Universität Ulm

Glueing curves of genus 2 and genus 1 along their 2-torsion

Vorgelegt von
Jeroen Hanselman

aus Ulm im Jahr 2018

Dissertation zur Erlangung des Doktorgrades Dr. rer. nat. der Fakultät für Mathematik und Wirtschaftswissenschaften der Universität Ulm

Amtierender Dekan:
Prof. Dr. Alexander Lindner

Gutacher:
Jun.-Prof. Dr. Jeroen Sijsling

Tag der Promotion:

Contents

Introduction

Motivation

Goals and Results

Outline

Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Acknowledgments

Chapter 1

General theory of glueing curves

1.1 Glueing curves

Definition 1.1.1. Let X, Y be two curves over a field k of genus g_X, g_Y respectively. If there exists a curve Z of genus $g_X + g_Y$ over k and an isogeny $\phi : \mathrm{Jac}(X) \times \mathrm{Jac}(Y) \to \mathrm{Jac}(Z)$, then we call the pair (ϕ, Z) a *weak glueing* of X and Y.

Lemma 1.1.2. *Let (ϕ, Z) be a weak glueing of two curves X and Y. Then there exists some n such that* $\ker(\phi) \subset \mathrm{Jac}(X)[n] \times \mathrm{Jac}(Y)[n]$.

Proof. As ϕ is an isogeny, $\ker(\phi)$ is a finite group. Let $n = |\ker(\phi)|$. It follows that $\ker(\phi) \subset (\mathrm{Jac}(X) \times \mathrm{Jac}(Y))[n]\mathrm{Jac}(X)[n] \times \mathrm{Jac}(Y)[n]$. □

A weak glueing only uses the Jacobians of the curves. As Torelli's Theorem tells us that any curve actually gives rise to a principally polarized abelian variety, it makes sense to also demand a condition on the relation between the principal polarizations on X, Y and Z.

Definition 1.1.3. Let A_1, A_2 be two abelian varieties over a fieldf k, and let $\mathcal{L}_1$ be a line bundle on A_1 and $\mathcal{L}_2$ be a line bundle on A_2 that give rise to principal polarizations on the respective abelian varieties. Now consider the product $A_1 \times A_2$ along with the projection maps pr_1, pr_2. If there exist integers n_1, n_2, an abelian variety B with a line bundle $\mathcal{M}_B$ over k, and an isogeny $\phi : A_1 \times A_2 \to B$, such that

(D1) the line bundle $\mathcal{M}_B$ induces a principal polarization on B; and

(D2) we have
$$\mathcal{L} = \mathrm{pr}_1^*(\mathcal{L}_1)^{n_1} \otimes \mathrm{pr}_2^*(\mathcal{L}_2)^{n_2} \cong_{\mathrm{alg}} \phi^*(\mathcal{M}_B),$$

then we call the triple $(\phi, B, \mathcal{M}_B)$ an (n_1, n_2)-*glueing* of A_1 and A_2. If there exists a curve Z with the induced polarization $\mathcal{P}_Z$ on $\mathrm{Jac}(Z)$, such that $(B, \mathcal{M}_B) \cong_{\mathrm{alg}} (\mathrm{Jac}(Z), \mathcal{P}_Z)$, then we will also call the curve Z an (n_1, n_2)-*glueing* of A_1 and A_2.

Definition 1.1.4. Let X, Y be two curves over k. These curves give rise to principally polarized abelian varieties $(\mathrm{Jac}(X), \mathcal{P}_X)$ and $(\mathrm{Jac}(Y), \mathcal{P}_Y)$. We call the triple $(\phi, A, \mathcal{P}_A)$ an (n_1, n_2)-*glueing* of X and Y if $(\phi, A, \mathcal{M}_A)$ is an (n_1, n_2)-glueing of $(\mathrm{Jac}(X), \mathcal{P}_X)$ and $(\mathrm{Jac}(Y), \mathcal{P}_Y)$. We similarly say that a triple $(\phi, \mathrm{Jac}(Z), \theta_Z)$ is an (n_1, n_2)-*glueing* of X and Y if it is an (n_1, n_2)-*glueing* of $(\mathrm{Jac}(X), \mathcal{P}_X)$ and $(\mathrm{Jac}(Y), \mathcal{P}_Y)$.

Remark 1.1.5. In Definition 1.1.3 the class of $\phi^*(\mathcal{M}_B)$ in the Néron-Severi group of $A_1 \times A_2$ is a sum of powers of $\mathrm{pr}_1^* \mathcal{L}_1$ and $\mathrm{pr}_2^* \mathcal{L}_2$. In general one could consider using a more general element of the Néron-Severi group, but as it always contains $\mathbb{Z}\,\mathrm{pr}_1^*(\mathcal{L}_1) \times \mathbb{Z}\,\mathrm{pr}_2^*(\mathcal{L}_2)$ and is generically isomorphic to $\mathbb{Z} \times \mathbb{Z}$, we will only consider the (n_1, n_2) case.

Definition 1.1.6. Let (ϕ, J, θ_J) be a potential (m, n)-glueing of two curves X and Y. If $\ker(\phi)$ is decomposable, we say that ϕ is a *decomposable glueing*.

Proposition 1.1.7. *Let (ϕ, J, θ_J) be a decomposable (m, n)-glueing of two curves X and Y. Then $J = A \times B$ where A is isogenous to* $\mathrm{Jac}(X)$ *and B is isogenous to* $\mathrm{Jac}(Y)$.

Proof. By assumption, $\ker(\phi) = K_X \times K_Y$ where K_X is a totally isotropic subgroup of $\mathrm{Jac}(X)[m]$ and K_Y is a totally isotropic subgroup of $\mathrm{Jac}(Y)[n]$. This means we get a natural isogeny:

$$\mathrm{Jac}(X) \times \mathrm{Jac}(Y) \to \mathrm{Jac}(X)/K(X) \times \mathrm{Jac}(Y)/K(Y)$$

and as this isogeny has $\mathrm{Jac}(X) \times \mathrm{Jac}(Y)$ as its kernel, we see that J is isogenous to the product $\mathrm{Jac}(X)/K(X) \times \mathrm{Jac}(Y)/K(Y)$ where the first term is isogenous to $\mathrm{Jac}(X)$ and the second term to $\mathrm{Jac}(Y)$.

□

Let A be an abelian variety and let n be a positive integer. We can then assign a bilinear form

$$\langle ., . \rangle_n : A[n] \times A[n] \to \mu_n$$

called the Weil pairing. See for example Definition 11.11 in [4]. In what follows, it will be important to study subgroups of $A[n]$ that are maximally isotropic with respect to the Weil pairing.

Definition 1.1.8. A maximal isotropic subgroup G of $\mathrm{Jac}(X)[n] \times \mathrm{Jac}(Y)[m]$ is called indecomposable if it cannot be written as the product of two isotropic subgroups of $\mathrm{Jac}(X)[n]$ and $\mathrm{Jac}(Y)[m]$.

Proposition 1.1.9. *Giving a triple $(B, \phi, \mathcal{M}_B)$ satisfying (D1) and (D2) is the same as giving a maximal isotropic subgroup G of $A_1[n_1] \times A_2[n_2]$. Given such a maximal isotropic subgroup G, we have $B \cong A/G$ and $\deg(\phi) = n_1^{d_1} n_2^{d_2}$.*

Proof. It suffices to show that $K(\mathcal{L}) = A_1[n_1] \times A_2[n_2]$, as we can then use [4, Corollary 8.14] to obtain (D1) and Proposition 7.6 and Corollary 8.16 in loc. cit. to obtain (D2). But by [4, Proposition 8.6] we have

$$K(\mathcal{L}) = K(\mathcal{L}_1^{n_1}) \times K(\mathcal{L}_2^{n_2}) = n_1^{-1}(K(\mathcal{L}_1)) \times n_2^{-1}(K(\mathcal{L}_2)) = A_1[n_1] \times A_2[n_2]. \quad (1.1)$$

□

Remark 1.1.10. Note in particular that the algebraic equivalence class of $\mathcal{M}_B$ is uniquely determined by the maximal isotropic subgroup G, which is also implied by [4, Corollary 7.25].

The main result of this section is the following.

Theorem 1.1.11. *Let $e = \gcd(n_1, n_2)$. Then any (n_1, n_2)-gluing $(B, \phi, \mathcal{M})$ factors as $\phi = \phi_e \psi$. Here*

(i) The isogeny $\psi = \psi_1 \times \psi_2$ is a product of isogenies $\psi_i : A_i \to B_i$ for $i \in \{1, 2\}$ such that $\psi_i(\mathcal{M}_i) \sim \mathcal{L}_i^{n_i/e}$ for some algebraic equivalence class $\mathcal{M}_i$ inducing a principal polarization on B_i;

(ii) The triple $(B, \phi_e, \mathcal{M})$ is an (e, e)-gluing for the pair $((B_1, \mathcal{M}_1), (B_2, \mathcal{M}_2))$.

To prove this theorem, we consider the inverse limit of the Weil pairings

$$\langle .,. \rangle_\infty : K(\mathcal{L}) \times K(\mathcal{L}) \to \mu_\infty. \quad (1.2)$$

By the compatibilities in [4, Proposition 8.6], this pairing on $K(\mathcal{L}) = A_1[n_1] \times A_2[n_2]$ is the product of the Weil pairings $\langle .,. \rangle_1$ and $\langle .,. \rangle_2$ on $A_1[n_1]$ and $A_2[n_2]$. It has values in $\mu_{n_1} \otimes \mu_{n_2} = \mu_{\mathrm{lcm}(n_1,n_2)}$. We need the following crucial Lemma.

Lemma 1.1.12. *Let $G \subset A_1[n_1] \times A_2[n_2]$ be maximal isotropic. Suppose that $v_p(n_1) \neq v_p(n_2)$ for some prime number p. Suppose that $v_p(n_1)$ (resp. $v_p(n_2)$) is the larger of $\{v_p(n_1), v_p(n_2)\}$. Then G contains a group of the form $H_1 \times \{0\}$ (resp. $\{0\} \times H_2$), where $H_i \subset A_i[p]$ is maximal isotropic.*

Proof. We may suppose that $v_p(n_1) > v_p(n_2)$. Consider the Weil pairing

$$\langle .,. \rangle_{n_1} : A_1[n_1] \times A_1[n_1] \to \mu_{n_1} \quad (1.3)$$

on the group $A_1[n_1]$. Similarly, denote the Weil pairing on $A_1[p]$ by

$$\langle .,. \rangle_p : A_1[p] \times A_1[p] \to \mu_p. \quad (1.4)$$

(Note that in general $\langle .,. \rangle_\infty$ does not restrict to $\langle .,. \rangle_p$ on $A_1[p]$!) The pairing (1.3) induces a pairing on $Q = A_1[n_1]/pA_1[n_1]$ with values in $\mu_{n_1}/\mu_{p^{-1}n_1}$, which we denote by

$$\langle .,. \rangle_Q : Q \times Q \to \mu_{n_1}/\mu_{p^{-1}n_1}. \tag{1.5}$$

Finally, the Weil pairing $\langle .,. \rangle$ induces a perfect mixed pairing

$$\langle .,. \rangle_{p,Q} : A_1[p] \times Q \to \mu_p. \tag{1.6}$$

Choosing a symplectic basis B of $A_1[n_1]$ as a free module over $\mathbb{Z}/n_1\mathbb{Z}$ gives induced bases for both $A_1[p]$ and Q, the former by multiplying the elements in B with $p^{-1}n_1$ and the latter by projecting down to Q. Using these bases, all pairings above can be described by a standard symplectic matrix. Now let G be as in the Lemma.

Claim 1: The image $\overline{\pi_1(G)}$ of $\pi_1(G)$ in Q is isotropic. In particular, it has rank at most d_1.

Proof: As was mentioned before the Lemma, the Weil pairing $\langle .,. \rangle_\infty$ on $A_1[n_1] \times A_2[n_2]$ is given by

$$\langle (x_1, x_2), (y_1, y_2) \rangle_\infty = \langle x_1, y_1 \rangle_{n_1} \langle x_2, y_2 \rangle_{n_2}, \tag{1.7}$$

where $\langle .,. \rangle_{n_2}$ is the Weil pairing on $A_2[n_2]$. If $\overline{\pi_1(G)}$ in Q were not isotropic, then on $G \times G$ the factor $\langle x_1, y_1 \rangle$ would attain values in μ_∞ of order equal to p^{n_1}. Due to our assumption at the beginning of the proof, the pairing $\langle .,. \rangle_{n_2}$ cannot attain such values. This precludes $\langle .,. \rangle_\infty$ from being trivial on $G \times G$ and contradicts G being isotropic.

Claim 2: The submodule $G \cap A_1[p]$ is of rank at least d_1.

Proof: Consider the orthogonal complement $\overline{\pi_1(G)}^\perp$ of $\overline{\pi_1(G)}$ under the mixed pairing $\langle .,. \rangle_{p,Q}$. Because the latter pairing is perfect, this is a submodule of $A_1[p]$ of rank at least d_1. By construction, it has trivial pairing with the elements of $\pi_1(G) \times \{0\}$. It is therefore contained in G since that group is maximal isotropic.

Claim 3: The submodule $G \cap A_1[p]$ contains a maximal isotropic submodule of $A_1[p]$ with respect to the Weil pairing $\langle .,. \rangle_p$.

Proof: This follows because after the choice of a symplectic basis above, the pairings $\langle .,. \rangle_p$ on $A_1[p]$ and $\langle .,. \rangle_Q$ on Q, as well as the mixed pairing $\langle .,. \rangle_{p,Q}$, are all given by the standard symplectic matrix. Indeed, this implies that since the image of $\pi_1(G)$ in Q is contained in a maximal isotropic submodule, its dual $\overline{\pi_1(G)}^\perp$ in $A_1[p]$ contains such a submodule.

With this series of claims, the statement of the Lemma follows by taking some maximal isotropic submodule H_1 of $G \cap A_1[p]$. $\square$

Proof of Theorem 1.1.11. The theorem follows from [4, Corollary 8.11]. Indeed, if $n_1 = n_2$, then we are done. Otherwise we can apply Lemma 1.1.12, as follows.

Let H_i be the submodule obtained by applying Lemma 1.1.12, and let $\psi_i : A_i \to A_i/H_i$ be the corresponding quotient. Suppose moreover (as we may, by symmetry) that $i = 1$. Because H_1 is maximal isotropic in $A_1[p]$, there exists a unique algebraic equivalence class $\mathcal{P}_1$ on A_1/H_1 such that $\psi_1^*(\mathcal{M}_1) \sim \mathcal{L}_1^p$, and this class $\mathcal{M}_1$ defines a principal polarization on A_1/H_1. Let $\mathcal{M}_2 = \mathcal{L}_2$.

Consider the composition

$$A_1 \times A_2 \to (A_1/H_1) \times A_2 = (A_1 \times A_2)/(H_1 \times \{0\}) \to (A_1 \times A_2)/G. \tag{1.8}$$

Let ψ_1 (resp. ϕ) be the quotient map by H_1 (resp. G). Then we can write $\phi = \phi_1(\psi_1 \times 1)$, and if we denote the projections of $(A_1/H_1) \times A_2$ onto its components by ρ_1 and ρ_2, then $(\psi_1 \times 1)^*(\rho_1^*(\mathcal{M}_1)) = \pi_1^*(\mathcal{L}_1^p)$ and $(\psi_1 \times 1)^*(\rho_1^*(\mathcal{M}_2)) = \pi_2^*(\mathcal{L}_2)$. This implies that

$$(\psi_1 \times 1)^*(\rho_1^*(\mathcal{M}_1^{n_1/p}) \otimes \rho_2^*(\mathcal{M}_2^{n_2})) = \pi_1^*(L_1^{n_1}) \otimes \pi_2^*(L_2^{n_2}) = L. \tag{1.9}$$

By the uniqueness Remark 1.1.10, the fact that $\mathcal{L} = \psi^*(\mathcal{M}) = (\psi_1 \times 1)^*(\phi_1^*(\mathcal{M}))$ then allows us to conclude

$$\phi_1^*(\mathcal{M}) = \rho_1^*(\mathcal{M}_1^{n_1/p}) \otimes \rho_2^*(\mathcal{M}_2^{n_2}). \tag{1.10}$$

Both $\mathcal{M}_1$ and $\mathcal{M}_2$ define principal polarizations on the corresponding factors, so that ϕ_1 is a $(p^{-1}n_1, n_2)$-gluing of the pair of principally polarized abelian varieties $((A_1/H_1, \mathcal{M}_1), (A_2, \mathcal{M}_2))$.

This process can be continued inductively. Composing all morphisms $\psi_1 \times 1$ and $1 \times \psi_2$ thus obtained, we get the Theorem. □

1.2 Structure of isotropic subgroups

As maximal isotropic subgroups play a big role in glueing, it makes sense to study them in more detail. In the most general setting one could study the maximal isotropic subgroups of $\mathbb{Z}/k\mathbb{Z}^{2n}$ with respect to a non-degenerate symplectic paring for some positive integers k and n. In this section we will restrict ourselves to the case where k is a prime number p.

Lemma 1.2.1. *Let G be a maximal isotropic subgroup of $\mathbb{F}_p^{2n}$ with respect to the standard symplectic pairing. Then $|G| = p^n$.*

Proof. See [8] 3.1 Corollary a). □

Proposition 1.2.2. *There are exactly*

$$\prod_{k=0}^{n-1}\left(p^{n-k}+1\right)$$

maximally isotropic subgroups in $\mathbb{F}_p^{2n}$ with respect to the standard pairing.

Proof. We are first going to count the number of ways we can construct a maximal isotropic vector space by adjoining vectors. After that, we will divide this number by the amount of possible ways to choose a basis for this vector space to find the number of maximally isotropic subspaces.

Let $v_1 \in \mathbb{F}_p^{2n}$ be a non-zero vector. There are $p^{2n}-1$ possible ways to choose this vector, and $< v_1 >$ gives us a 1-dimensional isotropic subspace of $\mathbb{F}_p^{2n}$. Assume we have already found a k-dimensional isotropic subspace V_k of $\mathbb{F}_p^{2n}$ with $k < n$. Then we need to find a vector $v_{k+1} \in V_k^{\perp} - V_k$ to construct a $k+1$-dimensional isotropic subspace. For this, we have $p^{2n-k}-p^k$ choices. So there are $\prod_{k=0}^{n-1}\left(p^{2n-k}-p^k\right)$ possible ways of constructing a basis for a maximal isotropic subspace of $\mathbb{F}_p^{2n}$.

The number of possible distinct bases for $\mathbb{F}_p^n$ is equal to $\prod_{k=0}^{n-1}(p^n-p^k)$. Combining these we find that the number of maximal isotropic subspaces is

$$\frac{\prod_{k=0}^{n-1}\left(p^{2n-k}-p^k\right)}{\prod_{k=0}^{n-1}(p^n-p^k)} = \prod_{k=0}^{n-1}\left(p^{n-k}+1\right).$$

□

We will restrict ourselves to the following situation. We have a vector space ${\mathbb{F}_p}^2 \times \mathbb{F}_p^{2n}$ which comes equipped with the natural projection maps π_1 and π_2.

The standard pairing on $\mathbb{F}_p^{2k}$ will be written as $\langle .,. \rangle_{\mathbb{F}_p^{2k}}$ The product pairing $\langle .,. \rangle$ on $\mathbb{F}_p^2 \times \mathbb{F}_p^{2n}$ is given by

$$\langle x, y\rangle = \langle \pi_1(x), \pi_1(y)\rangle_{\mathbb{F}_p^2} + \langle \pi_2(x), \pi_2(y)\rangle_{\mathbb{F}_p^{2n}}.$$

Remark 1.2.3. This situation occurs naturally when glueing an elliptic curve to another curve along their p-torsion.

Lemma 1.2.4. *Let G be an indecomposable maximally isotropic subgroup of ${\mathbb{F}_p}^2 \times \mathbb{F}_p^{2n}$ with respect to the product pairing. Then π_1 is surjective.*

Proof. If π_1 is not surjective, its image will be either 0 or a 1-dimensional vector space. In the first case, G would be isomorphic to $\{0\} \times G_2$ where G_2 is some isotropic subgroup of $\mathbb{F}_p^{2n}$. This causes a contradiction as G is indecomposable. Now assume $\pi_1(G)$ consists of a 1-dimensional vector space

V. Then $\pi_1(G)$ is a maximal isotropic subspace because it is 1-dimensional. Now we see that

$$0 = \langle x, y\rangle = \langle \pi_1(x), \pi_1(y)\rangle_{\mathbb{F}_p^2} + \langle \pi_2(x), \pi_2(y)\rangle_{\mathbb{F}_p^{2n}} = 0 + \langle \pi_2(x), \pi_2(y)\rangle_{\mathbb{F}_p^{2n}}.$$

This shows that $\pi_2(K)$ is also a maximal isotropic subgroup of $\mathbb{F}_p^{2n}$. Now as $|G| = p^{n+1}$, $|\pi_1(G)| = p$, and $|\pi_2(G)| \leq p^n$ by Lemma 3.1, it follows that

$$G \cong \pi_1(G) \times \pi_2(G).$$

This contradicts our assumption that G was indecomposable. Hence π_1 is surjective.

□

Definition 1.2.5. Let G be a group that comes equipped with a pairing $\langle\cdot,\cdot\rangle \to \mathbb{F}_p^*$ and let H be a subgroup of G. We write $H^\perp$ for the orthogonal complement of H in G with respect to the pairing.

Lemma 1.2.6. *Let G be an indecomposable maximally isotropic subgroup of ${\mathbb{F}_p}^2 \times \mathbb{F}_p^{2n}$ with respect to the product pairing. Let G' be the kernel of the map $\pi_1 : G \to \mathbb{F}_p^2$. Consider the subgroup $H = \pi_2(G')$ in $\mathbb{F}_p^{2n}$.*

(i) The vector space $H^\perp/H$ is 2-dimensional.

(ii) There exists a well-defined pairing on $H^\perp/H$ which we will denote by $\langle .,.\rangle_{H^\perp/H}$ that is induced by the pairing $\langle .,.\rangle_{\mathbb{F}_p^{2n}}$ on $\mathbb{F}_p^{2n}$.

(iii) There exists an isomorphism $\phi : \mathbb{F}_p^2 \to H^\perp/H$ such that

$$\langle x_1, x_2\rangle_{\mathbb{F}_p^2} = -\langle \phi(x_1), \phi(x_2)\rangle_{H^\perp/H}.$$

Proof. (i) We know that G is an $n+1$-dimensional vector space, and that G' is the kernel of π_1 which surjects onto $\mathbb{F}_p^2$, so G' is an $n-1$-dimensional subvectorspace. This also implies that H is $n-1$-dimensional as G' is isomorphic to H by construction. Now $H^\perp$ is a subvector space of $\mathbb{F}_p^{2n}$ which is defined by $n-1$ linear equation. This shows that $H^\perp$ is an $n+1$ dimensional subvectorspace. Hence $H^\perp/H$ has dimension 2.

(ii) Note that $\langle x_1 + h_1, x_2 + h_2\rangle_{\mathbb{F}_p^{2n}} = \langle x_1, x_2\rangle_{\mathbb{F}_p^{2n}}$ for all $x_1, x_2 \in H^\perp$ and $h_1, h_2 \in H$ as the elements of H pair to 0 with the elements of $H^\perp$, so the following pairing will be well-defined on $H/H^\perp \times H/H^\perp$:

$$\langle [x_1], [x_2]\rangle_{H/H^\perp} = \langle x_1, x_2\rangle_{\mathbb{F}_p^{2n}}.$$

where we use $[.]$ to denote the class in $H/H^\perp$.

