Value(m,[x],[fp[6]])));;
orbit3 := Set(List(moeb,m->Value(m,[x],[fp[8]])));;

p1 := Product(orbit1, l->x-l);
p2 := Product(orbit2, l->x-l);
p3 := Product(orbit3, l->x-l);
```

Listing 2: nonfreeorbitsS4.gap

```
M1 := [[E(4),0],[0,1]]/E(8);;
M2 := -[[1,-1],[1,1]];;
M2 := M2 / RootsOfPolynomial(CF(8), x^2 - Determinant(M2))[1];;

Gt := Group(M1,M2);;
G  := Gt / Group(-IdentityMat(2));;
f  := NaturalHomomorphism(G);;
elePGL := List(Elements(G), g->PreImagesRepresentative(f,g));;
moeb := List(elePGL, g->(g[1][1]*x+ g[1][2])/(g[2][1]*x+g[2][2]));;

fp := Set(Union(List(moeb,m->RootsOfPolynomial(CF(24),
   NumeratorOfRationalFunction(m) - x*DenominatorOfRationalFunction(m)))));;
orbit1 := Set(List(Filtered(moeb,m->Value(DenominatorOfRationalFunction(m),
           [x],[fp[1]])<>0),m->Value(m,[x],[fp[1]])));;
orbit2 := Set(List(moeb,m->Value(m,[x],[fp[6]])));;
orbit3 := Set(List(moeb,m->Value(m,[x],[fp[20]])));;
```

```
p1 := Product(orbit1, l->x-l);
p2 := Product(orbit2, l->x-l);
p3 := Product(orbit3, l->x-l);
```

Listing 3: nonfreeorbitsA5.gap

```
om := (-1+Sqrt(5))/2;;
M1 := [[E(5),0],[0,1]]/E(10);;
M2 := [[om,1],[1,-om]];;
x  := X(Rationals,"x");;
M2 := M2 / RootsOfPolynomial(CF(5), x^2 - Determinant(M2))[1];;



Gt := Group(M1,M2);;
G  := Gt / Group(-IdentityMat(2));;
f  := NaturalHomomorphism(G);;
elePGL := List(Elements(G), g->PreImagesRepresentative(f,g));;
moeb := List(elePGL, g->(g[1][1]*x+ g[1][2])/(g[2][1]*x+g[2][2]));;

fp := Set(Union(List(moeb,m->RootsOfPolynomial(CF(60),
  NumeratorOfRationalFunction(m) - x*DenominatorOfRationalFunction(m)))));;
orbit1 := Set(List(Filtered(moeb,m->Value(DenominatorOfRationalFunction(m),
         [x],[fp[1]])<>0),m->Value(m,[x],[fp[1]])));;
orbit2 := Set(List(moeb,m->Value(m,[x],[fp[2]])));;
orbit3 := Set(List(moeb,m->Value(m,[x],[fp[14]])));;

p1 := Product(orbit1, l->x-l);
p2 := Product(orbit2, l->x-l);
p3 := Product(orbit3, l->x-l);
```

B.2. Calculating elliptic quotients of X_8 and X_{15}

Listing 4: quotientcurveX8.gap

```
GL23:=GL(2,3);;
tblGL23:=CharacterTable(GL23);;
char1:=Irr(tblGL23)[4]+Irr(tblGL23)[8];;
char2:=Irr(tblGL23)[5]+Irr(tblGL23)[8];;

sgs:=List(ConjugacyClassesSubgroups(GL23),h->Representative(h));;
List(sgs,g->ScalarProduct(TrivialCharacter(g),RestrictedClassFunction(char1,g
    )));
List(sgs,g->ScalarProduct(TrivialCharacter(g),RestrictedClassFunction(char2,g
    )));
# [ 6, 0, 3, 2, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0 ]
```

