The inverse Galois problem and explicit computation of families of covers of $\mathbb{P}^1\mathbb{C}$ with prescribed ramification

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

vorgelegt von

Joachim König

Würzburg, März 2014.

Institut für Mathematik der Universität Würzburg

Eingereicht am 5.3.2014

Erster Gutachter: Prof. Dr. Peter Müller
Zweiter Gutachter: Prof. Dr. Kay Magaard
Dritter Gutachter: Prof. Dr. Michael Dettweiler

Tag der mündlichen Prüfung: 25.6.2014

Contents

Chapter 1

Introduction

Riemann's existence theorem famously solves the regular inverse Galois problem over $\mathbb{C}$, guaranteeing for every finite group G the existence of Galois extensions $F|\mathbb{C}(t)$ with Galois group G.
In attempting to solve the regular inverse Galois problem for smaller fields $K \subset \mathbb{C}$ (particularly for $K = \mathbb{Q}$), a very important result by Fried and Völklein (cf. Thm. 2.3) reduces the existence of regular Galois extensions $F|K(t)$ with Galois group G to the existence of K-rational points on components of certain moduli spaces for families of covers of the projective line, known as Hurwitz spaces.

In some cases, the existence of rational points on Hurwitz spaces has been proven by theoretical criteria. A famous example is Matzat's regular realization of the Mathieu group M_{24} over $\mathbb{Q}$ ([41]).

In general, however, the question whether a given Hurwitz space has any rational point remains a very difficult problem. In concrete cases, it may be tackled by an explicit computation of a Hurwitz space and the corresponding family of covers.

This explicit computation of families of covers of the projective line has been of interest in Galois theory for many years, not only for the sake of theoretical existence results. Notable results have been achieved by various authors, e.g. Malle, Matzat, Granboulan, Couveignes, Hallouin and others (cf. e.g. [7], [8], [19], [22], [23] and [35]). The aim of this work is to collect and expand on the various techniques that may be used to solve such computational problems and apply them to tackle several families of Galois theoretic interest. In particular, in Chapters 5.1 and 5.3, we compute explicit curve equations for Hurwitz spaces for certain families of M_{24} and M_{23}. These are (to my knowledge) the first examples of explicitly computed Hurwitz spaces of such high genus. They might be used to realize M_{23} as a regular Galois group over $\mathbb{Q}$ if one manages to find suitable points on them.

Apart from the calculation of explicit algebraic equations, we produce complex approximations for polynomials with genus zero ramification of several different ramification types in M_{24} and M_{23}. These may be used as starting points for similar computations.

The main motivation for these computations is the fact that M_{23} is currently the only remaining sporadic group that is not known to occur as a Galois group over $\mathbb{Q}$ (see e.g. [39, Thms. II.9.9 and III.7.12]).

We also compute the first explicit polynomials with Galois groups $G = P\Gamma L_3(4), PGL_3(4), PSL_3(4)$ and $PSL_5(2)$ over $\mathbb{Q}(t)$.
Special attention will be given to reality questions. As an application we compute the first examples of totally real polynomials with Galois groups $PGL_2(11)$ and $PSL_3(3)$ over $\mathbb{Q}$.

As a suggestion for further research, we describe an explicit algorithmic version of "Algebraic Patching", following the theory described e.g. in [27]. This could be used to conquer some problems regarding families of covers of genus $g > 0$.
Finally, we present explicit Magma implementations for several of the most important algorithms involved in our computations.

Acknowledgement:
I would like to thank Prof. Peter Müller for introducing me into many of the subjects of this work as well as carefully reading earlier versions.
I would also like to thank Ruben Schulze for many interesting talks about Algebraic Patching.

Remark:
The text files referred to at various points throughout this work were originally contained on an attached CD. They are now available for download under

`www.mathematik.uni-wuerzburg.de/∼koenig`.

Chapter 2

The regular inverse Galois problem and Hurwitz spaces

We begin with an outline of theoretical prerequisites for the later computations. In particular, this chapter explains the definition of Hurwitz spaces and their connection with the inverse Galois problem.

2.1 The regular inverse Galois problem

The inverse Galois problem (IGP) asks which finite groups occur as Galois groups over $\mathbb{Q}$ (or more generally, over any given base field). In 1892, David Hilbert proved his famous irreducibility theorem, stating the following (see e.g. [55, Def. 1.9 and Th. 1.23.]):

Theorem 2.1 (Hilbert's irreducibility theorem)**.** *Let $f(t, X)$ be an irreducible polynomial in two variables over $\mathbb{Q}$, of degree at least one in X. Then there are infinitely many specializations $t \mapsto t_0 \in \mathbb{Q}$ such that the specialized polynomial $f(t_0, X) \in \mathbb{Q}[X]$ remains irreducible.*

Definition 2.1 (Regular extension of function fields)**.** An extension $E \mid F$ of function fields is called regular, if E and F have the same field of constants.

In analogy to the (IGP), the regular inverse Galois problem (RIGP) asks which groups occur as Galois groups of regular extensions of $\mathbb{Q}(t)$.

As an easy corollary of Hilbert's irreducibility theorem, any group that occurs as a Galois group over $\mathbb{Q}(t)$ will also occur as a Galois group over $\mathbb{Q}$.

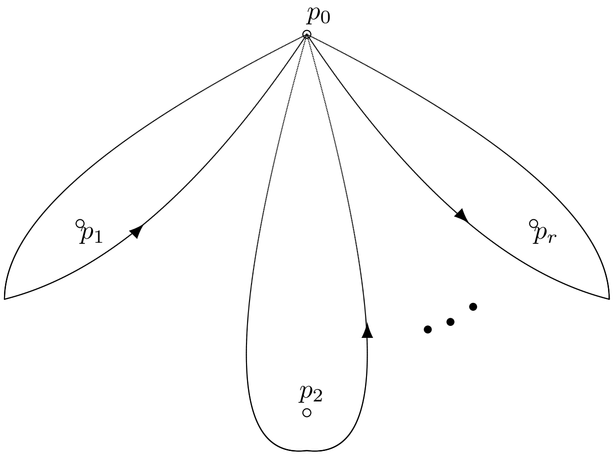
A positive answer to the (RIGP) would therefore imply a positive answer to the (IGP). The stronger (RIGP) might seem even harder to tackle than the (IGP) itself, but it has the advantage that one can apply methods from complex analysis and topology. This helps to solve the (RIGP) over $\mathbb{C}(t)$. The main tool herefore is Riemann's existence theorem.

2.2 Topological prerequisites: Fundamental groups and Riemann's existence theorem

Here we collect some of the basic topological results needed for the study of ramified coverings of the projective line. These are well-known. For a detailed explanation cf. [55, Chapter 4], which we here follow with regard to general notation.

Let $r \in \mathbb{N}$, and let $P = \{p_1, ..., p_r\}$ be a subset of $\mathbb{P}^1\mathbb{C}$ of cardinality r. Let $\pi_1(\mathbb{P}^1\mathbb{C} \setminus P, p_0)$ the topological fundamental group of the punctured projective line, with base point $p_0 \in \mathbb{P}^1\mathbb{C} \setminus P$. This group is generated by the homotopy classes of paths $\gamma_1, ..., \gamma_r$, where γ_i is any path starting and ending in p_0 and turning counter-clockwise around p_i (and around no other p_j). We denote the path and its homotopy class by the same letter, as there is no risk of confusion.
Assume in addition that the paths $\gamma_1, ..., \gamma_r$ are ordered counter-clockwise as in Figure 2.1. The fundamental group generators then satisfy the relation $\gamma_1 \cdots \gamma_r = 1$.

Figure 2.1: Standard configuration for fundamental group generators



Definition 2.2 (Covering maps of manifolds). Let R, S be topological manifolds. A surjection $f : R \to S$ is called a covering if for every $p \in S$ there exists a connected open neighborhood U such that every connected component of the preimage $f^{-1}(U)$ is open and mapped homeomorphically onto U by f.

If in the above situation S is connected and $p_0 \in S$ such that $|f^{-1}(p_0)| = n$ is finite, then all other fibers $f^{-1}(p)$ for $p \in S$ are of cardinality n as well. In this case, f can therefore be referred to as an *n-fold* covering of S.

Definition 2.3 (Lifts of paths)**.** Let $f : R \to S$ be a covering and γ a path in S. A lift of γ is a path $\overline{\gamma}$ in R such that $f \circ \overline{\gamma} = \gamma$.

Lifting the paths γ_i to their preimages (numbered by $1, ..., n$) then leads to a homomorphism φ of the fundamental group into the symmetric group S_n, with $a^{(\gamma_i)\varphi} = b$ if and only if the preimage of γ_i beginning in point $a(\in \{1, ..., n\})$ ends in point b (cf. e.g. [55, Th. 4.12]).
The image of the fundamental group under this action is called the monodromy group of the covering f.
We will refer to the ordered tuple of images of the fundamental group generators $\gamma_1, ..., \gamma_r$ under this action as the branch cycle description $(\overline{\gamma_1}, ..., \overline{\gamma_r})$ of the cover. This tuple is then unique up to simultaneous conjugation in S_n.

Another point of view of monodromy action is via deck transformations:

Definition 2.4 (Deck transformations)**.** A deck transformation of a covering $f : R \to S$ is a homeomorphism $\alpha : R \to R$ such that $f\alpha = f$.

It is easy to see that the deck transformations of a covering form a group which acts on the fibers $f^{-1}(p)$ of the cover.

Definition 2.5 (Galois covering)**.** A covering $f : R \to S$ is called a Galois covering if R and S are connected and the group of deck transformations acts transitively on each fiber $f^{-1}(p)$.

In fact, for Galois coverings, the action of the deck transformation group on a fiber and the action of the fundamental group via lifting of paths can be identified (technically, they differ by an anti-isomorphism).

Remark: If the set $P = \{p_1, ..., p_r\}$ of a covering $f : R \to \mathbb{P}^1\mathbb{C} \setminus P$ is understood (or not relevant for certain considerations), we simply speak of a covering f of $\mathbb{P}^1\mathbb{C}$. This is justified by the fact that every n-fold covering $f : R \to \mathbb{P}^1\mathbb{C} \setminus P$ in the above sense can be uniquely extended to a *branched* covering $\widehat{f} : \widehat{R} \to \mathbb{P}^1\mathbb{C}$ of algebraic varieties, with fibers $\widehat{f}^{-1}(p)$ of cardinality less than n at most for $p \in P$.

A central and well-known result for n-fold Galois coverings of a punctured projective line $\mathbb{P}^1\mathbb{C} \setminus P$ is the topological version of Riemann's existence theorem (cf. e.g. [55, Th. 4.32]):

Theorem 2.2 (Riemann's existence theorem, topological version)**.** *Let G be a finite group of order n; $C_1, ..., C_r$ be conjugacy classes of G, all $\neq \{1\}$, and $P = \{p_1, ..., p_r\}$ be an r-subset of $\mathbb{P}^1\mathbb{C}$.*
Then the following are equivalent:

- *There exists an n-fold Galois covering of $\mathbb{P}^1\mathbb{C} \setminus P$ with deck transformation group isomorphic to G and branch cycle description $(\overline{\gamma_1}, ..., \overline{\gamma_r})$ such that $\sigma(\overline{\gamma_i}) \in C_i$ for all $i = 1, ..., r$ (with some isomorphism $\sigma : \langle \overline{\gamma_1}, ..., \overline{\gamma_r} \rangle \to G$).*
- *There exists $(g_1, ..., g_r) \in C_1 \times ... \times C_r$, with $\langle g_1, ..., g_r \rangle = G$ and $g_1 \cdots g_r = 1$.*

As we want to obtain information about the Galois groups of function fields via topological methods it is of decisive importance that there is a natural correspondence between finite coverings $f : R \to \mathbb{P}^1\mathbb{C}$ (with R connected) and finite extensions $L \mid \mathbb{C}(t)$. Here L is the field of meromorphic functions of (the compact Riemann surface) R.
For Galois coverings and Galois field extensions respectively, this leads to an identification of the Galois group of a Galois extension $L \mid \mathbb{C}(t)$ with the group of deck transformations (or, equivalently, the monodromy group) of an appropriate Galois covering $f : R \to \mathbb{P}^1\mathbb{C}$.
This correspondence is stated e.g. in [55, Theorem 5.14].

In particular, as $L = \mathbb{C}(t, x)$ is a function field of one variable, f can be expressed through a polynomial equation $p(t, x) = 0$, i.e. R is (the projective closure of) the curve defined by p, and f is just the projection to the first component.
The lifting property above can then be used to compute the monodromy action of the fundamental group numerically, by starting at an unramified point $t_0 \in \mathbb{C}$, moving t_0 in small steps along a path around a branch point, and taking preimages in R via the equation $p(t_0, x) = 0$. This approach, of course, works for arbitrary (not only Galois) coverings of finite degree of $\mathbb{P}^1\mathbb{C}$, i.e. for arbitrary intermediate fields of a finite Galois extension of $\mathbb{C}(t)$.

2.3 Moduli spaces for families of covers and the Hurwitz braid group

Hurwitz spaces are known as a very important tool to study families of covers with given ramification. They were studied by various authors.
The following fundamental properties can be found (with slightly different methods of construction) in several papers and monographs, e.g. in [16], [39, Chapter III], [48], [55] etc.

Define $\mathcal{U}^r \subset (\mathbb{P}^1)^r$ as $\mathcal{U}^r := \{(x_1, ..., x_r) \in (\mathbb{P}^1)^r \mid x_i \neq x_j$ for $i \neq j\}$, in other words: The space consisting of all ordered sets of cardinality exactly r, with elements in $\mathbb{P}^1$ (the projective line over $\mathbb{C}$).
Furthermore denote by $\mathcal{U}_r$ the quotient of this space modulo the action of S_r (i.e. the space of *unordered* r-sets).
These spaces carry a natural structure as topological manifolds (via the structure of $\mathbb{P}^1\mathbb{C}$).

Definition 2.6 (Hurwitz braid group)**.** Let $r \geq 4$. The Hurwitz braid group $\mathcal{H}_r$ can be defined abstractly as the group generated by elements $\beta_1, ..., \beta_{r-1}$, satisfying the relations

$$\beta_i \beta_{i+1} \beta_i = \beta_{i+1} \beta_i \beta_{i+1},\ i = 1, ..., r-2$$

$$\beta_i \beta_j = \beta_j \beta_i,\ 1 \leq i < j-1 \leq r-1$$

$$\beta_1 \beta_2 ... \beta_{r-1} \beta_{r-1} \beta_{r-2} ... \beta_1 = 1$$

It is well known that this group is isomorphic to the topological fundamental group of the space $\mathcal{U}_r$ defined above, i.e.:

$$\mathcal{H}_r \cong \pi_1(\mathcal{U}_r, p),$$

where $p \in \mathcal{U}_r$ is a base point.

As $\mathcal{U}_r$ is a quotient of $\mathcal{U}^r$, the fundamental group of $\mathcal{U}^r$ is a normal subgroup of $\mathcal{H}_r$.
This subgroup (also referred to as the *pure* Hurwitz braid group) is generated by the elements

$$\beta_{i,j} := (\beta_i^2)^{\beta_{i+1}^{-1} \cdots \beta_{j-1}^{-1}}, \quad \text{with } 1 \leq i < j \leq r,$$

cf. [39, III.1.2].

Braid groups are directly linked to moduli spaces of covers of the projective line:
Let G be a given finite group. Let S be a subset of the projective line $\mathbb{P}^1\mathbb{C}$ of cardinality r, P_0 be any point in $\mathbb{P}^1 \setminus S$ and $f : \pi_1(\mathbb{P}^1 \setminus S, P_0) \to G$ be an epimorphism mapping none of the canonical generators $\gamma_1, ..., \gamma_r$ of the fundamental group to the identity. On the set of such triples (S, P_0, f) one defines an equivalence relation via $(S, P_0, f) \sim (S', P_0', f') :\Leftrightarrow S = S'$ and there exists a path γ from P_0 to P_0' in $\mathbb{P}^1 \setminus S$ such that the induced map $\gamma^\star : \pi_1(\mathbb{P}^1 \setminus S, P_0) \to \pi_1(\mathbb{P}^1 \setminus S, P_0')$ on the fundamental groups fulfills $f' \circ \gamma^\star = f$.
Identifying the group G with the deck transformation group of a Galois cover $\varphi : X \to \mathbb{P}^1 \setminus S$, Riemann's existence theorem leads to a natural identification of these equivalence classes $[S, P_0, f]$ with equivalence classes $[\varphi, h]$, where $\varphi : X \to \mathbb{P}^1 \setminus S$ is a Galois cover that can be extended to a branched cover of $\mathbb{P}^1$ with exactly r branch points, and h is an isomorphism from the group of deck transformations of φ to G. Cf. [16, Section 1.2.] (especially for the precise identification between the two different sets of equivalence classes) and [55, 10.1].

Denote the set of these equivalence classes by $\mathcal{H}_r^{in}(G)$.
Note that the path γ in the definition of the equivalence relation is not unique. In particular, for $P_0 = P_0'$, γ may be chosen arbitrarily in $\pi_1(\mathbb{P}^1 \setminus S, P_0)$, so $(S, P_0, f) \sim (S, P_0, f')$ iff $f' \circ \gamma^\star = f$ for some $\gamma \in \pi_1(\mathbb{P}^1 \setminus S, P_0)$, i.e. iff $a \circ f' = f$ for some $a \in Inn(G)$ (namely conjugation with $f'(\gamma)$).

This allows a generalization of the definition of $\mathcal{H}_r^{in}(G)$, by substituting $Inn(G)$ with other groups of automorphisms, cf. [55, 10.1.3.1].

Especially, if G is given as a transitive permutation group, we define $\mathcal{H}_r^{ab}(G)$ as the set of equivalence classes $[S, P_0, f]$, where the above definition of an equivalence relation is altered to $a \circ f' \circ \gamma^\star \overset{!}{=} f$, where a is an automorphism of G induced by some element of the symmetric normalizer of G.

The sets $\mathcal{H}_r^{ab}(G)$ and $\mathcal{H}_r^{in}(G)$ become topological spaces in a natural way if one defines neighborhood bases in the following way (as outlined e.g. in [16], Chapter 1.2.):
First, if $S := \{P_1, ..., P_r\}$ is the set of branch points of a given cover φ and $P_0 \notin S$, choose disjoint open discs $D_1, ..., D_r$ around the points $P_1, ..., P_r$ such that $P_0 \notin D_1 \cup ... \cup D_r$. A neighborhood of $[S, P_0, f] \in \mathcal{H}_r^{in}(G)$ (and analogously for $\mathcal{H}_r^{ab}(G)$) is then given by the set of all $[S', P_0, f']$[1] with branch point set S' such that one branch point lies in each of $D_1, ..., D_r$, and f' and f are equal up to composition with the canonical isomorphisms of fundamental groups $\pi_1(\mathbb{P}^1 \setminus S', P_0) \to \pi_1(\mathbb{P}^1 \setminus (D_1 \cup ... \cup D_r), P_0) \to \pi_1(\mathbb{P}^1 \setminus S, P_0)$.

If one now defines $\Psi : \mathcal{H}^{ab} \to \mathcal{U}_r$ and $\Psi' : \mathcal{H}^{in} \to \mathcal{U}_r$ by mapping the respective equivalence classes to the sets S (i.e. by mapping the respective equivalence classes of covers to their branch point sets), one obtains unramified coverings. The fundamental group of $\mathcal{U}_r$ therefore acts on the fibers via lifting of paths. Translating this action into group theory leads to the action in (2.1).

Apart from the topological structure outlined above, the spaces $\mathcal{U}^r$ and $\mathcal{U}_r$ are also (quasi-projective) algebraic varieties. A suitable (higher dimensional) version of Riemann's existence theorem then assures that the spaces $\mathcal{H}^{in}$ and $\mathcal{H}^{ab}$ become (usually reducible) algebraic varieties as well, via the covering maps Ψ and Ψ'. In other words, $\Psi : \mathcal{H}^{ab} \to \mathcal{U}_r$ and and $\Psi' : \mathcal{H}^{in} \to \mathcal{U}_r$ become algebraic morphisms.

This directly links the inverse Galois problem with the existence of rational points on certain algebraic varieties.

The main result is the following (cf. [55, Cor. 10.25] and [11, Th. 4.3]):

Theorem 2.3. *Let G be a finite group with $Z(G) = 1$.*
There is a universal family of ramified coverings $\mathcal{F} : \mathcal{T}_r(G) \to \mathcal{H}_r^{in}(G) \times \mathbb{P}^1\mathbb{C}$, such that for each $h \in \mathcal{H}_r^{in}(G)$, the fiber cover $\mathcal{F}^{-1}(h) \to \mathbb{P}^1\mathbb{C}$ 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.

[1] Note that demanding $P_0' = P_0$ for some representative of an equivalence class is not a restriction!

2.4 Components of moduli spaces and braid orbit genera

The connection of the topological spaces introduced above with group theoretic methods leads to the definition of Nielsen classes:

Definition 2.7 (Nielsen class)**.** Let G be a finite group, $r \geq 2$ and $\mathcal{E}_r(G) := \{(\sigma_1, ...\sigma_r) \in (G \backslash \{1\})^r \mid \sigma_1 \cdot ... \cdot \sigma_r = 1, \langle \sigma_1, ..., \sigma_r \rangle = G\}$ the set of all generating r-tuples in $G \setminus \{1\}$ with product 1. Furthermore let $\mathcal{E}_r^{in}(G)$ be the quotient of $\mathcal{E}_r(G)$ modulo conjugating the tuples simultaneously with elements of G; and if $G \leq S_n$ is given as a transitive permutation group, denote by $\mathcal{E}_r^{ab}(G)$ the quotient under the analogous action of the symmetric normalizer of G.
For any r-tuple $C := (C_1, ..., C_r)$ of non-trivial conjugacy classes of G the Nielsen class $Ni(C)$ is defined as the set of all $(\sigma_1, ...\sigma_r) \in \mathcal{E}_r(G)$ such that for some permutation $\pi \in S_r$ it holds that $\sigma_i \in C_{\pi(i)}$ for all $i \in \{1, ..., r\}$. The definition of $Ni^{in}(C)$ and $Ni^{ab}(C)$ is then possible in analogy to the above notation (in the last case, one should factor out the action of $SN(C) := \{\gamma \in N_{S_n}(G) \mid \exists \pi \in S_r : (C_i)^\sigma = C_{\pi(i)}$ for all $1 \leq i \leq r\})$.

The Hurwitz braid group $\mathcal{H}_r$ acts naturally on the set $\mathcal{E}_r(G)$ (with an induced action on $\mathcal{E}_r^{in}(G)$ resp. $\mathcal{E}_r^{ab}(G)$) via

$$(\sigma_1, ..., \sigma_r)^{\beta_i} := (\sigma_1, ..., \sigma_{i-1}, \sigma_{i+1}, \sigma_i^{\sigma_{i+1}}, ..., \sigma_r), \text{ for } i = 1, ..., r-1 \tag{2.1}$$

It is obvious that the sets $Ni^{ab}(C)$ and $Ni^{in}(C)$ are unions of orbits under these actions.

As $\mathcal{H}_r$ is the fundamental group of $\mathcal{U}_r$, it acts on the fibers $\Psi^{-1}(p)$ and $\Psi'^{-1}(p)$ respectively (for $p \in \mathcal{U}_r$ a base point).
However, the elements of a given fiber are in 1-1 correspondence with elements of $\mathcal{E}_r^{ab}(G)$ (for Ψ) and $\mathcal{E}_r^{in}(G)$ (for Ψ'). Indeed, the above action on equivalence classes of r-tuples of elements on G is, via this correspondence, essentially the same as the action of the fundamental group on the fiber via lifting of paths.

Via the above topological construction, each of the orbits of the braid group acting on $Ni^{in}(C)$ corresponds to a connected component of $\mathcal{H}_r^{in}(G)$. The union of all connected components corresponding to $Ni^{in}(C)$ is what is usually referred to as a Hurwitz space:

Definition 2.8 (Hurwitz spaces)**.** For an r-tuple C of conjugacy classes of a group G with a non-empty Nielsen class $Ni^{in}(C)$, the union of components of $\mathcal{H}_r^{in}(G)$ corresponding to $Ni^{in}(C)$ is called the (inner) Hurwitz space of C.

Remarks:

1. In the case that the braid group action on $Ni^{in}(C)$ is transitive, the corresponding Hurwitz space $\mathcal{H}_r^{in}(G)$ is connected.
2. In analogy to the definition of $\mathcal{H}_r^{ab}(G)$, there is of course also a notion of an absolute Hurwitz space of a class tuple (cf. [16]).
   Rational points on these spaces are also quite important, if one looks for polynomials with *geometric*, but not necessarily *arithmetic* Galois group G over $\mathbb{Q}(t)$. For our purposes, however, the inner Hurwitz space will usually suffice.
   Note that our use of "absolute" always requires a permutation representation of the group G.

If one leaves out the permutation π in the above definition of a Nielsen class, one gets the notion of a straight Nielsen class:

$$SNi(C) := \{(\sigma_1, ...\sigma_r) \in \mathcal{E}_r(G) \mid \sigma_i \in C(i) \text{ for } i = 1, ..., r\}$$

The definition of $SNi^{in}(C)$ is then possible in analogy to Def. 2.7.

As the braid group permutes the components of the class tuple transitively it is clear that as soon as the C_i are not all the same class, straight Nielsen classes are not unions of orbits under the braid group action.
It is however very useful to consider the stabilizers of straight Nielsen classes in the braid group.

The appropriate generators of these subgroups enable one to compute braid orbit genera and therefore, particularly in the case $r = 4$, to obtain informations about points on Hurwitz spaces.

To do this, assign a partial ordering to the branch points of a cover $\varphi : X \to \mathbb{P}^1$ via ordering the conjugacy classes involved in the branch cycle description, as in the above definition of $SNi(C)$. Now, if the class C_i occurs k_i times in C $(i = 1, ..., s)$, denote by

$$\tilde{\mathcal{U}_r} := \tilde{\mathcal{U}_r}(C) := \{(S_1, ..., S_s) | S_i \subset \mathbb{P}^1\mathbb{C}, |S_i| = k_i; | \cup_{i=1}^s S_i| = r\}$$

the according space of partially ordered r-sets in $\mathbb{P}^1$. Then the map $\mathcal{H}^{in}(C) \to \tilde{\mathcal{U}_r}$, assigning to each $h \in \mathcal{H}^{in}(C)$ the partially ordered branch point set, is well-defined. One obtains a sequence of topological covers (by first mapping a cover to its partially ordered branch point set, and then further to the unordered one), which can be completed to morphisms of varieties:

$$\mathcal{H}^{in}(C) \xrightarrow{\alpha} \mathcal{H}^{ab}(C) \xrightarrow{\Psi_0} \tilde{\mathcal{U}_r} \xrightarrow{\beta} \mathcal{U}_r$$

with $\beta \circ \Psi_0 \circ \alpha = \Psi'_{|\mathcal{H}^{in}(C)}$, the branch point reference map defined in the previous section.

By Theorem 2.3, it is of Galois theoretic interest whether the variety $\mathcal{H}^{in}(C)$ has a K-rational point (for some field $K \subset \mathbb{C}$). Of course, as a necessary condition, it needs to be defined over K. This latter question can be answered by purely group theoretic means (cf. [16, Th. 1]), and is related to the branch cycle argument (see Lemma 3.3 in the next chapter).

Theorem 2.4. *Let $(C_1, ..., C_r)$ be an r-tuple of classes of a finite group G with trivial center, $n := |G|$, K a subfield of $\mathbb{C}$ and $\zeta_n \in \mathbb{C}$ a primitive n-th root of unity.*
$\mathcal{H}^{in}(C)$ is defined over K if and only if the following holds:
For all $\gamma \in Aut(\overline{K}|K)$, if $\gamma^{-1}(\zeta_n) = \zeta_n^m$ (for $m \in \mathbb{N}$), then $(C_1^m, ..., C_r^m)$ is a permutation of $(C_1, ..., C_r)$.

In this case, the class tuple $(C_1, ..., C_r)$ is called K-rational.