(iii) Consider the natural map $\pi_2 : G \to H^\perp \subset \mathbb{F}_p^{2n}$. We claim that this map gives an isomorphism. As the map is linear and both spaces have the same dimension, it is enough to show the map is injective. Assume it is not. Now there exists a $0 \neq t_1 \in \mathbb{F}_p^2$ such that $(t_1, 0) \in G$. Additionally, there should exist $(s_1, s_2) \in G$ with $s_1 \neq 0 \neq t_1$ and $s_2 \neq 0$. To see this, first note that we know there exists an element $(\alpha, s_2) \in G$ with $s_2 \neq 0$. Otherwise the image of π_2 would be trivial. Similarly, we find an element $(s_1, \beta) \in G$ with $s_1 \neq 0 \neq x$ using that π_1 is surjective. Now at least one of $(\alpha, s_2), (s_1, \beta)$ or $(\alpha + s_1, \beta + s_2)$ will have the required properties.

It follows that

$$\langle (t_1, 0), (s_1, s_2) \rangle = \langle t_1, s_1 \rangle_{\mathbb{F}_p^2} + \langle 0, s_2 \rangle_{\mathbb{F}_p^{2n}} = \langle t_1, s_1 \rangle_{\mathbb{F}_p^2} + 0 \neq 0.$$

This causes a contradiction, so π_2 is an isomorphism. From this we get an isomorphism on the quotient: $\pi_2 : G/G' \to H^\perp/H$. Writing τ for the natural isomorphism $\tau : G/G' \to \mathbb{F}_p^2$ induced by π_1 and setting $\phi = \pi_2 \circ \tau^{-1}$ gives us the sought after isomorphism.

A similar argument to the one in (ii) shows that the following pairing will be well-defined on $G/G' \times G/G'$:

$$\langle [(t_1, t_2)], [(s_1, s_2)] \rangle_{G/G'} = \langle t_1, s_1 \rangle_{\mathbb{F}_p^2}.$$

where we use $[.]$ to denote the class in G/G'. The morphism τ will preserve the pairing by construction.

We will now check if ϕ has the required property. Let $t_1, s_1 \in \mathbb{F}_p^2$. By construction $\phi(t_1) = t_2 \mod H$ and $\phi(s_1) = s_2 \mod H$ for some $(t_1, t_2), (s_1, s_2) \in G$. We know that

$$0 = \langle (t_1, t_2), (s_1, s_2) \rangle = \langle t_1, s_1 \rangle_{\mathbb{F}_p^2} + \langle t_2, s_2 \rangle_{\mathbb{F}_p^{2n}} = \langle [(t_1, t_2)], [(s_1, s_2)] \rangle_{G/G'} + \langle t_2, s_2 \rangle_{H^\perp/H},$$

so

$$\langle t_1, s_1 \rangle_{\mathbb{F}_p^2} = \langle [(t_1, t_2)], [(s_1, s_2)] \rangle_{G/G'} = -\langle \phi(t_1), \phi(s_1) \rangle_{H^\perp/H}.$$

We conclude that ϕ is a pairing-reversing isomorphism.

□

Lemma 1.2.7. *Conversely, any tuple (H, ϕ) of an $n-1$-dimensional subvectorspace H of $\mathbb{F}_p^{2n}$ and a pairing-reversing isomorphism $\phi : \mathbb{F}_p^2 \to H^\perp/H$ defines a maximally isotropic subgroup G of $\mathbb{F}_p^2 \times \mathbb{F}_p^{2n}$.*

Proof. Let $G = \{(x, \phi(x) + h) | x \in \mathbb{F}_p^2,\ \ h \in H\}$. Note that $H^\perp$ is not an isotropic subgroup as it consists of p^{n+1} elements, and a maximally isotropic subgroup of $\mathbb{F}_p^{2n}$ has p^n elements. As a result, the induced pairing on $H^\perp/H$ is non-trivial, so there exist $x_1, x_2 \in \mathbb{F}_p^2$ such that $\langle \phi(x_1), \phi(x_2) \rangle_{H^\perp/H} = \langle \phi(x_1), \phi(x_2) \rangle_{\mathbb{F}_p^{2n}}$ is non-zero. Therefore the group G is indecomposable.

We also see that

$$
\begin{aligned}
\langle (x_1, \phi(x_1) + h_1), (x_2, \phi(x_2) + h_2) \rangle &= \langle x_1, x_2 \rangle_{\mathbb{F}_p^2} + \langle \phi(x_1) + h_1, \phi(x_2) + h_2 \rangle_{\mathbb{F}_p^{2n}} \\
&= \langle x_1, x_2 \rangle_{\mathbb{F}_p^2} + \langle \phi(x_1), \phi(x_2) \rangle_{\mathbb{F}_p^{2n}} + \\
&\langle (h_1, \phi(x_2)) \rangle_{\mathbb{F}_p^{2n}} + \langle \phi(x_1), h_2 \rangle_{\mathbb{F}_p^{2n}} + \langle h_1, h_2 \rangle_{\mathbb{F}_p^{2n}} \\
&= \langle x_1, x_2 \rangle_{\mathbb{F}_p^2} + \langle \phi(x_1), \phi(x_2) \rangle_{H/H^\perp} + 0 + 0 + 0 \\
&= 0.
\end{aligned}
$$

This shows that G is an isotropic subgroup. As it is of order $n+1$, it is maximal.

□

Corollary 1.2.8. *There are exactly 90 distinct simple maximal isotropic subgroups in* $\mathbb{F}_2^2 \times \mathbb{F}_2^4$.

Proof. A maximally isotropic subgroup is determined by a choice of a tuple (H, ϕ) where H is a 1-dimensional subvectorspace of $\mathbb{F}_2^4$, and ϕ is a pairing reversing isomorphism $\mathbb{F}_2^2 \to H^\perp/H$. As any non-zero element in $\mathbb{F}_2^4$ gives us an order 2 subgroup, there are $2^4 - 1$ possible choices for H. After fixing H, there are 6 possible pairing reversing isomorphisms $\phi : \mathbb{F}_2^2 \to H^\perp/H$. We conclude that there are $6 \cdot 15 = 90$ distinct maximally isotropic subgroups in $\mathbb{F}_2^2 \times \mathbb{F}_2^4$.

□

Corollary 1.2.9. *There are exactly 90 distinct simple maximal isotropic subgroups in* $\mathrm{Jac}(X_1)[2] \times \mathrm{Jac}(Y_2)[2]$.

1.3 Explicit description of maximal isotropic subgroups

Let X_1 be given by the equation $y^2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)$, and let Y_2 be given by the equation $y^2 = (x-\beta_1)(x-\beta_2)(x-\beta_3)(x-\beta_4)(x-\beta_5)(x-\beta_6)$. We are now going to give a more explicit description of the indecomposable maximal isotropic subgroups of $\mathrm{Jac}(X_1) \times \mathrm{Jac}(Y_2)$ in terms of the roots of these curves.

For that we first need the following lemma about the structure of the 2-torsion group of hyperelliptic curves.

Lemma 1.3.1. *Let C be a hyperelliptic curve given by the equation*

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

where f is a monic polynomial of either degree $2g+1$ or of degree $2g+2$. Denote the roots of f by α_i. If $\deg f = 2g+1$, we let $B = \{1,2,\dots,2g+1,\infty\}$. Otherwise, $B = \{1,2,\dots,2g+1,2g+2\}$. For any two subsets S_1, S_2 of B, we define $S_1 + S_2 = (S_1 \cup S_2)\backslash(S_1 \cap S_2)$. We define S^c to be the complement of S in B. Then the set $G = \{S \subset B | \#S \cong 0 \mod 2\}\backslash\{S \sim S^c\}$ forms a group under the operation $+$. Let $O = \infty$ if f is of degree $2g+1$ and let O be $(\alpha_{2g+2}, 0)$ otherwise. Let $\psi : B \to \mathrm{Div}(C)$ be given by $\psi(s) = (\alpha_s, 0) - O$ if $s \neq \infty$ and $\psi(\infty) = \infty - O$. Then the morphism $\phi_C : G \to \mathrm{Jac}(C)[2]$ given by $[S] \mapsto \sum_{s \in S}[\psi(s)]$ is an isomorphism.

Proof. See [12] Lemma 2.4

□

Lemma 1.3.2. *Let G be as in Lemma 1.3.1. Then the Weil pairing $\langle\cdot,\cdot\rangle$ is given by $\langle S_1, S_2\rangle = \#(S_1 \cap S_2) \mod 2$.*

Proof. See [12] Proposition 6.3 □

Definition 1.3.3. Let R be a set. We define

$$G_R = \{S \subset R | \#S \cong 0 \mod 2\}\backslash\{S \sim S^{c_R}\}$$

where S^{c_R} is the complement of S in the set R.

Let $A = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ be the set of roots of the equation for X_1, and let $B = \{\beta_1, \beta_2, \dots, \beta_6\}$ consist of the roots of the equation for Y_2. Let

$$M(A,B) = \{(T,f) | T \subset B, |T| = 2, f : A \to B\backslash T \text{ injective}\}.$$

Remark 1.3.4. As A has only four elements a morphism $f : A \to B\backslash T$ is specified when we know where to send the four elements. We will sometimes write $((\alpha_1,\beta_1),(\alpha_2,\beta_2),(\alpha_3,\beta_3),(\alpha_4,\beta_4))$ for the morphism defined by $f(\alpha_i) = \beta_i$.

Now let $m_1 = (T_1, f_1), m_2 = (T_2, f_2) \in M$. Assume that $T_1 = T_2$. In this case, f_1 and f_2 have the same domain. Let V_4 be Klein's four group and let V_4 act transitively on $B\backslash T_2$. We say that $m_1 \sim m_2$ if there exists some $g \in V$ such that $f_1 = f_2 \circ g$.

Definition 1.3.5. We define the *set of isotropic subgroups with respect to A and B* as

$$\mathrm{Isot}(A,B) = M(A,B)/\sim.$$

Corollary 1.3.6. *Let A and B be as above. Then $\left(\mathrm{Jac}(X_1), \langle\cdot,\cdot\rangle_{X_1,2}\right) \cong (G_A, \langle\cdot,\cdot\rangle_A)$ and $\left(\mathrm{Jac}(Y_2), \langle\cdot,\cdot\rangle_{Y_2,2}\right) \cong (G_B, \langle\cdot,\cdot\rangle_B)$ as vector spaces with a bilinear pairing. Here, $\langle\cdot,\cdot\rangle_{X_1,2}$ and $\langle\cdot,\cdot\rangle_{Y_2,2}$ are the respective Weil pairings.*

Proof. This follows from Lemma 1.3.1 and Lemma 1.3.2. □

Proposition 1.3.7. *(i) There exists a map τ from* $\mathrm{Isot}(A,B)$ *to the set of indecomposable maximal isotropic subgroups of* $\mathrm{Jac}(X_1)\times\mathrm{Jac}(Y_2)$.

(ii) The map σ is a bijection

Proof. (i) By Corollary 1.3.6 it suffices to establish a map from $\mathrm{Isot}(A,B)$ to the set of indecomposable maximal isotropic subgroups of $G_A\times G_B$. The bilinear pairing $\langle\cdot,\cdot\rangle$ on $G_A\times G_B$ will be the product pairing of $\langle\cdot,\cdot\rangle_A$ and $\langle\cdot,\cdot\rangle_B$.

Let $m=[(T,f)]\in\mathrm{Isot}(A,B)$. We will construct a tuple $(\widetilde{H}_T,\widetilde{\phi}_T)$ as defined in Lemma 1.2.7 to specify a maximally isotropic subgroup of $G_A\times G_B$ with respect to $\langle\cdot,\cdot\rangle$. Define $\widetilde{H}_T$ to be the 1-dimensional subvectorspace of G_B as $\widetilde{H}_T=\langle[T]\rangle$. In order to use f to define $\widetilde{\phi}_T$ we will first give an explicit description of $\widetilde{H}_T^t/\widetilde{H}_T$. Because $\langle S_1,S_2\rangle=0$ if and only if $\#(S_1\cap S_2)$ is even, the orthogonal complement $\widetilde{H}_T^t$ in G_B with respect to $\langle\cdot,\cdot\rangle_B$ is given by

$$\widetilde{H}_T^t=\{[S]\in G_B|\#(S\cap T)=0\text{ or }\#(S\cap T)=2\}=\{[S]\in G_B|S\cap T=\emptyset\text{ or }S\cap T=T\}.$$

Remark that if $S\cap T=T$ then $S^{c_B}\cap T=\emptyset$. This implies that if $[S]\in H_T^t$ either $S\subset B\backslash T$ or $S^{c_B}\subset B\backslash T$. By always choosing the representative contained in B/T, we can conclude that

$$\widetilde{H}_T^t\cong\{S\subset B\backslash T|\#S\cong 0\mod 2\}$$

as vector spaces over $\mathbb{F}_2$. Write ψ for this isomorphism. We have $\psi([T])=B/T$, so we find that

$$\widetilde{H}_T^t/\widetilde{H}_T\cong\{S\subset B\backslash T|\#S\cong 0\mod 2\}\backslash\{S\sim S^{c_{B\backslash T}}\}=G_{B/T}.$$

As $f:A\to B\backslash T$ is an injective morphism, it induces an injective morphism

$$\widetilde{\phi}_T:\mathrm{Jac}(X_1)[2]\cong G_A\to G_{B\backslash T}\cong\widetilde{H}_T^t/\widetilde{H}_T$$

by $\widetilde{\phi}_T([S])=[f(S)]\in G_{B\backslash T}$ Now $\langle\widetilde{\phi}_T(S_1),\widetilde{\phi}_T(S_2)\rangle_{B\backslash T}=\#f(S_1)\cap f(S_2)\mod 2$ and $\langle S_1,S_2\rangle_A=S_1\cap S_2\mod 2$. As f is injective, we see that $\widetilde{\phi}_T$ is pairing preserving. But as we are working over $\mathbb{F}_2$, being pairing preserving is the same as being pairing reversing, so $\widetilde{\phi}_T$ is also pairing reversing. Now we have found a tuple $(\widetilde{H}_T,\widetilde{\phi}_T)$ as in Lemma 1.2.7. We define

$$\tau([(T,f)])=\left(\phi_{Y_2}(\widetilde{H}_T),\phi_{Y_2}\circ\widetilde{\phi}_T\circ\phi_{X_1}^{-1}\right)=(H_T,\phi_f).$$

We still need to show that τ is well-defined. It suffices to show that $(\widetilde{H}_T,\widetilde{\phi}_T)$ is well-defined. Assume that $(T,f_1)\sim(T,f_2)$. We want to show that $(\widetilde{H}_T,\phi_{f_1})=(\widetilde{H}_T,\phi_{f_2})$, so we need to prove that ϕ_{f_1} and ϕ_{f_2} give us the same morphism. Let $\sigma\in V_4$ and let $[S]\subset G_A$. Then either $\sigma(S)=S$ or $\sigma(S)=S^{c_A}\sim S$, so $[S]=[\sigma(S)]$ in G_A. It follows that $\phi_{f_1}=\phi_{f_2}$, and we see that the map is well-defined.

(ii) We will now prove that the map is a bijection. The map $T \mapsto \widetilde{H}_T$ is bijective as every subset $T \in B$ with $\#T = 2$ gives us a different non-zero 2-torsion point in $\mathrm{Jac}(X_2)$ and there are 15 of those. As the f_i are injective, $\phi_{f_1} = \phi_{f_2}$ implies that $f_1 = f_2 \circ \sigma$ for some $\sigma \in V$. It follows that $f \mapsto \widetilde{\phi}_T$ is injective. It remains to show that $f \mapsto \widetilde{\phi}_T$ is surjective. Assume that $A = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ and $B \backslash T = \{\beta_1, \beta_2, \beta_3, \beta_4\}$ and that we have $\phi(\alpha_1 + \alpha_2) = \beta_1 + \beta_2$ and $\phi(\alpha_1 + \alpha_3) = \beta_i + \beta_j$ with $i \neq j$. Then after potentially taking the complement,we get that $\phi(\alpha_1 + \alpha_3) = \beta_1 + \beta_k$ with $k \neq 1, 2$. Now define $f(\alpha_1) = \beta_1, f(\alpha_2) = \beta_2, f(\alpha_3) = \beta_k$ and $f(\alpha_4) = \beta_m$ where $m \neq 1, 2, k$. Then it follows that $\widetilde{\phi}_T = \phi$ by construction.

□

Corollary 1.3.8. *Let $T = \{\beta_5, \beta_6\}$ and assume $f(\alpha_i) = \beta_i$ for $i = 1, \ldots 4$. Then the tuple (H_T, ϕ_f) corresponds to the maximally isotropic subgroup*

$$\begin{aligned} G = \langle &(0, [(\beta_5, 0) - (\beta_6, 0)]), \\ &([(\alpha_1, 0) - (\alpha_4, 0)], [(\beta_1, 0) - (\beta_4, 0)]), \\ &([(\alpha_2, 0) - (\alpha_4, 0)], [(\beta_2, 0) - (\beta_4, 0)])\rangle. \end{aligned}$$

Proof. By definition

$$H_T = \langle \phi_{Y_2}([T])\rangle = \langle [(\beta_5, 0) - (\beta_6, 0)]\rangle$$

and

$$\phi_f([(0, \alpha_i) - (0, \alpha_j)]) = [(0, \beta_i) - (0, \beta_j)]$$

for $i, j \in [1, \ldots 4]$. Applying the construction in Lemma 1.2.7 gives us that the corresponding maximally isotropic subgroup is defined as

$$G = \{(x, \phi(x) + h) | x \in \mathrm{Jac}(X_1), \quad h \in H\}.$$

We see that G is generated by the elements $(0, h)$ with $h \neq 0$ and $(x, \phi_f(x))$ with $x \in \mathrm{Jac}(X_1)$. As $[(\alpha_1, 0) - (\alpha_4, 0)] + [(\alpha_2, 0) - (\alpha_4, 0)] = [(\alpha_3, 0) - (\alpha_4, 0)]$, we get that

$$\begin{aligned} G = \langle &(0, [(\beta_5, 0) - (\beta_6, 0)]), \\ &([(\alpha_1, 0) - (\alpha_4, 0)], [(\beta_1, 0) - (\beta_4, 0)]), \\ &([(\alpha_2, 0) - (\alpha_4, 0)], [(\beta_2, 0) - (\beta_4, 0)])\rangle. \end{aligned}$$

□

Example 1.3.9. Let the equation of Y_2 be given by

$$y^2 = x(x+2)(x^2 - 2x - 2)(x^2 - 6)$$

and let X_1 be given by

$$x(x^2-6).$$

Write β_i for the roots of x^2-2x-2. Then $M = (\{\beta_1,\beta_2\},(0,0),(-2,\infty),(\sqrt{6},\sqrt{6}),(-\sqrt{6},-\sqrt{6}))$ defines an element of $\mathrm{Isot}(X_1,Y_2)$. We can, moreover, show that the maximally isotropic subgroup given by M is Galois-invariant. Indeed, we have the following proposition.

Proposition 1.3.10. *Let X_1 and Y_2 be curves over a field k. Let $(T,f) \in \mathrm{Isot}(X_1,Y_2)$. Then, the induced maximally isotropic subgroup $G = (H_T,\phi_f)$ is invariant under the action of $Gal(\overline{k}/k)$ if and only if T is Galois-invariant, and $\phi_f \circ \sigma = \sigma \circ \phi_f$ for all $\sigma \in Gal(\overline{k}/k)$.*

Proof. Assume that (H_T,ϕ_f) is Galois-invariant. More explicitly, we assume that $G = \{(x,\phi_f(x)+h) | x \in \mathrm{Jac}(X_1)[2], h \in H_T\}$ (which is a subgroup of $\mathrm{Jac}(X_1)[2]\times \mathrm{Jac}(Y_2)[2]$) is Galois-invariant. We will first show that the set T is Galois-invariant.

Let $\sigma \in Gal(\bar{K}/K)$ and assume that $T = \{\beta_5,\beta_6\}$. Then $(0,h) = (0,(\beta_5,0)-(\beta_6,0)$. Let $\sigma(0,h) = (x,\phi_f(x)+h)$ for $x \in \mathrm{Jac}(X_1)[2]$. As σ preserves the Weil pairing and h pairs to 0 with everything, we find that

$$\langle \phi_f(x)+h, \phi_f(y)+h'\rangle_{Y_2,2} = 0$$

for all $y \in H_T^t$ and $h' \in H$. It follows that

$$\langle \phi_f(x)+h, \phi_f(y)+h'\rangle_{Y_2,2}\langle \phi_f(x), \phi_f(y)\rangle_{Y_2,2} = -\langle x,y\rangle_{X_1,2} = 0$$

for all $y \in H_T^t$ and $h' \in H$. Then $x = 0$ as the Weil-pairing on X_1 is non-degenerate. So $\sigma((0,h)) = (0,h')$ with $h' \in H_T$. As the point $(0,0)$ is rational, $\sigma((0,h)) \neq (0,0)$. It follows that $\sigma((0,h)) = (0,h)$, so we have $\sigma(T) = T$.

We will now show that $\phi_f \circ \sigma = \sigma \circ \phi_f$. We know that

$$\sigma((x,\phi_f(x))) = (\sigma(x),\sigma(\phi_f(x))) = (\sigma(x),\phi_f(\sigma(x))+h)$$

for some $h \in H_T$. It follows that $\sigma(\phi_f(x)) = \phi_f(\sigma(x)) \mod H_T$, which is what we wanted to show.

Now assume that T is Galois-invariant, and that $\phi_f\sigma = \sigma\phi_f$ for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$. Let $(x,\phi_f(x)+h) \in G$. Then

$$\sigma((x,\phi_f(x)+h)) = (\sigma(x),\sigma(\phi_f(x))+\sigma(h)) = (\sigma(h),\phi_f(\sigma(x))+h')$$

for some $h' \in H_T$. So, $\sigma((x,\phi_f(x)+h)) \in G$, which concludes the proof. $\square$

Corollary 1.3.11. *Let X_1 be a curve of genus 1 over k, and let Y_2 be a curve of genus 2 over k. If there exists a curve Z over k such that $(\phi, \mathrm{Jac}(Z), \mathcal{P}_Z)$ is a 2,2-glueing of X_1 and Y_2, then Y_2 has a model of the form*

$$y^2 = g(x)$$

over k where g contains a quadratic factor.

Proof. As $\ker(\phi)$ is defined over k, the maximally isotropic subgroup $(H, \psi) = \ker(\phi)$ needs to be fixed by $\mathrm{Gal}(\bar{k}/k)$. Write down some model of Y_2 of the form

$$y^2 = g(x)$$

where g is of degree 6. Assume that $g = \prod_{i=1}^{6}(x-\beta_i)$ over $\bar{k}$. The subgroup H of $\mathrm{Jac}(Y_2)[2]$ is generated by a unique 2-torsion element, which we can write as $(\beta_i, 0) - (\beta_j, 0)$ with $i \neq j$. Let $\sigma \in \mathrm{Gal}(\bar{k}/k)$. As the description of the 2-torsion point in terms of the roots is unique (up to permutation of i and j), and as σ fixes $(\beta_i, 0) - (\beta_j, 0)$, σ either fixes the roots or it permutes them. This means that $p(x) = (x-\beta_i)(x-\beta_j)$ remains fixed under all elements in $\mathrm{Gal}(\bar{k}/k)$, so $p(x)$ is a polynomial over k. This shows that $g(x)$ has a quadratic factor.

□

Definition 1.3.12. Let X be a hyperelliptic curve over a field k and let $y^2 = f$ be an equation for X over k. We define f to be of type $(d_1 \dots d_n)$ if there exists a factorzation $f = f_1 \dots f_n$ into irreducible factors with $d_i = \deg(f_i)$.

Definition 1.3.13. Let g be a polynomial of degree 6. We will say that g has a *legal type* if g contains a quadratic factor.

Remark 1.3.14. The legal types are

$$(111111), (2111), (2211), (222), (3111), (321), (411) \text{ or } (42).$$

Proposition 1.3.15. *Let X_1 and Y_2 be curves over a finite field k. Let X_1 be given by the equation $y^2 = f$, and let Y_2 be given by the equation $y^2 = g$. Then there exists a (2,2)-glueing of X_1 and Y_2 if and only if g is of legal type and f and g satisfy one of the following criteria*

(i) f *is of type* (1111) *and* g *does not contain an irreducible factor of degree* ≥ 3.