```
M1:=[[E(8),0],[0,E(8)^7]];;
M2:=[[-1,1],[1,1]];;
x:=X(Rationals,"x");;
M2:=M2/RootsOfPolynomial(CF(8),x^2-Determinant(M2))[1];;

Gt:=Group(M1,M2);
G:=Gt/Group(-IdentityMat(2));
pr:=NaturalHomomorphism(G);;

sgsG:=ConjugacyClassesSubgroups(G);;
List(sgsG,H->Order(Representative(H))); # Only one group of order 6
Display(StructureDescription(Representative(sgsG[8])));
S3:=Representative(sgsG[8]);;
S3t:=List(Elements(S3),g->PreImagesRepresentative(pr,g));;
S3moeb:=List(S3t,g->(g[1][1]*x+g[1][2])/(g[2][1]*x+g[2][2]));;

roots1:=RootsOfPolynomial(CF(12),x^8+14*x^4+1);;
roots2:=RootsOfPolynomial(CF(4),x*(x^4-1));;

rami1:=Set(List(S3moeb,m->Value(m,[x],[roots1[1]]))); # Length(rami1)=2
rami2:=Set(List(S3moeb,m->Value(m,[x],[roots1[2]]))); # Length(rami2)=6

# Length(rami3)=6 (including Infinity)
rami3:=Set(List(Filtered(S3moeb,s->Value(DenominatorOfRationalFunction(s),
[x],[roots2[1]])<>0),s->Value(s,[x],[roots2[1]])));

fixedpointsS3:=Set(Union(List(S3moeb,m->RootsOfPolynomial(CF(24),
 NumeratorOfRationalFunction(m) - x*DenominatorOfRationalFunction(m)))));;

rami4:=Set(List(S3moeb,m->Value(m,[x],[fixedpointsS3[1]]))); # Length(rami4)
    =3
rami5:=Set(List(S3moeb,m->Value(m,[x],[fixedpointsS3[2]]))); # Length(rami5)
    =3
rami6:=Set(List(S3moeb,m->Value(m,[x],[fixedpointsS3[7]]))); # = rami1
```

Listing 5: quotientcurveX8.sage

```
K.<e24>=CyclotomicField(24)
e4 = e24^6
e8 = e24^3
e12 = e24^2
R.<x,y>=K[]

S= [x, ((-1/2+1/2*e4)*x+(1/2-1/2*e4))/((-1/2-1/2*e4)*x+(-1/2-1/2*e4)),
  ((-1/2-1/2*e4)*x+(-1/2+1/2*e4))/((1/2+1/2*e4)*x+(-1/2+1/2*e4)),
  ((-1/2*e8-1/2*e8^3)*x+(-1/2*e8-1/2*e8^3))/((-1/2*e8-1/2*e8^3)*x+\
(1/2*e8+1/2*e8^3)), (-e4)*x^-1,
  ((1/2*e8+1/2*e8^3)*x+(-1/2*e8+1/2*e8^3))/((1/2*e8-1/2*e8^3)*x+(-\
1/2*e8-1/2*e8^3))]
```

```
Sym=SymmetricFunctions(K).elementary()
S1=Sym([1,0]).expand(6).substitute(x0=S[0],x1=S[1],x2=S[2],x3=S[3],x4=S[4],x5
    =S[5])

# we calculate the images of the points in V under the map P^1->P^1/S_3
# the ramification points
r1=S1.substitute(x=e12^7+e12^8)
r2=S1.substitute(x=-e12^4-e12^11)
r3=S1.substitute(x=-e8+e8^2-e8^3)
r4=S1.substitute(x=-e8^3)
# r5 = S1(infinity) = infinity

print(Jacobian(y^2 - (x-r1)*(x-r2)*(x-r3)).j_invariant())
print(Jacobian(y^2 - (x-r1)*(x-r2)*(x-r3)*(x-r4)).j_invariant())
print(Jacobian(y^2 - (x-r1)*(x-r2)*(x-r4)).j_invariant())
print(Jacobian(y^2 - (x-r1)*(x-r3)*(x-r4)).j_invariant())
print(Jacobian(y^2 - (x-r2)*(x-r3)*(x-r4)).j_invariant())
```

Listing 6: quotientcurveX15.gap

