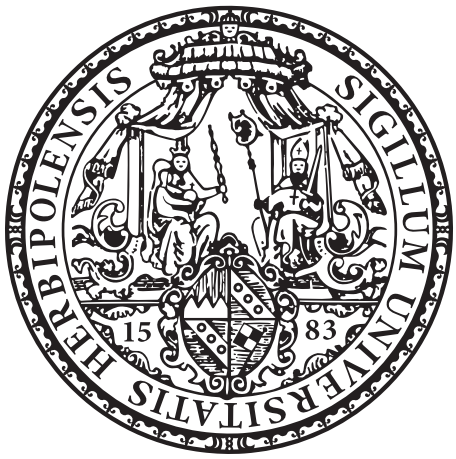
Computation of multi-branch-point covers and applications in Galois theory

Dissertation zur Erlangung des
naturwissenschaftlichen Doktorgrades
der Bayerischen Julius-Maximilians-Universität
Würzburg



vorgelegt von

Dominik Barth

Würzburg, 2022

Eingereicht am 22.02.2022
bei der Fakultät für Mathematik und Informatik
der Bayerischen Julius-Maximilians-Universität Würzburg.

Erster Gutachter: Prof. Dr. Peter Müller
Zweiter Gutachter: Prof. Dr. Michael Dettweiler

Acknowledgements

First and foremost, I would like to thank my supervisor Peter Müller for his guidance throughout the last years. This dissertation was only made possible by his excellent mathematical intuition.

My special gratitude goes to Andreas Wenz who was my research partner for the last six years. Thanks for many fruitful discussions and for carefully reading earlier versions of this work.

More thanks are due to Joachim König for collaborating with me on the project on computing polynomials with symplectic Galois groups. Also, his PhD thesis served me as an inexhaustible source of knowledge many times during my research.

Additionally, I would like to thank Stephan Elsenhans for valuable discussions on the verification of Galois groups and for sharing his Magma expertise with me.

Finally, I am grateful to the Magma team for quickly fixing several bugs reported by me; cf. the release notes for the versions `2.23-4`[1], `2.23-12`[2] and `2.25-5`[3]. Fixing these bugs greatly helped me with my computations.

Würzburg, February 2022 *Dominik Barth*

[1] `https://magma.maths.usyd.edu.au/magma/releasenotes/2/23/4`
[2] `https://magma.maths.usyd.edu.au/magma/releasenotes/2/23/12`
[3] `https://magma.maths.usyd.edu.au/magma/releasenotes/2/25/5`

Contents

Acknowledgements iii

Chapter 1. Introduction 1

Chapter 2. Theoretical background 3
2.1. Covers of the Riemann sphere 3
2.2. Monodromy and Galois theory 5
2.3. Families of covers and Hurwitz spaces 7
2.4. Curves on Hurwitz spaces 9

Chapter 3. Computation of families of covers 15
3.1. Main idea 15
3.2. Outline of our algorithm 17
3.3. An algorithm to compute genus-0 Belyi maps 21

Chapter 4. Verification techniques 31
4.1. Definitions and basic properties 31
4.2. Gathering information about subgroups of a Galois group 32
4.3. Reduction and specialization in function fields 37
4.4. Avoiding the classification of finite simple groups 39

Chapter 5. Computation of polynomials with symplectic Galois groups 43
5.1. Multi-parameter polynomials with Galois groups $\mathrm{PSp}_4(3).C_2$ and $\mathrm{PSp}_4(3)$ 43
5.2. Totally real polynomials with Galois group $\mathrm{PSp}_6(2)$ 49
5.3. Multi-parameter degree-36 polynomials with Galois group $\mathrm{PSp}_6(2)$ 56

Chapter 6. Families of polynomials with Galois groups $\mathrm{PSL}_4(3)$ and $\mathrm{PGL}_4(3)$ over $\mathbb{Q}(t)$ 63
6.1. Theoretical properties 63
6.2. A complex approximation of a single 4-point cover 64
6.3. Turning a single cover into a family 66
6.4. Verification 67
6.5. From $\mathrm{PGL}_4(3)$ to the index-2 subgroup $\mathrm{PSL}_4(3)$ 69

6.6. Polynomials with Galois group $\mathrm{Aut}(\mathrm{PGL}_4(3))$ 70

Chapter 7. A family of 4-point covers with monodromy group $\mathrm{PSL}_6(2)$ 73
7.1. Computation 73
7.2. Verification and Consequences 79
7.3. Extensions with Galois group $\mathrm{Aut}(\mathrm{PSL}_6(2))$ 83
7.4. Addendum: A Belyi map with monodromy group $\mathrm{PSL}_6(2)$ 84

Chapter 8. On Elkies' method to bound the transitivity degree of Galois groups 87
8.1. Preliminaries 87
8.2. A method by Elkies 88
8.3. New Applications 90

Bibliography 93

CHAPTER 1

Introduction

This dissertation deals with the explicit computation of (families of) multi-branch-point covers of $\mathbb{P}^1\mathbb{C}$ with prescribed ramification.

Such calculations are in several ways important for the inverse Galois problem. On the one hand, they yield explicit polynomials with interesting Galois groups. On the other hand, they sometimes seem to be necessary to decide existence problems that can not be answered by theoretical criteria alone: for example, the question whether a Hurwitz space contains rational points.

Techniques for such computations as well as examples of interest have been exhibited in several papers, notably Malle [**37**], Couveignes [**18**], Hallouin [**29**] and König [**33, 34**]. Methods used include Gröbner basis calculations (often referred to as "direct methods"), complex and p-adic deformation methods, interpolation techniques, Riemann–Roch space computations etc. Since direct methods become expensive quite quickly as the degree and number of branch points increase, an idea used extensively was the deformation of covers with small branch point number into covers with larger branch point number, ideally reducing the computation of a cover with many branch points to computation of covers with only three branch points. While this procedure has been applied successfully in several special cases, it also has obvious downsides, notably possible problems with numerical instability as well as its length in case of iterative application.

Here, we present an alternative approach, reducing the computation of Galois covers with group G and r branch points directly to the computation of 3-point covers. This comes at the cost of increasing the degree of the cover; however, in light of recent improvements regarding the calculation of 3-point covers (see the joint article [**11**] with Andreas Wenz), this is a price worth paying.

This dissertation is structured as follows: The required theoretical background will be established in Chapter 2, including covers of the Riemann sphere, their connection to Galois theory, families of covers parameterized by Hurwitz spaces, and the Hurwitz curves on them. Chapter 3 introduces the key idea of reducing multi-branch-point covers to those with three branch points, and

how this helps to compute an entire family of polynomials with prescribed Galois group. We also present the technique for computing high degree genus-0 Belyi maps used in the journal article [**11**] to calculate polynomials for several interesting Galois groups up to degree 280. Some verification techniques for Galois groups, in particular for 2-transitive Galois groups, are presented in Chapter 4.

In Chapter 5 we compute polynomials for several symplectic groups. More precisely, we present polynomials over $\mathbb{Q}(\alpha, t)$ for the primitive rank-3 groups $\mathrm{PSp}_4(3)$ and $\mathrm{PSp}_4(3).C_2$ of degree 27 and for the 2-transitive group $\mathrm{PSp}_6(2)$ in its actions on 28 and 36 points, respectively. Moreover, the degree-28 polynomial for $\mathrm{PSp}_6(2)$ admits infinitely many totally real specializations. Chapter 6 contains the first (to the best of our knowledge) explicit polynomials for the 2-transitive linear groups $\mathrm{PSL}_4(3)$ and $\mathrm{PGL}_4(3)$ of degree 40, and the imprimitive group $\mathrm{Aut}(\mathrm{PGL}_4(3))$ of degree 80. In Chapter 7 we negatively answer a question by Joachim König whether there exists a degree-63 rational function with rational coefficients and monodromy group $\mathrm{PSL}_6(2)$ ramified over at least four points. This is achieved due to the explicit computation of the corresponding hyperelliptic genus-3 Hurwitz curve parameterizing this family, followed by a search for rational points on it. As a byproduct of our calculations we obtain the first explicit $\mathrm{Aut}(\mathrm{PSL}_6(2))$-realizations over $\mathbb{Q}(t)$.

In the last and self-contained Chapter 8 we present a technique by Elkies for bounding the transitivity degree of Galois groups. This provides an alternative way to verify the Galois groups from the previous chapters and also yields a proof that the monodromy group of a degree-276 cover computed by Monien [**44**] is isomorphic to the sporadic 2-transitive Conway group Co_3.

CHAPTER 2

Theoretical background

This chapter contains the necessary theoretical background regarding covers of the Riemann sphere, their connection to Galois theory, families of covers parameterized by Hurwitz spaces, and the Hurwitz curves on them.

2.1. Covers of the Riemann sphere

We present some basic properties of covers of the Riemann sphere, see e.g. [**52**, Chapter 4] and [**36**, Chapter 1] as references.

DEFINITION 2.1. Let R and S be topological manifolds. An (unramified) *covering* from R to S is a surjective map $f : R \to S$ with the property that every $p \in S$ has a connected open neighbourhood U such that each of the connected components of $f^{-1}(U)$ is open and mapped homeomorphically onto U by f.

If S is connected, then all fibers $f^{-1}(p)$, $p \in S$, have the same number of elements. This common cardinality is called the *degree* of the covering and is denoted by $\deg(f)$.

An important property of a covering is its monodromy action, indeed it even determines the cover topologically.

DEFINITION 2.2. Let $f : R \to S$ be a degree-n covering and $p_0 \in S$ a base point. Then the topological fundamental group $\pi_1(S, p_0)$ acts on the fiber $f^{-1}(p_0)$ by lifting of paths, yielding the *monodromy action*

$$\pi_1(S, p_0) \to \operatorname{Sym} f^{-1}(p_0) \cong S_n$$

of f. The image of this action is called the *monodromy group* of the cover f. It is unique up to conjugation in S_n.

An important special case are coverings of the form $f : R \to \mathbb{P}^1\mathbb{C} \setminus P$ for some finite r-set $P = \{p_1, \ldots, p_r\}$. Such a cover can always be extended (in a unique way) to a *branched cover* of compact Riemann surfaces $X \to \mathbb{P}^1\mathbb{C}$. Conversely, a meromorphic function $f : X \to \mathbb{P}^1\mathbb{C}$ always restricts to an

(unramified) covering $X \setminus f^{-1}(P) \to \mathbb{P}^1\mathbb{C} \setminus P$ where P is the set of *branch points* of f; that is, the set of points having less than $\deg(f)$ preimages.

It is well known that the fundamental group of $\mathbb{P}^1\mathbb{C} \setminus \{p_1, \dots, p_r\}$ with base point $p_0 \notin \{p_1, \dots, p_r\}$ is generated by (the homotopy classes of) the paths $\gamma_1, \dots, \gamma_r$ where γ_i is a path winding counter-clockwise only around p_i (and no other p_j). Furthermore, we always assume that the p_i are ordered counter-clockwise such that the relation $\gamma_1 \cdots \gamma_r = 1$ holds. We remark that the group $\pi_1(\mathbb{P}^1\mathbb{C} \setminus \{p_1, \dots, p_r\}, p_0)$ is free of rank $r-1$, see [**38**, Theorem 1.1] where this theorem is attributed to Hurwitz.

DEFINITION 2.3. Let $X \to \mathbb{P}^1\mathbb{C}$ be a degree-n (branched) cover of compact Riemann surfaces with branch points $p_1, \dots, p_r$. Then the tuple of images $(\sigma_1, \dots, \sigma_r)$ of $(\gamma_1, \dots, \gamma_r)$ under the monodromy action of $\pi_1(\mathbb{P}^1\mathbb{C} \setminus \{p_1, \dots, p_r\})$ is called the *branch cycle description* of the cover.

The elements $\sigma_1, \dots, \sigma_r$ satisfy $\sigma_1 \cdots \sigma_r = 1$, generate a transitive group and are unique up to simultaneous conjugation in S_n.

Riemann's famous existence theorem, see [**36**, Theorem 1.8.14], asserts that for given elements $\sigma_1, \dots, \sigma_r$ having the above properties there always exists a (basically unique) cover with the prescribed branch cycle description:

THEOREM 2.4 (Riemann's existence theorem). *Let $\sigma_1, \dots, \sigma_r \in S_n$ such that $\sigma_1 \cdots \sigma_r = 1$ and $\sigma_1, \dots, \sigma_r$ generate a transitive subgroup of S_n. Then, for any given distinct $p_1, \dots, p_r \in \mathbb{P}^1\mathbb{C}$ there exists a ramified covering $f : X \to \mathbb{P}^1\mathbb{C}$ ramified over $p_1, \dots, p_r$ with branch cycle description $(\sigma_1, \dots, \sigma_r)$. Furthermore, f is unique up to isomorphism of covers: if $f' : X' \to \mathbb{P}^1\mathbb{C}$ is another such cover, then there is an isomorphism $i : X \to X'$ such that $f = f' \circ i$.*

The important Riemann–Hurwitz formula, see [**36**, Remark 1.2.21], relates the genus of the curve X to the branch cycle description of $f : X \to \mathbb{P}^1$.

THEOREM 2.5 (Riemann–Hurwitz genus formula). *Let $f : X \to \mathbb{P}^1$ be a meromorphic function of degree n with branch cycle description $(\sigma_1, \dots, \sigma_r)$. Then the genus g of the compact Riemann surface X is given by*

$$g = 1 - n + \frac{1}{2} \sum_{i=1}^{r} \operatorname{ind}(\sigma_i) \tag{2.1}$$

where $\operatorname{ind}(\sigma_i)$ is defined as n minus the number of cycles of $\sigma_i \in S_n$.

DEFINITION 2.6. A tuple $\sigma_1, \dots, \sigma_r \in S_n$ with $\sigma_1 \cdots \sigma_r = 1$ generating a transitive group will be called *genus-g tuple* where g is given by (2.1).

Obviously, knowledge of the cycle structures of $\sigma_1, \ldots, \sigma_r$ suffices to compute the genus g. Consequently, a class vector $C = (C_1, \ldots, C_r)$ consisting of conjugacy classes C_i of a group G will be called a *genus-g class vector* for G, when there exist $\sigma_i \in C_i$ such that $(\sigma_1, \ldots, \sigma_r)$ is a genus-g tuple generating G.

2.2. Monodromy and Galois theory

There is an important correspondence between covers of $\mathbb{P}^1\mathbb{C}$ and complex function fields of one variable, i.e., finite extensions of $\mathbb{C}(t)$:

A (branched) cover $f : X \to \mathbb{P}^1_t$ of compact Riemann surfaces naturally yields an extension $\mathbb{C}(X) \mid \mathbb{C}(\mathbb{P}^1_t) = \mathbb{C}(t)$ of their fields of meromorphic functions. The (topological) monodromy then translates into field-theoretic properties: The monodromy group of $f : X \to \mathbb{P}^1_t$ is isomorphic to the Galois group of (a Galois closure of) $\mathbb{C}(X) \mid \mathbb{C}(t)$. Furthermore, if f is ramified over $p_1, \ldots, p_r$ with branch cycle description $(\sigma_1, \ldots, \sigma_r)$, then the conjugacy class of σ_i is the class of inertia group generators of any extension of the ramified place $t \mapsto p_i$ in the Galois closure of $\mathbb{C}(X) \mid \mathbb{C}(t)$. Conversely, given a finite extension $L \mid \mathbb{C}(t)$ there always exists a compact Riemann surface X and a meromorphic function $f : X \to \mathbb{P}^1_t$ yielding the function field extension $L \mid \mathbb{C}(t)$ in the above sense.

Let G be a finite group. By choosing r sufficiently large we may assume that G admits a generating r-tuple satisfying the product-1 condition. Now, Riemann's existence theorem yields the existence of a cover $f : X \to \mathbb{P}^1_t$ having G as its monodromy group. Thus, G is the Galois group (of the Galois closure) of the function field extension $\mathbb{C}(X) \mid \mathbb{C}(t)$. Consequently, the inverse Galois problem for the field $\mathbb{C}(t)$ has a positive answer: every finite group occurs as a Galois group over $\mathbb{C}(t)$.

In order to tackle the inverse Galois problem for smaller fields we introduce some notion of *descent* meaning that the extension $\mathbb{C}(X) \mid \mathbb{C}(t)$ actually comes from a smaller extension $L \mid K(t)$ for some number field K. To preserve the geometric nature of the field extension it is natural to demand that $L \mid K(t)$ is *regular*:

DEFINITION 2.7. We call an extension $L \mid K(t)$ of function fields *regular* if K is algebraically closed in L; that is, when $L \cap \overline{K} = K$ holds.

A cover $f : X \to \mathbb{P}^1_t$ is called *Galois cover* if the corresponding field extension $\mathbb{C}(X) \mid \mathbb{C}(t)$ is a Galois extension.

DEFINITION 2.8 (see Section 3.1.1 in [**52**]). Let $f : X \to \mathbb{P}^1_t$ be a Galois cover with corresponding function field extension $\mathbb{C}(X) \mid \mathbb{C}(t)$. We say f (or

equivalently $\mathbb{C}(X) \mid \mathbb{C}(t)$) is *defined over a subfield* K of $\mathbb{C}$ if there exists a subfield L of $\mathbb{C}(X)$, Galois over $K(t)$ and regular over K with $[L : K(t)] = [\mathbb{C}(X) : \mathbb{C}(t)]$.

If f is defined over K, then the Galois groups of $\mathbb{C}(X) \mid \mathbb{C}(t)$ and $L \mid K(t)$ are naturally isomorphic, and in particular the monodromy group of f occurs regularly over K. Hilbert's famous irreducibility theorem then realizes G over the number field K.

Although some properties (such as the genus) carry over from $\mathbb{C}(X) \mid \mathbb{C}(t)$ to $L \mid K(t)$, a genus-0 function field over a non-algebraically closed constant field is no longer guaranteed to be rational. However, if the ramification of $L \mid K(t)$ is known, then it is sometimes possible to deduce the existence of a place of odd degree and, therefore, ensuring the rationality of $L \mid K(t)$. This yields a sufficient criterion, in the following usually referred to as *oddness condition*, for a genus-0 function field to be rational.

REMARK 2.9. Let $L \mid K(t)$ be a regular extension with branch cycle description $(\sigma_1, \dots, \sigma_r)$ and Galois group G. If $(\sigma_1, \dots, \sigma_r)$ is of genus 0 and for some $i = 1, \dots, r$

- at least one exponent in the cycle description of σ_i is odd, or
- the normalizer of the inertia group $\langle \sigma_i \rangle$ in G fixes a cycle of σ_i,

then [**38**, Theorem I.9.1] implies that the genus-0 function field L contains a divisor of odd degree. Consequently, L is a rational function field, see [**1**, Theorem XVI.7].

A necessary condition for descending to $\mathbb{Q}$ is given by Fried's branch cycle argument, see [**52**, Lemma 2.8] or [**33**, Lemma 3.3]. It roughly states that the absolute Galois group of $\mathbb{Q}$ acts on the ramification locus in the same way as it acts on the inertia classes where the latter action is given by the cyclotomic character.

THEOREM 2.10 (Fried's branch cycle argument). *Let $L \mid \mathbb{Q}(t)$ be a finite regular Galois extension with Galois group G of order n. For a ramified place $t \mapsto p$ let C_p denote the corresponding inertia class. Let ζ_n be a primitive n-th root of unity, and $\gamma \in \mathrm{Aut}(\overline{\mathbb{Q}} \mid \mathbb{Q})$, $m \in \mathbb{N}$ such that $\gamma^{-1}(\zeta_n) = \zeta_n^m$. Then the inertia class associated to $\gamma(p)$ is equal to $(C_p)^m$.*

In particular, the set of branch points is invariant under $\mathrm{Aut}(\overline{\mathbb{Q}} \mid \mathbb{Q})$.

COROLLARY 2.11. *Let $L \mid \mathbb{Q}(t)$ be as in the previous theorem with inertia class vector C. Then the following holds.*

(i) The class vector $C = (C_1, \dots, C_r)$ must necessarily be rational: *for all integers m coprime to the order of G the tuple $((C_1)^m, \dots, (C_r)^m)$ is a permutation of $(C_1, \dots, C_r)$.*

(ii) If C consists only of distinct rational classes, then all branch points are rational.

(iii) If $C = (C_1, C_1, C_2, C_3)$ with distinct rational conjugacy classes C_1, C_2, C_3, then either

- *all four branch points are rational, or*
- *the branch points corresponding to C_2 and C_3 are rational and the remaining two branch points (with inertia class C_1) are algebraically conjugate of degree 2.*

Recall that Riemann's existence theorem states that a G-cover is determined by its branch cycle description and its ramification locus. Although for a given group G the possible branch cycle descriptions of a given length are finite, the set of possible ramification loci is infinite.

This motivates the following question: What is a good choice for the ramification locus such that the field of definition becomes as small as possible? To answer this question one studies families of covers and their associated Hurwitz spaces, see the next two sections. In particular, we present a sufficient criterion for realizing a group G regularly over $\mathbb{Q}$, thus complementing the necessary conditions given in Theorem 2.10.

2.3. Families of covers and Hurwitz spaces

We present the basic definitions and results regarding families of covers and their Hurwitz spaces, see e.g. [**52**, Chapter 10], [**26**] or [**46**] for further details. A few sentences were taken over from the journal article [**4**] joint with Joachim König and Andreas Wenz.

Fix a finite group G and an integer $r \geq 3$ such that G can be generated by $r-1$ elements. Assume further that $Z(G) = 1$. Then, by Riemann's existence theorem the set of all Galois covers of $\mathbb{P}^1\mathbb{C}$ with Galois group G and with exactly r branch points is non-empty. The set of equivalence classes of these covers is denoted by $\mathcal{H}_r^{in}(G)$ (we refer to [**26**, Section 1.2] for the precise definition of the equivalence relation).

The set $\mathcal{H}_r^{in}(G)$ carries a natural topological structure, and also the structure of an algebraic variety, see [**26**, Theorem 1]. Finding rational points

on this variety is crucial when tackling the inverse Galois problem, see [**52**, Corollary 10.25] or [**24**, Theorem 4.3]:

THEOREM 2.12. *Let G be a finite group with $Z(G) = 1$. There is a unique family of ramified coverings $\mathcal{F} : \mathcal{T}_r(G) \to \mathcal{H}_r^{in}(G) \times \mathbb{P}^1$, such that for each $h \in \mathcal{H}_r^{in}(G)$, the fiber cover $\mathcal{F}^{-1}(h) \to \mathbb{P}^1$ is a ramified Galois cover with group G. This cover is defined regularly over a field $K \subseteq \mathbb{C}$ if and only if h is a K-rational point. In particular, the group G occurs regularly as a Galois group over $\mathbb{Q}$ if and only if $\mathcal{H}_r^{in}(G)$ has a rational point for some r.*

The search of rational points on $\mathcal{H}_r^{in}(G)$ in view of Theorem 2.12 leads to the problem of finding the (absolutely) irreducible components of $\mathcal{H}_r^{in}(G)$ defined over $\mathbb{Q}$.

The main tool to answer this question is the monodromy action of the *branch point reference map*

$$\Psi : \mathcal{H}_r^{in}(G) \to \mathcal{U}_r$$

mapping a cover to its ramification locus, where $\mathcal{U}_r$ denotes the space of (unordered) r-sets in $\mathbb{P}^1$. In order to understand the monodromy of Ψ we first need a description of the fundamental group of $\mathcal{U}_r$, the Hurwitz braid group:

DEFINITION 2.13. The *Hurwitz braid group* $\mathcal{B}_r$ is the group generated by elements $\beta_1, \dots, \beta_{r-1}$ satisfying the following relations:

(i) $\beta_i\beta_{i+1}\beta_i = \beta_{i+1}\beta_i\beta_{i+1}$ for $i = 1, \dots, r-2$,
(ii) $\beta_i\beta_j = \beta_j\beta_i$ for $|i-j| \geq 2$,
(iii) $\beta_1\beta_2 \cdots \beta_{r-1}\beta_{r-1}\beta_{r-2} \cdots \beta_1 = 1$.

After fixing a base point $p_0 \in \mathcal{U}_r$, for example, $p_0 = \{1, 2, \dots, r\}$, it is well known that the fundamental group of $\mathcal{U}_r$ is isomorphic to $\mathcal{B}_r$:

$$\pi_1(\mathcal{U}_r, p_0) \cong \mathcal{B}_r.$$

By identifying a cover with its branch cycle description, Riemann's existence theorem implies that the fiber $\Psi^{-1}(p_0)$ consisting of all G-covers with ramification locus p_0 is parameterized by $\mathcal{E}_r^{in}(G) := \mathcal{E}_r(G)/\operatorname{Inn}(G)$ where

$$\mathcal{E}_r(G) := \{(\sigma_1, \dots, \sigma_r) \in (G \setminus \{1\})^r \mid \sigma_1 \cdots \sigma_r = 1, \langle \sigma_1, \dots, \sigma_r \rangle = G\}$$

and $\operatorname{Inn}(G)$ acts by conjugating the tuples simultaneously. Through this translation the monodromy action of $\pi_1(\mathcal{U}_r, p_0) \cong \mathcal{B}_r$ on $\Psi^{-1}(p_0)$ is as follows:

$$(\sigma_1, \dots, \sigma_r)^{\beta_i} := (\sigma_1, \dots, \sigma_{i-1}, \sigma_{i+1}, \sigma_i^{\sigma_{i+1}}, \dots, \sigma_r), \quad i = 1, \dots, r-1. \tag{2.2}$$

By basic covering theory the connected components of $\mathcal{H}_r^{in}(G)$ now correspond to the orbits of $\mathcal{B}_r$ on $\mathcal{E}_r^{in}(G)$ — which can be computed in a purely group-theoretical way by using the braiding operations defined in (2.2).

An important invariant of a component of $\mathcal{H}_r^{in}(G)$, or equivalently of an orbit of the braid group on $\mathcal{E}_r^{in}(G)$, is the unordered tuple of conjugacy classes of the elements σ_i in the branch cycle description $(\sigma_1, \ldots, \sigma_r) \in \mathcal{E}_r(G)$. This motivates the following definition.

DEFINITION 2.14. Let $C = (C_1, \ldots, C_r)$ be a class vector of G; that is, a tuple of non-trivial conjugacy classes of G. We define the *Nielsen class* $\mathrm{Ni}(C)$ of C to be the set of all $(\sigma_1, \ldots, \sigma_r) \in \mathcal{E}_r(G)$ such that there exists a permutation $\pi \in S_r$ with the property $\sigma_i \in C_{\pi(i)}$ for all $i \in \{1, \ldots, r\}$. Furthermore, we define the *straight Nielsen class* $\mathrm{SNi}(C)$ to be the subset of $\mathrm{Ni}(C)$ by forcing $\pi = \mathrm{id}$ (i.e., $\sigma_i \in C_i$ for all i). Factoring out $\mathrm{Inn}(G)$ yields the definitions of $\mathrm{Ni}^{in}(C)$ and $\mathrm{SNi}^{in}(C)$, the *inner Nielsen class* and *straight inner Nielsen class*, respectively.

Accordingly we define the (inner) *Hurwitz space* $\mathcal{H}^{in}(C)$ to be the union of all components of $\mathcal{H}_r^{in}(G)$ that correspond to the class vector C. From now on we assume that $\mathcal{B}_r$ acts transitively on $\mathrm{Ni}^{in}(C)$ and, consequently, that $\mathcal{H}^{in}(C)$ is connected. A necessary and sufficient condition for $\mathcal{H}^{in}(C)$ to be defined over $\mathbb{Q}$ is that C is a rational class vector, see Corollary 2.11 for the definition of rationality. Since we are only interested in Hurwitz spaces defined over $\mathbb{Q}$, we always assume that our class vector C is rational.

These conditions together with $Z(G) = 1$ imply that $\mathcal{H}^{in}(C)$ is an absolutely irreducible variety defined over $\mathbb{Q}$. Denoting the restriction of the branch point reference map to $\mathcal{H}^{in}(C)$ again by Ψ we have a cover

$$\Psi : \mathcal{H}^{in}(C) \to \mathcal{U}_r$$

of degree $|\mathrm{Ni}^{in}(C)|$ with monodromy given by the (transitive) action of $\mathcal{B}_r$ on $\mathrm{Ni}^{in}(C)$.

2.4. Curves on Hurwitz spaces

In order to find rational points on the r-dimensional Hurwitz spaces a common strategy is to study certain curves on them. Using theoretical criteria the inspected curves sometimes turn out to be rational and consequently contain lots of rational points. We only study "standard curves" obtained by fixing all but one branch point. A more sophisticated approach is described by Dettweiler **[21]**.

Of particular importance is the case of four branch points, as it turns out that for $r = 4$ the question of existence for rational points on Hurwitz spaces often can be answered completely by considering suitable curves on them:

REMARK 2.15. Suppose $C = (C_1, C_2, C_3, C_4)$ with distinct rational conjugacy classes $C_1, \dots, C_4$ and assume that there exists a cover f of $\mathbb{P}^1$ with class vector C that is defined (regularly) over $\mathbb{Q}$.

Under the given conditions Corollary 2.11 implies that all branch points of f are rational, i.e., f is ramified over $p_1, \dots, p_4 \in \mathbb{P}^1\mathbb{Q}$. Applying an outer Möbius transformation $\mu \in \mathbb{Q}(X)$ mapping p_1, p_2, p_3 to $0, 1, \infty$ (in this order) we obtain a cover $\mu \circ f$ ramified over $0, 1, \infty, \lambda$ for some $\lambda \in \mathbb{Q} \setminus \{0, 1\}$. Of course, $\mu \circ f$ is still defined over $\mathbb{Q}$.

So we have seen that the 4-dimensional variety $\mathcal{H}^{in}(C)$ has a rational point if and only if the curve $\mathcal{C}$ on $\mathcal{H}^{in}(C)$ consisting of all covers with branch point locus of the form $0, 1, \infty, \lambda$ has a rational point. In the following we will describe how properties of $\mathcal{C}$ such as the genus can be computed, sometimes guaranteeing the existence of rational points by purely theoretical criteria.

Let $C = (C_1, \dots, C_r)$ be a class vector with distinct conjugacy classes $C_1, \dots, C_r$ of a finite group G with non-empty Nielsen class. Then, the branch point reference map $\Psi : \mathcal{H}^{in}(C) \to \mathcal{U}_r$ from Section 2.3 factors through the space $\mathcal{U}^r$ of ordered r-sets of $\mathbb{P}^1$ as follows

$$\mathcal{H}^{in}(C) \stackrel{\Psi'}{\to} \mathcal{U}^r \to \mathcal{U}_r,$$

where the cover $\Psi' : \mathcal{H}^{in}(C) \to \mathcal{U}^r$ has degree $|\mathrm{SNi}^{in}(C)|$ and its monodromy is given by the action of $\pi_1(\mathcal{U}^r)$ on $\mathrm{SNi}^{in}(C)$.

Of course, the fundamental group of $\mathcal{U}^r$ is the subgroup of $\mathcal{B}_r$ consisting exactly of those braids that fix all branch points. It is called the *pure braid group* and is generated by the elements

$$\beta_{i,j} := (\beta_i^2)^{\beta_{i+1}^{-1} \cdots \beta_{j-1}^{-1}} \text{ for } 1 \le i < j \le r.$$

Now restrict to the case $r = 4$. Motivated by Remark 2.15 we study the curve

$$\mathcal{C} := \Psi'^{-1}(\{(0, 1, \infty, \lambda) \mid \lambda \in \mathbb{C} \setminus \{0, 1\}\})$$

on $\mathcal{H}^{in}(C)$ consisting of all G-covers with ramification as follows:

branch point	0	1	∞	λ
inertia class	C_1	C_2	C_3	C_4

The branch point reference map $\Psi' : \mathcal{H}^{in}(C) \to \mathcal{U}^r$ restricts to a Belyi map $\Psi' : \mathcal{C} \to \mathbb{P}^1_\lambda$ ramified over $0, 1, \infty$ with branch cycle description

$$(\tilde{\beta}_1, \tilde{\beta}_2, \tilde{\beta}_3) := (\beta_{1,4}, \beta_{2,4}, \beta_{3,4}), \tag{2.3}$$

see [**38**, Section III.5.2]. Geometrically, the braid group element $\beta_{i,4}$, $i = 1, 2, 3$, can be interpreted as moving the fourth branch point λ around the i-th (fixed) branch point (one of $0, 1, \infty$).

Apart from the case where C_1, C_2, C_3, C_4 are distinct the only other case occurring in the work at hand is the following: $C = (C_1, C_1, C_2, C_3)$ with distinct and rational classes C_1, C_2, C_3. Here, we consider the curve $\mathcal{C}$ on $\mathcal{H}^{in}(C)$ consisting of covers with ramification as follows:

branch point	$1 - \sqrt{\lambda}$	$1 + \sqrt{\lambda}$	0	∞
inertia class	C_1	C_1	C_2	C_3

Again, restriction of the branch point reference map yields a Belyi map $\Psi' : \mathcal{C} \to \mathbb{P}^1_\lambda$ with branch cycle description

$$(\tilde{\beta}_1, \tilde{\beta}_2, \tilde{\beta}_3) := (\beta_{1,4}, \beta_1\beta_{1,4}, \beta_1) \tag{2.4}$$

in their action on the straight inner Nielsen class $\mathrm{SNi}^{in}(C)$, see [**38**, Theorem III.7.8].

In both cases we refer to $\mathcal{C}$ as the *Hurwitz curve* corresponding to C; in the literature the term *reduced Hurwitz space* is also used.

A sufficient criterion for realizing G over $\mathbb{Q}$. Knowledge of the branch cycle description $(\tilde{\beta}_1, \tilde{\beta}_2, \tilde{\beta}_3)$ of $\Psi' : \mathcal{C} \to \mathbb{P}^1_\lambda$ is very useful, e.g., for computing the genus of $\mathcal{C}$ and potentially deducing the rationality of $\mathcal{C}$. We outline a useful application to the inverse Galois problem:

Assume that C is a rational class vector and that $(\tilde{\beta}_2, \tilde{\beta}_2, \tilde{\beta}_3)$ as defined above is a genus-0 triple in its action on $\mathrm{SNi}^{in}(C)$. Then, as $(\tilde{\beta}_2, \tilde{\beta}_2, \tilde{\beta}_3)$ is the branch cycle description of the cover $\mathcal{C} \to \mathbb{P}^1_\lambda$, the genus of $\mathcal{C}$ turns out to be 0 by the Riemann–Hurwitz formula. If, in addition, $(\tilde{\beta}_2, \tilde{\beta}_2, \tilde{\beta}_3)$ fulfils an oddness condition as described in Remark 2.9, then $\mathcal{C}$ is a $\mathbb{Q}$-rational curve. In particular, in this case, $\mathcal{C}$ contains lots of rational points leading to infinitely many regular realizations of G over $\mathbb{Q}$. Note that this criterion is of purely theoretical nature and works without explicitly computing a single cover of the family. A particular simple special case occurs when C is a *rigid* class vector, i.e., when $|\mathrm{SNi}^{in}(C)| = 1$ holds. Then, $\mathcal{C} \cong \mathbb{P}^1_\lambda$ is of course rational.