(ii) f *is of type* (211) *and* g *is of type* $(21111), (2211), (411)$ *or* (42).

(iii) f *is of type* (22), g *is of type* $(21111), (2211)$ *or* (222).

(iv) f *is of type* (31) *and* g *is of type* (3111) *or* (321),

(v) f *is of type* (4), g *is not of type* $(111111), (222), (3111)$ *or* (321)

Proof. Assume $f = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)$ and $g = (x-\beta_1)(x-\beta_2)(x-\beta_3)(x-\beta_4)(x-\beta_5)(x-\beta_6)$ over the algebraic closure of k. Let $(\{\beta_5, \beta_6\}, (\alpha_1, \beta_1), (\alpha_2, \beta_2), (\alpha_3, \beta_3)) \in \mathrm{Isot}(X_1, Y_2)$, assume T is Galois-invariant and that $[F\sigma] = [\sigma F]$ for all $\sigma \in \mathrm{Gal}(\overline{k}/k)$. The statement that g needs to be of legal type follows from Corollary 1.3.11.

First we assume f is of type (1111). This implies that $[F \circ \sigma] = [F]$ for all $\sigma \in Gal(\overline{k}/k)$. So $\sigma \in V_4$ and $\mathrm{Gal}(f,g) \subset V_4$. This means that either $\mathrm{Gal}(f,g) \cong C_1$ or $\mathrm{Gal}(f,g) \cong C_2$. So g cannot contain a factor of degree ≥ 3.

Assume f is of type (211). Then either $\mathrm{Gal}(f,g) \cong C_2$ or $\mathrm{Gal}(f,g) \cong C_4$. So g cannot contain an irreducible factor of degree 3.

Assume $\mathrm{Gal}(f,g) \cong C_2$ and let σ be a generator for this group. Then g needs to contain a quadratic factor. Assume g is of type (222). W.l.o.g. we can assume $\sigma(\beta_1) = \beta_2, \sigma(\beta_3) = \beta_4$, $\sigma(\beta_5) = \beta_6$. Then because $[\sigma F] = [F\sigma]$ it follows that the action of σ on the α_i is either (12)(34), (12)(34)(12)(34) = id. But the first case cannot happen a f contains only one quadratic factor. The second case cannot happen as σ is not the trivial element. We conclude that g is of type (21111), (2211), (411) or (42).

Assume f is of type (22). Then either $\mathrm{Gal}(f,g) \cong C_2$ or $\mathrm{Gal}(f,g) \cong C_4$. So g cannot contain an irreducible factor of degree 3.

Assume $\mathrm{Gal}(f,g) \cong C_4$ and let σ be a generator for this group. As β_5 and β_6 form a Galois-orbit, σ has to permute $\beta_1, \ldots \beta_4$ cyclically. Assume σ acts like (1234) on the β_i. Then because $[\sigma F = F\sigma]$ it follows that the action of σ on the α_i is either (1234) or (1234)(12)(34) = (13). The first case is impossible as g has no irreducible factor of degree 4. The second case is also impossible because if σ permutes one quadratic factor, it also needs to permute the other one. So, $\mathrm{Gal}(f,g) \cong C_2$, which implies that g is of type (21111), (2211) or (222).

Assume f is of type (31). Then $\mathrm{Gal}(f,g) \cong C_3$ or $\mathrm{Gal}(f,g) \cong C_6$. In the first case g will be of type (3111). In the second case g will be of type (321)

Assume f is of type (4). Then $\mathrm{Gal}(f,g) \cong C_4$. Let σ be a generator for this group. Assume σ acts like (1234) on the α_i. Then because $[\sigma F] = [F\sigma]$ it follows that the action of σ on the β_i is either (1234), (1234)(56), (1234)(12)(34) = (13) or (13)(56). This implies that g is not of type (111111), (222), (3111) or (321).

Conversely, we can easily find a group satisfying $[\sigma F] = [F\sigma]$ in all other cases. See Table 1.7.

□

Table 1.1: Galois stable groups in the finite field case

Type of f	Type of g	Group
(1111)	(111111)	$\langle \mathrm{id}, \mathrm{id} \rangle$
(1111)	(21111)	$\langle \mathrm{id}, (56) \rangle$
(1111)	(2211)	$\langle \mathrm{id}, (12)(34) \rangle$
(1111)	(222)	$\langle \mathrm{id}, (12)(34)(56) \rangle$
(211)	(21111)	$\langle (12), (12) \rangle$
(211)	(2211)	$\langle (12), (12)(56) \rangle$
(211)	(411)	$\langle (13), (1234) \rangle$
(211)	(42)	$\langle (13), (1234)(56) \rangle$
(22)	(21111)	$\langle (12)(34), (56) \rangle$
(22)	(2211)	$\langle (12)(34), (12)(34) \rangle$
(22)	(222)	$\langle (12)(34), (12)(34)(56) \rangle$
(31)	(3111)	$\langle (123), (123) \rangle$
(31)	(321)	$\langle (123), (123)(56) \rangle$
(4)	(21111)	$\langle (1234), (13) \rangle$
(4)	(2211)	$\langle (1234), (13)(56) \rangle$
(4)	(411)	$\langle (1234), (1234) \rangle$
(4)	(42)	$\langle (1234), (1234)(56) \rangle$

Table 1.2: Galois stable groups of type (1111, 111111)

Gal(f)	Gal(g)	Gal(f,g)	Group
C_1	C_1	C_1	$\langle (\mathrm{id}, \mathrm{id}) \rangle$

Table 1.3: Galois stable groups of type (22, 111111)

Gal(f)	Gal(g)	Gal(f,g)	Group
C_2	C_1	C_2	$\langle ((12)(34), \mathrm{id}) \rangle$

Theorem 1.3.16. *Let X_1, Y_2 be curves of genus 1 and genus 2 respectively. Assume X_1 is given by the equation $y^2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)$ and that Y_2 is given by the equation $y^2 = (x-\beta_1)(x-\beta_2)(x-\beta_3)(x-\beta_4)(x-\beta_5)(x-\beta_6)$. Let $A = \{\alpha_1, \ldots, \alpha_4\}$ and let $B = \{\beta_1, \ldots, \beta_6\}$. There exist bijections between the following sets:*

Table 1.4: Galois stable groups of type (4, 111111)

Gal(f)	Gal(g)	Gal(f,g)	Group
V_4	C_1	V_4	$\langle ((12)(34), \mathrm{id}), ((13)(24), \mathrm{id}) \rangle$

Table 1.5: Galois stable groups of type $(1111, 21111)$

$\mathrm{Gal}(f)$	$\mathrm{Gal}(g)$	$\mathrm{Gal}(f,g)$	Group
C_1	C_2	C_2	$\langle(\mathrm{id},(12))\rangle$

Table 1.6: Galois stable groups of type $(211, 21111)$

$\mathrm{Gal}(f)$	$\mathrm{Gal}(g)$	$\mathrm{Gal}(f,g)$	Group
C_2	C_2	C_2	$\langle((12),(12))\rangle$

Table 1.7: Galois stable groups of type $(22, 21111)$

$\mathrm{Gal}(f)$	$\mathrm{Gal}(g)$	$\mathrm{Gal}(f,g)$	Structure of $\mathrm{Gal}(f,g)$	$\lvert\mathrm{Gal}(f,g)\rvert$
C_2	C_2	C_2	$\langle((12)(34),(12))\rangle$	2
C_2	C_2	V_4	$\langle(\mathrm{id},(56)),((12)(34),\mathrm{id})\rangle$	4
V_4	C_2	V_4	$\langle((12),(12)),((12)(34),\mathrm{id})\rangle$	4

(i) *Tuples (H,ϕ) where H is a subgroup of $\mathrm{Jac}(Y_2)$ of order 2 and $\phi : \mathrm{Jac}(X_1) \to H^{\perp}/H$ is an isomorphism.*

(ii) *The elements of $\mathrm{Isot}(A,B)$ as defined in Proposition 1.3.7.*

(iii) *Potential $(2,2)$-glueings $(A,\mathcal{P})$ of X_1 and Y_2.*

Chapter 2

Glueing over $\mathbb{C}$

2.1 Abelian varieties over $\mathbb{C}$

Let X, Y be two curves over $\mathbb{C}$ of genus g_X, g_Y respectively. We want to study the Jacobians $\mathrm{Jac}(X)$ and $\mathrm{Jac}(Y)$ of X and Y and give an explicit description of the glueing process. For this, we study abelian varieties over $\mathbb{C}$. But first, we will repeat some general facts and definitions.

Proposition 2.1.1. *Let A be an abelian variety. Then the group of all line bundles on A up to linear equivalence, A^t is also an abelian variety and is called the dual abelian variety of A.*

Proof. See [4] Theorem 6.18 □

Proposition 2.1.2. *Let A be an abelian variety and let $\mathcal{L}$ be an ample line bundle on A. Then the map $\phi_{\mathcal{L}} : A \to A^t$ given by $\phi_{\mathcal{L}}(x) = t_x^*(\mathcal{L}) \otimes \mathcal{L}^{-1}$ is an isogeny. Furthermore, this map does not depend on the choice of the class of $\mathcal{L}$ modulo algebraic equivalence.*

Proof. See [4] Corollary 2.10. □

Definition 2.1.3. Let A be an abelian variety and let $\mathcal{L}$. A *polarization* on A is the choice of the class of an ample line bundle on A modulo algebraic equivalence or equivalently the choice of a map $\phi_{\mathcal{L}}$ as above. If $\phi_{\mathcal{L}}$ is an isomorphism, then $\mathcal{L}$ is called a principal polarization.

Definition 2.1.4. A tuple $(A, \mathcal{L})$ where A is an abelian variety and $\mathcal{L}$ is an ample line bundle is called a *polarized abelian variety*. If $\mathcal{L}$ is a principal polarization, then we call $(A, \mathcal{L})$ a *principally polarized abelian variety.*

Definition 2.1.5. Let $(A_1, \mathcal{L}_1), (A_2, \mathcal{L}_2)$ be two polarized abelian varieties. A map $\phi : A_1 \to A_2$ is called a morphism of polarized abelian varieties if $\phi^*(\mathcal{L}_2) \cong_{\mathrm{alg}} \mathcal{L}_1$.

We will now study these concepts over $\mathbb{C}$.

Theorem 2.1.6. *Let A be an abelian variety over $\mathbb{C}$ of dimension g. Then A is analytically isomorphic to a complex torus V/Λ where V is a g-dimensional complex vector space and Λ is a discrete subgroup of V of rank $2g$.*

Proof. See [1] Lemma 1.1. □

Definition 2.1.7. Let A be a complex torus where $A = V/\Lambda$ where V is a g-dimensional complex vector space and Λ is a discrete subgroup of V of rank $2g$. If we fix a basis $\mathcal{E} = \{e_1, \ldots e_g\}$ for V, and a basis $\mathcal{B} = \{\lambda_1, \ldots, \lambda_{2g}\}$ of Λ, we can write $\lambda_i = \sum_{j=1}^{g} \lambda_{i,j} e_j$. We will use the notation $(\lambda_i)_{\mathcal{E}}$ for the vector $(\lambda_{i,1}, \ldots, \lambda_{i,g})$.

Now consider the $g \times 2g$ matrix

$$\Pi = \begin{bmatrix} | & \cdots & | \\ (\lambda_1)_{\mathcal{E}} & & (\lambda_{2g})_{\mathcal{E}} \\ | & \cdots & | \end{bmatrix}$$

which has the λ_i as its column vectors with respect to $\mathcal{E}$.

Definition 2.1.8. The matrix Π we defined above is called *the period matrix* of the complex torus A with respect to $\mathcal{E}$ and $\mathcal{B}$.

Proposition 2.1.9. *Let $A = V/\Lambda$ and $B = V'/\Lambda'$ be two complex tori over $\mathbb{C}$ of dimension g and g′ respectively. Let $\phi : A \to B$ be a homomorphism. Then there exists a unique $\mathbb{C}$-linear map T_ϕ such that the following diagram commutes*

$$\begin{array}{ccc} V & \xrightarrow{T_\phi} & V' \\ \downarrow & & \downarrow \\ A & \xrightarrow{\phi} & B \end{array} .$$

Moreover, $T_\phi(\Lambda) \subset \Lambda'$ and the restriction $T_\phi|_\Lambda : \Lambda \to \Lambda'$ induces a $\mathbb{Z}$-linear map $R_\phi \Lambda \to \Lambda'$.

Proof. See [1] Proposition 2.1. □

Definition 2.1.10. We define T_ϕ to be the *analytic representation* of ϕ, and we define R_ϕ to be the *rational representation* of ϕ.

Proposition 2.1.11. *Let $A = V/\Lambda$ and $A' = V'/\Lambda'$ be two complex tori over $\mathbb{C}$ of dimension g and g′ respectively. Let $\phi : A \to A'$ be a homomorphism. Fix bases $\mathcal{E}, \mathcal{E}'$ for V and V' and bases $\mathcal{B}, \mathcal{B}'$ for Λ, Λ'. Let Π be the period matrix for A with respect to $\mathcal{B}$ and $\mathcal{E}$ and let Π' be the period matrix for A' with respect to $\mathcal{B}'$ and $\mathcal{E}'$. Identify R_ϕ and T_ϕ with their matrix representations with respect to the chosen bases.*

Then

$$T_\phi \Pi = \Pi' R_\phi.$$

Conversely, if we have $T \in \mathrm{Mat}_{g' \times g}(\mathbb{C})$ *and* $R \in \mathrm{Mat}_{2g',2g}(\mathbb{Z})$ *such that*

$$T\Pi = \Pi' R.$$

Then there exist some $\phi \in \mathrm{Hom}(A, B)$ *such that* $T_\phi = T$ *and* $R_\phi = R$.

Proof. See [1] Proposition 2.3. □

Remark 2.1.12. The condition

$$T_\phi \Pi = \Pi' R_\phi$$

is equivalent to stating that $\phi(\Lambda) \subset \Lambda'$.

Not every complex torus gives rise to an abelian variety. If A is a projective group scheme over $\mathbb{C}$. Then A comes equipped with an algebraic embedding $i : A \hookrightarrow \mathbb{P}^n_{\mathbb{C}}$. The existence of such an embedding i for a complex torus V/Λ is equivalent to the existence of an ample line bundle $\mathcal{L}$ on V/Λ. So to understand which complex tori correspond to abelian varieties we need to consider line bundles on V/Λ.

Lemma 2.1.13. *Let V be a complex vector space. There is a bijection between the Hermitian forms H on V and the real alternating forms E on V with $E(ix, iy) = E(x, y)$ given by*

$$E(x, y) = \mathrm{Im}\, H(x, y) \tag{2.1}$$

$$H(x, y) = E(ix, y) + iE(x, y) \tag{2.2}$$

Proof. See [11] page 19. □

Definition 2.1.14. Let V/Λ be a complex torus and let H be a Hermitian form on V such that $E = \mathrm{Im}\, H$ with $E(\Lambda \times \Lambda) \subset \mathbb{Z}$. Let $\alpha : \Lambda \to S^1 = \{z \in \mathbb{C}^* \mid \ |z| = 1\}$ be a map satisfying

$$\alpha(\lambda_1 + \lambda_2) = e^{i\pi E(\lambda_1, \lambda_2)} \cdot \alpha(\lambda_1)\alpha(\lambda_2) \text{ with } \lambda_1, \lambda_2 \in \Lambda.$$

Then we define $L(H, \alpha)$ to be the line bundle given by the quotient of $V \times \mathbb{C}$ by the action of Λ given by

$$\phi_\lambda(c, z) = (c \cdot \alpha(\lambda) \cdot e^{\pi H(z,\lambda) + \frac{1}{2}\pi H(\lambda,\lambda)}, z + \lambda).$$

The function $f_\lambda(c, z)$ is called a factor of automorphy for $L(H, \alpha)$.

Theorem 2.1.15 (Appel-Humbert). *Any line bundle L on a complex torus V/Λ is isomorphic to an $L(H,\alpha)$ for a unique tuple (H,α) as above. Furthermore, the class of $L(H,\alpha)$ modulo algebraic equivalence only depends on the choice of H.*

Proof. See [11] page 20. □

Lemma 2.1.16. *Let $A = V/\Lambda$ be a complex torus of dimension g. Let $\mathcal{E}$ be a basis for V, and let $\mathcal{B}$ be a basis for Λ. Let Π be its period matrix with respect to the chosen bases. Let H be a Hermitian form on V such that $E = \operatorname{Im} H$ with $E(\Lambda \times \Lambda) \subset \mathbb{Z}$. Write $M_E \in \operatorname{Mat}_{2g\times 2g}(\mathbb{Z})$ for the matrix representation of E with respect to $\mathcal{B}$. Then H is positive-definite if and only if*

(i) $\Pi M_E^{-1} \Pi^t = 0$,

(ii) $i\Pi M_E^{-1} \Pi^t > 0$.

Theorem 2.1.17 (Lefschetz). *Let $A = V/\Lambda$ be a complex torus of dimension g. Let H be a Hermitian form on V such that $\operatorname{Im}(H)$ is integral on $\Lambda \times \Lambda$. Let α be a function as in Definition 2.1.14. Then $L(H,\alpha)$ is ample if and only if H is positive definite.*

Proof. See [11] page 35. □

Lemma 2.1.18 (Frobenius). *Let Λ be a lattice of rank $2g$. Let $E : \Lambda \times \Lambda \to \mathbb{Z}$ be a nondegenerate bilinear alternating form. There exist positive integers $d_1, \dots d_g$ with $d_i | d_{i+1}$ and a basis $e_1, \dots e_g, f_1, \dots f_g$ of Λ such that if we set $D = \operatorname{diag}(d_1, \dots, d_g)$ then the matrix of E with respect to this basis has the form*

$$\begin{bmatrix} 0 & D \\ -D & 0 \end{bmatrix}.$$

Proof. See [9] A.5.3.1 □

Definition 2.1.19. Such a basis is called a *Frobenius basis* for E, and the integers d_i are called the *invariants* of E.

Let $A = V/\Lambda$ be an abelian variety. We can explicitly construct the dual abelian variety in the following way:

Let $V^t = \operatorname{Hom}_{\mathbb{C}-antilinear}(V, \mathbb{C})$ and let $\Lambda^t = \{l \in V^t | \operatorname{Im} l(\lambda) \in \mathbb{Z}$, for all $\lambda \in \Lambda$. We can identify V^t/Λ^t with A^t using the isomorphism

$$l \mapsto L\Big(0, \lambda \mapsto e^{2\pi i \operatorname{Im} l(u)}\Big).$$

Lemma 2.1.20. *Let $A = V/\Lambda$ and $A' = V'/\Lambda'$ be abelian varieties and let $\phi : A \to A'$ be an isogeny. Fix bases $\mathcal{B}$ and $\mathcal{B}'$ for the lattices Λ and Λ' respectively. Let $L(H',\alpha')$ be a polarization on A'. Let E' be the alternating form with matrix* *representation $M_{E'}$ with respect to $\mathcal{B}'$ and let R_ϕ be the rational representation of ϕ with respect to Λ and Λ'. Then $L(H,\alpha) = \phi^*(L(H',\alpha')) = L(H'(T_\phi, T_\phi), \alpha' \circ R_\phi)$ and the matrix representation of the alternating bilinear form $E = \phi^*(E)$ corresponding to $L(H,\alpha)$ with respect to the basis $\mathcal{B}$ is given by $M_E = R_\phi^t M_{E'} R_\phi$.*

Proof. Appendix B of [1] tells us that if $f'_\lambda(c,z)$ is a factor of automorphy for $L'(H',\alpha')$ then

$$f_\lambda(c,z) = (c \cdot \alpha'(R_\phi \lambda) \cdot e^{\pi H'(T_\phi z, R_\phi \lambda) + \frac{1}{2}\pi H'(R_\phi \lambda, R_\phi \lambda)}, T_\phi z + R_\phi \lambda)$$

is a factor of automorphy for $\phi^*(L'(H',\alpha'))$. As $T_\phi \lambda = R_\phi \lambda$ for all $\lambda \in \Lambda$, it follows that that $L(H,\alpha) = \phi^* L(H',\alpha') = L(H'(T_\phi, T_\phi), \alpha' \circ R_\phi)$. And we see that $H = H'(T_\phi, T_\phi)$. Using once again that $T_\phi \lambda = R_\phi \lambda$ for all $\lambda \in \Lambda$, we find that the alternating bilinear form E induced by H is represented by $M_E = R_\phi^t M_{E'} R_\phi$. □

Corollary 2.1.21. *Let $\phi : A = V/\Lambda \to A' = V'/\Lambda'$ be a morphism of abelian varieties. Assume that R_ϕ is the rational representation of ϕ with respect to a choice of bases on Λ and Λ'. Let $\phi^t : (A')^t \to A^t$ be the dual morphism defined by pulling back line bundles. Then ϕ^t is given by $l \mapsto R_\phi^t l$ with respect to the induced bases on the dual abelian varieties.*

Proof. Let $L(0,\alpha)$ be a line bundle. Now

$$\phi^*\Big(L\Big(0, e^{2\pi i \operatorname{Im} l(u)}\Big)\Big) = L\Big(0, e^{2\pi i \operatorname{Im} l(R_\phi u)}\Big) = L\Big(0, e^{2\pi i \operatorname{Im} R_\phi^t l(u)}\Big).$$

So ϕ^t is given by $l \mapsto R_\phi^t l$. □

Remark 2.1.22. One can show that given H, a compatible α as in Definition 2.1.14 always exists. See [11] page 19-20. As we saw in Theorem 2.1.15 the polarization only depends on H or the corresponding alternating bilinear form E. If we want to study polarized abelian varieties, we can therefore restrict ourselves to studying tuples $(A = V/\Lambda, E)$ where S is an alternating bilinear form $E : \Lambda \times \Lambda \to \mathbb{Z}$ with $E(ix,iy) = E(x,y)$.

To complete our survey of all the ingredients we need in order to glue explicitly, we will discuss the Weil pairing.

Proposition 2.1.23. *Let $\phi : A = V/\Lambda \to A' = V/\Lambda'$ be an isogeny and let $\phi^t : (A')^t \to A^t$ be its dual isogeny. There is an isomorphism of group schemes*

$$\beta : \ker(\phi^t) \to \ker(\phi)^D$$

explicitly given by $(0, e^{2\pi i \psi}) \to (\lambda \mapsto e^{2\pi i \psi \circ \phi}|_{\ker(\phi^t)})$

Proof. The proof of that this isomorphism exists can be found in [4] Theorem 7.5. Let us see what this map looks like explicitly.

Let $\mathcal{L} \in \ker(\phi^t)$. Then $\mathcal{L} = L(0, e^{2\pi i\psi})$ where ψ is an element of $\mathrm{Hom}_{\mathbb{C}-antilinear}(V', \mathbb{C})$ that takes integer values on Λ'. Now the pullback of L is given by $(0, e^{2\pi i\psi\circ\phi})$ by Lemma 2.1.20. Now $\psi \in \ker(\phi^t)$ if and only if $(0, e^{2\pi i\psi\circ\phi})$ is the trivial bundle, i.e. if and only if $\psi \circ \phi$ is the identity map on Λ. According to the proof of Theorem 7.5, the character $\beta(L)$ corresponds to is given by $\lambda \mapsto e^{2\pi i\psi\circ\phi(\lambda)}$ with $\lambda \in \Lambda'/\Lambda = \ker(f^t)$. □

Definition 2.1.24. Let $n_A : A \to A$ be multiplication by n on the abelian variety A over $\mathbb{C}$. Let $\beta : \ker(f^t) \to \ker(f)^D$ be the isomorphism described in 2.1.23.

(i) Define
$$e_n : \ker(f) \times \ker(f^t) \to \mathbb{G}_{m,k}$$
to be the perfect bilinear pairing given by $e_n(x, y) = \beta(y)(x)$.