To compute braid orbit genera, one progresses to certain curves on Hurwitz spaces.
Always assume that $Z(G) = \{1\}$, and that the braid group action on $SNi^{in}(C)$ is transitive.[2] Following [11, Theorem 4.3], one has the following morphisms between (quasi-projective) varieties:

- $\mathcal{F} : \mathcal{T} \to \mathcal{H}^{in}(C) \times \mathbb{P}^1$, the universal family of covers in the Nielsen class $Ni^{in}(C)$.
- $\mathcal{H}^{in}(C) \to \tilde{\mathcal{U}}_r$ resp. $\mathcal{H}^{in}(C) \to \mathcal{U}_r$, mapping each point of $\mathcal{H}^{in}(C)$ to its (partially ordered or unordered) set of branch points.
- Proceeding to the pullback $(\mathcal{H}^{in})'(C) := \mathcal{H}^{in}(C) \times_{\mathcal{U}_r} \mathcal{U}^r$, one also obtains a morphism $(\mathcal{H}^{in})'(C) \to \mathcal{U}^r$.
  This remains true for the pullback over $\tilde{\mathcal{U}}_r$.
- Via PGL_2-action, $(\mathcal{H}^{in})'(C)$ is birationally equivalent to $\mathbb{P}^1\mathbb{C} \times \mathbb{P}^1\mathbb{C} \times \mathbb{P}^1\mathbb{C} \times \mathcal{H}^{red}(C)$, where $\mathcal{H}^{red}(C)$ is the image under the above map of the subvariety of $(\mathcal{H}^{in})'(C)$ consisting of covers with the first three branch points equal to 0, 1, and ∞ (in this order).
- This restriction gives a morphism of $r-3$-dimensional varieties $\mathcal{H}^{red}(C) \to \mathcal{U}^{r-3}$.

In particular, via the action of $PGL_2(\mathbb{C})$, the dimension of the Hurwitz spaces can be reduced by 3. E.g., for the case of covers with r branch points and a *total* ordering on the conjugacy classes involved in the branch cycle description, one can assume that the first three branch points are $0, 1$ and ∞. Of course, for an arbitrary set of branch points this transformation cannot be defined over $\mathbb{Q}$. It can be, however, if all the branch points are rational - which in some cases is necessary for a

[2] This condition assures that the Hurwitz space is an absolutely irreducible variety over its field of definition. But even in the case of intransitive braid group action, there may still be an absolutely irreducible component, granted that there is a “rigid” braid orbit, e.g. a unique orbit of a given length.

cover to be defined over $\mathbb{Q}$ - see Lemma 3.3. In those cases, fixing three branch points to 0, 1 and ∞ does not affect the existence of $\mathbb{Q}$-points in the Hurwitz space.

Particularly in the case $r = 4$, $\mathcal{C} := \mathcal{H}^{red}(C)$ is a curve. The existence of Galois covers defined over a field K is therefore directly linked to the existence of K-points on such curves (often called reduced Hurwitz spaces). We also refer to these reduced Hurwitz spaces as Hurwitz curves[3].
If in addition C is a rational class tuple with transitive braid group action on $SNi^{in}(C)$, then the Hurwitz curve is an absolutely irreducible curve defined over $\mathbb{Q}$.
The genus of this curve, called (unsymmetrized) braid orbit genus, can be computed combinatorially (cf. [39, III 5.2.]), as $\mathcal{H}^{red}(C) \to \mathcal{U}^{r-3} = \mathbb{P}^1\mathbb{C}$ is a ramified covering of $\mathbb{P}^1\mathbb{C}$ with monodromy given by the action of the braids $\beta_{i,4}$ $(i = 1, 2, 3)$ on the straight Nielsen class $SNi^{in}(C)$.
Therefore the genus of $\mathcal{C}$ is given by the Riemann-Hurwitz genus formula (cf. Th. 3.8).

In a similar way, a PGL_2-action can be applied for cases with only partially ordered branch point sets (i.e. the case that the conjugacy classes C_i involved in the Nielsen class are not pairwise different):
E.g., if $C = (C_1, C_1, C_2, C_3)$, with C_1, C_2, C_3 pairwise different, consider those covers with partially ordered branch point set of the form $(\{-\sqrt{a}, \sqrt{a}\}$[4] $, 1, \infty)$ with $a \in \mathbb{C} \setminus \{0, 1\}$. As the set S of all such branch point sets is birationally isomorphic to a projective line via $(\{-\sqrt{a}, \sqrt{a}\}, 1, \infty) \mapsto a$, the restriction of the cover $\mathcal{H}^{in}(C) \to \tilde{\mathcal{U}}_4$ to the preimage of S again yields a morphism of curves $\mathcal{C} \to \mathbb{P}^1$.
This time, the fundamental group of the space of partially ordered 4-tuples leads to branch cycles for the cover $\mathcal{C} \to \mathbb{P}^1$, namely the images of the braids $\beta_{1,4}$, β_1 and $\beta_1 \cdot \beta_{1,4}$ (cf. [39, Th. III 7.8]), and again, the genus of $\mathcal{C}$ is given by the Riemann-Hurwitz genus formula.
Also, if $C = (C_1, C_1, C_1, C_2)$, with $C_1 \neq C_2$, consider only those covers with partially ordered branch point set $(\{t_1, t_2, t_3\}, \infty)$, where t_1, t_2, t_3 are the roots of $t^3 + at + a$ for some $a \in \mathbb{C} \setminus \{-\frac{27}{4}, 0\}$[5].

These most important cases for $r = 4$ can be summarized in the following "Braid orbit theorem" (cf. [39, Thms. 7.8 and 7.10], as well as [42, Satz 7.2] for the last of the three cases):

Theorem 2.5 (Braid Orbit Theorem). *Let G be a finite group with trivial center and $C := (C_1, C_2, C_3, C_4)$ be a 4-tuple of non-trivial rational conjugacy classes of G.*

$$\text{Let } (\tilde{\beta}_1, \tilde{\beta}_2, \tilde{\beta}_3) := \begin{cases} (\beta_{1,4}, \beta_{2,4}, \beta_{3,4}) \text{ if } |\{C_1, ...C_4\}| = 4, \\ (\beta_{1,4}, \beta_1, \beta_1\beta_{1,4}) \text{ if } C_1 = C_2 \neq C_3 \\ (\beta_1, \beta_1\beta_{1,4}, \beta_1\beta_2) \text{ if } C_1 = C_2 = C_3 \neq C_4. \end{cases}$$

[3] Not to be confused with the curves with maximal number of automorphisms, called Hurwitz curves in a different context.
[4] i.e. the roots of $t^2 - a$
[5] An explicit computational example with this approach is [22].

Furthermore assume that, under the action of the group $\langle\tilde{\beta}_1, \tilde{\beta}_2, \tilde{\beta}_3\rangle$ on $SNi^{in}(C)$, $B \subseteq SNi^{in}(C)$ is an orbit which is unique of its length and let $\pi(\tilde{\beta}_i) \in Sym(B)$ be the image under this action. If $(\pi(\tilde{\beta}_1), \pi(\tilde{\beta}_2), \pi(\tilde{\beta}_3))$ is a genus zero tuple (in the sense of Th. 3.8) and for some $i \in \{1, 2, 3\}$, one of the cycle lengths of $\pi(\tilde{\beta}_i)$ occurs an odd number of times, then G can be realized regularly as a Galois group over $\mathbb{Q}$.

More generally, one can consider curves on Hurwitz spaces of r-tuples for $r \geq 5$ as well. This has been done by Dettweiler in [12], and will be used for the explicit computations e.g. in Chapter 8. The key idea is to determine the fundamental groups for rational curves in various configuration spaces (such as the spaces of partially ordered tuples $\tilde{\mathcal{U}}_r$), which again are subgroups of the braid group $\mathcal{H}_r$.
The generators of these fundamental groups act via lifting of paths on the fibers of $\mathcal{H}^{in}(C) \longrightarrow \tilde{\mathcal{U}}_r$, and eventually lead to a branch cycle description for a cover $\mathcal{C} \to \mathbb{P}^1\mathbb{C}$, where $\mathcal{C}$ is a curve on $\mathcal{H}^{in}(C)$.

Remark:
Reduced Hurwitz spaces can be introduced more generally than for the cases in Theorem 2.5, by defining PGL_2-equivalence of covers. In many cases (particularly in all the cases that appear in the computations in this work), $\mathbb{Q}$-points on the reduced Hurwitz space $\mathcal{H}^{red}$ automatically yield $\mathbb{Q}$-points in the Hurwitz space $\mathcal{H}^{in}$, and therefore the PGL_2-quotient map, leading from $\mathcal{H}^{in}$ to $\mathcal{H}^{red}$, can be applied w.l.o.g.
However, in general the problem whether rational points on a reduced Hurwitz space lift to rational points on $\mathcal{H}^{in}$ is a subtle one and depends e.g. on the precise structure of the configuration spaces $\tilde{\mathcal{U}}_r$. See [5] for problems and results in the general case.

Chapter 3

Overview: Computation of covers of the projective line

3.1 Preliminaries from group theory and function field theory

In addition to the topological interpretation laid out above, we need some results from the theory of function fields of one variable. These can be found in detail e.g. in [53].

Definition 3.1 (Places of algebraic function fields)**.** Let $F|K$ be an algebraic function field of one variable. A place of $F|K$ is a maximal ideal P of some valuation ring $\mathcal{O}$ of $F|K$.
If $F'|K'$ is a function field extension of $F|K$, and P' is a place of $F'|K'$ such that $P \subseteq P'$, then P' is called an extension of P.

An important special case is the case where $F = K(x)$ (for some transcendental x over K) is a rational function field. In this case, the set of places of $F|K$ can be described in a simple way.

Theorem 3.1 (Places of the rational function field)**.** *Let $K(x)|K$ be the rational function field for some field K, and P be a place of $K(x)|K$. Then P is either of the form $P = P_{p(x)} := \{\frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], p|f \text{ and } p \nmid g\}$ with some irreducible polynomial $p(x) \in K[x]$ or of the form $P = P_\infty := \{\frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], deg(f) < deg(g)\}$.*
Conversely, all of these sets are indeed places of $K(x)|K$.
In the special case that K is an algebraically closed field, one therefore obtains a natural correspondence between places of $K(x)|K$ and points of the projective line $\mathbb{P}^1(K)$.

By the last remark, we can equivalently write $P : x \mapsto \alpha \in K \cup \{\infty\}$ for a place P of the rational function field over an algebraically closed field.

For any function field $F|K$, the group of K-automorphisms of F acts naturally on the set of places of $F|K$. Especially for a rational function field $K(x)|K$, it is well known that $Aut(K(x)|K) \cong PGL_2(K)$, and more precisely every K-automorphism is of the form $\mu : K(x) \to K(x)$, $K(x) \ni f \mapsto \frac{af+b}{cf+d}$, with $ad - bc \neq 0$. (In analogy to the terminology for $Aut(\mathbb{P}^1\mathbb{C})$, we call such an automorphism a Moebius transformation in x.)
As the group of Moebius transformations in x, $PGL_2(K)$, is 3-transitive on $\mathbb{P}^1K$, one can use them to map three given (pairwise distinct) degree one places $P_i := (x - \alpha_i)$ (where $\alpha_i \in K$, $i = 1, ..., 3$) to any three (pairwise distinct) degree one places, w.l.o.g. $P_1 \mapsto (x)$, $P_2 \mapsto (x - 1)$, $P_3 \mapsto (\frac{1}{x})$.

For explicit computations of polynomials with prescribed Galois group, the concepts of inertia groups and decomposition groups are very important.
Let $F'|F$ be a Galois extension of algebraic function fields with Galois group G, and P' an extension to F' of the place P of F.

Definition 3.2 (Inertia group, decomposition group)**.** The subgroup $G_Z(P'|P) := \{\sigma \in G \mid \sigma(P') = P'\}$ is called the decomposition group (Zerlegungsgruppe) of P' over P.
The subgroup $G_T(P'|P) := \{\sigma \in G \mid \nu_{P'}(\sigma z - z) > 0 \text{ for all } z \in \mathcal{O}_{P'}\}$ of the decomposition group is called the inertia group (Trägheitsgruppe) of P' over P.

Some basic and well-known properties of inertia groups and decomposition groups:

Lemma 3.2.

a) The inertia subgroup is a normal subgroup of the decomposition subgroup.

b) For $char(F) = 0$, the inertia subgroup is always cyclic.

c) The inertia groups of places of F' extending a given place of F are conjugate in G.

3.1.1 K-Rationality and rigidity

We now return to the case that the field of constants K is a subfield of $\mathbb{C}$.
In this case, the topological viewpoint outlined in Chapter 2.2 can be united with the algebraic one outlined here (with the help of Riemann surfaces, cf. [55, Chapter 5]).
I.e., if $f : R \to \mathbb{P}^1\mathbb{C} \setminus \{p_1, ..., p_r\}$ is a finite Galois covering and $F'|F := \mathbb{C}(f)$ the corresponding extension of function fields of compact Riemann surfaces, then the group of deck transformations of the cover is isomorphic to $Gal(F'|F)$, such that the conjugacy class of the monodromy image of $\gamma_i \in \pi_1(\mathbb{P}^1\mathbb{C} \setminus \{p_1, ..., p_r\}, p_0)$ can be identified with the unique conjugacy class of inertia group generators of any extension of the place $f \mapsto p_i$ to F'.

A consequence of the identification of algebraic ramification and topological monodromy is that, in the case where the field of constants K is an algebraically closed subfield of $\mathbb{C}$ - and more generally in case that the extension $F'|F$ is regular - it holds that the Galois group $Gal(F'|F)$ is generated by the set of all inertia subgroups. On the other hand, for arbitrary field of constants K, there are some necessary conditions on the ramification to yield a regular extension defined over K, originating from Fried's branch cycle argument:

Lemma 3.3 ((Special case of) Fried's branch cycle argument[1]). *Let $char(K) = 0$ and $L|K(t)$ a finite regular Galois extension of degree n, with Galois group G. For $p \in \mathbb{P}^1\overline{K}$, let $C_p \subset G$ be the class associated to p, i.e. the unique conjugacy class of inertia group generators of places extending the degree-one place $t \mapsto p$ in the extension $\overline{K}L \mid \overline{K}(t)$.*
Let ζ_n be a primitive n-th root of unity, and $\gamma \in Aut(\overline{K}|K)$, $m \in \mathbb{N}$ such that $\gamma^{-1}(\zeta_n) = \zeta_n^m$.
Then the class of inertia group generators associated to $\gamma(p)$ is equal to $(C_p)^m$.
In particular, the set of branch points is invariant under $Aut(\overline{K}|K)$.

Some immediate consequences:

Corollary 3.4. *a) If $K = \mathbb{Q}$ and $p \in \mathbb{P}^1\mathbb{Q}$, then C_p is a rational class, i.e. $C_p = C_p^m$ for all m coprime to the order of the inertia group.*

b) If $K = \mathbb{R}$ and $p \in \mathbb{P}^1\mathbb{R}$, then $C_p = C_p^{-1}$.

Again, let $K \subseteq \mathbb{C}$. If one picks the set of branch points $P = \{p_1, ..., p_r\}$, with $p_i \in \mathbb{P}^1\mathbb{C}$ and a class tuple $C := (C_1, ..., C_r) \subset G^r$ of associated inertia group generators, generating G, so that the restrictions arising from the branch cycle argument are fulfilled for all $\gamma \in Aut(\overline{K}|K)$, then the data (G, P, C) is called a K-rational ramification type. In this case, the Rigidity Criterion (cf. [55, Th. 3.17.]) gives a sufficient condition for a Galois extension with the given ramification data to be defined over K.

Theorem 3.5 (Rigidity Criterion). *Let G be a finite group with trivial center, and (G, P, C) be a K-rational ramification type. If $|SNi^{in}(C)| = 1$, then G occurs regularly as a Galois group over K (with this ramification type).*

Remark: If $l := |SNi^{in}(C)| > 1$, one still has an upper bound for a minimal field of definition $\widehat{K}|K$ of a regular Galois extension with group G and the given ramification type, namely $[\widehat{K} : K] \leq l$.

3.1.2 Genus zero systems

If an intermediate field E of the Galois extension $F|K(t)$ is a rational function field, $E = K(x)$ - which is the case of genus zero tuples that we will deal with for large parts - then the orbits of the inertia subgroups can be easily interpreted in the following way, cf. [44, Lemma 3.1.]:

Lemma 3.6. *Let $K \subseteq \mathbb{C}$, $K(x)|K(t)$ be a degree n extension of rational function fields, $f(X) - t \cdot g(X)$ the minimal polynomial of x over $K(t)$, and F its splitting field. Let $\mathcal{P}$ be a place of F*

[1] cf. [55, Lemma 2.8]

extending the place $t \mapsto \alpha \in K$ of $K(t)$.[2]
If $G \leq S_n$ denotes the Galois group of $F|K(t)$ in its action on the conjugates of x, and the inertia group generator $\sigma \in G$ of $\mathcal{P}$ has cycle lengths $m_1, ..., m_k$, then the specialized polynomial $f(X) - \alpha g(X)$ has roots of multiplicity m_1,..., m_k.[3]

Similarly, one has a natural interpretation of the orbits of the decomposition subgroup (which obviously are unions of orbits of the inertia subgroup):

Lemma 3.7 (Orbits of the decomposition subgroup[4])**.** *In the situation of lemma 3.6, let $G_Z \leq G \leq S_n$ be the decomposition group of $\mathcal{P}$, and assume that G_Z has orbits $O_1, ..., O_r$, each O_i being a union of k_i orbits of $\langle\sigma\rangle$.*
Then $f(X) - \alpha g(X) \in K[X]$ has factors of degree k_i with multiplicity $\frac{|O_i|}{k_i}$.

Proof. As $\langle\sigma\rangle \trianglelefteq G_Z$, the k_i orbits for a given O_i are of the same length. By [39, Ch.I, Th.9.1.], the place $t \mapsto \alpha$ (as a valuation ideal $(t-\alpha)$) splits in $K(x)$ into a product $\prod_{i=1}^r \mathcal{Q}_i^{k_i}$ of places of degrees $\frac{|O_i|}{k_i}$ with multiplicity k_i.
By the classification of places of rational function fields, each $\mathcal{Q}_i$ is of the form $(q_i(x))$ for an irreducible polynomial $q_i \in K[x]$ of degree $\frac{|O_i|}{k_i}$ (here we have excluded the infinite place in x, which can be done w.l.o.g., as in the previous lemma).
Therefore $t - \alpha = (\prod_{i=1}^r q_i(x)^{k_i}) \cdot r$ for some $r \in K(x)$ with denominator coprime to $\prod_{i=1}^r q_i$. But also $t - \alpha = \frac{f(x) - \alpha g(x)}{g(x)}$. This proves the assertion. □

These properties are essential for the explicit computation of polynomials with prescribed ramification type.

Let $K \subseteq \mathbb{C}$ and assume now that $F|K(t)$ is a regular function field extension. If the ramification of $F|K(t)$ is known, then by the well-known Riemann-Hurwitz genus formula (cf. e.g. [53, Theorem 3.4.13] or [45, Chapter 4.1.1.]), the genus of F can be computed:

Theorem 3.8 (Riemann-Hurwitz genus formula)**.** *Let $F|K(t)$ be a regular function field extension of degree n, and let $G \leq S_n$ be the Galois group of the corresponding Galois closure. Let $\sigma_1, ..., \sigma_r$ be the inertia subgroup generators of all the places of $K(t)$ which ramify in F. Then the genus g of F is equal to*

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

where $ind(\sigma_i)$ is defined as n minus the number of cycles of σ_i.

For a transitive group $G \leq S_n$, we therefore call a tuple $(\sigma_1, ..., \sigma_r) \in G^r$ a genus zero system of G if $\sigma_1 \cdots \sigma_r = 1$, $\langle\sigma_1, ..., \sigma_r\rangle = G$ and $0 = -(n-1) + \frac{1}{2}\sum_{i=1}^r ind(\sigma_i)$.

[2] The infinite place $t \mapsto \infty$ is left out in this notation, but can just be obtained via transformation $s := \frac{1}{t}$.

[3] Here of course, one needs to think "projectively": ∞ is a root of multiplicity m if specialization reduces the degree by m.

[4] This is a special case of [39, I, Th.9.1.].

3.2 Computational standard methods

3.2.1 The Groebner basis approach

Let $(\sigma_1, ..., \sigma_r) \in G^r$ be a genus zero tuple of a transitive group $G \leq S_n$. Then, for any choice of branch points $p_1, ..., p_r \in \overline{\mathbb{Q}} \cup \{\infty\}$ Riemann's existence theorem, together with descent arguments, yields the existence of an extension of rational function fields $\overline{\mathbb{Q}}(x) \mid \overline{\mathbb{Q}}(t)$, and therefore the existence of a polynomial equation $f(x) - tg(x) = 0$, with $f, g \in \overline{\mathbb{Q}}[X]$, such that $f(X) - p_i \cdot g(X)$ (or $g(X)$, in case $p_i = \infty$) becomes inseparable with multiplicities determined by the σ_i.
For a genus zero system of length r, this leads to a system of $(r-2)n$ equations in $(r-2)n$ variables over $\overline{\mathbb{Q}}$ in the following way:
The total number of cycles of a genus zero system of length r is $= (r-2)n + 2$ by the Riemann-Hurwitz formula. We get one variable for each cycle, plus one for the leading coefficient of f (g can be assumed to be monic). Using Moebius transformations, we can fix three places of $\overline{\mathbb{Q}}(x)$ (e.g. to (x), $(x-1)$ and $(\frac{1}{x})$) to drop three variables.

The solution set of this system of $(r-2)n$ equations in $(r-2)n$ variables is then a zero-dimensional variety, i.e there will be only finitely many solutions (their exact number can be determined by structure constants). Theoretically, this system can always be solved via Groebner bases, using Buchberger's algorithm.
In practice however, increasing the permutation degree and especially the number of branch points will quickly make the systems very difficult to solve. We will therefore mainly use this approach for genus zero triples[5], i.e. only as a starting point for the computations of families, as outlined in the following sections.

Note that it is often important to reduce the degrees of the equations to obtain practically computable Groebner bases. This can be done by using derivatives, as was first noted in [1] (also cf. e.g. the computations in [39, Chapter I.9]).

In the following, we list a few more methods that are useful to ensure a polynomial for a given ramification type to be defined over as small a field as possible.

Ideally, in the above approach, we would like to fix three given places of $K(x)$, lying over ramified places of $K(t)$ (via Moebius transformations).
Over an algebraically closed base field K, this can be done without problems, as all places of $K(x)$ have degree one.
However, if one wants to obtain covers over small base fields, this direct approach is not always

[5] The Groebner basis method is not without alternative in the case of triples either: Recently powerful approaches using modular functions have been developed, cf. [28].

optimal, because if there are no extensions of ramified places of small degree, a transformation as above would increase the degree of the base field too much.
Instead one can use the following easy observation:

Lemma 3.9. *Let $f, g \in K[X]$ be monic irreducible polynomials of degrees n resp. m over a field K of characteristic not deviding n. For any non-constant $p \in K[X]$, $\deg(p) = k \in \mathbb{N}$, denote by $tr(p)$ the quotient of the coefficient of p at X^{k-1} by the leading coefficient.*
Then there exist $a, b \in K$, $a \neq 0$, such that $tr(f(aX + b)) = 0$ and $tr(g(aX + b)) = 1$, unless $n \cdot tr(g) = m \cdot tr(f)$.

Proof. Straightforward computation yields $b = \frac{-tr(f)}{n}$ and $a = tr(g) - \frac{m}{n} tr(f)$. The latter is $= 0$ if and only if $n \cdot tr(g) = m \cdot tr(f)$. □

We can use this in the following way: Among all extensions of ramified places of $K(t)$ to $K(x)$, choose a place $\mathcal{P} = (f(x))$ of smallest possible degree d (using the action of inertia and decomposition groups as in Lemmas 3.6, 3.7). Let $\alpha \in \overline{K}$ be a root of f and $E := K(\alpha)$. Then one can map $(x - \alpha)$ to $(\frac{1}{x})$ by a Moebius transformation of E (this procedure yields a degree d extension of the base field). After that, by the previous lemma, one can map the traces of the defining polynomials of two places of $E(x)$ to 0 and 1 respectively (unless the exception of the lemma occurs) without further extension of the base field.

In the case of computations of families of covers, as in Chapters 5ff., the field of definition K is an algebraic function field (the function field of a Hurwitz space, e.g. a Hurwitz curve in a suitably reduced case). If there is no ramified place of degree one available in $K(x)$, the above approach, yielding coefficients in a degree-d extension $E|K$, will usually increase the genus. This can on the one hand affect the existence of rational points, which by Theorem 2.3 are essential for Galois realizations, and on the other hand, explicit numerical computations will become more complicated, as the degrees of algebraic dependencies between the coefficients will increase.
One therefore needs to retrieve the actual Hurwitz space. This can be done by using cross ratios.

Definition 3.3. Let $a_1, ..., a_4 \in \mathbb{C} \cup \{\infty\}$ be four different points on the projective line. The cross ratio $[a_1, a_2, a_3, a_4]$ is defined as

$$[a_1, a_2, a_3, a_4] := \frac{(a_1 - a_3)(a_2 - a_4)}{(a_1 - a_4)(a_2 - a_3)}.$$

If one of the a_i is ∞, the factors containing it should cancel each other out, e.g.

$$[a_1, a_2, a_3, \infty] := \frac{(a_1 - a_3)}{(a_2 - a_3)}.$$

Cross ratios have the following obvious, but important properties:

Lemma 3.10. *a) Cross ratios are invariant under Moebius transformations.*

b) Cross ratios are invariant under the action of the Klein four group $V < A_4$ acting via permutation of the components.

This allows us to regain the actual Hurwitz space of a family, by using symmetric functions built out of cross ratios.
As an example, assume that our cover can be defined over a field K and $(f(x))$ is a degree-4 place of $K(x)$ extending some ramified place of $K(t)$. Lacking a place of degree one, we do not actually know f, but only some $\overline{f} \in E[X]$, differing from f by a Moebius transformation, with some extension E of K. However, if $\overline{f} = (X - a_1) \cdot ... \cdot (X - a_4)$ is a factorization over $\overline{K}$, the cross ratios $\lambda_\sigma := [a_{\sigma(1)}, a_{\sigma(2)}, a_{\sigma(3)}, a_4]$ (with $\sigma \in S_3$) are the same as those of f, and because of part b) of the above lemma, the elementary symmetric functions in the λ_σ lie in the field of coefficients of f, i.e. in K.
These elementary symmetric functions are also symmetric functions in the a_i, and can therefore be expressed through the coefficients of $\overline{f}$.

From the point of view of covering spaces, we are considering two actions on the space $\mathcal{U}^4 = \{(a_1, a_2, a_3, a_4) \in (\mathbb{P}^1\overline{K})^4 \mid a_i \neq a_j \text{ for all } 1 \leq i < j \leq 4\}$. The first one is the action of $PGL_2(\overline{K})$, the second one is the natural S_4-action corresponding to the cover $\mathcal{U}^4 \to \mathcal{U}_4$. We are looking for rational functions in the variables $a_1, ..., a_4$ that remain invariant under *both* actions. Firstly, all rational functions in $\lambda := \lambda(a_1, ..., a_4) := [a_1, a_2, a_3, a_4]$ are invariant under the first action, and also under the action of $V_4 < S_4$. Consequently, there is an S_3-cover $J : \mathbb{P}^1 \to \mathbb{P}^1$, $\lambda \mapsto J(\lambda)$, such that $J(\lambda)$ is invariant under both actions. A possible parameterization is given by the well-known j-invariant $J(\lambda) := 2^8 \cdot \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$. (These considerations can be found e.g. in [9, Section 5].)

In particular, for concrete computations involving $\overline{f}$ with $deg(\overline{f}) \leq 4$, the following functions in the coefficients of $\overline{f}$ can be used to retrieve the field K:

Lemma 3.11. *Let E be a field of characteristic zero, and assume always that $\overline{f} \in E[X]$ is a separable monic polynomial.*

a) If $\overline{f} = X^4 - e_1X^3 + e_2X^2 - e_3X + e_4$, with roots $a_1, ..., a_4$ in $\overline{E}$, then $\frac{(3e_1e_3-e_2^2-12e_4)^3}{disc(\overline{f})}$ is an S_3-invariant rational expression in the cross ratios $\lambda_\sigma := [a_{\sigma(1)}, a_{\sigma(2)}, a_{\sigma(3)}, a_4]$, with $\sigma \in S_3$.

b) If $\overline{f} = X^3 - e_1X^2 + e_2X - e_3$, with roots a_1, a_2, a_3 in $\overline{E}$, then $\frac{(e_1^2-3e_2)^3}{disc(\overline{f})}$ is an S_3-invariant rational expression in the cross ratios $\lambda_\sigma := [a_{\sigma(1)}, a_{\sigma(2)}, a_{\sigma(3)}, \infty]$, with $\sigma \in S_3$.

c) If $\overline{f} = X^2 - e_1X + e_2$, with roots a_1 and a_2 in $\overline{E}$, then $\frac{e_1^2}{e_2}$ is a $\langle(1,2)\rangle$-invariant rational expression in the cross ratios $\lambda_\sigma := [a_{\sigma(1)}, a_{\sigma(2)}, 0, \infty]$, with $\sigma \in \langle(1,2)\rangle$.