In the following cases, however, we can not deduce the existence of rational points a priori:

- The genus of $\mathcal{C}$ is 0, but the triple $(\tilde{\beta}_2, \tilde{\beta}_2, \tilde{\beta}_3)$ does not satisfy an oddness condition. Here, $\mathcal{C}$ is a conic but possibly without rational points.
- The genus of $\mathcal{C}$ is larger than 0.

In both cases it seems necessary to compute explicit equations for $\mathcal{C}$ in order to search for rational points on $\mathcal{C}$. This approach is carried out in Chapter 6 for the group $\mathrm{PSL}_4(3)$ where $\mathcal{C}$ is of genus 0 not satisfying an oddness condition, and in Chapter 7 for the group $\mathrm{PSL}_6(2)$ where $\mathcal{C}$ is hyperelliptic of genus 3.

Hurwitz curves and the function field setting. For the explicit computation of multi-parameter polynomials with prescribed Galois group it is important to know how Hurwitz curves translate into the function field setting. This will be outlined in the following.

Restricting the universal family $\mathcal{T}_r(G)$ from Theorem 2.12 to the Hurwitz curve $\mathcal{C}$ consisting only of G-covers with class vector C and branch point set $0, 1, \infty, \lambda$ (or $1 \pm \sqrt{\lambda}, 0, \infty$, respectively), we obtain the following varieties and morphisms:

$$\mathcal{T}_{\mathcal{C}} \xrightarrow{|G|} \mathcal{C} \times \mathbb{P}^1_t \xrightarrow{|\mathrm{SNi}^{in}(C)|} \mathbb{P}^1_\lambda \times \mathbb{P}^1_t$$

In the function field setting this gives us[1]

$$\mathbb{Q}(\mathcal{T}_{\mathcal{C}}) > \mathbb{Q}(\mathcal{C})(t) > \mathbb{Q}(\lambda)(t)$$

where $\mathbb{Q}(\mathcal{T}_{\mathcal{C}})$ is Galois over $\mathbb{Q}(\mathcal{C})(t)$ with group G. The main goal in the following chapters is to compute explicit defining equations for $\mathcal{C}$ and the extension $\mathbb{Q}(\mathcal{T}_{\mathcal{C}}) \mid \mathbb{Q}(\mathcal{C})(t)$. More precisely, assume G acts transitively and faithfully on n elements, then we usually compute the degree-n minimal polynomial $f \in \mathbb{Q}(\mathcal{C})(t)[X]$ for some primitive element of the fixed field K of a point stabilizer.

The genus of K can be computed by applying the Riemann–Hurwitz genus formula for function fields, see [**48**, Corollary 3.4.14], to elements in the class vector C in their action of degree n. In all of our cases K turns out to have genus 0. Furthermore, in all examples presented in the thesis the rationality of the function field K can be deduced a priori via an oddness condition as described in Remark 2.9.

[1]Under our general assumptions that C is rational, $Z(G) = 1$, and $\mathcal{B}_r$ acts transitively on $\mathrm{Ni}^{in}(C)$.

Now assume $K \mid \mathbb{Q}(\mathcal{C})(t)$ is rational, i.e., $K = \mathbb{Q}(\mathcal{C})(x)$ for some $x \in K$. Then there exist coprime polynomials $p, q \in \mathbb{Q}(\mathcal{C})[X]$ such that $t = p(x)/q(x)$. In particular, the degree-n polynomial

$$f := p(X) - tq(X) \in \mathbb{Q}(\mathcal{C})(t)[X]$$

defines a regular Galois extension of $\mathbb{Q}(\mathcal{C})(t)$ with Galois group G and class vector C. The explicit computation of p, q and $\mathcal{C}$ is the main goal in this thesis and methods for it are presented in the next chapter.

CHAPTER 3

Computation of families of covers

We describe the method used for the explicit computation of families of 4-point covers for the examples presented in this thesis. More precisely, assume we are given a class vector C of length 4 for a transitive group $G \leq S_n$ with the following properties:

(i) $Z(G) = 1$,
(ii) C is of genus 0 and fulfils an oddness condition as stated in Remark 2.9,
(iii) $\mathrm{Ni}^{in}(C)$ is non-empty and $\mathcal{B}_4$ acts transitively on it,
(iv) either $C = (C_1, C_2, C_3, C_4)$ with distinct rational classes C_1, C_2, C_3, C_4 or $C = (C_1, C_1, C_2, C_3)$ with distinct rational classes C_1, C_2, C_3.

Then, by the theory of Hurwitz spaces as explained in Chapter 2, there exist an absolutely irreducible curve $\mathcal{C}$ defined over $\mathbb{Q}$ — the inner Hurwitz curve — and coprime polynomials $p, q \in \mathbb{Q}(\mathcal{C})[X]$ such that $p(X) - tq(X)$ has regular Galois group G over $\mathbb{Q}(\mathcal{C})(t)$. Furthermore, $p(X) - tq(X)$ parameterizes all covers $\mathbb{P}^1\mathbb{C} \to \mathbb{P}^1\mathbb{C}$ with class vector C ramified over $0, 1, \infty, \lambda$ or $1 \pm \sqrt{\lambda}, 0, \infty$ for $\lambda \in \mathbb{C} \setminus \{0, 1\}$.

In this chapter we describe an approach by Joachim König, Andreas Wenz and the author on how to compute defining equations for $\mathcal{C}$ as well as the polynomials $p, q \in \mathbb{Q}(\mathcal{C})[X]$. This algorithm was previously outlined in the journal article [**4**] from which some passages in the following chapter have been taken. The approach heavily makes use of the fact that recently powerful methods to compute Belyi maps were developed, see for example [**11**] or [**53**].

3.1. Main idea

3.1.1. Reducing to Belyi maps. Recall that a covering $f : X \to \mathbb{P}^1\mathbb{C}$ is called a *Belyi map* if it is unramified outside of $\{0, 1, \infty\}$. Belyi's famous theorem asserts that every compact Riemann surface which can be defined over $\overline{\mathbb{Q}}$ admits a Belyi map to $\mathbb{P}^1$. Belyi's proof uses a clever composition of covers, successively reducing the number of branch points. It was first suggested to us by Peter Müller to use such an idea to reduce calculation of multi-branch-point

covers to Belyi maps. This can be achieved efficiently due to the following result.

PROPOSITION 3.1. *Let $r \geq 3$, and let $C = (C_1, \ldots, C_r)$ be a class vector for the finite group G with non-empty Nielsen class* $\mathrm{Ni}(C)$. *Then for every Belyi map $g : \mathbb{P}^1\mathbb{C} \to \mathbb{P}^1\mathbb{C}$ of degree at least $r-2$, there exists a cover $f : X \to \mathbb{P}^1\mathbb{C}$ of type C such that $g \circ f : X \to \mathbb{P}^1\mathbb{C}$ is a Belyi map. Furthermore, $r-2$ is the minimal degree with this property.*

PROOF. Assume that g is as above with $\deg(g) \geq r-2$. From the Riemann–Hurwitz genus formula, it follows that the set $g^{-1}(\{0, 1, \infty\}) \subset \mathbb{P}^1$ is of cardinality exactly $\deg(g)+2 \geq r$. Using Riemann's existence theorem, we may pick a cover $f : X \to \mathbb{P}^1$ of type C ramified only inside $g^{-1}(\{0, 1, \infty\})$. By construction, $g \circ f$ is then unramified outside $\{0, 1, \infty\}$. Conversely, if $\deg(g) < r-2$, then the above shows that any cover of type C has to be ramified at some point outside $g^{-1}(\{0, 1, \infty\})$, implying that $g \circ f$ is not a Belyi map. □

The point of Proposition 3.1 is that, assuming that we have an efficient algorithm to compute explicit equations for Belyi maps with a prescribed ramification type, we automatically get, as a component of the resulting map $g \circ f$, an explicit equation for *some* cover in a prescribed family with more than three branch points. The technique for computation of Belyi maps which we use (see Section 3.3) has been developed by Andreas Wenz and the author, and has previously been applied to calculate Belyi maps with interesting monodromy groups of degree up to 280 (see **[5]**, **[6]**, **[7]**, **[8]**, **[11]** and **[53]**). Of course, any other method that allows the computation of high degree Belyi maps works as well. Alternative approaches for computing Belyi maps are discussed in **[47]**, **[45]**, **[51]**, **[31]**, **[42]**, **[43]** and **[44]**.

3.1.2. Comparison with previous approaches. There have been many previous papers on the computation of families of covers, notably by Malle (**[37]**), Couveignes (**[18]**) and König (**[33]**, **[34]**). In these, either the permutation degree of the group in question is sufficiently low to allow finding an equation for at least one cover of the prescribed ramification type "directly" (e.g., via a Gröbner basis approach, or via brute-force search modulo a small prime, followed by p-adic lifting), or the starting point of the calculation is an $(r-1)$-point cover with monodromy $(\sigma_1\sigma_2, \sigma_3, \ldots, \sigma_r)$, which is then deformed into an r-point cover with monodromy $(\sigma_1, \ldots, \sigma_r)$ — possibly iteratively, to eventually get from a 3-point cover to an r-point one. Unless the permutation degree and the number of branch points are "small", these methods have obvious

downsides. Firstly, direct methods like the Gröbner basis approach become very expensive as the number of variables (which is roughly the permutation degree times $r-2$, where r is the number of branch points) grows.[1] Also, for $r \geq 5$, the iterated deformation process to obtain a larger number of branch points is quite time-consuming. Finally, the complex deformation techniques turn out to be numerically rather delicate in many cases. Especially where there is no *transitive* tuple $(\sigma_1\sigma_2, \sigma_3, \ldots, \sigma_r)$ available, experiments by Joachim König showed numerically unstable behaviour in many examples. The main improvement in the use of Proposition 3.1 — which can be considered a "vertical" approach (going from three to many branch points by composing covers on top of each other), compared to the "horizontal" one of deformation and moving branch points in $\mathbb{P}^1$ — is to circumvent the lengthy process of deformation and get directly into the prescribed family of r-point covers, after which the remaining calculations are rather smooth. The obvious price is that the degree of the initial Belyi map is increased by a factor of $r-2$. However, due to the far-developed methods in computation of Belyi maps, this is (often) worth the effort.

3.2. Outline of our algorithm

Here, we give a brief description of our algorithmic application of Proposition 3.1 to compute explicit equations for the Hurwitz curve $\mathcal{C}$ and polynomials $p, q \in \mathbb{Q}(\mathcal{C})[X]$ that parameterize covers with class vector C. The algorithm can be divided into the following parts:

(1) We obtain a *single* multi-branch-point cover of ramification type C
(2) and interpolate the whole Hurwitz curve $\mathcal{C}$ starting from the single cover computed in (1).

In the first part the number r of branch points is arbitrary, while the second part is described only for the case $r = 4$ since we have introduced the notions of (reduced) Hurwitz spaces and Hurwitz curves only for $r = 4$. However, one could iterate the second step to obtain Hurwitz spaces of higher dimensions.

[1]While it is of course not possible to give a precise bound, computations with 3 branch points are generally considered feasible for a degree into the 20s, and correspondingly lower degree for a larger branch point number.

3.2.1. A complex approximation of a single r-point cover.

Step 1: Finding the monodromy for a suitable Belyi map. We are given a class r-tuple $C = (C_1, \dots, C_r)$ of a group G. We choose $g : \mathbb{P}^1 \to \mathbb{P}^1$ to be the cyclic cover $g : x \mapsto x^{r-2}$, ramified only at 0 and ∞. We then compute a triple $(\sigma_0, \sigma_1, \sigma_\infty)$ corresponding to a Belyi map $g \circ f$ as in Proposition 3.1. This can be done rather easily by observing some elementary group-theoretical invariants of such a cover $g \circ f$. In particular,

(i) its Galois group embeds naturally into the imprimitive wreath product $G \wr C_{r-2} = G^{r-2} \rtimes C_{r-2}$, with C_{r-2} permuting the copies of G cyclically.
(ii) Its monodromy $(\sigma_0, \sigma_1, \sigma_\infty)$ has the following properties: σ_0^{r-2} (resp., σ_∞^{r-2}) is an element of G^{r-2} projecting into class C_1 (resp., C_r) in every copy of G; and σ_1 is an element of $C_2 \times \cdots \times C_{r-1} \subseteq G^{r-2}$.

Indeed, the embedding of the Galois group in (i) is an elementary fact in Galois theory, see Section 14.2 in **[19]**; in the same way, (ii) follows directly from our choice of branch points and inertia group generators in Proposition 3.1.

Permutation triples fulfilling the above conditions are then found via computer search.

Step 2: Computation of the Belyi map. Using the permutation triple $(\sigma_0, \sigma_1, \sigma_\infty)$ from the first step, we calculate a complex approximation of an equation $F(u, X) = 0$ (with $F \in \mathbb{C}[u, X]$) for the underlying Belyi map $g \circ f$. Using the definition of g, we can set $u = t^{r-2}$ and factor F over $\mathbb{C}[t]$, which gives us an approximate equation for the (r-point) subcover $f : X \to \mathbb{P}^1$ as described in Proposition 3.1.

Especially for this step, we refer to Section 3.3 for details where our method to compute Belyi maps is described.

3.2.2. Turning a single cover into a family. In the following, we describe how to obtain an equation for the entire universal family starting from a single member. This part of the computation is relatively "routine", see e.g. previous occurrences in **[34]**.

To simplify the exposition we only describe the case where the class vector $C = (C_1, C_2, C_3, C_4)$ consists of distinct rational classes C_i and $\mathcal{C}$ parameterizes covers ramified over $0, 1, \infty, \lambda$. The case of partially ordered ramification locus $1 \pm \sqrt{\lambda}, 0, \infty$ can be carried out analogously with minor changes.

Recall, there exists a polynomial $f \in \mathbb{Q}(\mathcal{C})(t)[X]$ with Galois group G that parameterizes (through specialization at points on $\mathcal{C}$) the universal family $\mathcal{T}_\mathcal{C} \to \mathcal{C} \times \mathbb{P}^1_t$ of all covers with class vector C and ramified over $0, 1, \infty, \lambda$. As

C is assumed to be of genus 0 and to satisfy an oddness condition as described in Remark 2.9, the root field of f is rational. Thus, we may assume that f is linear in t, i.e., $f(t, X) = p(X) - tq(X)$ with coprime $p, q \in \mathbb{Q}(\mathcal{C})[X]$.

The ramification at the places $t \mapsto 0$ and $t \mapsto \infty$ implies an inseparability behaviour of p and q of the following form (see e.g. [**33**, Lemma 3.6]):

$$f(t, X) = p_1^{e_1} \cdots p_r^{e_r} - tq_1^{m_1} \cdots q_s^{m_s},$$

where p_i and q_i are separable and pairwise coprime polynomials in $\mathbb{Q}(\mathcal{C})[X]$. Analogously, the ramification indices at 1 and λ yield similar conditions on the factorizations of $f(1, X)$ and $f(\lambda, X)$, respectively.

Since a generator of the (rational!) root field of $f(t, X)$ is only unique up to PGL_2-action, we may apply Möbius transformations in X to assert certain *normalization conditions*:

> In all examples discussed in this thesis, it is a priori clear that at least one place lying above $t \mapsto 0$ or $t \mapsto \infty$ is rational, and, consequently, can and will be assumed to lie at $X \mapsto \infty$. Afterwards, if possible, some linear translation $X \mapsto aX + b$ is applied to fix the traces of two of the polynomials p_i or q_i to be 0 and 1, respectively; see also [**33**, Lemma 3.9].

Up to Möbius transformation, the computed genus-0 Belyi map F (from the first part 3.2.1) of degree $2n$ is of the form $f_0(X)^2$ with a rational function f_0 of degree n having the four branch points $0, 1, \infty, -1$, monodromy group G and the prescribed ramification type C. We now apply an inner Möbius transformation to f_0 such that f_0 satisfies the aforementioned normalization conditions. Then, we use f_0 as a starting point to compute the Hurwitz curve $\mathcal{C}$ of all covers with ramification type (C_1, C_2, C_3, C_4) and branch points $0, 1, \infty, \lambda$, with $\lambda \in \mathbb{C} \setminus \{0, 1\}$, by assembling equations for many fiber covers $\mathcal{T}_{\mathcal{C}}(h) \to \mathbb{P}^1$ in our universal family.

This can be done by complex deformation techniques, slowly increasing the parameter λ and using Newton approximation to adjust the coefficients of f_0. The point is that this is numerically stable, since the starting point is already a cover with 4 sufficiently separated branch points, leading to a sufficiently "far from singular" matrix in Newton's method.[2]

As $\mathbb{Q}(\mathcal{C})$ is of transcendence degree 1, two "random" (non-constant) coefficients of f can usually be expected to generate the entire function field $\mathbb{Q}(\mathcal{C})$.

[2]Of course, this observation should be understood as a qualitative statement, not something that can be quantified in generality.

We use this and let a coefficient β (of one of the polynomials p_i or q_i) converge to a rational value, using Newton approximation. Then any further coefficient γ will converge to an algebraic number of degree at most $[\mathbb{Q}(\beta,\gamma) : \mathbb{Q}(\beta)]$ (which is bounded by the index of $\mathbb{Q}(\beta)$ in the function field of the Hurwitz curve), and given a sufficient complex precision, we can recognize this algebraic number γ using the LLL algorithm. Doing this for several rational values of β, we obtain by interpolation the algebraic dependency between β and γ (viewed as transcendentals) parameterizing the function field of our Hurwitz curve $\mathcal{C}$, i.e., $\mathbb{Q}(\mathcal{C}) = \mathbb{Q}(\beta,\gamma)$.

The remaining steps depend on whether the curve $\mathcal{C}$ is birationally isomorphic to $\mathbb{P}^1$.

(i) If $\mathcal{C}$ is a rational curve, we use Riemann–Roch space computations as explained in **[33**, Lemma 3.16] to explicitly obtain a parameter α with $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta,\gamma)$. Next, we use Newton approximation again to let α converge to several rational values. Then all the coefficients of the p_i and q_i must also be rational values and can easily be recognized from their complex approximations by using continued fractions. Interpolating between these several values once again yields dependencies between α and each coefficient, i.e., expressions of each coefficient as a rational function in α. This, finally, yields a multi-parameter polynomial $f(\alpha,t,X) \in \mathbb{Q}(\alpha,t)[X]$.

(ii) If $\mathcal{C}$ is not rational (for example, if the genus of $\mathcal{C}$ is non-zero) one may at least try and search for rational points on $\mathcal{C}$ (possibly after obtaining a nicer equation for $\mathcal{C}$ using Riemann–Roch space computations) leading to covers of the prescribed ramification type defined over $\mathbb{Q}$, cf. Theorem 2.12.

In Chapter 7, we carry out this approach for the group $\mathrm{PSL}_6(2)$ where $\mathcal{C}$ turns out to be a hyperelliptic genus-3 curve unfortunately having no (unramified) rational points.

In the above algorithm recognizing algebraic numbers from their complex approximations can be quite tedious, especially if their degrees become large. Therefore, we conclude with some remarks on how to reduce the degrees of the algebraic numbers occurring in the algorithm.

As mentioned before, when letting β converge to a rational value, all other coefficients converge to algebraic numbers of degree at most $[\mathbb{Q}(\mathcal{C}) : \mathbb{Q}(\beta)]$ for which no a priori bound can be given. However, for the particular choice of $\beta := \lambda$, we have an explicit upper bound of $[\mathbb{Q}(\mathcal{C}) : \mathbb{Q}(\lambda)] = |\operatorname{SNi}^{in}(C)|$ making

λ a good choice for β when the straight inner Nielsen class is small. Additionally, if the branch point reference map $\Psi : \mathcal{C} \to \mathbb{P}^1_\lambda$ is indecomposable (which can be decided by checking its monodromy group $\langle \tilde{\beta}_1, \tilde{\beta}_2, \tilde{\beta}_3 \rangle$ for primitivity), we already know that λ together with any other coefficient γ not contained in $\mathbb{Q}(\lambda)$ generates the full function field $\mathbb{Q}(\mathcal{C})$.

However, sometimes the imprimitivity of $\Psi : \mathcal{C} \to \mathbb{P}^1_\lambda$ may be even more valuable than the primitivity: In the following we outline an approach to reduce the degrees of the algebraic numbers provided the branch point reference map $\Psi : \mathcal{C} \to \mathbb{P}^1_\lambda$ has a genus-0 subcover and we have an algorithm at hand to compute (genus-0) Belyi maps.

Suppose $\Psi : \mathcal{C} \to \mathbb{P}^1_\lambda$ splits[3] as follows

$$\Psi : \mathcal{C} \to \mathbb{P}^1_\mu \xrightarrow{\Psi'} \mathbb{P}^1_\lambda$$

and assume further that the genus-0 Belyi map $\Psi' : \mathbb{P}^1_\mu \to \mathbb{P}^1_\lambda$ has been computed (for example, with the algorithm described in Section 3.3) and, consequently, a relation between λ and μ is explicitly known. Then, after letting μ converge to a rational value, all coefficients of f become algebraic numbers of degree at most $[\mathbb{Q}(\mathcal{C}) : \mathbb{Q}(\mu)]$ which may be considerably smaller than the previous upper bound $[\mathbb{Q}(\mathcal{C}) : \mathbb{Q}(\lambda)]$.

In Chapter 7 we present a successful application of this approach where we reduce the algebraic degree of the occurring numbers from 48 to 2.

3.2.3. Verification of computed results. In the above computation process there are some potential points of failure (e.g., Newton's method converges to a wrong cover, algebraic numbers are inaccurately recognized from their complex approximations, or the interpolation process fails), mostly due to the fact that the algorithm works with inexact complex approximations.

Thus, as a last step, it remains to strictly verify that the obtained polynomial $p(X) - tq(X) \in \mathbb{Q}(\mathcal{C})(t)[X]$ indeed has the prescribed Galois group. Some verification techniques are presented in the next Chapter 4.

3.3. An algorithm to compute genus-0 Belyi maps

In the following we will provide the missing ingredient in Section 3.2.1 by sketching an algorithm developed by Andreas Wenz and the author for computing genus-0 Belyi maps. The algorithm outlined here is used for the examples presented in this thesis but of course any other algorithm capable of computing high degree Belyi maps may be used as well.

[3]The special case where $\mathcal{C}$ is already rational, i.e. $\mathcal{C} = \mathbb{P}^1_\mu$ and $\Psi = \Psi'$, is also allowed.

Our algorithm combines and extends ideas from both [**31**] and [**39, 14, 3**]. In the work at hand we only give a terse overview; for a more detailed description and an implementation using Magma [**15**] and Matlab [**40**] see Andreas Wenz' doctoral dissertation [**53**]. The method has also been sketched in the article [**11**] by Andreas Wenz and the author; in the following description some passages were taken over from this article.

The algorithm takes as input permutations $\sigma_0, \sigma_1, \sigma_\infty \in S_n$ with the following properties

(i) $\sigma_0, \sigma_1, \sigma_\infty$ generate a transitive subgroup of S_n,
(ii) $\sigma_0\sigma_1\sigma_\infty = 1$,
(iii) the genus of $(\sigma_0, \sigma_1, \sigma_\infty)$ is 0,
(iv) $(\sigma_0, \sigma_1, \sigma_\infty)$ is *hyperbolic*[4], i.e., $1/\operatorname{ord}(\sigma_0)+1/\operatorname{ord}(\sigma_1)+1/\operatorname{ord}(\sigma_\infty) < 1$,

and tries to compute a complex approximation of a Belyi map $f : \mathbb{P}^1 \to \mathbb{P}^1$ with branch cycle description $(\sigma_0, \sigma_1, \sigma_\infty)$.

In order to present the algorithm we firstly recall some basic facts about Belyi maps and their dessin d'enfants.

3.3.1. Preliminaries: Belyi maps and dessin d'enfants. To a Belyi map $f : X \to \mathbb{P}^1\mathbb{C}$ of degree n we associate its *dessin d'enfant* or just *dessin* for short. It is the bipartite graph (drawn on the Riemann surface X) consisting of

- the set $f^{-1}(0)$ as black vertices,
- the set $f^{-1}(1)$ as white vertices,
- the connected components of $f^{-1}(]0, 1[)$ as edges.

The branch cycle description $(\sigma_0, \sigma_1, \sigma_\infty)$ of f can be derived from the dessin in the following way, see [**27**, Section 4.1.1]: Label the n edges of the dessin from 1 to n. When walking a small circle (counter-clockwise) around each black node, the edge labelled j is followed by the edge $\sigma_0(j)$. Similarly, σ_1 can be obtained by doing the same procedure with the white nodes. In particular, the cycles of σ_0 and σ_1 correspond to the black and white vertices, respectively, and the cycle length is equal to the respective vertex degree, which in turn is equal to the multiplicity of the corresponding preimage of 0 or 1.

The following example was presented by Gunter Malle at a conference in 1993, see [**54**, Example 1.2].

[4]A technical hypothesis that is fulfilled for most triples generating "interesting" monodromy groups.

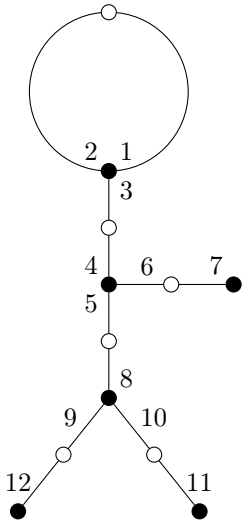


FIGURE 1. Sketched M_{12}-dessin

EXAMPLE 3.2. Consider the permutations $\sigma_0, \sigma_1, \sigma_\infty \in S_{12}$ given by

$$\begin{aligned}\sigma_0 &= (1,2,3)(4,5,6)(8,9,10),\\ \sigma_1 &= (1,2)(3,4)(5,8)(6,7)(9,12)(10,11),\\ \sigma_\infty &= (2,3,6,7,5,10,11,9,12,8,4).\end{aligned}$$

Then $\sigma_0\sigma_1\sigma_\infty = 1$ and $\sigma_0, \sigma_1, \sigma_\infty$ generate the sporadic simple Mathieu group M_{12} with cycle structures as follows:

	σ_0	σ_1	σ_∞
cycle structure	$3^3.1^3$	2^6	$11^1.1^1$

The Riemann–Hurwitz genus formula shows that $(\sigma_0, \sigma_1, \sigma_\infty)$ is of genus 0 which implies that the corresponding Belyi map with branch cycle description $(\sigma_0, \sigma_1, \sigma_\infty)$ is a rational function $f : \mathbb{P}^1\mathbb{C} \to \mathbb{P}^1\mathbb{C}$.

See Figure 1 for the corresponding *sketched*[5] dessin, in the literature sometimes called *Monsieur Mathieu*.

3.3.2. Computation. Our method for calculating f consists of constructing an approximate dessin of f. We illustrate it with a low degree example, namely the M_{12}-triple from Example 3.2. The algorithm to compute genus-0 Belyi maps consists of three steps:

[5]By *sketched* we mean that the dessin is drawn topologically correct but is not the actual preimage under a Belyi map as, for example, the angles and proportions are incorrect.

Step 1: Realize f as an "abstract" 3-point cover of quotient structures

$$\Phi : \mathbb{H}/\Gamma \to \mathbb{H}/\Delta$$

and draw the dessin on $\mathbb{H}/\Gamma$.[6] Here, $\mathbb{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ denotes the upper half plane that comes into play as we work with hyperbolic triples.

Step 2: Use the "welding" technique to construct an explicit isomorphism between $\mathbb{H}/\Gamma$ and $\mathbb{P}^1\mathbb{C}$ that allows transferring the dessin from $\mathbb{H}/\Gamma$ to $\mathbb{P}^1\mathbb{C}$. The genus-0 property of $(\sigma_0, \sigma_1, \sigma_\infty)$ asserts that $\mathbb{H}/\Gamma$ is isomorphic to $\mathbb{P}^1\mathbb{C}$.

Step 3: Reconstruct the Belyi map from the dessin and use Newton's method to obtain sufficiently good complex approximations.

The first step is basically identical to **[31]** while the second step uses ideas from **[39]**, **[14]** and **[3]**. The third step is standard.

Step 1: Drawing the dessin on $\mathbb{H}/\Gamma$.
Let $a := \mathrm{ord}(\sigma_0)$, $b := \mathrm{ord}(\sigma_1)$, $c := \mathrm{ord}(\sigma_\infty)$, and

$$\Delta := \left\langle \delta_a, \delta_b, \delta_c \,|\, \delta_a^a = \delta_b^b = \delta_c^c = \delta_c\delta_b\delta_a = 1 \right\rangle.$$

We work with the embedding $\Delta \hookrightarrow \mathrm{PSL}_2(\mathbb{R})$ described in **[31**, Proposition 2.5], where δ_a (resp. δ_b) is mapped to a hyperbolic rotation around i (resp. μi for some $\mu > 1$) of angle $2\pi/a$ (resp. $2\pi/b$). Thus Δ acts on the upper half-plane $\mathbb{H}$ via the natural action of $\mathrm{PSL}_2(\mathbb{R})$ on $\mathbb{H}$, that is

$$\mathrm{PSL}_2(\mathbb{R}) \to \mathrm{Aut}(\mathbb{H}) : \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mapsto \left(z \mapsto \frac{\alpha z + \beta}{\gamma z + \delta} \right).$$

A fundamental domain can be chosen to be the shape of a hyperbolic kite with vertices $i, h, \mu i, -\bar{h}$ for some $h \in \mathbb{H}$.

Furthermore, let φ denote the homomorphism from Δ onto $G = \langle \sigma_0, \sigma_1 \rangle$ such that $\delta_a \mapsto \sigma_0$ and $\delta_b \mapsto \sigma_1$. Using $\Gamma := \varphi^{-1}(\mathrm{Stab}_G(1)) < \Delta$ we will study

$$\Phi : \mathbb{H}/\Gamma \to \mathbb{H}/\Delta,\ z \bmod \Gamma \mapsto z \bmod \Delta.$$

This is a three-point branched cover of degree n with monodromy group isomorphic to G, see **[31]** for more details. Because $\mathbb{H}/\Delta$ is homeomorphic to $\mathbb{P}^1\mathbb{C}$, we may assume that the ramification locus of Φ is given by $\{0, 1, \infty\}$ such

[6]For a topological space X and a group G acting on X let X/G denote the corresponding orbit space.

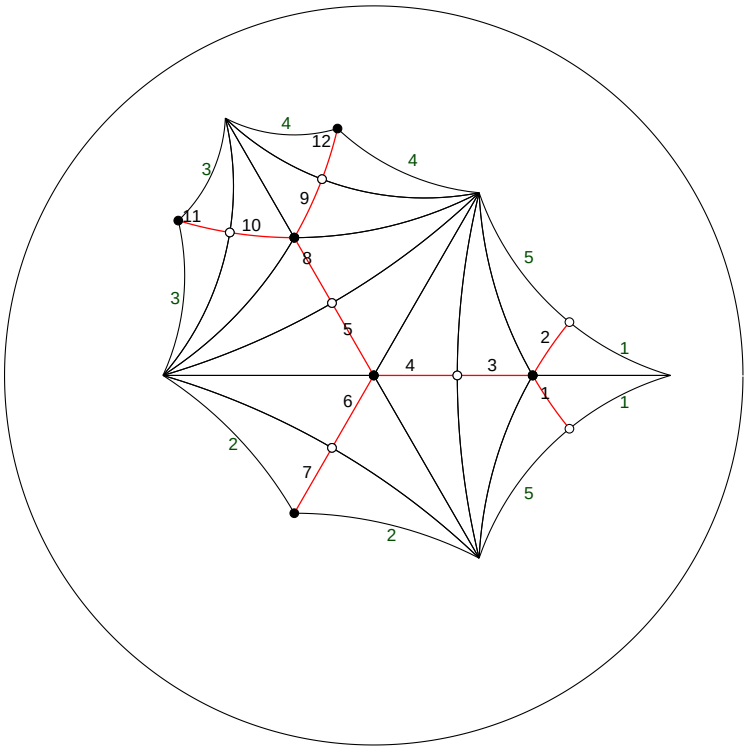


FIGURE 2. fundamental domain D and dessin of Φ

that the coloured line segments in Figure 2 represent $\Phi^{-1}([0,1])$ in a suitable connected fundamental domain D of $\mathbb{H}/\Gamma$.

Step 2: Welding.

By using for example the Schwarz–Christoffel Toolbox **[22]** for Matlab we can conformally map the interior of D onto $\mathbb{H}$. Note that $\partial\mathbb{H} = \mathbb{R}\cup\{\infty\}$ inherits the structure of $\overline{D}$ induced by the quotient relation in $\mathbb{H}/\Gamma$, see Figure 3.

In order to glue adjacent real line segment we will work with slit maps of type

$$\mathrm{slit}_A : \mathbb{H} \to \mathbb{H}, z \mapsto (z-A)^A(z+1-A)^{A-1}$$

where $A \in (0,1)$, see also Figure 4. In Figure 5 we illustrate the first gluing process for the dessin in $\mathbb{H}/\Gamma$. Similar applications can be found in **[39]** and **[3]**.

According to the corresponding quotient structure on $\partial\mathbb{H}$ we keep applying suitable slit maps until we remain with two line segments on $\partial\mathbb{H}$, see Figure 6.

In order to glue the remaining two line segments we apply a conformal map from $\mathbb{H}$ to the unit disc $\mathbb{D}$ that maps these lines to the upper and lower semicircle on $\partial\mathbb{D}$. We will now work with the conformal map

$$\chi : \mathbb{D} \to \mathbb{P}^1\mathbb{C}, z \mapsto z + \frac{1}{z}$$

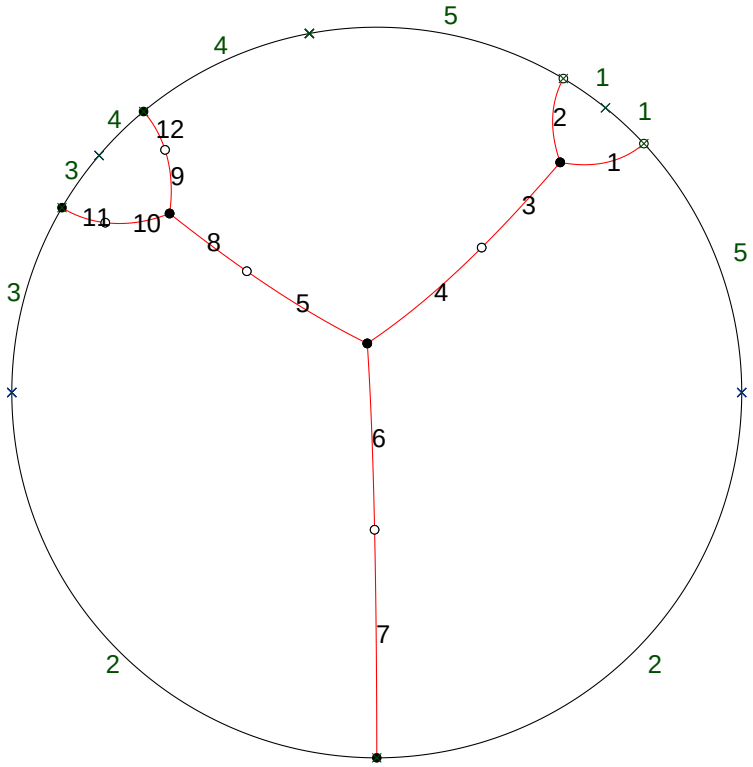


FIGURE 3. $\overline{D}$ conformally mapped onto $\overline{\mathbb{D}}$ (instead of $\overline{\mathbb{H}}$ for the sake of clarity) with quotient structure on $\partial\mathbb{D}$ induced by $\mathbb{H}/\Gamma$, i.e., circular line segments labelled with the same number are considered equivalent modulo Γ

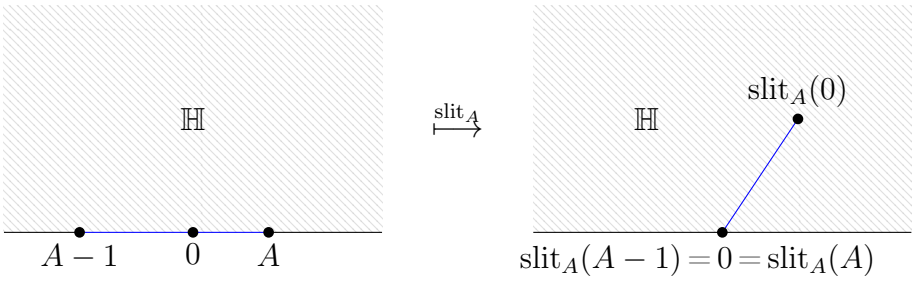


FIGURE 4. conformal map slit_A and its behaviour on $\partial\mathbb{H}$

having the following obvious properties:

- $\chi(\mathbb{D}) = \mathbb{P}^1\mathbb{C} \setminus [-2, 2]$,
- $\chi(z) = 2 \cdot \mathrm{Real}(z)$ for $z \in \partial\mathbb{D}$.