(ii) Let $\phi : A \to A^t$ be a polarization. We write
$$e_n^\phi : A[n] \times A[n] \to \mu_n$$
for the bilinear pairing given by $e_n^\phi(x, y) = e_n(x, \phi(y))$.

Proposition 2.1.25. *Let $A = V/\Lambda$. Let ϕ be a polarization $A \to A^t$ and let E be the alternating bilinear form corresponding to ϕ. Then*
$$e_n^\phi\left(\frac{1}{n}\lambda_1, \frac{1}{n}\lambda_2\right) = e^{2\pi i \frac{1}{n} E(\lambda_1, \lambda_2)}$$
where $\lambda_i \in \Lambda$.

Proof. Using Proposition 2.1.23 we can describe the Weil pairing in terms of the polarization. We have
$$e_n^\phi(x, y) = e_n\left(x, \left(0, e^{2\pi i E(y,-)}\right)\right) = \beta\left(\left(0, e^{2\pi i E(y,-)}\right)\right)(x) = e^{2\pi i n E(y,x)}.$$
As $y \in \ker(n_X)$ we see that $y = \frac{1}{n}\lambda$ with $\lambda \in \Lambda$. So,
$$e_n^\phi\left(\frac{1}{n}\lambda_1, \frac{1}{n}\lambda_2\right) = e^{2\pi i n E(\frac{1}{n}\lambda_1, \frac{1}{n}\lambda_2)} = e^{2\pi i \frac{1}{n} E(\lambda_1, \lambda_2)}$$
which concludes the proof. □

2.2 (2,2)-Glueing over $\mathbb{C}$

We now want to give an explicit description of the glueing process over $\mathbb{C}$. We will initially only concern ourselves with glueing principally polarized abelian varieties. Later on, we will discuss in which cases the glued abelian variety actually corresponds to the Jacobian of a curve.

Definition 2.2.1. We define the *standard symplectic matrix* $S_n \in \mathrm{Mat}_{2n\times 2n}(\mathbb{C})$ as

$$S_n = \begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix}$$

where I_n is the n-dimensional identity matrix.

Definition 2.2.2. Let $A_1 = V_1/\Lambda_1$, $A_2 = V_2/\Lambda_2$ be abelian varieties and fix bases $\mathcal{B}_1, \mathcal{B}_2$ for Λ_1, Λ_2 and $\mathcal{E}_1, \mathcal{E}_2$ for V_1 and V_2. Let Π_1, Π_2 be the period matrices with respect to these choices of bases. Now let $\mathcal{B}_{1,2} = \{(b_i, 0) | b_i \in \mathcal{B}_1\} \cup \{(0, b_i') | b_i' \in \mathcal{B}_2\}$ be the natural basis for $V_{1,2} = V_1 \times V_2$. We similarly define a basis $\mathcal{E}_{1,2}$ for $\Lambda_{1,2} = \Lambda_1 \times \Lambda_2$ using $\mathcal{E}$ and $\mathcal{E}'$. Then the matrix $\Pi_1 \times \Pi_2$ given by

$$\Pi_1 \times \Pi_2 = \begin{bmatrix} \Pi & 0 \\ 0 & \Pi' \end{bmatrix}$$

is the period matrix for $A_1 \times A_2$ with respect to the bases $\mathcal{B}_{1,2}$ and $\mathcal{E}_{1,2}$. We will call it the *product period matrix* of $A_1 \times A_2$ for Π_1 and Π_2.

Now let (A_1, E_1) and (A_2, E_2) be principally polarized abelian varieties over $\mathbb{C}$ of genus 1 and genus 2 respectively. Let $A_1 = V_1/\Lambda_1$ and $A_2 = V_2/\Lambda_2$ and choose Frobenius bases $\mathcal{B}_1$ and $\mathcal{B}_2$ of the lattices for E_1 and E_2.

Let $\mathcal{E}_i$ be the standard basis for $\mathbb{C}^i$ for $i = 1, 2$. Let Π_1 be the period matrix of A_1 with respect to $\mathcal{B}_1$ and $\mathcal{E}_1$ and let Π_2 be the period matrix of A_2 with respect to $\mathcal{B}_2$ and $\mathcal{E}_2$. Let $\Pi_1 \times \Pi_2$ be the product period matrix of $A_1 \times A_2$ with respecto to the bases $\mathcal{E}_{1,2}$ and $\mathcal{B}_{1,2}$. With respect to the chosen bases, the matrix representation M_{E_i} of the alternating form E_i will look like the standard symplectic matrix S_i (for $i = 1, 2$), and for the induced product polarization $E_{1,2}$ on $A_1 \times A_2$ we get

$$M_{E_{1,2}} = \begin{bmatrix} S_1 & 0 \\ 0 & S_2 \end{bmatrix}.$$

By definition, a (2,2)-glueing of A_1 and A_2 is a triple (B, E_B, ϕ) of a polarized abelian variety B, a polarization E_B on B and an isogeny $\phi : A_1 \times A_2 \to B$ such that $\phi^*(E_B) = 2E_{1,2}$. Finding such an isogeny is equivalent to looking for a subgroup of $A_1[2] \times A_2[2]$ that is maximally isotropic with respect to the Weil pairing e_2.

Write $\lambda_1,\ldots,\lambda_6$ for the column vectors of $\Pi_{1,2}$. Then we have a natural isomorphism $\sigma : A_1[2]\times A_2[2] \cong (1/2\Pi_{1,2})/\Pi_{1,2} \to \mathbb{F}_2^6$ by $\frac{1}{2}\lambda_i \mapsto v_i$ where the v_i form a standard basis of $\mathbb{F}_2^6$. Proposition 2.1.25 now tells us that the Weil pairing e_2 on $A_1[2]\times A_2[2]$ can be respresented by the matrix $E_{\mathbb{F}_2}$ where $E_{\mathbb{F}_2 i,j} = E_{i,j} \mod 2$. Using this identification and making a base change if necessary, Proposition 1.2.2 tells us there are 135 maximally isotropic subgroups in $\mathbb{F}_2^6$ with respect to the Weil pairing, which means there are 135 different ways to glue A_1 and A_2.

Now fix a subgroup G of $A_1[2]\times A_2[2]$ that is maximally isotropic with respect to the Weil pairing. We will now construct the glued abelian variety.

Let $g_1, g_2, g_3 \in G$ be such that $< g_1, g_2, g_3 >= G$. and choose lifts $\lambda_1', \lambda_2', \lambda_3' \in \Lambda$ such that $\sigma\left(\frac{1}{2}\lambda_i'\right) = g_i$.

Consider the lattice $\Lambda_G =< \lambda_1,\ldots,\lambda_6,\lambda_1',\lambda_2',\lambda_3' >$. We calculate a new LLL-reduced basis $\mathcal{M} = \mu_1,\ldots,\mu_6$ for Λ_G. Write

$$\Pi_G = \begin{bmatrix} | & \cdots & | \\ (\mu_1)_{\mathcal{E}_{1,2}} & & (\mu_6)_{\mathcal{E}_{1,2}} \\ | & \cdots & | \end{bmatrix}.$$

for the period matrix of V/Λ_G.

Lemma 2.2.3. *Let $\mu_i = \sum_{j=1}^{6} \mu_{i,j}\lambda_j$ and write $(\mu_i)_{\mathcal{B}_{1,2}} = (\mu_{i,1},\ldots,\mu_{i,6})$. note that $\mu_{i,j} \in 1/2\mathbb{Z}$. Set*

$$R = \begin{bmatrix} | & \cdots & | \\ (\mu_1)_{\mathcal{B}_{1,2}} & & (\mu_6)_{\mathcal{B}_{1,2}} \\ | & \cdots & | \end{bmatrix}.$$

Then R^{-1} is the rational representaion of the quotient morphism $\phi_G : V/\Lambda \to V/\Lambda_G$ with respect to the bases $\mathcal{B}$ and $\mathcal{M}$. In particular, $R^{-1}(\mu_i) \subset \Lambda_G$ and $\ker\phi_G =< \mu_i >$.

Proof. As μ_i is a column vector of R^{-1}, we find that $R^{-1}((\mu_i)_{\mathcal{B}_{1,2}}) = (\mu_i)_{\mathcal{M}}$. This also implies that $R^{-1}(\Lambda) \subset \Lambda_G$, and if we define $R_\phi = R^{-1}$ there exists a corresponding T_ϕ, such that $T_\phi\Pi_{1,2} = \Pi_G R_\phi$, which induces a morphism $\phi_G : V/\Lambda \to V/\Lambda_G$. Furthermore, $v \in \ker\phi_G$ if and only if $\phi(v)$ has integer coefficients. This can only happen if v is contained in the $\mathbb{Z}$-span of the μ_i, so $\ker\phi_G =< \mu_i >$. □

Now that we have calculated the rational representation of the morphism $\phi_G : V/\Lambda \to V/\Lambda_G$, we can use this to calculate a polarization with alternating form E_G on V/Λ_G whose pullback to V/λ via ϕ will have alternating form equal to $2E_{1,2}$. We get that

$$M_{E_G} = (R_\phi^t)^{-1} 2E_{1,2} R_\phi^{-1}$$

has the required properties. As E_G completely determines the class of the polarization, this suffices to determine the glueing.

Proposition 2.2.4. *Let $(A_1, E_1), (A_2, E_2)$ be abelian varieties as above, and let G be a maximally isotropic subgroup of $A_1[2] \times A_2[2]$ with respect to $E_{\mathbb{F}_2}$. Let $B_G = V/\Lambda_G$ as above. Then (B_G, E_G) is a (2,2)-glueing of (A_1, E_1) and (A_2, E_2).*

Proof. We have
$$R_\phi^t M_{E_G} R_\phi = 2E_{1,2}$$
by construction, and M_{E_G} is the alternating form corresponding to a principal polarization by Proposition 1.1.9 and Lemma 2.1.20. □

2.3 Reconstructing the curve

Before we begin, we first remark that we will need to use a different algorithm depending on whether B_G is the Jacobian of a hyperelliptic curve or of a non-hyperelliptic curve. For this we need a way to distinguish between the two cases. We will do this by using theta constants.

Definition 2.3.1. Let $(A = V/\Lambda, E)$ be a principally polarized abelian variety with $\Pi = (\Omega_1, \Omega_2)$ a period matrix for A. Here $\Omega_1, \Omega_2 \in \mathrm{Mat}_{g\times g}(\mathbb{C})$. Then $\tau = \Omega_1^{-1}\Omega_2$ is called the small period matrix of (A, E).

Definition 2.3.2. Let $\omega \in \mathbb{C}^3$ and let τ be the small period matrix. We define the theta series
$$\theta(\omega, \tau) = \sum_{n \in \mathbb{Z}^g} \exp(\pi i n^t \tau n + 2\pi i n^t \omega).$$

Let $\xi \in V$ such that $\pi(\xi) \in A[2]$ where $\pi : V \to A$ is the quotient map. This means that $\xi = \frac{1}{2}\xi_1 + \frac{1}{2}\tau\xi_2$ with $\xi_i \in \mathbb{Z}^g$.

Definition 2.3.3. We define

$$\theta[\xi](\tau) = \exp(\pi i \xi_1^T \tau \xi_1 + 2\pi i \xi_1^T \xi_2)\theta(\xi_2 + \tau\xi_1, \tau).$$

The value $\theta[\xi](\tau)$ is called a theta constant.

Theorem 2.3.4. *Assume that τ corresponds to the Jacobian of a curve. If there exists an even theta constant that vanishes, then τ corresponds to a non-hyperelliptic curve.*

Proof. See Theorem 4 in [7] □

Now assume that we have two curves X_1 and Y_2 over $\mathbb{C}$ of genus 1 and genus 2 respectively. Let G be a maximally isotropic subgroup of $\mathrm{Jac}(X_1)[2] \times \mathrm{Jac}(Y_2)[2]$ and let (B_G, E_g) be the glueing of $\mathrm{Jac}(X_1)$ and $\mathrm{Jac}(Y_2)$ along G. This B_G does not necessarily correspond to the Jacobian of a curve. For genus 3 it is known that the set of Jacobians is equal to the set of indecomposable principally polarized abelian varieties. See for example the exposition in [6]. We can therefore restrict ourselves to studying the 90 simple maximally isotropic subgroups saw in Corollary 1.2.8.

From now on, we will assume that G is indecomposable and reconstruct the curve from its period matrix.

The algorithm will work as follows. We first calculate period matrices Π_1, Π_2 for the curves X_1 and Y_2 in the following way.

Let $\gamma_{1,1}, \gamma_{1,2}$ be a homology basis for X_1, and let $\gamma_{2,1}, \dots \gamma_{2,4}$ be a homology basis for Y_2. Let $\omega_{1,1}$ be a differential form on X_1, and let $\omega_{2,1}, \omega_{2,2}$ be linearly independent differential forms on Y_2. We can calculate

$$\lambda_{g,j} = \left(\int_{\gamma_{g,j}} \omega_{g,1}, \dots \int_{\gamma_{g,j}} \omega_{g,g} \right)$$

for $g = 1, 2$, $j = 1, \dots 2g$ using the work by Christian Neurohr [13]. Let $\Lambda_g = \langle \lambda_{g,j} \rangle$. Let $V_1 = \mathbb{C}, V_2 = \mathbb{C}^2$. Then $\mathrm{Jac}(X_1) \cong V_1/\Lambda_1$ and $\mathrm{Jac}(Y_2) \cong V_2/\Lambda_2$.

We get the period matrices

$$\Pi_g = \begin{bmatrix} | & \cdots & | \\ \lambda_{g,1} & & \lambda_{g,2g} \\ | & \cdots & | \end{bmatrix}$$

and the polarizations E_G will already be in standard form with respect to these choices of bases. We use the process in Section 2.2 to find the rational representation R_ϕ of taking the quotient by G. Now the matrix representation M_{E_G} of E_G satisfies $M_{E_G} = (R_\phi^t)^{-1} 2E_{1,2} R_\phi^{-1}$ by Proposition 2.2.4. But M_{E_G} is not necessarily the standard symplectic matrix. In order to find the correct corresponding period matrix, we need to make a change of coordinates to put M_{E_G} into standard form. As M_{E_G} is a principal polarization, there exists a symplectic base change matrix S such that $(S^t)^{-1} M_{E_G} S^{-1} = S_3$. As a consequence,

$$(S^{-1})^t (R_\phi^t)^{-1} 2E_{1,2} R_\phi^{-1} S^{-1} = S_3$$

and the period matrix Π_G corresponding to the glueing will be

$$\Pi_G = (\Pi_1 \times \Pi_2) R_\phi^{-1} S^{-1}.$$

We now calculate the theta constants for Π_G. If there exists an even theta constant that vanishes, we expect the resulting curve C to be hyperelliptic, and we can use the algorithm developed by Balakrishnan, Ionica, Lauter, and Vincent in [7] to compute the Rosenhain invariants of C.

If there are no even theta constants that vanIsh, we expect the curve to be non-hyperelliptic however, and we can use the methods developed by Lercier, Ritzenthaler, and Sijsling in [15] to reconstruct a quartic plane model of C that has the same Dixmier-Ohno invariants as Π_G.

2.4 Reconstructing over $\mathbb{Q}$

Given two curves X_1 and Y_2 over $\mathbb{Q}$ of genus 1 and genus 2 respectively, it will also be interesting to understand when we can actually use the above methods to construct a 2,2-glueing over $\mathbb{Q}$. As discussed in section 1.3 we can describe maximally isotropic subgroups of $X_1[2] \times Y_2[2]$ in the following way. We first write down equations

$$X_1 : y^2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)$$

$$Y_2 : y^2 = (x-\beta_1)(x-\beta_2)(x-\beta_3)(x-\beta_4)(x-\beta_5)(x-\beta_6)$$

and let $A = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ and $B = \{\beta_1, \dots, \beta_6\}$. Choosing a tuple (T, f), where T consists of two elements of B, and $f : B/T \to A$ is bijective is the same as giving an isotropic subgroup of $X_1[2] \times Y_2[2]$. If T and f are chosen in such a way that T is Galois-invariant and $f \circ \sigma = \sigma \circ f$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, then the induced maximally isotropic subgroup $G = (H_T, \phi_f)$ will be Galois-invariant, which is a necessary and sufficient condition for a glueing over $\mathbb{Q}$ to exist. Without loss of generality, we can assume that

$$G = \langle (0, [(\beta_5,0)-(\beta_6,0)]), ([(\alpha_1,0)-(\alpha_4,0)], [(\beta_1,0)-(\beta_4,0)]), ([(\alpha_2,0)-(\alpha_4,0)], [(\beta_2,0)-(\beta_4,0)]) \rangle$$

using Corollary 1.3.8.

Calculate the period matrices Π_1 and Π_2 for X_1 and Y_2 and choose $P_1 = (\alpha_4, 0), P_2 = (\beta_4, 0)$. Fixing these objects allows us to explicitly construct G. We first compute the Abel-Jacobi map,

$$\mathrm{AJ}_g(Q) = \left(\int_{P_g}^{Q} \omega_{g,1}, \dots \int_{P_g}^{Q} \omega_{g,g} \right) \mod \Lambda_g$$

where $\mathrm{AJ}_1 : X_1 \to \mathrm{Jac}(X_1)$ and $\mathrm{AJ}_2 : Y_2 \to \mathrm{Jac}(Y_2)$ explicitly using the methods in [13]. If we consider the elements of the Jacobians as divisor classes, this map will correspond to $\mathrm{AJ}_g(Q) = [Q - P_g]$.

We can now use AJ_1 to explicitly calculate $A_i = \mathrm{AJ}_1([(\alpha_i, 0) - (\alpha_4, 0)])$ with $i = 1, 2, 3, 4$ in $\mathrm{Jac}(X_1)$ and we can use AJ_2 to explicitly calculate the image of the points $B_i = \mathrm{AJ}_2((\beta_i, 0) - (\beta_4, 0))$ with $i = 1, 2, 3, 4$ and $T = \mathrm{AJ}_2((\beta_5, 0) - (\beta_6, 0))$. Then the points (A_i, B_i) and $(0, T)$ lie in $\mathrm{Jac}(X_1) \times \mathrm{Jac}(Y_2)[2]$ and generate G.

Now that we know everything explicitly, we can proceed as in Section 2.3 to find a period matrix Π_G and a principal polarization E_G that correspond to glueing along G. But the algorithms used to reconstruct the curve will not necessarily be give us an equation with coefficients in $\mathbb{Q}$. We will use the following proposition to construct a curve with coefficients over $\mathbb{Q}$.

Proposition 2.4.1. *Let*

$$T = \begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{bmatrix}$$

be an invertible matrix. Let $\phi_T : \mathbb{P}^2_k \to \mathbb{P}^2_k$ be the induced isomorphism given by

$$\phi_T(x : y : z) = (a_1 x + a_2 y + a_3 z : b_1 x + b_2 y + b_3 z : c_1 x + c_2 y + c_3 z).$$

Let C be a quartic curve of genus 3 in $\mathbb{P}^2_k$ given by the equation $F_C(x : y : z) = 0$ and let D be another quartic genus 3 curve given by the equation $F_D = F_C \circ \phi(x : y : z) = 0$ in $\mathbb{P}^2_k$. Let

$$\omega_{C,1} = \frac{x dx}{dF_C/dy}, \omega_{C,2} = \frac{y dx}{dF_C/dy}, \omega_{C,3} = \frac{z dx}{dF_C/dy}$$

be a basis of differentials for C and let Π_C be the period matrix of C calculated with respect to this basis. Let

$$\omega_{D,1} = \frac{x dx}{dF_D/dy}, \omega_{D,2} = \frac{y dx}{dF_D/dy}, \omega_{D,3} = \frac{z dx}{dF_D/dy}$$

be a basis of differentials for D and let Π_D be the period matrix of D calculated with respect to this basis. Then there exists a non-zero constant $e \in k$ such that

$$\Pi_D = (eT)^{-1} \Pi_C.$$

Proof. The differentials $\omega_{D,i}$ form a basis for the global sections of the canonical sheaf $H^0(\Omega_D)$ and the corresponding canonical embedding $D \to \mathbb{P}^2_k$ given by $P \mapsto (x(P) : y(P) : z(P))$ is simply the inclusion of $D \to \mathbb{P}^2_k$. Now ϕ_T maps D isomorphically to C as $0 = F_D(P) = F_C \circ \phi_T(P)$ and as T is an invertible matrix. The differentials $\phi^*(\omega_{C,i})$ form a basis for $H^0(\Omega_D)$. So ϕ^* needs to be an invertible linear map, and we find that

$$\begin{aligned} \phi^*(\omega_{C,1}) &= \alpha_1 \omega_{D,1} + \alpha_2 \omega_{D,2} + \alpha_3 \omega_{D,3}, \\ \phi^*(\omega_{C,2}) &= \beta_1 \omega_{D,1} + \beta_2 \omega_{D,2} + \beta_3 \omega_{D,3}, \\ \phi^*(\omega_{C,3}) &= \gamma_1 \omega_{D,1} + \gamma_2 \omega_{D,2} + \gamma_3 \omega_{D,3} \end{aligned}$$

for certain $\alpha_i, \beta_i, \gamma_i$. Now note that

$$\phi^*\left(\frac{\omega_{C,2}}{\omega_{C,3}}\right) = \phi^*(y/z) = \frac{b_1x + b_2y + b_3z}{c_1x + c_2y + c_3z}.$$

This means that

$$\phi^*(\omega_{C,2}) = \frac{b_1x + b_2y + b_3z}{c_1x + c_2y + c_3z}\phi^*(\omega_{C,3}).$$

As $\phi^*(\omega_{C,2})$ does not have poles, it follows that $\gamma_i = ec_i$ for $i = 1,2,3$ and for some constant e. We can also immediately conclude that $\beta_i = eb_i$ for $i = 1,2,3$. Using furthermore, that

$$\phi^*(\omega_{C,1}) = \frac{a_1x + a_2y + a_3z}{c_1x + c_2y + c_3z}\phi^*(\omega_{C,3}),$$

we can conclude that we also have $\alpha_i = ea_i$ for $i = 1,2,3$ and the same constant e. This implies then, that if we take the $\omega_{C,i}$ as a basis on Ω_C and the $\omega_{D,i}$ as a basis on Ω_D, the linear map $\phi^* : H^0(\Omega_C) \to H^0(\Omega_D)$ is represented by the matrix eT^t with respect to these bases. So the dual map $H^0(\Omega_D)^\vee \to H^0(\Omega_C)^\vee$ is represented by the matrix $(eT^t)^t$ with respect to the natural dual bases. This tells us that $(eT)\Pi_D = \Pi_C$ and shows that the curve D with the equation $F \circ \phi$ and the basis of differentials $\omega_{D,i}$ has period matrix $\Pi_D = (eT)^{-1}\Pi_C$. □

Corollary 2.4.2. *Let X_1 and Y_2 be two curves over $\mathbb{Q}$ of genus 1 and genus 2 respectively, and let K be a numberfield. Let G be a maximally isotropic subgroup of $\mathrm{Jac}(X_1) \times \mathrm{Jac}(X_2)$ that is Galois-invariant. Let Π_G be a period matrix that corresponds to the glueing along G. Assume that $\mathrm{Jac}(X_1) \times \mathrm{Jac}(X_2)/G$ is a Jacobian over $\mathbb{Q}$. Now let C be a quartic curve of genus 3 in $\mathbb{P}^2_K$ given by the equation $F_C(x:y:z) = 0$ (where F_C is not necessarily over $\mathbb{Q}$). Assume that there exists a matrix T such that $\Pi_G = T^{-1}\Pi_C$ where Π_C is the period matrix of C with respect to the basis of differentials*

$$\omega_{C,1} = \frac{xdx}{dF_C/dy}, \omega_{C,2} = \frac{ydx}{dF_C/dy}, \omega_{C,3} = \frac{zdx}{dF_C/dy}.$$

Write

$$T = \begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{bmatrix}.$$

Let $\phi_T : \mathbb{P}^2_K \to \mathbb{P}^2_K$ be the induced isomorphism given by

$$\phi_T(x:y:z) = (a_1x + a_2y + a_3z : b_1x + b_2y + b_3z : c_1x + c_2y + c_3z).$$

Then there exists a non-zero constant $e \in k$ such that the polynomial $eF \circ \phi_T$ is rational and such that the curve D defined by $eF \circ \phi_T = 0$ in $\mathbb{P}^2_K$ has period matrix Π_G (up to a scalar?).