```
G:=DirectProduct(CyclicGroup(2),AlternatingGroup(5));;
tbl:=CharacterTable(G);;

char:=Irr(tbl)[3]+Irr(tbl)[4]+Irr(tbl)[8]+Irr(tbl)[10];

sgs:=List(ConjugacyClassesSubgroups(G),h->Representative(h));;
List(sgs,g->ScalarProduct(TrivialCharacter(g),RestrictedClassFunction(char,g)
    ));
# output: [ 15, 0, 7, 8, 5, 3, 0, 4, 3, 2, 3, 0, 0, 0, 1, 2, 1, 0, 0, 0, 0, 0
    ]
StructureDescription(sgs[17]); # A4

x:=X(Rationals,"x");;

om:=(-1+Sqrt(5))/2;;
M1:=[[om,1],[1,-om]] / (E(5)^2-E(5)^3);;
M2:=[[E(5),0],[0,E(5)^4]];;
GMt:=Group(M1,M2);;
GM:=GMt/Group(-IdentityMat(2));;
phi:=NaturalHomomorphism(GM);;
sgsGM:=ConjugacyClassesSubgroups(GM);;
List(sgsGM,H->StructureDescription(Representative(H)));

A4t:=List(Elements(Representative(sgsGM[8])),g->PreImagesRepresentative(phi,g
    ));;
A5t:=List(Elements(GM),g->PreImagesRepresentative(phi,g));
roots1:=RootsOfPolynomial(CF(15),x^20-228*x^15+494*x^10+228*x^5+1);
roots2:=RootsOfPolynomial(CF(20),x*(x^10+11*x^5-1));

A4moeb:=List(A4t,g->(g[1][1]*x+ g[1][2])/(g[2][1]*x+g[2][2]));
```

```
fixedpointsA4:=Set(Union(List(A4moeb,m->RootsOfPolynomial(CF(60),
NumeratorOfRationalFunction(m) - x*DenominatorOfRationalFunction(m)))));

rami1:=Set(List(A4moeb,m->Value(m,[x],[roots1[1]]))); # Length(rami1)=4
rami2:=Set(List(A4moeb,m->Value(m,[x],[roots1[2]]))); # Length(rami2)=12
rami3:=Set(List(A4moeb,m->Value(m,[x],[roots1[3]]))); # Length(rami3)=4
Set(roots1) = Union(rami1,rami2,rami3);

# Length(rami4)=12 (including infinity)
rami4:=Set(List(Filtered(A4moeb,m->Value(DenominatorOfRationalFunction(m),
[x],[roots2[1]])<>0),m->Value(m,[x],[roots2[1]])));

rami5:=Set(List(A4moeb,m->Value(m,[x],[fixedpointsA4[1]])));  # = rami3
rami6:=Set(List(A4moeb,m->Value(m,[x],[fixedpointsA4[2]])));  # = rami1
rami7:=Set(List(A4moeb,m->Value(m,[x],[fixedpointsA4[9]])));
```

Listing 7: quotientcurveX15.sage

```
# A5_4 quotient by A4:

K.<e60>=CyclotomicField(60)
R.<x,y>=K[]
e4=e60^15;
e5=e60^12;
e15=e60^4;
e20=e60^3;