As χ glues both of the above semicircles together we obtain the conformal image of $\mathbb{D}$ onto $\mathbb{P}^1\mathbb{C} \setminus [-2, 2]$ respecting the quotient structure. In particular, this gives us the transformed dessin of Φ contained in $\mathbb{P}^1\mathbb{C}$, see Figure 7.

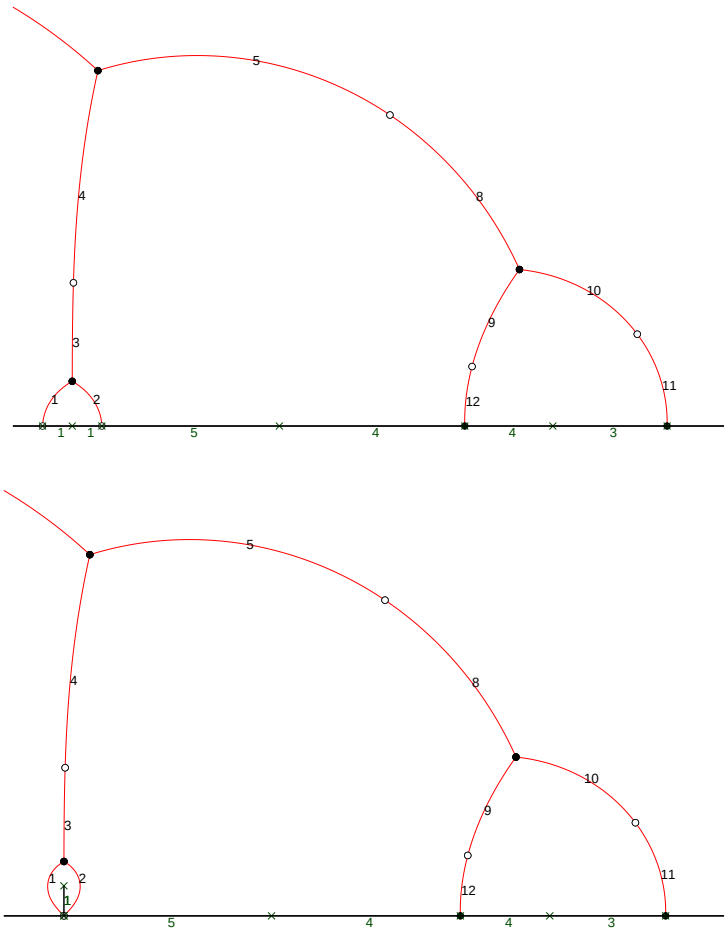


FIGURE 5. gluing process using the slit map $\text{slit}_{\frac{1}{2}}$ for the adjacent real line segments with label 1

Additionally, applying a Möbius transformation yields the dessin shown in Figure 8 that allows a better comparison to the sketched dessin from Figure 1.

Step 3: From the dessin to the Belyi map.

Due to the fact that the cycle structures of σ_0, σ_1 and σ_∞ are given by $(3^3.1^3)$, (2^6) and $(11^1.1^1)$, respectively, we know that the Belyi map f has to obey the following inseparability behaviours over 0, 1 and ∞:

$$f = \frac{cp}{q} = 1 + \frac{(c-1)r}{q}$$

with $p = p_1^3 \cdot p_2$, $q = q_1^{11} \cdot q_2$, $r = r_1^2$, where p_1, p_2, q_1, q_2 and r_1 are monic and pairwise coprime complex polynomials of the following degrees: $\deg(p_1) = \deg(p_2) = 3$, $\deg(q_1) = \deg(q_2) = 1$ and $\deg(r_1) = 6$. Additionally, c denotes a complex scalar.

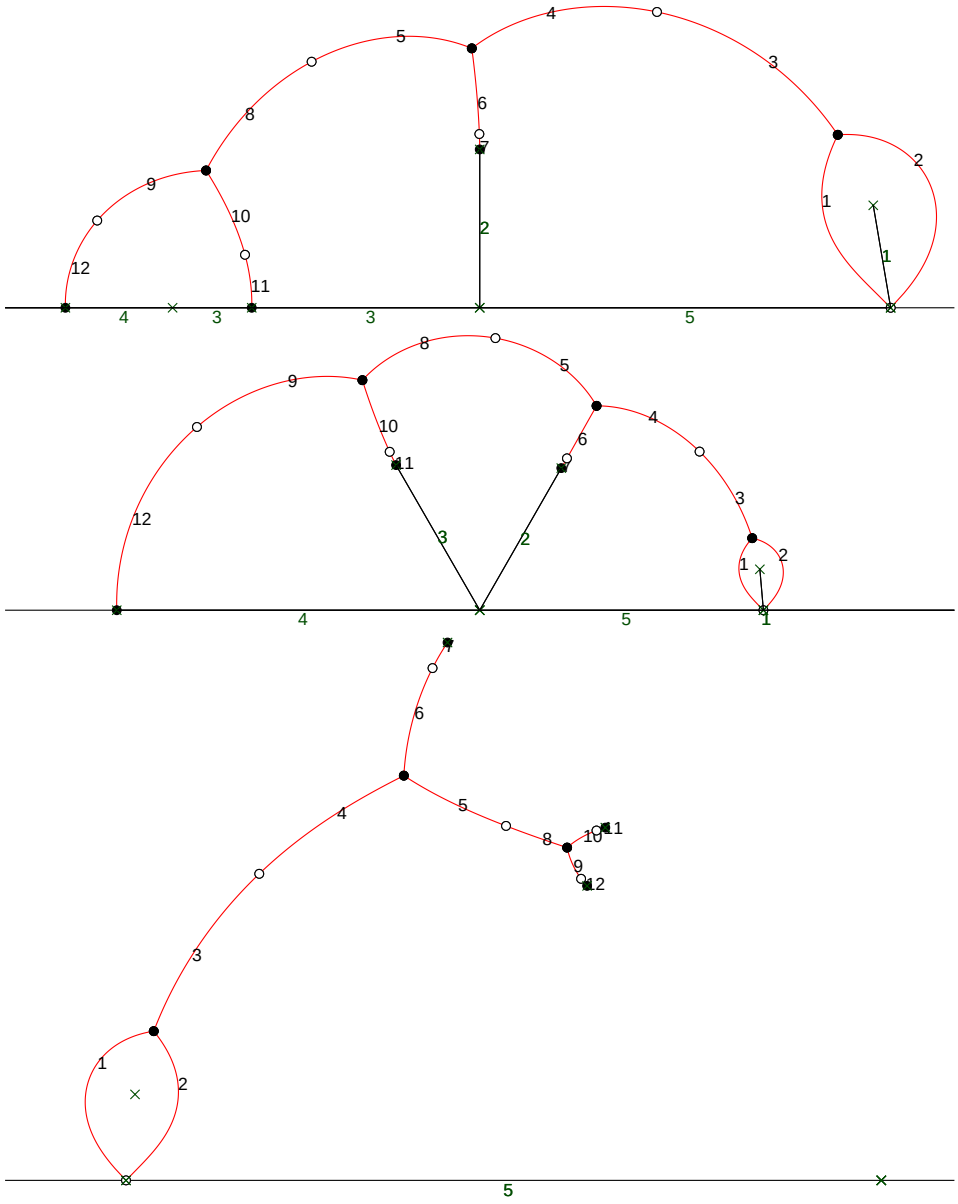


FIGURE 6. next three welding steps (gluing the real line segments labelled 2, 3, 4, respectively)

Now, having constructed an approximate dessin, the values for $c \in \mathbb{C}$ and the monic complex polynomials p_1, p_2, q_1, q_2, r_1 can be picked with respect to the coordinates and multiplicities of the zeroes, ones and poles in the dessin. This gives a starting point for a successful application of Newton's method, allowing us to find an approximation of the Belyi map f of sufficiently high precision such that, if desired, coefficients can be recognized as algebraic numbers.

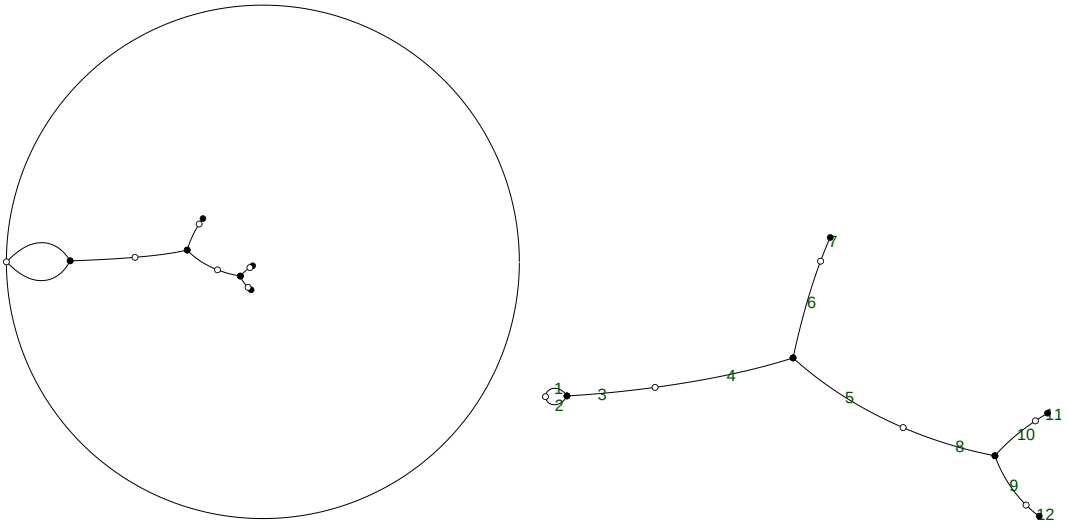


FIGURE 7. fifth and last welding step using χ and the resulting approximate dessin in $\mathbb{P}^1\mathbb{C}$

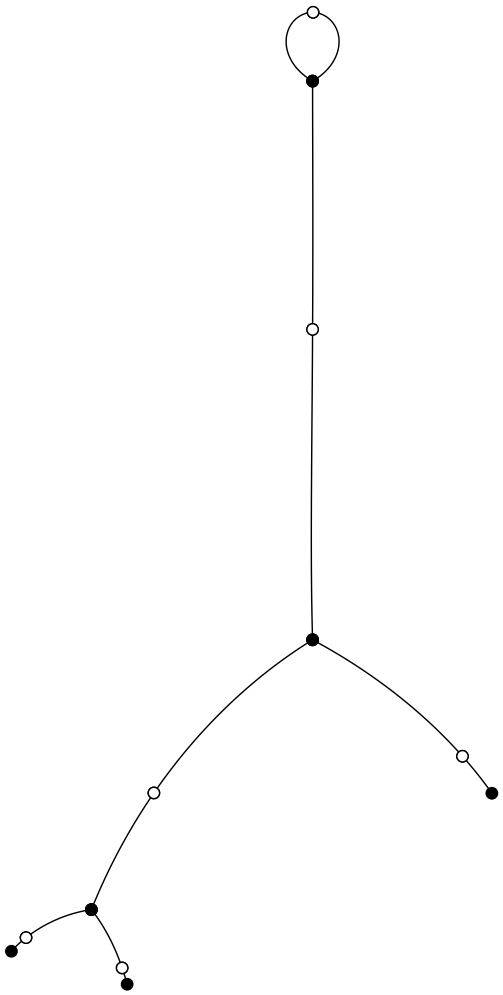


FIGURE 8. M_{12}-dessin after a Möbius transformation

CHAPTER 4

Verification techniques

We present some techniques for determining the Galois groups of (the Galois closure) of rational function fields $K(x) \mid K(t)$ or equivalently the Galois groups of polynomials of the form $p(X) - tq(X) \in K(t)[X]$ with coprime polynomials $p, q \in K[X]$. Some of these techniques may also be applied for polynomials having a stem field of positive genus.

The general approach when computing the Galois group G of a polynomial is to gather enough permutation group theoretic properties of G to uniquely determine it. Our goal in this chapter is to list some tools yielding information about the Galois group. We remark that by far not all groups can be recognized using these tools and we stay far away from giving a complete algorithmic approach for computing Galois groups, as e.g. provided by Stauduhar's algorithm. However, for the groups encountered in this work, the tools we present are sufficient.

Due to the topological interpretation of Galois groups over $\mathbb{C}(t)$, numerical verification by a path lifting algorithm would also be possible; for an implementation of such an algorithm see [**33**, Section 11.1]. However, it is quite hard to obtain rigorous results this way without putting lots of work in choosing a small enough step size. Therefore, we try not to use such numerical algorithms, but rather put emphasis on the fact that we only use exact algorithms yielding rigorous results.

4.1. Definitions and basic properties

Let K be a field of characteristic zero, $p, q \in K[X]$ coprime polynomials and $n := \max(\deg(p), \deg(q))$. Let Ω denote the splitting field of $p(X) - tq(X)$ over $K(t)$. Then, the Galois group of $\Omega \mid K(t)$ is the *arithmetic monodromy group* A of $f := p - tq$. Of course, A is just the Galois group of f and — since p and q are coprime — acts transitively on the n roots of f in Ω.

Denote by $\hat{K}$ the algebraic closure of K in Ω, that is, $\hat{K} = \Omega \cap \overline{K}$, then the *geometric monodromy group* G of f is the Galois group of $\Omega \mid \hat{K}(t)$. It can be easily seen that G is normal in A and also acts transitively on the roots of

f. In particular, we have $G \trianglelefteq A \leq N_{S_n}(G) \leq S_n$ where $N_{S_n}(G)$ denotes the *symmetric normalizer* of G; that is, its normalizer in the symmetric group S_n.

Recall that the extension $\Omega \mid K(t)$ is called regular if $\hat{K} = K$ or equivalently $A = G$. In this case we say that the Galois group of f is regular — not to be confused with the term "regular permutation group". Of course, sufficient conditions for regularity are that G is self-normalizing in S_n, i.e., $G = N_{S_n}(G)$, or that A is a simple group.

If K is a number field, it can be seen that the groups G, $\mathrm{Gal}(f \mid \overline{\mathbb{Q}}(t))$, $\mathrm{Gal}(f \mid \mathbb{C}(t))$ and the (topological) monodromy group of the rational function p/q are all permutation isomorphic to each other. In particular, G is generated by the elements $\sigma_1, \ldots, \sigma_r$ from the branch cycle description of p/q. Note that the cycle structure of σ_i corresponds to the inseparability behaviour of f above the i-th branch point and can thus be easily determined.

REMARK. Sometimes we use the notion of arithmetic and geometric monodromy groups also when working in characteristic p. However, we always exclude cases of wild ramification and only consider tame ramification. This can be guaranteed, for example, by choosing p larger than the polynomial's degree.

4.2. Gathering information about subgroups of a Galois group

It is usually simple to obtain lower bounds for Galois groups, for example, using the well known Dedekind criterion. But, of course, lower bounds alone can not exclude the groups A_n or S_n as possibilities. In order to exclude these large groups as candidates for the Galois group it is often useful to prove the existence of subgroups with certain properties in the Galois group.

One way to obtain information about subgroups of the Galois group of a polynomial $f \in K(t)[X]$ is to factor f over some extension L of $K(t)$. In general, this can be a computationally expensive task, but if L is still a rational function field, the factorization can be carried out without enlarging the field:

LEMMA 4.1. *Let $f(t, X) \in K(t)[X]$ be a polynomial and $p, q \in K[X]$ coprime. Let s be a root of $p(X) - tq(X) \in K(t)[X]$. Then $f(t, X)$ factors over the rational function field $K(s)$ in the same pattern as the specialized polynomial $f(\frac{p(t)}{q(t)}, X)$ factors over $K(t)$.*

PROOF. As s is a root of $p(X) - tq(X)$ we have $t = \frac{p(s)}{q(s)}$. Thus, by a change of variables, factoring $f(t, X) = f(\frac{p(s)}{q(s)}, X)$ over $K(s)$ corresponds to factoring $f(\frac{p(t)}{q(t)}, X)$ over $K(t)$. □

A useful application of Lemma 4.1 lies in computing the *subdegrees* of Galois groups of polynomials of the form $p(X) - tq(X) \in K(t)[X]$. Recall that the subdegrees of a transitive group G are the orbit lengths of any point stabilizer of G.

COROLLARY 4.2. *Let $p, q \in K[X]$ be coprime polynomials such that $p(X) - tq(X)$ is separable. Then the subdegrees of* $\mathrm{Gal}(p(X) - tq(X) \mid K(t))$ *are given by the degrees of the irreducible factors of $p(X) - \frac{p(t)}{q(t)}q(X)$ over $K(t)$.*

PROOF. Let x be a root of $p(X) - tq(X) \in K(t)[X]$ in a splitting field and denote by G the Galois group of $p(X) - tq(X)$ over $K(t)$. Then the point stabilizer G_x is equal to the Galois group of $p(X) - tq(X)$ over $K(x)$ and, in particular, the subdegrees of G are given by the degrees of the irreducible factors of $p(X) - tq(X)$ over $K(x)$. Due to the previous lemma these degrees can be determined by factoring $p(X) - \frac{p(t)}{q(t)}q(X)$ over the smaller field $K(t)$. □

A transitive group of degree n is 2-transitive if and only if its subdegrees are 1 and $n - 1$. In particular, using Corollary 4.2 we can decide whether a Galois group is 2-transitive. Notably, when the Galois group turns out to be not 2-transitive often only a few groups remain with the given subdegrees. The case of 2-transitivity (which is most common in this thesis) is typically more difficult to deal with as it can be hard to exclude the large and highly transitive groups A_n and S_n. For these groups some of the following results come in handy; they yield information on subgroups other than point stabilizers. An alternative way to exclude A_n and S_n is Elkies' method for bounding the transitivity degree of Galois groups in the function field setting, see Chapter 8 for more details.

The following lemma gives a sufficient criterion that some field has non-trivial intersection with a polynomial's splitting field.

LEMMA 4.3. *Let $f \in K[X]$ be an irreducible polynomial with splitting field Ω (in some fixed algebraic closure of K). Further assume that f becomes reducible over some field L (extending K). Then $L \cap \Omega \gneqq K$.*

PROOF. Without loss of generality, we assume that f is monic and write

$$f = (X - \alpha_1) \cdots (X - \alpha_n)$$

with $\alpha_1, \ldots, \alpha_n \in \Omega$. Since f is irreducible over K but splits nontrivially over L, we have $f = pq$ for monic polynomials $p, q \in L[X] \setminus K[X]$. The coefficients of p and q are polynomials in the roots $\alpha_1, \ldots, \alpha_n$ of f and lie therefore in the splitting field $\Omega = K(\alpha_1, \ldots, \alpha_n)$, implying $p, q \in \Omega[X]$. It follows that there

exists at least one coefficient of p or q lying in $(L \cap \Omega) \setminus K$ which proves the lemma. □

Lemma 4.3 yields information about the Galois group of f over K by factoring f over fields L extending K. If L is a rational function field, Lemma 4.1 allows efficient factorization over L, yielding the following proposition. It can be seen as a generalization of Corollary 4.2 to subgroups other than point stabilizers.

PROPOSITION 4.4. *Let K be an arbitrary field and $f(t, X) \in K(t)[X]$ a separable and irreducible polynomial. Furthermore, let $p, q \in K[X]$ be coprime polynomials such that $f(\frac{p(t)}{q(t)}, X) \in K(t)[X]$ splits nontrivially into irreducible factors of degree $d_1, \ldots, d_r$. Then the Galois group $\mathrm{Gal}(f \mid K(t))$ has a proper subgroup of index dividing $\deg(p - tq)$ with orbit lengths $d_1, \ldots, d_r$.*

PROOF. Let Ω be the splitting field of f over $K(t)$ and s a root of the irreducible polynomial $p - tq \in K(t)[X]$. According to the assumption and Lemma 4.1, $f(t, X)$ splits over $K(s)$ into irreducible factors of degree $d_1, \ldots, d_r$. As shown in the proof of Lemma 4.3 this also holds when factorizing f over $\Omega \cap K(s)$. Therefore, $\mathrm{Gal}(\Omega \mid \Omega \cap K(s)) < \mathrm{Gal}(\Omega \mid K(t))$ is of index dividing $[K(s) : K(t)] = \deg(p - tq)$ with orbit lengths $d_1, \ldots, d_r$. □

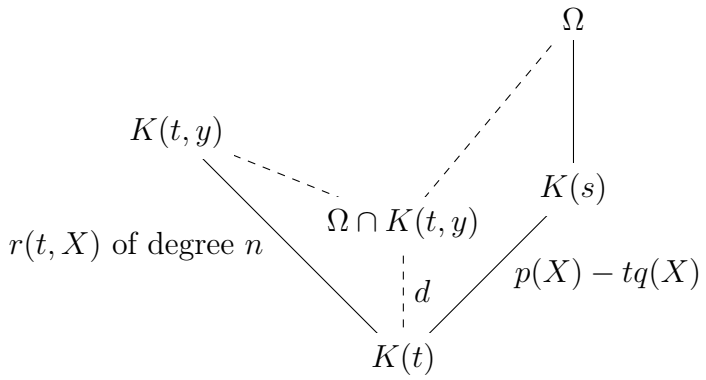
In the above proposition we used the fact that the splitting field of f contains a rational function field $K(s)$ over which the factorization process becomes easy due to Lemma 4.1. The following well known result in basic field theory helps to factor polynomials of the form $p - tq$ over non-rational subfields of their splitting fields.

LEMMA 4.5. *Let K be a field, and a, b algebraic over K with minimal polynomials $\mu_a, \mu_b \in K[X]$. Then μ_a is irreducible over $K(b)$ if and only if μ_b is irreducible over $K(a)$.*

We use Lemma 4.5 to prove a variant of Proposition 4.4:

PROPOSITION 4.6. *Let K be an arbitrary field, $p, q \in K[X]$ be coprime such that $p(X) - tq(X) \in K(t)[X]$ is separable and let $G := \mathrm{Gal}(p(X) - tq(X) \mid K(t))$. Further assume there exists an irreducible polynomial $r(t, X) \in K(t)[X]$ of degree n such that $r(\frac{p(t)}{q(t)}, X) \in K(t)[X]$ becomes reducible. Then there exists a divisor $d \neq 1$ of n such that G possesses an index d subgroup.*

PROOF. Let Ω denote the splitting field of the irreducible polynomial $p(X) - tq(X)$ over $K(t)$, y be a root of $r(X)$ in a splitting field over $K(t)$ and $s \in \Omega$ a root of $p(X) - tq(X)$:



The reducibility of $r(\frac{p(t)}{q(t)}, X) \in K(t)[X]$ together with Lemma 4.1 implies that $r(t, X)$ splits nontrivially over $K(s)$. Now, Lemma 4.5 yields that the polynomial $p(X) - tq(X)$ is reducible over $K(t, y)$, thus $K(t) \lneqq \Omega \cap K(t, y)$ according to Lemma 4.3. Via Galois correspondence $\mathrm{Gal}(\Omega \mid K(t))$ must contain an index d subgroup where $d \neq 1$ is a divisor of n. □

Propositions 4.4 and 4.6 are our main tools to obtain information about subgroups of a Galois group. Similar tricks are, of course, long known in the literature and have been used, for example, in **[37]**. We conclude this section with a short outline on how (and under which conditions) these results yield information about a polynomial's Galois group.

4.2.1. Using the previous propositions in the determination of Galois groups. Let $f(t, X) \in K(t)[X]$ be an irreducible polynomial with splitting field Ω and Galois group G. Using Propositions 4.4 or 4.6 to get information about the group G usually boils down to compute an auxiliary polynomial $r(t, X) \in K(t)[X]$ defining a subfield of Ω. Then, of course, the Galois group G acts on the roots of $r(t, X)$, leading to a second permutation representation of G (apart from the "natural" one acting on the roots of f).

We divide the procedure into two steps: First, how to pick a suitable permutation representation of G and, second, how to actually obtain the auxiliary polynomial r.

Step 1: Picking the right permutation representation. The above propositions can only be applied successfully if f splits over a stem field of r which is equivalent to the fact that the stabilizer of a root of r acts intransitively on the roots of f (or vice versa).

Of course, it is possible to compute (e.g., with Magma) whether a given finite group G possesses suitable permutation representations, i.e., if G possesses subgroups H_1 and H_2 such that H_1 acts intransitively on the cosets of H_2 in G.

In addition to this computational approach, the question can also be decided in a character-theoretic way suggested to us by Peter Müller, which will be outlined in the following: Assume G acts transitively on two finite sets Ω_1 and Ω_2 with permutation characters denoted by π_1 and π_2, respectively. Additionally, let H_1 and H_2 be stabilizers of elements of Ω_1 and Ω_2, respectively. Then, it is an easy exercise to show that G has as many orbits on $\Omega_1 \times \Omega_2$ as the stabilizer H_1 has on Ω_2. By symmetry, there are as many H_1-orbits on Ω_2 as there are H_2-orbits on Ω_1. Moreover, by the Cauchy-Frobenius orbit counting formula and the fact that the permutation character of G on $\Omega_1 \times \Omega_2$ is given by $\pi_1\pi_2$, this common number of orbits is given by the standard inner product $[\pi_1, \pi_2]$.

Thus, denoting the permutation characters of G on the roots of f and r by π_1 and π_2, respectively, a prerequisite for the successful application of Proposition 4.4 or 4.6 is that $[\pi_1, \pi_2] > 1$. For almost simple groups this condition often can be easily checked using, for example, the Atlas of finite simple groups [**17**]. A special case where $[\pi_1, \pi_2] > 1$ occurs is when G has two non-equivalent actions with the same permutation character. This often occurs when dealing with linear groups, cf. Section 4.4.1.

Step 2: Obtaining the auxiliary polynomial r. The second and more difficult step is to actually obtain the polynomial r having the desired properties described in the previous step. We present two strategies to solve this.

First, one can use the Magma commands `GaloisGroup` and `GaloisSubgroup` to compute r. Often these commands can be carried out only after a suitable mod-p reduction. These Magma commands work with approximations of the roots and thus are not guaranteed to yield proven results. However, this poses no problem as the factorization algorithms used in the applications of Propositions 4.4 or 4.6 yield rigorous results.

In some cases one can circumvent the (potentially expensive!) use of the Magma commands `GaloisGroup` and `GaloisSubgroup`, for example, in the following setting (that occurs often in the case of linear groups):

Assume we have computed a Hurwitz curve $\mathcal{C}$ together with a multi-parameter polynomial $f \in \mathbb{Q}(\mathcal{C})(t)[X]$ for a group G and we are in the case $\pi_1 = \pi_2$ from above, i.e., G has two non-conjugate subgroups H_1 and H_2 inducing the same permutation character.[1] From $\pi_1 = \pi_2$ we can conclude, see the proof of [**35**, Corollary 3.2], that the inertia group generators $\sigma_1, \ldots, \sigma_r$

[1]Such triples (G, H_1, H_2), also known as *Gassmann triples*, have connections, for example, to arithmetically equivalent number fields, Davenport pairs and isospectral Riemannian manifolds.

have the same cycle structures in their action on the cosets of the group H_2 as they have in their action on the cosets of H_1. So it is reasonable to expect that the polynomial r lies in the same Hurwitz family as f, and, consequently, may already be computed (or can be obtained from f relatively easily).

For simplicity, we give a brief outline of this procedure in the special case $\mathcal{C} = \mathbb{P}^1_\alpha$. Then, our usual approach is to pick distinct $\alpha_0, \alpha_1 \in \mathbb{Q}$ such that $f_0 := f(\alpha_0, t, X)$ and $f_1 := f(\alpha_1, t, X)$ have the same ramification locus (which, of course, is a necessary condition for f_0 and f_1 to have the same splitting field) and factor f_0 over a stem field of f_1 to see whether it splits. In practice, one often picks $\alpha_0 \in \mathbb{Q}$ arbitrarily and uses the explicitly computed branch point reference map Ψ to find $\alpha_1 \in \mathbb{Q} \setminus \{\alpha_0\}$ with $\Psi(\alpha_0) = \Psi(\alpha_1)$. In all of our examples where we use this technique, we have $\mathrm{Out}(G) = C_2$ and the branch point reference map splits because of the imprimitivity caused by the $\mathrm{Aut}(G)$-blocks on $\mathrm{SNi}^{in}(C)$ of size 2. Thus, the picked values α_0 and α_1 usually correspond to $\mathrm{Aut}(G)$-conjugate branch cycle descriptions. For such a choice of α_0 and α_1, the Hurwitz classification (see the next section) suggests that f_0 and f_1 have the same splitting field. In the described setting the polynomial f_1 then takes the role of the auxiliary polynomial r to provide information about the Galois group of f_0.

4.3. Reduction and specialization in function fields

Dedekind's well known criterion states that after reducing a separable polynomial modulo a prime ideal (or alternatively specializing a parameterized polynomial), the Galois group of the new polynomial is a subgroup of the original polynomial's Galois group. In doing so, of course, one only allows such reductions and specializations that preserve the polynomial's degree and its separability. This condition will be assumed in the following without further notice.

In the setting of function field extensions and their geometric interpretation as covers (or even families of covers), it is often possible to assert that the Galois group (or at least the geometric monodromy group) does not change after reduction or specialization. The main condition here is that we have to reduce or specialize in such a way that the ramification locus does not become smaller, meaning that no two branch points coincide after reduction or specialization. When reducing into positive characteristic, we also require that the characteristic does not divide the group order. In both cases we are basically invoking Grothendieck's good reduction theorem, see [**23**, Theorem 2.6]. In the

following we describe these two powerful techniques and how we use them in the verification process.

4.3.1. Specializing multi-parameter polynomials. Suppose, we want to obtain information about the Galois group of a multi-parameter polynomial $f(t, X) \in \mathbb{Q}(\mathcal{C})(t)[X]$ parameterized by an (absolutely) irreducible curve $\mathcal{C}$, for example, the corresponding Hurwitz curve.

Let $G := \mathrm{Gal}(f \mid \overline{\mathbb{Q}(\mathcal{C})}(t))$ be the geometric monodromy group of f. Furthermore, let $c_0 \in \mathcal{C}$ be an *unramified point* (with respect to the branch point reference map) — that is, we demand that the specialized polynomial f_0 at the point $c_0 \in \mathcal{C}$ still has the same number of branch points as f. Denote by $G_0 := \mathrm{Gal}(f_0 \mid \overline{\mathbb{Q}}(t))$ the geometric monodromy group of f_0. The fields $\overline{\mathbb{Q}(\mathcal{C})}$ and $\overline{\mathbb{Q}}$ are both algebraically closed of characteristic zero and for such fields $\overline{K}$ the *Hurwitz classification* holds: the Galois G-extensions of $\overline{K}(t)$ unramified outside a fixed r-subset of $\mathbb{P}^1\overline{K}$ are in bijection to the set $\mathcal{E}_r(G)/\operatorname{Aut}(G)$, see [**38**, Theorems III.6.1, I.2.2, I.4.1]. This is basically Riemann's existence theorem generalized to algebraically closed fields of characteristic zero. Moreover, [**38**, Corollary III.6.3] and [**38**, Theorem III.6.4] state that specialization at an unramified point is compatible with the Hurwitz classification implying that f and f_0 possess the same ramification type and, in particular, their geometric monodromy groups G and G_0 are isomorphic.

Thus, we have seen that specialization of a (connected) family of covers at an unramified point does not change the geometric monodromy group. For the case where $\mathcal{C}$ is a rational variety and the splitting field of f is additionally assumed to be regular, this statement is explicitly formulated in [**37**, Lemma 3.1].

4.3.2. Reducing covers modulo a prime. An analogous result as in the previous section holds when reducing a cover modulo p under the additional condition that p does not divide the group order. Let K be a number field with ring of integers $\mathcal{O}_K$ and $f \in K(t)[X]$ a polynomial with ramification locus $\mathcal{R}$. Furthermore, let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ lying over the rational prime p and denote by $\overline{f} \in (\mathcal{O}_K/\mathfrak{p})(t)[X]$ the image under the canonical projection.[2] Denote by G and $G_\mathfrak{p}$ the geometric monodromy groups of f and $\overline{f}$, i.e., the Galois groups over $\overline{\mathbb{Q}}(t)$ and $\overline{\mathbb{F}_p}(t)$, respectively. Assume further that the ramification locus $\mathcal{R}$ is $\mathfrak{p}$-stable meaning that we have $|\mathcal{R}| = |\overline{\mathcal{R}}|$ for the mod-$\mathfrak{p}$ reduced ramification locus $\overline{\mathcal{R}}$.

[2]We implicitly assume that all coefficients of f lie in the localization of $\mathcal{O}_K$ at the prime ideal $\mathfrak{p}$.

Under the additional assumption that the order of G is not divisible by p, a fact that can even be assumed without exactly knowing $|G|$ by picking p larger than the polynomial's degree, again, the Hurwitz classifications of Galois G-extensions unramified outside of $\mathcal{R}$ and $\overline{\mathcal{R}}$ coincide, see [**38**, Theorem I.10.6]. Moreover, similar as in Section 4.3.1, reduction modulo a prime ideal leaves the ramification data and the geometric monodromy group invariant, in particular, $G \cong G_{\mathfrak{p}}$, see [**38**, Corollary I.10.7]. Beckmann proved this statement and variants thereof using different methods, see [**13**] or [**38**, Proposition I.10.9].

4.4. Avoiding the classification of finite simple groups

The Galois groups occurring in this work are either 2-transitive groups or primitive of rank 3. Through the classification of finite simple groups all such finite groups are classified allowing us to exclude all but one permutation group after having gathered enough permutation group theoretic information about the Galois group. The remaining group must necessarily be the polynomial's Galois group.