Proof. a) and b): Straightforward computation, using $J(\lambda)$ as defined above.
c) is designed for calculations involving two degree-2 places over K (one of which is split up into two degree-1 places (0 and ∞) over a quadratic extension E of K). In this case, the S_4-cover $\mathcal{U}^4 \to \mathcal{U}_4$ in the above considerations can be replaced by a $(C_2 \times C_2)$-cover given by the action of $\langle (1,2),(3,4) \rangle < S_4$. Therefore, $\lambda + \lambda^{(1,2)}$ is already invariant under both considered actions. But $\lambda + \lambda^{(1,2)} + 2 = \frac{e_1^2}{e_2}$. □

3.2.2 Hensel lifting

It is often difficult to directly solve large systems of equations over the rationals (or other number fields).
We therefore need results about when (and how) a solution modulo a prime of such a system can be lifted to obtain a rational solution. This can be achieved by more-dimensional versions of Newton approximation resp. Hensel's lemma.
As these techniques play a role in different contexts (e.g. over p-adic numbers or rings of power series), we state a sufficiently general version.

Lemma 3.12 (Newton approximation)**.** *Let K be a complete field under a discrete valuation, with valuation ring $\mathcal{O}$ and maximal ideal $\mathcal{P}$.*
Let $n \in \mathbb{N}$, $f_1, ..., f_n \in \mathcal{O}[x_1, ..., x_n]$ be polynomials in n variables, and $J = \left(\frac{df_i}{dx_j}\right)_{i,j}$ be the corresponding Jacobian matrix. Assume that $a := (a_1, ..., a_n) \in \mathcal{O}^n$ fulfills

$$f_i(a) \in \mathcal{P}, \text{ for all } i \in \{1, ..., n\},$$

and

$$det(J(a)) \notin \mathcal{P}.$$

Then there is $b \in \mathcal{O}^n$, with $b \equiv a \bmod \mathcal{P}$, such that

$$f_i(b) = 0, \text{ for all } i \in \{1, ..., n\}$$

Furthermore, the sequence

$$a_0 := a, \qquad a_{i+1} := a_i - J(a_i)^{-1} \cdot (f_1(a_i), ..., f_n(a_i))^t$$

converges to the solution b.

Proof. Using the fact that the absolute value induced by a discrete valuation is non-archimedean, the proof can be carried out in analogy to one-dimensional versions, e.g. Proposition 7.6. in [31, Chapter XII]. □

In our context, $K = \mathbb{Q}_p$, with the p-adic valuation, is an important case. Under the above assumptions, standard Hensel lifting of a mod-p solution of a system of polynomial equations yields a solution modulo p^k, for arbitrarily large $k \in \mathbb{N}$.
This enables one to compute, from "good" solutions modulo a prime, arbitrarily close p-adic expansions.
Next, the p-adic solutions $a \in \mathbb{Z}_p$ should be recognized as algebraic numbers. Ideally, we would like rational solutions, but this is not always possible, e.g. by the rigidity criteria or the branch cycle argument.
If the cover we are looking for is ramified over only three points, then the solution is zero-dimensional and can directly be obtained by lifting a single mod-p-solution (and, if necessary, look for algebraic dependencies in the p-adic approximation).
For higher-dimensional systems (i.e. with four or more ramification points) we can lift one mod-p-solution to arbitrarily many p-adic solutions by moving the ramification points. E.g., if we have a mod-p-solution $f(t, X) = 0$, ramified in $t = (0, 1, \infty, \chi)$ with $\chi \in \mathbb{F}_p$ we separately lift this to $\mathbb{Z}_p$-solutions ramified in $t \mapsto (0, 1, \infty, \chi + kp)$ with many $k \in \mathbb{Z}$.
This corresponds to collecting many points in the Hurwitz space of the family of covers. After that one can interpolate between these points. This approach has e.g. been used in [35].

3.3 Advanced methods

3.3.1 Deformation of covers via extensions of fields of Laurent series

We now proceed to more advanced techniques for the computation of families of covers.
The goal of this section is to motivate, in a way that allows for explicit algorithms, how to obtain parameterized families $f_\mu(t, X)$ of polynomials describing covers of $\mathbb{P}^1\mathbb{C}$ with r branch points from a degenerate cover $f_0(t, X)$ with $r - 1$ branch points.
An important source for these techniques is Couveigne's paper on the computation of families of genus zero covers ([7]). In this work, the special case a) discussed below is outlined with an S_7-example. Also the general case b) can be extracted from the considerations in Chapter 6 of that paper. The goal of this section is however to make these considerations explicit and applicable for concrete computations of as many families of covers as possible. See also the Magma implementation of case a) given in Chapter 11.

Let $Ni(C)$ be a Nielsen class of genus zero 4-tuples generating a group finite G (assume always $Z(G) = \{1\}$). Recall from Chapter 2 that, if $SNi^{in}(C)$ contains a unique orbit of length n under the action of the braid group, then there is a natural degree-n cover from the corresponding connected component $\mathcal{H}$ of the (inner) Hurwitz space to the space $\tilde{\mathcal{U}}_4$ of partially ordered 4-sets. Proceeding to an appropriate pullback of $\mathcal{H}$, one also obtains a degree-n cover $\mathcal{H}' \to \mathcal{U}^4$, where $\mathcal{H}'$ is birationally equivalent to $\mathcal{C} \times (\mathbb{P}^1\mathbb{C})^3$, and a degree-$n$ cover $\mathcal{C} \to \mathbb{P}^1\mathbb{C}$ of (irreducible projective non-singular) curves.

If, via Moebius transformations, one fixes three of the four branch points of the genus zero covers, say to 0, 1 and ∞, one obtains a family of branched covers $\mathcal{T}_0 \to \mathcal{C} \times \mathbb{P}^1\mathbb{C}$. Let t be a parameter for the projective line on the right side, then this family will have ordered ramification locus in t: $(0, \lambda, 1, \infty)$, where λ is a function on $\mathcal{C}$. As $\mathcal{C}$ is an irreducible curve, its function field is of one variable (and of degree n over $\mathbb{C}(\lambda)$), i.e. equal to $\mathbb{C}(\lambda, \alpha)$ for some function α.

Therefore the family $\mathcal{T}_0 \to \mathcal{C} \times \mathbb{P}^1\mathbb{C}$ can be expressed by a polynomial equation $f(X, \lambda, \alpha, t) = 0$, where $f \in \mathbb{C}(\lambda, \alpha)[t, X]$ is linear in t (because of the genus zero condition).

For every specialization $t \mapsto t_0$ (e.g. to a ramification point), the coefficients of $f(X, \lambda, \alpha, t_0)$ lie in the function field $\mathbb{C}(\lambda, \alpha)$.

To determine these coefficients, embed $\mathbb{C}(\lambda)$ into the Laurent series field $\mathbb{C}((\lambda))$. Then, using the fact that the finite extensions of $\mathbb{C}((\lambda))$ are all equal to some $\mathbb{C}((\mu))$ with $\mu^e = \lambda$, for some $e \in \mathbb{N}$ (cf. [55, Chapter 2.1.3]), all of these coefficients have a Puiseux expansion in λ, i.e. can be written as a Laurent series in $\mu := \lambda^{\frac{1}{e}}$ with some $e \in \mathbb{N}$.

Here the exponent e is nothing but the ramification index in the Hurwitz space of some place lying over $\lambda \mapsto 0$. This ramification index can be determined by group theoretical means: it is the number of equivalence classes of covers, i.e. of equivalence classes of 4-tuples $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ in $SNi^{in}(C)$, that lead to the same degenerate cover, i.e. class triple $(\sigma_1\sigma_2, \sigma_3, \sigma_4)$, upon letting λ converge to zero.

There are two important cases for practical computations:

- If one knows an explicit polynomial for some degenerate (3-point) cover with monodromy $(\sigma_1\sigma_2, \sigma_3, \sigma_4)$ as above, one can determine e and then develop Puiseux expansions to regain a cover with 4 branch points, as described in detail in p. 24ff.
- If one even knows an explicit polynomial for some non-degenerate (4-point) cover of the family (say, ramified in $t \mapsto (0, 1, \infty, a)$ for some $a \in \mathbb{C} \setminus \{0, 1\}$), then by mapping the branch points of the family to $t \mapsto (0, 1, \infty, a + \lambda)$ one can develop from an *unramified* point, i.e. actually obtain Laurent series in λ for the above coefficients. As one starts from a non-ramified point on the Hurwitz space, there is also no concern of getting into the Hurwitz space of a wrong four-point family by deforming, so computations can be done modulo suitable primes (as one doesn't need to double-check the monodromy via numerical methods in $\mathbb{C}$).

Remarks:

- Of course all this remains true for r-tuples with $r \geq 5$ as well. In this case one either has to increase the transcendence degree to get the full Hurwitz space, or work at first only with a curve on the Hurwitz space, by fixing $r-1$ branch points in t (in the unsymmetrized case).
- So far, all considerations were made over $\mathbb{C}$. However, for suitable choice of the conjugacy classes in $Ni(C)$, the corresponding Hurwitz space can be defined over $\mathbb{Q}$. The Puiseux expansion approach may therefore be carried out over an appropriate number field.
- The above condition on the ordered ramification locus in t to be $t \mapsto (0, \lambda, 1, \infty)$ corresponds to the unsymmetrized case; analogously, suitable Moebius transformations lead to different symmetrized cases; e.g. in the C_2-symmetrized case one can w.l.o.g. consider all covers with ordered ramification locus $(\{\text{ zeroes of } t^2-\lambda\}, 1, \infty)$, etc.

From degenerate to non-degenerate covers

We take a closer look at the deformation process leading from a degenerate cover (with $r-1$ branch points) to a non-degenerate one (with r branch points).
We look at two cases. The first one can technically be regarded as a special case of the second one, but as it is often much more comfortable to deal with in practical computations, we outline it separately.

a) First case: $\langle\sigma_1\sigma_2, \sigma_3, ..., \sigma_r\rangle$ is transitive.

The case that the subgroup $G_0 := \langle\sigma_1\sigma_2, \sigma_3, ..., \sigma_r\rangle$ of $G \leq S_n$, associated to a degenerate cover with $r-1$ branch points, is still transitive, is the most comfortable case for explicit computations, at least assuming that the degenerate cover can be computed explicitly.
So for the moment assume that $G_0 \leq G$ is transitive and the inertia group generators have the following cycle structures:

$$(e_{i,1}^{a_{i,1}}, ..., e_{i,k_i}^{a_{i,k_i}}), \quad \text{for the element } \sigma_i \ (i \in \{1, ..., r\})$$

$$(f_1^{b_1}, ..., f_m^{b_m}), \quad \text{for the element } \sigma_1 \cdot \sigma_2$$

(Here $m \in \mathbb{N}$ and $k_i \in \mathbb{N}$ for $i = 1, ..., r$.)

Of course, $(\sigma_1\sigma_2, \sigma_3, ..., \sigma_r)$ is still a genus zero tuple.
By a suitable version of Riemann's existence theorem there is a degree-n extension $\mathbb{C}(x)|\mathbb{C}(t)$ of (rational) function fields, where t and x fulfill an equation $p(x) - tq(x) = 0$ with $p, q \in \mathbb{C}[x]$ such that the following hold:

- $p = p_1^{f_1} \cdot ... \cdot p_m^{f_m}$, with polynomials p_i of degree b_i $(i = 1, ..., m)$.
- $q = q_1^{e_{r,1}} \cdot ... \cdot q_{k_r}^{e_{r,k_r}}$, with polynomials q_i of degree $a_{r,i}$ $(i = 1, ..., k_r)$.
- $p(x) - t_0 q(x)$ is inseparable for exactly $r-3$ further values $t_0 \in \mathbb{C} \setminus \{0\}$, with multiplicities given by the σ_i $(i = 3, .., r-1)$.

(We have therefore w.l.o.g. assumed that the place $t \mapsto 0$ ramifies in $\mathbb{C}(x)|\mathbb{C}(t)$, with inertia group generator $\sigma_1\sigma_2$, and the infinite place of $\mathbb{C}(t)$ ramifies with inertia group generator σ_r).

Now the element $\sigma_1 \cdot \sigma_2 \in G_0$ has exactly $b_1 + ... + b_m$ cycles, and by the Riemann-Hurwitz genus formula, the orbits of the subgroup $\langle \sigma_1, \sigma_2 \rangle \leq G$ are exactly the orbits of $\sigma_1\sigma_2$ (cf. Cor. 3.14). These orbits, on the other hand, correspond one to one (via monodromy action) to the distinct complex roots of $p(x)$. Let $\zeta_1, ..., \zeta_m$ be these roots.

Now assume a genus zero cover branched over r points, with monodromy given by $(\sigma_1, ..., \sigma_r)$, with inertia group generator σ_1 at $T = 0$, σ_2 at $T = \lambda$, σ_r at the infinite place in T, and with $r-3$ further branch points. To study the family $\mathcal{T}_0$ (as on p. 23), view λ as a transcendental. Let $K(X) \mid K(T)$ be the corresponding (genus zero) function field extension, $K \supset \mathbb{C}(\lambda)$ being the function field of the Hurwitz curve, which we are studying locally around $\lambda \mapsto 0$. Thus X and T fulfill a polynomial equation $P(X) - T \cdot Q(X) = 0$.
The analytical interpretation of ramification indices (via Puiseux expansions) shows that the coefficients of P can be developed as Laurent series in $\mu := \lambda^{1/e}$ (where e is the ramification index in the Hurwitz space, at the point corresponding to the above G_0-cover).

More precisely, if ζ_i is a root of the above polynomial $p(x)$ of multiplicity f_i (for $i = 1, ..., m$), then

$$P(X) = \alpha \cdot (X - \zeta_1 + O(\mu^{\frac{e}{f_1}})) \cdot ... \cdot (X - \zeta_m + O(\mu^{\frac{e}{f_m}})),$$

with some leading coefficient α, so that $Q(X)$ can be assumed to be monic w.l.o.g. (It should be clear that factors of the form $(X - \zeta_i + O(\mu^{\frac{e}{f_i}}))$ occur in $P(X)$ for different $O(\mu^{\frac{e}{f_i}})$-terms and also with certain multiplicities, depending on the cycle structures of σ_1 and $\sigma_1\sigma_2$ respectively. We have suppressed these multiplicities here to ease the notation.)

Introduce new coordinates Y_i by setting

$$Y_i := \mu^{-e/f_i} \cdot (X - \zeta_i), \text{ for } i = 1, ..., m \tag{3.1}$$

The reason for this is that, for $\mu \to 0$, these parameter transformations lead to degenerate covers with monodromy $(\sigma_1, \sigma_2, (\sigma_1\sigma_2)^{-1})$, and this monodromy together with the monodromy of the above cover with group G_0 will be sufficient to regain the non-degenerate monodromy $(\sigma_1, ..., \sigma_r)$.

Namely, for the parameter Y_1, we obtain

$$P(X) = \alpha \cdot (\mu^{e/f_1})^{f_1} \cdot \underbrace{(Y_1 + O(1)) \cdot ... \cdot (Y_1 + O(1))}_{f_1 \text{ times}} \cdot (\mu^{e/f_1} Y_1 + (\zeta_1 - \zeta_2)) \cdot ...$$

And therefore for $\mu \to 0$ the function $S := \mu^{-e} T = \mu^{-e} \cdot \frac{P(X)}{Q(X)}$ tends to

$$\tilde{\alpha} \cdot \underbrace{((Y_1 + O(1)) \cdot ... \cdot (Y_1 + O(1)))}_{f_1 \text{ times}}$$

(with $\tilde{\alpha} = \alpha \cdot \frac{(p(x)/(x-\zeta_1)^{f_1})(\zeta_1)}{q(\zeta_1)}$).
The extension $K(X)|K(T)$ is ramified over $T = 0, T = \mu^e$ and $r - 2$ more points $T = a_i$, i.e. over $S = 0$, $S = 1$ and $S = \mu^{-e} \cdot a_i$. For $\mu \to 0$ the points $\mu^{-e} \cdot a_i$ all tend to infinity (as do the Y_1-places extending them!), and one therefore obtains a cover ramified over $S \in \{0, 1, \infty\}$, given by a polynomial $S - \widehat{P}_1(Y_1) = 0$.

Repeating this for all the Y_i $(i = 1, ..., m)$ leads to a reducible cover defined by $(S - \widehat{P}_1(Y)) \cdot ... \cdot (S - \widehat{P}_m(Y)) = 0$. Its monodromy is given, up to simultaneous conjugation in S_n, by $(\sigma_1, \sigma_2, (\sigma_1\sigma_2)^{-1})$, and each irreducible component $S - \widehat{P}_i(Y) = 0$ corresponds to one orbit of the subgroup $\langle \sigma_1, \sigma_2 \rangle \leq S_n$.
These component covers (ramified over three points, with full ramification at infinity!) can usually be easily computed, especially if the orbits are small (i.e. if $\sigma_1\sigma_2$ has many short cycles), which therefore is a desirable situation.

For the explicit computation, it needs to be noted that our assumptions have already determined the leading coefficient of the polynomial $\widehat{P}_i$, and also fixed the infinite place in Y_i to lie over the infinite place in S. PGL_2-action allows for one more degree of freedom, e.g. fixing in addition the place $Y_i \mapsto 0$ over $S \mapsto 0$. However, the resulting transformation is not unique in PGL_2: Multiplication of Y_i with appropriate roots of unity changes neither the leading coefficients nor the places at zero and infinity! This needs to be taken into account to avoid ambiguity (cf. Section 3.3.2), and actually reach the *correct* Hurwitz space via deformation.

b) Second case: $G_0 := \langle \sigma_1\sigma_2, \sigma_3, ..., \sigma_r \rangle$ is intransitive.

Here one first needs to find equations $f_i(x) - t \cdot g_i(x) = 0$ for each orbit of G_0.

For each i choose a parameter x_i and consider $f_i(x_i) - t \cdot g_i(x_i) = 0$.

Similarly, find equations for each orbit of the group $\langle \sigma_1, \sigma_2 \rangle$ (with parameters y_i). The x_i and y_i now need to be related in accordance with the cycle structures in the groups $\langle \sigma_1\sigma_2, \sigma_3, ..., \sigma_r \rangle$ and $\langle \sigma_1, \sigma_2 \rangle$.

This can be done by studying trees of projective lines, as outlined in [7, Section 6]:

To every orbit of G_0 and of $\langle \sigma_1, \sigma_2 \rangle$ there corresponds a genus zero function field (i.e. function field of a projective line) $\mathbb{C}(x_i)$ resp. $\mathbb{C}(y_i)$. Define a graph with the set of these orbits as set of vertices and draw an edge between two orbits if and only if they intersect.

The resulting graph T is obviously connected, with no edges between two orbits of G_0 or two orbits of $\langle \sigma_1, \sigma_2 \rangle$.

It is even a tree as can be deduced from Lemma 3.13: there are no more edges than cycles of $\sigma_1\sigma_2$ (because every such cycle must lie in a non-empty intersection of an orbit of G_0 with one of $\langle \sigma_1, \sigma_2 \rangle$), and by Lemma 3.13, the latter number equals the number of nodes minus 1. Note also that this enforces the number of edges to *equal* the number of cycles of $\sigma_1\sigma_2$, so every non-empty intersection of an orbit of G_0 with one of $\langle \sigma_1, \sigma_2 \rangle$ is given by a *unique* cycle of $\sigma_1\sigma_2$.

Now begin with some orbit O_1 of G_0 and calculate an equation $f_1(x_1) - t \cdot g_1(x_1) = 0$. If $(x_1 - \zeta)$ is some linear factor of f_1 over $\mathbb{C}$ (i.e. $x_1 \mapsto \zeta$ is some place extending the place $t \mapsto 0$) the eventual cover ramified over r points $(0, \mu^e, \infty$ and $r-3$ more), with e the ramification index in the Hurwitz space, will have a linear factor $(x - \zeta + O(\mu^{e/l_\zeta}))$. Here, if we assume e to equal the order of $\sigma_1\sigma_2$ (which can be achieved by replacing μ with some root $\sqrt[k]{\mu}$, if necessary), l_ζ is the multiplicity of $(x_1 - \zeta)$ in f_1, i.e. the length of an appropriate cycle of $\sigma_1\sigma_2$.

Now, inductively assume some equation $f_i(x_i) - t \cdot g_i(x_i) = 0$ for the orbit O_i of G_0 has been computed.

For all neighbors Q_j of O_i in the tree T that haven't yet been computed, let $(x_i - \zeta_j)$ be the linear factor corresponding, via monodromy action, to the cycle of $\sigma_1\sigma_2$ that intersects with the orbit Q_j of $\langle \sigma_1, \sigma_2 \rangle$.

Next, define $y_j := \mu^{-e/l_{\zeta_j}} \cdot (x_i - \zeta_j)$, just as in Case a) and compute an equation in y_j and $s := \mu^{-e} \cdot t$ for the orbit Q_j. This will yield first order approximations for the desired r-point cover, i.e. for a linear factor $(x_i - \zeta_j + O(\mu^{e/l_{\zeta_j}}))$, the $\mu^{e/l_{\zeta_j}}$-term will be obtained.

Now, for each orbit Q_j visited in the previous step, consider the set of neighbors O_k that have not yet been visited.

Again, as Q_j and O_k intersect in a unique cycle of $\sigma_1\sigma_2$, let $(y_i - \eta_k)$ be the corresponding linear factor in the cover for the orbit Q_j (note that this corresponds to a place extending the *infinite* place in s, as this is the place with inertia group generator conjugate to $(\sigma_1\sigma_2)^{-1}$).

Note also that we can always assure that this place in the function field $\mathbb{C}(y_j)$ is *not* the infinite place by choosing the cover for the orbit Q_j such that the place over $s \mapsto \infty$ corresponding to the intersection with the orbit O_i (in the *previous* step) is the infinite place in y_j! This is possible via Moebius transformations.

Now we have almost the same situation as in the previous step (except that we are dealing with places over $s \mapsto \infty$ instead of places over $t \mapsto 0$).

So, define new parameters $x_j := \mu^{-e/l_{\eta_k}} \cdot (y_j - \eta_k)$ (with the appropriate exponents $\frac{e}{l_{\eta_k}}$), and $\frac{1}{\tilde{t}} := \mu^e \cdot \frac{1}{s}$ (i.e. simply $\tilde{t} = t$).

Next, compute the cover $f_k(x_k) - t \cdot g_k(x_k) = 0$, and move on through the tree T.

As this algorithm moves through T on paths, with a well-defined parameter transformation for every edge, the parameters x_i can all be expressed as functions in $x := x_1$ inductively. Also, as T is a tree, each orbit will only be reached via a single path, so there will be no ambiguity in the definition of the x_i.

One thus eventually obtains approximations for a polynomial $f(x) - tg(x)$ of degree $deg(G)$ in x.

To verify that this approach indeed yields the correct degenerate covers for all the orbits, choose a variable x_i and consider the linear factors of $f(x)$ and of $g(x)$ (i.e. the places of the non-degenerate cover extending $t \mapsto 0$ and $t \mapsto \infty$), written as polynomials in x_i. Every such linear factor corresponds to exactly one orbit of G_0, and by the choice of coordinates it is clear that for all orbits in the set of successors of O_i (in the tree T with direction given by the above algorithm), each linear factor of f belonging to such an orbit converges towards the same value as a linear factor of g as μ tends to 0. I.e. these factors cancel each other out. On the other hand, for every orbit of G_0 other than O_i and its successors, all the corresponding roots of f and of g (as polynomials in x_i) tend towards $x_i \mapsto \infty$ as $\mu \to 0$. This leaves only the linear factors belonging to O_i and therefore a degenerate cover with the correct monodromy, for each orbit O_i.

In the same way, expressing $f(x) - tg(x)$ as a polynomial in the variables s (instead of t) and y_j will leave exactly the linear factors of some orbit Q_j of $\langle \sigma_1, \sigma_2 \rangle$ as μ tends to 0. Note especially that the corresponding degenerate cover will be ramified over $s \mapsto 0, 1$ and ∞ by the choice of the coordinate y_j.

Finally, this procedure will yield first order approximations for all the places extending the place $t \mapsto 0$ in the function field of the desired r-pointed cover (and ditto for all the places extending $t \mapsto \mu^e$). Thus, specialize μ to some small complex number and apply Newton iteration to obtain better approximations.

We illustrate this second case with a computational example in Chapter 7. It should be noted that even though this general case is more complicated in terms of explicit implementation, it often cannot be avoided, especially for primitive permutation groups G of larger degree, as it may then be difficult to find a 3-point cover with a transitive subgroup $G_0 \leq G$ to start with.

3.3.2 Some lemmas about families of covers

In this section, we want to take a closer look at the group-theoretic implications of progressing from a degenerate to a non-degenerate cover of a certain monodromy. Let $(\sigma_1, ..., \sigma_r)$ be the monodromy of the desired (non-degenerate) cover. As in the previous section, assume that a degenerate cover with monodromy $(\sigma_1\sigma_2, \sigma_3, ..., \sigma_r)$ is known. Also assume that $(\sigma_1, ..., \sigma_r)$ is a genus zero tuple generating the transitive permutation group $G \leq S_N$.

The first lemma relates the cycles of $\sigma_1\sigma_2$ with the number of orbits of the subgroups G_0 and $\langle\sigma_1, \sigma_2\rangle$ of G, i.e. with the number of components of the degenerate covers with monodromy $(\sigma_1\sigma_2, \sigma_3, ..., \sigma_r)$ and $(\sigma_1, \sigma_2, (\sigma_1\sigma_2)^{-1})$ occurring in the approach outlined in the previous section.

Lemma 3.13. *With the above assumptions, the number of cycles of $\sigma_1\sigma_2$ is equal to $n(\langle\sigma_1, \sigma_2\rangle) + n(G_0) - 1$, where $n(U)$ denotes the number of orbits of a subgroup $U \leq S_N$.*

Proof. As the element $\sigma_1\sigma_2$ is contained in both groups $\langle\sigma_1, \sigma_2\rangle$ and G_0, each of its cycles must be contained in an intersection $O_i \cap Q_j$ of an orbit O_i of G_0 and an orbit Q_j of $\langle\sigma_1, \sigma_2\rangle$. The number of non-empty subsets of $\{1, ..., N\}$ that are of this form must be at least $n(\langle\sigma_1, \sigma_2\rangle) + n(G_0) - 1$, because the graph T introduced in case b) of Section 3.3.1 is obviously connected, with $n(\langle\sigma_1, \sigma_2\rangle) + n(G_0)$ nodes.

The proof of the opposite inequality reduces to a theorem of Ree (in [47]) stating that for any set of permutations $\tau_1, ..., \tau_r \in S_N$ with product 1, the inequality $\sum_{i=1}^{r} ind(\tau_i) \geq 2(N - s)$ holds, with s the number of orbits of the group $\langle\tau_1, ..., \tau_r\rangle$ and $ind(\tau_i) := N$ minus the number of cycles of τ_i.

To prove this statement group-theoretically (as done in [15]), one can obviously look at each orbit individually, and therefore demand w.l.o.g. that $s = 1$. Also, as any k-cycle can be written as a product of $k - 1$ transpositions, and the sum of indices does not change upon replacing it by these transpositions, one can w.l.o.g. assume that all the τ_i are transpositions. Ree's theorem now follows quickly from the observation that a minimal subset of the transpositions $\tau_1, ..., \tau_r$ generating a transitive group must be of cardinality $N - 1$ and the product of these $N - 1$ transpositions will be an N-cycle.

Now apply Ree's theorem to each of the tuples $(\sigma_1, \sigma_2, (\sigma_1\sigma_2)^{-1})$, $(\sigma_1\sigma_2, \sigma_3, ..., \sigma_r)$ and $(\sigma_1, ..., \sigma_r)$, and note that of course the number of cycles of $\sigma_1\sigma_2$ and its inverse are the same.

One obtains $2ind(\sigma_1\sigma_2) + \sum_{i=1}^{r} ind(\sigma_i) \geq 2(2N - n(G_0) - n(\langle\sigma_1, \sigma_2\rangle))$ by adding the first two inequalities, and subtracting the third one then yields $ind(\sigma_1\sigma_2) \geq N + 1 - n(G_0) - n(\langle\sigma_1, \sigma_2\rangle)$.

This proves the opposite inequality. □

Remark: Lemma 3.13 also follows easily via Riemann's existence theorem (interpreting tuples of permutations with product 1 as branch cycles for covers of $\mathbb{P}^1\mathbb{C}$) and application of the Riemann-Hurwitz genus formula for each orbit of the respective groups. In fact, Ree originally proved his theorem in this way.