S=[x,-e5^2/x,(x+(-e5^2-e5^3))/((e5+e5^2+e5^3)*x+(-e5^2)),
  (x+(-e5-e5^4))/((e5+e5^3+e5^4)*x+(-e5)),
  (x+(e5^2+e5^3+e5^4))/((-e5^2-e5^3)*x+(-e5^3)),
  (x+(-e5^2-e5^4))/((-e5^2-e5^4)*x+(-e5)),
  (x+(e5+e5^2+e5^3))/((-e5^3-e5^4)*x+(-e5^3)),
  (x+(-e5-e5^3))/((-e5-e5^3)*x+(-e5^4)),
  (x+(-e5^3-e5^4))/((-e5-e5^2)*x-1),
  (x+(e5+e5^3+e5^4))/((e5+e5^2+e5^4)*x-1),
  (x+(e5+e5^2+e5^4))/((-e5-e5^4)*x+(-e5^4)),
  (x+(-e5-e5^2))/((e5^2+e5^3+e5^4)*x+(-e5^2))];

Sym=SymmetricFunctions(K).elementary()
S1=Sym([1,0]).expand(12).substitute(x0=S[0],x1=S[1],x2=S[2],x3=S[3],
     x4=S[4],x5=S[5],x6=S[6],x7=S[7],x8=S[8],x9=S[9],x10=S[10],x11=S[11])

r1=S1.substitute(x=-e15-e15^4-e15^8-e15^11)
r2=S1.substitute(x=-e15-e15^2-e15^4-e15^14)
r3=S1.substitute(x=-e15-e15^2-e15^7-e15^8)
r4=S1.substitute(x=-e20-e20^4-e20^12-e20^16+e20^17)

print(Jacobian(y^2-(x-r1)*(x-r2)*(x-r3)).j_invariant())
print(Jacobian(y^2-(x-r1)*(x-r2)*(x-r3)*(x-r4)).j_invariant())
print(Jacobian(y^2-(x-r1)*(x-r2)*(x-r4)).j_invariant())
```

```
print(Jacobian(y^2-(x-r1)*(x-r3)*(x-r4)).j_invariant())
print(Jacobian(y^2-(x-r2)*(x-r3)*(x-r4)).j_invariant())
```

B.3. Calculating associated trees

Listing 8: associatedTrees.sage

```
def findChildCircles(points, pi):
    if len(points)<2:
        raise Exception("At␣least␣two␣points␣needed")
    circles = set()
    pointsLeft = set(points)
    while pointsLeft:
        p = next(iter(pointsLeft))
        minValDist = min({(p-q).ord(pi) for q in points})
        c = frozenset({q for q in points if (p-q).ord(pi) > minValDist})
        circles.add(c)
        pointsLeft = pointsLeft.difference(c)
    return circles