In this last section we present some strategies to avoid the classification of finite simple groups in the verification process. Our strategies focus on 2-transitive linear groups and rank-3 groups and use the theories of block designs and strongly regular graphs, respectively.

4.4.1. 2-transitive linear groups: Design theoretic argument.

Definition 4.7. Let v, k, λ be natural numbers with $1 < k < v - 1$. A (v, k, λ)-*design* is an incidence structure consisting of blocks and points such that:

(i) v is the number of points,
(ii) each block contains k points,
(iii) for any 2 points there are exactly λ blocks containing both of them.

A design is called *symmetric* if it has as many points as blocks.

An important family of block designs arises in projective geometry:

Example 4.8. Let q be a prime power and $d \geq 2$. Consider the incidence structure whose points are the 1-dimensional subspaces of $\mathbb{F}_q^{d+1}$, its blocks are the d-dimensional subspaces of $\mathbb{F}_q^{d+1}$, and incidence is given by inclusion. This defines a symmetric (v, k, λ)-design with parameters as follows:

$$v = \frac{q^{d+1} - 1}{q - 1}, \quad k = \frac{q^d - 1}{q - 1}, \quad \lambda = \frac{q^{d-1} - 1}{q - 1}.$$

It is called *desarguesian projective space* $\mathrm{PG}(d,q)$ and has the 2-transitive automorphism group $\mathrm{Aut}(\mathrm{PG}(d,q)) = \mathrm{P\Gamma L}_{d+1}(q)$.

One can construct symmetric designs from certain 2-transitive permutation groups in the following way.

THEOREM 4.9 ([**20**], 2.4.5). *Let $G \leq S_v$ be a 2-transitive permutation group having an intransitive subgroup H of index $[G:H] \leq v$ which has an orbit B with $1 < |B| < v-1$. Then there exists a symmetric $(v, |B|, \lambda)$-design $\mathcal{D}$ such that $G \leq \mathrm{Aut}(\mathcal{D})$.*

Among all designs with 2-transitive automorphism group, desarguesian projective space is characterized by its parameters.

THEOREM 4.10 ([**30**]). *Let $\mathcal{D}$ be a symmetric (v,k,λ)-design with parameters*

$$v = \frac{q^{d+1}-1}{q-1}, \quad k = \frac{q^d-1}{q-1}, \quad \lambda = \frac{q^{d-1}-1}{q-1}$$

for some prime power q and some integer $d \geq 2$. Then $\mathcal{D}$ is isomorphic to $\mathrm{PG}(d,q)$ if and only if $\mathcal{D}$ has an automorphism group 2-transitive on its points.

Combining the previous theorems yields:

PROPOSITION 4.11. *Let $G \leq S_v$ be a 2-transitive permutation group having an intransitive subgroup H of index $[G:H] \leq v$ that has an orbit of length k where v and k are of the form*

$$v = \frac{q^{d+1}-1}{q-1} \quad \textit{and} \quad k = \frac{q^d-1}{q-1}$$

for some prime power q and some integer $d \geq 2$. Then $G \leq \mathrm{P\Gamma L}_{d+1}(q)$.

PROOF. Applying Theorem 4.9 yields $G \leq \mathrm{Aut}(\mathcal{D})$ for some symmetric (v,k,λ)-design $\mathcal{D}$. Since $\mathcal{D}$ has the same parameters v and k as $\mathrm{PG}(d,q)$ and λ is determined (in a symmetric design) by the equation

$$\lambda(v-1) = k(k-1),$$

we conclude that $\mathcal{D}$ also has the same λ-value as the projective space $\mathrm{PG}(d,q)$, thus $\lambda = \frac{q^{d-1}-1}{q-1}$. As $\mathcal{D}$ possesses a 2-transitive automorphism group and has the same parameters as $\mathrm{PG}(d,q)$, Theorem 4.10 yields that $\mathcal{D}$ is indeed isomorphic to $\mathrm{PG}(d,q)$. It follows $G \leq \mathrm{Aut}(\mathcal{D}) = \mathrm{Aut}(\mathrm{PG}(d,q)) = \mathrm{P\Gamma L}_{d+1}(q)$. □

For later use, we note an application of Proposition 4.11 dealing with the groups $\mathrm{PGL}_4(3)$ and $\mathrm{PSL}_6(2)$:

COROLLARY 4.12.

(a) Let G be a 2-transitive subgroup of S_{40} that contains a subgroup of index dividing 40 with orbit lengths 13 and 27. Then G is isomorphic to $\mathrm{PSL}_4(3)$ or $\mathrm{PGL}_4(3)$.

(b) Let G be a 2-transitive subgroup of S_{63} that contains a subgroup of index dividing 63 with orbit lengths 31 and 32. Then G is isomorphic to $\mathrm{PSL}_6(2)$.

PROOF.

(a) After setting $d := 3$, $q := 3$ and observing $40 = \frac{q^{d+1}-1}{q-1}$ and $13 = \frac{q^d-1}{q-1}$, Proposition 4.11 (applied with $v = 40$ with $k = 13$) yields $G \leq \mathrm{P\Gamma L}_4(3) = \mathrm{PGL}_4(3)$. The assertion now follows from the fact that $\mathrm{PSL}_4(3)$ and $\mathrm{PGL}_4(3)$ are the only 2-transitive subgroups of $\mathrm{PGL}_4(3)$.

(b) Note that $v = 63 = \frac{2^{5+1}-1}{2-1}$ and $k = 31 = \frac{2^5-1}{2-1}$. Thus, Proposition 4.11 with $d = 5$ and $q = 2$ yields $G \leq \mathrm{P\Gamma L}_6(2) = \mathrm{PSL}_6(2)$. As $\mathrm{PSL}_6(2)$ does not contain proper 2-transitive subgroups, we get $G = \mathrm{PSL}_6(2)$.

□

Alternatively, the result would also follow from the classification of finite 2-transitive groups which however relies on the classification of finite simple groups.

REMARK. According to [**35**, Theorem 3.1], the group of automorphisms of a symmetric design possesses the same permutation character on both points and blocks. Consequently, these groups, and most prominent linear groups, are good candidates for the strategies outlined in Section 4.2.1.

4.4.2. Rank-3 groups: Graph theoretic argument. In the case of rank-3 groups one can sometimes use the theory of strongly regular graphs to avoid invoking the classification of finite simple groups. We use this later on for the primitive rank-3 group $\mathrm{PSp}_4(3).C_2$ of degree 27.

The first half of this subsection is mainly identical to a passage in the article [**11**] where the same approach was carried out for the group Aut(HS).

An undirected k-regular graph $\mathcal{G}$ with n vertices is called *strongly regular* if there exist $\lambda, \mu \in \mathbb{N}_0$ such that adjacent vertices have exactly λ common neighbours and non-adjacent vertices have exactly μ common neighbours. We say that $\mathcal{G}$ is of type $\mathrm{srg}(n, k, \lambda, \mu)$ if $\mathcal{G}$ fulfils the aforementioned conditions.

Some well known properties of strongly regular graphs are collected in the following lemma, see also [**16**, Theorem 1.1, Theorem 3.1].

LEMMA 4.13. *Let $\mathcal{G}$ be of type* $\mathrm{srg}(n,k,\lambda,\mu)$. *Then the following conditions hold:*

(i) $k(k-\lambda-1)=(n-k-1)\mu$,

(ii) $\frac{1}{2}\left(n-1\pm\frac{(n-1)(\mu-\lambda)-2k}{\sqrt{(\mu-\lambda)^2+4(k-\mu)}}\right)$ *are non-negative integers.*

Another key observation is the fact that rank-3 groups can be considered as automorphism groups of strongly regular graphs, see [**16**, Theorem 6.1].

LEMMA 4.14. *Let G be a rank-3 subgroup of S_n having subdegrees* 1, k, ℓ *with* $1<k<\ell$. *Then there exists a strongly regular graph $\mathcal{G}$ of type* $\mathrm{srg}(n,k,\lambda,\mu)$ *for some $\lambda,\mu\in\mathbb{N}_0$ such that G is a subgroup of* $\mathrm{Aut}(\mathcal{G})$.

LEMMA 4.15. *Let G be a transitive subgroup of S_{27} with subdegrees 1, 10, 16. Then G is isomorphic to* $\mathrm{PSp}_4(3)$ *or* $\mathrm{PSp}_4(3).C_2$.

PROOF. Due to Lemma 4.14 there exists a strongly regular graph $\mathcal{G}$ of type $\mathrm{srg}(27,10,\lambda,\mu)$ for some $\lambda,\mu\in\{0,\dots,27\}$ such that G is a subgroup of $\mathrm{Aut}(\mathcal{G})$. According to Lemma 4.13(i) the parameters λ and μ have to satisfy the equation $10(10-\lambda-1)=(27-10-1)\mu$. From this we find $(\lambda,\mu)\in\{(1,5),(9,0)\}$. Among these pairs the condition from Lemma 4.13(ii) is only fulfilled for $(\lambda,\mu)=(1,5)$. Therefore, $\mathcal{G}$ is of type $\mathrm{srg}(27,10,1,5)$.

From [**28**, Lemma 10.9.4] we find that $\mathcal{G}$ must be isomorphic to the complement of the Schläfli graph with $\mathrm{Aut}(\mathcal{G})=\mathrm{PSp}_4(3).C_2$ and, therefore, G is a subgroup of $\mathrm{PSp}_4(3).C_2$. As $\mathrm{PSp}_4(3)$ and $\mathrm{PSp}_4(3).C_2$ are the only transitive subgroups of $\mathrm{PSp}_4(3).C_2$ having subdegrees 1, 10, 16, we find $G=\mathrm{PSp}_4(3)$ or $G=\mathrm{PSp}_4(3).C_2$. □

Alternatively, one can prove Lemma 4.15 using the classification of finite primitive rank-3 groups (that however depends on the classification of finite simple groups!): First, note that a group with subdegrees 1, 10, 16 must necessarily be primitive as no subset of the subdegrees adds up to a proper non-trivial divisor of 27. Now, according to the classification of finite primitive rank-3 permutation groups, $\mathrm{PSp}_4(3)$ and $\mathrm{PSp}_4(3).C_2$ are the only groups with these subdegrees.

CHAPTER 5

Computation of polynomials with symplectic Galois groups

We compute polynomials with certain symplectic groups as Galois groups. More precisely, we compute two-parameter families of polynomials having the symplectic groups $\mathrm{PSp}_4(3).C_2 \leq S_{27}$, $\mathrm{PSp}_6(2) \leq S_{28}$ and $\mathrm{PSp}_6(2) \leq S_{36}$ as Galois groups over $\mathbb{Q}$. Additionally, it turns out that the computed degree-28 polynomials with group $\mathrm{PSp}_6(2)$ allow infinitely many totally real specializations.

The results presented in this chapter were previously published in the journal article [**4**] joint with Joachim König and Andreas Wenz. Some passages were taken over from the article.

Remark. The examples $\mathrm{PSp}_4(3).C_2 \leq S_{27}$ and $\mathrm{PSp}_6(2) \leq S_{28}$ were firstly computed in cooperation with Joachim König in 2018: Andreas Wenz and the author computed the Belyi map leading to a single 4-point cover while Joachim König carried out the interpolation of the Hurwitz space starting from the previously computed single cover (cf. parts (1) and (2) in Section 3.2). Later on, in the course of writing up this thesis, the author reproduced König's computations using his own implementation.

5.1. Multi-parameter polynomials with Galois groups $\mathrm{PSp}_4(3).C_2$ and $\mathrm{PSp}_4(3)$

As a first application of the algorithm described in Chapter 3, we calculate degree-27 polynomials $f(\alpha, t, X)$ with Galois groups $\mathrm{PSp}_4(3)$ and $\mathrm{PSp}_4(3).C_2$ over $\mathbb{Q}(\alpha, t)$. Belyi maps defined over $\mathbb{Q}$ with monodromy group $\mathrm{PSp}_4(3).C_2 \cong \mathrm{PSU}_4(2).C_2$ were known before, see [**38**, p. 500]. However, here we present (to the best of our knowledge) the first families of 4-point covers with groups $\mathrm{PSp}_4(3).C_2$ and $\mathrm{PSp}_4(3)$.

5.1.1. Theoretical properties. The group $G := \mathrm{PSp}_4(3).C_2$ happens to possess a rigid genus-0 four-tuple C of rational conjugacy classes. More precisely, if G is viewed in its transitive permutation action on 27 points, the

tuple $C := (C_1, C_1, C_2, C_3)$ is rigid, where C_1 denotes the class of involutions of cycle structure $(2^6.1^{15})$, C_2 the class of cycle structure $(4^6.1^3)$, and C_3 the class of length 720 whose elements have cycle structure $(6^4.3^1)$.

By $\mathcal{H}^{in}(C)$, we denote the (inner) Hurwitz space corresponding to the class vector (C_1, C_1, C_2, C_3), and by $\mathcal{C}$ the curve on $\mathcal{H}^{in}(C)$ corresponding to the branch point loci $(1+\sqrt{\lambda}, 1-\sqrt{\lambda}, 0, \infty)$ with $\lambda \in \mathbb{C} \setminus \{0, 1\}$. An oddness condition in the sense of Remark 2.9 is satisfied as elements in the class C_3 have unique cycles of length 3. Thus, the theory of Hurwitz spaces, see Chapter 2, yields the existence of polynomials $p, q \in \mathbb{Q}(\mathcal{C})[X]$ such that $f(t, X) := p(X) - tq(X)$ has regular Galois group $\mathrm{PSp}_4(3).C_2$ over $\mathbb{Q}(\mathcal{C})(t)$. Furthermore, the Hurwitz curve $\mathcal{C}$ comes equipped with the branch point reference map $\Psi : \mathcal{C} \to \mathbb{P}^1_\lambda$ of degree $|\,\mathrm{SNi}^{in}(C)|$. As we are in the special case of rigidity (i.e., $|\,\mathrm{SNi}^{in}(C)| = 1$), we have $\mathcal{C} = \mathbb{P}^1_\lambda$ and $\mathbb{Q}(\mathcal{C}) = \mathbb{Q}(\lambda)$ is a rational function field.

In the next sections we describe the computation of the polynomials $p, q \in \mathbb{Q}(\lambda)[X]$ following the algorithm in Chapter 3.

5.1.2. A complex approximation of a single 4-point cover. Our first step lies in computing a single 4-point cover $F : \mathbb{P}^1 \to \mathbb{P}^1$ with monodromy group $\mathrm{PSp}_4(3).C_2$ having the following ramification type:

branch point	1	-1	0	∞
inertia class	C_1	C_1	C_2	C_3
cycle structures	$2^6.1^{15}$	$2^6.1^{15}$	$4^6.1^3$	$6^4.3^1$

For such a cover F, the squared cover F^2 is a Belyi map with monodromy group contained in the wreath product $\mathrm{PSp}_4(3).C_2 \wr C_2$ and has the following ramification data:

branch point	1	0	∞
cycle structures	$2^{12}.1^{30}$	$8^6.2^3$	$12^4.6^1$

We now search in the wreath product $\mathrm{PSp}_4(3).C_2 \wr C_2$ for triples having the above cycle structures and generating a transitive group respecting the block structure. As it turns out there is exactly one such triple (up to simultaneous conjugation) and it generates the direct product $(\mathrm{PSp}_4(3).C_2) \times C_2 \leq (\mathrm{PSp}_4(3).C_2) \wr C_2$. It

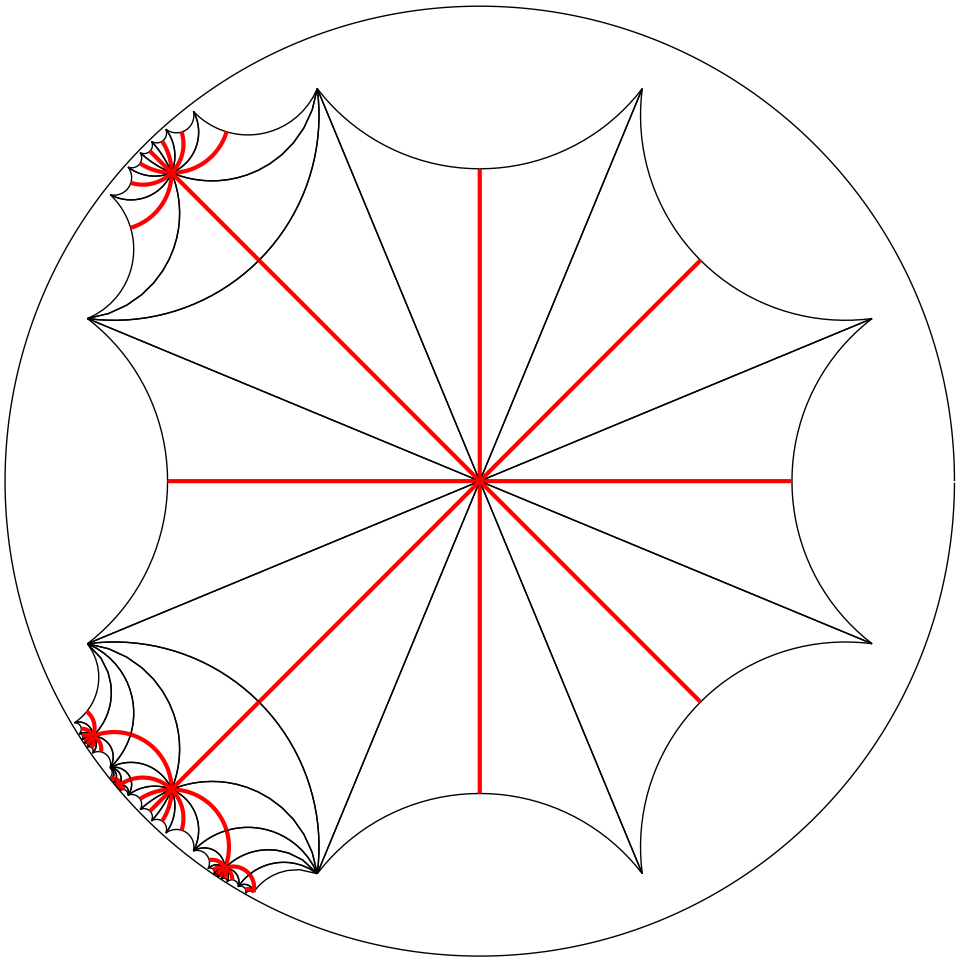


FIGURE 1. fundamental domain for $\mathrm{PSp}_4(3).C_2 \times C_2 \leq S_{54}$

is given by

$$\begin{aligned}
\sigma_0 &:= (1,51,18,53,6,41,23,39)(2,40,25,44,16,54,9,50)\\
&\quad (3,33,5,32,21,34,17,31)(4,46,10,42,20,48,24,52)(7,35)\\
&\quad (8,30,13,38,12,29,11,37)(14,49,22,47,27,43,19,45)(15,36)(26,28),\\
\sigma_1 &:= (8,10)(9,11)(14,15)(16,17)(20,21)(26,27)\\
&\quad (35,37)(36,38)(41,42)(43,44)(47,48)(53,54)
\end{aligned}$$

and $\sigma_\infty := (\sigma_0\sigma_1)^{-1}$.

Using the method described in Section 3.3 we compute a Belyi map corresponding to this triple. The fundamental domain used for the computation is given in Figure 1 whereas the resulting dessin is presented in Figure 2.

As the triple is rigid, the Belyi map $f_{54} = p_{54}/q_{54}$ of degree 54 turns out to be defined over $\mathbb{Q}$ and its rational coefficients can be recognized using continued

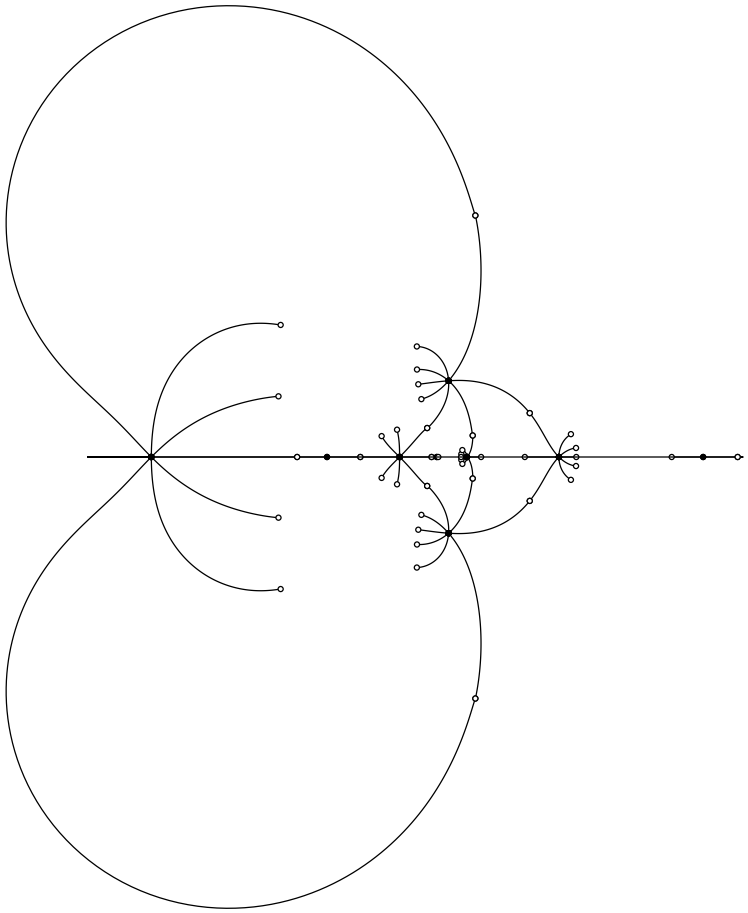


FIGURE 2. dessin d'enfant for $\mathrm{PSp}_4(3).C_2 \times C_2 \leq S_{54}$

fractions:

$$p_{54} = x^2 \left(x^2 - \frac{3}{2}\right)^2 \left(x^2 + \frac{3}{2}\right)^8 \left(x^4 - 9x^2 + \frac{9}{4}\right)^8,$$
$$q_{54} = 2^3 \cdot 3^6 \left(x^4 - 3x^2 - \frac{3}{4}\right)^{12}.$$

The Belyi map[1] is also contained in the file `psp43_data`.[2]

Taking the square root of $f_{54} = F^2$ yields the desired 4-point cover F of type C ramified over 1, -1, 0, ∞. This ramification locus is not yet of the form $1 \pm \sqrt{\lambda}$, 0, ∞, but after a slight deformation of the branch points followed by Newton iteration we actually obtain a cover f_0 with desired ramification locus lying on our Hurwitz curve.

[1]Note that the Belyi map p_{54}/q_{54} is a rational function in x^2. This is no surprise as its monodromy group $\mathrm{PSp}_4(3).C_2 \times C_2$ has blocks of size 2 (apart from those of size 27).
[2]All accompanying files are plain text files carrying the file extension `txt`. For better readability we usually omit the file extension.

5.1.3. Turning a single cover into a family. The next step is to compute $f(t,X) = p(X) - tq(X) \in \mathbb{Q}(\lambda)(t)[X]$ with Galois group $\mathrm{PSp}_4(3).C_2$ and class vector C starting from the previously computed cover f_0.

The covers in our family have unique poles of multiplicity 3 which we assume to lie at ∞. Together with the cycle structures occurring in the class vector C, this implies that f has the following form:

$$f(t,X) = c \cdot p_3(X)p_6(X)^4 - tq_4(X)^6 \tag{5.1}$$

with $c \in \mathbb{Q}(\lambda)$ and monic polynomials $p_3, p_6, q_4 \in \mathbb{Q}(\lambda)[X]$ with $\deg(p_3) = 3$, $\deg(p_6) = 6$ and $\deg(q_4) = 4$. Using affine-linear transformations in X we further assume the following *normalization condition*:[3]

$$p_3(X) = X^3 + aX + a \text{ for some } a \in \mathbb{Q}(\lambda). \tag{5.2}$$

Now, starting from the cover f_0 computed in the previous section (ramified over $1 \pm \sqrt{\lambda_0}, 0, \infty$), we first apply the above normalization condition to f_0, and afterwards slightly move λ_0 to nearby rational values and use Newton iteration to adjust the coefficients of f_0.

Since every coefficient occurring in equation (5.1) is some rational function in λ, we can then recognize all coefficients as rational numbers (via continued fractions). Doing this for many rational values for λ we obtain data that can be interpolated to express all coefficients of f explicitly as rational functions in λ.

5.1.4. Verification. After slight simplifications using transformations in X and λ we obtain the following particularly nice parametric family of polynomials with group $\mathrm{PSp}_4(3).C_2$, see also `psp43_data`.

THEOREM 5.1. *Let*

$$\begin{aligned} p(\alpha,X) := &\left(2X^6 - 10\alpha X^4 + 10\alpha X^3 - 10\alpha^2X^2 + 2\alpha^2X + 2\alpha^3 - \alpha^2\right)^4 \cdot \\ &\left(4X^3 - 4\alpha X + \alpha\right) \end{aligned}$$

and

$$q(\alpha,X) := \left(3X^4 - 6\alpha X^2 + 3\alpha X - \alpha^2\right)^6.$$

Then, the polynomial $f(\alpha,t,X) := p(\alpha,X) - tq(\alpha,X) \in \mathbb{Q}(\alpha,t)[X]$ *has regular Galois group* $\mathrm{PSp}_4(3).C_2 \leq S_{27}$ *over* $\mathbb{Q}(\alpha,t)$ *and branch cycle structure* $(2^6.1^{15}, 2^6.1^{15}, 4^6.1^3, 6^4.3^1)$ *with respect to* t.

[3]Our usual approach described in 3.2.2 setting the traces of two polynomials to 0 and 1, respectively, fails here: After setting any trace to 0 all other traces vanish as well.

PROOF. The branch cycle structure can be easily computed by observing the inseparability behaviour of p, q and of the specialized polynomials $f(\alpha, t_0, X)$, where $t_0 \in \mathbb{Q}(\sqrt{3\alpha})$ is a non-zero root of the discriminant $\Delta(\alpha, t) \in \mathbb{Q}(\alpha)[t]$ of f. Next, a computer calculation shows that $p(X)q(Y) - q(X)p(Y)$ is reducible in $\mathbb{Q}(\alpha)[X, Y]$, with three factors of X-degree 1, 10 and 16, respectively. Now, Corollary 4.2 implies that the arithmetic monodromy group $A := \mathrm{Gal}(f \mid \mathbb{Q}(\alpha, t))$ has subdegrees 1, 10 and 16. As Lemma 4.15 states that $\mathrm{PSp}_4(3)$ and $\mathrm{PSp}_4(3).C_2$ are the only groups with these subdegrees, we get $A = \mathrm{PSp}_4(3)$ or $A = \mathrm{PSp}_4(3).C_2$. Since the geometric monodromy group G of f is a transitive normal subgroup of A, we also get $G = \mathrm{PSp}_4(3)$ or $G = \mathrm{PSp}_4(3).C_2$. The inseparability behaviour at one of the finite, non-zero branch points shows that G contains an element of cycle structure $(2^6.1^{15})$, which $\mathrm{PSp}_4(3)$ does not. This shows $A = G = \mathrm{PSp}_4(3).C_2$ and, in particular, the splitting field of f is regular. □

It turns out that also the index-2 subgroup $\mathrm{PSp}_4(3)$ can be explicitly realized over a rational function field in two variables:

COROLLARY 5.2. *Let $f(\alpha, t, X)$ be as in Theorem 5.1. Then the polynomial $f(3\alpha^2, t(s), X)$ where*

$$t(s) := \frac{((-8\alpha/3)^3 + (-8\alpha/3)^2)\,(3s^2 - (\alpha + 3/8)/(\alpha - 3/8))}{3s^2 + 1}$$

has Galois group $\mathrm{PSp}_4(3)$ over $\mathbb{Q}(\alpha, s)$.

PROOF. Note that only the conjugacy class C_1 lies outside the index-2 normal subgroup $\mathrm{PSp}_4(3)$. Furthermore, upon replacing α by $3\alpha^2$ (which does not change the Galois group), computation of the discriminant of f shows that the two branch points with inertia group generator in C_1 become $\mathbb{Q}(\alpha)$-rational, say $t \mapsto k$ and $t \mapsto \ell$ with $k, \ell \in \mathbb{Q}(\alpha)$.[4] Let N denote the splitting field of $f(3\alpha^2, t, X)$ over $\mathbb{Q}(\alpha, t)$ and $K \leq N$ the quadratic extension of $\mathbb{Q}(\alpha, t)$ fixed by $\mathrm{PSp}_4(3)$.

The previous observations imply that $K \mid \mathbb{Q}(\alpha, t)$ is (with respect to t) ramified at exactly two points, both rational, yielding that K is a rational function field, given by an equation $cY^2 = (t - k)(t - \ell)$ for some $c \in \mathbb{Q}(\alpha)$.

To determine the missing unknown c we follow an approach similar to the proof of [**41**, Satz 8.7]: Denote by K_∞ and N_∞ the residue fields of K and N at some place lying over $t \mapsto \infty$. Note that N_∞ is the splitting field of $3X^4 - 6(3\alpha^2)X^2 + 3(3\alpha^2)X - (3\alpha^2)^2$ over $\mathbb{Q}(\alpha)$, having Galois group S_4

[4] More precisely, k and ℓ are given by $\frac{64}{27}\alpha^2(3 \pm 8\alpha)$.

and, consequently, containing a unique degree-2 subfield, which can be easily computed to be $\mathbb{Q}(\alpha)(\sqrt{-3})$. From $[K_\infty : \mathbb{Q}(\alpha)] \leq 2$ we get that K_∞ must be contained in this unique degree-2 subfield of N_∞, i.e., $\mathbb{Q}(\alpha) \leq K_\infty \leq \mathbb{Q}(\alpha)(\sqrt{-3})$.

On the other hand, using the defining equation for K, the residue field K_∞ can easily be seen to be equal to $\mathbb{Q}(\alpha)(\sqrt{c})$. The previous facts together now imply that $c = -3$ or $c = 1$ (up to squares). The latter case can be easily excluded by observing that the Galois group of $f(3\alpha^2, t, X)$ is preserved after specializing t to some value that corresponds to a rational point on the curve $1Y^2 = (t-k)(t-\ell)$. Thus $c = -3$.

Now, a fractional linear transformation easily yields a parameter s for such a function field, providing the equation $t = t(s)$ as above. □

REMARK. We mention briefly that the value for c could also have been obtained in an alternative way by inspecting the ramification behaviour of the $\mathrm{PSp}_4(3)$-extension $N \mid K$ and combining Fried's branch cycle argument with the fact that C_3 is a non-rational conjugacy class of $\mathrm{PSp}_4(3)$ (with character values generating the field $\mathbb{Q}(\sqrt{-3})$). For a similar application with a more detailed description see [**11**, Section 2.6].

5.2. Totally real polynomials with Galois group $\mathrm{PSp}_6(2)$

A classical variant of the inverse Galois problem is the question whether, for a given finite group G, there exists a Galois extension $F \mid \mathbb{Q}$ with $F \subset \mathbb{R}$ such that $\mathrm{Gal}(F \mid \mathbb{Q}) \cong G$. It is known that if every finite group is a Galois group over $\mathbb{Q}$, then also every finite group is a Galois group of such a totally real extension, see [**32**, Proposition 1].

Computation of multi-branch-point covers is particularly important for the computation of totally real Galois extensions. This is due to the fact that, with very few exceptions, a $\mathbb{Q}$-regular Galois extension of $\mathbb{Q}(t)$ with totally real specializations (that is, specializations in t leading to totally real residue fields) must have at least 4 branch points, see [**38**, Example I.10.2].

In the current section we compute the first polynomials with Galois group $\mathrm{PSp}_6(2)$ that allow infinitely many totally real specializations.[5]

[5]A Belyi map over $\mathbb{Q}$ with monodromy group $\mathrm{PSp}_6(2)$ can be found in [**38**, p. 500].

5.2.1. Theoretical properties. First, we deduce the existence of totally real $\mathrm{PSp}_6(2)$-realizations theoretically from known criteria. For this, we view $\mathrm{PSp}_6(2) < S_{28}$ in its 2-transitive action on 28 points. We define

(i) C_1 to be the (unique) conjugacy class of involutions of cycle structure $(2^6.1^{16})$ in G,
(ii) C_2 the class of involutions of cycle structure $(2^{12}.1^4)$ and length 3780,
(iii) and C_3 the class of elements of order 7 (and cycle structure (7^4)).

By $\mathcal{H}^{in}(C)$, we denote the Hurwitz space corresponding to the rational class vector $C := (C_1, C_2, C_2, C_3)$, and by $\mathcal{C}$ the curve on $\mathcal{H}^{in}(C)$ corresponding to the branch point loci $(0, 1-\sqrt{\lambda}, 1+\sqrt{\lambda}, \infty)$ with $\lambda \in \mathbb{C} \setminus \{0, 1\}$.

Rationality of the Hurwitz curve. The Hurwitz curve $\mathcal{C}$ comes equipped with the branch point reference map $\Psi : \mathcal{C} \to \mathbb{P}^1_\lambda$ with branch cycle description given by $(\tilde{\beta}_1, \tilde{\beta}_2, \tilde{\beta}_3)$ acting on $\mathrm{SNi}^{in}(C)$. Using equation (2.4) a Magma computation yields that the monodromy group $\langle \tilde{\beta}_1, \tilde{\beta}_2, \tilde{\beta}_3 \rangle$ of Ψ acts transitively on $\mathrm{SNi}^{in}(C)$. Together with the rationality of C we obtain that $\mathcal{C}$ is an absolutely irreducible curve defined over $\mathbb{Q}$.

Closer examination yields that Ψ is of degree 70 and the inertia group generators $\tilde{\beta}_1$, $\tilde{\beta}_2$, $\tilde{\beta}_3$ act on $\mathrm{SNi}^{in}(C)$ with cycle structures $(15^1.12^2.9^1.8^1.7^2)$, $(3^{13}.2^{14}.1^3)$ and (2^{35}). Since there is a unique cycle of length 15 in the first permutation, the Riemann–Hurwitz genus formula and Remark 2.9 yield that $\mathcal{C}$ is a rational genus-0 curve over $\mathbb{Q}$; that is, $\mathcal{C} = \mathbb{P}^1_\alpha$ for some parameter α. Consequently, the universal family $\mathcal{T}_\mathcal{C} \to \mathcal{C} \times \mathbb{P}^1$ can be parameterized by a multi-parameter polynomial $f(\alpha, t, X) \in \mathbb{Q}(\alpha)(t)[X]$.

Rationality of the stem field. Next, observe that the tuples in our Nielsen class are of genus 0 and that the normalizer in G of a cyclic subgroup generated by an element of C_3 fixes one of the 7-cycles. This ensures that the degree-28 root field of $f(t, X)$ is a rational genus-0 function field, compare Remark 2.9. It follows that the polynomial $f(t, X)$ can be assumed to be linear in t, i.e., $f(t, X) = p(X) - tq(X)$ for coprime polynomials $p, q \in \mathbb{Q}(\alpha)[X]$.