For sake of simplicity assume from now on that $G_0 := \langle \sigma_1\sigma_2, \sigma_3, ..., \sigma_r \rangle$ is still transitive. This firstly leads to an obvious corollary of the previous lemma:

Corollary 3.14. *In addition to the assumptions of Lemma 3.13, assume that G_0 is still transitive. Then the orbits of $\langle \sigma_1, \sigma_2 \rangle$ are exactly the cycles of $\sigma_1\sigma_2$.*

Next, we look at how many essentially different covers, i.e. how many equivalence classes of tuples $(\tau_1, \tau_2, \sigma_3, ..., \sigma_r)$, (with $\tau_1, \tau_2 \in S_N$, $\tau_1\tau_2 = \sigma_1\sigma_2$ and τ_i of the same cycle type as σ_i) can arise from the given degenerate cover with monodromy $(\sigma_1\sigma_2, \sigma_3, ..., \sigma_r)$. This is clarified by the following lemma.

Lemma 3.15. *Let $G_0 \leq G \leq S_N$ be transitive groups and $\sigma_1, ..., \sigma_r \in G$ be as above.*
Let $O_1, ...O_k$ be the orbits of $\langle \sigma_1, \sigma_2 \rangle$ (i.e. the cycles of $\sigma_1\sigma_2$ in some ordering), and for any $x \in S_N$ fixing the orbit O_k setwise, denote by $x_{|k}$ the image of x in $Sym(O_k)$.
Let $m \in \mathbb{N}$ be the number of equivalence classes of genus zero covers $f : R \to \mathbb{P}^1\mathbb{C}$ with ordered ramification locus $(0, \lambda, p_3, ..., p_r) \in \mathcal{U}^r$,[6] such that the following hold:

- *For $\lambda \to 0$, f converges to a cover with monodromy (simultaneously conjugate to) $(\sigma_1\sigma_2, ..., \sigma_r)$.*
- *For each orbit O_j, the corresponding parameter transformation introduced in (3.1) leads, for $\lambda \to 0$, to a cover with monodromy (simultaneously conjugate to) $(\sigma_{1|j}, \sigma_{2|j}, (\sigma_{1|j} \cdot \sigma_{2|j})^{-1})$.*

Then $m \leq \prod_{|O_j| \geq 3} |O_j|$.

Proof. The monodromy of each such cover is, w.l.o.g. (i.e. after suitably conjugating with some $x \in S_N$) of the form $(\tau_1, \tau_2, \sigma_3, ..., \sigma_r)$, where τ_1 and τ_2 fulfill the following:

- $\tau_1\tau_2 = \sigma_1\sigma_2$,
- τ_i is of the same cycle type as σ_i and fixes all orbits O_j setwise ($i = 1, 2$, $j = 1, ..., k$),
- For each orbit O_j, $(\sigma_{1|j}, \sigma_{2|j}) = (\tau_{1|j}, \tau_{2|j})^x$ for some $x \in Sym(O_j)$.

As $\tau_1\tau_2 = \sigma_1\sigma_2$ is fixed, one has $x \in C_{Sym(O_j)}((\sigma_1\sigma_2)_{|j}) = \langle (\sigma_1\sigma_2)_{|j} \rangle$, as this element is a full cycle.
This leaves only $ord(\sigma_1\sigma_2)_{|j})/|Z(\langle \sigma_{1|j}, \sigma_{2|j} \rangle)|$ different possibilities for $(\tau_{1|j}, \tau_{2|j})$.
If the length of the orbit is ≤ 2, this number is obviously $= 1$, otherwise it is certainly no larger than $|O_j|$.
This proves the assertion. □

[6] Here two covers shall be called equivalent, if their monodromies $(\sigma_1, ...\sigma_r)$ and $(\tau_1, ..., \tau_r)$ differ only by conjugating simultaneously with some $x \in S_N$.

On the other hand, one can determine the number of equivalence classes of covers fulfilling the assumptions of Lemma 3.15 that belong to the desired braid orbit with group G. In fact, this number is just the ramification index of the Hurwitz space cover at the place corresponding to the $(\sigma_1\sigma_2, \sigma_3, ..., \sigma_r)$-cover.

Lemma 3.15 therefore bounds the ambiguity of the result of the deformation process described in Section 3.3.1.

3.3.3 Galois group verification via Hurwitz spaces

There is one more important application of the observation of Lemma 3.15 :
The explicit computation of a Hurwitz space for a family of covers with group G (and prescribed ramification structure) may enable one to confirm the group G as the Galois group of a polynomial f obtained via this Hurwitz space. The computation of the family itself involves a lot of numerical procedures and therefore does not immediately suffice to strictly prove $Gal(f) \cong G$. Of course, for complex approximations, there is always the possibility to check the monodromy numerically, but this also is merely heuristic (unless one makes considerable efforts to obtain constraints for the precision of the numerical calculations (step sizes for Newton iteration etc.) under which one can obtain proven results).

Especially for polynomials with Galois group M_{24} or M_{23}, it is often difficult to prove that the Galois group is actually not the alternating group. This is because the high transitivity of these groups makes them hard to distinguish from the alternating and symmetric groups.
If one has computed polynomial equations for the Hurwitz space, one can of course confirm that the data (genus, ramification indices etc.) fit those predicted by the braid group action, but there could still be a Hurwitz space for, e.g., an A_{24}-family with the same ramification type and the same braid group action. The structure constants in A_{24} will usually be much too large to allow explicit computation of all braid orbits. One can however avoid this, as we illustrate with an M_{24}-example.

A family of polynomials over $\mathbb{Q}(t)$ with Galois group M_{24} and branch cycles of conjugacy classes $(2A, 2A, 2A, 12B)$ was explicitly computed in [43] (previously, a single member of this family was given in [19]). Verification of the Galois group involved numerical approximations to compute the monodromy.
To avoid this, with the universal family explicitly computed, one can plug in values for the parameters that lead to ramified points on the Hurwitz space, i.e. degenerate covers.
E.g. plugging in the value $s = 1$ in the family $f(s, X, t) = (t - A_s(x))^2 + (X^2 + 1)B_s(X)^2$ given in [43] yields a polynomial with an imprimitive Galois group over $\mathbb{Q}(t)$, and parameterizing this genus-0 extension (with inertia group generators of cycle types $(3^8, 2^{12}, 12^2)$) as a composition of two rational functions over $\mathbb{Q}$ makes it easy to retrieve its exact monodromy, without relying on

numerical approximations.[7]

By Lemma 3.15, the number of all covers with ramification of the given cycle type, which degenerate to this 3-point cover is limited. Inertia group generators for all these covers can quickly be computed, by group theoretic means (and in particular, without relying on numerical approximation methods!). Now, apply the braid group to all the A_{24}-generating tuples among these. It suffices to show that this yields a braid orbit that does not correspond with the data computed (as one braid orbit gives rise to one irreducible component of the moduli space of covers), i.e. an orbit that is too long or one where one of the braid group generators, in the action on the orbit, possesses cycles that do not occur in the ramification structure of the already computed Hurwitz space.

3.3.4 Using the braid group action: walking through a Hurwitz space

After computing a complex approximation of one cover with a prescribed ramification type, it is still a difficult computational problem to obtain any results over $\mathbb{Q}$ (or number fields in general).

One way to achieve this is to compute (from this one approximation) complex approximations for covers with all the ramification types in the Nielsen class. This amounts to computing a complete fiber of the reduced Hurwitz space cover, which in the case of four branch points is a branched cover of curves $\mathcal{C} \to \mathbb{P}^1\mathbb{C}$.

This can be done explicitly, using the actions of the braids on Nielsen classes (see (2.1)).

E.g., assume a given cover with ordered branch point set $(p_1, ..., p_r)$ and monodromy $(\sigma_1, ..., \sigma_r)$. Also, assume for simplicity that the disc around $\frac{p_i+p_{i+1}}{2}$ with radius $|\frac{p_i-p_{i+1}}{2}|$ contains no other branch points.

Because of the occurrence of the Hurwitz braid group as a fundamental group of the space $\mathcal{U}_r$, applying the braid β_i ($i \in \{1, ..., r-1\}$) to this cover has a topological interpretation via lifting the corresponding path in $\mathcal{U}_r$ to its preimages in the Hurwitz space. This path may, under the above assumptions for the position of the branch points, be defined by

$$t \mapsto \{p_1, ..., p_{i-1}, p_i, (p_i - c) \cdot e^{\sqrt{-1}\pi t} + c, (p_{i+1} - c) \cdot e^{\sqrt{-1}\pi t} + c, ..., p_r\},\ t \in (0, 1),$$

where $c := \frac{p_i+p_{i+1}}{2}$. In particular it starts in $\{p_1, ..., p_i, p_{i+1}, ..., p_r\}$ and ends in $\{p_1, ..., p_{i+1}, p_i, ..., p_r\}$ (cf. [55, Lemma 10.9] for an affine version).

When a sufficiently close complex approximation for the cover with monodromy $(\sigma_1, ..., \sigma_r)$ is given, one can translate this braid group action into an analytical procedure, by slowly moving the branch points p_i and p_{i+1} (counter-clockwise) along a circle, as above and using Newton iteration to obtain sufficiently close approximations for the new cover with slightly altered ramification locus, until p_i and p_{i+1} have swapped their initial positions.

[7] Note that this degenerate cover corresponds to a place of degree one over one of the ramified points in the Hurwitz space cover, and was also used as a starting point for the calculations in [19]!

This then yields the monodromy action of the braid β_i on the Hurwitz space cover. The result at the end of the path is therefore a complex approximation for a cover with monodromy $(\sigma_1, ..., \sigma_r)^{\beta_i}$.

Computing a complete fiber of a reduced Hurwitz space (or of a connected component of it, in case the braid group acts intransitively) then amounts to finding a sequence of braids which permutes the corresponding straight inner Nielsen class transitively, and successively perform the corresponding braiding "turns".

As this method can take quite some time, especially for long Nielsen classes, it is important to do as few "braiding" turns as possible, and therefore to check group theoretically which monodromies have already been found and which braiding actions will lead to new covers, in order to avoid computing unnecessarily many braiding actions.

Remark:

Practical problems in the computations may occur from the fact that some points in a fiber may be very close (in terms of complex absolute value) to a different Hurwitz space (especially if one computes a family with group $G \notin \{A_n, S_n\}$ and there is a very large Nielsen class with the same ramification cycle types and group A_n or S_n). In these cases almost all points in a fiber may be obtained rather comfortably but a few remain hard to approach because Newton approximation is only possible with very small step sizes. Here it might be possible to symmetrize in a different way: Specialize a given coefficient (occurring in a model of the family of all covers belonging to a given braid orbit, as developed in Section 3.3.1) to a rational number and try to find all the points on the Hurwitz space (of course not all in the same fiber of the original setting) with this specialized value. This requires Newton approximation in various branches of the Hurwitz curve, but this may still be easier than finding the remaining, "badly conditioned" branches.

3.3.5 Finding algebraic dependencies

Assume for simplicity that the reduced Hurwitz space (obtained from $\mathcal{H}^{in}(C)$ via PGL_2-action) for a given family of covers with r branch points can be defined over $\mathbb{Q}$.[8]

As this reduced Hurwitz space is an $(r-3)$-dimensional algebraic variety, its function field has transcendence degree $r-3$. Therefore, any $r-2$ elements of this function field must fulfill a non-trivial algebraic equation over $\mathbb{Q}$. In particular, the coefficients of a model as developed in Section 3.3.1 are such elements. This enables one to obtain explicit equations defining the Hurwitz space over $\mathbb{Q}$.

Again, for sake of simplicity, assume $r = 4$, then the function field extension corresponding to the reduced Hurwitz space cover is of the form $F := \mathbb{Q}(\lambda, \alpha)|\mathbb{Q}(\lambda)$, with a function field F of one variable. The Puiseux expansion approach has embedded F into the Laurent series field $K((\lambda^{1/e}))$ (for a suitable number field K). There are now different ways to obtain dependencies between two coefficients α_1, α_2 of the model. Under certain additional conditions, it will be clear that $\mathbb{Q}(\alpha_1, \alpha_2)$ is

[8] Otherwise one gets the analogous results as in this section, over some number field K.

already the full function field F and therefore the algebraic dependency between α_1 and α_2 is actually a defining equation for the Hurwitz curve. E.g., if the braid group acts primitively on the given Nielsen class, then there is no intermediate field between F and $\mathbb{Q}(\lambda)$, so $\alpha_1 := \lambda$ and α_2 any coefficient not contained in $\mathbb{Q}(\lambda)$ will suffice. This is usually not the best try, as $[F : \mathbb{Q}(\lambda)] = |SNi^{in}(C)|$ is often considerably larger than some other degrees $[F : \mathbb{Q}(\alpha_i)]$ (see the next section for theoretical results on the gonality of F).

The following approaches will be used in the following sections to obtain algebraic dependencies:

- If the coefficients α_i are actually given as Laurent series in $\mu := \lambda^{1/e}$, simply solve a system of linear equations in order to see whether α_1, α_2 fulfill a polynomial equation of degrees n_1, n_2 respectively. As such an equation has $N := (n_1 + 1)(n_2 + 1)$ unknowns, series need to be expanded to precision at least μ^N in order to obtain sufficiently many equations via comparison of coefficients.

  An explicit (and precise!) Laurent series expansion is usually difficult to obtain over $\mathbb{Q}$, as the coefficients grow quite rapidly. Therefore this approach, at least for dependencies of high degrees, can often be only obtained modulo some prime.

- Once the degrees for algebraic dependencies are known (or can be conjectured, e.g. after mod-p reduction), the corresponding systems of linear equations can also be solved numerically for complex approximations, with many different specialized values for λ, instead of one high-order Laurent series in λ.

- Instead of solving approximate complex equations numerically, a mod-p solution can be lifted to many different solutions in $\mathbb{Z}_p$. The algebraic dependencies can then be retrieved via interpolation.

- If the degrees are not too high, algebraic dependencies can be obtained from complex approximations via the LLL-algorithm: suppose that α_1, α_2 fulfill a rational polynomial equation of degrees n_1 and n_2 respectively, specializing α_1 to a rational value will leave α_2 in a number field of degree at most n_2 over $\mathbb{Q}$. With sufficient precision, we managed to retrieve the minimal polynomials for these specialized values of α_2 for degrees n_2 up to 100. Again, repeating this for many (at least $n_1 + 1$) different specializations for α_1 will allow interpolation to retrieve the original equation.

3.3.6 Considerations about the gonality of function fields

Usually the algebraic dependencies $f(a, b) = 0$ will not be ideal with regard to the degrees of the variables a, b involved. One can therefore use considerations about the gonality of the function field $K(a, b)$, involving computations of Riemann-Roch spaces[9], to find good parameters, i.e. rational

[9] See [53, Def. 1.4.4.] for a definition.

function fields with low index in the function field $K(a,b)$.
This is especially useful in function fields of genus 0 or 1, or in hyperelliptic function fields.

Definition 3.4 (Gonality)**.** Let $F|K$ be a function field of one variable. The gonality $gon(F|K)$ of $F|K$ is defined as the minimum of the degree $[F : K(x)]$ (for $x \in F$), i.e. the minimal index of a rational function field in F.

We use the following estimates on the gonality of function fields. The proof (see [27, Lemma 6.6.5]) also yields a method to explicitly find rational function fields $K(x) \subseteq F$ of low index.

Lemma 3.16. *Let g be the genus of the function field $F|K$. Then*

a) If $g = 0$, then $gon(F|K) \leq 2$.

b) If $g \geq 2$, then $gon(F|K) \leq 2g - 2$.

c) If $F|K$ has a prime divisor of degree one, then $gon(F|K) \leq g + 1$.

d) If in addition $g \geq 2$, then $gon(F|K) \leq g$.

See [27, Lemma 6.6.5] for the proof. In each of the cases, the following method produces an element $x \in F$ fulfilling the respective inequality:

- Compute the Riemann-Roch space[10] for a certain divisor a of $F|K$. In cases a) and b) a can be chosen as $-\omega$ resp. ω, where ω is a canonical divisor, in case c) set $a = (g+1) \cdot p$ with a divisor p of degree 1, and in case d) set $a = \omega - (g-2)p$ with a degree-one divisor p and a canonical divisor ω.
- For some non-zero element f of that Riemann-Roch space, compute the divisor $\widehat{a} := a + div(f)$. This divisor will fulfill $\widehat{a} \geq 0$.
- Compute again the Riemann-Roch space of $\widehat{a}$. This space will then contain an element x, fulfilling the respective inequality (actually, in many cases equality can be expected).

Note that the second Riemann-Roch space computation can actually be avoided as there is a natural isomorphism between the Riemann-Roch spaces of linearly equivalent divisors a and $a + div(f)$, given by $x \in \mathcal{L}(a) \mapsto xf^{-1}$, cf. [53, Lemma 1.4.6b)].

[10] The computation of divisors and their Riemann-Roch spaces is implemented e.g. in MAGMA, although for high gonality the computations can be quite complicated, especially in characteristic zero.

Chapter 4

Reality questions for covers of $\mathbb{P}^1\mathbb{C}$

The question when a given Galois extension of $\mathbb{C}(t)$ can be defined over $\mathbb{R}$ can be answered easily by group theoretic means, if the ramification data are known. This has been investigated e.g. by Fried and Debes in [10], and is also summarized in [39, I.10.2]. We first develop the main criteria and then apply them to some cases of Galois theoretic interest.

4.1 Theoretical criteria

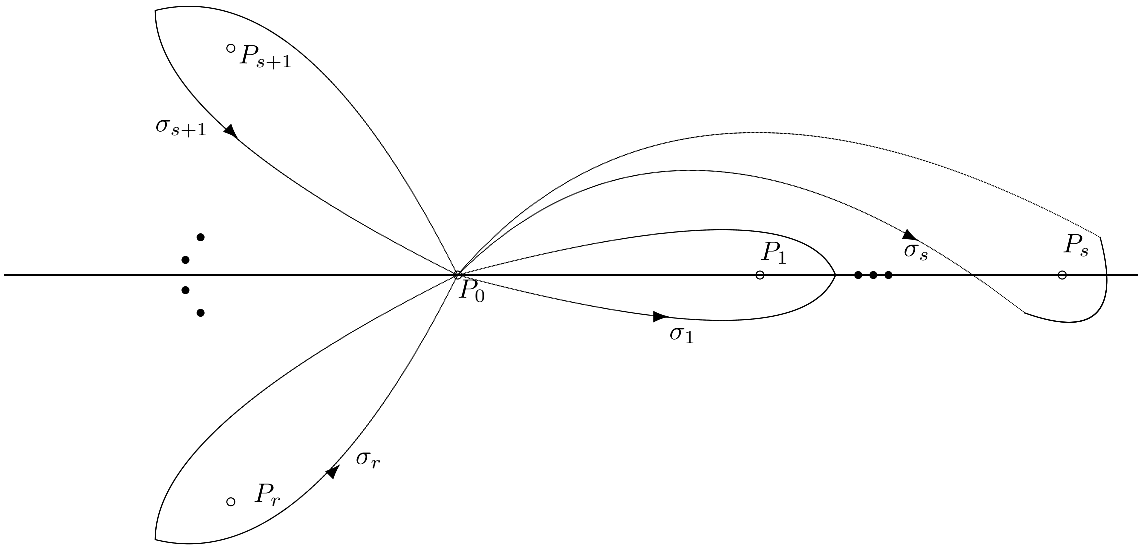
Let $X \to \mathbb{P}^1\mathbb{C}$ be a ramified cover of compact Riemann surfaces, with ramification type $(G, S, (\sigma_1, ...\sigma_r))$ (i.e., $G := Gal(E|\mathbb{C}(t)) = \langle\sigma_1, ...\sigma_r\rangle$, where E is the Galois closure of the function field of X; and $S = \{P_1, ..., P_r\} \subset \mathbb{C}$ is the set of branch points).
Assume that this cover can be defined over $\mathbb{R}$ (which forces S to consist only of real points and pairs of complex conjugate points) and let $P_0 \in \mathbb{R} \setminus S$. Then by [10, Lemma 2.1.], complex conjugation induces an automorphism ρ of the fiber over P_0. More precisely, if one labels the points in the fiber over P_0 by $1, ..., n$, then $\rho \in N_{S_n}(G)$ and for every closed path γ in $\mathbb{P}^1\mathbb{C} \setminus S$, starting and ending in P_0, the following holds:

$$\rho T(\gamma)\rho = T(\overline{\gamma}),$$

where $T(\gamma)$ is the image of γ in S_n, obtained by the action of the fundamental group via lifting of paths.

From this, one obtains an explicit description of the action of ρ on the generators $\sigma_1, ..., \sigma_r$ of G.
To see this, let $\pi_1(\mathbb{P}^1\mathbb{C} \setminus S, P_0)$ be the fundamental group of the punctured line at the base point P_0 and γ_i the homotopy class of closed counter-clockwise paths from P_0 around the branch point P_i (and only this one) $(i = 1, ..., r)$.
Assume the following ordering of the branch point set and the γ_i, cf. Figure 4.1:

Figure 4.1: Example for the choice of branch points and paths in $\mathbb{P}^1 \setminus S$



- $P_1, ..., P_s$ are real, for some $0 \leq s \leq r$.
- P_{s+i} is complex conjugate to $P_{r-(i-1)}$ for $i = 1, ..., \frac{r-s}{2}$.
- $\gamma_1, ..., \gamma_r$ are ordered counter-clockwise in $\mathbb{P}^1\mathbb{C}$.

Then the above action of ρ on G obviously leads to:

$$\sigma_1^\rho = \rho T(\gamma_1)\rho = T(\gamma_1^{-1}) = \sigma_1^{-1},$$

$$\sigma_2^\rho = \rho T(\gamma_2)\rho = T(\gamma_1\gamma_2^{-1}\gamma_1^{-1}) = (\sigma_2^{-1})^{\sigma_1^{-1}},$$

and in general

$$\sigma_i^\rho = (\sigma_i^{-1})^{\sigma_{i-1}^{-1}\cdots\sigma_1^{-1}}, \text{ for all } 1 \leq i \leq s.$$

Similarly, for the paths around the non-real branch points, one simply obtains

$$\sigma_{s+i}^\rho = \sigma_{r-(i-1)}^{-1}, \text{ for all } i = 1, ..., \frac{r-s}{2}.$$

This leads to a necessary condition for a cover to be defined over $\mathbb{R}$ (cf. again [10]):

Lemma 4.1. *Let $X \to \mathbb{P}^1\mathbb{C}$ be a ramified n-fold cover defined over $\mathbb{R}$, with corresponding function field extension $F|\mathbb{R}(t)$, and let E be the Galois closure of F over $\mathbb{R}(t)$. Let $S = \{P_1, ..., P_r\}$ be the set of branch points, $P_0 \in \mathbb{R} \setminus S$, with the position of branch points and ordering of paths around them as above. Let $G := Gal(E\mathbb{C}|\mathbb{C}(t))$ (the geometric monodromy group), and $(\sigma_1, ..., \sigma_r) \in G^r$ the monodromy corresponding to the above choices of branch points.*
Then there is an element $\rho \in Gal(E|\mathbb{R}(t)) \leq N_{S_n}(G)$, acting on the σ_i like complex conjugation on the respective paths in $\mathbb{P}^1$, i.e.

$$(\sigma_1, ..., \sigma_s, \sigma_{s+1}, ...\sigma_r)^\rho = (\sigma_1^{-1}, (\sigma_2^{-1})^{\sigma_1^{-1}}, ..., (\sigma_s^{-1})^{\sigma_{s-1}^{-1}\cdots\sigma_1^{-1}}, \sigma_r^{-1}, ...\sigma_{s+1}^{-1}).$$

Remark:

a) If furthermore $Z(G) = \{1\}$, then the element ρ is uniquely determined by the above conditions.

b) Of course, if the function field extension $E|\mathbb{R}(t)$ is additionally required to be regular, then the condition $\rho \in N_{S_n}(G)$ becomes $\rho \in G$.

Assume from now on $Z(G) = \{1\}$.
The s real ramification points divide $\mathbb{P}^1\mathbb{R}$ into s connected components. Now we move the base point P_0 (and thereby also the paths γ_i corresponding to our monodromy group generators σ_i) continuously along a path δ in $\mathbb{P}^1\mathbb{C} \setminus S$, into the next of those components. So our new paths $\tilde{\gamma_i}$ are homotopic to $\delta^{-1}\gamma_i\delta$.
Of course this yields an isomorphism of fundamental groups, and consequently, via lifting of the path δ, a permutation isomorphism of monodromy groups $\langle\sigma_1, ..., \sigma_r\rangle \to \langle\tilde{\sigma_1}, ..., \tilde{\sigma_r}\rangle$. Namely, number the elements of the fiber above the initial point P_0 from 1 to n, and identify the end points of the n different liftings of δ with the same numbers.
(If for the "transfer" of the monodromy group we choose a different path δ' with the same end points, this identification becomes a different one, but remains unique up to conjugation in G, with the conjugating element being simply the monodromy image of the path ${\delta'}^{-1}\delta$. Therefore $(\sigma_1, ..., \sigma_r) = (\tilde{\sigma_1}, ..., \tilde{\sigma_r})$ modulo action of $Inn(G)$).
However to determine the complex conjugation uniquely (with the conditions of Lemma 4.1), we need only the equivalence class of $(\sigma_1, ..., \sigma_r)$ modulo $Inn(G)$.

So now we get conditions for a complex conjugation in a new component of $\mathbb{P}^1\mathbb{R} \setminus S$.
By repeating this process, we get a unique complex conjugation in each component of $\mathbb{P}^1\mathbb{R} \setminus S$.
After computing a complex conjugation ρ_1 in a first component of the punctured real line, it can easily be described how this conjugation changes after jumping over real ramification points:

Lemma 4.2. *With the notation of Lemma 4.1, assume that complex conjugation for a base point P_0 in the component of $\mathbb{P}^1\mathbb{R} \setminus S$ to the left of P_1 is described by the involution $\tau \in N_{S_n}(G)$, then complex conjugation in the sector left of P_i $(i = 1, ..., s)$ is described by $\tau\sigma_1 \cdots \sigma_{i-1}$.*

Proof. After the translation of the base point described above, in the segment left of P_i $(i = 1, ..., s)$ the paths $\sigma_1, ...\sigma_{i-1}$ lie left of the base point, so complex conjugation ρ in this segment acts on the "real" branch cycles via

$$(\sigma_1, ...\sigma_{i-1})^\rho = ((\sigma_1^{-1})^{\sigma_2 \cdots \sigma_{i-1}}, ..., \sigma_{i-1}^{-1}),$$

$$(\sigma_i, ...\sigma_s)^\rho = (\sigma_i^{-1}, ..., (\sigma_s^{-1})^{\sigma_{s-1}^{-1} \cdots \sigma_i^{-1}}),$$

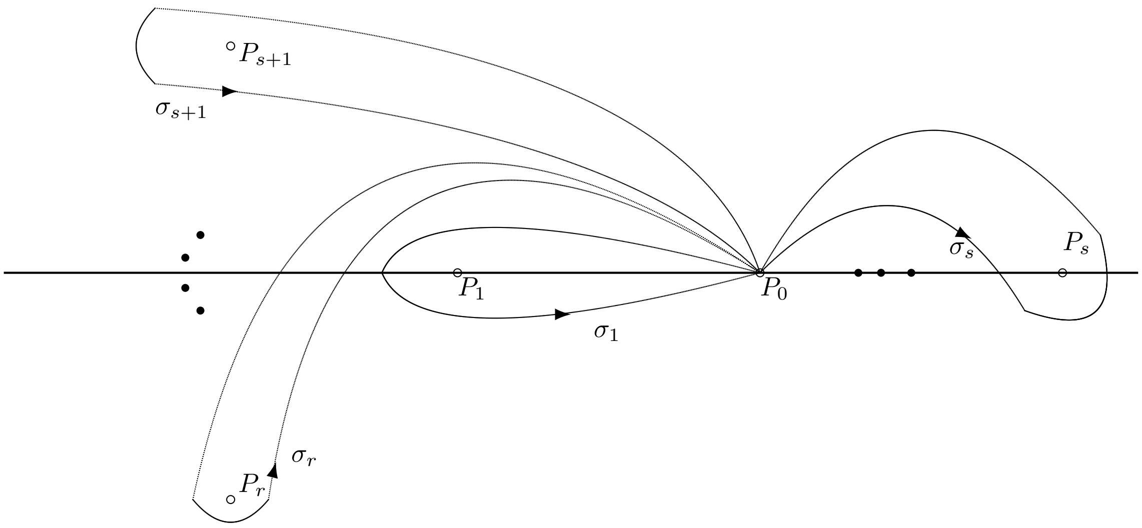
and on every pair (σ_j, σ_k) corresponding to complex conjugate branch points via

$$(\sigma_j, \sigma_k)^\rho = ((\sigma_k^{-1})^{\sigma_1 \cdots \sigma_{i-1}}, (\sigma_j^{-1})^{\sigma_1 \cdots \sigma_{i-1}}).$$

This last action becomes clear if one bears in mind that moving the branch point does not change the (counter-clockwise) sequence of the σ_i, so jumping *over* a real branch point P in the complex plane will bend the path corresponding to a branch point in the *lower* half-plane around P (cf. Fig. 4.2).
Now compare these conditions with the conditions in the initial setting (Lemma 4.1), and because of $Z(G) = 1$ it follows that $\tau\sigma_1 \cdots \sigma_{i-1}$ is the unique element that fulfills these conditions. □

As a converse to the necessary condition of Lemma 4.1, the field E can be defined over $\mathbb{R}$ (and then, for a suitable choice of branch points, even over a real number field!) if and only if such a comlex conjugation exists in one (and then automatically in all!) of the segments of $\mathbb{P}^1\mathbb{R} \setminus S$, see [39, Chapter I, Cor. 10.5].