Remark 2.4.3. In general $\mathrm{Jac}(X_1) \times \mathrm{Jac}(Y_2)/G$ might not always be a Jacobian as in Corollary 2.4.2. But using the above method, we will always be able to find a rational quartic curve C' in $\mathbb{P}^3_k$ such that $\mathrm{Jac}(C')$ is isomorphic to a quadratic twist of the glueing $\mathrm{Jac}(X_1) \times \mathrm{Jac}(Y_2)/G$.

Chapter 3

Fixing a factor

3.1 Characterizing 2,2-glued hyperelliptic genus 3 curves

In this section we will try to characterize the hyperelliptic curves of genus 3 that are 2,2-glueings. We will need the following proposition from [14].

Proposition 3.1.1. *Let $C : y^2 = f(x)$ and $C' : y^2 = f'(x)$ be two hyperelliptic curves of genus g over a field k. Every isomorphism $\phi : C \to C'$ is given by an expression of the form*

$$(x,y) \mapsto \left(\frac{ax+b}{cx+d}, \frac{ey}{(cx+d)^{g+1}} \right),$$

for some $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(k)$ and $e \in k^*$. The pair (M,e) is unique up to replacement by $(\lambda M, \lambda^{g+1} e)$ for $\lambda \in k^*$. The composition of isomorphisms (M,e) and (M',e') is $(M'M, e'e)$.

Proposition 3.1.2. *Let p be a prime and let (ϕ, Z, θ_Z) be a curve of genus g that is the (p,p)-glueing of two curves X and Y. Let $(\mathrm{Jac}(X), \theta_X)$ and $(\mathrm{Jac}(Y), \theta_Y)$ be the corresponding principally polarized abelian varieties. Let $\phi^t : Z^t \to X^t \times Y^t$ be the dual morphism with respect to the polarization θ_Z on Z and $p\theta_X \times Y + pX \times \theta_Y$. Then $\phi^t \circ \phi = [n]_{X \times Y}$.*

Proof. For this proof we will assume our base field is $\mathbb{C}$. A similar argument can be made for a more general base field using Tate modules.

Let $E_{X\times Y}$ be the alternating bilinear form corresponding to the algebraic equivalence class of $P_{X\times Y} = \theta_X \times Y + X \times \theta_Y$ and let E_Z be the alternating bilinear form corresponding to the algebraic equivalence class of θ_Z. As ϕ is a (p,p)-glueing, $\ker\phi$ is a subgroup of order p^g of $\mathrm{Jac}(X)[p] \times \mathrm{Jac}(Y)[p]$ that is maximally isotropic with respect to the pairing induced by $E_{X\times Y}$ (See Lemma

). Now choose a basis $e_1,\dots,e_{2g}$ for $H_1(\mathrm{Jac}(X)\times\mathrm{Jac}(Y),\mathbb{Z})$ such that the matrix representation $M_{E_{X\times Y}}$ of $E_{X\times Y}$ is

$$M_{E_{X\times Y}} = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}.$$

and $\ker\phi = \langle \frac{1}{p}e_1,\dots,\frac{1}{p}e_g, e_{g+1},\dots e_{2g}\rangle$. Such a basis exists because the kernel of ϕ is isotropic with respect to the Weil pairing. If we now choose $e_1,\dots,e_{2g}$ as the basis for $H_1(\mathrm{Jac}(Z),\mathbb{Z})$, the matrix representation M_ϕ of ϕ with respect to the bases chosen above will be

$$M_\phi = \begin{pmatrix} p\cdot I_g & 0 \\ 0 & I_g \end{pmatrix}.$$

By the glueing construction, we have that $\phi^*(\theta_Z) = p(\theta_X\times Y) + p(X\times\theta_Y)$. Let θ_Z correspond to the line bundle $L(H,\alpha)$. As we saw before, $\phi^*(\theta_Z)$ is given by $L(H(M_\phi\cdot, M_\phi\cdot), \alpha\circ M_\phi)$. In terms of matrices, this translates to:

$$M_\phi^t M_{E_Z} M_\phi = pM_{E_{X\times Y}}.$$

As M_{E_Z} should correspond to an alternating bilinear form corresponding to a principal polarization, it necessarily follows that

$$M_{E_Z} = \begin{bmatrix} 0 & I_g \\ -I_g & 0 \end{bmatrix}$$

with respect to the basis chosen on $H_1(\mathrm{Jac}(Z),\mathbb{Z})$. In [11] II.9 we find that the isogeny induced by the the polarization, $\phi_{P_{X\times Y}}$, is given by $x\mapsto L(0,e^{2\pi i E_{X\times Y}(x,u)})$. So, fixing bases on the homology of the dual abelian varieties, we can choose to represent the polarizations $\mathrm{Jac}(X)\times\mathrm{Jac}(Y)\to(\mathrm{Jac}(X)\times\mathrm{Jac}(Y))^t$ and $\mathrm{Jac}(Z)\to\mathrm{Jac}(Z)^t$ as the matrices $M_E X\times Y$ and M_{E_Z} respectively. We are now ready to compute $\phi^t\circ\phi$. We have the following chain of maps:

$$\mathrm{Jac}(X)\times\mathrm{Jac}(Y) \xrightarrow{\phi} \mathrm{Jac}(Z) \longrightarrow \mathrm{Jac}(Z)^t \xrightarrow{\phi^t} (\mathrm{Jac}(X)\times\mathrm{Jac}(Y))^t \longrightarrow \mathrm{Jac}(X)\times\mathrm{Jac}(Y).$$

By Lemma 2.1.21 this composes as

$$M_{E_{X\times Y}}^t (M_\phi)^t M_{E_Z} M_\phi = \begin{bmatrix} 0 & -I_g \\ I_g & 0 \end{bmatrix}\begin{bmatrix} pI_g & 0 \\ 0 & I_g \end{bmatrix}\begin{bmatrix} 0 & I_g \\ -I_g & 0 \end{bmatrix}\begin{bmatrix} pI_g & 0 \\ 0 & I_g \end{bmatrix} = \begin{bmatrix} pI_g & 0 \\ 0 & pI_g \end{bmatrix},$$

which is what we wanted to show. □

Proposition 3.1.3. *Let $(\phi, Z_g, \theta_{Z_g})$ be a (2,2)-glueing of a genus 1 curve X_1 and a genus $g-1$ curve Y_{g-1}. Then there exists a degree 2 morphism $\pi_1: Z_g\to X_1$.*

Proof. Let $i : Z_g \to \mathrm{Jac}(Z_g)$ be the Abel-Jacobi map and let $\mathrm{pr}_1 : \mathrm{Jac}(X_1) \times \mathrm{Jac}(Y_{g-1}) \to \mathrm{Jac}(X_1)$ be the projection to the first component. Now the map $\pi_1 = \mathrm{pr}_1 \circ \phi^t \circ i$ gives us a morphism of curves $\pi_1 : Z_g \to X_1$. This map cannot be constant as it would contradict the fact that ϕ is an isogeny, and as π_1 maps to a connected abelian variety, it needs to be surjective. We will now determine the degree of π_1. We first remark that $\pi_{1,*} = (\mathrm{pr}_1 \circ \phi \circ i_*)$. Indeed, let $D = \sum P_i - Q_i$ be a divisor on Z_g. Now

$$\pi_*(D) = \sum \mathrm{pr}_1 \circ \phi \circ i(P_i) - \mathrm{pr}_1 \circ \phi \circ i(Q_i) = \sum \mathrm{pr}_1 \circ \phi \circ i_*(D)$$

as i_* is the linear extension of i.

Note that

$$\begin{aligned}
\pi_{1,*} \circ \pi_1^* &= (\mathrm{pr}_1 \circ \phi \circ i_*)(\mathrm{pr}_1 \circ \phi \circ i)^* \\
&= \mathrm{pr}_1 \circ \phi \circ i_* \circ i^* \circ \phi^t \circ \mathrm{pr}_1^t \\
&= \mathrm{pr}_1 \circ \phi \circ \phi^t \circ \pi_1^t \\
&= \mathrm{pr}_1 \circ [2]_{\mathrm{Jac}(Z_g)^t} \circ \mathrm{pr}_1^t \\
&= [2]_{\mathrm{Jac}(X_1)^t} \mathrm{pr}_1 \circ \mathrm{pr}_1^t = [2]_{\mathrm{Jac}(X_1)^t}.
\end{aligned}$$

In the third equality, we use that $i_* \circ i^* = \mathrm{Id}$ on $i(Z_3) \cap \mathrm{Jac}(Z_3)$. Because $i_* \circ i^*$ is a linear map, and $\mathrm{Jac}(Z_3)$ is generated by linear combinations of elements of $i(Z_3) \cap \mathrm{Jac}(Z_3)$, we conclude that $i_* \circ i^* = \mathrm{Id}_{\mathrm{Jac}(Z_3)}$. In the fourth equality, we used Proposition 3.1.2.

To see that $\mathrm{pr}_1 \circ \mathrm{pr}_1^t = \mathrm{Id}_{\mathrm{Jac}(X_1)}$ we consider p_1 as the map $\mathrm{id} \times 0$ from $\mathrm{Jac}(X_1) \times \mathrm{Jac}(Y_{g-1}) \to \mathrm{Jac}(X_1) \times \mathrm{Jac}(Y_{g-1})$ and p_2 as the map $0 \times \mathrm{id}$ from $\mathrm{Jac}(X_1) \times \mathrm{Jac}(Y_{g-1}) \to \mathrm{Jac}(X_1) \times \mathrm{Jac}(Y_{g-1})$. Then

$$\begin{aligned}
\mathrm{Id}_{\mathrm{Jac}(X_1) \times \mathrm{Jac}(Y_{g-1})} &= (p_1 + p_2) \circ (p_1^t + p_2^t) \\
&= p_1 p_1^t + p_1 p_2^t + p_2 p_1^t + p_2 p_2^t \\
&= p_1 p_1^t + p_2 p_2^t.
\end{aligned}$$

So $p_1 p_1^t = \mathrm{id} \times 0$ on $(\mathrm{Jac}(X_1) \times \mathrm{Jac}(X_2))^t$. As we have $(\mathrm{Jac}(X_1) \times \mathrm{Jac}(Y_{g-1}))^t \cong \mathrm{Jac}(X_1)^t \times \mathrm{Jac}(Y_{g-1})^t$, we can restrict to line bundles of the form $(L, \mathcal{O}_{\mathrm{Jac}(Y_{g-1})})$ which can be identified with line bundles on $\mathrm{Jac}(X_1)$ to see that $(\mathrm{pr}_1)^t = (p_1)^t|_{\mathrm{Jac}(X_1)^t \times \{0\}}$ when we identify $\mathrm{Jac}(X_1)^t \times \{0\}$ with $\mathrm{Jac}(X_1)^t$.

We conclude that $\pi_{1,*} \circ \pi_1^* = [2]_{\mathrm{Jac}(X_1)^t}$, so $\pi_1 : Z_3 \to X_1$ is a map of degree 2, which is what we wanted to show.

□

Proposition 3.1.4. *Let Z_3 be a curve of genus 3 and assume that Z_3 is a (2,2)-glueing of a genus 1 curve X_1 and a genus 2 curve Y_2. Assume there exists a degree 2 morphism $\pi_2 : Z_3 \to Y_2$. Then Z_3 is a hyperelliptic curve.*

Proof. By Proposition 3.1.3 we also have a degree 2 morphism $\pi_1 : Z_3 \to X_1$. Both π_1 and π_2 correspond to degree 2 automorphisms of the curve Z_3. Let us denote them by i_1 and i_2 respectively. These two morphisms induce automorphisms i_1^*, i_2^* of degree 2 on the Jacobian of Z_3. As i_1 fixes the divisor classes pulled back from X_1 and i_2 fixes the divisors classes pulled back from Y_2 by construction, i_1^* and i_2^* will be represented by the matrices

$$M_{i_1^*} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \quad M_{i_2^*} = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

in $\mathrm{End}_k^0(\mathrm{Jac}(Z_3)) \cong \mathrm{End}_k^0(\mathrm{Jac}(X_1)) \times \mathrm{End}_k^0(\mathrm{Jac}(X_2))$ after making a certain choice of basis. Now the morphism $i_0 = i_1 \circ i_2$ will also induce a morphism of degree 2 $\pi_0 : Z_3 \to Z_3/\langle i_0 \rangle$ with

$$M_{i_0^*} = M_{i_2^*} M_{i_1^*} = \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

So i_0 does not fix any divisor class on Z_3. As $\mathrm{Jac}(Z_3/\langle i_0 \rangle) = \mathrm{Jac}(Z_3)/(i^*) = \{*\}$, we conclude that $Z_3/\langle i_0 \rangle$ is a curve of genus 0. So π_0 is a degree 2 morphism from Z_3 to $\mathbb{P}_k^1$ and is therefore a hyperelliptic curve.

□

$$i_1(x,y) = \left(\frac{ax+b}{cx+d}, \frac{ey}{(cx+d)^{g+1}} \right),$$

Proposition 3.1.5. *Let Z_g be a nonsingular hyperelliptic curve of genus g over an algebraically closed field k, that comes equipped with an involution that is not the hyperelliptic involution. Let $g_1 = \lfloor \frac{g}{2} \rfloor$ and $g_2 = g - g_1$. Then there exist curves X_{g_1} and Y_{g_2} of genus g_1 and genus g_2 respectively and degree 2 maps $\pi_1 : Z_g \to X_{g_1}$, $\pi_2 : Z_g \to X_{g_2}$. After an appropriate choice of isomorphisms, we have the following equations for Z_g, X_{g_1} and Y_{g_2}*

$$\begin{aligned} Z_g : \quad & y^2 = \prod_{i=1}^{g+1} (x^2 - \alpha_i), \\ X_{g_1} : \quad & v^2 = \prod_{i=1}^{g+1} (u - \alpha_i), \\ Y_{g_2} : \quad & s^2 = t \prod_{i=1}^{g+1} (t - \alpha_i) \end{aligned}$$

and the degree 2 maps are given by

$$\pi_{g_1} : Z_g \to X_{g_1}, \quad \pi_1(x,y) \mapsto (x^2, y)$$
$$\pi_{g_2} : Z_g \to Y_{g_2}, \quad \pi_2(x,y) \mapsto (x^2, y/x^2).$$

Proof. Let us embed Z_g into $\mathbb{A}_k^2$ with some equation $y^2 = f(x)$ for some f of degree $2g+2$ and let i_0 be the hyperelliptic involution corresponding to $(x,y) \mapsto (x,-y)$. By assumption Z_g comes equipped with a second involution $j : Z_g \to Z_g$ which is not the hyperelliptic involution. According to Proposition 3.1.1 we are able to write

$$i_1(x,y) = \left(\frac{ax+b}{cx+d}, \frac{ey}{(cx+d)^{g+1}}\right),$$

for some $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(k)$ and $e \in k^*$. As i_1 is an involution, we find that i_1^2 corresponds to the tuple $(\lambda I, \lambda^{g+1})$ for some $\lambda \in k^*$. After rescaling if necessary, we can assume $i^2 = (I, 1)$. Now choose a matrix S that diagonalizes M. W.l.o.g, we can assume that

$$SMS^{-1} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}.$$

as SMS^{-1} is not the identity map. We also get that $e \pm 1$ and by multiplying with i_0 if necessary, we can assume $e = 1$. In the new choice of coordinates given by multiplying with S and rescaling, we can write down a new equation F for the curve Z_g for which the three involutions are given by the following maps:

$$i_0(x,y) \mapsto (x,-y)$$
$$i_1(x,y) \mapsto (-x,y)$$
$$i_2 = i_0 \circ i_1(x,y) \mapsto (-x,-y).$$

As F needs to remain invariant (up to a scalar) under these involutions, it needs to be formed by monomials that lie in the same eigenspace for the maps i_0 and i_1. By assumption $F \in \langle 1, y^2, x, x^2, \ldots, x^{2g+2} \rangle$. The map i_1 divides this set into two distinct spaces $E_1 = \langle y^2, 1, x^2, x^4, \ldots, x^{2g+2} \rangle$ and $E_{-1} = \langle x, x^3, \ldots, x^7 \rangle$. As the latter does not contain the y-variable, any equation in it will give us a variety of dimension 0. So, F needs to be of the form $y^2 = \prod_{i=1}^{g+1}(x^2 - \alpha_i)$ for some $\alpha_i \in k$.

Let $X_{g_1} = Z_g / < i_1 >$. The function field $K(X_{g_1})$ will contain all polynomials in $K(Z_g)$ that remain fixed under i_1, and the quotient map $\pi_1 : Z_g \to X_{g_1}$ will induce a natural inclusion of function fields $\pi_1^* : K(X_{g_1}) \to K(Z_g)$. As $u = x^2$ and $v = y$ are both invariant under i_1, we have that

$$L_1 = k(u,v)/(v^2 - \prod_{i=1}^{g+1}(u - \alpha_i)) \subset K(X_{g_1}).$$

In fact, we claim that $K(X_{g_1}) = F$, and that π_1^* is given by $u \mapsto x^2, v \mapsto y$. Indeed, $v^2 - \prod_{i=1}^{g+1}(u-\alpha_i)$ is irreducible because $y^2 = \prod_{i=1}^{g+1}(x^2-\alpha_i)$ was and $u \mapsto x^2, v \mapsto y$ is a well-defined inclusion of function fields $L_1 \to K(Z_g)$ of degree 2. As $[K(Z_g) : K(X_{g_1})] = 2$ and $L_1 \subset K(X_{g_1})$, it follows that that $K(X_{g_1}) = L_1$. The curve X_{g_1} will then be given by the equation

$$v^2 = \prod_{i=1}^{g+1}(u - \alpha_i)$$

and π_1 is given by $\pi_1(x,y) \mapsto (u,v)$. As the equation contains $g+1$ roots and is hyperelliptic, the curve will have genus $(g-1)/2$ if g is odd and genus $g/2$ if g is even. So $g_1 = \lfloor \frac{g}{2} \rfloor$. Now because Z_g is non-singular, the α_i have to be distinct and non-zero. This implies that X_{g_1} is also non-singular.

Let $Y_{g_2} = Z_3/ < i_2 >$. Similarly, $K(Y_{g_2})$ needs to contain the monomials xy and x^2 which remain invariant under i_2. Setting $t = x^2, s = xy$, we find that

$$L_2 = k(s,t)/\left(s^2 - t\prod_{i=1}^{g+1}(t-\alpha_i)\right) \subset K(Y_2)$$

The natural inclusion $L_2 \to K(Z_g)$ given by $t \mapsto x^2, s \mapsto xy$ is once again a field extension of degree 2, which implies that $K(Y_{g_2}) = L_2$. So, Y_{g_2} is given by the equation

$$s^2 = t\prod_{i=1}^{g+1}(t-\alpha_i)$$

which is also non-singular. To see this, remark that besides being distint, the α_i are also non-zero as one of them being zero would imply that Z_g is singular. Now the map π_2 is given by $(x,y) \mapsto (x^2, xy)$. As the equation contains $g+2$ roots and is hyperelliptic, the curve will have genus $(g+1)/2$ if g is odd and genus $g/2$ if g is even. So $g_2 = g - g_1$, which completes the proof. $\square$

We are now going to show that Z_g is a (2,2)-glueing of the two other curves.

Proposition 3.1.6. *The curve Z_g in Proposition 3.1.5 is a (2,2)-glueing of the curves X_{g_1} and Y_{g_2} defined in the same proposition.*

Proof. Let $\langle du/v, udu/v, \ldots u^{g_1-1}du/v\rangle$ be a basis for the differential forms on X_{g_1} and let $\langle dt/s, tdt/s, \ldots t^{g_2-1}dt/s\rangle$ be a basis for the differential forms on Y_{g_2}. Now

$$\pi_1^*(u^k du/v) = x^{2k}dx^2/y = x^{2k}dx/y,$$
$$\pi_2^*(t^k dt/s) = x^{2k}dx^2/y = x^{2k}dx/xy = x^{2k-1}dx/y.$$

This implies that the map $\phi = \pi_1^* \times \pi_2^* : \mathrm{Jac}(X_{g_1}) \times \mathrm{Jac}(Y_{g_2}) \to \mathrm{Jac}(Z_g)$ is surjective, and therefore an isogeny. We want to show that ϕ is a (2,2)-glueing. First remark, that because both π_1 and π_2 are of degree 2, $\phi^t \circ \phi = [2]_{\mathrm{Jac}(X_{g_1}) \times \mathrm{Jac}(Y_{g_2})}$. This means that $\ker \phi \subset \mathrm{Jac}(X_{g_1})[2] \times \mathrm{Jac}(Y_{g_2})[2]$. We can use Lemma 1.3.1 to determine the kernel exactly.

Let

- $P_i = (\alpha_i, 0) + (\alpha_{g+1}, 0)$ be a divisor on X_{g_1},
- $Q_0 = (0,0) + \infty$ and $Q_i = (\alpha_i, 0) + (\alpha_{g+1}, 0)$ be divisors on Y_{g_2},
- $R_i = (\sqrt{\alpha_i}, 0) + (-\sqrt{\alpha_i}, 0) + (\sqrt{\alpha_{g+1}}, 0) + (-\sqrt{\alpha_{g+1}}, 0)$ a divisor on Z_g.

Then $\pi_1^*(P_i) = R_i$ and $\pi_2^*(Q_i) = R_i$. As a consequence, the points (P_i, Q_i) in $\mathrm{Jac}(X_{g_1}) \times \mathrm{Jac}(Y_{g_2})$ will be contained in $\ker \phi$. Furthermore, $Q_0 = \sum_{i=1}^{g+1} Q_i$, so $\pi_2^*(Q_0) = \sum_{i=1}^{g+1} R_i = 0$. As a result, $(0, Q_0)$ is also contained in the kernel of ϕ. We claim that $\ker(\phi) = \langle (P_i, Q_i), (0, Q_0) \rangle$. Assume that $\phi^*(\sum_{i \in I} P_i, \sum_{j \in J} Q_j) = 0$ for some index sets I and J. Then $\phi^*(\sum_{i \in I} P_i + \sum_{j \in J} P_j, 0) = 0$ (where $P_0 = 0$). If $\sum_{i \in I} P_i, \sum_{j \in J} Q_j$ is not an element of $\langle (P_i, Q_i), (0, Q_0) \rangle$, then J/I contains non-zero elements. Therefore, there exists some $0 \neq P \in \mathrm{Jac}(X_{g_1})[2]$ such that $\pi_1^*(P) = 0$. But $\pi_1^*(\sum_{i \in I} P_i) = \sum_{i \in I} R_i$ and $\sum_{i \in I} R_i = 0$ if and only if $I = \emptyset$ or $I = \{1, 2, \ldots, g+1\}$. Now $\langle (P_i, Q_i) \rangle$ has $g+1$ generators, but they are not linearly independent. Using the relations in Lemma 1.3.1, we can show that $\ker \phi = \langle (P_1, Q_1), \ldots (P_g, Q_g), (0, Q_0) \rangle \cong (\mathbb{Z}/2\mathbb{Z})^g$. So the degree of ϕ is 2^g.