Existence of totally real specializations. Furthermore, the above Nielsen class contains tuples $(\sigma_1, \sigma_{2,1}, \sigma_{2,2}, \sigma_3)$ fulfilling $\sigma_3 = (\sigma_3^{-1})^{\sigma_{2,2}}$ and $\sigma_1 = (\sigma_1^{-1})^{\sigma_{2,1}}$. Theorem 10.3 in Chapter I of **[38]** now implies that there are G-covers $X \to \mathbb{P}^1$ of ramification type (C_1, C_2, C_2, C_3), defined over $\mathbb{R}$, such that all four branch points are real and the complex conjugation in the segment between the two branch points of class C_2 is induced by the identity element of G. Since the rational points of (the rational genus-0 curve) $\mathcal{C}$ are dense in the set of

real points, there are also infinitely many G-covers with the above property that correspond to rational points on $\mathcal{C}$. Each of those yields a $\mathbb{Q}$-regular Galois extension $E \mid \mathbb{Q}(t)$ of ramification type (C_1, C_2, C_2, C_3) such that any specialization $t_0 \in \mathbb{Q}$ in the segment between the two C_2-branch points yields a totally real extension. Of course, Hilbert's irreducibility theorem ensures that many of these specializations preserve the Galois group G.

We now turn these theoretical results into an explicit polynomial, using the approach outlined in Chapter 3.

5.2.2. A complex approximation of a single 4-point cover. As explained before, we start by computing an approximate equation for a decomposable genus zero Belyi map $X \to \mathbb{P}^1$ such that the following holds: for a degree-2 subcover Y of $X \to \mathbb{P}^1$, the (genus zero) cover $X \to Y$ has ramification type (C_1, C_2, C_2, C_3). Then $X \to \mathbb{P}^1$ is of degree 56 with monodromy group embedding into $\mathrm{PSp}_6(2) \wr C_2$, and if $(\sigma_0, \sigma_1, \sigma_\infty) \in S_{56}^3$ is a triple describing the ramification of this Belyi map, the elements σ_0, σ_1 and σ_∞ are of cycle structure (14^4), $(2^{24}, 1^8)$ and $(4^6, 2^{16})$, respectively.

A computer computation shows that there are 35 triples (up to simultaneous conjugation) in $\mathrm{PSp}_6(2) \wr C_2$ satisfying property (ii) from Section 3.2.1. Among these possible triples the permutations $\sigma_0, \sigma_1, \sigma_\infty = (\sigma_0\sigma_1)^{-1}$ can be chosen arbitrarily. We pick

$$\begin{aligned}\sigma_0 = &(1, 55, 27, 36, 8, 54, 26, 32, 4, 50, 22, 30, 2, 29)\\ &(3, 34, 6, 35, 7, 56, 28, 42, 14, 52, 24, 40, 12, 31)\\ &(5, 47, 19, 45, 17, 37, 9, 43, 15, 49, 21, 44, 16, 33)\\ &(10, 51, 23, 39, 11, 46, 18, 53, 25, 48, 20, 41, 13, 38)\end{aligned}$$

and

$$\begin{aligned}\sigma_1 = &(1, 20)(3, 6)(4, 21)(5, 15)(8, 25)(9, 19)(10, 18)\\ &(11, 24)(12, 23)(13, 22)(14, 28)(16, 26)(30, 41)\\ &(31, 52)(32, 44)(33, 49)(35, 56)(36, 48)(37, 45)\\ &(38, 53)(39, 40)(43, 47)(46, 51)(50, 54).\end{aligned}$$

Using the method described in Section 3.3 we compute a Belyi map corresponding to this triple. The fundamental domain used for the computation is given in Figure 3 and the resulting dessin is shown in Figure 4. A complex approximation (after refinement using Newton's method) for the resulting Belyi

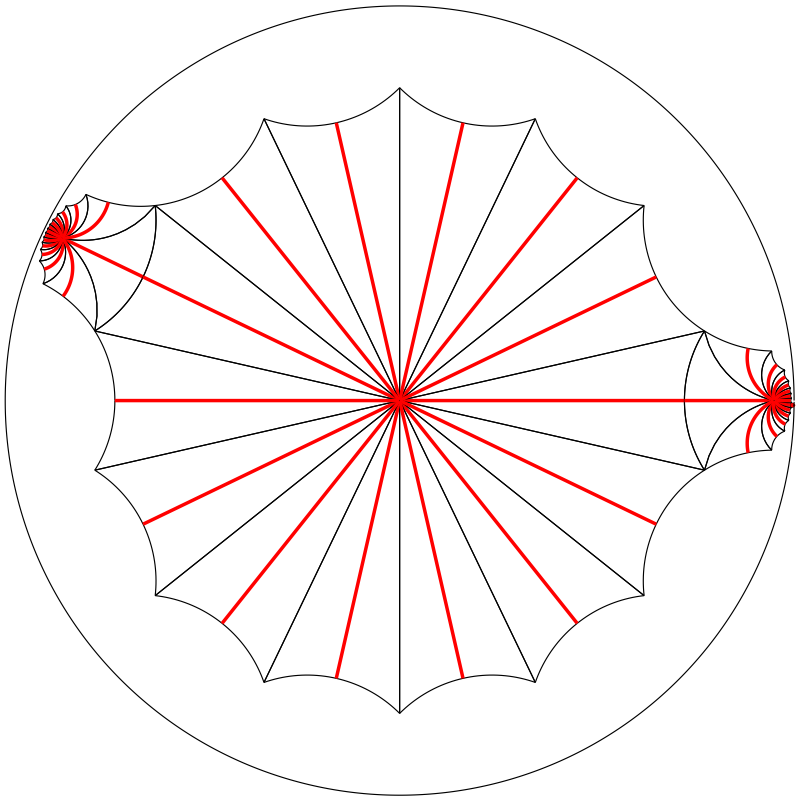


FIGURE 3. fundamental domain for $\mathrm{PSp}_6(2) \wr C_2 \leq S_{56}$

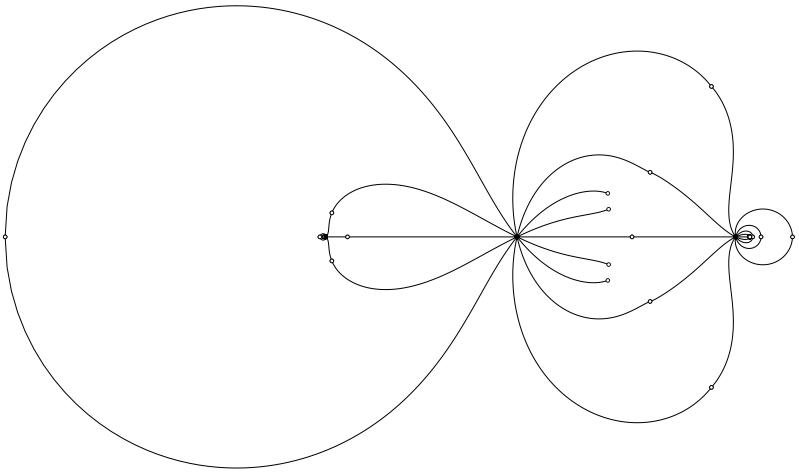


FIGURE 4. dessin for $\mathrm{PSp}_6(2) \wr C_2 \leq S_{56}$

map can be found in the ancillary file `psp62_deg28_data`.[6] As a subcover of the computed Belyi map, we obtain a 4-point cover f_0 with class vector C from which we will start to interpolate the universal family in the next section.

[6]We remark that it is not necessary to recognize the Belyi map's coefficients as algebraic numbers (presumably lying in a degree-35 number field).

5.2.3. Turning a single cover into a family. According to the ramification over $t \mapsto 0$ and $t \mapsto \infty$ and the fact that one place over $t \mapsto \infty$ is fixed by the normalizer of the respective inertia group and can be assumed to lie at $X \mapsto \infty$, the universal family $\mathcal{T}_\mathcal{C} \to \mathcal{C} \times \mathbb{P}^1$ can be parameterized by

$$f(t, X) = c \cdot f_6(X)^2 f_{16}(X) - t f_3(X)^7,$$

with $c \in \mathbb{Q}(\alpha)$ and monic polynomials $f_6, f_{16}, f_3 \in \mathbb{Q}(\alpha)[X]$ satisfying $\deg(f_6) = 6$, $\deg(f_{16}) = 16$ and $\deg(f_3) = 3$.

Since a generator of the (rational!) root field of $f(t, X)$ is only unique up to PGL_2-action, we may apply linear transformations in X and fix the coefficient at X^2 in f_3 to be 0 and the one at X^5 in f_6 to be 1. It is vital for the method's success that we apply the same normalization conditions to the 4-point cover f_0 computed in the previous section. In particular, one needs to pick the correct of the four poles to be sent to infinity.

Starting from the cover f_0, we now let the coefficient β at X^{15} in f_{16} converge to a rational value, using Newton approximation. Afterwards, given a sufficient complex precision, we recognize the coefficient γ at X^1 in f_3 in a degree-5 number field using the LLL algorithm. Doing this for several rational values of β, we obtain by interpolation the following algebraic dependency between β and γ (viewed as transcendentals):

$$\begin{aligned}
0 &= \gamma^5 + (285/448 \cdot \beta^2 - 47/56 \cdot \beta - 421/126)\gamma^4 \\
&+ (34785/351232 \cdot \beta^4 - 20037/87808 \cdot \beta^3 - 61871/65856 \cdot \beta^2 \\
&- 95161/98784 \cdot \beta + 868717/148176)\gamma^3 + \\
&(-351/702464 \cdot \beta^6 + 4833/702464 \cdot \beta^5 + 4119/351232 \cdot \beta^4 \\
&- 89063/175616 \cdot \beta^3 + 168267/87808 \cdot \beta^2 - 2783/4032 \cdot \beta - 1331/12348)\gamma^2 + \\
&(405/275365888 \cdot \beta^8 - 2403/34420736 \cdot \beta^7 + 13863/9834496 \cdot \beta^6 - \\
&38511/2458624 \cdot \beta^5 + 253495/2458624 \cdot \beta^4 - 552365/1382976 \cdot \beta^3 + \\
&4582633/5531904 \cdot \beta^2 - 2093663/3226944 \cdot \beta - 23030293/130691232)\gamma + \\
&243/53971714048 \cdot \beta^{10} - 7209/26985857024 \cdot \beta^9 + 93969/13492928512 \cdot \beta^8 - \\
&176187/1686616064 \cdot \beta^7 + 238733/240945152 \cdot \beta^6 - 2221439/361417728 \cdot \beta^5 + \\
&13513643/542126592 \cdot \beta^4 - 183437089/2846164608 \cdot \beta^3 + \\
&1755616951/17076987648 \cdot \beta^2 - 2669742427/25615481472 \cdot \beta + 2786665453/38423222208.
\end{aligned}$$

It is now easy to find the yet unknown parameter α of $\mathbb{Q}(\beta, \gamma) = \mathbb{Q}(\alpha)$ using a Riemann–Roch space computation as described in [**33**, Lemma 3.16].

Finally, we use Newton approximation again to let α converge to several rational values. Then all the coefficients of f_6, f_{16}, f_3 must also be rational

values. These can easily be recognized from their complex approximation, and interpolating between these several values once again yields dependencies between α and each coefficient, i.e., expressions of each coefficient as a rational function in α.

5.2.4. Verification. We then obtain a polynomial $f = f(\alpha, t, X) \in \mathbb{Q}[\alpha, t, X]$ whose Galois group over $\mathbb{Q}(\alpha, t)$ is expected to be isomorphic to $\mathrm{PSp}_6(2)$. Since the coefficients of f are too large to present it here, we refer to the file `psp62_deg28_data`.

THEOREM 5.3. *The polynomial $f(\alpha, t, X) = p(\alpha, X) - tq(\alpha, X)$, where p and q are given in the file `psp62_deg28_data`, has regular Galois group $\mathrm{PSp}_6(2) \leq S_{28}$ over $\mathbb{Q}(\alpha, t)$ and possesses infinitely many totally real specializations. The ramification with respect to t is of type $(2^6.1^{16}, 2^{12}.1^4, 2^{12}.1^4, 7^4)$.*

PROOF. Let $f_2, p_2, q_2 \in \mathbb{Q}(t)[X]$ denote the specializations of f, p, q at the place $\alpha \mapsto 2$, and $\bar{f}_2, \bar{p}_2, \bar{q}_2$ their images in $\mathbb{F}_{31}(t)[X]$ under the canonical projection. By computing the discriminant Δ of f we see that f, f_2 and $\bar{f}_2$ have exactly four branch points with respect to t. Furthermore, the branch cycle structure of f can be derived by inspecting the inseparability behaviour of f evaluated at the places $t \mapsto 0$, $t \mapsto \infty$, and $t \mapsto r_i$ for $i = 1, 2$ where r_1 and r_2 denote the non-zero roots of $\Delta \in \mathbb{Q}(\alpha)[t]$.

Since $\frac{1}{X-t} \cdot \bar{f}_2\left(\frac{\bar{p}_2(t)}{\bar{q}_2(t)}, X\right) \in \mathbb{F}_{31}(t)[X]$ is irreducible, the Galois group of $\bar{f}_2$ over $\mathbb{F}_{31}(t)$ must be 2-transitive according to Corollary 4.2. As the — even further specialized — polynomial $\bar{f}_2(1, X)$ splits into irreducible polynomials of degrees $3, 5, 5, 15$; Dedekind's criterion yields that the order of $\mathrm{Gal}(\bar{f}_2 \mid \mathbb{F}_{31}(t))$ is divisible by 5. Due to the classification of finite 2-transitive groups the only 2-transitive groups of degree 28 having elements of order 5 are $\mathrm{PSp}_6(2)$, A_{28}, S_{28} which implies $\mathrm{Gal}(\bar{f}_2 \mid \mathbb{F}_{31}(t)) \in \{\mathrm{PSp}_6(2), A_{28}, S_{28}\}$. Let $r(t, X) \in \mathbb{F}_{31}(t)[X]$ be the irreducible polynomial of degree 63 in the ancillary file `psp62_deg28_data`, then $r\left(\frac{\bar{p}_2(t)}{\bar{q}_2(t)}, X\right)$ becomes reducible over $\mathbb{F}_{31}(t)$. Due to Proposition 4.6 this guarantees the existence of an index-d subgroup of $\mathrm{Gal}(\bar{f}_1 \mid \mathbb{F}_{31}(t))$ where $d \neq 1$ is a divisor of 63. Since A_{28} and S_{28} do not contain such subgroups, we end up with $\mathrm{Gal}(\bar{f}_2 \mid \mathbb{F}_{31}(t)) = \mathrm{PSp}_6(2)$. As $\mathrm{PSp}_6(2)$ is simple and the geometric monodromy group $\bar{G}$ of $\bar{f}_2$ is normal in $\mathrm{Gal}(\bar{f}_2 \mid \mathbb{F}_{31}(t)) = \mathrm{PSp}_6(2)$, we get $\bar{G} = \mathrm{PSp}_6(2)$.

By the arguments in Sections 4.3.1 and 4.3.2, the geometric monodromy groups of f and $\bar{f}_2$ coincide; thus, the geometric monodromy group of f is equal

to $\mathrm{PSp}_6(2)$. Since $\mathrm{PSp}_6(2)$ is self-normalizing in S_{28}, we obtain that f defines a regular $\mathrm{PSp}_6(2)$-extension of $\mathbb{Q}(\alpha, t)$.

Finally, we specialize $\alpha \mapsto 0$ (which does not decrease the number of branch points) and verify that for some specialization of t in the interval $[-2.8 \cdot 10^{12}, 0]$ (the left bound being approximately the only negative branch point of $f(0, t, X)$), the number of real roots of $f(0, t, X)$ is equal to 28. The same then follows for *all* specializations $t \mapsto t_0$ in that interval; indeed, it is elementary that the number of real preimages of $t \in \mathbb{R}$ under a rational function $s(X) \in \mathbb{R}[X]$ can only change (as a function in t) at a critical value of $s(X)$, i.e., at a branch point of the corresponding function field extension. □

REMARK. The Magma calculations used in the proof can be found in the ancillary file `psp62_deg28_verify`. Furthermore, in the original proof contained in [**4**], it was mistakenly assumed that there are no 2-transitive groups of degree 28 besides $\mathrm{PSp}_6(2)$, A_{28} and S_{28}. In the modified proof given above this minor gap was fixed by showing that the group order is divisible by 5.

REMARK. For the primitive rank-3 group $\mathrm{PSp}_4(3).C_2$ from Section 5.1 computing the subdegrees was the main part of the verification process. However, as the group $\mathrm{PSp}_6(2) \leq S_{28}$ is 2-transitive we needed to make use of some of the more advanced tools as described in Section 4.2.1:

Consulting the ATLAS [**17**] yields that $\mathrm{PSp}_6(2)$ possesses a permutation character π' of degree 63 decomposing into irreducible characters as follows $\pi' = 1_G + \pi_{27} + \pi_{35}$. Here π_{27} and π_{35} are of degree 27 and 35, respectively, and $\pi := 1_G + \pi_{27}$ is the permutation character corresponding to the 2-transitive permutation action of degree 28. The splitting behaviour of $r\left(\frac{\bar{p}_2(t)}{\bar{q}_2(t)}, X\right)$ in the proof above is explained by $[\pi, \pi'] = 2$. The auxiliary polynomial r was computed with respect to the degree-63 permutation representation π' using the Magma commands `GaloisGroup` and `GaloisSubgroup`.

We conclude with an explicit one-parameter polynomial allowing totally-real specializations: Specializing $\alpha \mapsto 0$ in p and q from Theorem 5.3 and applying some linear transformations to decrease the coefficients, we obtain the following:

COROLLARY 5.4. *Let* $\tilde{f}(t, X) :=$

$(X^6 - 33/2X^5 - 42924X^4 - 1525664X^3 + 477587712X^2 + 40478785536X + 863547424768)^2 \cdot$

$(X^{16} + 271X^{15} - 430719/4X^{14} - 35366300X^{13} + 3314214496X^{12} + 1797598385556X^{11}$

$+ 28249865746816X^{10} - 4251753969397894X^9 - 3546884171151604080X^8 +$

$38816528964236519552X^7 + 67637298931930365811712X^6 + 11573759790022038591897 60X^5$

$-37036504465003866103644160 0X^4 - 30197279842907494819422011392X^3 - 81483048856896074491717327257 6X^2 + 16266668951133534171190997811 2X + 25603832558094671580474913901772 8) - t\left(X^3 - 21952X - 1229312\right)^7 \in \mathbb{Q}(t, X)$.
Then every specialization of t in the interval $[-4.9 \cdot 10^{13}, 0]$ which preserves the Galois group yields a totally real $\mathrm{PSp}_6(2)$-polynomial.

5.3. Multi-parameter degree-36 polynomials with Galois group $\mathrm{PSp}_6(2)$

In this section we present a multi-parameter polynomial of degree 36 having Galois group $\mathrm{PSp}_6(2)$ over $\mathbb{Q}$. It was computed by Andreas Wenz and the author and firstly appeared as a note [**9**] on the arXiv. Later, the polynomial was incorporated in the journal article [**4**]. Additionally, we present a complex approximation for a 5-point cover with monodromy group $\mathrm{PSp}_6(2) \leq S_{36}$.

5.3.1. Theoretical properties. Let $C := (C_1, C_2, C_2, C_3)$ be the class vector of the 2-transitive group $\mathrm{PSp}_6(2) \leq S_{36}$, where the conjugacy classes C_1, C_2, C_3 are unique of type (3^{12}), $(1^{12}.2^{12})$ and $(1^6.2^1.4^7)$, respectively. Denote by $\mathcal{C}$ the associated Hurwitz curve parameterizing all 4-point covers of $\mathbb{P}^1\mathbb{C}$ ramified over 0, $1 \pm \sqrt{\lambda}$, ∞ with ramification data C. The corresponding straight inner Nielsen class is of length 2 and forms a single orbit under the braid group action. Therefore, the branch point reference map $\mathcal{C} \to \mathbb{P}^1\mathbb{C}$ is of degree 2 and is ramified over two rational points. Combining this observation with the rationality of all classes in C yields that $\mathcal{C}$ is a rational genus-0 curve over $\mathbb{Q}$. This implies that $\mathrm{PSp}_6(2)$ occurs as a Galois group over $\mathbb{Q}(\alpha, t)$ where the ramification with respect to t is described by C.

5.3.2. A complex approximation of a single 4-point cover. In order to obtain an explicit polynomial with $\mathrm{PSp}_6(2)$ as Galois group we follow the method described in Chapter 3 by firstly computing a single 4-point cover F corresponding to C. Assume F has the ramification locus consisting of $0, 1, -1, \infty$; then F^2 turns out to be a Belyi map ramified over 0, 1, ∞, and its (transitive) monodromy group is contained in the imprimitive wreath product $\mathrm{PSp}_6(2) \wr C_2 \leq S_{72}$. The corresponding ramification has to be of type (6^{12}), $(1^{24}.2^{24})$ and $(2^6.4^1.8^7)$. Now, $\mathrm{PSp}_6(2) \wr C_2$ contains exactly one triple $(\sigma_0, \sigma_1, \sigma_\infty)$ (up to simultaneous conjugation) which satisfies $\sigma_0\sigma_1\sigma_\infty = 1$ and the above

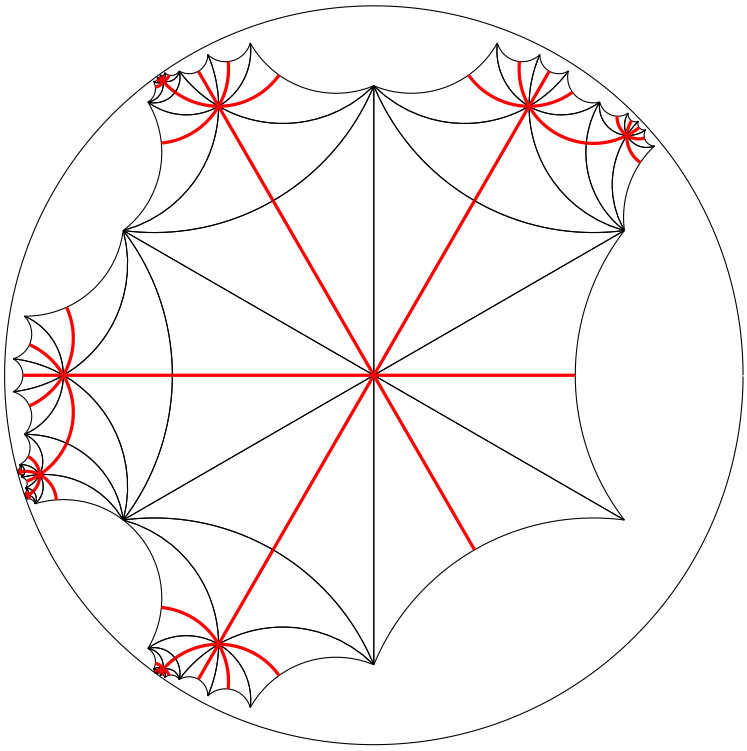


FIGURE 5. fundamental domain for $\mathrm{PSp}_6(2) \wr C_2 \leq S_{72}$

conditions describing the monodromy of F^2. It is given by

$$\begin{aligned}\sigma_0 = {} & (1,37,16,70,23,59)(2,51,13,43,7,49)(3,39,32,71,28,46)\\ & (4,66,26,72,34,52)(5,42,31,67,10,64)(6,41,22,69,29,65)\\ & (8,56,12,48,21,54)(9,45,30,40,14,50)(11,47,33,58,18,57)\\ & (15,38,19,60,24,55)(17,53,20,44,35,68)(25,61,27,63,36,62)\end{aligned}$$

and

$$\begin{aligned}\sigma_\infty = {} & (1,71,35,40,4,52,16,37)(2,46,10,67,31,65,29,38)\\ & (3,49,13,56,20,68,32,39)(5,64,28,59,23,72,36,41)(6,42)\\ & (7,43)(8,54,18,66,30,50,14,44)(9,45)(11,57,21,47)\\ & (12,51,15,55,19,69,33,48)(17,53)(22,63,27,61,25,62,26,58)\\ & (24,60)(34,70).\end{aligned}$$

Applying the method explained in Section 3.3 we compute the desired Belyi map with branch cycle description $(\sigma_0, \sigma_1, \sigma_\infty)$:

$$F^2(X) = \frac{p(X)}{q(X)} \in \mathbb{Q}(X)$$

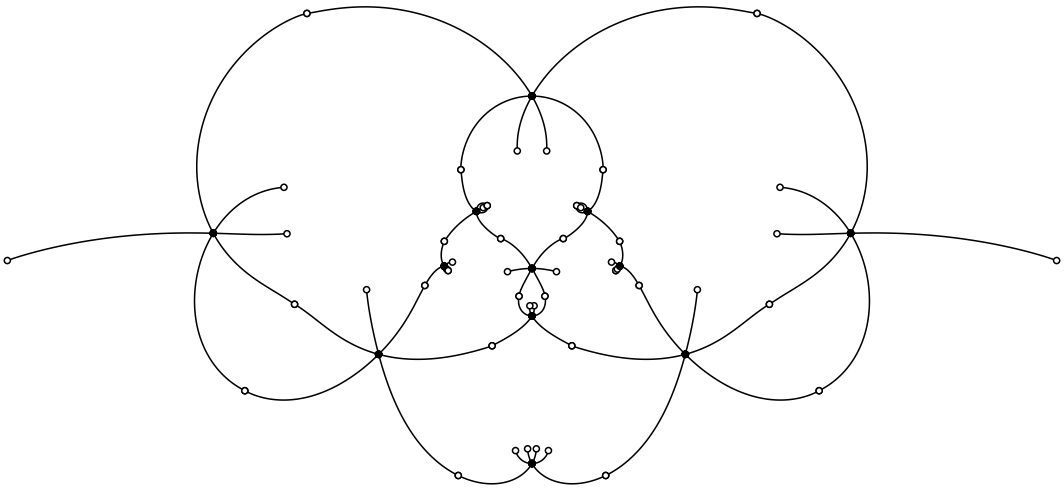


FIGURE 6. dessin for $\mathrm{PSp}_6(2) \wr C_2 \leq S_{72}$

where

$$\begin{aligned} p(X) = & -\left(X^{12} + 8X^{11} - 10X^{10} - 40X^9 - 69X^8 - 96X^7 - 84X^6\right. \\ & \left. -48X^5 - 21X^4 - 40X^3 - 26X^2 - 8X + 1\right)^6, \\ q(X) = & \, 2^4 \cdot 3^8 \cdot \left(X^3 + 3X + 2\right)^8 \left(X^4 + \frac{4}{3}X^3 - \frac{1}{3}\right)^8 \left(X^6 + \frac{3}{2}X^4 + \frac{1}{2}\right)^2. \end{aligned}$$

The fundamental domain used in the computation and the approximate resulting dessin are shown in Figure 5 and Figure 6, respectively. Taking the square root gives us $F \in \mathbb{C}(X)$ ramified over 0, 1, -1 and ∞. Next, we follow the approach in Section 3.2.2 to find a one-parameter family of polynomials with Galois group $\mathrm{PSp}_6(2)$ over $\mathbb{Q}(t)$ corresponding to $\mathcal{C}$.

5.3.3. Turning a single cover into a family. The covers parameterized by $\mathcal{C}$ have a unique pole of multiplicity 2 which we assume to lie at ∞. Combined with the cycle structures occurring in C, this yields the following form for the polynomial f describing the universal family of covers:

$$f(t, X) = c \cdot p_{12}(X)^3 - t q_6(X) q_7(X)^4$$

with monic polynomials $p_{12}, q_6, q_7 \in \mathbb{Q}(\mathcal{C})[X]$ of respective degree as denoted in the index and some scalar $c \in \mathbb{Q}(\mathcal{C})$. Using affine-linear transformations in X we further assume that the coefficient at X^{11} in p_{12} is 1 while the coefficient at X^5 in q_6 is assumed to be 0.

Now, we let λ converge to nearby rational numbers and recognize the other coefficients in degree-2 number fields. Interpolation yields dependencies between λ and other coefficients (viewed as transcendentals). For example, c and λ obey

the equation

$$6561c^2 - 2592c - 256\lambda + 256 = 0. \tag{5.3}$$

As $\mathbb{Q}(\lambda)$ has index-2 in the Hurwitz curve's function field $\mathbb{Q}(\mathcal{C})$, we deduce $\mathbb{Q}(\mathcal{C}) = \mathbb{Q}(\lambda, c)$. Inspecting the explicit equation (5.3) it turns out that c can be chosen as parameter of the Hurwitz curve, i.e., $\mathbb{Q}(\lambda, c) = \mathbb{Q}(c)$. In particular, in this example there is no need for computing Riemann–Roch spaces.

Thus, all coefficients of f must lie in the rational function field $\mathbb{Q}(c)$. We now let c (instead of λ) converge to several rational values and recognize the other coefficients as rational numbers. Interpolating yields explicit representations of all coefficients of f as rational functions in c. After simplification using Möbius transformations we obtain the following nice polynomials:

$$\begin{aligned} p(\alpha, X) = \Bigg(& X^{12} + X^{11} + \left(144\alpha + \frac{1}{8}\right) X^{10} + 40\alpha X^9 + \left(-1728\alpha^2 + \frac{21}{4}\alpha\right) X^8 \\ & + \left(-576\alpha^2 + \frac{3}{8}\alpha\right) X^7 - 84\alpha^2 X^6 - 6\alpha^2 X^5 + \left(144\alpha^3 - \frac{3}{64}\alpha^2\right) X^4 \\ & + 40\alpha^3 X^3 + \frac{13}{4}\alpha^3 X^2 + \frac{1}{8}\alpha^3 X + \alpha^4 \Bigg)^3 \end{aligned}$$

and

$$\begin{aligned} q(\alpha, X) = & \left(X^6 - 12\alpha X^4 + \frac{1}{2}\alpha^2\right) \cdot \left(X^3 - 24\alpha X - 2\alpha\right)^4 \\ & \cdot \left(X^4 + \frac{1}{6}X^3 + \frac{1}{24}\alpha\right)^4. \end{aligned}$$

5.3.4. Verification. The degree-36 polynomial appearing in the following theorem as well as the corresponding degree-72 Belyi map are also listed in the ancillary file `psp62_deg36_data`.

THEOREM 5.5. *Let $f(\alpha, t, X) = p(\alpha, X) - tq(\alpha, X) \in \mathbb{Q}(\alpha, t)[X]$ where p and q are given as above. Then the (regular) Galois group of f over $\mathbb{Q}(\alpha, t)$ is isomorphic to $\mathrm{PSp}_6(2) \leq S_{36}$ and the branch cycle structure of f with respect to t is given by $(3^{12}, 1^{12}.2^{12}, 1^{12}.2^{12}, 1^6.2^1.4^7)$.*

PROOF. Using Magma the discriminant Δ of f turns out to be

$$\begin{aligned} \Delta = & 2^{732} \cdot 3^{168} \cdot \left(a - \frac{1}{512}\right)^{154} \cdot \alpha^{290} \cdot t^{24} \\ & \cdot \left(t^2 + \left(-2592\alpha - \frac{81}{16}\right) t + 1679616\alpha^2 - 6561\alpha + \frac{6561}{1024}\right)^{12}. \end{aligned}$$

With this formula we see that f has exactly four branch points with respect to t. Furthermore, the branch cycle structure of f can be derived by inspecting the inseparability behaviour of f evaluated at the places $t \mapsto 0$, $t \mapsto \infty$ and $t \mapsto r_i$ for $i = 1, 2$ where r_1 and r_2 denote the non-zero roots of $\Delta \in \mathbb{Q}(\alpha)[t]$.

Let $f_1, p_1, q_1 \in \mathbb{Q}(t)[X]$ denote the specializations of f, p, q at the place $\alpha \mapsto 1$, and $\bar{f}_1, \bar{p}_1, \bar{q}_1$ their images in $\mathbb{F}_{37}(t)[X]$ under the canonical projection. Since $\frac{1}{X-t} \cdot \bar{f}_1 \left(\frac{\bar{p}_1(t)}{\bar{q}_1(t)}, X \right) \in \mathbb{F}_{37}(t)[X]$ is irreducible, Corollary 4.2 implies that the Galois group of $\bar{f}_1$ over $\mathbb{F}_{37}(t)$ must be 2-transitive. Now, the classification of finite 2-transitive groups implies $\mathrm{Gal}(\bar{f}_1 \mid \mathbb{F}_{37}(t)) \in \{\mathrm{PSp}_6(2), A_{36}, S_{36}\}$.

Let $r(t, X) \in \mathbb{F}_{37}(t)[X]$ be the irreducible polynomial of degree 63 from the ancillary file `psp62_deg36_data`, then $r \left(\frac{\bar{p}_1(t)}{\bar{q}_1(t)}, X \right)$ becomes reducible over the field $\mathbb{F}_{37}(t)$. Therefore, Proposition 4.6 guarantees the existence of an index-d subgroup of $\mathrm{Gal}(\bar{f}_1 \mid \mathbb{F}_{37}(t))$ where $d \neq 1$ is a divisor of 63. Since both A_{36} and S_{36} do not contain such subgroups, we end up with $\mathrm{Gal}(\bar{f}_1 \mid \mathbb{F}_{37}(t)) = \mathrm{PSp}_6(2)$. Since the geometric monodromy group of $\bar{f}_1$ is a transitive normal subgroup of $\mathrm{PSp}_6(2)$, we get that the geometric monodromy group of $\bar{f}_1$ is also given by $\mathrm{PSp}_6(2)$. Now the arguments from Sections 4.3.1 and 4.3.2 imply that f has $\mathrm{PSp}_6(2)$ as its geometric monodromy group. Since $\mathrm{PSp}_6(2)$ is self-normalizing in S_{36}, it follows that the Galois extension defined by f is regular. □

The Magma calculations used in the proof can be found in the verification file `psp62_deg36_verify`. We used the same degree-63 permutation representation for $\mathrm{PSp}_6(2)$ as in the proof of Theorem 5.3.

Addendum: A complex approximation of a 5-point cover for $\mathbf{PSp_6(2)}$. The advantage of our approach compared to previous ones increases as the number of branch points grows. We give just one example of a complex approximation for a 5-point cover with Galois group $\mathrm{PSp}_6(2)$. Using the techniques of Chapter 3, one could again use this to obtain an equation for a family of covers. This time, we take a genus-0 tuple of type $(2^{10}.1^{16}, 2^{12}.1^{12}, 2^{12}.1^{12}, 2^{12}.1^{12}, 3^{12})$ in the 2-transitive degree-36 permutation action of $\mathrm{PSp}_6(2)$. Using Proposition 3.1, we turn this into a Belyi function of degree 108, with imprimitive Galois group contained in $\mathrm{PSp}_6(2) \wr C_3$, by composing with the rational function $x \mapsto x^3$, see Figures 7 and 8. The third root of this Belyi map then gives the desired 5-branch point $\mathrm{PSp}_6(2)$-cover. We have included it in the file `psp62_deg36_data`.

The monodromy of the computed complex cover can be checked numerically with the path lifting algorithm in [**33**, Section 11.1].