Figure 4.2: Branch points and paths in $\mathbb{P}^1 \setminus S$ after moving the base point (compare Fig. 4.1)



So far, the action of ρ on the tuple $(\sigma_1, ..., \sigma_r)$ has been described. We now return to the action of ρ on the fiber over the base point P_0, arising from lifting the action on the fundamental group $\pi(\mathbb{P}^1\mathbb{C} \setminus S, P_0)$. This action leads naturally to an action on the residue class field $F_0|\mathbb{R}$ of a given place of $F|\mathbb{R}(t)$ over $t \mapsto P_0 \in \mathbb{R}$.

Lemma 4.3. *For an n-fold ramified covering $X \to \mathbb{P}^1\mathbb{C}$, defined over $\mathbb{R}$, let $F =: \mathbb{R}(t,y)|\mathbb{R}(t)$ be the corresponding function field extension, and let $f(Y) \in \mathbb{R}(t)[Y]$ be the minimal polynomial of a primitive element y of $F|\mathbb{R}(t)$.*
Furthermore, let the ramification data $(G, S, (\sigma_1, ..., \sigma_r))$ be as in Lemma 4.1, and let $\rho \in N_{S_n}(G)$ be the element induced by complex conjugation for a base point $P_0 \in \mathbb{R}$.
Then ρ acts naturally on the zeroes of the specialized polynomial $f_0(Y)$ arising from $t \mapsto P_0$, fixing exactly the real zeroes of f_0.

Proof. The zeroes of f_0 generate the residue class field of a place $\mathcal{P}$ of the Galois closure of F over $t \mapsto P_0$. As the latter place does not ramify, the decomposition group G_Z of $\mathcal{P}$ is equal to $\langle\rho\rangle$, and is mapped canonically onto the Galois group of the residue class field (cf. [53, Th. 3.8.2]).
Furthermore the permutation representation of $\langle\rho\rangle$ on the n zeroes of f can be identified with the action on the zeroes of the reduced polynomial f_0 (cf. [39, Th. I.9.2.]). This proves the assertion. □

As a special case, consider the situation that $(\sigma_1, ...\sigma_r)$ is a genus-zero system in the transitive group G, i.e. $\mathbb{R}(t,y)$ is a function field of genus zero. Over an algebraically closed constant field

that would of course automatically force this field to be a rational function field. However, this is not true for arbitrary fields of constants in characteristic zero (in particular, over the real numbers there are two isomorphy classes of genus zero function fields: the rational one, and the function field of the conic $x^2 + y^2 = -1$, without real points).
So in addition to the question when the Galois closure E can be defined over a real number field k, we want to know whether this fixed field still remains rational over the reals.
If this is the case, we have a realization not only of $G = Gal(E|k(t))$, but also of the point stabilizer G_1, as a Galois group over a real number field (and in some cases over $\mathbb{Q}$).

So we try to see from the cycle structures of the complex conjugations obtained above, whether or not the fixed field of a point stabilizer is still rational over the field of descent.
Elementary analytic considerations yield the following lemma:

Lemma 4.4. *In addition to the assumptions of Lemma 4.3 let $f(Y,t) = p(Y) - tq(Y)$, with polynomials p, q defined over a real number field.*
Then

a) The complex conjugations $\rho_i, ..., \rho_r$ (obtained in the different segments) cannot all be fixed point free.

b) If ρ_i, ρ_{i+1} are the complex conjugations in the segments near the real ramification point t_0, and $f(Y,t_0)$ has exactly m different real roots (including ∞ if specializing reduces the degree), then the sum of the number of fixed points of ρ_i and ρ_{i+1} is $2m$.

Proof. The first assertion follows from the simple observation that a genus zero cover which is rationally defined over a real field automatically has a real point in *some* fiber.
Also, by Lemma 4.3, the sum of the number of fixed points of ρ_i and ρ_{i+1} equals the sum of the number of real roots of $f(Y,t_0+\epsilon)$ and of $f(Y,t_0-\epsilon)$ for sufficiently small $\epsilon > 0$. By a continuity argument, this number is just twice the number of real roots of $f(Y,t_0)$. □

An even more straightforward consequence about rationality in real fields of definition is given by the observation that a non-rational genus zero curve over $\mathbb{R}$ cannot have a real point. In other words, we have a converse to part a) of the above lemma:

Lemma 4.5. *In the setting of Lemma 4.1 assume that $(\sigma_1, ...\sigma_r)$ is a genus-zero system and the involution $\rho \in N_{S_n}(G)$ fulfilling the requirements for complex conjugation has at least one fixed point. Let F be the fixed field in E of a point stabilizer of G. Then $F\mathbb{R}$ is a rational field over $\mathbb{R}$.*

By these observations we have characterizing criteria for rationality over $\mathbb{R}$ (of course one should bear in mind that in many cases rationality over *any* field of definition can immediately be deduced from the genus zero property, by using an oddness argument).

Application to braid group action

An important variant of the above situation deals with the cover $f : \mathcal{C} \to \mathbb{P}^1\mathbb{C}$ of the (reduced) Hurwitz space $\mathcal{C}$ of a family of covers branched over (e.g.) $(0, 1, \lambda, \infty)$ with some $\lambda \in \mathbb{C}$.
Every cover in this family corresponds to a point on $\mathcal{C}$ and the geometric monodromy group H of the Hurwitz space cover is given by the braid group action, so if $\mathcal{C}$ can be defined over a real field (e.g. in the case of a Nielsen class with transitive braid group action and rational conjugacy classes), the symmetric normalizer of H will contain an element σ acting as complex conjugation on a fiber $f^{-1}(P_0)$ of the cover, and therefore on the tuples of the corresponding Nielsen class (for any choice of a base point $P_0 \in \mathbb{R} \setminus \{0, 1\}$).
Still assuming $Z(G) = \{1\}$ (to assure that every K-point of the Hurwitz space leads to a cover defined over K), the fixed points under this action are then the covers in the family that can be defined over a real field.

In this way, instead of just checking definedness over $\mathbb{R}$ for each member of the family individually, one obtains information on how the “real” members are related via the braid group action. Apart from theoretical considerations, this can be important for concrete computations, as the search for rational points can be restricted to certain branches of the Hurwitz space by purely group theoretic arguments. I.e., an algorithmic implementation of the braid group action on covers as described in Section 3.3.4 may be shortened to perform only the “braiding turns” leading to “real” members of the family.

4.2 Application to groups of interest

An example with 3 branch points:

M_{12} has a rational genus-zero class vector $(3A, 3A, 6A)$, where the elements of order 3 have 3 fixed points, and the element of order 6 consists of two cycles of the same length. Computations, e.g. with MAGMA, yield that a cover with these data can be defined over the reals[1], i.e. complex conjugation exists; but not with a rational function field, as the complex conjugation is fixed point free in all sectors.
This last result can also be seen by elementary arguments, considering that M_{12} has only involutions with zero or four fixed points:
We only need to distinguish between a case with only real branch points, and a case with just one real branch point. In the latter case, the real line remains connected, so there is only one complex conjugation ρ, and as the element of order 6 has only two cycles, by Lemma 4.4 b), ρ has at most two fixed points, i.e. zero fixed points, which is also impossible by Lemma 4.4 a).

[1] And even over the rationals, because the group $Aut(M_{12})$ has a rigid rational class vector $(2, 3, 12)$, so by the Hurwitz genus formula, the fixed field of M_{12} in a corresponding regular extension over $\mathbb{Q}(t)$ is still rational, and the ramification above this field is given by the above class vector of M_{12}.

In the case with three real branch points, complex conjugation always maps at least one of the elements of order 3 to its inverse, which of course is not possible without fixed points. So complex conjugation has at least 4 fixed points in all segments, but this again contradicts the fact that the element of order 6 only has two cycles.

Cf. also [45, Section 5.3.4], where the same result is obtained via explicit computation of a polynomial with this ramification type.

Examples for the case with 4 branch points:

For reality questions we only need to distinguish between three different settings:

a) Only real branch points

b) Two real branch points

c) Only pairs of complex conjugate branch points

By the branch cycle argument, complex conjugate branch points over a real constant field must have inertia group generators of the same cycle type.

Consider for example the genus zero class vector $(2A, 2A, 2A, 12B)$ in M_{24}, consisting of three involutions with 8 fixed points, and an element of order 12 with two cycles of the same length. This tuple has enabled the first realization of M_{24} as a Galois group over the rationals, as the ((12)−symmetrized) Hurwitz space is a rational curve. In [19], a polynomial with this ramification type was computed, and it turned out that the fixed point field of the point stabilizer M_{23} was no longer rational over $\mathbb{R}$.
This can also be seen easier (and in particular for *all* 144 equivalence classes of tuples of this type!), using the arguments above. Straightforward computation with Magma shows that, for cases with four as well as for those with two real branch points, several covers are defined over $\mathbb{R}$; but in all those cases, complex conjugation is a fixed point free involution, which excludes rationality of the fixed field in question.

As the above class vector is the only one in M_{24} that both fulfills the genus zero condition and has a rational Hurwitz curve, this result means that M_{23} cannot be realized over $\mathbb{Q}$ with this "point stabilizer" method, unless one finds rational points on Hurwitz curves of higher genus, or on the two-dimensional Hurwitz space of the only genus zero 5-tuple (of cycle type $(4B, 2A, 2A, 2A, 2A)$) in M_{24}, see [33] and the computations in Chapter 5.

In the same way, the genus zero four tuples of cycle structure $(2^4.1^4, 2^4.1^4, 2^4.1^4, 6^2)$ of M_{12} have a Hurwitz space of genus zero (which with some effort can be shown to be a rational curve over $\mathbb{Q}$

- see the table in Appendix A for a polynomial over $\mathbb{Q}$ belonging to this family, i.e. corresponding to a $\mathbb{Q}$-point on this rational curve). However, independently of the choice of the ramification locus, complex conjugation is always a fixed point free involution for the members of this family that are defined over $\mathbb{R}$. Therefore, in the same way as in the previous example, polynomials $f(t, X) \in \mathbb{Q}(t)[X]$ with this ramification type do exist, but not of degree 1 in t. (A theoretical argument for this last tuple is also contained in [45], with the slight restriction that the fiber over the point with (6^2)-ramification consists of real points.)

Results about the Mathieu groups, like the above examples, together with classifications obtained in [45], yield a classification result about monodromy groups of rational functions of a special type. We have included this result in Chapter 9 (Propositions 9.3 and 9.5).

4.2.1 An overview over reality questions with regard to M_{24}-covers

In the following we discuss the genus zero 4- and 5-tuples in M_{24}, with regard to reality questions. We clarify which of them give rise to M_{23}-covers defined over the reals (and therefore may be used to try to realize M_{23} as a Galois group over the rationals).

This is of course also dependent on the exact choice of the branch points (all real, pairwise complex conjugate etc.).

Proposition 4.6.

a) M_{24} has exactly the following generating genus-zero 4-tuples of rational class vectors:[2]

i) $(2A, 2A, 2A, 12B)$, $l = 144$, $g = 0$.

ii) $(2A, 2A, 2B, 8)$, $l = 416$, $g = 11$.

iii) $(2A, 2A, 3A, 4C)$, $l = 248$, $g = 12$.

iv) $(2A, 2A, 3A, 8)$, $l = 1128$, $g = 48$.

v) $(2A, 2A, 3B, 4B)$, $l = 696$, $g = 58$.

vi) $(2A, 2A, 4A, 4B)$, $l = 464$, $g = 36$.

vii) $(2A, 2A, 4B, 5)$, $l = 1970$, $g = 129$.

viii) $(2A, 2A, 4B, 6A)$, $l = 5730$, $g = 432$.

ix) $(2A, 2B, 3A, 4B)$, $l = 684$, $g = 136$.

[2] There are a few non-rational class vectors as well, even with genus zero Hurwitz spaces, but because of the branch cycle argument, these cannot yield realizations over $\mathbb{Q}$ (and in fact not even over $\mathbb{R}$, as the elements in the non-rational classes involved are never conjugate to their inverse).

(Here l always denotes the length of the Nielsen class $SNi^{in}(C)$, and g the genus of the (C_2-symmetrized, if possible) Hurwitz space.)
All these classes give rise to regular Galois extensions of $\mathbb{R}(t)$. The tuples i) and iii) hereby are the only ones that cannot yield a regular extension of $\mathbb{R}(t)$ with the fixed field of M_{23} still a rational function field.

b) M_{24} has exactly one generating genus-zero 5-tuple, namely $(2A, 2A, 2A, 2A, 4B)$. The corresponding Nielsen class has length 72000.

Proof. For the existence, lengths and genera, compute e.g. with Magma (also, cf. [33] for the 5-tuple).
For the statement about real definedness and rationality of the M_{23}-fixed field, apply complex conjugations as laid out earlier in this chapter.
As an example, we discuss the possibilities in detail for the 5-tuple:
Consider the 5-tuple of elements of S_{24}

$$((1,10)(4,17)(5,16)(6,19)(8,12)(11,20)(15,23)(21,24),$$

$$(2,9)(4,24)(6,15)(7,17)(8,18)(13,20)(14,21)(16,23),$$

$$(2,16)(5,12)(7,17)(8,18)(9,23)(10,11)(13,14)(20,21),$$

$$(3,7)(4,24)(5,9)(6,13)(8,22)(12,16)(14,20)(15,21),$$

$$(1,10,20,11)(2,15,13,23)(3,7)(4,17)(6,24,21,19)(8,22,12,9)),$$

generating M_{24}; choosing all branch points real and ordered with the above monodromy, the action of complex conjugation obtained when choosing the base point between the first and the second of these points is given by the identity, i.e. there is a rational function over $\mathbb{R}$ with this monodromy, such that the corresponding cover has real fibers.

Also, if one chooses only one of the five branch points real and the other four pairwise complex conjugate, then there are several possible monodromies of type $(4B, 2A, 2A, 2A, 2A)$ defined rationally over a real field (although real fibers are of course impossible in this case). E.g., among the total of 72000 equivalence classes (modulo simultaneous conjugation) of M_{24}-5-tuples (with product one) of this cycle type, there are $2^3 \cdot 23^2 = 4232$ that lead to a 4-tuple of type $(23A/B, 2A, 2A, 2A)$ when letting the first two branch points converge to the same point. This number arises in the following way: There are 92 equivalence classes of such 4-tuples (in two orbits of the braid group, corresponding to the conjugacy class $23A$ and $23B$ of M_{24} respectively). Each 23-cycle can be split into a product of elements of the classes $4B$ and $2A$ in a total of 46 ways, as the resulting triple $(23, 4B, 2A)$ is an M_{23}-triple with structure constant 2 and can be conjugated by the centralizer of the 23-cycle (which is just the subgroup generated by this cycle) in 23 different ways, each of which leaves the 23-cycle, and therefore the degenerate $(23, 2A, 2A, 2A)$-4-tuple unchanged, but gives rise to a new $(4B, 2A, 2A, 2A, 2A)$-tuple.

Now, computation with MAGMA shows that 4 of the 4232 tuples described above allow a complex conjugation represented by an involution with eight fixed points (when choosing only one of the branch points real, as described above), and therefore give rise to a rationally defined cover over a real field.

On the other hand, for exactly three real branch points, complex conjugation never exists, so there are no covers defined over $\mathbb{R}$ in this case.

Note also that in the cases ii) and iv) above, the cycle structure of the element of order 8 actually shows that over *any* field of definition of these covers, the M_{23}-fixed field is still a rational function field. □

We conclude this chapter by emphasizing that all the genus zero M_{24}-families treated in Chapter 5 have members that can be rationally defined over a real field, and are therefore potential candidates for M_{23}-realizations over $\mathbb{Q}$.

Chapter 5

Computations of Hurwitz spaces for the large Mathieu groups

We now proceed to explicit computation of Hurwitz spaces and covers with prescribed ramification. The large Mathieu groups, mainly M_{24} and M_{23}, are of particular interest for the inverse Galois problem, and thus also for explicit computation.
The main reason is that M_{23} is the only sporadic simple group not yet known to occur as a Galois group over $\mathbb{Q}$ (cf. e.g. [39, Th. II.10.3]). However, M_{24} itself is also of interest. The only known realization of M_{24} over $\mathbb{Q}$ (with a theoretical argument given by Malle and Matzat in [39, Th. III.7.12], and explicit polynomials by Granboulan ([19]) and Müller ([43])) uses a Nielsen class of 4-tuples $(2A, 2A, 2A, 12B)$ in M_{24}. Here the definedness over $\mathbb{Q}$ is guaranteed by the ((1, 2)-symmetrized) Hurwitz curve being a rational genus zero curve; however, as remarked in Chapter 4 this family cannot be used to realize M_{24} as the monodromy group of a rational function over $\mathbb{Q}$ (or even over $\mathbb{R}$). It is therefore still an open question, whether M_{24} is the monodromy group of a rational function over $\mathbb{Q}$, i.e. $M_{24} = Gal(f(X) - tg(X)|\mathbb{Q}(t))$, with $f, g \in \mathbb{Q}[X]$.

Apart from theoretical interest, especially Sections 5.1 and 5.3 show different approaches that should be generally useful to practically tackle problems involving long braid orbits.

5.1 A family of covers ramified over four points with Galois group M_{24}

There are two obvious approaches to realizing M_{23} as a regular Galois group over $\mathbb{Q}$:
One can search for rational points on a Hurwitz space for *any* generating class tuple in M_{23} itself, or for points on a Hurwitz space for a *genus zero* system in M_{24}. In this chapter, we explic-

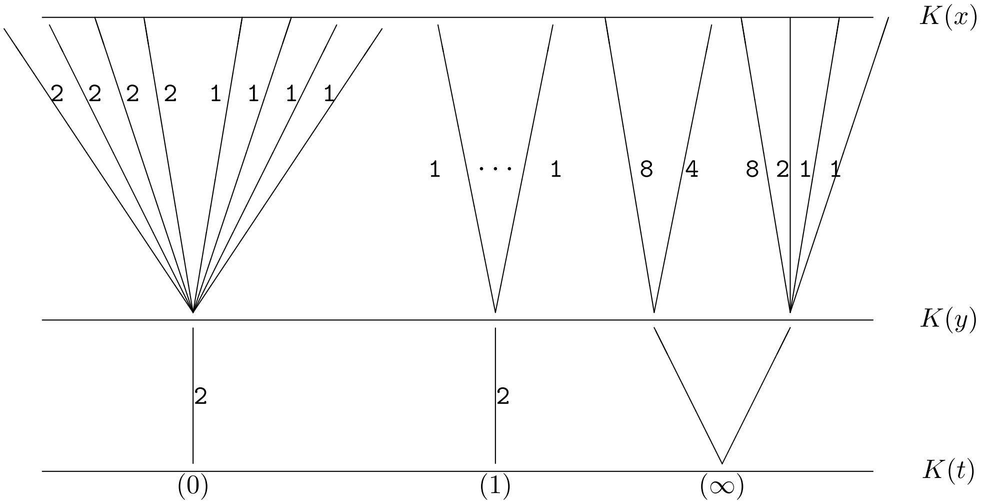
itly compute the Hurwitz space for a family of the second type, i.e. a family of genus-zero covers with Galois group M_{24}, ramified over four places with inertia group generators of cycle types $(2^8.1^8, 2^8.1^8, 2^{12}, 8^2.4.2.1^2)$. During the computation, several methods that may be useful for similar computations are displayed, including complex approximations, p-adic computations, numerical implementation of the action of the Hurwitz braid group etc. Particular interest lies in the question about rational points on Hurwitz spaces, as well as considerations about M_{23}. In Chapter 5.3, we will then give an example of a Hurwitz space for a tuple in M_{23}.

5.1.1 Finding an approximate cover with the desired monodromy via numerical computations

Let $G = M_{24}$, $C_1 = C_2$ the unique conjugacy class of involutions with eight fixed points in G, C_3 the unique class of fixed point free involutions, and C_4 the unique class of elements of cycle type $8^2.4.2.1^2$ in G. Then there are elements $\sigma_i \in C_i$ such that $\langle \sigma_1, ...\sigma_4 \rangle = G$ and $\sigma_1 \cdot ... \cdot \sigma_4 = 1$.
Therefore by Riemann's existence theorem there are degree-24-covers of $\mathbb{P}^1\mathbb{C}$ with Galois group G and monodromy given by the σ_i. Also the Riemann-Hurwitz genus formula shows that these are genus-zero covers, i.e. they can be parameterized by polynomials $f(X) - tg(X)$, with $f, g \in \mathbb{C}[X]$, and $\mathbb{C}(X) \mid \mathbb{C}(t)$ a degree 24 extension of rational function fields.
The exact number of these tuples, modulo simultaneous conjugacy by elements of G, is $l = 416$, with the braid group acting transitively. The action of the braids given in Theorem 2.5 (cf. [39, Theorem III 7.8]) yields that the C_2-symmetrized braid orbit genus is $g_{C_2} = 11$. Therefore the reduced Hurwitz space parameterizing the covers in this Nielsen class is an absolutely irreducible curve $\mathcal{C}$ of genus 11, given through a cover $\mathcal{C} \to \mathbb{P}^1\mathbb{C}$ of degree 416.
We try to compute the covers in this family by first using complex approximations and later identifying certain complex numbers as algebraic numbers. This will eventually lead to an explicit defining equation for the Hurwitz curve over $\mathbb{Q}$.

We start with a cover ramified over three places, with monodromy $(4^4.2^4, 2^{12}, 8^2.4.2.1^2)$. This corresponds to letting the two places with inertia groups $\langle \sigma_1 \rangle$ and $\langle \sigma_2 \rangle$, of cycle structure $2^8.1^8$, converge to one and the same place, thereby obtaining a cover with monodromy $(\sigma_1\sigma_2, \sigma_3, \sigma_4)$.
The class triple is not rigid, therefore we cannot expect to get a cover defined over the rationals, but only over a suitable number field K (in this case of degree 4 over $\mathbb{Q}$). The group generated by $\sigma_1\sigma_2, \sigma_3$ and σ_4 is $Aut(M_{12})$ in an imprimitive action on 24 points, so we obtain an inclusion $K(t) \subset K(y) \subset K(x)$ of rational function fields, with $|K(y) : K(t)| = 2$, $|K(x) : K(y)| = 12$.
Closer examination of the class triple shows that these field extensions will have the structure of ramified places given in Figure 5.1.

Figure 5.1: Ramification structure corresponding to the class triple with group $Aut(M_{12})$



Therefore we are left with computing an ($M_{12}-$) cover ramified over three places, with monodromy $(2^4.1^4, 8.2.1^2, 8.4)$. This can be done easily with the Groebner basis approach. Upon suitable specializations, we get the equation $y = \frac{\alpha \cdot f(x)^2 \cdot g(x)}{x^4}$, where

$f(x) := x^4 + 1/412 \cdot (72 \cdot \zeta^3 - 1733 \cdot \zeta^2 + 15340 \cdot \zeta - 5370) \cdot x^3 + 1/412 \cdot (-419 \cdot \zeta^3 + 10015 \cdot \zeta^2 - 87834 \cdot \zeta + 24358) \cdot x^2 + 1/206 \cdot (1884 \cdot \zeta^3 - 45055 \cdot \zeta^2 + 395560 \cdot \zeta - 84998) \cdot x + 1/206 \cdot (1979 \cdot \zeta^3 - 47323 \cdot \zeta^2 + 415394 \cdot \zeta - 90238)$, $g(x) := x^4 + 1/206 \cdot (68 \cdot \zeta^3 - 1631 \cdot \zeta^2 + 14236 \cdot \zeta - 3870) \cdot x^3 + 1/206 \cdot (-\zeta^3 + 77 \cdot \zeta^2 - 276 \cdot \zeta + 890) \cdot x^2 + 1/103 \cdot (-49 \cdot \zeta^3 + 1095 \cdot \zeta^2 - 9816 \cdot \zeta + 762) \cdot x + \zeta$, and $\alpha := 1/2618256295484181 \cdot (-48201799061 \cdot \zeta^3 + 1146658040179 \cdot \zeta^2 - 9966578857818 \cdot \zeta + 864486650075)$,
with $\zeta \in \overline{\mathbb{Q}}$ a root of the polynomial $X^4 - 24 \cdot X^3 + 212 \cdot X^2 - 64 \cdot X + 4$. The corresponding cover is ramified over $y = 0, 1$ and ∞. Now getting the imprimitive degree-24-cover simply corresponds to suitable concatenation with a degree-2-cover, e.g. $t = \frac{y^2}{4(y-1)}$.

Setting $y = y(x) = \frac{\alpha \cdot f(x)^2 \cdot g(x)}{x^4}$ (as above) in this equation, we get the imprimitive degree 24-cover, ramified over $t = 0, 1$ and ∞, with the prescribed monodromy.
As we will later be interested in polynomials over the rationals, it is suitable to apply some parameter transformation to the variable x, e.g. to choose the two degree-one places over $t \mapsto \infty$, as well as the linear coefficient of the degree-2-polynomial corresponding to the degree-2-place of ramification degree 8 over $t \mapsto \infty$, to be rational. Denote the equation that is finally obtained this way by $\alpha_0 \cdot f_0(x) - t \cdot g_0(x) = 0$, with monic polynomials $f_0, g_0 \in \overline{\mathbb{Q}}[x]$ and a leading coefficient $\alpha_0 \in \overline{\mathbb{Q}}$.

Next we want to use Newton approximation to gain a cover with branch cycle description $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$, ramified at the four places $t \mapsto (-\chi, \chi, 1, \infty)$, where the variable χ will be specialized to some complex number of small absolute value.

Because of the given ramification and the genus zero condition, our cover can be defined by $\alpha \cdot f(X) - tg(X) = 0$, with some $\alpha \in \mathbb{C}$ and monic polynomials f of degree 24 and $g(X) = g_1(X)^8 \cdot g_2(X)^2 \cdot g_3(X)$, the g_i being polynomials of degrees 2, 1 and 2 respectively (we have thus assumed that the place of ramification degree 4 over $t \mapsto \infty$ is $X \mapsto \infty$, which can be done w.l.o.g.). Furthermore, we know $\alpha f(X) - g(X) = \alpha f_1(X)^2$, $\alpha f(X) - \chi g(X) = \alpha f_2(X)^2 f_3(X)$ and $\alpha f(X) + \chi g(X) = \alpha f_4(X)^2 f_5(X)$, where $\deg(f_1) = 12$ and $\deg(f_i) = 8$ for $i = 2, ..., 5$. Upon further suitable transformations (namely fixing $g_2(X) := X$ and mapping the coefficient at X^1 of $g_1(X)$ to -1), we receive a model with 48 unknown coefficients α_i $(i = 1, ..., 48)$, namely:

$$\begin{aligned}
&\alpha_1 := \alpha,\\
&g_1(X) = X^2 - X + \alpha_2,\ g_2(X) = X,\ g_3(X) = X^2 + \alpha_3 X + \alpha_4,\\
&f_1(X) = X^{12} + \alpha_5 X^{11} + ... + \alpha_{16},\\
&f_i(X) = \prod_{j=1}^{8}(X - \alpha_{8\cdot i+j}),\ \text{for } i \in \{2,3,4,5\}.
\end{aligned} \tag{5.1}$$

As the cover will converge to the three pointed cover described above for $\chi \to 0$, we know that the α_i can be expanded as power series in a variable μ, where $\chi = O(\mu^4)$, because our three-point cover corresponds to a ramified place of ramification index 4 in our Hurwitz space, as can easily be verified by counting the tuples $(\tau_1, \tau_2, \sigma_3, \sigma_4) \in C_1 \times ... \times C_4$ with $\tau_1\tau_2 = \sigma_1\sigma_2$. In fact, we can set $\chi = \mu^4$ without restriction.

We then have $\alpha_i = \alpha_i^0 + O(\mu)$ for all the coefficients α_i, where the α_i^0 are the corresponding coefficients from our three-pointed cover given by $\alpha_0 f_0(x) - tg_0(x) = 0$.