Let $\mathcal{P}_{Z_g}$ be the polarization on $\mathrm{Jac}(Z_g)$. Then $\phi^t \mathcal{P}_{\mathcal{Z}_\rceil} \phi$ is a polarization on $\mathrm{Jac}(X_{g_1}) \times \mathrm{Jac}(X_{g_2})$ of degree $\deg(\phi)^2 = 2^{2g}$. Let $\mathcal{P}_{X_{g_1}}$ be the polarization on $\mathrm{Jac}(X_{g_1})$ and $\mathcal{P}_{Y_{g_2}}$ be the polarization on $\mathrm{Jac}(Y_{g_2})$. As the π_i induce morphisms of polarized abelian varieties, it follows that ϕ is a morphism of polarized abelian varieties. So, $\phi^t \mathcal{P}_{\mathcal{Z}_\rceil} \phi = m\mathcal{P}_{X_{g_1}} + n\mathcal{P}_{Y_{g_2}}$ for some m and n. The degree of $m(\mathcal{P}_{X_{g_1}}, n\mathcal{P}_{Y_{g_2}})$ is equal to $m^{2g_1} n^{2g_2}$. This can only be equal to 2^{2g} if $m = n = 2$. So $\phi^* \mathcal{P}_{\mathcal{Z}_\rceil} = 2(\mathcal{P}_{X_{g_1}}, \mathcal{P}_{Y_{g_2}})$ and ϕ induces a (2,2)-glueing, which is what we wanted to show.

□

Remark 3.1.7. The structure of the kernel in Proposition 3.1.6 is similar to the one described in Theorem 1.3.16.

Corollary 3.1.8. *Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be distinct and non-zero. Let $H_3(t)$ be the genus 3 curve given by the equation*

$$F_3(t)(x,y) = y^2 - (x^2 - \alpha_1 + t)(x^2 - \alpha_2 + t)(x^2 - \alpha_3 + t)(x^2 - \alpha_4 + t).$$

Then $t \mapsto H_3(t)$ is a non-constant family of hyperelliptic genus 3 curves for which H_3 is generaically the (2,2)-glueing of $X_1 : y^2 = (x^2 - \alpha_1, \alpha_2, \alpha_3, \alpha_4)$ and some genus 2 curve.

Proof. Let $H_1(t)$ be the genus 1 curve given by the equation

$$y^2 = (x - \alpha_1 + t)(x - \alpha_2 + t)(x - \alpha_3 + t)(x - \alpha_4 + t).$$

In Proposition 3.1.5, we showed that we always have a degree 2 map $\pi_1 : H_3(t) \to H_1(t)$. Now note that $H_1(0)$ is isomorphic to $H_1(t)$ by the isomorphism $(x, y) \mapsto (x + t, y)$. So we can assume that we always have a degree 2 map $\widetilde{\pi}_1 : H_3(t) \to H_1(0)$. According to Proposition 3.1.6 the curve $H_3(t)$ is a (2,2)-glueing of $H_1(0)$ and some genus 2 curve. It remains to be shown that $t \mapsto H_3(t)$ is a non-constant family. Now choosing an automorphism of $\mathbb{P}^1_k$ such that $\sqrt{\alpha_1 + t}$ get mapped to 1, $\sqrt{\alpha_2 + t}$ gets mapped to 0, and $-\sqrt{\alpha_1 + t}$ gets mapped to ∞ we get the Rosenhain invariants:

$$\lambda_1 = \frac{2\sqrt{\alpha_1+t}\sqrt{\alpha_2+t} - 2\sqrt{\alpha_1+t}\sqrt{\alpha_2+t}}{-\sqrt{\alpha_1+t}^2 + \sqrt{\alpha_1+t}\sqrt{\alpha_2+t} - \sqrt{\alpha_1+t}\sqrt{\alpha_2+t} + \sqrt{\alpha_2+t}\sqrt{\alpha_2+t}},$$
$$\lambda_2 = \frac{2\sqrt{\alpha_1+t}\sqrt{\alpha_2+t} - 2\sqrt{\alpha_1+t}\sqrt{\alpha_3+t}}{-\sqrt{\alpha_1+t}^2 + \sqrt{\alpha_1+t}\sqrt{\alpha_2+t} - \sqrt{\alpha_1+t}\sqrt{\alpha_3+t} + \sqrt{\alpha_2+t}\sqrt{\alpha_3+t}},$$
$$\lambda_3 = \frac{-4\sqrt{\alpha_1+t}\sqrt{\alpha_2+t}}{\alpha_1 + t - 2\sqrt{\alpha_1+t}\sqrt{\alpha_2+t} + \alpha_2 + t},$$
$$\lambda_4 = \frac{-2\sqrt{\alpha_1+t}\sqrt{\alpha_2+t} - 2\sqrt{\alpha_1+t}\sqrt{\alpha_2+t}}{\alpha_1 + t - \sqrt{\alpha_1+t}\sqrt{\alpha_2+t} - \sqrt{\alpha_1+t}\sqrt{\alpha_2+t} + \sqrt{\alpha_2+t}\sqrt{\alpha_2+t}},$$
$$\lambda_5 = \frac{-2\sqrt{\alpha_1+t}\sqrt{\alpha_2+t} - 2\sqrt{\alpha_1+t}\sqrt{\alpha_3+t}}{\alpha_1 + t - \sqrt{\alpha_1+t}\sqrt{\alpha_2+t} - \sqrt{\alpha_1+t}\sqrt{\alpha_3+t} + \sqrt{\alpha_2+t}\sqrt{\alpha_3+t}}.$$

As the Rosenhain invariants are non-constant in t, there needs to exist at least one t for which $H_3(t)$ is a non-singular hyperelliptic curve that is not isomorphic to $H_3(0)$. Therefore $t \mapsto H_3(t)$ gives us a non-constant family of genus 3 curves with the property that all of them are a (2,2)-glueing of X_1 and some genus 2 curve.

□

Remark 3.1.9. There does not exist a family of hyperelliptic genus 3 curves that are the glueing of a fixed genus 2 curve Y_2 and some elliptic curve. To see this, remark that both the moduli space of curves of the form $y^2 - (x^2 - \alpha_1)(x^2 - \alpha_2)(x^2 - \alpha_3)(x^2 - \alpha_4)$ and the moduli space of genus 3 curves have dimension 3. This means that any map between them has to have finite fibers, so a continuous family cannot exist.

Corollary 3.1.10. *Let $(\phi, Z_g, \theta_{Z_g})$ be a (2,2)-glueing of a genus 1 curve X_1 and a principally polarized abelian variety of dimension g-1. If Z_g is hyperelliptic, then g has to be either 2 or 3.*

Proof. Assume Z_g is hyperelliptic. Then $g \geq 2$. Proposition 3.1.3 tells us that there exists a morphism $p : Z_g \to X_1$ of degree 2. So Z_g comes equipped with an involution that is not the hyperelliptic involution. Now Proposition 3.1.5 gives us an explicit description of all possible involutions on Z_g and the corresponding quotient morphisms of degree 2. As p needs to be one of these maps, either $\lfloor \frac{g}{2} \rfloor$ or $g - \lfloor \frac{g}{2} \rfloor$ needs to be equal to 1. This is only possible if $g \leq 3$. □

3.2 Fixing a genus 2 factor in the non-hyperelliptic genus 3 curve case

Let k be a field of characteristic $\neq 2, 3$ and let Y_2 be a curve over k of genus 2. In this section, we will (under mild assumptions) construct a non-hyperelliptic curve Z_3 of genus 3 over k such that Z_3 is a $(2,2)$–glueing of Y_2 and an elliptic curve. In fact we will find a non-constant infinite family of such curves. And as the Z_3 vary, the j-invariants of the genus 1 factor will also vary as there are only finitely many ways we can glue an elliptic curve to a genus 2 curve. We are going to use the following result by Ritzenthaler and Romagny [2, Theorem 1.1]:

Theorem 3.2.1. *Let Z_3 be a non-hyperelliptic curve of genus 3 over k given by the equation:*

$$Z_3 : y^4 - h(x,z)y^2 + f(x,z)g(x,z) = 0$$

in $\mathbb{P}^2$ where

$$f = f_2x^2 + f_1xz + f_2z^2, \qquad g = g_2x^2 + g_1xz + g_2z^2, \qquad h = h_2x^2 + h_1xz + h_0z^2$$

are homogeneous degree 2 polynomials. It defines a cover of the genus 1 curve

$$X_1 : y^2 - h(x,z)y + f(x,z)g(x,z)$$

in the weighted projective space $\mathbb{P}^{(1,2,1)}$. Let

$$A = \begin{bmatrix} f_2 & f_1 & f_0 \\ h_2 & h_1 & h_0 \\ g_2 & g_1 & g_0 \end{bmatrix}$$

and assume that A is invertible. Let

$$A^{-1} = \begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{bmatrix}.$$

Then $\mathrm{Jac}(Z_3)$ *is isogenous to* $\mathrm{Jac}(X_1) \times \mathrm{Jac}(Y_2)$ *where Y_2 is given by the equation $y^2 = b \cdot (b^2 - ac)$ in $\mathbb{P}^{(1,3,1)}$ where*

$$a = a_1 + 2a_2x + a_3x^2, \quad b = b_1 + 2b_2x + b_3x^2, \quad c = c_1 + 2c_2x + c_3x^2.$$

Proof. See [2, Theorem 1.1]. □

Given three quadratic polynomials

$$a = a_1 + 2a_2x + a_3x^2, \quad b = b_1 + 2b_2x + b_3x^2, \quad c = c_1 + 2c_2x + c_3x^2,$$

in $k[x]$, we can consider the curve $Y_2 : y^2 = b(b^2 - ac)$ in $\mathbb{P}^{(1,3,1)}$ and reverse the above construction to find a genus 3 curve Z_3 that is a glueing of Y_2 and an elliptic curve. We set

$$B = \begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{bmatrix}.$$

and under the assumption that B is invertible, we can write

$$B^{-1} = \begin{bmatrix} f_2 & f_1 & f_0 \\ h_2 & h_1 & h_0 \\ g_2 & g_1 & g_0 \end{bmatrix}.$$

Setting

$$f = f_2x^2 + f_1xz + f_0z^2, \quad g = g_2x^2 + g_1xz + g_0z^2, \quad h = h_2x^2 + h_1xz + h_0z^2,$$

we define Z_3 to be the non-hyperelliptic curve of genus 3 over k given by the equation:

$$Z_3 : y^4 - h(x,z)y^2 + f(x,z)g(x,z) = 0 \tag{3.1}$$

in $\mathbb{P}^2$.

By construction, Z_3 will be a glueing of Y_2 and the elliptic curve X_1 in $\mathbb{P}^{(1,2,1)}$ given by

$$X_1 : y^2 - h(x,z)y + f(x,z)g(x,z) = 0. \tag{3.2}$$

Theorem 3.2.2. *The curve Z_3 as constructed above is a $(2,2)$-glueing of Y_2 and X_1.*

Proof. TBD □

Definition 3.2.3. Let

$$a = a_1 + 2a_2x + a_3x^2, b = b_1 + 2b_2 + b_3x^2, c = c_1 + 2c_2 + c_3x^2 \in k[x]$$

be quadratic polynomials such that the matrix

$$B = \begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{bmatrix}$$

is invertible. We will call such a triple (a,b,c) a *regular quadratic triple*, and we will write $Y_2(a,b,c)$ for the genus 2 curve given by the equation $y^2 - b(b^2 - ac)$ and $F_2(a,b,c)$ for the equation. We will furthermore write $Z_3(a,b,c)$ for the genus 3 curve (3.1) ($F_3(a,b,c)$ for its equation) and $X_1(a,b,c)$ for the genus 1 curve (**??**) we constructed above. For convenience, we will also write $(f,g,h) = \mathrm{Inv}(a,b,c)$ for the polynomials we get by inverting the matrix.

Given a regular triple (a,b,c), we are interested in finding other regular triples (a_2,b_2,c_2) such that $Y_2(a,b,c)$ is isomorphic to $Y_2(a_2,b_2,c_2)$, but such that $Z_3(a,b,c)$ is not isomorphic to $Z_3(a_2,b_2,c_2)$, so we are going to consider operations on the triple (a,b,c) that fix the isomorphism class of $Y_2(a,b,c)$.

Lemma 3.2.4. *Let (a,b,c) be a regular triple and $\lambda \in k^*$. Then*

(i) $F_2(a,b,c) = F_2(\lambda a, b, \lambda^{-1} c)$ *and* $F_3(a,b,c) = F_3(\lambda a, b, \lambda^{-1} c)$.

(ii) $F_2(a,b,c) = F_2(c,b,a)$ *and* $F_3(a,b,c) = F_3(c,b,a)$.

(iii) $Y_2(a,b,c) \cong_{\bar{k}} Y_2(\lambda a, \lambda b, \lambda c)$ *and* $Z_3(a,b,c) \cong_{\bar{k}} Z_3(\lambda a, \lambda b, \lambda c)$.

Proof. For (i) we have $F_2(a,b,c) = F_2(\lambda a, b, \lambda^{-1} c)$ as $ac = \lambda a \lambda^{-1} c$. Now write

$$B = \begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{bmatrix}$$

and $(f,g,h) = \mathrm{Inv}(a,b,c)$. We see that

$$B(\lambda a, b, \lambda^{-1} c) = B \begin{bmatrix} \lambda & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \lambda^{-1} \end{bmatrix},$$

so

$$B(\lambda a, b, \lambda^{-1} c)^{-1} = \begin{bmatrix} \lambda^{-1} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \lambda \end{bmatrix} B^{-1}.$$

From this we can conclude that $(\lambda^{-1} f, g, h) = \mathrm{Inv}(\lambda a, b, \lambda^{-1})$ which shows that $F_3(a,b,c) = F_3(\lambda a, b, \lambda^{-1} c)$.

For (ii), we get $F_2(a,b,c) = F_2(c,b,a)$ for the same reason. We see that

$$B(c,b,a) = B \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix},$$

so

$$B(c,b,a)^{-1} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} B^{-1}.$$

which gives us that $(g,f,h) = \mathrm{Inv}(c,b,a)$, so $F_3(a,b,c) = F_3(c,b,a)$.

For (iii), we have that $F_2(a,b,c) = y^2 - b(b^2 - ac)$ and $F_2(\lambda a, \lambda b, \lambda c) = y^2 - \lambda^3 b(b^2 - ac)$. So the map $\phi : Y_2(a,b,c) \to Y_2(\lambda a, \lambda b, \lambda c)$ given by $(x,y) \mapsto x, \sqrt{\lambda^{-3}}y$ gives us an isomorphism over $\bar{k}$. For the genus 3 curve, we remark that:

$$B(\lambda a, \lambda b, \lambda c) = B \begin{bmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{bmatrix},$$

so

$$B(\lambda a, \lambda b, \lambda c)^{-1} = \begin{bmatrix} \lambda^{-1} & 0 & 0 \\ 0 & \lambda^{-1} & 0 \\ 0 & 0 & \lambda^{-1} \end{bmatrix} B^{-1}.$$

which gives us that $F_3(\lambda a, \lambda b, \lambda c) = y^4 - \lambda^{-1} h y^2 + \lambda^{-2} f g$. With $(f,g,h) = \mathrm{Inv}(a,b,c)$. Here the map $\phi : Z_3(a,b,c) \to Z_3(\lambda a, \lambda b, \lambda c)$ given by $(x,y,z) \mapsto x, \sqrt{\lambda} y, z)$ gives us an isomorphism over $\bar{k}$.

□

These operations change the triple (a,b,c) and fix the isomorphism class of $Y_2(a,b,c)$, but they do not change $Z_3(a,b,c)$, which is what we wanted. A more fruitful approach is the following:

Lemma 3.2.5. *Let $\Delta \in k$ and let $(a, b = x^2 - \Delta, c)$ be a regular quadratic triple. Write*

$$b^2 - ac = p_0 x^4 + p_1 x^3 + p_2 x^2 + p_3 x + p_4 = p.$$

Now let $t \in k$ and assume we have $a', c' \in k[x]$ such that $tb^2 - a'c' = p$. Then $Y_2(ta', tb, c')$ is isomorphic to $Y_2(a,b,c)$.

Proof. The curve $Y_2(ta', tb, c')$ is given by the equation

$$\begin{aligned} y^2 &= tb(t^2 b^2 - ta'c') \\ &= t^2 b(tb^2 - a'c') \\ &= t^2 bp, \end{aligned}$$

so we see that the map $(x,y) \mapsto (x, yt)$ sends $Y_2(ta', tb, c')$ isomorphically to $Y_2(a,b,c)$.

□

Remark 3.2.6. Lemma 3.2.4 tells us that $Y_2(a'/t, b', c')$ and $Y_2(a', b', c'/t)$ are also isomorphic to $Y_2(ta', tb', c)$ with $Z_3(a'/t, b', c')$ and $Z_3(a', b', c'/t)$ isomorphic to $Z_3(ta', tb', c)$.

Remark 3.2.7. Fixing t in Lemma 3.2.5 and searching for suitable triples is essentially the same as finding a different quadratic factorization of p. This comes down to a combination of rescaling and choosing two of the four roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ of p. One pair of roots will form one quadratic factor, the other pair the second. As the order of the two chosen roots does not matter, there are 3 distinct factorizations. We have seen above that scaling does not change the isomorphism class of Z_3, but as we will see in the following example, choosing two distinct quadratic factorizations, say

$$a = (x - \alpha_1)(x - \alpha_2), c = (x - \alpha_3)(x - \alpha_4)$$

and

$$a' = (x - \alpha_1)(x - \alpha_4), c'(x - \alpha_1)(x - \alpha_3)$$

will generally give us a curve $Z_3(ta', tb', c')$ that is not isomorphic to $Z_3(ta, tb, c)$.

Example 3.2.8. Fix $t = 1$ and let $a = (x-1)(x-2), b = x^2 - 5, c = (x-3)(x-4)$. We calculate that

$$B(a, b, c) = \begin{bmatrix} 1 & 1 & 1 \\ -3/2 & 0 & -7/2 \\ 2 & -5 & 12 \end{bmatrix},$$

so

$$B(a, b, c)^{-1} = \begin{bmatrix} -35/2 & -17 & -7/2 \\ 11 & 10 & 2 \\ 15/2 & 7 & 3/2 \end{bmatrix}$$

and we find $\mathrm{Inv}(a, b, c) = (f, g, h)$ where

$$f = -35/2x^2 - 17xz - 7/2z^2, \quad g = 15/2x^2 + 7xz + 3/2z^2, \quad h = 11x^2 + 10xz + 2z^2.$$

This gives us the curve $X_1(a, b, c)$ with equation

$$-525/4x^4 - 250x^3z - 343/2x^2z^2 - 50xz^3 - 21/4z^4 - 11x^2y - 10xyz - 2yz^2 + y^2.$$

If we make the change of coordinates $y' = y - 1/2h$, we find a different equation for the curve, namely $y'^2 = 1/4h^2 - f \cdot g$ where the right hand side is given by a binary quartic form. The binary quartic form is given by:

$$1/4h^2 - f \cdot g = 323/2x^4 + 305x^3z + 415/2x^2z^2 + 60xz^3 + 25/4z^4,$$

which has binary quartic invariants

$$I = 1075/4, \quad J = -8800.$$

Using these, we calculate that the j-invariant of $X_1(a,b,c)$ is 127211200/193.

We now set $a' = (x-1)(x-3), b = x^2-5, c' = (x-2)(x-4)$. In this case, we find

$$B(a',b',c') = \begin{bmatrix} 1 & 1 & 1 \\ -2 & 0 & -3 \\ 3 & -5 & 8 \end{bmatrix},$$

so

$$B(a',b',c')^{-1} = \begin{bmatrix} -15/2 & -13/2 & -3/2 \\ 7/2 & 5/2 & 1/2 \\ 5 & 4 & 1 \end{bmatrix}$$

and we find $\mathrm{Inv}(a',b',c') = (f',g',h')$ where

$$f' = -15/2x^2 - 13/2xz - 3/2z^2, \quad g' = 5x^2 + 4xz + z^2, \quad h' = 7/2x^2 + 5/2xz + 1/2z^2.$$

This gives us the curve $X_1(a',b',c')$ with equation

$$-75/2x^4 - 125/2x^3z - 41x^2z^2 - 25/2xz^3 - 3/2z^4 - 7/2x^2y + -5/2xyz - 1/2z^2y + y^2.$$

If we make the change of coordinates $y' = y - 1/2h'$, we find a different equation for the curve, namely $y'^2 = 1/4h'^2 - f' \cdot g'$ where the right hand side is given by a binary quartic form. The binary quartic form is given by:

$$1/4h'^2 - f' \cdot g' = 649/16x^4 + 535/8x^3z + 695/16x^2z^2 + 105/8xz^3 + 25/16z^4,$$

which has binary quartic invariants

$$I = 3625/256, \quad J = 210475/2048.$$

Using these, we calculate that the j-invariant of $X_1(a',b',c')$ is 76215625/3088.

As the j-invariants of $X_1(a,b,c)$ and $X_1(a',b',c')$ are distinct, we see that permuting the roots of a and c gives us two non-isomorphic curves $X_3(a,b,c)$ and $X_3(a',b',c')$ that share the same genus 2 factor as $F_2(a,b,c) = F_2(a',b',c')$.

Finding tuples as in Lemma 3.2.5 is equivalent to solving the equation $tb^2 - ac = p$. Because of Lemma 3.2.4, we can assume c to be monic. Writing out the polynomials, we get

$$\begin{aligned} &p_0x^4 + p_1x^3 + p_2x^2 + p_3x + p_4 \\ &\quad = p \\ &\quad = tb^2 - ac \\ &\quad = (t-a_0)x^4 - (a_0c_1 + a_1)x^3 - (a_0c_2 + a_1c_1 + a_2 + 2\Delta t)x^2 - (a_1c_2 + a_2c_1)x - a_2c_2 + t\Delta^2. \end{aligned}$$

And comparing coefficients gives us the following set of equations:

$$\begin{aligned} t - a_0 &= p_0 \\ -a_0 c_1 - a_1 &= p_1 \\ -a_0 c_2 - a_1 c_1 - a_2 - 2t\Delta &= p_2 \\ -a_1 c_2 - a_2 c_1 &= p_3 \\ -a_2 c_2 + t\Delta^2 &= p_4. \end{aligned} \tag{3.3}$$

Lemma 3.2.9. *Let p be a monic polynomial of degree 4 over k and let $\mathbb{A}_k^6$ be the affine space of dimension 6 with coordinates $a_0, a_1, a_2, c_1, c_2, t$. The curve $C \subset \mathbb{A}_k^6$ given by the set of equations in (3.3) is birational to the curve D given by*

$$(p_0\Delta^2 - p_4)x^3 + p_3x^2y - (2p_0\Delta + p_2)xy^2 + p_1y^3 - p_1\Delta^2x^2 + (-2p_0\Delta^2 + 2p_4)xy + \\ (2p_1\Delta - p_3)y^2 + (p_2\Delta^2 + 2p_4\Delta)x + (p_1\Delta^2 - 2p_3\Delta)y - p_3\Delta^2.$$

in $\mathbb{A}_k^2$.

Proof. Let U be the open subset of $\mathbb{A}_k^6$ where $c_1^3 - 2c_1c_2 - 2c_1\Delta \neq 0$, and let V be the open subset of $\mathbb{A}_k^2$ where $x^3 - 2xy - 2x\Delta \neq 0$. We define $\phi : U \to V$ by

$$\phi(a_0, a_1, a_2, c_1, c_2, t) \to (c_1, c_2)$$

and $\psi : V \to U$ by

$$(x,y) \mapsto (f(x,y), p_1 - xf(x,y), f(x,y)(x^2 - y - 2\Delta) - xp_1 + 2p_0\Delta + p_2, x, y, p_0 - f(x,y)).$$

Here

$$f(x,y) = ((x^2 - y)p_1 - xp_2 - 2xp_0\Delta + p_3)/(x^3 - 2xy - 2x\Delta).$$

We claim that $\psi \circ \phi$ is the identity on U.