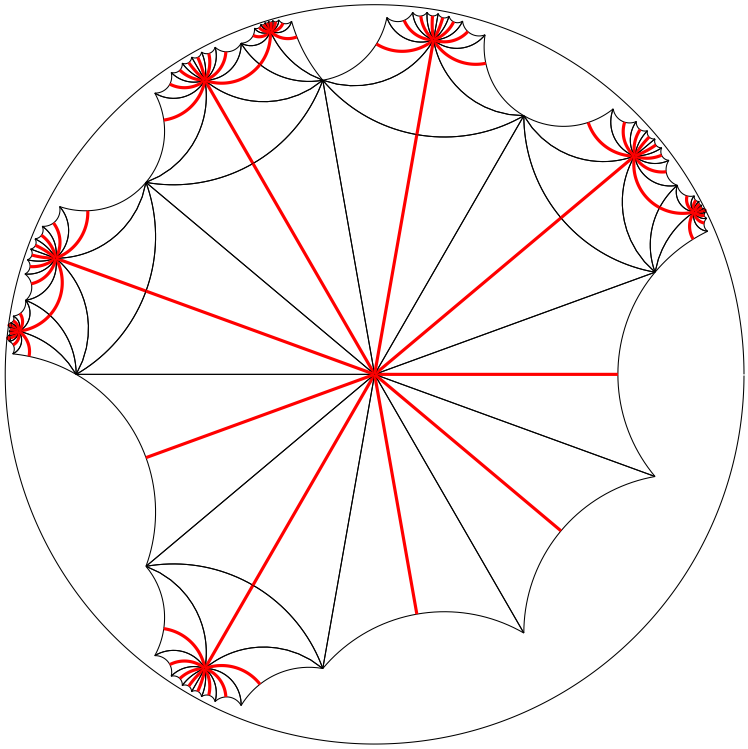


FIGURE 7. fundamental domain for $\mathrm{PSp}_6(2) \wr C_3$ of degree 108

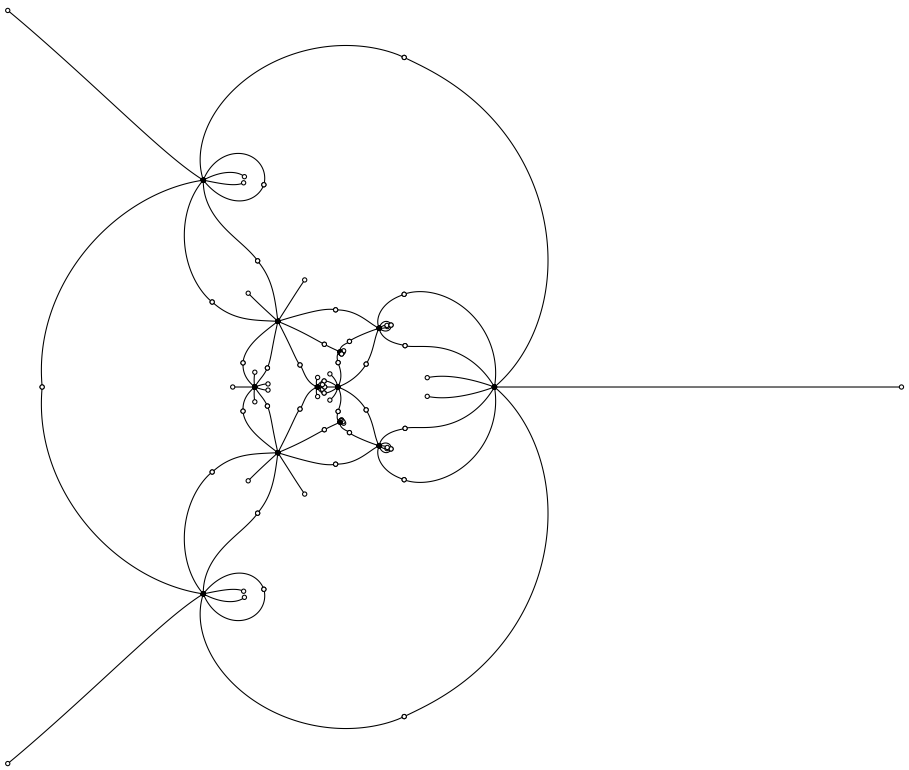


FIGURE 8. approximate dessin for $\mathrm{PSp}_6(2) \wr C_3$ of degree 108 in $\mathbb{P}^1$

CHAPTER 6

Families of polynomials with Galois groups $\mathrm{PSL}_4(3)$ and $\mathrm{PGL}_4(3)$ over $\mathbb{Q}(t)$

In this chapter we compute the first (to the best of our knowledge) polynomials with Galois groups $\mathrm{PSL}_4(3)$, $\mathrm{PGL}_4(3)$, $\mathrm{Aut}(\mathrm{PGL}_4(3))$ over $\mathbb{Q}(\alpha, t)$. Up to now these polynomials are not available to the public, neither on the arXiv nor in the literature.

6.1. Theoretical properties

Let G be the group $\mathrm{PSL}_4(3)$ in its natural 2-transitive action on the $\frac{3^4-1}{3-1} = 40$ points of the projective space $\mathrm{PG}(3,3)$. Furthermore, let C_1 be the unique conjugacy class of G of cycle structure $(3^{12}.1^4)$ and length 74880, C_2 be the unique class of cycle structure $(3^9.1^{13})$, C_3 the class of cycle structure $(2^{16}.1^8)$, and C_4 the unique class of fixed point free involutions. Then $C := (C_1, C_2, C_3, C_4)$ is a rational genus-0 class vector and it can be seen that for any $g \in C_2$ exactly one length-1-cycle of g is fixed under $N_{\mathrm{PSL}_4(3)}(\langle g \rangle)$; thus C satisfies an oddness condition as described in Remark 2.9.

Let $\mathcal{C}^{in}$ be the inner Hurwitz curve parameterizing all (regular) 4-point covers ramified over $0, \infty, 1, \lambda$ (for some $\lambda \neq 0, 1, \infty$) with group $\mathrm{PSL}_4(3)$ and branch cycle description as follows:

branch point	0	∞	1	λ
inertia class	C_1	C_2	C_3	C_4
cycle structures	$3^{12}.1^4$	$3^9.1^{13}$	$2^{16}.1^8$	2^{20}

Calculation with Magma yields that $|\mathrm{SNi}^{in}(C)| = 12$ and that the braid group acts transitively on $\mathrm{SNi}^{in}(C)$ with $(\tilde{\beta}_1, \tilde{\beta}_2, \tilde{\beta}_3)$ having branch cycle structure $(4^2.2^2, 3^4, 4^2.1^4)$. The Riemann–Hurwitz genus formula now implies that the absolutely irreducible curve $\mathcal{C}^{in}$ is of genus 0. However, the triple $(\tilde{\beta}_1, \tilde{\beta}_2, \tilde{\beta}_3)$ does not seem to satisfy an oddness condition, thus the rationality of $\mathcal{C}^{in}$ is unclear (without explicit computation).

In contrast to the monodromy groups appearing in the previous chapter, the group $\mathrm{PSL}_4(3)$ is not self-normalizing in S_{40} but has index 2 in its symmetric

normalizer $A := N_{S_{40}}(\mathrm{PSL}_4(3)) = \mathrm{PGL}_4(3)$. As a consequence, the 12 tuples in $\mathrm{SNi}^{in}(C)$ form 6 blocks, each block consisting of two tuples that are conjugate in $\mathrm{PGL}_4(3)$ but not in $\mathrm{PSL}_4(3)$. In particular, the degree-12 branch point reference map $\Psi : \mathcal{C}^{in} \to \mathbb{P}^1_\lambda$ factors through the *absolute Hurwitz curve* $\mathcal{C}^{ab}$ as follows:

$$\Psi : \mathcal{C}^{in} \xrightarrow{\Psi_2} \mathcal{C}^{ab} \xrightarrow{\Psi_6} \mathbb{P}^1_\lambda \tag{6.1}$$

The branch cycle description of the degree-6 map Ψ_6 is given by the action of $(\tilde{\beta}_1, \tilde{\beta}_2, \tilde{\beta}_3)$ on $\mathrm{SNi}^{ab}(C) := \mathrm{SNi}(C)/\mathrm{PGL}_4(3)$ having cycle structures $(4^1.2^1, 3^2, 2^2.1^2)$. In particular, as the latter satisfies an oddness condition, $\mathcal{C}^{ab}$ turns out to be a rational curve, i.e., $\mathcal{C}^{ab} = \mathbb{P}^1_\alpha$ for some parameter α.

While the inner Hurwitz curve $\mathcal{C}^{in}$ parameterizes *regular* G-extensions, the absolute Hurwitz curve $\mathcal{C}^{ab}$ can be interpreted as a parametrization of not-necessarily regular G-extensions. To be more explicit, there are polynomials $p, q \in \mathbb{Q}(\mathcal{C}^{ab})[X]$ such that $f(t, X) := p(X) - tq(X)$ has arithmetic monodromy group $\mathrm{PGL}_4(3)$ over $\mathbb{Q}(\mathcal{C}^{ab})(t)$ and geometric monodromy group $\mathrm{PSL}_4(3)$ (with the fixed field of $\mathrm{PSL}_4(3)$ being given by $\mathbb{Q}(\mathcal{C}^{in})(t)$). For more information about absolute Hurwitz spaces see **[26]**, **[52**, Chapter 10] or **[24]**.

Our goals in the next sections are as follows. First, we compute $p, q \in \mathbb{Q}(\alpha)[X]$ such that $p(X) - tq(X)$ has Galois group $\mathrm{PGL}_4(3)$. Next, we confirm through explicit computation that the genus-0 inner Hurwitz curve $\mathcal{C}^{in}$ is in fact a rational curve over $\mathbb{Q}$ which yields multi-parameter polynomials having $\mathrm{PSL}_4(3)$ as Galois group. At last, we also obtain degree-80 polynomials for the group $\mathrm{Aut}(\mathrm{PSL}_4(3))$.

6.2. A complex approximation of a single 4-point cover

Assume $f_0 \in \mathbb{C}(X)$ is ramified over $0, \infty, 1, -1$ with monodromy group $\mathrm{PSL}_4(3)$ and inertia classes C_1, C_2, C_3, C_4. Squaring f_0 yields a genus-0 Belyi map $g = f_0^2$ of degree 80 with monodromy group contained in the imprimitive wreath product $\mathrm{PSL}_4(3) \wr C_2$ and branch cycle structure $(6^{12}.2^4, 2^{36}.1^8, 6^9.2^{13})$. A Magma computation shows that $\mathrm{PSL}_4(3) \wr C_2$ contains 12 such triples $(\sigma_0, \sigma_1, \sigma_\infty)$,

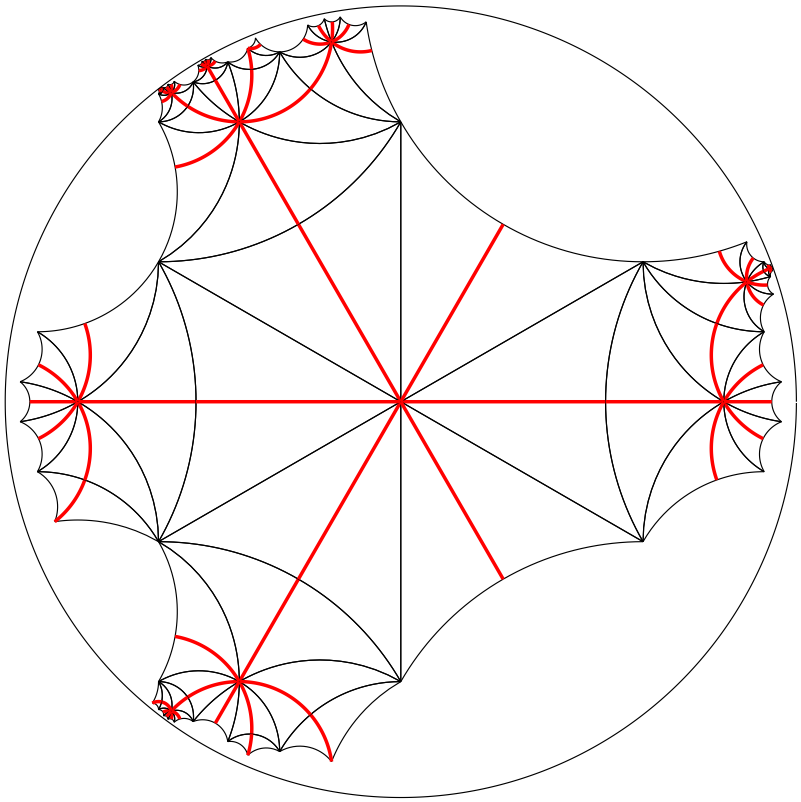


FIGURE 1. fundamental domain for $\mathrm{PSL}_4(3) \wr C_2 \leq S_{80}$

one of them given by

$$\begin{aligned}\sigma_0 := {} & (1,72,12,79,2,60)(3,66,11,44,6,71)(4,51,13,77,9,47)\\ & (5,58,7,49,8,56)(10,64)(14,57,39,52,28,80)(15,69,19,63,25,70)\\ & (16,48,23,59,31,46)(17,54,38,61,21,78)(18,45)\\ & (20,42,40,68,32,41)(22,75,24,50,35,62)(26,43,30,65,36,67)\\ & (27,76,37,53,33,74)(29,55)(34,73),\end{aligned}$$

$$\begin{aligned}\sigma_1 := {} & (1,32)(2,20)(3,26)(4,11)(5,18)(6,31)(7,9)(8,16)(10,24)(12,39)(13,37)\\ & (14,17)(15,29)(19,23)(21,38)(22,35)(25,30)(27,36)(28,40)(33,34)\\ & (41,60)(42,79)(43,71)(44,47)(45,58)(46,56)(48,64)(50,77)(52,66)\\ & (53,72)(54,80)(55,70)(57,78)(59,69)(65,75)(68,74)\end{aligned}$$

and $\sigma_\infty := (\sigma_0\sigma_1)^{-1}$.

Using the algorithm described in Section 3.3 we compute a complex approximation for the Belyi map g with branch cycle description $(\sigma_0, \sigma_1, \sigma_\infty)$. The fundamental domain used for the computation is shown in Figure 1 and the

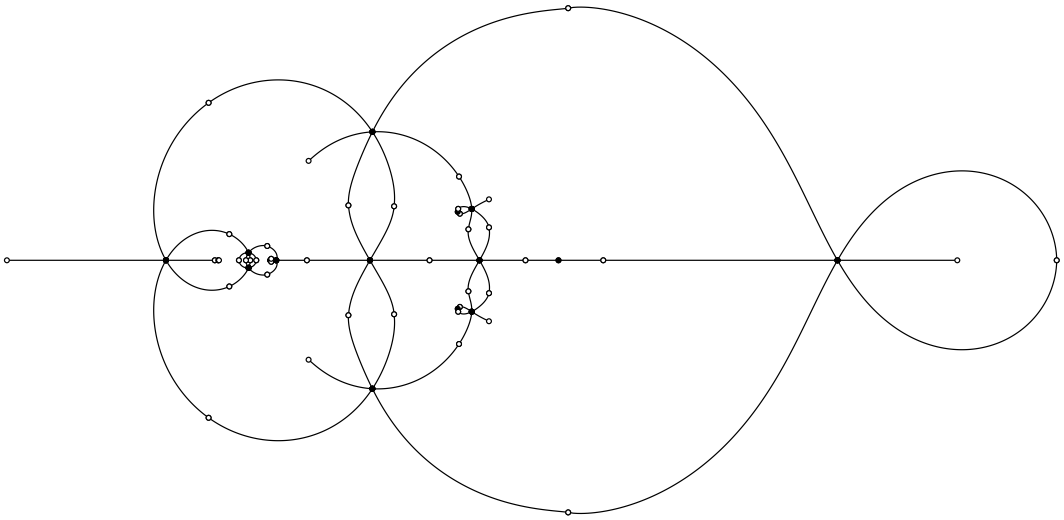


FIGURE 2. dessin for $\mathrm{PSL}_4(3) \wr C_2 \leq S_{80}$

resulting dessin d'enfant for the Belyi map g is presented in Figure 2. Taking the square root of g yields a complex approximation for f_0.

6.3. Turning a single cover into a family

Starting from f_0 we now compute polynomials $p, q \in \mathbb{Q}(\mathcal{C}^{ab})[X]$ such that $f(t, X) = p(X) - tq(X)$ possesses (arithmetic) Galois group $\mathrm{PGL}_4(3)$ and parametrizes $\mathrm{PSL}_4(3)$-covers ramified over $0, \infty, 1, \lambda$ with class vector C.

Since for any $g \in C_2$ there is exactly one length-1-cycle of g that is fixed under $N_{\mathrm{PGL}_4(3)}(\langle g \rangle)$, there is a rational place lying over $t \mapsto \infty$ (in a stem field of f) and, without loss of generality, we assume this place to lie at $X \mapsto \infty$. Combining the previous observation with the inseparability behaviour of p and q yields the following form for f:

$$f(t, X) = c \cdot p_{12}(X)^3 p_4(X) - t q_9(X)^3 q_{12}(X)$$

with $c \in \mathbb{Q}(\mathcal{C}^{ab})$ and monic polynomials $p_{12}, p_4, q_9, q_{12} \in \mathbb{Q}(\mathcal{C}^{ab})[X]$ of respective degree denoted in the index. Moreover, using affine-linear transformations we may assume the coefficient at X^{11} of q_{12} to be 0 and the coefficient at X^3 of p_4 to be equal to 1.

Now, starting from the 4-point cover f_0 computed in the previous section, we first apply the aforementioned normalization conditions, then we move the fourth branch point λ to several close rational values, and recognize the leading coefficient c in a degree-6 number field. Interpolation yields the following degree-6 dependency between λ and c (viewed as transcendentals):

$$\begin{aligned}0 =& 5283615080448c^6 + (660451885056\lambda - 880602513408)c^5\\ &+ (-137594142720\lambda^2 - 125936861184\lambda + 36691771392)c^4\\ &+ (-13377208320\lambda^3 - 44348276736\lambda^2 + 27011432448\lambda)c^3\\ &+ (1433272320\lambda^4 - 3879705600\lambda^3 - 1062519552\lambda^2 - 293530176\lambda)c^2\\ &+ (71663616\lambda^5 + 192201984\lambda^4 - 181185120\lambda^3 - 228698352\lambda^2 - 30013344\lambda)c\\ &- 5971968\lambda^6 + 11741868\lambda^5 - 138024\lambda^4 - 8703009\lambda^3 - 5404396\lambda^2 - 1119364\lambda.\end{aligned}$$

The function field $\mathbb{Q}(c,\lambda)$ is of genus 0. After finding a $\mathbb{Q}$-rational place a Riemann–Roch space computation as described in [**33**, Lemma 3.16] yields an explicit parameter α with $\mathbb{Q}(\alpha) = \mathbb{Q}(c,\lambda)$. We expect all coefficients of p and q to lie in the function field $\mathbb{Q}(\lambda, c) = \mathbb{Q}(\alpha)$. Thus, letting α converge to several rational values allows the interpolation of all coefficients as rational functions in α.

This way we obtain explicit polynomials $p, q \in \mathbb{Q}(\alpha)[X]$ such that $f(t,X) = p(X) - tq(X)$ has Galois group $\mathrm{PGL}_4(3)$ over $\mathbb{Q}(\alpha,t)$. It is ramified over $0, \infty, 1, \lambda$ where the variable branch point λ turns out (after interpolation) to be

$$\lambda = \Psi_6(\alpha) = \frac{p_6(\alpha)}{q_6(\alpha)} = \frac{243(\alpha - 410/5727510537)^2(\alpha + 2460/1909170179)^4}{2048(\alpha - 205/272738597)^3(\alpha + 1025/3818340358)^3}. \quad (6.2)$$

6.4. Verification

THEOREM 6.1. *The polynomial $f(t,X) := p(X) - tq(X)$ (with $p, q \in \mathbb{Q}(\alpha)[X]$ given in the file `psl43_data`) has Galois group $\mathrm{PGL}_4(3)$ over $\mathbb{Q}(\alpha,t)$ and is ramified over $0, \infty, 1, \Psi_6(\alpha)$ with class vector C. The geometric monodromy group is $\mathrm{PSL}_4(3)$.*

PROOF. A simple Magma computation confirms that f is ramified over $0, \infty, 1, \Psi_6(\alpha)$ with branch cycle structure $(3^{12}.1^4,\ 3^9.1^{13},\ 2^{16}.1^8,\ 2^{20})$. The Riemann–Hurwitz formula allows no other ramification points.

We choose $\alpha_1 = -1640/13364191253$ and $\alpha_2 = 656/1909170179$ with the property $\Psi_6(\alpha_1) = \Psi_6(\alpha_2) = -4$. Let $f_1 = p_1 - tq_1 \in \mathbb{Q}(t)[X]$ be the specialization of $f = p - tq \in \mathbb{Q}(\alpha,t)[X]$ at the place $\alpha \mapsto \alpha_1$ and $f_2 = p_2 - tq_2 \in \mathbb{Q}(t)[X]$ be the specialization of f at $\alpha \mapsto \alpha_2$. Then $p_1(X)q_1(t) - p_1(t)q_1(X)$ factors into irreducible polynomials of degrees 1 and 39, while $p_1(X)q_2(t) - p_2(t)q_1(X)$ factors into irreducible polynomials of degrees 13 and 27.

Thus, by Proposition 4.4 the group $A_1 := \mathrm{Gal}(f_1 \mid \mathbb{Q}(t))$ is 2-transitive having a subgroup of index dividing 40 with orbit lengths 13 and 27. Now the design-theoretic Corollary 4.12 yields that $A_1 = \mathrm{PSL}_4(3)$ or $A_1 = \mathrm{PGL}_4(3)$.

As the geometric monodromy group G_1 of f_1 is normal in the arithmetic monodromy group A_1, we conclude $G_1 = \mathrm{PSL}_4(3)$ or $G_1 = \mathrm{PGL}_4(3)$. Due to the topological interpretation of geometric monodromy groups we know that G_1 is generated by elements having cycle structures $(3^{12}.1^4,\ 3^9.1^{13},\ 2^{16}.1^8,\ 2^{20})$. The fact that these are only even permutations rules out the odd permutation group $\mathrm{PGL}_4(3)$ as a possibility for G_1, thus $G_1 = \mathrm{PSL}_4(3)$.

As specialization at the point α_1 preserves geometric monodromy groups (see Section 4.3.1), we have $G = G_1 = \mathrm{PSL}_4(3)$ for the geometric monodromy group G of f. Since G is normal in the arithmetic monodromy group $A := \mathrm{Gal}(f \mid \mathbb{Q}(\alpha, t)) \leq S_{40}$, we conclude $A = \mathrm{PSL}_4(3)$ or $A = \mathrm{PGL}_4(3)$. The discriminant of f is not a square (which can be easily checked modulo a prime or after specializations in α and t) ruling out the even group $\mathrm{PSL}_4(3)$. Thus $A = \mathrm{PGL}_4(3)$.

A Magma computation shows that among all class vectors of $\mathrm{PSL}_4(3)$ having cycle structures $(3^{12}.1^4,\ 3^9.1^{13},\ 2^{16}.1^8,\ 2^{20})$ the vector $C = (C_1, C_2, C_3, C_4)$ is the only class vector with non-empty Nielsen class. This implies that f actually has class vector C and not some other class vector with the same cycle structures. □

The Magma computations appearing in the above proof are contained in the file `psl43_verify`. The proof makes use of the fact that $\mathrm{PGL}_4(3)$ has two permutation actions having the same permutation character, compare the strategy outlined in Section 4.2.1.

As the whole family of 4-point covers is too large to present it here, we give only one explicit cover of the whole family. Namely, specializing $\alpha \mapsto 656/1909170179$ with $\Psi_6(\alpha) = -4$ (as in the previous proof) and performing some inner Möbius transformations yields the following 4-point cover.

COROLLARY 6.2. *Let*

$$\begin{aligned} p := & -5/48 \cdot (X - 1/5)\, X^3 \left(X^2 + 2/5X - 1/5\right)^3 \left(X^3 - 39/10X^2 + 6/5X - 1/10\right) \\ & \left(X^9 + 9/2X^8 + 27/2X^7 - 309/10X^6 - 9/2X^5 + 153/10X^4\right. \\ & \left. -363/50X^3 + 81/50X^2 - 9/50X + 1/125\right)^3 \end{aligned}$$

and

$$\begin{aligned} q := &\left(X^9 - 339/80X^8 - 3/10X^7 + 51/20X^6 - 21/10X^5\right.\\ &+273/200X^4 - 27/50X^3 + 57/500X^2 - 3/250X + 1/2000\left.\right)^3\\ &\left(X^{12} + 63/5X^{11} + 2771/60X^{10} + 1237/30X^9 - 207/20X^8 - 16X^7 + 211/50X^6\right.\\ &+207/125X^5 - 263/250X^4 + 33/125X^3 - 99/2500X^2 + 13/3750X - 1/7500\left.\right). \end{aligned}$$

Then $p(X) - tq(X)$ *has Galois group* $\mathrm{PGL}_4(3)$ *over* $\mathbb{Q}(t)$ *and the geometric monodromy group is* $\mathrm{PSL}_4(3)$.

6.5. From $\mathrm{PGL}_4(3)$ to the index-2 subgroup $\mathrm{PSL}_4(3)$

As established before, the polynomial $f = p - tq$ with p and q from file `psl43_data` has Galois group $\mathrm{PGL}_4(3)$ over $\mathbb{Q}(\mathcal{C}^{ab})(t) = \mathbb{Q}(\alpha, t)$. This section's goal is to descend to the index-2 subgroup $\mathrm{PSL}_4(3)$.

As the fixed field of $\mathrm{PSL}_4(3)$ in the splitting field of f is given by $\mathbb{Q}(\mathcal{C}^{in})(t)$, descending to $\mathrm{PSL}_4(3)$ boils down to compute the inner Hurwitz curve $\mathcal{C}^{in}$. Fortunately, $\mathcal{C}^{in}$ will turn out to be rational yielding multi-parameter polynomials with (regular) Galois group $\mathrm{PSL}_4(3)$.

Recall from equation (6.1) that the branch point reference map Ψ splits through $\mathcal{C}^{ab} = \mathbb{P}^1_\alpha$ as follows

$$\Psi : \mathcal{C}^{in} \xrightarrow{\Psi_2} \mathbb{P}^1_\alpha \xrightarrow{\Psi_6} \mathbb{P}^1_\lambda$$

with ramification structures $(4^2.2^2, 3^4, 4^2.1^4)$ and $(4^1.2^1, 3^2, 2^2.1^2)$ of the covers $\Psi = \Psi_6 \circ \Psi_2$ and $\Psi_6 = p_6/q_6$, respectively. Comparing these cycle structures implies that Ψ_2 is ramified exactly over the degree-2 place

$$\alpha^2 + 336200/3644930772382892041$$

of $\mathbb{Q}(\alpha)$ lying over $\lambda \mapsto 1$, i.e., the polynomial of multiplicity 2 in the factorization of $p_6(\alpha) - q_6(\alpha)$ with p_6, q_6 given in (6.2). Translation to function fields[1] implies $\mathbb{Q}(\mathcal{C}^{in}) = \mathbb{Q}(\alpha)(y)$ with

$$y^2 = c \cdot (\alpha^2 + 336200/3644930772382892041)$$

and some square-free integer c, yet to be computed.

Since $\mathrm{PSL}_4(3) = \mathrm{PGL}_4(3) \cap A_{40}$, the fixed field $\mathbb{Q}(\mathcal{C}^{in})(t)$ of $\mathrm{PSL}_4(3)$ may also be obtained by adjoining the square root of the discriminant of $p(X) - tq(X)$ to the base field $\mathbb{Q}(\alpha)(t)$. Thus, y^2 is up to squares equal to the discriminant of $p(X) - tq(X)$.

[1]Note that all varieties are defined over $\mathbb{Q}$.

We now specialize $\alpha \mapsto \alpha_0 := 656/1909170179$ (with $\Psi_6(\alpha_0) = -4$) and $t \mapsto t_0 := 2$ to obtain $f_0 = p_0 - t_0 q_0 \in \mathbb{Q}[X]$. After this double specialization Magma is able to quickly compute the discriminant of f_0, which turns out to have a square-free part equal to 6. Knowing that

$$c \cdot (\alpha_0^2 + 336200/3644930772382892041)$$

must have the same square-free part, we conclude $c = 19$. Therefore, a model for $\mathcal{C}^{in}$ is given by the conic

$$\mathcal{C}^{in} : y^2 = 19(\alpha^2 + 336200/3644930772382892041) \tag{6.3}$$

and we are finally able to answer the question whether $\mathcal{C}^{in}$ is rational over $\mathbb{Q}$: A Magma computation yields that the conic (6.3) possesses $\mathbb{Q}$-rational points. Consequently, the function field $\mathbb{Q}(\mathcal{C}^{in}) = \mathbb{Q}(\alpha, y)$ is a rational function field and another Magma computation yields $\mathbb{Q}(\alpha, y) = \mathbb{Q}(\gamma)$ with

$$\alpha = \Psi_2(\gamma) := \frac{410\gamma^2 + 5740\gamma + 4510}{-5727510537\gamma^2 - 7636680716\gamma + 9545850895}. \tag{6.4}$$

Combining the above observations yields an explicit multi-parameter polynomial having Galois group $\mathrm{PSL}_4(3)$.

Corollary 6.3. *The polynomial $p(\Psi_2(\gamma), X) - tq(\Psi_2(\gamma), X)$ with p, q from file `psl43_data` and Ψ_2 from equation (6.4) has regular Galois group $\mathrm{PSL}_4(3)$ over the rational function field $\mathbb{Q}(\gamma, t)$.*

6.6. Polynomials with Galois group $\mathrm{Aut}(\mathrm{PGL}_4(3))$

In the previous sections we obtained polynomials for the groups $G = \mathrm{PSL}_4(3)$ and $A = N_{S_{40}}(\mathrm{PSL}_4(3)) = \mathrm{PGL}_4(3)$ as Galois groups over the fields $\mathbb{Q}(\mathcal{C}^{in})(t)$ and $\mathbb{Q}(\mathcal{C}^{ab})(t)$, respectively. These extensions were parameterized by the inner Hurwitz curve $\mathcal{C}^{in}$ and the absolute[2] Hurwitz curve $\mathcal{C}^{ab}$, respectively.

Additionally, it is also possible to obtain polynomials with Galois group $\mathrm{Aut}(\mathrm{PGL}_4(3)) = \mathrm{Aut}(\mathrm{PSL}_4(3))$. In fact, after denoting the splitting field of $p(X) - tq(X)$ over $\mathbb{Q}(\alpha, t)$ by $\mathbb{Q}(\mathcal{T}_\mathcal{C})$ (as in Chapter 2), the theory of absolute Hurwitz spaces implies that $\mathrm{Aut}(\mathrm{PGL}_4(3))$ is the Galois group of the extension $\mathbb{Q}(\mathcal{T}_\mathcal{C}) \mid \mathbb{Q}(\mathcal{C}^{out})(t)$ where the curve $\mathcal{C}^{out}$ is the intermediate curve in the sequence

$$\Psi : \mathcal{C}^{in} \xrightarrow{2} \mathcal{C}^{ab} \xrightarrow{2} \mathcal{C}^{out} \xrightarrow{3} \mathbb{P}^1_\lambda$$

where the degree-12 mapping Ψ is the branch point reference map $\Psi : \mathcal{C}^{in} \to \mathbb{P}^1_\lambda$.

[2]Here, the notion of *absolute* was taken with respect to the action of degree 40.

We already know that $\mathcal{C}^{ab} = \mathbb{P}^1_\alpha$ is rational and the relation $\lambda = \Psi_6(\alpha)$ between α and λ is given explicitly in equation (6.2). In particular, the curve $\mathcal{C}^{out}$ is also rational and a parameter β with $\mathcal{C}^{out} = \mathbb{P}^1_\beta$ can be easily computed (as a degree-2 rational function in α) by applying the Magma command `Decomposition` to the degree-6 rational function Ψ_6. The result is $\mathbb{Q}(\mathcal{C}^{out}) = \mathbb{Q}(\beta)$ with

$$\beta = \frac{\alpha^2 - 4920/32455893043\alpha}{\alpha + 3485/5727510537}.$$

Thus $\mathbb{Q}(\mathcal{T}_C) \mid \mathbb{Q}(\beta)(t)$ is a Galois extension with Galois group Aut(PGL$_4$(3)). If desired, one can compute explicit Aut(PGL$_4$(3))-polynomials as follows: The conjugate to α with respect to the field extension $\mathbb{Q}(\alpha) \mid \mathbb{Q}(\beta)$ is given by

$$\alpha' := -\alpha + \beta + 4920/32455893043$$

and, therefore, we obtain the following result.

COROLLARY 6.4. *Let β and α' be as above. Then, the degree-80 polynomial*

$$f(\alpha, t, X) \cdot f(\alpha', t, X) \in \mathbb{Q}(\beta, t)[X]$$

with f as given in file `psl43_data` has Galois group Aut(PGL$_4$(3)) *over* $\mathbb{Q}(\beta, t)$.

CHAPTER 7

A family of 4-point covers with monodromy group $\mathrm{PSL}_6(2)$

In this chapter we compute a family of 4-branch-point rational functions of degree 63 with monodromy group $\mathrm{PSL}_6(2)$. This, in particular, negatively answers a question by Joachim König [**33**, p. 109] whether there exists such a function with rational coefficients. The computed family also gives rise to the first degree-126 realizations of $\mathrm{Aut}(\mathrm{PSL}_6(2))$ over $\mathbb{Q}$. This chapter's main results are also available in the preprint article [**10**] joint with Andreas Wenz.

REMARK. The groups $\mathrm{PSL}_6(2)$ and $\mathrm{PSp}_6(2)$ of degree 63 are expected to be the largest (with respect to the permutation degree) almost simple primitive groups having a generating genus-0 tuple of length at least 4 with the socle being a simple group of Lie type. While multi-parameter families of polynomials with Galois group $\mathrm{PSp}_6(2)$ of degree 28 and 36 were calculated in Chapter 5, this chapter deals with the remaining case $\mathrm{PSL}_6(2)$.

7.1. Computation

Let $C := (C_1, C_2, C_3, C_3)$ be the genus-0 class vector of $\mathrm{PSL}_6(2)$ in its natural 2-transitive action on the 63 non-zero elements of $\mathbb{F}_2^6$, where C_1, C_2 and C_3 are the unique conjugacy classes of cycle structure $(2^{28}.1^7)$, $(2^{16}.1^{31})$ and $(3^{20}.1^3)$, respectively. Furthermore, let $\mathcal{F}$ be the family of all $\mathrm{PSL}_6(2)$-covers $f : \mathbb{P}^1 \to \mathbb{P}^1$ of degree 63 such that:

(i) f is ramified over $0, \infty, 1 \pm \sqrt{\lambda}$ for some $\lambda \in \mathbb{P}^1 \setminus \{0, 1, \infty\}$ with ramification structure:

branch point	0	∞	$1+\sqrt{\lambda}$	$1-\sqrt{\lambda}$
inertia class	C_1	C_2	C_3	C_3
cycle structure	$2^{28}.1^7$	$2^{16}.1^{31}$	$3^{20}.1^3$	$3^{20}.1^3$

(ii) f is normalized in the following sense: The sum of all simple roots of f is 0 and the sum of all double poles is 1. Furthermore, ∞ is the unique simple pole of f fixed under the action of the normalizer of the inertia group at ∞. Note that for any $g \in C_2$ exactly one length-1-cycle of g is fixed under $N_{\mathrm{PSL}_6(2)}(\langle g \rangle)$.