def createAssociatedTree(branchPoints, pi):
    if len(branchPoints)<3:
        raise Exception("At␣least␣3␣points␣are␣required")
    if len(set(branchPoints)) < len(branchPoints):
        raise Exception("Points␣must␣be␣pairwise␣different")
    K = branchPoints[0].parent()
    if not K.is_field() or K.characteristic() > 0:
        raise Exception("The␣points␣must␣lie␣in␣in␣a␣field␣of␣characteristic␣
            0")
    for p in branchPoints:
        if p.parent() != K:
            raise Exception("Base␣field␣must␣be␣same␣for␣all␣points")
    if pi.parent() != K or not pi.is_prime():
        raise Exception("pi␣must␣be␣a␣prime␣in␣the␣base␣field")
    T = DiGraph()
    v0 = frozenset(branchPoints)
    T.add_vertex(frozenset(branchPoints))
    to_process = [v0]
    while to_process:
        current = to_process.pop()
        if len(current) == 1:
            continue
        circles = findChildCircles(current,pi)
        for c in circles:
            cfrozen = frozenset(c)
            T.add_path([current,cfrozen])
            to_process.append(cfrozen)
    return T
```

References

[Bel83] G. V. Belyĭ, *On extensions of the maximal cyclotomic field having a given classical Galois group*, J. Reine Angew. Math. **341** (1983), 147–156. MR 697314

[BGG93] E. Bujalance, J. M. Gamboa, and G. Gromadzki, *The full automorphism groups of hyperelliptic Riemann surfaces*, Manuscripta Math. **79** (1993), no. 3-4, 267–282. MR 1223022

[BL04] C. Birkenhake and H. Lange, *Complex abelian varieties*, second ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 302, Springer-Verlag, Berlin, 2004.

[Bli17] H. F. Blichfeldt, *Finite collineation groups*, University of Chicago Press Chicago, 1917.

[BLR90] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990. MR 1045822

[BM00] J. Bertin and A. Mézard, *Déformations formelles des revêtements sauvagement ramifiés de courbes algébriques*, Invent. Math. **141** (2000), no. 1, 195–238 (French). MR 1767273

[Bos80] S. Bosch, *Formelle Standardmodelle hyperelliptischer Kurven*, Math. Ann. **251** (1980), no. 1, 19–42 (German). MR 583822

[BS86] R. Brandt and H. Stichtenoth, *Die Automorphismengruppen hyperelliptischer Kurven. (The groups of automorphisms of hyperelliptic curves).*, Manuscr. Math. **55** (1986), 83–92 (German).

[Bys09] J. Byszewski, *Cohomological aspects of equivariant deformation theory*, Ph.D. thesis, Utrecht University, May 2009.

[Con02] B. Conrad, *A modern proof of Chevalley's theorem on algebraic groups*, J. Ramanujan Math. Soc. **17** (2002), no. 1, 1–18. MR 1906417

[CS86] G. Cornell and J. H. Silverman (eds.), *Arithmetic geometry*, Springer-Verlag, New York, 1986, Papers from the conference held at the University of Connecticut, Storrs, Connecticut, July 30–August 10, 1984. MR 861969

[FGI+05] B. Fantechi, L. Göttsche, L. Illusie, S. L. Kleiman, N. Nitsure, and A. Vistoli, *Fundamental algebraic geometry: Grothendieck's FGA explained.*, Providence, RI: American Mathematical Society (AMS), 2005.

[FK92] H. M. Farkas and I. Kra, *Riemann surfaces.*, 2nd ed., Graduate Texts in Mathematics, Springer, New York, 1992.

[GAP17] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.8.7*, 2017.

[GHvdP88] L. Gerritzen, F. Herrlich, and M. van der Put, *Stable n-pointed trees of projective lines*, Nederl. Akad. Wetensch. Indag. Math. **50** (1988), no. 2, 131–163. MR 952512

[Gro57] A. Grothendieck, *Sur quelques points d'algèbre homologique*, Tôhoku Math. J. (2) **9** (1957), 119–221 (French). MR 0102537

[Har77] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York-Heidelberg, 1977, Graduate Texts in Mathematics, No. 52.

[Hat02] A. Hatcher, *Algebraic topology*, Cambridge University Press, Cambridge, 2002. MR 1867354

[Kee92] S. Keel, *Intersection theory of moduli space of stable n-pointed curves of genus zero*, Trans. Amer. Math. Soc. **330** (1992), no. 2, 545–574. MR 1034665