Let us first show that $\phi(C) \subset D$. We first remark that $t = a_0 + p_0$, $a_1 = -a_0c_1 - p_1$. and $a_2 = -a_1c_1 - a_0c_2 - 2t\Delta - p_2$. Combining these three gives us that

$$a_2 = (a_0c_1 + p_1)c_1 - a_0c_2 - 2(a_0 + p_0)\Delta - p_2.$$

If we then substitute a_1 and a_2 into the equation: $p_3 = -a_2c_1 - a_1c_2$ from 3.3, we get a relationship between a_0, c_1 and c_2. We find:

$$-a_0c_1^3 + 2a_0c_1c_2 + 2a_0c_1\Delta + 2c_1\Delta p_0 - (c_1^2 - c_2)p_1 + c_1p_2 - p_3 = 0.$$

Isolating a_0 gives us:

$$a_0 = (c_1^2 - c_2)p_1 - c_1p_2 - 2c_1p_0\Delta + p_3)/(c_1^3 - 2c_1c_2 - 2c_1\Delta) = f(c_1, c_2).$$

If we now add in the last equation

$$-a_2c_2 + t\Delta^2 - p_4$$

and substitute $t = f(c_1,c_2) + p_0$ and

$$a_2 = (f(c_1,c_2)c_1 + p + 1)c_1 - f(c_1,c_2)c_2 - 2(f(c_1,c_2) + p_0)\Delta - p_2],$$

we will get

$$\frac{F(c_1,c_2)}{(c_1^3 - 2\Delta c_1 - 2c_1c_2)}$$

where

$$F(c_1,c_2) = (p_0\Delta^2 - p_4)c_1^3 + p_3c_1^2c_2 - (2p_0\Delta + p_2)c_1c_2^2 + p_1c_2^3 - p_1\Delta^2c_1^2 + (-2p_0\Delta^2 + 2p_4)c_1c_2 + \\ (2p_1\Delta - p_3)c_2^2 + (p_2\Delta^2 + 2p_4\Delta)c_1 + (p_1\Delta^2 - 2p_3\Delta)c_2 - p_3\Delta^2,$$

so $\phi(V) \subset D$. We have that $\phi \circ \psi(x,y) = (x,y)$ by construction, so it remains to check that $\psi \circ \phi = \mathrm{id}$. We have

$$\begin{aligned}
&\psi \circ \phi(a_0,a_1,a_2,c_1,c_2,t) \\
&\quad = (f(c_1,c_2), p_1 - c_1f(c_1,c_2), f(c_1,c_2)(c_1^2 - c_2 - 2\Delta) - c_1p_1 + 2p_0\Delta + p_2, c_1, c_2, p_0 - f(c_1,c_2)) \\
&\quad = (a_0, p_1 - c_1a_0, a_0(c_1^2 - c_2 - 2\Delta) - c_1p_1 + 2p_0\Delta + p_2, c_1, c_2, p_0 - a_0) \\
&\quad = (a_0,a_1,a_2,c_1,c_2,t).
\end{aligned}$$

Now we have shown that C is birational to D. □

Lemma 3.2.10. *The curve D as in Lemma 3.2.9 has a rational singular point in*

$$(0,-\Delta)$$

and a rational point in

$$\left(\frac{\Delta^2p_1 + \Delta p_3}{\Delta^2p_0 - p_4}, -\Delta\right)$$

which is (usually) non-singular.

Proof. Filling in $y = -\Delta$ in the equation of D, we find:

$$(p_0\Delta^2 - p_4)x^3 - (\Delta^2p1 + \Delta p3)x^2 + (-2p_0\Delta^3 - p_2\Delta^2 + p_2\Delta^2 + 2p_4\Delta - 2\Delta^3p_0 - 2p_4\Delta)x - \\ p_1\Delta^3 - \Delta^2p_3 + 2\Delta^3p_1 - p_3\Delta^2 - \Delta^3p_1 + 2\Delta^2p_3 = \\ (p_0\Delta^2 - p_4)x^3 - (\Delta^2p1 + \Delta p3)x^2 + 0 + 0.$$

So now we see that we get solutions for $x = 0$ and

$$x = \left(\frac{\Delta^2p_1 + dp_3}{\Delta^2p_0 - p_4}\right).$$

To check whether these points are singular or not, we calculate the derivatives.
Now we find

$$\frac{dF}{dx} = 3x^2(p_0\Delta^2 - p_4) + 2p_3xy - (2p_0\Delta + p_2)y^2 - 2xp_1\Delta^2 - 2(p_0\Delta^2 - p_3x - p_4)y + p_2\Delta^2 + 2p_4\Delta$$

and

$$\frac{dF}{dy} = 3p_1y^2 + 2(2\Delta p_1 - (2\Delta p_0 + p_2)x - p_3)y\Delta^2 p_1 + p_3x^2 - 2\Delta p_3 - 2(\Delta^2 p_0 - p_4)x.$$

We get

$$\frac{dF}{dx}(x, -\Delta) = 3(\Delta^2 p_0 - p_4)x^2 - 2(\Delta^2 p_1 + \Delta p_3)x$$

and

$$\frac{dF}{dy}(x, -\Delta) = p_3x^2 + 2(\Delta^2 p_0 + \Delta p_2 + p_4)x$$

which already shows that $(0, -\Delta)$ is a singular point.

$$\frac{dF}{dx}\left(\left(\frac{\Delta^2 p_1 + \Delta p_3}{\Delta^2 p_0 - p_4}\right), -\Delta\right) = \frac{(\Delta^4 p_1^2 + 2\Delta^3 p_1 p_3 + \Delta^2 p_3^2)}{(\Delta^2 p_0 - p_4)}$$

$$\begin{aligned}\frac{dF}{dy}\left(\left(\frac{\Delta^2 p_1 + \Delta p_3}{\Delta^2 p_0 - p_4}\right), -\Delta\right) = {} & \frac{1}{(\Delta^4 p_0^2 - 2\Delta^2 p_0 p_4 + p_4^2)}(2\Delta^6 p_0^2 p_1 + 2\Delta^5 p_0 p_1 p_2 + 2\Delta^3 p_1 p_3^2 + \\ & \Delta^2 p_3^3 - 2(\Delta^2 p_1 + \Delta p_3)p_4^2 + (2\Delta^5 p_0^2 + \Delta^4 p_1^2 + 2\Delta^4 p_0 p_2)p_3 - \\ & 2(\Delta^3 p_1 p_2 + \Delta^2 p_2 p_3)p_4).\end{aligned}$$

The latter is almost always non-zero. So,

$$\left(\frac{\Delta^2 p_1 + \Delta p_3}{\Delta^2 p_0 - p_4}\right)$$

is usually a non-singular point. □

Lemma 3.2.11. *Let D be the curve as in Lemma 3.2.9. Assume that*

$$\left(\frac{\Delta^2 p_1 + \Delta p_3}{\Delta^2 p_0 - p_4}, -\Delta\right)$$

is non-singular. Then D is a rational curve. More specifically, let

$$g(z) = \frac{(\Delta^2 p_1 + (\Delta p_1 + p_3)z^2 + \Delta p_3 - (2\Delta^2 p_0 + 2\Delta p_2 + 2p_4)z)}{(p_1 z^3 - (2\Delta p_0 + p_2)z^2 + (\Delta^2 p_0 - p_4) + p_3 z)}.$$

Then the morphism: $\phi : \mathbb{A}^1_k \to D$ defined by $z \mapsto (g(z), zg(z) - \Delta)$ gives us a parametrization of D.

Proof. The curve D is given by a cubic equation and has a singular point at $(0,-\Delta)$. As D is a singular cubic, it has to be of genus 0. It moreover has a rational non-singular point at $P = \left((p_1\Delta^2 + p_3\Delta)/(p_0\Delta^2 - p_4), -\Delta\right)$, so the curve has to be rational. We are going to find a rational parametrization by drawing a line through the singular point with slope equal to z. We substitute $y = zx - \Delta$ in the equation for D and we find:

$$x^2\left(p_1xz^3 + (\Delta^2p_0 - p_4)x - (\Delta^2p_1 + \Delta p_3) - ((2\Delta p_0 + p_2)x + (\Delta p_1 + p_3))z^2 + (p_3x + 2(\Delta^2p_0 + \Delta p_2 + p_4))z\right).$$

After dividing by x^2, we can isolate the x to get the equation:

$$x = \frac{(\Delta^2p_1 + (\Delta p_1 + p_3)z^2 + \Delta p_3 - (2\Delta^2p_0 + 2\Delta p_2 + 2p_4)z)}{(p_1z^3 - (2dp_0 + p_2)z^2 + (\Delta^2p_0 - p_4) + p_3z)} = g(z).$$

By construction, $y = zg(z) - \Delta$, which gives us the parametrization ϕ.

□

Corollary 3.2.12. *Let $a, b = x^2 - \Delta, c$ be a regular quadratic triple and let $p = b^2 - ac$. The curve D as in 3.2.9 is a rational curve parametrizing a non-constant family of genus 3 curves X_3 for which X_3 is a 2,2-glueing of the genus 2 curve $Y_2(a,b,c)$ and some elliptic curve.*

Proof. Let $(a_0, a_1, a_2, c_1, c_2, t)$ be any set of solutions on D. Let $a' = a_0x^2 + a_1x + a_2$, $\quad b' = b$ and $c' = x^2 + c_1x + c_2$. Then $tb^2 - a'c' = b^2 - ac$. Then Lemma 3.2.5 tells us that $Y_2(a,b,c)$ is isomorphic to $Y_2(ta', tb, c')$, so the curve $X_3(ta', tb, c')$ is a 2,2-glueing of $Y_2(a,b,c)$ and some elliptic curve. This shows that all points on D give rise to genus 3 curves that are 2,2-glueings of Y_2 and some elliptic curve.

To show that this family is non-constant, we remark that Remark 3.2.7 and Example 3.2.8 show us that (after possibly taking a field extension) there generically exists at least one solution $(a_0, a_1, a_2, c_1, c_2, 1)$ for which $X_1(a,b,c)$ is not isomorphic to $X_1(a', b, c')$. Let ϕ be the rational parametrization of D defined in Lemma 3.2.11. Let $(a_0, a_1, a_2, c_1, c_2, t) \in D$ and write $\tau(a_0, a_1, a_2, c_1, c_2, t, b) = (t(a_0x^2 + a_1x + a_2), tb, x^2 + c_1x + c_2)$. The function $J : \mathbb{A}^1_k \to k$ given by taking the j-invariant of the curve $X_1(\tau(\phi(z))$ is some polynomial function in terms of the rational parameter z. As we have shown above, there exists at least one point $(a_0, a_1, a_2, c_1, c_2, 1)$ for which $j(X_1(a,b,c))$ is not equal to $j(X_1(a', b, c'))$, so the J-fuction is a non-constant polynomial on a connected curve. We conclude that the curve D gives us a non-constant rational family of genus 3 curves, in which every curve is the 2,2-glueing of $Y_2(a,b,c)$ and some elliptic curve.

□

Remark 3.2.13. We could also have chosen $b = x$ instead of $b = x^2 - d$ to find a slightly simpler family of curves.

Example 3.2.14. We are going to use the above described technique to construct a non-hyperelliptic genus 3 curve with QM. Let Y_2 be given by

$$y^2 = x^5 + x^4 + 4x^3 + 8x^2 + 5x + 1.$$

This curve is on `www.lmfdb.org` under label 262144.d.524288.2 and the endomorphism ring of its Jacobian is a quaternion algebra of discriminant 6 over $\bar{\mathbb{Q}}$. After the endomorphism $(x,y) \mapsto \left(\frac{2x}{-x+1}, y/(-x+1)^3\right)$, we get the equation

$$y^2 = -25x^6 + 12x^5 + 27x^4 - 16x^3 - 3x^2 + 4x + 1.$$

and the right hand side factors as

$$-(x^2 - 1)(25x^4 - 12x^3 - 2x^2 + 4x + 1)$$

which puts it into a form we can use to describe the map ϕ in Lemma 3.2.10. Indeed, we have $p = -25x^4 + 12x^3 + 2x^2 - 4x - 1$, so $p_0 = -25, p_1 = 12, p_2 = 2, p_3 = -4, p_4 = 1$ and we find that

$$g(z) = \frac{8z^2 + 48z + 8}{12z^3 + 48z^2 - 4z - 24}$$

and $\phi(z) = (g(z), zg(z))$. Setting $z = -2$, we get $c_1 = g(-2)$ and $c_2 = -2(g(-2))$ to calculate a triple of polynomials:

$$a = 3320/147x^2 + 80/21x - 520/147, \qquad b = x^2 - 1, \qquad c = x^2 - 7/10x + 2/5$$

and the variable $t = -355/147$ using the relations in (3.3). Now the curve $Z_3(a/t, b, c)$ will be given by the equation

$$\begin{aligned} -355/19208x^4 + y^4 + 1065/9604x^3 + (103x^2 + 132x + 5)/98y^2 \\ + 6745/9604x^2 + 1065/9604x - 355/19208, \end{aligned}$$

which we can simplify to

$$-x^4 + 19208/355y^4 + 6x^3 + 196/355(103x^2 + 132x + 5)y^2 + 38x^2 + 6x - 1$$

by multiplying with 19208/355. And this curve is a (2,2)-glueing of Y_2 and some elliptic curve (Using Lemma 3.2.5 and Remark 3.2.6), and will therefore also have QM.

Remark 3.2.15. In order to glue, we need a factor of the form $x^2 - \Delta$ in the equation of our hyperelliptic curve. This is equivalent to the condition that two of the 2-torsion points lie in the same Galois orbit over the base field. We can use this observation to determine a field extension of minimal degree over which we can glue.

Remark 3.2.16. It is also possible to construct a family of genus 3 curves that are (2,2)-glueings of a genus 2 curve and a fixed genus 1 factor X_1. Assume X_1 is given by the equation $y^2 - hy + fg$ for some quadratic polynomials f, g and h. Let $t \in k$ then any curve $X_{1,t} = v^2 + hv(t-1) + (t^2h^2 - 2th^2)/4 + fg$ is isomorphic to X_1 using the substitution $y = v + th/2$. Now the curve $Z_{3,t} = v^4 + hv^2(t-1) + (t^2h^2 - 2th^2)/4 + fg$ gives us a corresponding genus 3 cover of degree 2. To see that this family will generically be non-constant, remark that the curve $Z_{3,1}$ will have CM by the automorphism $(x, v) \mapsto (x, iv)$ even though for $t \neq 1$, $Z_{3,t}$ will generally not have this property.

Chapter 4

Algebraic glueing

4.1 Theory behind algebraic glueing

Lemma 4.1.1. *Let k be a field, and let Y_2 be a curve of genus 2. Let* $\mathrm{Kum}(Y_2) = \mathrm{Jac}(Y_2)/(-\mathrm{Id}_{Y_2}) \subset \mathbb{P}^3_k$ *be the Kummer surface associated to Y_2 with singular points $P_1, \ldots, P_{16}$. Let H be a plane in $\mathbb{P}^3_k$. Then $\widetilde{X}_1 = H \cap K$ defines a curve of arithmetic genus 3. Furthermore, if H intersects with exactly two of the P_i, the desingularization X_1 of $\widetilde{X}_1$ is a curve of genus 1.*

Theorem 4.1.2. *Let k be a field, and let Y_2 be a curve of genus 2. Let* $\mathrm{Kum}(Y_2) = \mathrm{Jac}(Y_2)/(-\mathrm{Id}_{Y_2}) \subset \mathbb{P}^3_k$ *be the Kummer surface associated to Y_2. Let H be a plane in $\mathbb{P}^3_k$ that passes through exactly two singular points P, Q, such that $\widetilde{X}_1 = H \cap K$ is isomorphic to a genus 1 curve with two nodes. Write $i : \widetilde{X}_1 \to \mathrm{Kum}(Y_2)$ for the inclusion map, and let $p : X_1 \to \widetilde{X_1}$ be the desingularization. Now let $Z_3 = X_1 \times_K \mathrm{Jac}(Y_2)$ be the pullback. We get the following diagram:*

$$\begin{tikzcd}
Z_3 = X_1 \times_{\mathrm{Kum}(Y_2)} \mathrm{Jac}(Y_2) \arrow[r, "\tau_3"] \arrow[d, "\overline{\pi}"] & \widetilde{Z}_3 = \widetilde{X}_1 \times_{\mathrm{Kum}(Y_2)} \mathrm{Jac}(Y_2) \arrow[r, hook, "i_3"] \arrow[d, "\widetilde{\pi}"] & \mathrm{Jac}(Y_2) \arrow[d, "\pi"] \\
X_1 \arrow[r, "\tau_1"] & \widetilde{X}_1 \arrow[r, hook, "i_1"] & \mathrm{Kum}(Y_2)
\end{tikzcd}.$$

Then X_3 is an irreducible curve of genus 3 and $\mathrm{Jac}(Z_3)$ *is a 2,2-glueing of* $\mathrm{Jac}(Y_2)$ *and* $\mathrm{Jac}(X_1)$.

Proof. First note that because i is a closed immersion, the morphism $j : \widetilde{Z}_3 \to \mathrm{Jac}(Y_2)$ is also a closed immersion. Now the morphism $\widetilde{\pi} : \widetilde{Z}_3 \to \widetilde{X}_1$ is finite because the morphism $\mathrm{Jac}(X_2) \to \mathrm{Kum}(Y_2)$ is of degree 2. It follows that $\widetilde{Z}_3$ is of dimension 1, and that the morphism $\widetilde{Z}_3 \to \widetilde{X}_1$ is also of degree 2. The map $\widetilde{Z}_3 \to \widetilde{Z}_1$ is ramified above $i^{-1}(P)$ and $i^{-1}(Q)$. As $\overline{\pi} : Z_3 \to X_1$ is the desingularization of $\widetilde{\pi}$), it is a degree 2 cover of a genus 1 curve. The points $i^{-1}(P)$ and $i^{-1}(Q)$ are nodes by assumption, so $\overline{\pi}$ is ramified above the points

$P_1, P_2 \in p_1^{-1}(\{i^{-1}(P)\})$ and $Q_1, Q_2 \in \tau_1^{-1}(\{i^{-1}(P)\})$. Using the Riemann-Hurwitz formula, it follows that Z_3 is an irreducible curve of genus 3.

We will now show that $\mathrm{Jac}(Z_3)$ is a 2,2-glueing of $\mathrm{Jac}(X_1)$ and $\mathrm{Jac}(Y_2)$. As Z_3 covers X_1 by a morphism of degree 2, we naturally get a morphism $p_1 : \mathrm{Jac}(X_1)$ $to\mathrm{Jac}(Z_3)$. The morphism p_1 is injective because otherwise, we would be able to find an elliptic curve E' with

$$\mathrm{Jac}(X_1) \to E' \hookrightarrow \mathrm{Jac}(Z_3),$$

which would imply that $\overline{\pi}$ also factors as

$$Z_3 \to E' \to X_1.$$

But this contradicts the fact that $\overline{\pi}$ is of degree 2. So p_1 is injective. We also have a morphism $X_3 \to \mathrm{Jac}(Y_2)$. By considering the Jacobian of Z_3 as an Albanese variety, this morphism factors through a morphism $p_2 : \mathrm{Jac}(Z_3) \to \mathrm{Jac}(Y_2)$. We claim ϕ is a surjective morphism. If it were not surjective, the image of ϕ would be contained in an abelian subvariety. So its image would either be a point or an elliptic curve. The first case is impossible as the image of Z_3 is not contained in a point. Now assume $p_2(\mathrm{Jac}(Z_3))$ is an elliptic curve F. In this case $p_2(Z_3) = E$, and as E contains four 2-torsion points, $\pi(E) = Y_1$ would have to contain 4 singular points. But $\pi(E)$ has arithmetic genus 3 by construction. And this gives us a contradiction as X_1 has arithmetic genus 1. Hence, p_2 is a surjective morphism.

TODO: Proof of being a 2,2-glueing

□

4.2 Families of planes on the Kummer surface going through two singular points

Proposition 4.2.1. *Let k be a field, and let Y_2 be a curve of genus 2. Let* $\mathrm{Kum}(Y_2) = \mathrm{Jac}(Y_2)/(-\mathrm{Id}_{Y_2}) \subset \mathbb{P}^3$ *be the Kummer surface associated to Y_2 with singular points $P_1, \ldots, P_{16}$. Let $P \in \mathrm{Jac}(Y_2)[2]$. Then P induces an automorphism σ_P of* $\mathrm{Kum}(Y_2)$ *in the following way*

$$\begin{array}{ccc} \mathrm{Jac}(Y_2) & \xrightarrow{x \mapsto x+P} & \mathrm{Jac}(Y_2) \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathrm{Kum}(Y_2) & \xrightarrow{\sigma_P} & \mathrm{Kum}(Y_2) \end{array}.$$

Lemma 4.2.2. *Let* $\mathrm{Kum}(Y_2)$ *and σ_P be as above. Let $H \subset \mathbb{P}^3$ be a plane going through P_1 and P_2. Then σ_P maps H to another plane $\sigma(H)$ going through two singular points. If $\sigma(H) = H$, then either σ swaps P_1 and P_2 or $\sigma = \mathrm{Id}$.*

Proof. By Corollary 2.18 and Theorem 2.20 in [5], there exist $A, B, C, D, a, b, c, d \in k$, such that we can realize $\mathrm{Kum}(Y_2)$ as a quartic equation in $\mathbb{P}^3_k$ of the form

$$K(x,y,z,t) = x^4+y^4+z^4+t^4+2Dxyzt+A(x^2t^2+y^2z^2)+B(y^2t^2+x^2z^2)+C(z^2t^2+x^2y^2)$$

and such that its 16 singular points are given by:

$$(a,b,c,d),(d,-c,b,-a),(d,c,-b,-a),(c,d,-a,-b)$$

$$(-c,d,a,-b),(-b,a,d,-c),(b,-a,d,-c),(d,c,b,a)$$

$$(c,d,a,b),(b,a,d,c),(a,-b,-c,d),(-a,b,-c,d)$$

$$(-a,-b,c,d),(d,-c,-b,a),(-c,d,-a,b),(-b,-a,d,c)$$

with the additional conditions that

$$ad \neq \pm bc,$$

$$ac \neq \pm bd,$$

$$ab \neq \pm cd,$$

$$a^2+d^2 \neq b^2+c^2,$$

$$a^2+c^2 \neq b^2+d^2,$$

$$a^2+b^2 \neq c^2+d^2,$$

$$a^2+b^2+c^2+d^2 \neq 0.$$

Every element in the group $\mathrm{Jac}(Y_2)[2]$ induces an automorphism on $\mathrm{Kum}(Y_2)$ that coincides with permuting two of these points. In particular, the automorphisms are generated by six maps, namely:

- α: swaps x with t and y with z.
- β: swaps y with t and x with z.
- γ: swaps x with y and z with t.
- α': maps z to $-z$ and y to $-y$.
- β': maps x to $-x$ and z to $-z$.
- γ': maps x to $-x$ and y to $-y$.

Without loss of generality, we can assume that $P_1 = (d, -c, b, -a)$ and $P_2 = (d, c, -b, -a)$. In this case, the family of planes, parametrized by λ, going through these two points is given by

$$ax + by + cz + dt + \lambda(ax - by - cz + dt).$$

The automorphisms $\alpha, \beta, \gamma, \alpha', \beta', \gamma'$ only swap variables or signs, so it is clear that they map planes to planes.

Lemma 1.7 in [5]tells us that given two points P_1, P_2, there are only two planes H, H' that contain both of them. In our case these planes are $H : ax + by + cz + dt = 0$ and $H' : ax - by - cz + dt = 0$. As any automorphism σ coming from $\mathrm{Jac}(Y_2)[2]$ fixes P_1 and P_2, it also needs to fix $H + \lambda H'$. This can only happen if σ is the identity or if σ swaps h and H'.

$\square$

Remark 4.2.3. Consider P_1, P_2, H and H' as above. Let σ be the automorphism that swaps P_1 and P_2. In this case, $\sigma = \alpha'$. We see that the plane $H + \lambda_0 H'$ is invariant under α' if and only if $\lambda_0 = \pm 1$.