Denote by $\mathcal{C}$ the inner Hurwitz curve parameterizing the family $\mathcal{F}$ of covers. The normalization conditions (with respect to inner Möbius transformations) stated in (ii) guarantee that each point on $\mathcal{C}$ corresponds to exactly one cover in $\mathcal{F}$.

In order to decide whether $\mathrm{PSL}_6(2)$ occurs regularly as a Galois group over $\mathbb{Q}$ with ramification structure C, one has to check the existence of $\mathbb{Q}$-rational points on the inner Hurwitz curve $\mathcal{C}$ that lead to Galois group preserving specializations, cf. Theorem 2.12. Joachim König [**33**, p. 109] mentions that without explicit computation of $\mathcal{C}$ there seems to be no way of finding an answer to this question.

7.1.1. Properties of $\mathcal{C}$. A computer computation with Magma yields that the straight inner Nielsen class $\mathrm{SNi}^{in}(C)$ is of size 48. Consequently, the branch point reference map

$$\Psi : \begin{cases} \mathcal{C} \to \mathbb{P}^1_\lambda \\ \text{cover with ramification locus } \left\{0, \infty, 1 \pm \sqrt{\lambda}\right\} \mapsto \lambda \end{cases} \tag{7.1}$$

turns out to be a Belyi map of degree 48 with ramification locus $(0, 1, \infty)$. The branch cycle description of Ψ, denoted by $(\sigma_0, \sigma_1, \sigma_\infty) \in \mathrm{Sym}(\mathrm{SNi}^{in}(C))^3$, can be calculated explicitly using the formula (2.4) which arises from the action of the braid group on $\mathrm{SNi}^{in}(C)$. This triple generates a transitive group and consists of cycle structures $(6^5.4^4.2^1, 7^4.4^3.3^2.2^1, 2^{24})$. From this we can deduce that $\mathcal{C}$ is connected of genus 3 (by the Riemann–Hurwitz formula). Furthermore, the curve $\mathcal{C}$ can be defined over $\mathbb{Q}$ since all classes of C are rational.

In the following the function field of $\mathcal{C}$ will be denoted by $\mathbb{Q}(\mathcal{C})$. The family $\mathcal{F}$ can be parameterized by a rational function

$$F = \frac{p}{q} \in \mathbb{Q}(\mathcal{C})(X) \tag{7.2}$$

with $p, q \in \mathbb{Q}(\mathcal{C})[X]$ such that any element of $\mathcal{F}$ is obtained via specializing F at some point in $\mathcal{C}$.

In the remaining chapter we will occasionally identify the curve $\mathcal{C}$ with the family $\mathcal{F}$ and thus consider, for example, the branch point reference Ψ to be defined on both $\mathcal{C}$ and $\mathcal{F}$.

7.1.2. Defining equations for elements in $\mathcal{F}$. Fix $f_{\lambda_0} \in \mathcal{F}$ with $\Psi(f_{\lambda_0}) = \lambda_0$ for some $\lambda_0 \in \mathbb{P}^1 \setminus \{0, 1, \infty\}$. According to (i) and (ii) there exist a scalar c_0 and separable, monic and mutually coprime polynomials

$p_7, p_{28}, q_{16}, q_{30}, r_3, r_{20}, s_3, s_{20}$ of respective degree denoted in the index such that

$$f_{\lambda_0} = \frac{c_0 \cdot p_7 \cdot p_{28}^2}{q_{30} \cdot q_{16}^2} = 1 + \sqrt{\lambda_0} + \frac{c_0 \cdot r_3 \cdot r_{20}^3}{q_{30} \cdot q_{16}^2} = 1 - \sqrt{\lambda_0} + \frac{c_0 \cdot s_3 \cdot s_{20}^3}{q_{30} \cdot q_{16}^2} \tag{7.3}$$

where the traces of p_7 and q_{16} are 0 and 1, respectively.

By comparing coefficients, (7.3) can be considered as a system of polynomial equations where c_0 and the coefficients of $p_7, p_{28}, \ldots, s_{20}$ are considered to be the unknowns. This system consists of 126 unknowns and 126 equations, hence it is expected to have at most finitely many solutions with f_{λ_0} being one of them.

7.1.3. Walking on $\mathcal{F}$. Assume we are given an explicit approximate equation for f_{λ_0}, then we are able to compute another approximate equation of a cover $f_{\lambda_0+\delta} \in \mathcal{F}$ with $\Psi(f_{\lambda_0+\delta}) = \lambda_0 + \delta$ for some sufficiently small $\delta \in \mathbb{C}$. This can be achieved via Newton iteration by assembling the corresponding polynomial equations similar to (7.3) and using f_{λ_0} as the initial value.

Starting from an approximate equation of a cover $f_{\text{start}} \in \mathcal{F}$ we can find an approximate equation for another cover $f_{\text{end}} \in \mathcal{F}$ with prescribed $\lambda_{\text{end}} := \Psi(f_{\text{end}}) \in \mathbb{P}^1 \setminus \{0, 1, \infty\}$ and prescribed ramification $\sigma_{\text{end}} \in \text{SNi}^{in}(C)$:

Let $\lambda_{\text{start}} := \Psi(f_{\text{start}})$ and γ_1 be a path in $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ connecting λ_{start} to λ_{end}. Lift γ_1 via Ψ to $\mathcal{F}$ from a path starting in f_{start} and ending in some element denoted by $f^*_{\text{end}} \in \mathcal{F}$, then $\Psi(f^*_{\text{end}}) = \lambda_{\text{end}}$. The ramification of f^*_{end} will be denoted by σ^*_{end}. According to the ramification of Ψ we can give a closed path γ_2 in $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ starting in λ_{end} with the property: The lifted path of γ_2 in $\mathcal{F}$ via Ψ connects f^*_{end} to another element f_{end} with $\Psi(f_{\text{end}}) = \lambda_{\text{end}}$ and ramification σ_{end}. Using Newton iteration as explained before we can slightly deform f_{start} at its ramification locus along $\gamma_2 \circ \gamma_1$ to obtain an approximate equation for f_{end} having the prescribed ramification data.

7.1.4. Splitting behaviour of Ψ. The monodromy group of Ψ, generated by $\sigma_0, \sigma_1, \sigma_\infty$, turns out to be imprimitive acting on 24 blocks, each of size 2, caused by the automorphism group $\text{Aut}(\text{PSL}_6(2))$. The induced action of $(\sigma_0, \sigma_1, \sigma_\infty)$ on the set $\mathcal{B}$ of these blocks, denoted by $(\sigma'_0, \sigma'_1, \sigma'_\infty) \in \text{Sym}(\mathcal{B})^3$, consists of cycle structures $(4^2.3^5.1^1,\ 7^2.4^1.3^1.2^1.1^1,\ 2^{12})$. Since $(\sigma'_0, \sigma'_1, \sigma'_\infty)$ describes a genus-0 triple, the cover Ψ splits as follows:

$$\Psi : \mathcal{C} \xrightarrow{\Psi_2} \mathbb{P}^1_\mu \xrightarrow{\Psi_{24}} \mathbb{P}^1_\lambda \tag{7.4}$$

with a degree-2 subcover Ψ_2 and a degree-24 subcover Ψ_{24} with branch cycle description $(\sigma'_0, \sigma'_1, \sigma'_\infty)$ over $(0, 1, \infty)$. The latter cover can be computed

explicitly (using for example the method explained in Section 3.3):

$$\lambda = \Psi_{24}(\mu) = \frac{p_{24}}{q_{24}} = 1 - \frac{r_{24}}{q_{24}} \tag{7.5}$$

where

$$p_{24} := \left(\mu - \frac{1}{4}\right)\left(\mu^2 - \frac{11}{16}\mu + \frac{1}{8}\right)^4 \left(\mu^5 - \frac{137}{4}\mu^4 + \frac{178}{3}\mu^3 - 34\mu^2 + 8\mu - \frac{2}{3}\right)^3,$$

$$r_{24} := 243\left(\mu - \frac{1}{2}\right)^3 \left(\mu - \frac{1}{3}\right)^4 \left(\mu - \frac{5}{16}\right)^2 \left(\mu^2 + \frac{1}{3}\mu - \frac{1}{6}\right)^7,$$

$$q_{24} := p_{24} + r_{24}.$$

Recall that the cycle structures of $(\sigma_0, \sigma_1, \sigma_\infty)$ and $(\sigma_0', \sigma_1', \sigma_\infty')$ are given by

$$(6^5.4^4.2^1, 7^4.4^3.3^2.2^1, 2^{24}) \qquad \text{and} \qquad (4^2.3^5.1^1, 7^2.4^1.3^1.2^1.1^1, 2^{12}).$$

It is now easy to see that these cycle structures in combination with p_{24}, q_{24} and r_{24} uniquely determine the ramification locus $\mathcal{R}_{\Psi_2} \subseteq \mathbb{P}^1_\mu$ of the degree-2 subcover Ψ_2. We find $\mathcal{R}_{\Psi_2} = R_0 \cup R_1 \cup R_\infty$ with

$$\begin{aligned} R_0 &:= \Psi_{24}^{-1}(0) \cap \mathcal{R}_{\Psi_2} \\ &= \left\{\frac{1}{4}\right\} \cup \left\{\text{roots of } \mu^5 - \frac{137}{4}\mu^4 + \frac{178}{3}\mu^3 - 34\mu^2 + 8\mu - \frac{2}{3}\right\}, \\ R_1 &:= \Psi_{24}^{-1}(1) \cap \mathcal{R}_{\Psi_2} = \left\{\frac{5}{16}, \infty\right\}, \\ R_\infty &:= \Psi_{24}^{-1}(\infty) \cap \mathcal{R}_{\Psi_2} = \emptyset. \end{aligned}$$

7.1.5. A model for $\mathcal{C}$. Since σ_0' has a unique fixed point and $\mathcal{C}$ is defined over $\mathbb{Q}$, the function field analogue of (7.4) can be stated as

$$\mathbb{Q}(\mathcal{C}) \overset{2}{\geq} \mathbb{Q}(\mu) \overset{24}{\geq} \mathbb{Q}(\lambda) \tag{7.6}$$

where μ is a root of $p_{24} - \lambda q_{24} \in \mathbb{Q}(\lambda)[X]$ and $\mathbb{Q}(\mathcal{C})$ being the degree-2 extension of $\mathbb{Q}(\mu)$ corresponding to Ψ_2. The computation of $\mathcal{R}_{\Psi_2}$ guarantees the existence of a primitive element $y \in \mathbb{Q}(\mathcal{C})$, i.e., $\mathbb{Q}(\mathcal{C}) = \mathbb{Q}(\mu, y)$, with defining equation

$$y^2 = cP(\mu) := c\left(\mu^5 - \frac{137}{4}\mu^4 + \frac{178}{3}\mu^3 - 34\mu^2 + 8\mu - \frac{2}{3}\right)\left(\mu - \frac{1}{4}\right)\left(\mu - \frac{5}{16}\right)$$

for some square-free $c \in \mathbb{Q}$ which will be determined in 7.1.7. For this reason a hyperelliptic $\mathbb{Q}$-model for $\mathcal{C}$ can be chosen to be

$$\left\{(\mu, y) : y^2 = cP(\mu)\right\}. \tag{7.7}$$

Using this particular model Ψ_2 is then given by $\Psi_2(\mu, y) = \mu$ for all $(\mu, y) \in \mathcal{C}$.

7.1.6. Field of definition for elements in $\mathcal{F}$. Recall that elements of $\mathcal{F}$ are obtained via specializing F at points in $\mathcal{C}$. Using the explicit hyperelliptic model (7.7) for $\mathcal{C}$, the coefficients of a cover $f_0 \in \mathcal{F}$ are then contained in

$$\mathbb{Q}\left(\mu_0, \sqrt{cP(\mu_0)}\right) \qquad \text{where} \qquad \mu_0 := \Psi_2(f_0). \tag{7.8}$$

The explicit computation of $\Psi_2(f_0)$ can be done in the following way: Write $\lambda_0 := \Psi(f_0)$. Then the fundamental group $\pi_1(\mathbb{P}^1 \setminus \{0, 1, \infty\}, \lambda_0)$ acts on $\mathcal{B}$ and on $\Psi_{24}^{-1}(\lambda_0)$ in equivalent ways, yielding an explicitly computable bijection $\chi : \mathcal{B} \to \Psi_{24}^{-1}(\lambda_0)$ respecting these equivalent actions. We obtain

$$\Psi_2(f_0) = \chi(B) \tag{7.9}$$

whenever the branch cycle description of f_0 is contained in a block $B \in \mathcal{B}$.

In particular, if an explicit cover contained in $\mathcal{F}$ is already known with algebraic numbers as coefficients, it is possible to determine the unknown rational scalar c.

7.1.7. Obtaining elements in $\mathcal{F}$. By Riemann's existence theorem there exists a $\mathrm{PSL}_6(2)$-cover $h : \mathbb{P}^1 \to \mathbb{P}^1$ ramified over $(0, \infty, -1, 1)$ with ramification structure (C_3, C_3, C_1, C_2). Then h^2 turns out to be a Belyi map with ramification locus $(0, \infty, 1)$ and monodromy group contained in $\mathrm{PSL}_6(2) \wr C_2 \leq S_{126}$. Its ramification consists of cycle structures $(6^{20}.2^3,\ 6^{20}.2^3,\ 2^{44}.1^{38})$. Using Magma one sees that there are 24 such triples (up to simultaneous conjugation), all generating the full wreath product $\mathrm{PSL}_6(2) \wr C_2$. We pick one of these triples and compute the corresponding Belyi map h^2 of degree 126 explicitly using the method described in Section 3.3. The fundamental domain used for the computation is shown in Figure 1 and the resulting (approximate) dessin d'enfant is presented in Figure 2. Taking the square root yields a defining (approximate) equation for h.

After applying suitable Möbius transformations and slightly moving the ramification points of h using Newton iteration we obtain a complex approximation of a cover $f_{\text{start}} \in \mathcal{F}$ with $\Psi(f_{\text{start}}) = \lambda_0 := \Psi_{24}(\frac{1}{6})$. The approach described in 7.1.3 allows the computation of a complex approximation of a cover $f_{\text{end}} \in \mathcal{F}$ with $\Psi(f_{\text{end}}) = \lambda_0$ and branch cycle description contained in $B \in \mathcal{B}$ such that $\chi(B) = \frac{1}{6}$. In combination with (7.9) this implies $\Psi_2(f_{\text{end}}) = \frac{1}{6} \in \mathbb{Q}$. Due to (7.8) the coefficients of f_{end} can be recognized in the quadratic number field $\mathbb{Q}\left(\frac{1}{6}, \sqrt{cP(\frac{1}{6})}\right) = \mathbb{Q}\left(\sqrt{-c \cdot 3 \cdot 7 \cdot 457}\right)$. With the help of Magma we find $c = 3$. Note that $\mathcal{C}$ from (7.7) is finally computed.

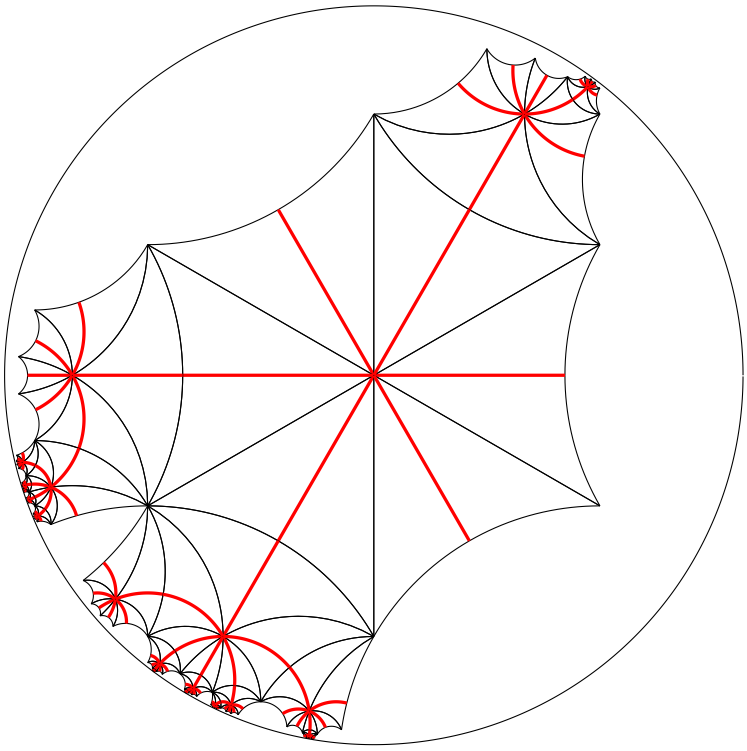


FIGURE 1. fundamental domain for $\mathrm{PSL}_6(2) \wr C_2 \leq S_{126}$

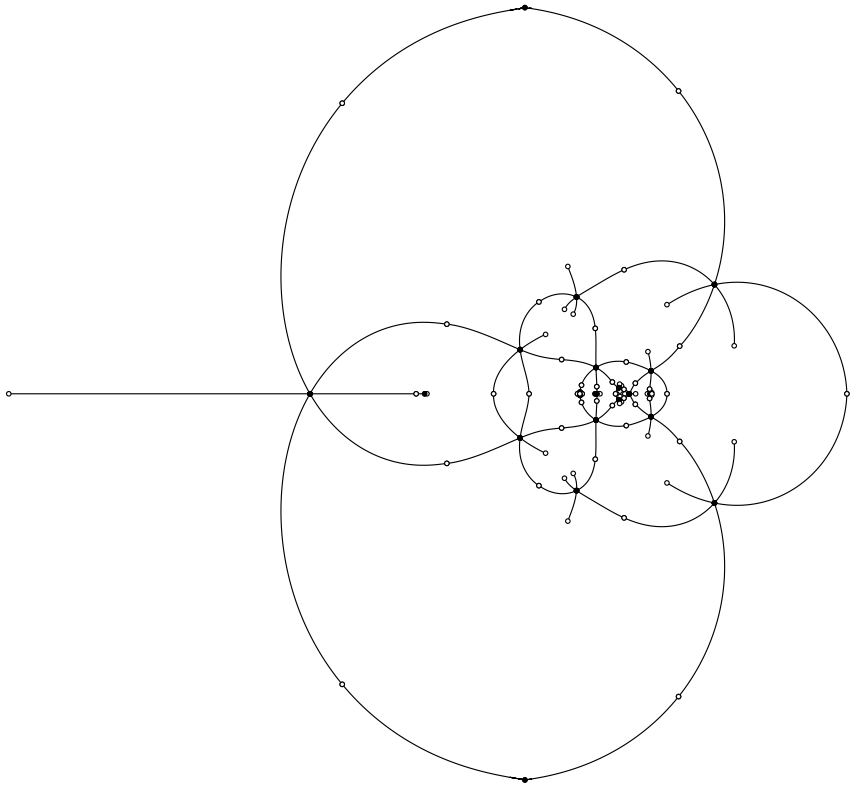


FIGURE 2. dessin for $\mathrm{PSL}_6(2) \wr C_2 \leq S_{126}$

7.1.8. Computing the universal cover F. Any coefficient of $F \in \mathbb{Q}(\mathcal{C})(X) = \mathbb{Q}(\mu, y)(X)$ from (7.2) can be expressed as

$$H_1(\mu) + yH_2(\mu)$$

where $H_1, H_2 \in \mathbb{Q}(\mu)$. By slightly moving the ramification points of f_{end} via Newton iteration as described in 7.1.3 we obtain many defining equations of covers $f \in \mathcal{F}$ such that $\Psi_2(f)$ is a rational number close to $\Psi_2(f_{\text{end}}) = \frac{1}{6}$. Considering (7.8) the coefficients of f are then contained in $\mathbb{Q}(\sqrt{3P(\Psi_2(f))})$, allowing us to read off $H_1(\Psi_2(f))$ and $H_2(\Psi_2(f))$. Therefore, both H_1 and H_2 can be computed by interpolation. The resulting universal cover $F = \frac{p}{q}$ is presented in file `psl62_family`.

REMARK. The standard approach of computing a hyperelliptic model for $\mathcal{C}$ consists of finding a polynomial relation between λ and a fixed coefficient of F which are usually expected to generate the entire function field $\mathbb{Q}(\mathcal{C})$ with $[\mathbb{Q}(\mathcal{C}) : \mathbb{Q}(\lambda)] = 48$. This is achieved by interpolation via computing several elements $f \in \mathcal{F}$ such that $\Psi(f) \in \mathbb{Q}$ and recognizing the previously fixed coefficient as algebraic degree-48 numbers. A Riemann–Roch space computation then leads to the hyperelliptic model for $\mathcal{C}$.

Our approach takes advantage that the branch point reference map Ψ is decomposable with an explicitly computable genus-0 subcover Ψ_{24}. As explained in 7.1.5 and 7.1.7 this yields a defining equation for $\mathcal{C}$ after recognizing only a degree-2 number.

7.2. Verification and Consequences

THEOREM 7.1. *Let $\mathcal{C}$ be the curve computed in 7.1.5 and 7.1.7 with defining equation*

$$y^2 = 3\left(\mu^5 - \frac{137}{4}\mu^4 + \frac{178}{3}\mu^3 - 34\mu^2 + 8\mu - \frac{2}{3}\right)\left(\mu - \frac{1}{4}\right)\left(\mu - \frac{5}{16}\right).$$

Furthermore, let

$$F := \frac{p}{q} \in \mathbb{Q}(\mathcal{C})(X) = \mathbb{Q}(\mu, y)(X)$$

be the rational function computed in 7.1.8*, see ancillary file* `psl62_family`*, and $\Psi_{24} = p_{24}/q_{24}$ the map from* (7.5)*. Then the following holds:*

(a) The polynomial $p(X) - tq(X)$ defines a regular $\mathrm{PSL}_6(2)$*-extension of $\mathbb{Q}(\mu, y)(t)$. The ramification locus with respect to t is given by $\mathcal{R} := (0, \infty, 1 + \sqrt{\Psi_{24}(\mu)}, 1 - \sqrt{\Psi_{24}(\mu)})$ with ramification structure $(2^{28}.1^7, 2^{16}.1^{31}, 3^{20}.1^3, 3^{20}.1^3)$.*

(b) Every cover in $\mathcal{F}$ is obtained in a unique way via specialization of F at some point in $\mathcal{C}$.

PROOF. (a) We firstly verify that $f := p - tq$ is ramified over $\mathcal{R}$ with ramification structure $(2^{28}.1^7, 2^{16}.1^{31}, 3^{20}.1^3, 3^{20}.1^3)$. This can be done by studying the inseparability behaviour of f at the places $t \mapsto t_0$ for $t_0 \in \mathcal{R}$. The corresponding factorizations are given in the file `psl62_family`. In particular, the behaviour above $1 \pm \sqrt{\Psi_{24}(\mu)}$ was obtained by interpolating the factorizations of several specialized polynomials. The ramification locus of f cannot be larger than $\mathcal{R}$, otherwise it would contradict the Riemann–Hurwitz formula.

Let Ω be the splitting field of $p - tq$ over $\mathbb{Q}(\mu, y, t)$. Then, the geometric monodromy group $G := \mathrm{Gal}(\Omega \mid (\Omega \cap \overline{\mathbb{Q}(\mu, y)})(t))$ is normal in the arithmetic monodromy group $A := \mathrm{Gal}(\Omega \mid \mathbb{Q}(\mu, y, t))$. We now consider the specialization of $f = p - tq$ at the point $(\mu_0, y_0) := (0, \frac{1}{8}\sqrt{-10}) \in \mathcal{C}$, denoted by

$$f_0 = p_0 - tq_0 \in \mathbb{Q}(\sqrt{-10}, t)[X]. \tag{7.10}$$

Note that f_0 is still ramified over 4 points. Write Ω_0 for the splitting field of f_0 over $\mathbb{Q}(\sqrt{-10}, t)$. Then, by the arguments in Section 4.3.1, we find $G \cong G_0 := \mathrm{Gal}(\Omega_0 \mid (\Omega_0 \cap \overline{\mathbb{Q}})(t))$. A Magma computation (see file `psl62_verify1`) shows that $f_0(\frac{p_0(t)}{q_0(t)}, X)$ and $f_0(\frac{\overline{p_0}(t)}{\overline{q_0}(t)}, X)$ split over $\mathbb{Q}(\sqrt{-10}, t)$ into irreducible factors of degree $1, 62$ and $31, 32$, respectively. Hence, Proposition 4.4 implies that $A_0 := \mathrm{Gal}(\Omega_0 \mid \mathbb{Q}(\sqrt{-10}, t))$ must be a 2-transitive group that contains a subgroup of index dividing 63 with orbit lengths 31 and 32. According to Corollary 4.12 the group A_0 turns out to be $\mathrm{PSL}_6(2)$. Since A_0 is simple and G_0 is normal in A_0, we find $G \cong G_0 \cong \mathrm{PSL}_6(2)$. As $\mathrm{PSL}_6(2)$ is also self-normalizing in S_{63}, we end up with $A \cong \mathrm{PSL}_6(2)$.

(b) We will use the following notation: For a rational function P over a field of characteristic 0 we denote by $\mathbb{Q}_P$ the field extension of $\mathbb{Q}$ generated by the coefficients of P.

The normalized discriminant Δ of $f(t, X) = p(X) - tq(X)$ with respect to X is a polynomial in $\mathbb{Q}_F[t]$. Since the roots of Δ are given by the ramification locus of f its factorization in $\mathbb{Q}_F[t]$ is either of the form

$$\Delta = t^k \left(t - (1 + \sqrt{\lambda})\right)^\ell \left(t - (1 - \sqrt{\lambda})\right)^h \quad \text{or} \quad \Delta = t^k \left(t^2 - 2t + 1 - \lambda\right)^\ell$$

for some $k, \ell, h \in \mathbb{N}$ where $\lambda := \Psi_{24}(\mu)$. Both cases yield $\lambda \in \mathbb{Q}_F$, therefore $\mathbb{Q}(\lambda) \subseteq \mathbb{Q}_F \subseteq \mathbb{Q}(\mu, y)$ with $[\mathbb{Q}(\mu, y) : \mathbb{Q}(\lambda)] = 48$. Fix $(\mu_0, y_0) \in \mathcal{C}$ such that $\Psi_{24}(\mu_0) = \frac{1}{2}$. Then, for the specialization of F at (μ_0, y_0), denoted by $F_{(\mu_0, y_0)}$, we compute $[\mathbb{Q}_{F_{(\mu_0, y_0)}} : \mathbb{Q}] = 48$ using Magma. We end

up with $\mathbb{Q}_F = \mathbb{Q}(\mu, y)$. From the latter we see that μ and y are rational functions in the coefficients of F. Recall that for any $\lambda_0 \in \mathbb{P}^1 \setminus \{0, 1, \infty\}$ we find distinct points $(\mu_1, y_1), \ldots, (\mu_{48}, y_{48}) \in \mathcal{C}$ such that $\Psi_{24}(\mu_k) = \lambda_0$ for $k = 1, \ldots, 48$. If we specialize F at these points we obtain 48 distinct $\mathrm{PSL}_6(2)$-covers $F_{(\mu_1,y_1)}, \ldots, F_{(\mu_{48},y_{48})}$ with ramification locus $(0, \infty, 1 \pm \sqrt{\lambda_0})$ and ramification structure C, which are all normalized with respect to inner Möbius transformations (in the sense of (ii)). Therefore, all covers $F_{(\mu_1,y_1)}, \ldots, F_{(\mu_{48},y_{48})}$ lie in $\mathcal{F}$ and correspond to all 48 quadruples in $\mathrm{SNi}^{in}(C)$. As a consequence, each element in $\mathcal{F}$ can be obtained uniquely via specialization. □

Remark. By looking at Theorem 7.1(b) and its proof we do not get any information about the specialization behaviour of F at a point $(\mu_0, y_0) \in \mathcal{C}$ with $\Psi_{24}(\mu_0) \in \{0, 1, \infty\}$. Assume, the specialization of F at (μ_0, y_0), denoted by $F_{(\mu_0,y_0)}$, is a degree-63 cover, then one of the following cases occurs:

$\Psi_{24}(\mu_0)$	ramification locus of $F_{(\mu_0,y_0)}$	ramification structure of $F_{(\mu_0,y_0)}$
0	$\{0, 1, \infty\}$	contains C_1, C_2
1	$\{0, 2, \infty\}$	contains C_2, C_3
∞	$\{0, \infty\}$	only contains C_1

In none of these cases $\mathrm{PSL}_6(2)$ is the monodromy group of $F_{(\mu_0,y_0)}$: Using Magma we see that $\mathrm{PSL}_6(2)$ does not contain genus-0 tuples of length at most 3 that correspond to the respective conjugacy classes.

With a little more effort we can deduce from Theorem 7.1 that $\mathrm{PSL}_6(2)$ does not occur as the monodromy group of a rational function in $\mathbb{Q}(X)$ ramified over at least 4 points.

In order to achieve this result, we still have to study $\mathrm{PSL}_6(2)$-covers with ramification structure C and ramification locus of type $(0, \infty, \pm\sqrt{c})$. These covers can be calculated explicitly by deforming the ramification locus of covers contained in $\mathcal{F}$ via Newton iteration by assembling the defining equations explained in 7.1.2.

Theorem 7.2. *Let K be the degree-24 number field, $c \in K$ the non-square and $p, q \in K[X]$ the monic polynomials given in the ancillary file* `psl62_data2`. *Then the Galois group* $\mathrm{Gal}(p - tq \mid K(t))$ *is isomorphic to* $\mathrm{PSL}_6(2)$ *in its natural 2-transitive action on 63 elements. The ramification structure is given by* $(2^{28}.1^7, 2^{16}.1^{31}, 3^{20}.1^3, 3^{20}.1^3)$ *and the ramification locus with respect to t is given by* $(0, \infty, \sqrt{c}, -\sqrt{c})$.

PROOF. In the same fashion as in the proof of Theorem 7.1(a) it can be calculated easily that the ramification locus of $p - tq$ is indeed given by $(0, \infty, \sqrt{c}, -\sqrt{c})$ with ramification structure $(2^{28}.1^7, 2^{16}.1^{31}, 3^{20}.1^3, 3^{20}.1^3)$.

Let Ω be the splitting field of $p - tq$ over $K(t)$. Recall that the geometric monodromy group $G := \mathrm{Gal}(\Omega \mid (\Omega \cap \overline{K})(t))$ is normal in $A := \mathrm{Gal}(\Omega \mid K(t))$. Let $\mathfrak{p} = (67, a + 7)$ and $\mathfrak{q} = (67, a + 42)$ be the unique prime ideals of norm 67 in the ring of integers $\mathcal{O}_K$ of K where a denotes the primitive element of K used in file `psl62_data2`. Write $p_\mathfrak{p}$ and $q_\mathfrak{p}$ for the reduction of p and q modulo $\mathfrak{p}$. Accordingly, we define $A_\mathfrak{p} := \mathrm{Gal}(\Omega_\mathfrak{p} \mid (\mathcal{O}_K/\mathfrak{p})(t))$ and $G_\mathfrak{p} := \mathrm{Gal}(\Omega_\mathfrak{p} \mid (\Omega_\mathfrak{p} \cap \overline{\mathcal{O}_K/\mathfrak{p}})(t))$ with $\Omega_\mathfrak{p}$ being the splitting field of $p_\mathfrak{p} - tq_\mathfrak{p}$ over $(\mathcal{O}_K/\mathfrak{p})(t)$. Again, $G_\mathfrak{p}$ is normal in $A_\mathfrak{p}$. Of course, we will use the same notation for the reduction modulo $\mathfrak{q}$.

Note that $p_\mathfrak{p} - \frac{p_\mathfrak{p}(t)}{q_\mathfrak{p}(t)} q_\mathfrak{p}$ and $p_\mathfrak{p} - 16 \cdot \frac{p_\mathfrak{q}(t)}{q_\mathfrak{q}(t)} q_\mathfrak{p}$ split into irreducible factors of $1, 62$ and $31, 32$ over $(\mathcal{O}_K/\mathfrak{p})(t) \cong \mathbb{F}_{67}(t)$. Therefore, by Proposition 4.4 and Corollary 4.12, the group $A_\mathfrak{p}$ must be isomorphic to $\mathrm{PSL}_6(2)$. As $A_\mathfrak{p}$ is simple, we see that $A_\mathfrak{p}$ and $G_\mathfrak{p}$ coincide. Since $\mathfrak{p}$ is a prime of good reduction for $p - tq$, we have $G_\mathfrak{p} \cong G$ by the results in Section 4.3.2. Due to the fact that $\mathrm{PSL}_6(2)$ is self-normalizing in S_{63} we end up with $A = \mathrm{PSL}_6(2)$. □

All computational steps occurring in the previous proof are reproduced in the Magma file `psl62_verify2`.

COROLLARY 7.3. *The group* $\mathrm{PSL}_6(2)$ *does not occur as the monodromy group (neither arithmetic nor geometric) of a rational function in* $\mathbb{Q}(X)$ *ramified over at least 4 points.*

PROOF. If f has the simple group $\mathrm{PSL}_6(2)$ as arithmetic monodromy group, then the geometric monodromy group is $\mathrm{PSL}_6(2)$ anyway. Consequently, it suffices to assume that there exists a rational function $f \in \mathbb{Q}(X)$ ramified over at least 4 points having $\mathrm{PSL}_6(2)$ as its geometric monodromy group. A Magma computation shows that C is the only genus-0 class vector of length at least 4 containing generating tuples for $\mathrm{PSL}_6(2)$; thus, f has degree 63 with ramification structure $C = (C_1, C_2, C_3, C_3)$. As $\mathrm{PSL}_6(2)$ of degree 63 is self-normalizing in S_{63}, we get that arithmetic and geometric monodromy group of f are both equal to $\mathrm{PSL}_6(2)$. The branch cycle lemma, see Corollary 2.11, asserts that the ramification locus of f is of the form (a_1, a_2, a_3, a_4) where $a_1, a_2 \in \mathbb{P}^1(\mathbb{Q})$ and a_3, a_4 fulfil a degree-2 relation over $\mathbb{Q}$. Hence, after applying a suitable outer Möbius transformation we may assume — without altering

the field of definition — that f either has ramification locus $(0, \infty, 1 \pm \sqrt{\lambda_0})$ or $(0, \infty, \pm\sqrt{\lambda_0})$ for some $\lambda_0 \in \mathbb{P}^1(\mathbb{Q}) \setminus \{0, 1, \infty\}$. We will now study both cases:

(1) case $(0, \infty, 1 \pm \sqrt{\lambda_0})$:

Using the notation and result from Theorem 7.1(b) there exist 48 specialized covers $F_{(\mu_1,y_1)}, \dots, F_{(\mu_{48},y_{48})} \in \mathcal{F}$ with $\Psi(F_{(\mu_k,y_k)}) = \lambda_0$ for $k \in \{1, \dots, 48\}$. Since $|\operatorname{SNi}^{in}(C)| = 48$, the cover f has to coincide with some $F_{(\mu_k,y_k)}$ up to inner Möbius transformations. Because the normalization conditions (ii) can be achieved without enlarging the field of definition, it follows that $F_{(\mu_k,y_k)}$ is also defined over $\mathbb{Q}$. In particular, (μ_k, y_k) must be a $\mathbb{Q}$-rational point on $\mathcal{C}$ with $\lambda_0 = \Psi_{24}(\mu_k) \notin \{0, 1, \infty\}$.