Note that, upon viewing χ (and thus also the α_i) as a transcendental over $\mathbb{C}$, the Hurwitz curve cover $\mathcal{C} \to \mathbb{P}^1\mathbb{C}$ corresponds naturally to a degree-416 function field extension $F|\mathbb{C}(\chi^2)$. Also, we know that this function field can be defined over $\mathbb{Q}$, and the transformations that led to our model (5.1) do not affect definedness over $\mathbb{Q}$.

To obtain first order approximations for all the coefficients in our model, especially for $\alpha_{17}, ..., \alpha_{48}$, we need to look at the "opposite" degenerate cover (as described in Chapter 3), i.e. the cover with ramification $(\sigma_1, \sigma_2, \sigma_3\sigma_4)$. This ramification type yields a group generated by two involutions with product of order 4, i.e. a dihedral group D_4, acting intransitively with four orbits of length 4 and four of length 2 (in the latter case the image of D_4 in the action is of course C_2), each orbit corresponding to a connected component of the cover. We can easily compute each of these components separately.

Next, introduce parameter changes to link these small covers to the $Aut(M_{12})$-cover computed above.
To do this, let $\gamma_1, ..., \gamma_8$ be the eight different zeroes of the polynomial $\widehat{f_0}$, from the $Aut(M_{12})$-cover, with multiplicities $e_1 = ... = e_4 = 4$, $e_5 = ... = e_8 = 2$.
Define $X_i := X - \gamma_i$, $Y_i := \mu^{-4/e_i} \cdot \zeta_i \cdot X_i$ $(i = 1, ..., 8)$, with an e_i-th root of unity ζ_i, and $s := \chi^{-1} \cdot t$.
For each of the eight roots γ_i we change the parameters, using the equation

$$\alpha f(X) - tg(X) = \alpha f(\mu^{4/e_i}\zeta_i Y_i + \gamma_i) - \chi \cdot s \cdot g(\mu^{4/e_i}\zeta_i Y_i + \gamma_i) = 0$$

Now the polynomial $f(\mu^{4/e_i}\zeta_i Y_i+\gamma_i)$ contains exactly e_i complex linear factors of the form $\mu^{4/e_i}\zeta_i Y_i + O(\mu^{4/e_i})$, so we get a factor $(\mu^{4/e_i}\zeta_i)^{e_i} = \chi$, i.e.:

$$\alpha \cdot \chi \cdot \tilde{f}(Y_i) = \chi \cdot s \cdot \tilde{g}(Y_i),$$

where $\tilde{f}(Y_i)$ contains exactly e_i linear factors of the form $(Y_i + O(1))$.
Because of the parameter transformation, our covers ramify at $s = (-1, 1, \frac{1}{\chi}, \infty)$, so upon canceling χ and specializing $\mu \mapsto 0$, these covers converge to the D_4- (resp. C_2-) covers we have already computed. This yields approximations for the coefficients $\alpha_{17}, ..., \alpha_{48}$.

So far, we have made use of the concrete monodromy of the degenerate covers, as well as the ramification type (i.e. the cycle structures, but not the concrete cycles!) of the desired 4-point cover. One should note, however, that all these data could still yield an A_{24}-cover instead of an M_{24} one as well. In our case, direct computation shows that only a fraction of 1/12 of the covers with the above degenerations will have group M_{24} (cf. Lemma 3.15).
However, as mentioned in Chapter 3.3.1, we can still choose ζ_i to be *any* e_i-th root of unity in the above definition of Y_i.
This trick will suffice to fix the exact monodromy of the M_{24}-cover: We simply compute the monodromy as described in the next section, compare it with an M_{24}-tuple that we hope to obtain and then, separately for each cycle that doesn't match the one of the expected tuple, we change the corresponding D_4-cover and repeat the process.

Now all the necessary preparations have been made, so one can start Newton iteration for the polynomial of the M_{24}-cover, with the degenerate 3-point cover as a starting point, and a sufficiently small value for μ.
To gain a cover with more stable numerical behaviour we repeat the Newton iteration a couple of times, in order to further separate the branch points associated to σ_1 and σ_2 respectively.
Finally, the following is an approximation for the coefficients $\alpha_1, ..., \alpha_{16}$ (determining completely

the polynomial $\alpha \cdot f(X) - tg(X))$ of a cover ramified over $t \mapsto \pm\frac{1}{2}$, $t \mapsto 1$ and $t \mapsto \infty$ (i.e. $\chi = \frac{1}{2}$ in model (5.1)):

$(\alpha_1, ..., \alpha_{16}) :=$

$(-0.000139596589661251246746906091593298853549781620599747138512307919699334860947260951219563905849455945 0,$

$-0.03571545967419582230359401061692819736320231869763110083591144535530355836823108244865045841702955512,$

$0.07897196113025267795722615735268343894125128234505253622699550571812382661283883493809662805831039497,$

$0.004531397626233030812658624938968081130223833019593614327881729608408838965894082136052935036361098550,$

$-6.51932300946041499810274543272364318085975398247374631237176159436735660797142066399473668524833916 0,$

$8.397456810812136190954124338877854741527149603306115734851055641818546264698533323723367238401941492,$

$83.11720454031705033613552440487845722245046956639385312858569627678514006369554637083620322730605006,$

$1973.125017083273191064614499209091475154005537870820262775621985423127034681155832226337295522622279,$

$501.7466100953769596507361088255424179844448408228653504922929100503740036810807112370826929053997252,$

$78.24829234679345588827277803199627017297562011069747366991165768618749139056922326682835336379783320,$

$0.7749203524856610156495902629394663080544079160899634326639832619224485266078509740784466347010348717,$

$0.5066735303268333795600098272927161757835805649336802364528053194065587076516586605461090488360043702,$

$0.03208458411664660665765254629551493430062150660291330057418576837452781509610397266619349119337545463,$

$0.002872006870513237540872488876896035306272816052374379428909634022552865249592648293352988124849779682,$

$-8.730719315135749723927055206617791157659228149710701070818073007477014095618803775263189989594752493E - 7,$

$6.661416968899303126249771207113264861876341037646897113684360577936394742881922439530283162627008325E - 9).$

5.1.2 Verification of the monodromy

To verify that our cover has the desired monodromy (especially, an M_{24}-monodromy, not an A_{24} one), we choose an unramified specialization $t \mapsto t_0 \in \mathbb{C}$ and identify the 24 zeroes of the specialized polynomial $f(t_0, X)$ with the numbers $1, ..., 24$. Now we move the base point t_0 slowly around each of the ramification points, always associating a zero of the new polynomial to the closest zero of the previous polynomial. After a full turn around a ramification point, we find that the zeroes have been permuted by the inertia group generator σ_i. Of course this numerical approach requires a sufficiently small stepsize. With additional considerations, one could find a stepsize that strictly guarantees the computations to be correct. However, in practical use it may be acceptable to use heuristic evidence at this point.

For the above approximation, we chose $\sqrt{-1}$ as a base point and drew paths around $-\frac{1}{2}, \frac{1}{2}$ and 1 (in this order), obtain the following monodromy:

$$\sigma_1 = (4,14)(6,8)(7,9)(10,12)(16,17)(18,22)(19,21)(20,24),$$

$$\sigma_2 = (1,12)(2,4)(3,9)(5,7)(10,11)(13,17)(14,15)(16,23),$$

$$\sigma_3 = (1,9)(2,13)(3,4)(5,8)(6,7)(10,11)(12,17)(14,15)(16,22)(18,19)(20,21)(23,24),$$

$$\sigma_4 := (\sigma_1 \cdot \sigma_2 \cdot \sigma_3)^{-1} = (1,3,2,16,18,21,24,17)(4,7,8,9,10,12,13,14)(5,6)(19,22,23,20).$$

Indeed, $\langle \sigma_1, ..., \sigma_4 \rangle \cong M_{24}$.

5.1.3 Moving through the Hurwitz space

So far, we have obtained complex approximations of the coefficients of a four point cover. Of course, as the Hurwitz curve is defined over $\mathbb{Q}$, these coefficients will actually be algebraic numbers. However, they should be expected to lie in a large extension of $\mathbb{Q}$ (namely of degree $|SNi^{in}(C)| = 416$ in the generic case), so it is not suitable to approximate the coefficients sufficiently to gain their minimal polynomials. Instead, as outlined in Section 3.3.4, we make use of the transitive action of the braid group on all 416 covers with fixed branch points.

The monodromy group of the degree 416-cover $\mathcal{C} \to \mathbb{P}^1\mathbb{C}$ is a homomorphic image of the stabilizer of $SNi^{in}(C)$ in the braid group $\mathcal{H}_4$, i.e. of $\langle \beta_1, \beta_{1,4} \rangle$ (cf. [39, Th. III. 7.8]). As the braiding action of this group on our 416 class tuples is transitive, we only need to let two generators of the group, e.g. β_1 and β_2^2, act repeatedly to gain covers for each of the class tuples. The action of β_1 corresponds to interchanging the branch points $p_1 := -\frac{1}{2}$ and $p_2 := \frac{1}{2}$ (with inertia group generators in the class C_1) by moving them slowly counterclockwise (and again using Newton iteration), say along a circle around 0 in the complex plane, until they have switched places (meanwhile the other branchpoints are left unchanged). We can keep track of which braid yet needs to be applied to which cover by keeping a list of the class tuples that have already been reached (always verifying the monodromy of a newly reached cover numerically as described above).

This way, we obtained complex approximations for a complete set of 416 covers for a fixed choice of branch points, i.e. a complete fiber of the Hurwitz curve cover $\mathcal{C} \to \mathbb{P}^1\mathbb{C}$. These approximations are included in the file "`m24_(2,2,2,8)_approx.txt`".

5.1.4 From numerical approximations to algebraic numbers via symmetric functions

Now, with a complete fiber computed, we can proceed from complex approximations to algebraic numbers:

Proposition 5.1. *Let α be any of the coefficients $\alpha_1, ..., \alpha_{16}$ of the model (5.1), let $\chi \in \mathbb{C}$ such that $\chi^2 \in \mathbb{Q}$, and let $a_1, ..., a_{416}$ be all the possible values of α for the (partially ordered) branch point set $(\{\pm\chi\}, 1, \infty)$.*
Then the polynomial $\prod_{i=1}^{416}(X - a_i)$ has rational coefficients.

Proof. With our assignment of the (partially ordered) branch point set to $(\{-\chi, \chi\}, 1, \infty)$, viewing χ as a transcendental, we obtain a function field extension $F|\mathbb{C}(\chi^2)$ for the morphism $\mathcal{C} \to \mathbb{P}^1$ of the Hurwitz curve $\mathcal{C}$. Because of the "good" choice of the model for the universal family, this function field is actually defined over $\mathbb{Q}$, and we refer to the function field over $\mathbb{Q}$ as F again. Clearly, for $\alpha \in \{\alpha_1, ..., \alpha_{16}\}$, the field $\mathbb{Q}(\chi^2, \alpha)$ is an intermediate field of the extension $F|\mathbb{Q}(\chi^2)$, as these α are coefficients of specializations $t \mapsto t_0 \in \mathbb{P}^1\mathbb{Q}$ of our universal family. The primitive braid group action shows that $F|\mathbb{Q}(\chi^2)$ has no proper intermediate fields, therefore $\mathbb{Q}(\chi^2, \alpha) = F$ or $\alpha \in \mathbb{Q}(\chi^2)$. In the first case, if f is the minimal polynomial of α over $\mathbb{Q}(\chi^2)$, the a_i are exactly the roots of the reduced polynomial $f_0 \in \mathbb{Q}[X]$, specializing χ^2 to a rational value. In the second case, all the a_i would even be rational. □

These rational coefficients can now be obtained from our complex approximations with well-known algorithms. We therefore obtain polynomials in our family which are defined over a number field (of degree 416 over $\mathbb{Q}$) - although with rather huge coefficients.

5.1.5 Reduction modulo a prime

We now look for a prime p such that the polynomials of degree 416 obtained in the previous step for several coefficients all have a root in $\mathbb{F}_p$. (In fact, we expect the function field of the Hurwitz space to be generated by just two of these coefficients, i.e. two of these polynomials having a root would be enough to enforce the other polynomials to have a root as well.) In our case, the choice $p = 17$ leads to the following polynomial:

$0 = f(t, X) := (X^{12} + X^{11} + 2 \cdot X^9 + 11 \cdot X^8 + 9 \cdot X^7 + 4 \cdot X^6 + 15 \cdot X^5 + 14 \cdot X^4 + 15 \cdot X^3 + 2 \cdot X + 15)^2 - t \cdot (X^2 + 16 \cdot X + 10)^8 \cdot (X + 11)^2 \cdot (X^2 + 4 \cdot X + 11)$,
ramified over $t \mapsto (0, 2, 6, \infty)$, with the correct cycle types of inertia subgroups.

Dedekind's criterion

To gain further evidence that we have actually obtained a regular M_{24}-Galois extension over $\mathbb{F}_{17}(t)$, we use Dedekind reduction.
As we have obtained a mod-17 reduced polynomial $f(t, X)$, any value $t \mapsto t_0 \in \overline{\mathbb{F}_{17}}$ that leaves the specialized polynomial separable leads to a cycle type contained in $Gal(f|\mathbb{F}_{17}(t))$ by Dedekind's criterion (cf. e.g. [39, Th. I.9.2]; note especially that specializing t cannot reduce the degree of f). For specializations in suitably large extensions of $\mathbb{F}_{17}$, the occurring cycle types are exactly the ones contained in M_{24}. Furthermore, by a function field version of Chebotarev's density theorem, every

cycle type of $Gal(f|\mathbb{F}_{17}(t))$ will occur with positive density. This yields strong evidence (although not strict proof) that $Gal(f|\mathbb{F}_{17}(t))$ is in fact M_{24} (and not A_{24}).
(If one wishes to obtain a strict proof, combining these arguments with estimates from the Hasse-Weil bound - as done in [14] to distinguish M_{23} from A_{23} - might succeed, after choosing a sufficiently large prime for the reduction, instead of a small one as done above.)

5.1.6 Finding algebraic relations between two coefficients of the family

Next, we can lift our $\mathbb{F}_p$-cover, ramified over $(0, 2, 6, \infty)$ to arbitrarily many $\mathbb{Q}_p$-covers ramified over $(0, 2-kp, 6+kp, \infty)$, with $k \in \mathbb{Z}$, via Hensel lifting. After obtaining several hundreds of such covers we can find algebraic relations between two of the coefficients. These relations will be over the p-adic integers, but with appropriate assumptions we know that they are in fact over the rationals. Therefore we can easily obtain the fitting rational numbers from the p-adic ones.

In our case, we obtained a polynomial relation of degrees 32 and 24 respectively, between the coefficients α_2 and α_3 (as in the model (5.1)). This is an absolutely irreducible polynomial giving rise to a curve of genus 11, which is the genus of the Hurwitz curve. We therefore expect this to already be a defining equation for (the affine part of) the Hurwitz curve as a plane curve. This can be verified, as the remaining coefficients can be expressed as rational functions in these two coefficients.

The precise polynomial in two variables, defining the Hurwitz curve, is given, in the form $h(t, x)$ in the appendix.

Theorem 5.2. *The polynomial $h(t, x) \in \mathbb{Q}[t, x]$ describes an absolutely irreducible curve of genus 11, which is the C_2-symmetrized Hurwitz curve of the M_{24}-family considered in this chapter.*

Proof. Via Magma, the absolute irreducibility can easily be checked, e.g. for smaller models of the mod-47 reduction of this curve, as given below on p. 59. Therefore the original curve is also absolutely irreducible. Furthermore it can be checked that the reduction modulo 47 of this curve has genus 11 (via computations of suitable divisors, as described above). Therefore the original curve has genus no less than 11. Monodromy calculations show that some point on this curve (and therefore, by irreducibility, the entire curve) gives rise to M_{24}-polynomials, with the desired ramification type. It also follows that the function field $\mathbb{Q}(t, x)$ described by this curve is already the full function field of the Hurwitz curve (and no proper subfield), as the full function field has genus 11 by the braid genus formulas, and therefore by Riemann-Hurwitz, any proper subfield would have strictly lower genus. □

5.1.7 An explicit polynomial equation for the degree-416 cover $\mathcal{C} \to \mathbb{P}^1$

The polynomial $h(t, x)$ is somewhat arbitrary in the sense that it yields function field extensions with many ramification points. We know however from the action of the braid group that the

function field F of the Hurwitz curve $\mathcal{C}$ has a rational subfield $E = \mathbb{Q}(\chi^2)$ of index 416 such that only three places (all of degree one) ramify in the extension $F|E$.
In order to compute a polynomial for this extension, we started from the complete fiber of 416 covers for a given choice of branch points and for all of them started to move the branch points. For each full fiber, we obtained a degree 416 minimal polynomial for the coefficient α_2 (as in model (5.1)) . We know already that $\mathbb{Q}(\alpha_2)$ has index 24 in the function field F , so after gaining sufficiently many full fibers, we can interpolate the coefficients of the degree 416 polynomials to obtain a polynomial in two variables, of degrees 24 and 416 respectively, describing the function field extension $F|E$. We have included this polynomial in the file "`deg416_hurwitz_equation.txt`". One can check the ramification data to coincide with those predicted by the braid group actions.

5.1.8 Totally real specializations

For some members of the family, criteria for complex conjugation show, that if all branch points are chosen real, then specializing t in the interval between the point with inertia group generator of cycle structure (2^{12}) and the closest $(2^8.1^8)$-point yields totally real polynomials (not necessarily over $\mathbb{Q}$ of course) for M_{24} (and then also for M_{23}) over some real number field K, i.e. the splitting field over K of these polynomials is a real field. This completely group theoretic argument can now be verified by picking an approximate polynomial with the correct monodromy.
In the list of approximations for all 416 covers with branch point set $t \mapsto (\{-1/2, 1/2\}, 1, \infty)$, given in the file "`m24_(2,2,2,8)_approx.txt`", the covers no. 296, 300, 302, 361, 411, 412, 415 and 416 have real fibers, each in the real interval $t \in (1/2, 1)$.

5.1.9 Alternative approaches

The above computations could possibly be shortened by trying to find algebraic dependencies between the complex approximations of coefficients right away, using some form of least squares algorithm, i.e. solving numerically certain systems of equations, and then finding the rational numbers corresponding to the complex solution of Least Squares. However, it still seems interesting to use the action of the braid group to proceed from complex approximations to precise rational or p-adic numbers.
Another possibility to avoid computing the full braid group orbit would be to compute (via Newton iteration) a cover with, e.g. the coefficient α_2 from model (5.1) rational, and then hope that this will lead to the other coefficients lying in more or less small extensions of $\mathbb{Q}$ (in our case, we know in retrospect that specializing α_2 to a rational number would lead to the remaining coefficients $\alpha_1, ..., \alpha_{16}$ lying in an extension of degree (at most) 24. The minimal polynomials of such algebraic numbers can be regained if one uses complex approximations of precision a few thousand digits).
Still, it can be important to have computed a full fiber, particularly for the search for rational points.

5.1.10 Open questions: Points on curves and M_{23}

It would be very interesting to know if the Hurwitz curve given by $h(t, x) = 0$ has a (non-singular) rational point. This could then imply that there is a cover with the above monodromy over the rationals.

However, one would still need to double-check after finding such a point. The important thing is to obtain an unramified place in the actual Hurwitz curve cover of degree 416. The function fields generated by our curve and the degree 416 cover are the same, but of course the ramification is different, therefore a non-singular point in our model could still give a singularity in the other model, and vice versa. This emphasizes the importance of the explicit equation for the degree-416 cover. (We refer to Chapter 5.3 for numerical arguments that may be used in the case that the "natural" ($|SNi^{in}(C)|$-fold, in the case of transitive braid group action) Hurwitz space cover $\mathcal{C} \to \mathbb{P}^1$ is too large to be parameterized explicitly.)

There are a few singular points on our curve (see Th. 5.3), but plugging the values into the original model always leads to some vanishing of discriminants amongst the coefficients, so these points will not lead to rational M_{24}-covers.

Note that the existence of "good" points would not only give rise to a new M_{24}-realization over $\mathbb{Q}$, but as our ramification type is of genus zero, with a place of degree 1 (e.g. over the infinite place of the base field), the fixed field of a point stabilizer would still be a rational function field. Therefore one would obtain a regular realization of M_{23} over the rationals. As mentioned before, it is still open whether such an extension exists or not. In fact, the family computed here gives rise to the Hurwitz curve with the smallest genus among all the four-point genus zero families of M_{24} with members that can be rationally defined over a real field, cf. Prop. 4.6.
Searching for rational points on the Hurwitz curve, we combined several mod-p reductions of the polynomial h for small primes p (as the direct search for rational zeroes over $\mathbb{Q}$ is quite time-consuming). E.g., whenever $t_0 \in \mathbb{Q}$ has denominator not divisible by p, and mod-p reduction of $h(t_0, x)$ neither decreases its degree nor leads to any zeroes modulo p, there cannot be any rational zeroes with t-coordinate t_0 either.
We checked all rational values with numerator and denominator of absolute value $\leq 5 \cdot 10^4$, and all integer values of absolute value $\leq 10^8$ (in t as well as in x; note also that for rational specializations $t \mapsto t_0$, $h(t_0, x)$ has *real* roots if and only if $t \in (-\infty, \frac{1}{4}]$. This can be verified easily as the number of real roots of $h(t_0, x)$ can only change at a real branch point.).
At least the following holds:

Theorem 5.3. *Every rational solution of $h(t, x) = 0$ (with h as given in the appendix), with $t \in \mathbb{Q} \setminus \{0, \frac{1}{4}\}$ yields a regular Galois realization of M_{24} and of M_{23} over $\mathbb{Q}$.*

Proof. The only rational solutions that do not yield such realizations are the ones that correspond to ramified points of the degree 416 Hurwitz curve cover $\mathcal{C} \to \mathbb{P}^1$. Given the explicit polynomial equation for this degree 416 cover, it only remains to compute the fibers over $-\chi^2 \mapsto 0$,$-\chi^2 \mapsto -1$ and $-\chi^2 \mapsto \infty$. It turns out that the only rational values in these fibers are for $t = 0$ and $t = \frac{1}{4}$. □

The curve $\mathcal{C}$ does have a non-singular point modulo all small primes (apart from the few cases where the defining polynomial becomes reducible). In fact, the polynomial $h(t, x)$ given in the appendix below remains irreducible as a polynomial in x for all odd primes. Finding non-singular points modulo p, for small primes p, then automatically yields $\mathbb{Q}_p$-points.

By the Hasse-Weil bound (see e.g. [53, Th. 5.2.3.]) this means that there are non-singular points for *all* primes for which the reduction remains irreducible.

Namely, by Hasse-Weil, the number N of degree one places in the mod-p reduced function field fulfills $|N - (p+1)| \leq 2g\sqrt{p}$, and it is known that the genus g of the mod-p reduced function field is never larger then the original genus (cf. [13] or [40] for this statement) - granted that the reduction is still a function field, of course - so we can estimate $|N - (p + 1)| \leq 22\sqrt{p}$, which yields $N > 0$ for all $p \geq 23$.

This leaves the case $p = 2$. Here, the equation $h(t, x) = 0$ does not have good reduction, and indeed, it does not seem obvious whether there are 2-adic points at all, apart from the singular $\mathbb{Q}$-points (see above).

We therefore end this section with a question:
Question: Is the set $\mathcal{C}(\mathbb{Q}_2)$ of non-singular 2-adic points of this curve empty?

5.1.11 Number field and mod-p results

To generalize the question about rational points, one might look for points over small number fields. The degrees of the defining polynomial of $\mathcal{C}$ are 24 and 32 respectively. Also, by Lemma 3.16, the gonality of the function field F of $\mathcal{C}$ is at most 20. Explicitly computing an element y such that $|F : \mathbb{Q}(y)| \leq 20$ (via Riemann-Roch spaces, as described immediately after Lemma 3.16) seems to be too difficult for current programs.

However, we have been able to compute smaller models for mod-p reductions of $\mathcal{C}$. E.g. for $p = 47$ (the choice of this prime is motivated by the proof of the following proposition), using the fact that $\mathcal{C}$ has an $\mathbb{F}_p$ point, one can compute models $\widehat{f}(t, x)$ for $\mathcal{C}$ of degrees 12 and 11 respectively (again cf. Lemma 3.16).

One such model over $\mathbb{F}_{47}$ is
$\widehat{f}(t,x) = (x^{11}+33x^{10}+27x^9+32x^8+6x^7+28x^6+5x^5+3x^4+43x^3+39x^2+18x+4)t^{12}+(36x^{11}+27x^{10}+4x^9+39x^8+8x^7+9x^6+42x^5+43x^4+23x^3+30x^2+39x+27)t^{11}+(12x^{11}+5x^{10}+23x^9+25x^8+25x^7+27x^6+14x^5+8x^4+36x^3+7x^2+43x+38)t^{10}+(2x^{11}+42x^{10}+12x^9+20x^8+30x^7+11x^6+21x^5+26x^4+42x^3+6x^2+15x+36)t^9+(41x^{11}+5x^{10}+11x^9+39x^8+43x^7+4x^6+38x^5+x^4+5x^3+25x^2+27x+25)t^8+(12x^{11}+15x^{10}+46x^9+29x^8+4x^7+8x^6+32x^5+21x^4+14x^3+26x^2+24x+46)t^7+(42x^{11}+7x^{10}+27x^9+2x^8+12x^7+41x^6+20x^5+11x^4+16x^3+16x^2+26x+39)t^6+(32x^{11}+43x^{10}+x^9+7x^8+7x^7+39x^6+46x^5+7x^4+22x^3+12x^2+26x+23)t^5+(4x^{11}+33x^{10}+26x^9+22x^8+32x^7+36x^6+15x^5+24x^4+11x^3+12x^2+8x+18)t^4+(7x^{11}+15x^{10}+30x^9+42x^8+38x^7+27x^6+21x^5+31x^4+5x^3+33x^2+44x+28)t^3+(30x^{11}+29x^{10}+8x^9+19x^8+x^7+36x^6+39x^5+28x^4+8x^3+37x^2+10x+20)t^2+(3x^{11}+11x^{10}+7x^9+30x^8+45x^7+33x^6+22x^5+27x^4+x^3+19x^2+6x+17)t+12x^{10}+43x^9+7x^8+45x^7+37x^6+36x^5+19x^4+15x^3+34x^2+13x+3.$

For this reduced curve, it is possible to explicitly compute with Magma invariants such as Weierstrass places, and automorphisms of the curve.
Non-trivial automorphisms could lead to subfields of the function field of the curve $\mathcal{C}$ of small index. By the Riemann-Hurwitz genus formula such a subfield would have genus at most 6, so it could be defined by a polynomial of significantly smaller degree. One could then again try to find rational places, and check whether they extend to rational points on the curve $\mathcal{C}$. This could be done quite efficiently if the subfield were a small index rational field (e.g. of index 2 if $\mathcal{C}$ were hyperelliptic) or a subfield of genus 1.

It however turns out that there are no non-trivial automorphisms over $\mathbb{F}_p$. Under a few extra conditions this leads to the conclusion that the original curve $\mathcal{C}$ does not possess any non-trivial automorphisms either, and in particular is not hyperelliptic:

Proposition 5.4. *The function field $\mathbb{Q}(t,x)$, with t and x fulfilling $h(t,x)=0$ (h as in the appendix) has no non-trivial automorphisms. In particular, $\mathbb{Q}(t,x)$ is not hyperelliptic.*

Proof. Let $p = 47$. The mod-p reduced function field, arising from reduction of the coefficients of $h(t,x)$ mod p, still has genus 11. One therefore has good reduction at ν for some prolongation ν of the p-adic valuation from $\mathbb{Q}$ to $\mathbb{Q}(t,x)$. By genus inequalities as in [20, Th. 3.1.], ν is the unique extension with good reduction of the valuation μ on $\mathbb{Q}(t)$, where $\mu(\frac{p(t)}{q(t)})$ is defined as the maximal p-adic valuation of coefficients of p minus the maximal one of coefficients of q.
Denote reduced objects by a bar.
Assume that σ were a non-trivial automorphism of $\mathbb{Q}(t,x)$, and w.l.o.g. of prime order. By (e.g.) [25, Theorem 6], the maximal possible prime order is $2g+1 = 23$. Let E be the fixed field of σ, and $z \in E$ such that $[E : \mathbb{Q}(z)]$ is minimal. By Riemann-Hurwitz, combined with gonality arguments as in Lemma 3.16, we can assume $[\mathbb{Q}(t,x) : \mathbb{Q}(z)] \leq 2\cdot(2g+1) = 46$. As $\mathbb{Q}(t,x)|\mathbb{Q}(t)$ and $\mathbb{Q}(t,x)|\mathbb{Q}(x)$ are both primitive extensions (of degree > 23), this means that $\mathbb{Q}(t,x) = \mathbb{Q}(t,z) = \mathbb{Q}(x,z)$.