[Knu83] F. F. Knudsen, *The projectivity of the moduli space of stable curves. II. The stacks $M_{g,n}$*, Math. Scand. **52** (1983), no. 2, 161–199. MR 702953

[Lan83] S. Lang, *Abelian varieties*, Springer-Verlag, New York-Berlin, 1983, Reprint of the 1959 original. MR 713430

[Løn80] K. Lønsted, *The structure of some finite quotients and moduli for curves*, Comm. Algebra **8** (1980), no. 14, 1335–1370. MR 583602

[Mil06] J. S. Milne, *Complex multiplication (v0.00)*, 2006, Available at `www.jmilne.org/math/`, pp. 1–113.

[Mil08] ———, *Abelian varieties (v2.00)*, 2008, Available at `www.jmilne.org/math/`, pp. 166+vi.

[Mir95] R. Miranda, *Algebraic curves and Riemann surfaces*, Graduate Studies in Mathematics, vol. 5, American Mathematical Society, Providence, RI, 1995.

[Mum74] D. Mumford, *Abelian varieties. With appendices by C. P. Ramanujam and Yuri Manin. 2nd ed.*, 2nd ed. ed., Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London, 1974.

[Nam84] M. Namba, *Geometry of projective algebraic curves*, Monographs and Textbooks in Pure and Applied Mathematics, vol. 88, Marcel Dekker, Inc., New York, 1984.

[Oja90] M. Ojanguren, *The Witt group and the problem of Lüroth*, Dottorato di Ricerca in Matematica. [Doctorate in Mathematical Research], ETS Editrice, Pisa, 1990, With an introduction by Inta Bertuccioni. MR 1077830

[Oor66] F. Oort, *Algebraic group schemes in characteristic zero are reduced*, Invent. Math. **2** (1966), 79–80. MR 0206005

[Pau13] J. Paulhus, *Elliptic factors in Jacobians of hyperelliptic curves with certain automorphism groups.*, ANTS X. Proceedings of the tenth algorithmic number theory symposium, San Diego, CA, USA, July 9–13, 2012, Berkeley, CA: Mathematical Sciences Publishers (MSP), 2013, pp. 487–505.

[Pin13] R. Pink, *Finiteness and liftability of postcritically finite quadratic morphisms in arbitrary characteristic*, `https://arxiv.org/abs/1305.2841v3`, 2013.

[Pop72] H. Popp, *On a conjecture of H. Rauch on theta constants and Riemann surfaces with many automorphisms.*, J. Reine Angew. Math. **253** (1972), 66–77.

[Rau70] H. E. Rauch, *Theta constants on a Riemann surface with many automorphisms*, Symposia Mathematica, Vol. III (INDAM, Rome, 1968/69), Academic Press, London, 1970, pp. 305–323. MR 0260996

[Roh09] J. C. Rohde, *Cyclic coverings, Calabi-Yau manifolds and complex multiplication*, Lecture Notes in Mathematics, vol. 1975, Springer-Verlag, Berlin, 2009. MR 2510071

[S^+17] W. A. Stein et al., *Sage Mathematics Software (Version 7.5.1)*, The Sage Development Team, 2017, `https://www.sagemath.org`.

[Ser06] E. Sernesi, *Deformations of algebraic schemes*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 334, Springer-Verlag, Berlin, 2006. MR 2247603

[Sha04] T. Shaska, *Some special families of hyperelliptic curves*, J. Algebra Appl. **3** (2004), no. 1, 75–89. MR 2047637

[Sha06] ______, *Subvarieties of the hyperelliptic moduli determined by group actions.*, Serdica Math. J. **32** (2006), no. 4, 355–374.

[Sil94] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR 1312368

[Sil09] ———, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094

[SS07] D. Sevilla and T. Shaska, *Hyperelliptic curves with reduced automorphism group A_5*, Appl. Algebra Engrg. Comm. Comput. **18** (2007), no. 1-2, 3–20. MR 2280308

[ST68] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517. MR 0236190

[Str01] M. Streit, *Period matrices and representation theory*, Abh. Math. Sem. Univ. Hamburg **71** (2001), 279–290. MR 1873049

[Tsu58] R. Tsuji, *On conformal mapping of a hyperelliptic Riemann surface onto itself*, Kōdai Math. Sem. Rep. **10** (1958), 127–136. MR 0100085

[Wol97] J. Wolfart, *The "obvious" part of Belyi's theorem and Riemann surfaces with many automorphisms*, Geometric Galois actions, 1, London Math. Soc. Lecture Note Ser., vol. 242, Cambridge Univ. Press, Cambridge, 1997, pp. 97–112. MR 1483112

[Wol00] ———, *Triangle groups and jacobians of CM type*, `http://www.math.uni-frankfurt.de/~wolfart/Artikel/jac.pdf`, 2000.