Since $\mathcal{C}$ is given by a hyperelliptic genus-3 model and its Jacobian is of Mordell–Weil rank 1, Chabauty's algorithm (with the implementation in Sage **[50]** presented in **[2]**) gives us the complete list of $\mathbb{Q}$-rational points of $\mathcal{C}$. We find $\mu_k \in \{\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{5}{16}, \infty\}$ and for all these values we see $\Psi_{24}(\mu_k) \in \{0, 1\}$, a contradiction.

(2) case $(0, \infty, \pm\sqrt{\lambda_0})$:

After a suitable scaling process Theorem 7.2 gives us 48 different PSL$_6$(2)-covers $f_1, \dots, f_{48}$ that satisfy condition (ii) with ramification locus $(0, \infty, \pm 1)$. Each cover is defined over a degree-48 number field.

Since $\frac{f}{\sqrt{\lambda_0}}$ has ramification locus $(0, \infty, \pm 1)$, the cover $\frac{f}{\sqrt{\lambda_0}}$ defined over a quadratic number field has to coincide with f_k for some $k \in \{1, \dots, 48\}$ up to inner Möbius transformations, a contradiction.

This shows that PSL$_6$(2) cannot be the monodromy group of f. □

7.3. Extensions with Galois group Aut(PSL$_6$(2))

Although our approach does not yield PSL$_6$(2)-polynomials over $\mathbb{Q}$ we at least get an explicit realization of Aut(PSL$_6$(2)) over $\mathbb{Q}(\mu, t)$.

Denoting the splitting field of $f(\mu, y, t, X)$ over $\mathbb{Q}(\mu, y, t)$ by $\mathbb{Q}(\mathcal{T}_\mathcal{C})$, the theory of (absolute) Hurwitz spaces implies that $\mathbb{Q}(\mathcal{T}_\mathcal{C}) \mid \mathbb{Q}(\mu, t)$ is a Galois extension with group Aut(PSL$_6$(2)). In particular, the degree-126 polynomial

$$f(\mu, y, t, X) \cdot f(\mu, -y, t, X) \in \mathbb{Q}(\mu, t)[X] \tag{7.11}$$

possesses the imprimitive Galois group Aut(PSL$_6$(2)) over the two-variable rational function field $\mathbb{Q}(\mu, t)$.

This polynomial's splitting field $\mathbb{Q}(\mathcal{T}_\mathcal{C})$ is $\mathbb{Q}$-regular but not $\mathbb{Q}(\mu)$-regular as it contains the quadratic extension $\mathbb{Q}(\mu, y)$ of $\mathbb{Q}(\mu)$. In particular, it is

impossible to obtain $\mathbb{Q}$-regular $\mathrm{Aut}(\mathrm{PSL}_6(2))$-extensions of $\mathbb{Q}(t)$ by specializing the parameter μ to rational values (as done in the proof of Theorem 7.1).

However, as suggested to us by Joachim König specializing μ to suitable polynomials in t, one may obtain (infinitely many) $\mathbb{Q}$-regular extensions over $\mathbb{Q}(t)$ with Galois group $\mathrm{Aut}(\mathrm{PSL}_6(2))$. In the following we present one particular example.

COROLLARY 7.4. *Let*

$$H := f(t, y, t, X) \cdot f(t, -y, t, X) \in \mathbb{Q}(t)[X].^1$$

Then the splitting field of the degree-126 polynomial H over $\mathbb{Q}(t)$ is regular and has Galois group $\mathrm{Aut}(\mathrm{PSL}_6(2))$.

PROOF. We know that the polynomial $f(\mu, y, t, X) \cdot f(\mu, -y, t, X)$ from (7.11) has $\mathrm{Aut}(\mathrm{PSL}_6(2))$ as Galois group over $\mathbb{Q}(\mu, t)$ with fixed field of $\mathrm{PSL}_6(2)$ given by $\mathbb{Q}(\mathcal{C})(t) = \mathbb{Q}(\mu, \sqrt{3P(\mu)}, t)$. Thus, Dedekind's theorem implies that $A := \mathrm{Gal}(H \mid \mathbb{Q}(t))$ is a subgroup of $\mathrm{Aut}(\mathrm{PSL}_6(2))$ and it is easy to see that in fact equality holds.[2]

Denote by Ω the splitting field of H over $\mathbb{Q}(t)$. Since the geometric monodromy group $G := \mathrm{Gal}(\Omega \mid (\Omega \cap \overline{\mathbb{Q}})(t))$ of H is normal in A, we conclude $G = \mathrm{Aut}(\mathrm{PSL}_6(2))$ or $G = \mathrm{PSL}_6(2)$. Assume $G = \mathrm{PSL}_6(2)$. Then the field of constants of Ω would be of the form $K(t)$ where K is some quadratic number field. On the other hand, we already know that the fixed field of $\mathrm{PSL}_6(2)$ in Ω is equal to $\mathbb{Q}(t, \sqrt{3P(t)})$, which can be easily seen not to be of the desired form $K(t)$ with a quadratic number field K. □

REMARK. Analogously, one may derive regular extensions with Galois group $\mathrm{PGL}_4(3)$ in Section 6.4.

7.4. Addendum: A Belyi map with monodromy group $\mathrm{PSL}_6(2)$

Coincidentally, $\mathrm{PSL}_6(2)$ also happens to contain a rigid, $\mathbb{Q}(\sqrt{-7})$-rational genus-0 generating triple leading to another $\mathrm{Aut}(\mathrm{PSL}_6(2))$-extension of $\mathbb{Q}(t)$. For the explicit realization we again apply the method explained in Section 3.3.

THEOREM 7.5. *Let $p, q \in \mathbb{Q}(\sqrt{-7})[X]$ be the polynomials of degree 63 from the ancillary file* `psl62_data3`.

[1] In comparison to equation (7.11) we have specialized $\mu \mapsto t$.

[2] E.g., specializing $t \mapsto 1$ and reducing modulo 13 yields an element of cycle structure $30^2.15^4.2^2.1^2$ but no proper transitive subgroup of $\mathrm{Aut}(\mathrm{PSL}_6(2))$ contains such an element.

(a) The polynomial $p-tq$ possesses the 2-transitive Galois group $\mathrm{PSL}_6(2) \leq S_{63}$ over $\mathbb{Q}(\sqrt{-7})(t)$ with ramification locus $(0,1,\infty)$ and branch cycle structure $(21^3, 4^8.2^{12}.1^7, 2^{28}.1^7)$.

(b) The degree-126 product $(p-tq)(\overline{p}-t\overline{q})$ has non-regular Galois group $\mathrm{Aut}(\mathrm{PSL}_6(2))$ over $\mathbb{Q}(t)$.

SKETCH OF PROOF. A computation with Magma, see file `psl62_verify3`, yields that $p(X) - \frac{p(t)}{q(t)}q(X)$ and $p(X) - \frac{\overline{p}(t)}{\overline{q}(t)}q(X)$ split in $\mathbb{Q}(\sqrt{-7},t)[X]$ into irreducible factors of degree 1, 62 and 31, 32, respectively. Analogously to the proof of Theorem 7.1 this implies that $p(X) - tq(X)$ and $\overline{p}(X) - t\overline{q}(X)$ both have the same splitting field Ω over $\mathbb{Q}(\sqrt{-7})(t)$ with $\mathrm{Gal}(\Omega \mid \mathbb{Q}(\sqrt{-7})(t)) = \mathrm{PSL}_6(2)$. It is now easy to see that $\Omega \mid \mathbb{Q}(t)$ is a Galois extension with group $\mathrm{Aut}(\mathrm{PSL}_6(2))$. □

However, in contrast to Corollary 7.4, due to the lack of an additional parameter, it is not possible to obtain *regular* $\mathrm{Aut}(\mathrm{PSL}_6(2))$-extensions from Theorem 7.5.

CHAPTER 8

On Elkies' method to bound the transitivity degree of Galois groups

In the previous chapters the most difficult part in the verification process was to exclude the highly transitive groups A_n or S_n. In this self-contained chapter we present a technique by Elkies [**25**] for bounding the transitivity degree of Galois groups of function field extensions, thus complementing the techniques described in Chapter 4. It works by collecting the factorization patterns of many specialized polynomials and comparing them to an effective version of Chebotarev's density theorem which arises from the Hasse–Weil bound.

We use Elkies' method to give alternative proofs for the correctness for the 2-transitive Galois groups $\mathrm{PSp}_6(2)$, $\mathrm{PSL}_4(3)$, $\mathrm{PSL}_6(2)$ appearing in the previous Chapters 5, 6 and 7. Additionally, we rigorously verify that the monodromy group of the degree-276 cover defined over a degree-12 number field computed by Monien [**44**] is isomorphic to the sporadic 2-transitive Conway group Co_3. The verification process for the Conway group is particularly difficult since it does not seem to be feasible with the techniques presented in Chapter 4.

Remark. The chapter is mainly identical to the journal article [**12**] by Andreas Wenz and the author. In comparison to the journal version an additional example, namely the group $\mathrm{PSL}_4(3)$, was added.

8.1. Preliminaries

For a fixed number field K let p and q be coprime polynomials in $K[X]$. Recall that the arithmetic monodromy group of the degree-n cover p/q is defined as

$$A := \mathrm{Gal}(N \mid K(t))$$

where N denotes the splitting field of $p(X) - tq(X)$ over $K(t)$. Furthermore, the geometric monodromy group of p/q is defined as

$$G := \mathrm{Gal}(N \mid (\overline{K} \cap N)(t)).$$

Since $p(X) - tq(X)$ is absolutely irreducible, the natural (faithful) action of both G and A on the n roots of $p(X) - tq(X)$ in N is transitive. Furthermore, it is well known that G is normal in A.

In order to study A and G, we will reduce the above polynomials modulo a suitable prime: The ring of integers of K will be denoted by $\mathcal{O}_K$. For a fixed prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ we write $p_\mathfrak{p}$ and $q_\mathfrak{p}$ for the reduction of p and q modulo $\mathfrak{p}$. In the same fashion as before we define

$$A_\mathfrak{p} := \mathrm{Gal}(N_\mathfrak{p} \mid (\mathcal{O}_K/\mathfrak{p})(t)) \quad \text{and} \quad G_\mathfrak{p} := \mathrm{Gal}(N_\mathfrak{p} \mid (\overline{\mathcal{O}_K/\mathfrak{p}} \cap N_\mathfrak{p})(t))$$

where $N_\mathfrak{p}$ denotes the splitting field of $p_\mathfrak{p}(X) - tq_\mathfrak{p}(X)$ over $(\mathcal{O}_K/\mathfrak{p})(t)$. Again, $G_\mathfrak{p}$ is a normal subgroup of $A_\mathfrak{p}$.

Thanks to a theorem of Beckmann (see Section 4.3.2), among other considerations, if $\mathfrak{p}$ is chosen to be lying over a sufficiently large rational prime we may assume the following:

(i) The ramification locus of $p(X) - tq(X)$ with respect to t is $\mathfrak{p}$-stable.
(ii) The inseparability behaviour of both $p(X) - tq(X) \in K(t)[X]$ and $p_\mathfrak{p}(X) - tq_\mathfrak{p}(X) \in (\mathcal{O}_K/\mathfrak{p})(t)[X]$ specialized at ramified places with respect to t coincides.
(iii) $G \cong G_\mathfrak{p}$.

8.2. A method by Elkies

The following technique described by Elkies (see [**25**]) bounds the transitivity degree of G:

Assume, G and therefore $G_\mathfrak{p}$ is k-transitive and $A_\mathfrak{p} = G_\mathfrak{p}$. Let C_0 and C_1 be the projective t- and x-lines over the finite field $\mathbb{F}_\lambda \cong \mathcal{O}_K/\mathfrak{p}$. By introducing the relation $p_\mathfrak{p}(x) - tq_\mathfrak{p}(x) = 0$ we obtain a cover C_1/C_0 ramified over exactly m points with ramification structure $(s_1, \ldots, s_m) \in (S_n)^m$. Its Galois closure will be denoted by $\tilde{C}$.

Let $(G_\mathfrak{p})_k$ be the stabilizer of a k-element set in $G_\mathfrak{p}$ and $C_k := \tilde{C}/(G_\mathfrak{p})_k$. The corresponding cover C_k/C_0 is of degree $\binom{n}{k}$ with ramification structure $(\sigma_1, \ldots, \sigma_m)$ induced by the natural action of $(s_1, \ldots, s_m)$ on k-element subsets. As $G_\mathfrak{p}$ acts faithfully on n elements, it can be shown easily that the action on k-element subsets is also faithful if $k \notin \{0, n\}$. In particular, $\mathrm{ord}(\sigma_i) = \mathrm{ord}(s_i)$ for $i = 1, \ldots, m$. Additionally note that C_k is an irreducible curve with full constant field $\mathbb{F}_\lambda$ due to $A_\mathfrak{p} = G_\mathfrak{p}$.

The number of $\mathbb{F}_\lambda$-rational points on C_k, denoted by $\#C_k(\mathbb{F}_\lambda)$, has to obey the Hasse–Weil bound $|\#C_k(\mathbb{F}_\lambda) - (\lambda+1)| \leq 2g(C_k)\sqrt{\lambda}$, in particular

$$\#C_k(\mathbb{F}_\lambda) \leq \lambda + 1 + 2g(C_k)\sqrt{\lambda}. \tag{8.1}$$

Here, $g(C_k)$ denotes the genus of C_k. In order to check if C_k is indeed compatible with the above bound, we need to determine $\#C_k(\mathbb{F}_\lambda)$ and $g(C_k)$.

We will use the following notation: For a permutation $s \in S_n$ let $\pi_k(s)$ be the number of invariant k-element subsets of s.

8.2.1. Counting $\mathbb{F}_\lambda$-rational points on C_k. Fix $t_0 \in \mathbb{P}^1(\mathbb{F}_\lambda)$ not contained in the ramification locus S of $p_\mathfrak{p}(X) - tq_\mathfrak{p}(X)$. Note that $\mathbb{F}_\lambda$-rational points on C_k lying over t_0 correspond to degree-k factors of the specialization $p_\mathfrak{p}(X) - t_0 q_\mathfrak{p}(X) \in \mathbb{F}_\lambda[X]$.

If $\mathrm{Frob}(t_0)$ denotes the Frobenius permutation on the n roots of the specialization $p_\mathfrak{p}(X) - t_0 q_\mathfrak{p}(X)$, then the number of $\mathbb{F}_\lambda$-rational points on C_k lying over t_0 is given by $\pi_k(\mathrm{Frob}(t_0))$, therefore

$$\#C_k(\mathbb{F}_\lambda) \geq \sum_{t_0 \in \mathbb{P}^1(\mathbb{F}_\lambda)\setminus S} \pi_k(\mathrm{Frob}(t_0)). \tag{8.2}$$

8.2.2. Computing the genus of C_k. Since the degree-$\binom{n}{k}$ cover C_k/C_0 has ramification structure $(\sigma_1, \ldots, \sigma_m)$, the Riemann–Hurwitz formula yields

$$g(C_k) = 1 - \binom{n}{k} + \frac{1}{2}\sum_{i=1}^{m} \mathrm{ind}(\sigma_i) \tag{8.3}$$

where $\mathrm{ind}(\sigma_i) := \binom{n}{k}$ − number of cycles of σ_i.

If $(\sigma_1, \ldots, \sigma_m)$ cannot be computed explicitly, one can deduce the upper bound

$$\mathrm{ind}(\sigma_i) \leq \left(\binom{n}{k} - \pi_k(s_i)\right)\left(1 - \frac{1}{\mathrm{ord}(s_i)}\right). \tag{8.4}$$

Note that equality holds if the order of s_i is prime.

8.2.3. Picking a sufficiently large prime. Note that the right hand side of (8.2) behaves differently if $G_\mathfrak{p}$ is not k-transitive: Let d be the number of orbits of $G_\mathfrak{p}$ acting on k-element subsets; then it is reasonable to expect

$$\sum_{t_0 \in \mathbb{P}^1(\mathbb{F}_\lambda)\setminus S} \pi_k(\mathrm{Frob}(t_0)) \approx d\lambda \tag{8.5}$$

for large λ due to the orbit-counting theorem in combination with Chebotarev's density theorem. By comparing (8.2) and (8.5) with the Hasse–Weil bound

(8.1) we obtain $d\lambda \leq \lambda + 2g(C_k)\sqrt{\lambda}$, which leads to $\lambda \leq \frac{4g(C_k)^2}{(d-1)^2}$ in the case $d > 1$.

This observation is a crucial ingredient in the verification process: If $\mathfrak{p}$ is picked such that its norm λ is sufficiently greater than $\frac{4g(C_k)^2}{(d-1)^2}$, we are able to establish a contradiction to the Hasse-Weil bound. This, in particular, allows us to disprove the k-transitivity of G.

8.2.4. Elkies' example: M_{23}. The previously described technique was key for the proof that the degree-23 polynomial $p \in \mathbb{Q}(\alpha)[X]$ given in **[25]** where $\alpha^4 + \alpha^3 + 9\alpha^2 - 10\alpha + 8 = 0$ has geometric monodromy group M_{23}.

With respect to t the ramification locus of $p(X) - t$ consists of exactly three points with ramification type $(4^4.2^2.1^3, 2^8.1^7, 23^1)$. It is standard practice to show that the geometric monodromy group G of p is either the 4-transitive group M_{23} or A_{23}.

Assume $G \cong A_{23}$, then for the prime ideal $\mathfrak{p} := (47\,000\,081, \alpha + 25\,037\,440)$ of norm $\lambda := 47\,000\,081$ we have $G \cong G_\mathfrak{p}$ and both G and $G_\mathfrak{p}$ are 5-transitive. Since the discriminant of $p_\mathfrak{p}(X) - t$ is a square, $A_\mathfrak{p} \cong A_{23} \cong G_\mathfrak{p}$. This leads us to work with the curve C_5: By explicitly computing $(\sigma_1, \sigma_2, \sigma_3)$ we find $g(C_5) = 3285$ using the Riemann–Hurwitz formula (8.3). In combination with the Hasse–Weil bound (8.1) this yields $\#C_5(\mathbb{F}_\lambda) \leq 92\,041\,771$. Counting $\mathbb{F}_\lambda$-rational points on C_5 according to (8.2) reveals the contradiction $\#C_5(\mathbb{F}_\lambda) \geq 93\,981\,891$ with a total computing time of approximately 12 hours using Magma. We obtain $G \cong G_\mathfrak{p} \cong M_{23}$.

8.3. New Applications

8.3.1. The sporadic Conway group Co_3. In this section we will refer to the polynomials $p := -k_3\tilde{p}_3$ and $q := k_2\tilde{p}_2$ presented in [**44**, Proposition 1] of degree 276 over a degree-12 number field $K := \mathbb{Q}(\alpha)$ where $\alpha^{12} - 2\alpha^{11} + 9\alpha^{10} - 20\alpha^9 + 38\alpha^8 - 73\alpha^7 + 101\alpha^6 - 86\alpha^5 + 55\alpha^4 - 46\alpha^3 + 42\alpha^2 - 24\alpha + 6 = 0$.

THEOREM 8.1. *The polynomial $p(X) - tq(X) \in K(t)[X]$ defines a regular Galois extension of $K(t)$ with Galois group isomorphic to the sporadic 2-transitive Conway group Co_3. With respect to t the ramification locus is given by $(0, 1, \infty)$ with corresponding ramification type $(3^{92}, 7^{39}.1^3, 2^{132}.1^{12})$.*

PROOF. An easy computation shows that $p(X) - tq(X)$ is ramified over 0, 1 and ∞ with the given ramification type. The ramification locus cannot be any larger, otherwise this would contradict the Riemann–Hurwitz formula.

Pick the prime ideal $\mathfrak{p} := (7 \cdot 10^9 + 1, \alpha + 2\,738\,443\,742)$ in $\mathcal{O}_K$ of norm $\lambda := 7 \cdot 10^9 + 1$. Note that $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_\lambda$. Because

$$\frac{p_\mathfrak{p}(X)q_\mathfrak{p}(t) - p_\mathfrak{p}(t)q_\mathfrak{p}(X)}{X - t} \in \mathbb{F}_\lambda(t)[X]$$

is irreducible, $A_\mathfrak{p}$ must be 2-transitive. Additionally, the discriminant of $p_\mathfrak{p}(X) - tq_\mathfrak{p}(X) \in \mathbb{F}_\lambda(t)[X]$ is a square. Combining both results, we find $A_\mathfrak{p} \in \{\mathrm{Co}_3, A_{276}\}$ by the classification of finite 2-transitive groups. In both cases we have $G_\mathfrak{p} = A_\mathfrak{p}$ because $G_\mathfrak{p}$ is normal in $A_\mathfrak{p}$.

Under the assumption that $G_\mathfrak{p}$ is 3-transitive we study the curve C_3: Combining (8.4) and (8.3) yields $g(C_3) = 40\,782$. Now, (8.2) gives us

$$\#C_3(\mathbb{F}_\lambda) \geq 13\,999\,925\,705$$

whereas

$$\#C_3(\mathbb{F}_\lambda) \leq 13\,824\,133\,842$$

by the Hasse–Weil bound (8.1). This is a contradiction, thus $G_\mathfrak{p}$ cannot be 3-transitive and we remain with $G_\mathfrak{p} = \mathrm{Co}_3$.

Since $\mathfrak{p}$ is a prime of good reduction for $p(X) - tq(X) \in K(t)[X]$, a theorem of Beckmann, see Section 4.3.2, implies $G \cong G_\mathfrak{p} = \mathrm{Co}_3$. Due to the fact that G is normal in A and $N_{S_{276}}(\mathrm{Co}_3) = \mathrm{Co}_3$ we end up with $A = G \cong \mathrm{Co}_3$. □

The most delicate part in the previous proof is the computation of the right hand side of (8.2). In the following we explain in greater detail this time consuming task (implementation in `PARI/GP` [**49**] with a total computing time of about 8 days using 550 threads simultaneously at the *High Performance Computing Cluster* at the University of Würzburg).

For the sake of simplicity we write $f := p_\mathfrak{p} - t_0 q_\mathfrak{p} \in \mathbb{F}_\lambda[X]$ for some $t_0 \notin S$. In the case $k = 3$ the following holds: If f has exactly d_i irreducible $\mathbb{F}_\lambda[X]$-factors of degree i for $i \in \{1, 2, 3\}$, then $\pi_3(\mathrm{Frob}(t_0)) = \binom{d_1}{3} + d_1 d_2 + d_3$. Note that if a specialization reduces the degree, we have to add 1 to d_1.

In order to find d_1 we compute $p_1 := \gcd(X^\lambda - X, f)$. Clearly, $d_1 = \deg(p_1)$. Since λ is too large for an efficient computation, we replace $X^\lambda - X$ with its reduction modulo f, which can be determined by the *exponentiation by squaring*-method. In the same fashion we find d_2 and d_3: For $p_2 := \gcd(X^{\lambda^2} - X, \frac{f}{p_1})$ and $p_3 := \gcd(X^{\lambda^3} - X, \frac{f}{p_1 p_2})$ we have $d_2 = \frac{1}{2}\deg(p_2)$ and $d_3 = \frac{1}{3}\deg(p_3)$.

Partial results for the computation of the right hand side of (8.2) can be found in the ancillary Magma-readable file `conway_partial_results`.

8.3.2. The symplectic group $\mathrm{PSp}_6(2)$. In Theorems 5.3 and 5.5 we computed 4-point covers of degrees 28 and 36 with respective geometric monodromy group G isomorphic to the 2-transitive symplectic group $\mathrm{PSp}_6(2)$. In order to verify $G = \mathrm{PSp}_6(2)$, standard techniques yield that G is either $\mathrm{PSp}_6(2)$ or an alternating group. In contrast to the arguments given in Chapter 5 to rule out the last case we now apply Elkies' method to give an alternative proof for $G = \mathrm{PSp}_6(2)$. Assume, G is 3-transitive, then for the above covers we get a contradiction regarding the Hasse–Weil bound:

degree	28	36
ramification type	$(2^6.1^{16}, 2^{12}.1^4, 2^{12}.1^4, 7^4)$	$(3^{12}, 2^{12}.1^{12}, 2^{12}.1^{12}, 4^7.2^1.1^6)$
$g(C_3)$	396	1275
λ	700 001	7 000 003
Hasse–Weil bound	$\leq$ 1 362 637	$\leq$ 13 746 671
$\#C_3(\mathbb{F}_\lambda)$	$\geq$ 1 405 359	$\geq$ 14 032 224
computing time	$\approx$ 2 minutes	$\approx$ 35 minutes

8.3.3. The linear groups $\mathrm{PSL}_4(3)$ and $\mathrm{PSL}_6(2)$. In Chapters 6 and 7 the author calculated 4-point covers with geometric monodromy groups isomorphic to the 2-transitive groups $\mathrm{PSL}_4(3)$ and $\mathrm{PSL}_6(2)$. Again, the main task in the verifying process boils down to exclude the large groups A_n or S_n as possibilities. By applying Elkies' method we are able to give alternative proofs that the monodromy groups cannot be 3-transitive:

group	$\mathrm{PSL}_4(3)$ of degree 40	$\mathrm{PSL}_6(2)$ of degree 63
ramification type	$(3^{12}.1^4, 3^9.1^{13}, 2^{16}.1^8, 2^{20})$	$(2^{28}.1^7, 3^{20}.1^3, 3^{20}.1^3, 2^{16}.1^{31})$
$g(C_3)$	1498	5300
λ	9 000 049	120 000 007
Hasse–Weil bound	$\leq$ 17 988 074	$\leq$ 236 117 193
$\#C_3(\mathbb{F}_\lambda)$	$\geq$ 17 993 006	$\geq$ 239 980 524
computing time	$\approx$ 50 minutes	$\approx$ 5 days

Computational remark. In the accompanying file `elkies_method` we provide a `Magma`-program to illustrate the computation of the right hand side of (8.2) for M_{23}, $\mathrm{PSp}_6(2)$, $\mathrm{PSL}_4(3)$ and $\mathrm{PSL}_6(2)$. The specified computing times for these examples refer to computers with an *AMD Ryzen 7 3700X* processor.

Bibliography

[1] E. Artin. *Algebraic numbers and algebraic functions*. Notes on Mathematics and its Applications. New York-London-Paris: Gordon and Breach, Science Publishers. xiv, 1967.

[2] J. S. Balakrishnan, F. Bianchi, V. Cantoral-Farfán, M. Çiperiani, and A. Etropolski. Chabauty–Coleman Experiments for Genus 3 Hyperelliptic Curves. In J. S. Balakrishnan, A. Folsom, M. Lalín, and M. Manes, editors, *Research Directions in Number Theory*, page 67–90, Cham, 2019. Springer International Publishing.

[3] J. Barnes. *Conformal welding of uniform random trees*. PhD thesis, 2014.

[4] D. Barth, J. König, and A. Wenz. An approach for computing families of multi-branch-point covers and applications for symplectic Galois groups. *Journal of Symbolic Computation*, 101:352–366, 2020.

[5] D. Barth and A. Wenz. Explicit Polynomials Having the Higman-Sims Group as Galois Group over $\mathbb{Q}(t)$. 2016, arXiv:1611.04314.

[6] D. Barth and A. Wenz. Belyi map for the sporadic group J_1. 2017, arXiv:1704.06419.

[7] D. Barth and A. Wenz. Belyi map for the sporadic group J_2. 2017, arXiv:1712.05268.

[8] D. Barth and A. Wenz. Explicit Belyi maps over $\mathbb{Q}$ having almost simple primitive monodromy groups. 2017, arXiv:1703.02848.

[9] D. Barth and A. Wenz. A one-parameter family of degree 36 polynomials with $\mathrm{PSp}_6(2)$ as Galois group over $\mathbb{Q}(t)$, 2018, arXiv:1809.09856.

[10] D. Barth and A. Wenz. A family of 4-branch-point covers with monodromy group $\mathrm{PSL}_6(2)$, 2020, arXiv:2004.10997.

[11] D. Barth and A. Wenz. Computation of Belyi maps with prescribed ramification and applications in Galois theory. *Journal of Algebra*, 569:616–642, 2021.

[12] D. Barth and A. Wenz. On Elkies' method for bounding the transitivity degree of Galois groups. *Journal of Symbolic Computation*, 108:17–22, 2022.

[13] S. Beckmann. On extensions of number fields obtained by specializing branched coverings. *J. Reine Angew. Math.*, 419:27–53, 1991.

[14] C. J. Bishop. True trees are dense. *Inventiones mathematicae*, 197(2):433–452, Oct. 2013.

[15] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[16] P. J. Cameron. Strongly regular graphs. In *Topics in algebraic graph theory*, page 203–221. Cambridge: Cambridge University Press, 2004.

[17] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups. With comput. assist. from J. G. Thackray.* Oxford: Clarendon Press. XXXIII, 252 p., 1985.

[18] J.-M. Couveignes. Tools for the computation of families of coverings. In *Aspects of Galois theory (Gainesville, FL, 1996)*, volume 256 of *London Math. Soc. Lecture Note Ser.*, page 38–65. Cambridge Univ. Press, Cambridge, 1999.

[19] D. A. Cox. *Galois Theory.* John Wiley & Sons, Inc., Mar. 2012.

[20] P. Dembowski. *Finite geometries.*, volume 44. Springer-Verlag, Berlin, 1968.

[21] M. Dettweiler. Plane curve complements and curves on Hurwitz spaces. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 2004(573), Jan. 2004.

[22] T. A. Driscoll. Algorithm 756: A MATLAB toolbox for Schwarz-Christoffel Mapping. *ACM Trans. Math. Softw.*, 22(2):168–186, June 1996.

[23] P. Dèbes. Reduction and specialization of polynomials. *Acta Arith.*, 172(2):175–197, 2016.

[24] P. Dèbes and M. D. Fried. Nonrigid constructions in Galois theory. *Pacific J. Math.*, 163(1):81–122, 1994.

[25] N. D. Elkies. The complex polynomials $P(x)$ with $\mathrm{Gal}(P(x) - t) \cong M_{23}$. In *ANTS X. Proceedings of the tenth algorithmic number theory symposium, San Diego, CA, USA, July 9–13, 2012*, page 359–367. Berkeley, CA: Mathematical Sciences Publishers (MSP), 2013.

[26] M. D. Fried and H. Völklein. The inverse Galois problem and rational points on moduli spaces. *Math. Ann.*, 290(4):771–800, 1991.

[27] E. Girondo and G. González-Diez. *Introduction to compact Riemann surfaces and dessins d'enfants*, volume 79. Cambridge: Cambridge University Press, 2012.

[28] C. Godsil and G. Royle. *Algebraic graph theory*, volume 207. New York, NY: Springer, 2001.

[29] E. Hallouin. Study and computation of a Hurwitz space and totally real $\mathrm{PSL}_2(\mathbb{F}_8)$-extensions of $\mathbb{Q}$. *Journal of Algebra*, 292(1):259–281, 2005. Computational Algebra.

[30] W. M. Kantor. Note on symmetric designs and projective spaces. *Math. Z.*, 122:61–62, 1971.

[31] M. Klug, M. Musty, S. Schiavone, and J. Voight. Numerical calculation of three-point branched covers of the projective line. *LMS Journal of Computation and Mathematics*, 17(1):379–430, 001 2014.

[32] J. Klüners and G. Malle. A database for field extensions of the rationals. *LMS J. Comput. Math.*, 4:182–196, 2001.

[33] J. König. *The inverse Galois problem and explicit computation of families of covers of* $\mathbb{P}^1\mathbb{C}$ *with prescribed ramification.* PhD thesis, Würzburg, 2014.

[34] J. König. Computation of Hurwitz spaces and new explicit polynomials for almost simple Galois groups. *Math. Comp.*, 86(305):1473–1498, 2017.

[35] E. S. Lander. *Symmetric designs: an algebraic approach.* London Mathematical Society Lecture Note Seris, 74: Cambridge University Press. XII, 1983.

[36] S. K. Lando and A. K. Zvonkin. *Graphs on surfaces and their applications. Appendix by Don B. Zagier.* Berlin: Springer, 2004.

[37] G. Malle. Multi-parameter polynomials with given Galois group. *J. Symbolic Comput.*, 30(6):717–731, 2000. Algorithmic methods in Galois theory.

[38] G. Malle and B. H. Matzat. *Inverse Galois theory.* Berlin: Springer, 2nd edition, 2018.

[39] D. E. Marshall and S. Rohde. Convergence of a variant of the zipper algorithm for conformal mapping. *SIAM J. Numer. Anal.*, 45(6):2577–2609, 2007.

[40] MATLAB. *version 9.11.0 (R2021b).* The MathWorks Inc., Natick, Massachusetts, 2021.

[41] B. H. Matzat. Konstruktion von Zahl- und Funktionenkörpern mit vorgegebener Galoisgruppe. *J. Reine Angew. Math.*, 349:179–220, 1984.

[42] H. Monien. How to calculate rational coverings for subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ efficiently. In Embedded Graphs 2014, 2014.

[43] H. Monien. The sporadic group J_2, Hauptmodul and Belyi map. 2017, arXiv:1703.05200.

[44] H. Monien. The sporadic group Co_3, Hauptmodul and Belyi map, 2018, arXiv:1802.06923.

[45] D. P. Roberts. Hurwitz-Belyi maps. In *Algèbre et théorie des nombres 2018*, page 25–67. Besançon: Presses Universitaires de Franche-Comté, 2018.

[46] M. Romagny and S. Wewers. Hurwitz spaces. In *Groupes de Galois arithmétiques et différentiels*, volume 13 of *Sémin. Congr.*, page 313–341. Soc. Math. France, Paris, 2006.

[47] J. Sijsling and J. Voight. On computing Belyi maps. In *Numéro consacré au trimestre "Méthodes arithmétiques et applications", automne 2013*, page 73–131. Besançon: Presses Universitaires de Franche-Comté, 2014.

[48] H. Stichtenoth. *Algebraic function fields and codes*, volume 254. Berlin: Springer, 2009.

[49] The PARI Group, Univ. Bordeaux. *PARI/GP version `2.13.3`*, 2021. available from `https://pari.math.u-bordeaux.fr`.

[50] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.5)*, 2022. `https://www.sagemath.org`.

[51] R. Vidunas and Y.-H. He. Composite genus one Belyi maps. *Indag. Math., New Ser.*, 29(3):916–947, 2018.

[52] H. Völklein. *Groups as Galois groups*, volume 53 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1996. An introduction.

[53] A. Wenz. *Computation of Belyi maps with prescribed ramification and applications in Galois theory.* PhD thesis, Würzburg, 2021.

[54] A. Zvonkin. How to draw a group? *Discrete Math.*, 180(1-3):403–413, 1998.