We can assume w.l.o.g. that the reduction $\overline{z}$ is again transcendental over its constant field (e.g. by [13, p.645], where it is proven that good reduction of a function field over a constant field k maps a d-dimensional k-module again onto a d-dimensional $\overline{k}$-module).
As the field $\mathbb{F}_p(\overline{z})$ has index at most $[\mathbb{Q}(t,x) : \mathbb{Q}(z)] \leq 2 \cdot (2g+1) = 46$ in $\overline{\mathbb{Q}(t,x)}$, $\overline{z}$ is even w.l.o.g. a primitive element for $\overline{\mathbb{Q}(t,x)}$ over $\overline{\mathbb{Q}(t)}$.
Again by genus inequalities, ν must also be the unique extension with good reduction of some valuation on $\mathbb{Q}(z)$, and more precisely the unique one with a residue field of genus > 0. Therefore σ fixes the valuation ring of ν (set-wise), and thus induces an automorphism $\overline{\sigma}$ on the reduced function field $\overline{\mathbb{Q}(t,x)}$, defined via $\overline{a} \mapsto \overline{\sigma(a)}$ for all $a \in R$. But by explicit computations with Magma, the reduced function field has trivial automorphism group, so $\overline{\sigma} = id$.
Let g_t be the minimal polynomial of t over $E := Fix(\sigma) \supset \mathbb{Q}(z)$, then g_t splits completely over $\mathbb{Q}(t,x)$. Let $\overline{g_t}$ be the mod-p reduction of g_t (if necessary, after multiplying g_t with powers of p). Then $\overline{g_t}(\bar{t}, \overline{z}) = 0$ and $\overline{g_t}$ splits over $\overline{\mathbb{Q}(t,x)}$, whereas over $\overline{\mathbb{Q}(z)}$, it has a factor of degree greater than 1 (the minimal polynomial of $\bar{t}$, which does not lie in $\overline{\mathbb{Q}(z)}$). But together with the fact that $\overline{\mathbb{Q}(t,x)}|\overline{\mathbb{Q}(z)}$ has trivial automorphism group, this enforces $\overline{g_t}$ to be inseparable, which means $\deg(\overline{g_t}) \geq p$. But on the other hand $\deg(\overline{g_t}) \leq \deg(g_t) \leq 2(2g+1) < p$, a contradiction. □

Question: Does the function field $\mathbb{Q}(t,x)$, with $h(t,x) = 0$ as in the appendix, have a place of degree 1?
This does not yet need to yield an M_{24}-realization over $\mathbb{Q}(t)$ (only if that place lies over an unramified place of the index-416 function field corresponding to the Hurwitz space cover). However, even a ramified degree one place might be used to compute a smaller model for the curve, which could be useful for the search for rational points on it.
As the action of the braids on the Nielsen class of length 416 does not seem to yield such a place, we have also computed the ramification structure of the degree-24 and degree-32 extensions of the function field of $h(t,x)$ over $\mathbb{Q}(t)$ and $\mathbb{Q}(x)$ respectively.
For the degree-24 extension, we found the following branch cycle structure (which again does not yield a place of degree one):

- 34 transpositions, yielding a degree-34 place of ramification index 2 over a degree-34 place of $\mathbb{Q}(t)$.
- Two more involutions, of cycle structure (2^{12}) and $(2^6.1^6)$ respectively.
- One element of order 4, with cycle structure $(4^4.2^4)$.

By the Riemann-Hurwitz genus formula, there are no more ramified places.
The ramification structure was found in the following way: firstly, compute the discriminant of $h(t,x)$, viewed as a polynomial over $\mathbb{Q}(t)$. There is a very large factor in this discriminant, which cannot actually lead to a ramified place, or one would obtain a contradiction to Riemann-Hurwitz.

Furthermore, there is a factor of degree 34, with multiplicity one, which can at most lead to transpositions in the ramification structure.
The remaining factors are of degree one. Compute the monodromy via numerical approximations to find the above cycle structure. The results can be double-checked by computing with Magma the ramified places of low degree for the reduction modulo some primes.

The same can of course be done for the degree 416 equation from Section 5.1.7. Unfortunately this defining equation of the Hurwitz curve does not seem to yield any obvious places of degree one either.

There are, however, degree-one places over the quadratic number fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$ (ramified with regard to the degree-416 cover $\mathcal{C} \to \mathbb{P}^1$). Therefore, over these fields, defining equations of the Hurwitz curve of degree at most 11 must be possible. Such a low-degree parameterization might ease the search for K-rational points over the respective number field K. In fact, for $K = \mathbb{Q}(\sqrt{2})$, such a parameterization could be especially interesting, as a "good" $\mathbb{Q}(\sqrt{2})$-rational point would lead to the (to my knowledge) first M_{23}-realization over a *real* quadratic number field. At least, all the M_{23}-realizations over quadratic number fields arising from the basic rigidity criteria or the braid genus criteria cannot be defined over real quadratic fields (by the branch cycle argument or the reality arguments from Chapter 4).

5.1.12 Appendix: A defining equation for the Hurwitz curve

The following is a defining polynomial for the reduced Hurwitz space of genus 11, corresponding to the M_{24}-family considered above (in the notation of model (5.1), we have $t := \alpha_2$, $x := \alpha_3$):

$$\begin{array}{l}
h(t,x) := 2^{92} \cdot 5^2 \cdot 31^2 \cdot t^{32} \\
+\, 2^{87}(10923791x^2 + 19543496x + 8110928)t^{31} \\
+\, 2^{80}(3701606885x^4 + 12089444672x^3 + 10054513600x^2 - 1752333696x - 3896239360)t^{30} \\
+\, 2^{77}(33553243303x^6 + 171351129026x^5 + 251937188380x^4 + 33571827552x^3 - 151227237504x^2 - 20274108288x + 57668772096)t^{29} \\
+\, 2^{71}(1205889847973x^8 + 9131043180696x^7 + 20650683503688x^6 + 7930709117360x^5 - 22724641020512x^4 - 17497305129984x^3 + 6835786731520x^2 + \\
1879746165760x - 4637627591680)t^{28} \\
+2^{67}(5634163635340x^{10}+62824782685155x^9+205539057067054x^8+121785620629056x^7-460862137561872x^6-645445594912288x^5+20816825165760x^4+ \\
216596182198784x^3 - 110175749152256x^2 - 19966775617536x + 64909362491392)t^{27} \\
+2^{58}(542492237695045x^{12}+7962845315979936x^{11}+35061165420204864x^{10}+25116450098084288x^9-164611871849797120x^8-326972643594982912x^7- \\
20266207383489536x^6 + 271266915079841792x^5 + 473283766612468736x^4 - 238465940324679 68x^3 + 89503540818345984x^2 + 6490901121466368x - \\
19038643868663808)t^{26} \\
+2^{57}(138959891913947x^{14}+2265575781086347x^{13}+11344526365867698x^{12}+928488021108360x^{11}-142407531614978460x^{10}-332144630435747504x^9+ \\
2610425963273248x^8 + 635738575285470464x^7 + 344283134465236992x^6 - 156195340550142464x^5 + 135644672940223488x^4 + 44323019483947008x^3 - \\
183218957468401664x^2 - 922512577101824x + 115428848939 17184)t^{25} \\
+2^{52}(245793481057999x^{16}+4102453575247108x^{15}+14560601737380600x^{14}-121415022333966976x^{13}-1075453257939229192x^{12}-2315306697746190960x^{11}+ \\
2187011126876104992x^{10}+13236549070552954048x^9+9998222582557045056x^8-7989709825345036288x^7-5060170852419068928x^6+2470039106935445504x^5- \\
7973773543535996928x^4 - 3027254754591899648x^3 + 3904885265785815040x^2 - 438949535956467712x + 337890889674915 84)t^{24} \\
+2^{49}(1694660567681x^{18}-154053874639558x^{17}-9094363278263824x^{16}-125772919155425920x^{15}-640195746251471120x^{14}-1332503920103830 24x^{13}+ \\
10178069624166363904x^{12} + 32442765405925389152x^{11} + 17078459727774341120x^{10} - 64642224823920884608x^9 - 77998503741008030720x^8 + \\
87180045912153436 16x^7-83171497992182241 28x^6-35554919676146530304x^5+42125567454425436160x^4+19979211696116826112x^3-16595073691498987520x^2+ \\
46222624168972124 16x - 7587061113883197 44)t^{23} \\
+\, 2^{44}(85154700841x^{20} - 3135276002184x^{19} + 557221936886176x^{18} + 29706711215806464x^{17} + 716742522699574720x^{16} + 7885971436505552992x^{15} + \\
40545012650310439424x^{14} + 68214606892794984064x^{13} - 197810759029367285568x^{12} - 963551129722082838784x^{11} - 1037528470868055764992x^{10} + \\
631783882570743896576x^9 + 1323031306895082974208x^8 - 453997365849381826 56x^7 + 3919178592316856033 28x^6 + 948945950553265397760x^5 - \\
559536357293840232448x^4 - 290918257263042232320x^3 + 272413320108251545600x^2 - 100855272314757971968x + 127783252750059438 08)t^{22}
\end{array}$$

$$+2^{43}(85602721x^{22}-16416761648x^{21}+65418801972x^{20}-400129341448 44x^{19}-4834272221296208x^{18}-138867956664857184x^{17}-2235246181553464496x^{16}-$$

$$20332359916825924112x^{15}-99547245674403279184x^{14}-217631410028466277504x^{13}+605100456375526441 60x^{12}+1175373537188460346112x^{11}+$$

$$1737894309313101495296x^{10}+1154872535885519779 84x^{9}-995492805245364486144x^{8}+645282450382002780 16x^{7}-312546420559972697088x^{6}-$$

$$862239121627541667840x^{5}+447656793131534557184x^{4}+202104454044130869248x^{3}-265276776494714519552x^{2}+86918842973990420480x-7685172181445115904)t^{21}$$

$$+2^{40}(390625x^{24}+13011000x^{23}-1263835698x^{22}-122645603716x^{21}+10023768550248x^{20}+1441027888009784x^{19}+69670385139121704x^{18}+1470482368765953296x^{17}+$$

$$18805232042083273568x^{16}+148917373507289042432x^{15}+692039815721576478976x^{14}+1665454013102260576576x^{13}+1033223324543282524032x^{12}-$$

$$3810476688892121736448x^{11}-7906132777539704465664x^{10}-3438073569152153296384x^{9}+1879325232776781753600x^{8}+3345698565664606023 68x^{7}+$$

$$1306384946650238164992x^{6}+2279450273434835144704x^{5}-1650592004940150341632x^{4}-676851933236811268096x^{3}+839111742006474571776x^{2}-$$

$$197467656677148327936x+111826414018143191 04)t^{20}$$

$$-2^{39}(2640625x^{24}-73341090x^{23}-12463468049x^{22}-742000298620x^{21}+75006505554584x^{20}+4906706913506836x^{19}+151509217243760004x^{18}+$$

$$2558140926548730552x^{17}+27883998293079839272x^{16}+199590392806375040224x^{15}+890573928209509452768x^{14}+2257342508097252798592x^{13}+$$

$$2446187344024426252416x^{12}-1481163741878987908864x^{11}-6403131951376971530816x^{10}-5119868986228426048896x^{9}-711790477224378763008x^{8}+$$

$$574848795396048693248x^{7}+1865526439023164171264x^{6}+1697115062440171907072x^{5}-1240133559053551656960x^{4}-639502015295403032576x^{3}+$$

$$478083122482392563712x^{2}-70415307438464434176x+1869954685459234816)t^{19}$$

$$+2^{36}(33236875x^{24}-2566810916x^{23}-155242978300x^{22}-1443354532432x^{21}+894154750710380x^{20}+39331400693165288x^{19}+905591088339530840x^{18}+$$

$$12650563604443861760x^{17}+120527270495813375856x^{16}+795140475299453472000x^{15}+3443534691176960398816x^{14}+9065186351958289163072x^{13}+$$

$$12541333522964254529888x^{12}+3741851492978183390848x^{11}-13056902141979333330432x^{10}-18305154225411979740672x^{9}-10229950911150169373184x^{8}-$$

$$986439119118034362880x^{7}+6691739518306303953920x^{6}+5773743636262571264000x^{5}-2153695574624478844928x^{4}-1835122146777379307520x^{3}+$$

$$704264072122092617728x^{2}-455705836278579200 00x-13150152742131466 24)t^{18}$$

$$-2^{35}(64778025x^{24}-7787518866x^{23}-217872110036x^{22}+11055224092184x^{21}+1599860723351256x^{20}+53605095010422116x^{19}+994211035094315380x^{18}+$$

$$11674350808622907152x^{17}+97311838740864713920x^{16}+593032925013962296384x^{15}+2502575927176876293760x^{14}+6795796274379747754272x^{13}+$$

$$10914618694159547252384x^{12}+8342388252487979988160x^{11}-15763925657700234534 40x^{10}-9786159979165555473152x^{9}-10164687614660080627712x^{8}-$$

$$4150937661583757763840x^{7}+2924842495911724918016x^{6}+3744466361936529485824x^{5}-1573170485617856921 60x^{4}-828431928912388374528x^{3}+$$

$$119722696193316454400x^{2}+94944225213072015 36x-1103784075663245312)t^{17}$$

$$+2^{32}(350948181x^{24}-56483517584x^{23}-428057570920x^{22}+124489450303536x^{21}+7963738722850456x^{20}+213582247362990168x^{19}+3340238876216028712x^{18}+$$

$$33343870263525543472x^{17}+239820294881657258864x^{16}+1328374307908308453088x^{15}+5423184409774102841760x^{14}+15065941217860806994880x^{13}+$$

$$26854002114307424673984x^{12}+28755459072702597927040x^{11}+13958400315793918730880x^{10}-8241588269148969182464x^{9}-21291594558918723737600x^{8}-$$

$$15200662338293600648192x^{7}+1809752237429604884 48x^{6}+5720846854687766891520x^{5}+1404923850788081188864x^{4}-728037312074027630592x^{3}-$$

$$974710168153787596 80x^{2}+30048089287331938304x-1112498111654592512)t^{16}$$

$$-2^{33}(87740981x^{24}-17780099891x^{23}+150742161950x^{22}+46287663752628x^{21}+1858384322402524x^{20}+40515970650543847x^{19}+550289682841340345x^{18}+$$

$4743678999046086910x^{17} + 28879966442669140102x^{16} + 139840175367996948852x^{15} + 537515218811376006284x^{14} + 1500991030828113912384x^{13} +$
$2878111404031698842160x^{12}+3745964272266063499344x^{11}+3146339566553635659568x^{10}+1019988067402782165600x^{9}-1238715886446794253728x^{8}-$
$1681006443545894411008x^{7} - 584838514144663057280x^{6} + 176022753150619114240x^{5} + 178356587327129780992x^{4} + 19943776125982998528x^{3} -$
$20452437946544090112x^{2} + 1898847440752984064x - 29225420503941120)t^{15}$
$+2^{29}(536686266x^{24}-133008488580x^{23}+3068709021388x^{22}+381992904537640x^{21}+10901231741400555x^{20}+192153409765917900x^{19}+2306253071936799820x^{18}+$
$17619238954534053040x^{17} + 90188661812477277832x^{16} + 358928605033175760720x^{15} + 1212572503610224717664x^{14} + 3243369491083447704512x^{13} +$
$6415436188235129999968x^{12}+9517999534882670902976x^{11}+10582119721307598642496x^{10}+7495952344907486498048x^{9}+1466941629273146328704x^{8}-$
$2241360311249662103552x^{7} - 2015620645871908623104x^{6} - 754739013322857506304x^{5} + 157444621241362799744x^{4} + 212422644026361991168x^{3} -$
$42936437091694485504x^{2} + 1619788383001903104x + 4846054525304832)t^{14}$
$-2^{28}(319935666x^{24}-95529608882x^{23}+3643023064571x^{22}+299018700210420x^{21}+6486848761951792x^{20}+90506817328616638x^{19}+961350062249575482x^{18}+$
$6743129508710451680x^{17} + 29906813633388511192x^{16} + 93061085282481007272x^{15} + 239282954308412296312x^{14} + 519677908940814629216x^{13} +$
$908863001294637074880x^{12}+1413900250435871072544x^{11}+2040120612271709519840x^{10}+2248592993176674542208x^{9}+1572547394528522908928x^{8}+$
$574711016320838862848x^{7} - 109392138737904405120x^{6} - 361694339672036368640x^{5} - 105389759046904012032x^{4} + 62812141844545787904x^{3} -$
$4784990223045167104x^{2} - 31102229979365376x + 2624216744263680)t^{13}$
$+2^{25}(600191029x^{24}-213935307164x^{23}+11925864469982x^{22}+741458932646228x^{21}+12859484945805948x^{20}+137637740317719236x^{19}+1259172125677806908x^{18}+$
$8381163693155075640x^{17} + 34585766777569943272x^{16} + 88886017173752300320x^{15} + 153088336044124940256x^{14} + 140440838916122321376x^{13} -$
$130917941170953150272x^{12} - 558344666885419364800x^{11} - 524542652774214398272x^{10} + 243856691015409629312x^{9} + 1147623290793402367616x^{8} +$
$1341688391862193138432x^{7} + 689656593980579665920x^{6} - 141897170888275433472x^{5} - 190516395083698955776x^{4} + 31027373584971825152x^{3} +$
$288249674326867968x^{2} - 73590853265915904x - 194319880519680)t^{12}$
$-2^{24}(221661095x^{24}-93388882952x^{23}+7387036514263x^{22}+372156970890532x^{21}+5422312545178808x^{20}+43409909271157682x^{19}+315493355867231210x^{18}+$
$2006171865388099460x^{17} + 8290433291813489708x^{16} + 20657137855602261920x^{15} + 32223263820217841536x^{14} + 14348897545885821184x^{13} -$
$106699434585742965568x^{12} - 364423882657075639712x^{11} - 613423498154089390784x^{10} - 595817866033709762176x^{9} - 238511025718474291264x^{8} +$
$132612941180851235200x^{7} + 221061327418708859136x^{6} + 55802434391720037376x^{5} - 29684867097112563712x^{4} - 189181552277180416x^{3} +$
$220458553100144640x^{2} + 1122668689489920x - 102848556957696)t^{11}$
$+2^{21}(256463057x^{24}-125154112872x^{23}+14345112078528x^{22}+610841542626760x^{21}+7891836091516990x^{20}+48092048800937276x^{19}+236220827200377188x^{18}+$
$1330149352455454240x^{17} + 5652824435408570440x^{16} + 14680806911468649632x^{15} + 28447726191294230640x^{14} + 43893376416033183264x^{13} +$
$19545434480196939280x^{12} - 116944893610956920704x^{11} - 377760034610187351616x^{10} - 590644359826593484800x^{9} - 500868765272529055744x^{8} -$
$197834429993725577216x^{7} + 54606829060226213888x^{6} + 66578647198835236864x^{5} - 14052017469157785600x^{4} - 1451713097784950784x^{3} -$
$8193120683360256x^{2} + 2867707724562432x + 11842938077184)t^{10}$
$-2^{20}(57549063x^{24}-30854306452x^{23}+5522323142920x^{22}+204826241910884x^{21}+2480342055492452x^{20}+12676240751261430x^{19}+35767453029433118x^{18}+$

$1221384990832793 36x^{17}+478649871027866000x^{16}+937601042860757360x^{15}+1610477564689290256x^{14}+6178681093255675824x^{13}+18263071553776031888x^{12}+$

$33260201429045651200x^{11}+28730546494444734240x^{10}-9688342363658054016x^{9}-45665643436866023680x^{8}-49976524190900693504x^{7}-19127193842014891008x^{6}+$

$3193091804720496640x^{5}+1406967999372509184x^{4}-1896758613540864x^{3}-8534272056459264x^{2}-77883412709376x+1196304629760)t^{9}$

$+2^{17}(39746997x^{24}-20032525076x^{23}+6725567618648x^{22}+222118418743512x^{21}+2646883632295268x^{20}+13043226410095300x^{19}+26512586367965756x^{18}+$

$16520004267636264x^{17}-44841060516993872x^{16}-820805198155063216x^{15}-3718033487204836976x^{14}-7616893434114977632x^{13}-6503652618305866144x^{12}+$

$1035906373835161126 4x^{11}+39410219306823067008x^{10}+51609773234069201920x^{9}+34953821792507598336x^{8}+2307896335030136832x^{7}-10486466441381867520x^{6}-$

$3147094270547214336x^{5}+112692497823940608x^{4}+558280178830540 80x^{3}+832632051400704x^{2}-33379383508992x-213175369728)t^{8}$

$-2^{17}x(2649081x^{23}-636914861x^{22}+797960876160x^{21}+23795430451484x^{20}+289272778314556x^{19}+1498582705936325x^{18}+3430329276204396x^{17}+$

$3005191033525228x^{16}+981411156397930x^{15}-498833270860605 40x^{14}-335065384539678100x^{13}-1073517570761824272x^{12}-2311311451977704240x^{11}-$

$3109338104777212640x^{10}-1960946794196734912x^{9}+5960488595471193 60x^{8}+2558327245285700608x^{7}+2018310883047692288x^{6}+420991642461542400x^{5}-$

$869494868967260 16x^{4}-27001057300217856x^{3}-550140837396480x^{2}+49821047488512x+722655903744)t^{7}$

$+2^{12}x^{2}(4432180x^{22}+2227474888x^{21}+2296058436392x^{20}+62047172057136x^{19}+791011970150793x^{18}+4335223164161616x^{17}+11379690555206440x^{16}+$

$17293608199083872x^{15}+58683493141986608x^{14}+190493083285750464x^{13}+290408928171156096x^{12}-22134424438257024x^{11}-193483365503963 2192x^{10}-$

$6120623692323426304x^{9}-9881352740945589248x^{8}-9715877747496558592x^{7}-4695922162253725696x^{6}+1908643487579504 64x^{5}+993746767089991680x^{4}+$

$247280787975831552x^{3}+5110510803812352x^{2}-1313573442158592x-32977493950464)t^{6}$

$-2^{11}x^{3}(363092x^{21}+681754500x^{20}+299393259251x^{19}+7242102205032x^{18}+100944513868020x^{17}+565796952291496x^{16}+1403057162825420x^{15}+$

$1036869139107584x^{14}+3122785240383424x^{13}+25303990162116480x^{12}+94028862348131808x^{11}+265751007958806784x^{10}+521967789311095680x^{9}+$

$618601559501476352x^{8}+331287695771024384x^{7}-246666372542144512x^{6}-560678286893506560x^{5}-352320289596997632x^{4}-77464247028645888x^{3}+$

$397293149749248x^{2}+1291929310199808x+50417742643200)t^{5}$

$+2^{8}x^{4}(93557x^{20}+317054368x^{19}+106030579846x^{18}+2195575303292x^{17}+37719911452384x^{16}+213323647652320x^{15}+400481202073152x^{14}-$

$1050198244904960x^{13}-6087078212031984x^{12}-13579764419009536x^{11}-23923684261583616x^{10}-19231175116546560x^{9}+57866089753520896x^{8}+$

$234025836660080640x^{7}+420644080487800832x^{6}+424181041879891968x^{5}+219089243134623744x^{4}+37945221551751168x^{3}-8290993950425088x^{2}-$

$3071214780678144x-174946557100032)t^{4}$

$-2^{7}x^{5}(4617x^{19}+16405810x^{18}+5796064747x^{17}+87896185332x^{16}+2724573849752x^{15}+16944587490264x^{14}+30521069525016x^{13}-131460699245696x^{12}-$

$786495449933952x^{11}-1989847296439808x^{10}-4502103084879616x^{9}-10984105100453888x^{8}-22384423401252864x^{7}-32036360292403200x^{6}-27552284287690752x^{5}-$

$9659525380964352x^{4}+3330121785311232x^{3}+3903894735224832x^{2}+1063202983575552x+83861910061056)t^{3}$

$+2^{4}x^{6}(683x^{18}+912180x^{17}+672117948x^{16}+642293312x^{15}+658505384464x^{14}+4896851991616x^{13}+11973155071872x^{12}-21060410873856x^{11}-$

$174535266827008x^{10}-270224031115264x^{9}+350886477678592x^{8}+1990456865734656x^{7}+3197136619524096x^{6}+1521845817753600x^{5}-2359681776156672x^{4}-$

$4200506540163072x^{3}-2697681750589440x^{2}-776054470606848x-79355701886976)t^{2}$

$-2^{3}x^{7}(x+2)^{2}(17x^{15}-19626x^{14}+6064864x^{13}-678223416x^{12}+31229956768x^{11}+107783297440x^{10}-146476766784x^{9}-3079271986560x^{8}-$

$11175244911360x^7 - 20126745257472x^6 - 14836838418432x^5 + 14307717076992x^4 + 419843444424448x^3 + 36894740668416x^2 + 14132960870400x + 1886544691200)t$

$+ x^8(x+2)^2(x^2-4x-4)(x^6-500x^5+61716x^4+274464x^3+731376x^2+907200x+388800)^2$

5.2 A family of M_{24}-covers ramified over five points

Another interesting family with regard to M_{24} and M_{23} is the family of 5-pointed genus zero covers with monodromy $(2^8.1^8, 2^8.1^8, 2^8.1^8, 2^8.1^8, 4^4.2^2.1^4)$. Here the reduced Hurwitz space is 2-dimensional, i.e. a surface. The length of the (unique) M_{24}-braid orbit is $l = 72000$. A rational point on this Hurwitz space would not necessarily lead to an M_{23}-realization. The problem lies again in the question whether or not the M_{23}-fixed field of a coresponding cover is a rational function field. However, the possibility of the M_{23}-fixed field being a rational function field at least cannot be excluded by reality considerations, cf. Prop. 4.6.

We have tried an approach similar to the one treated above, to obtain covers with this monodromy. Complex approximations of such covers have been obtained, and are given in the file "M24_(2,2,2,2,4)_approx.txt".

5.2.1 Related four point covers

Various Hurwitz curves for 4-tuples lie on the boundary of the 2-dimensional reduced Hurwitz space. They can be used as starting points for the computations.

1. Granboulan's cover with monodromy $(2A, 2A, 2A, 12B)$, cf. [43].
   In [19], L. Granboulan gave a polynomial $f(X,t)$ with group M_{24} and monodromy $(2A, 2A, 2A, 12B)$. In [43], P. Müller computed a defining equation for the whole family of M_{24}-polynomials with this monodromy.
   We used a polynomial in this family as a starting point to obtain complex approximations of a polynomial $f(X) - tg(X)$ $(f, g \in \mathbb{C}[X])$ with monodromy $(2A, 2A, 2A, 2A, 4B)$.

   In the file "M24_(2,2,2,2,4)_approx.txt" we give such an approximation, for a fixed set of branch points. Again, via numerical braid group action, it is possible to obtain further polynomials, with the same ramification locus, but different monodromy. It seems out of reach, however, to obtain a complete fiber as in the previous section, as the corresponding inner Nielsen class is of length 72000, with transitive braid group action.

2. The family with monodromy $(2A, 2A, 2A, 23A)$.
   An advantage of taking this family as a starting point for the deformation process is that, due to the 23-cycle in the monodromy of the degenerate family, the approach of Chapter 3.3.1 will automatically lead to M_{24}-covers in the $(2A, 2A, 2A, 2A, 4B)$-family (and not to A_{24} ones), as can be seen from Lemma 3.15. One can therefore develop Laurent series modulo some primes without worrying about monodromy.

   Another advantage is that the corresponding Nielsen class is relatively small (of length 46) and has a Hurwitz curve of genus zero, therefore it is not difficult to compute members of the family defined over small number fields (and over suitable finite fields).

We used an approach starting with two covers ramified over three points, related to each other as described in Section 3.3.1, with monodromy of type $(6^2.3^2.2^2.1^2, 2A, 23A)$ and $(2A, 2A, 6^2.3^2.2^2.1^2)$ respectively. The first class tuple gives rise to an M_{24}-cover, with normalized structure constant $l(C) = 5$. Together with the fact that the conjugacy class of a 23-cycle in M_{24} is not rational (splitting into two classes, as the 23-cycle is not conjugate to its inverse), this leads to the conjecture that this cover will be defined over a degree-10 number field. This is indeed the case. We obtained an explicit polynomial by first finding a solution modulo 13, and then applying p-adic lifting methods.

From this degenerate cover, we first obtain a non-degenerate one, as in the previous section. After this, it is not difficult to find an $\mathbb{F}_p$-point on the Hurwitz space (for a suitable prime p), i.e. a non-degenerate cover over $\mathbb{F}_p$. As before, this can either be done by computing a full fiber of the Hurwitz curve cover, or somewhat quicker by specializing a suitable coefficient (of low index in the function field of the Hurwitz curve) to a rational value and retrieving the minimal polynomials for the remaining coefficients.