Corollary 4.2.4. *Let H be a plane going through P_i and P_j. There always exists an automorphism σ such that $\sigma(H)$ goes through P_1.*

Proof. Let $\sigma \in \mathrm{Aut}(\mathrm{Jac}(Y_2))[2]$ be given by $x \mapsto x - P_i + P_1$. This automorphism descends to a linear automorphism of $\mathbb{P}^3$, and has the property that $P_i \mapsto P_1$. $\square$

Remark 4.2.5. Any curve given by the intersection of $\mathrm{Kum}(Y_2)$ with a plane, passing through two points can be mapped isomorphically to one containing P_1. This means that, if we glue curves using the construction from Theorem 4.1.2, fixing $P = P_1$ and letting Q vary in $\{P_2, \ldots, P_{16}\}$ will give us all possible ways we can calculate a 2,2-glueing of X_1 and Y_2 using this method.

Let $H(\lambda)$ be the family of planes going through two singular points P_1, P_2 of the Kummer surface $\mathrm{Kum}(Y_2)$. Given a curve of genus 1 X_1, we want to be able to find a λ_0 such that $H(\lambda_0)$ is isomorphic to X_1. In order to do this, we will consider a procedure to write the j-invariant of $H(\lambda)$ in terms of λ.

Lemma 4.2.6. *Let k be a field, and let Y_2 be a curve of genus 2. Let $\mathrm{Kum}(Y_2) = \mathrm{Jac}(Y_2)/(-\mathrm{Id}_{Y_2}) \subset \mathbb{P}^3$ be the Kummer surface associated to Y_2 with singular points $P_1, \ldots, P_{16}$. Let $H(\lambda)$ be the family of planes going through $P_1 = (x_1, y_1)$ and $P_2(x_2, y_2)$. Fix $\lambda_0 \in k$. Define the function $f : H(\lambda_0) \backslash \{P_1\} \to k$ in the following way:*

$$\widetilde{g}((x,y)) = \left(\frac{y_1 - y}{x_1 - x}\right).$$

Then $\widetilde{g}$ extends to a function of degree 2 on $H(\lambda_0)$.

Proof. □

Corollary 4.2.7. *Let g be as in Lemma 4.2.6 and let x_1, x_2, x_3, x_4 be the x-coordinates of the ramification points of g. Then the j-invariant of $H(\lambda_0)$ is the cross-ratio of x_1, x_2, x_3 and x_4.*

Theorem 4.2.8. *Let k be a field, and let Y_2 be a curve of genus 2. Let* $\mathrm{Kum}(Y_2) = \mathrm{Jac}(Y_2)/(-\mathrm{Id}_{Y_2}) \subset \mathbb{P}^3$ *be the Kummer surface associated to Y_2 with singular points $P_1, \dots, P_{16}$. Let $H(\lambda)$ be the family of planes going through P_1 and P_2. Then the j-invariant of the family $H(\lambda)$, is a polynomial $j(H(\lambda))$ of degree 12.*

Proof. As in Lemma 4.2.2, we can assume without loss of generality that $\mathrm{Kum}(Y_2)$ is given by the homogeneous polynomial

$$K(x,y,z,t) = x^4+y^4+z^4+t^4+2Dxyzt+A(x^2t^2+y^2z^2)+B(y^2t^2+x^2z^2)+C(z^2t^2+x^2y^2)$$

in $\mathbb{P}^3_k$ with singular points $P_1 = (d,-c,b,-a)$ and $P_2 = (d,c,-b-a)$, and that the family of planes going through P_1 and P_2 is given by

$$H(\lambda) = ax+by+cz+dt+\lambda(ax-by-cz+dt).$$

□

4.3 Explicitly describing the Kummer of a Jacobian of a genus 2 curve and the corresponding quotient map

In order to give an explicit algorithm to construct the glueing of a genus 2 curve Y_2 and a genus 1 curve X_1 over k, we will need an explicit description of the quotient map $\mathrm{Jac}(Y_2) \to \mathrm{Kum}(Y_2)$ where $\mathrm{Kum}(Y_2)$ is the Kummer surface of Y_2.

In order to do this we will first write down an equation for an affine open subset of the Jacobian using the ideas by Cantor in [3].

Proposition 4.3.1. *Let Y_2 be a curve of genus 2 over a field k given by the equation $y^2 = f(x)$ in $\mathbb{P}^2_k$. Let $i : Y_2 \to Y_2$ be the involution given by $(x,y) \mapsto (x,-y)$. Any point $(P,Q) \in \mathrm{Sym}^2(Y_2)$ where $Q \neq i(P)$ can be uniquely described by a pair of polynomials $a(x) = x^2 + a_1x + a_2$ and $b(x) = +b_1x + b_2$ satisfying*

$$\left(b(x)^2 - f(x)\right) \mod a(x) \equiv 0.$$

Corollary 4.3.2. *Let Y_2 be a curve of genus 2 over a field k given by the equation $y^2 = f(x)$ in $\mathbb{P}^2_k$. Let g_1 and g_2 be polynomials in $k[a_1, a_2, b_1, b_2]$ such that*

$$g_1(a_1, a_2, b_1, b_2)x + g_0(a_1, a_2, b_1, b_2) \equiv \left(b(x)^2 - f(x)\right) \mod a(x).$$

Then the system of equations

$$\begin{aligned} g_1(a_1, a_2, b_1, b_2) &= 0 \\ g_2(a_1, a_2, b_1, b_2) &= 0. \end{aligned}$$

describes an affine open subset U of $\mathrm{Jac}(Y_2)$ *in* $\mathbb{A}^4_k$.

We will now combine this with Müller's description of the Kummer surface in [10] to give an affine equation for the Kummer surface $\mathrm{Jac}(Y_2)$ in $\mathbb{P}^3_k$ and an explicit description of the map $\mathrm{Jac}(Y_2) \to \mathrm{Kum}(Y_2)$.

Proposition 4.3.3. *Let Y_2 be a curve of genus 2 over a field k given by the equation*

$$y^2 = f_0 + f_1x + f_2x^2 + f_3x^3 + f_4x^4 + f_5x^5 + f_6x^6$$

in $\mathbb{A}^2_k$. Suppose $P = (x, y)$ and $Q = (u, v)$ are two points on Y_2 and let $P + Q \in$ $\mathrm{Jac}(Y_2)$. *Let*

$$\begin{aligned} \kappa_1 &= 1 \\ \kappa_2 &= x + u \\ \kappa_3 &= xu \\ \kappa_4 &= \frac{F_0(x, u) - 2yv}{(x-u)^2}. \end{aligned}$$

where

$$F_0(x, u) = 2f_0 + f_1(x+u) + 2f_2(xu) + f_3(x+u)xu + 2f_4(xu)^2 + f_5(x+u)(xu)^2 + 2f_6(xu)^3.$$

Then $(x, u) \mapsto (\kappa_1 : \kappa_2 : \kappa_3 : \kappa_4)$ is a map $U \to$ $\mathrm{Kum}(Y_2)$.

The functions $\kappa_1, \kappa_2, \kappa_3, \kappa_4$ satisfy the quartic equation

$$K(\kappa_1, \kappa_2, \kappa_3, \kappa_4) = K_2(\kappa_1, \kappa_2, \kappa_3)\kappa_4^2 + K_1(\kappa_1, \kappa_2, \kappa_3)\kappa_4 + K_0(\kappa_1, \kappa_2, \kappa_3) = 0$$

and this equation gives us a projective embedding of $\mathrm{Kum}(Y_2)$ *in $\mathbb{P}^3_k$. In here*

$$\begin{aligned} K_2(\kappa_1, \kappa_2, \kappa_3) =& \kappa_2^2 - 4\kappa_1\kappa_3 \\ K_1(\kappa_1, \kappa_2, \kappa_3) =& -4\kappa_1^3 f_0 - 2\kappa_1^2\kappa_2 f_1 - 4\kappa_1^2\kappa_3 f_2 - 2\kappa_1\kappa_2\kappa_3 f_3 - 4\kappa_1\kappa_3^2 f_4 - 2\kappa_2\kappa_3^2 f_5 - 4\kappa_3^3 f_6 \\ K_0(\kappa_1, \kappa_2, \kappa_3) =& -4\kappa_1^4 f_0 f_2 + \kappa_1^4 f_1^2 - 4\kappa_1^3\kappa_2 f_0 f_3 - 2\kappa_1^3\kappa_3 f_1 f_3 - 4\kappa_1^2\kappa_2^2 f_0 f_4 + 4\kappa_1^2\kappa_2\kappa_3 f_0 f_5 \\ & -4\kappa_1^2\kappa_2\kappa_3 f_1 f_4 - 4\kappa_1^2\kappa_3^2 f_0 f_6 + 2\kappa_1^2\kappa_3^2 f_1 f_5 - 4\kappa_1^2\kappa_3^2 f_2 f_4 + \kappa_1^2\kappa_3^2 f_3^2 \\ & -4\kappa_1\kappa_2^3 f_0 f_5 + 8\kappa_1\kappa_2^2\kappa_3 f_0 f_6 - 4\kappa_1\kappa_2^2\kappa_3 f_1 f_5 + 4\kappa_1\kappa_2\kappa_3^2 f_1 f_6 \\ & -4\kappa_1\kappa_2\kappa_3^2 f_2 f_5 - 2\kappa_1\kappa_3^3 f_3 f_5 - 4\kappa_2^4 f_0 f_6 - 4\kappa_2^3\kappa_3 f_1 f_6 - 4\kappa_2^2\kappa_3^2 f_2 f_6 \\ & -4\kappa_2\kappa_3^3 f_3 f_6 - 4\kappa_3^4 f_4 f_6 + \kappa_3^4 f_2. \end{aligned}$$

Lemma 4.3.4. *Let U be an affine open subset of the Jacobian in $\mathbb{A}^4 = k[a_1, a_2, b_1, b_2]$ given by the system of equations $g_1 = 0, g_2 = 0$ as in Corollary 4.3.2. Then the restriction of the map described in Proposition 4.3.3 to U can be explicitly described by*

$$(a_1, a_2, b_1, b_2) \mapsto \left(1 : -a_1 : a_2 : \frac{F_0(-a_1, a_2) - 2(b_1^2 a_2 - b_1 b_2 a_1 + b_2^2)}{a_1^2 - 4a_2}\right)$$

where

$$F_0(x, y) = 2f_0 + f_1 x + 2f_2 y + f_3 xy + 2f_4 y^2 + f_5 xy^2 + 2f_6 y^3.$$

So, we have now found an explicit description of the degree 2 quotient map $\mathrm{Jac}(Y_2) \to \mathrm{Kum}(Y_2)$ on an affine open of $\mathrm{Jac}(Y_2)$. As this map is of degree 2, it will induce an inclusion of function fields of degree 2, $\phi : K(\mathrm{Kum}(Y_2)) \to K(\mathrm{Jac}(Y_2))$. For the glueing algorithm that we will describe in the next sections, we will also need to determine a function $h \in k[\kappa_1, \kappa_2, \kappa_3, \kappa_4]$ such that $K(\mathrm{Jac}(Y_2)) = K(\mathrm{Kum}(Y_2)[\sqrt{h}]$.

Lemma 4.3.5. *There exists $h \in K(\mathrm{Kum}(Y_2))$ such that $\phi(h) = b_1^2$.*

Proof. We know that $\phi(\kappa_2) = -a_1, \phi(\kappa_3) = a_2$ and

$$\phi(\kappa_4) = \frac{F_0(-a_1, a_2) - 2(b_1^2 a_2 - b_1 b_2 a_1 + b_2^2)}{a_1^2 - 4a_2}.$$

We will start by showing that $b_1 b_2$ and b_2^2 can be written as

$$\begin{aligned} b_1 b_2 &= \alpha_1(a_1, a_2) + \alpha_2(a_1, a_2) b_1^2 \\ b_1^2 &= \beta_1(a_1, a_2) + \beta_2(a_1, a_2) b_1^2 \end{aligned}$$

for some $\alpha_i, \beta_i \in k(x, y)$.

Remark that the polynomials g_1 and g_2 from Corollary 4.3.2 can be seen as elements of $k(a_1, a_2)[b_1^2, b_2^2, b_1 b_2]$. We can therefore write

$$\begin{aligned} g_1 &= \lambda_0 + \lambda_{1,1} b_1^2 + \lambda_{1,2} b_1 b_2 + \lambda_{2,2} b_2^2 \\ g_2 &= \mu_0 + \mu_{1,1} b_1^2 + \mu_{1,2} b_1 b_2 + \mu_{2,2} b_2^2 \end{aligned}$$

with $\lambda_i, \mu_i \in k(a_1, a_2)$. We can consider this as a set of linear equations with variables $1, b_1^2, b_1 b_2$ and b_2^2. Using these equations, we can write $b_1 b_2$ and b_2^2 in terms of a_1, a_2 and b_1^2, which is what we wanted to show. Now we have

$$\begin{aligned} \phi(\kappa_4) &= \frac{F_0(-a_1, a_2)}{a_1^2 - 4a_2} - \frac{2(b_1^2 a_2 - (\alpha_1(a_1, a_2) + \alpha_2(a_1, a_2) b_1^2) a_1 + \beta_1(a_1, a_2) + \beta_2(a_1, a_2) b_1^2)}{a_1^2 - 4a_2} \\ &= \frac{F_0(\phi(\kappa_2), \phi(\kappa_3))}{\phi(\kappa_2)^2 - 4\phi(\kappa_3)} - \frac{2(b_1^2 \phi(\kappa_3) - (\alpha_1(-\phi(\kappa_2), \phi(\kappa_3)) - \alpha_2(-\phi(\kappa_2), \phi(\kappa_3)) b_1^2) \phi(\kappa_2)}{\phi(\kappa_2)^2 - 4\phi(\kappa_3)} + \\ &\quad \frac{\beta_1(-\phi(\kappa_2), \phi(\kappa_3)) + \beta_2(-\phi(\kappa_2), \phi(\kappa_3)) b_1^2)}{\phi(\kappa_2)^2 - 4\phi(\kappa_3)}. \end{aligned}$$

It follows that

$$b_1^2 = \frac{(\phi(\kappa_2)^2 - 4\phi(\kappa_3)) \cdot (\phi_4(\kappa_4) - F_0(\phi(\kappa_2), \phi(\kappa_4)) + (\alpha_1(-\phi(\kappa_2), \phi(\kappa_3)) + \beta_1(-\phi(\kappa_2), \phi(\kappa_3))}{2\phi(\kappa_3) - \alpha_2(-\phi(\kappa_2), \phi(\kappa_3)))\phi(\kappa_2) + \beta_2(-\phi(\kappa_2), \phi(\kappa_3))}.$$

So we can define

$$h = \frac{(\kappa_2^2 - 4\kappa_3) \cdot (\kappa_4 - F_0(\kappa_2, \kappa_4) + (\alpha_1(-\kappa_2, \kappa_3) + \beta_1(-\kappa_2, \kappa_3)}{2\kappa_3 - \alpha_2(-\kappa_2, \kappa_3))\kappa_2 + \beta_2(-\kappa_2, \kappa_3)}$$

to get $\phi(h) = b_1^2$. □

Corollary 4.3.6. *Let h be as in Lemma 4.3.5. Then we can extend ϕ to a morphism $\overline{\phi} : (K(\mathrm{Kum}(Y_2)[\sqrt{h}] \to K(\mathrm{Jac}(Y_2))$ such that $\overline{\phi}$ is an isomorphism.*

Proof. Define $\overline{\phi}(x) = \phi(x)$ for $x \in K(\mathrm{Kum}(Y_2)$ and $\overline{\phi}(\sqrt{h} = b_1$. It suffices to show that a_1, a_2, b_1 and b_2 are in the image of $\overline{\phi}$. We already have $\overline{\phi}(\kappa_2) = -a1, \overline{\phi}(\kappa_3) = a_2$ and $\overline{\phi}(\sqrt{h}) = b_1$. As

$$\begin{aligned} \overline{\phi}(\kappa_4) &= \frac{F_0(-a_1, a_2) - 2(b_1^2 a_2 - b_1 b_2 a_1 + b_2^2)}{a_1^2 - 4a_2} \\ &= \frac{F_0(-a_1, a_2) - 2(b_1^2 a_2 - b_1 b_2 a_1 + \beta_1(a_1, a_2) + \beta_2(a_1, a_2) b_1^2)}{a_1^2 - 4a_2}, \end{aligned}$$

it follows that $b_1 b_2$ and therefore b_2 are also in the image of $\overline{\phi}$, which is what we wanted to show. □

4.4 Determining degree 2 covers of an elliptic curve that are ramified above four points

Proposition 4.4.1. *Let E be an elliptic curve over $\mathbb{C}$, and let P_1, P_2, P_3, P_4 be distinct points in $E(\mathbb{C})$. Then there are exactly four distinct covers of degree 2 that are ramified above the P_i.*

Proof. Let $p : X \to E$ be a cover of degree 2, and let $P_0 \in \overline{E} = E(\mathbb{C}) \backslash \{P_1, P_2, P_3, P_4\}$ be another point on E. By the general theory of covering spaces, giving an isomorphism class of covers is the same as specifying a monodromy action. As p is a cover of degree 2, the algebraic monodromy is given by a morphism

$$\phi : \pi_1(\overline{E}, P_0) \to \mathbb{Z}/2\mathbb{Z}.$$

Let $\pi_1(E, P_0) = \langle \alpha, \beta \rangle$. We know (reference?) that the fundamental group

$$\pi_1(\overline{E}, P_0) = \langle \gamma_1, \gamma_2, \gamma_3, \gamma_4, \alpha, \beta | \gamma_1 \gamma_2 \gamma_3 \gamma_4 = \alpha \beta \alpha^{-1} \beta^{-1} \rangle$$

where γ_i is a loop around the point P_i.

As the points P_i are ramification points, we need that $\phi(\gamma_i) = 1$. Otherwise, we would get a cover that is not ramified above P_i. Now the only choices we have are choosing $\phi(\alpha)$ and $\phi(\beta)$. As we can choose either 0 or 1 for both of them, we end up with four distinct possibilities for p.

□

Proposition 4.4.2. *Let E be an elliptic curve over k given by the equation*

$$E : y^2 - h(x,z)y + f(x,z)$$

in $\mathbb{P}_k^{1,2,1}$. Let P_1, P_2, P_3, P_4 be the points on E that have $y = 0$. These will be the ramification points of the covers we are going to construct.

Write $p(x,z) = f(x,z) - 1/4h(x,z)^2$. Assume that $p(x,z) = (x-\alpha_1 z)(x-\alpha_2 z)(x-\alpha_3 z)(x-\alpha_4 z)$. We will denote the four 2-torsion points by $T_i = (\alpha_i, h(\alpha_i, 1)/2, 1)$. We let

$$v_1^2 = \frac{y}{(x-\alpha_1 z)(x-\alpha_1 z)}, \qquad L_1 = K(E)(v_1),$$

$$v_2^2 = \frac{y}{(x-\alpha_1 z)(x-\alpha_2 z)}, \qquad L_2 = K(E)(v_2),$$

$$v_3^2 = \frac{y}{(x-\alpha_1 z)(x-\alpha_3 z)}, \qquad L_3 = K(E)(v_3),$$

$$v_4^2 = \frac{y}{(x-\alpha_1 z)(x-\alpha_4 z)}, \qquad L_4 = K(E)(v_4).$$

Then the curves $C(L_0), C(L_1), C(L_2)$ and $C(L_3)$ are all distinct degree 2 covers of E ramified over P_1, P_2, P_3, P_4.

Proof. We will first calculate $\operatorname{div}(y/(x-\alpha_1 z)^2)$. The points that have $y = 0$ are P_1, P_2, P_3 and P_4 and setting $x - \alpha_1 z = 0$ gives us the equation $(y - h(\alpha_1, 1)/2)^2 = 0$. So,

$$\operatorname{div}(v_1^2) = \operatorname{div}\left(\frac{y}{(x-\alpha_1 z)^2}\right) = P_1 + P_2 + P_3 + P_4 - 4T_1.$$

Similarly, we find that

$$\operatorname{div}(v_2^2) = \operatorname{div}\left(\frac{y}{(x-\alpha_1 z)(x-\alpha_2 z)}\right) = P_1 + P_2 + P_3 + P_4 - 2T_1 - 2T_2.$$

$$\operatorname{div}(v_3^2) = \operatorname{div}\left(\frac{y}{(x-\alpha_1 z)(x-\alpha_3 z)}\right) = P_1 + P_2 + P_3 + P_4 - 2T_1 - 2T_3.$$

$$\operatorname{div}(v_4^2) = \operatorname{div}\left(\frac{y}{(x-\alpha_1 z)(x-\alpha_4 z)}\right) = P_1 + P_2 + P_3 + P_4 - 2T_1 - 2T_4.$$

We now remark that $\operatorname{div}(v_i^2/v_j^2) = 2T_j - 2T_i$. This means that v_j/v_i is not a square in $K(E)$ if $i \neq j$, so L_i and L_j give us distinct field extensions. So the four covers induced by the L_i are distinct

□

Remark 4.4.3. The cover corresponding to L_1 is the one given in 3.2.1.

One can find equations for the above covers explicitly using Riemann-Roch. We first remark that as $\deg(2T_1 + 2T_i) > 3$ we have that $l(2T_1 + 2T_i) = 4$. Now we have that

$$\frac{y}{(x-\alpha_1)(x-\alpha_i)}, \frac{x}{(x-\alpha_i z)}, \frac{x^2}{(x-\alpha_1 z)(x-\alpha_i z)} \text{ and } 1$$

form a basis of $L(2T_1 + 2T_i)$. And as $l(4T_1 + 4T_i) = 8$, we will have a linear dependence between the functions

$$\frac{y}{(x-\alpha_1 z)(x-\alpha_i z)}, \frac{y^2}{(x-\alpha_1 z)^2(x-\alpha_i z)^2}, \frac{x}{(x-\alpha_i z)}, \frac{x^2}{(x-\alpha_1 z)(x-\alpha_i z)},$$

$$\frac{x^3}{(x-\alpha_1 z)(x-\alpha_i z)^2}, \frac{x^4}{(x-\alpha_1 z)^2(x-\alpha_i z)^2}, \frac{yx}{(x-\alpha_1 z)(x-\alpha_i z)^2}, \frac{yx^2}{(x-\alpha_1 z)^2(x-\alpha_i z)^2} \text{ and } 1.$$

Setting $v = \frac{y}{(x-\alpha_1 z)(x-\alpha_i z)}$ and writing down the linear dependence explicitly, we will get an equation of the curve of the form

$$v^2 + v h_i(x,z) - f_i(x,z).$$

When we have this, the cover we are looking for will be given by:

$$v^4 + v^2 h_i(x,z) - f_(x,z).$$

Appendices

Bibliography

[1] H. Lange C. Birkenhake. Complex abelian varieties.

[2] M. Romagny C. Ritzenthaler. On the prym variety of genus 3 covers of genus 1 curves.

[3] D. Cantor. Computing the jacobian of a hyperelliptic curve.

[4] B. Moonen G. van der Geer. Abelian varieties.

[5] M.R. Gonzalez-Dorrego. (16,6) configurations and geometry of kummer surfaces in $\mathbb{P}^3$.

[6] S. Grushevsky. The schottky problem.

[7] K. Lauter C. Vincent J. Balakrishnan, S. Ionica. Constructing genus-3 hyperelliptic jacobians with cm.

[8] A. Amitsur J.P. Tignol. Symplectic modules.

[9] J.H. Silverman M. Hindry. Diophantine geometry.

[10] J.S. Müller. Explicit kummer surface formulas for arbitrary characteristic.

[11] D. Mumford. Abelian varieties.

[12] D. Mumford. Tata lectures on theta ii.

[13] C. Neurohr. Efficient integration on riemann surfaces and applications.

[14] C. Ritzenthaler R. Lercier. Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects.

[15] J. Sijsling R. Lercier, C. Ritzenthaler. Reconstructing plane quartic from their invariants.

Ehrenwörtliche Erklärung

Ich versichere hiermit, dass ich die Arbeit selbstständig angefertigt habe und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt sowie die wörtlich oder inhaltlich übernommenen Stellen als solche kenntlich gemacht habe.

Ulm, den

. . . .

Jeroen Hanselman