Next, beginning from this non-degenerate cover, a Laurent series approach over $\mathbb{F}_p$ yields a defining equation for the Hurwitz curve cover of degree 46; as this curve is rational, it can be parameterized by an equation of the form $f(x) - tg(x) = 0$, with x a parameter of the genus zero function field of the Hurwitz curve (modulo p it is not difficult to explicitly find such a parameter, once a defining equation for the function field has been found).

Finally, lift this genus zero equation to obtain a rational parameterization $F(t, x) = 0$ of the Hurwitz curve of degree 46, defined over the field $\mathbb{Q}(\sqrt{-23})$. In our case, this parameterization was of the following form:

Set $F(t, x) := f^3 \cdot g^2 - t \cdot h^2$, where

$f := (x - 65/2) \cdot (x^{10} + 1/10 \cdot (11 \cdot \alpha - 1677) \cdot x^9 + 1/40 \cdot (-6457 \cdot \alpha + 495835) \cdot x^8 + 1/20 \cdot (214489 \cdot \alpha - 10537579) \cdot x^7 + 1/160 \cdot (-68788225 \cdot \alpha + 2243804947) \cdot x^6 + 1/160 \cdot (1858781485 \cdot \alpha - 37799897239) \cdot x^5 + 1/14720 \cdot (-3242903406369 \cdot \alpha + 34625456045619) \cdot x^4 + 1/3680 \cdot (10677543333853 \cdot \alpha - 36249941981191) \cdot x^3 + 1/7360 \cdot (-184255352619393 \cdot \alpha - 316677905680077) \cdot x^2 + 1/1840 \cdot (230139068653175 \cdot \alpha + 1173546750105867) \cdot x + 1/14720 \cdot (-3960449698542073 \cdot \alpha - 28493939813841093))$,

$g := x^4 + 1/20 \cdot (-33 \cdot \alpha - 829) \cdot x^3 + 1/120 \cdot (10351 \cdot \alpha + 30595) \cdot x^2 + 1/240 \cdot (-362329 \cdot \alpha + 1570139) \cdot x + 1/240 \cdot (1021493 \cdot \alpha - 20204719)$,

$h := x^{23} - 368 \cdot x^{22} + 1/40 \cdot (2783 \cdot \alpha + 2537843) \cdot x^{21} + 1/40 \cdot (-965701 \cdot \alpha - 271812321) \cdot x^{20} + 1/4000 \cdot (15671292857 \cdot \alpha + 2020362477573) \cdot x^{19} + 1/50000 \cdot (-19795532107989 \cdot \alpha - 1377409015370993) \cdot x^{18}$

$$
\begin{aligned}
&+ 1/400000 \cdot (11204269027871271 \cdot \alpha + 454448095942490331) \cdot x^{17}\\
&+ 1/400000 \cdot (-592437399414311451 \cdot \alpha - 14397720097497647295) \cdot x^{16}\\
&+ 1/1600000 \cdot (97837990987163242299 \cdot \alpha + 1415255334721558518111) \cdot x^{15}\\
&+ 1/400000 \cdot (-815734115126158870521 \cdot \alpha - 6867881768734494803141) \cdot x^{14}\\
&+ 1/6400000 \cdot (361877063741947808286837 \cdot \alpha + 1798798309667146715584657) \cdot x^{13}\\
&+ 1/6400000 \cdot (-853818567744601050451641 1\cdot \alpha - 2927906283584847310179670 3) \cdot x^{12}\\
&+ 1/25600000 \cdot (6950449426253872162856331 55 \cdot \alpha + 2179471785855115590210329863) \cdot x^{11}\\
&+ 1/12800000 \cdot (-6090979631961094970190235837 \cdot \alpha - 20260543672454024695342581049) \cdot x^{10}\\
&+ 1/102400000 \cdot (722106431429794734025918355349 \cdot \alpha + 2352973703671853490330898366769) \cdot x^{9}\\
&+ 1/102400000 \cdot (-8750514926878265686208186042293 \cdot \alpha - 20257263117415967085377068857041) \cdot x^{8}\\
&+ 1/51200000 \cdot (4129507162594668369393967360389 7 \cdot \alpha - 9050063408389035005656984336123) \cdot x^{7}\\
&+ 1/51200000 \cdot (-280987462543326507084263451781741 \cdot \alpha + 173056849433841001530901872088239 1) \cdot x^{6}\\
&+ 1/25600000 \cdot (580389448132173479922433354661673 \cdot \alpha - 1397917789306472752980709355233940 3) \cdot x^{5}\\
&+ 1/25600000 \cdot (-5009792380913878242927788175861 33 \cdot \alpha + 1293707718796298954174145573499022 23) \cdot x^{4}\\
&+ 1/51200000 \cdot (-1542766656635550654521821097880471 \cdot \alpha - 1543596749528918677305588705549819275) \cdot x^{3}\\
&+ 1/51200000 \cdot (5257531513606696629196245652087111 3 \cdot \alpha + 5853503694838041686667354808291445589) \cdot x^{2}\\
&+ 1/102400000 \cdot (26212614325507137271814950675291466 3 \cdot \alpha - 2557673586874736257362862169783035888 5) \cdot x\\
&+ 1/102400000 \cdot (-15223369416899011346035061003041127 91 \cdot \alpha + 2426272785842629794321018122822419800 5).
\end{aligned}
$$

Here $\alpha := \sqrt{-23}$.

Note that in spite of the Hurwitz curve having genus zero, this cover cannot be defined over the rationals because the class $23A$ is not rational in M_{24}. In fact it cannot even be defined over a real field, because the 23-cycle would then have to be conjugate to its inverse. For a suitable $\mathbb{Q}(\alpha)$-rational point on the Hurwitz space, we can find an explicit polynomial for a $(2A, 2A, 2A, 23A)$-cover defined over $\mathbb{Q}(\alpha)$. Here is one such polynomial:

$$
\begin{aligned}
&f(t,x) := (x^8+4x^7+(-\alpha+7)x^6+(6\alpha+30)x^5+(26\alpha+82)x^4+(16\alpha+272)x^3+(44\alpha+252)x^2+(80\alpha-240)x+40\alpha+8)^2\\
&\cdot(x^8-8x^7+(2\alpha+34)x^6+\tfrac{1}{2}(-3\alpha-135)x^5-(34\alpha+74)x^4+(238\alpha+470)x^3-(736\alpha+1248)x^2+(1082\alpha+1074)x-(920\alpha+184))-t\cdot x.
\end{aligned}
$$

Once we have found a cover of type $(2A, 2A, 2A, 23A)$, we once again take the "opposite" degenerate cover into consideration, to proceed to the family of type $(2A, 2A, 2A, 2A, 4B)$. This has to be a cover ramified over three points, with cycle structure $(2A, 4B, 23B)$, acting intransitively. The group generated by such a tuple turns out to be M_{23}. In fact such a cover was given by Elkies in [14].

In this way, we obtain formal Laurent series approximations for the 5-point family.

5.2.2 Rational translates of function fields

The M_{24}-family with four branch points and ramification structure $(2A, 2A, 2B, 8)$ is also closely related to this five-point family, although in a different way than the above families. It is not a degeneration obtained from the five-point family by glueing two branch points together. Instead representatives of the five-point family arise naturally from the four-point one through rational translates of the base field, more precisely via quadratic extensions.

Namely, assume that $\mathbb{C}(x)|\mathbb{C}(t)$ is an extension of genus zero function fields corresponding to a degree-24 cover with M_{24}-monodromy of type $(2A, 2A, 2B, 8)$.

Assume that the inertia group generator over the infinite place in t is the element of order 8 and the one over $t \mapsto 1$ is the involution of class $2B$ (as in the model in Chapter 5.1).

Now define an extension $\mathbb{C}(s)$ of $\mathbb{C}(t)$ by $s^2 + 1 = t$.

Then ramification in $\mathbb{C}(s)|\mathbb{C}(t)$ occurs only over $t \mapsto 1$ and $t \mapsto \infty$. Now a version of Abhyankar's Lemma (cf. [53, Th. 3.9.1]) clarifies the ramification in $\mathbb{C}(s, x)|\mathbb{C}(s)$ and $\mathbb{C}(s, x)|\mathbb{C}(x)$:

Lemma 5.5 (Abhyankar's Lemma). *Let $F'|F$ be a finite extension of function fields in characteristic zero, such that $F' = F_1F_2$ with two intermediate fields F_1 and F_2 of $F'|F$. Let $\mathcal{P}$ be a place of F, $\mathcal{P}'$ an extension of $\mathcal{P}$ to F', and $\mathcal{P}_i := P' \cap F_i$ $(i = 1, 2)$.*

Then the ramification index of $\mathcal{P}'$ over $\mathcal{P}$ is equal to the least common multiple of the ramification indices of $\mathcal{P}_i$ over $\mathcal{P}$ $(i = 1, 2)$.

Application to the fields $F' = \mathbb{C}(s, x)$ and $F = \mathbb{C}(t)$ (with intermediate fields $F_1 = \mathbb{C}(s)$ and $F_2 = \mathbb{C}(x)$) yields that exactly two places of $\mathbb{C}(x)$ ramify in $\mathbb{C}(s, x)$, namely the only places of ramification index 1 over the infinite place in t. In particular, $\mathbb{C}(s, x)$ is of genus zero by the Riemann-Hurwitz genus formula, and thus a rational function field, i.e. $\mathbb{C}(s, x) = \mathbb{C}(y)$ for some $y \in \mathbb{C}(s, x)$.

On the other hand, ramification in the degree-24 extension $\mathbb{C}(y)|\mathbb{C}(s)$ occurs over exactly five places, namely $s \mapsto \infty$ and the (total of four) places extending the two places of $\mathbb{C}(t)$ with inertia group generator in class $2A$. As these places are unramified in $\mathbb{C}(s)|\mathbb{C}(t)$, the inertia group generators in $\mathbb{C}(y)|\mathbb{C}(s)$ are still in class $2A$, in all four cases. Similarly, the inertia group generator over $s \mapsto \infty$ is in class $4B$ (cycle structure $(4^4.2^2.1^4)$) of M_{24}.

Therefore, $\mathbb{C}(y)|\mathbb{C}(s)$ is a genus zero function field, with branch cycles in classes $(2A, 2A, 2A, 2A, 4B)$.[1]

As the above is possible for arbitrary position of the branch points of a $(2A, 2A, 2B, 8)$-cover, this means that the Hurwitz space for the $(2A, 2A, 2A, 2A, 4B)$-5-tuples contains a curve of genus 11 (the genus of the symmetrized reduced Hurwitz space computed in Chapter 5.1).

This can also be verified group-theoretically with the methods developed by Dettweiler in [12]. Namely, the group generated by the braids $\beta_1\beta_4$ and $\beta_2\beta_3\beta_2$ acts intransitively on the straight

[1] Note especially that the Galois group of $E|\mathbb{C}(s)$, with E the Galois closure of $\mathbb{C}(y)$, must still be M_{24}!

Nielsen class of length 72000 of generating 5-tuples of the form $(2A, 2A, 4B, 2A, 2A)$, with an orbit of length 416.

This, together with the results about the four-point family already computed yields results about existence of points in relatively small number fields for the five-point family, a result that might otherwise be surprising, considering the huge length of the Nielsen class.

In particular, as we have already computed polynomials over some finite fields with $(2A, 2A, 2B, 8)$-ramification, it is now easy to obtain from those polynomials with $(2A, 2A, 2A, 2A, 4B)$-ramification. In the appendix we give such a polynomial for the field $\mathbb{F}_{17}$.

In order to look for algebraic dependencies, this polynomial can be used as a starting point. As the reduced Hurwitz space is a surface here, upon fixing appropriate places via Moebius transformations as usual, one can expect to find an algebraic dependency between three given coefficients of the model. However, the degree of such an equation might be huge, and in fact I have not been able to find one so far. One possible approach is to fix one more coefficient (e.g. one of the triple that one wants to use to find an algebraic dependency) to a given value c, and then search for a dependency between the remaining two coefficients (this corresponds to trying to compute a curve on the two-dimensional Hurwitz space, instead of the whole surface). Once this has been successful, one may repeat it for many values of c and then interpolate to retrieve an equation for the whole surface.
I have tried this for equations over $\mathbb{F}_{17}$ up to degree 120 in two variables (cross-ratios of coefficients of the model), but it seems that these degrees still do not suffice.

5.2.3 From 5 points back to 4 points

The importance of the $(2A, 2A, 2A, 2A, 4B)$-family lies not only in the possibility of finding rational points on the corresponding (2-dimensional) reduced Hurwitz space which might lead to M_{24}-realizations with these branch cycles, but also in the possibility to gain several 4-pointed families (with group M_{24} or M_{23}) by inverting the deformation process used so far, i.e. letting two branch points converge to each other and obtain a cover with monodromy $(\sigma_1\sigma_2, \sigma_3, \sigma_4, \sigma_5)$ from one with monodromy $(\sigma_1, ..., \sigma_5)$. By purely group theoretical methods, one confirms that the following class tuples can be obtained in this way:
$(2A, 2A, 3B, 4B)$, $(2A, 2A, 4A, 4B)$, $(2A, 2A, 4B, 5A)$, $(2A, 2A, 4B, 6A)$ (all of these with group M_{24}) and $(2A, 2A, 4A, 4A)$ (with group M_{23}).

(All these tuples consist of rational conjugacy classes, and are genus zero tuples that allow a rational function field realization over a real field by reality arguments as in Chapter 4, i.e. are potential candidates for a regular M_{23}-realization over $\mathbb{Q}$.)

Complex approximations for a cover in each of these 4-point families are given in five separate plain-text files.
We obtained these by starting with the cover in the file "M24_(2,2,2,2,4)_approx.txt", applying the braid group action (with as few braiding turns as possible) to obtain a cover with monodromy $(\sigma_1, ..., \sigma_5)$, such that $(\sigma_1\sigma_2, \sigma_3, \sigma_4, \sigma_5)$ is the desired 4-point monodromy, and then letting the first and second branch point converge towards each other.

Even though for all these families, the braid orbit length as well as the genus of the Hurwitz curve are larger than for the one computed in Chapter 5.1, the methods exhibited there may be used to proceed from complex approximations to algebraic equations for these families as well, and then try to find rational points.

5.3 A family of covers with Galois group M_{23}

Here we examine a family of covers with Galois group $G := M_{23}$, and ramification of type $(2A, 2A, 3A, 5A)$ (there is a unique class of elements of order k in M_{23} for $k \in \{2, 3, 5\}$).

The Nielsen class $SNi^{in}(C) := \{(\sigma_1, ..., \sigma_4) \in G^4 \mid \sigma_1, \sigma_2 \in 2A, \sigma_3 \in 3A, \sigma_4 \in 5A, \sigma_1 \cdots \sigma_4 = 1, \langle\sigma_1, ..., \sigma_4\rangle = G\}/Inn(G)$ is of length 980 (the shortest Nielsen class amongst all genus zero 4-tuples of rational classes in M_{23}), and becomes a single orbit under braid group action, with C_2-symmetrized braid orbit genus $g = 43$.
The aim of this chapter is to explicitly compute a defining equation for the Hurwitz curve of genus 43.

We start with a degenerate cover with inertia group generators of orders 2, 15 and 5, with the generated group still the full group M_{23}. Such a cover can be found by exhaustive search modulo a prime (with help of the Dedekind criterion, in order to recheck one has indeed an M_{23}-polynomial and not one for A_{23}).
Here is an equation for this three-point cover, reduced modulo $p = 17$:

$$\widehat{f}(t, x) := (x^4 + 10x^3 + 6x^2 + 9x + 10)^5 \cdot (x^3 + 14x^2 + 12x + 4) - t \cdot x^5 \cdot (x - 1)^3.$$

Next, we lift it to get a cover over a certain number field. In this case, the number field has degree 10 over $\mathbb{Q}$, which is to be expected as the $(2, 15, 5)$-tuples generating M_{23} have normalized structure constant 5 and in addition the classes of elements of order 15 in M_{23} are not rational; more precisely those elements split into two classes.

With the above notation, this degenerate cover has monodromy $(\sigma_1, \sigma_2\sigma_3, \sigma_4)$ for a suitable 4-tuple in the Nielsen class $SNi(C)$.

Now, looking again at the "opposite" degenerate cover, with monodromy $(\sigma_2, \sigma_3, (\sigma_2\sigma_3)^{-1})$ we obtain an intransitive group with orbits of length 3, 5 and 15 (the cycle lengths of the conjugacy class $15A/B$). The images of $\langle\sigma_2, \sigma_3\rangle$ in the actions on the respective orbits are C_3, A_5 and and $C_3 \times A_5$ in an imprimitive action on 5 blocks of length 3. Covers with monodromy corresponding to each orbit can therefore easily be computed, as in particular a function for the latter orbit can be composed of rational functions of degrees 5 and 3.

Furthermore, the ramification index in the Hurwitz space at the point corresponding to the 3-point ramified cover with monodromy $(\sigma_1, \sigma_2\sigma_3, \sigma_4)$ computed above is $e = 5$.
Therefore, as before, parameter transformations and computation of the component covers corresponding to the three cycles of $\sigma_2\sigma_3$ enable one to obtain a cover ramified over four points via Newton approximation. Once such a cover is approximated with sufficient precision (ramified in t over 0, μ^5, 1 and ∞, with some small complex number μ, where $\mathbb{C}(x)|\mathbb{C}(t)$ is the corresponding function field extension), the ramifiation locus can be slowly moved, to eventually satisfy the following conditions:

- The infinite place in t is ramified with inertia group generator of order 5.
- The inertia group generators of order 2 correspond to $(t - \sqrt{a}) \cdot (t + \sqrt{a}) = t^2 - a = 0$, with some $a \in \mathbb{Q}$.
- One more place $t \mapsto b$, with fixed $b \in \mathbb{Q}$ is ramified with inertia group generator of order 3.

We did this for $a = \frac{1}{4}$ and $b = -\frac{1}{4}$, i.e. branch point set $(\{-\frac{1}{2}, \frac{1}{2}\}, -\frac{1}{4}, \infty)$.
Next, via braid group action, we computed complex approximations for all 980 equivalence classes of covers with these ramification data.
These then form a complete fiber of the cover $f : \mathcal{C} \to \mathbb{P}^1\mathbb{C}$, with $\mathcal{C}$ the reduced Hurwitz curve. More precisely, if $F|\mathbb{Q}(a)$ is the corresponding function field extension of this cover (note that it is defined over $\mathbb{Q}$!), we obtain the complete fiber $f^{-1}(\frac{1}{4})$.

The complete fiber is given in the file "`m23_(2,2,3,5)_approx.txt`". Again one can verify certain invariants that already followed from theoretical criteria. As an example, the monodromy image of the braid group (isomorphic to A_{980}) contains an element representing complex conjugation on the equivalence classes of covers with our fixed choice of branch points. This element, in its action on the 980 elements of the straight Nielsen class, has exactly 26 fixed points, and indeed there are exactly 26 real points in our fiber.

With a full fiber computed, one can now proceed as in Chapter 5.1 to find an $\mathbb{F}_p$-point for some $p \in \mathbb{P}$. We did this for $p = 19$ to obtain the polynomial $f(t, X) = X^3 \cdot (X^5 + X^4 - X^3 - X^2 + 7)^3 \cdot (X^5 + 6X^4 + X^3 + 4X^2 + 12X + 1) - t \cdot (X^3 + 2X^2 + 13X + 5)^5 \cdot (X^3 + X^2 + 2X + 6)$ with Galois group M_{23} over $\mathbb{F}_{19}(t)$, cf. the table in Appendix A.

Now again, lifting this $\mathbb{F}_p$-point to many different $\mathbb{Q}_p$-points enables one to find a polynomial equation defining the function field of the Hurwitz curve. We found a polynomial of degrees 97 and 98 in two variables, vanishing for two coefficients α and β of the following model for the universal family:

$$\begin{aligned} t-\frac{1}{4} &= C\cdot\frac{f_1(X)^3\cdot f_2(X)}{g_1(X)^5\cdot g_2(X)},\\ t-\frac{1}{2}-\lambda &= C\cdot\frac{f_3(X)^2\cdot f_4(X)}{g_1(X)^5\cdot g_2(X)},\\ t-\frac{1}{2}+\lambda &= C\cdot\frac{f_5(X)^2\cdot f_6(X)}{g_1(X)^5\cdot g_2(X)}. \end{aligned} \tag{5.2}$$

Here the polynomials $f_1, ..., f_6$ are monic of degrees $6, 5, 8, 7, 8$ and 7 respectively, and g_1, g_2 are both monic of degree 3 (which is justified by the fact that one of the four places (over $\mathbb{C}$) of ramification index 5 can without restriction be mapped to infinity because the corresponding cycle is an isolated orbit under the action of the decomposition group).

The coefficients of f_1, f_2, g_1 and g_2, as well as the leading coefficient C can be assumed to lie in a degree 980 extension of $\mathbb{Q}(\lambda^2)$ (and the ones of $f_3, ..., f_6$ in a further degree-2 extension).

Furthermore, in our computations, we fixed the coefficient of g_1 at X^2 to $\frac{1}{3}$ and the one of g_2 at X^2 to $-\frac{1}{2}$.

Then, denoting by α the coefficient of f_2 at X^4 and by β the one of f_1 at X^5, we found the aforementioned algebraic dependency over $\mathbb{Q}$, of relative degrees 97 resp. 98.

This polynomial, defining the Hurwitz curve of genus 43, is given in the file
“`(2,2,3,5)_hurwitzcurve_parametrization.txt`”.

To find the p-adic dependency and retrieve the corresponding rational numbers, we developed series with a precision p^{100000}.

Verification of the genus of this curve is more difficult than in the previous section, because of the high degrees, which even make computations modulo some $p \in \mathbb{P}$ very difficult. We therefore used numerical methods to confirm (heuristically) that this curve actually has genus 43.

Proposition 5.6.
The polynomial $h(t,x)$ given in the file “`(2,2,3,5)_hurwitzcurve_parametrization.txt`” defines an absolutely irreducible curve of genus 43 over $\mathbb{Q}$.

Proof. Let $\mathbb{Q}(t,x)|\mathbb{Q}(t)$ be the extension of degree 98 given by the equation $h(t,x) = 0$.

The irreducibility is obvious, and indeed the Dedekind reduction criterion easily yields that
$Gal(\mathbb{Q}(t,x)|\mathbb{Q}(t)) \cong S_{98}$.

The absolute irreducibility now follows e.g. from the fact that the Newton polytope of this polynomial has vertices $(0,0), (97,0), (96,2), (0,98)$; and as the greatest common divisor of these coordinates is 1, [6, Lemma 1.3.] yields absolute irreducibility.

(Alternatively, the existence of simple rational points, as given in the next proposition, also yields absolute irreducibility immediately.)
By numerical methods, one verifies that ramification occurs only above the following places of $\mathbb{Q}(t)$:

- One place of degree 263, with all inertia group generators acting as transpositions in S_{98}.
- One degree two place (namely corresponding to the polynomial $t^2 - 145/9 \cdot t + 12850/81$) with a transposition as inertia group generator.
- Two degree one places (namely $t \mapsto 35/9$ and $t \mapsto 295/288$) with transpositions as inertia group generators.
- One degree one place (namely the infinite place of $\mathbb{Q}(t)$) with inertia group generator of cycle type $(4^2.3^2.2^3.1^{78})$.

By Riemann-Hurwitz, this yields genus 43 for the function field $\mathbb{Q}(t, x)$. □

Looking for rational points on this curve, one indeed finds several with "small" coordinate values (in terms of height), and there are even non-singular points. Magma computation for all rational values with numerator and denominator of absolute value at most 10000 yields:

Proposition 5.7. *Let $t_0, x_0 \in \mathbb{Q}$ such that either t_0 or x_0 has numerator and denominator of absolute value at most 10000. Then exactly the following values for (t_0, x_0) annihilate the polynomial h given in the file "`(2,2,3,5)_hurwitzcurve_parametrization.txt`":*

$$(\frac{31}{18}, 0), (\frac{5}{9}, \frac{2}{3}), (\frac{35}{9}, \frac{2}{3}), (\frac{410}{9}, \frac{2}{3}), (\frac{295}{288}, -\frac{11}{96})$$

Here the points $(\frac{31}{18}, 0)$, $(\frac{5}{9}, \frac{2}{3})$ and $(\frac{410}{9}, \frac{2}{3})$ are non-singular points on the curve.
However, this does not guarantee an M_{23}-realization over $\mathbb{Q}$, as the actual question is whether these correspond to unramified points on the original Hurwitz curve cover (980-fold covering of $\mathbb{P}^1\mathbb{C}$). We found it too hard to explicitly compute a polynomial describing the degree-980 covering, although in theory this could be done by computing many fibers and then interpolating, as in Chapter 5.1 (this polynomial would have to be of degree 980 in one variable, and possibly degree close to 100 in the other one). There are several ways to check whether the non-singular points actually correspond to covers with 4 branch points.
Firstly, for the mod-p reduction of the family, we managed to express the parameter a, as well as all the coefficients of the polynomials f_1, f_2, g_1 and g_2 in model (5.2), as a polynomial in the two coefficients α and β (which should of course be possible if these two actually generate the whole function field of the Hurwitz curve). Plugging in the values of the $\mathbb{Q}$-rational points, one can check whether the value of a leads to a degenerate or a non-degenerate cover modulo p. In our cases, all

points lead to degenerate cases[2].
In addition, one can try to find the points on the Hurwitz space, using again the complex approximations, moving through the various branches of the Hurwitz space. As there are quite a lot of branches, and some of them show rather bad numerical behaviour, it is useful to use reality arguments as in Chapter 4 to find out the branches defined over $\mathbb{R}$ (these are considerably less) and only move through them.

Taking into account the results of the numerical monodromy computations, there are at least five degree one places (namely three corresponding to non-singular points and two of ramification index 2 over degree one places of $\mathbb{Q}(t)$, as given above). Moving through the branches of the Hurwitz spaces (combined with mod-p calculations) seems to yield evidence that all these places correspond to degenerate covers, with $\lambda \mapsto 1/4$ in the notation of model (5.2). As these degenerate covers are in 1-1 correspondence with the cycles of the braid group generator $\beta_{1,2}$ in its action on the Nielsen class of length 980, we can express them more concretely:

Let the 980 equivalence classes of covers in our Nielsen class be ordered as in the file "`m23_(2,2,3,5)_approx.txt`". Then the following orbits of $\beta_{1,2}$ in its action on this ordered set correspond to the five rational points:

- $\{84, 143, 237\}$ to the point $(\frac{410}{9}, \frac{2}{3})$,
- $\{106, 177, 291, 447\}$ to the point $(\frac{35}{9}, \frac{2}{3})$,
- $\{332, 497\}$ to the point $(\frac{5}{9}, \frac{2}{3})$,
- $\{137, 228, 370\}$ to the point $(\frac{295}{288}, -\frac{11}{96})$, and
- $\{538, 733, 870, 961\}$ to the point $(\frac{31}{18}, 0)$.

I.e., starting with any cover in one of these orbits and moving through the Hurwitz space by letting the parameter λ converge to $1/4$, the coefficients of α and β will converge towards the respective rational values. Also, the Galois group of the 3-point cover arising in this way is a proper subgroup of M_{23} in all cases.

Even though none of our rational points led to M_{23}-realizations over $\mathbb{Q}$, the existence of non-singular points in the above model nevertheless yields some useful information about the function field of the Hurwitz curve. Namely, as there exist places of degree one, gonality arguments as in Lemma 3.16 show that this curve has an affine model of degree 43 (in at least one of the two variables).

[2] Note however that this is only heuristic as a non-degenerate point over $\mathbb{Q}$ may very well become degenerate modulo some primes.

As in Chapter 5.1, it would be interesting to explicitly obtain such a model, as it might considerably reduce the height of possible rational points.
We did manage to compute such a model over the finite field $\mathbb{F}_{19}$ (although the computations are very lengthy; computing the model and verifying that the genus of the function field over $\mathbb{F}_{19}$ is 43 took several days with Magma).
This model then may be used to look for possible automorphisms, Weierstrass places etc. of the Hurwitz curve.
E.g. for the mod-19 reduced function field, extensive computations yielded 59 degree-1 places, four of which are Weierstrass, however all of weight 1. In particular, these computations yielded no evidence for the function field to be hyperelliptic.

5.4 A five point family in M_{23}

Just as M_{24}, the group M_{23} has exactly one Nielsen class of generating genus-zero 5-tuples, namely of classes $(2A, 2A, 2A, 2A, 3A)$. One computes that $|SNi^{in}(C)| = 21456$, with transitive braid group action. To obtain an approximation for a cover in this family, a 4-tuple of classes $(5A, 2A, 2A, 3A)$ may be taken as a starting point for the usual deformation process.

We include one complex approximation for a cover in the five point family in the file "`M23_(2,2,2,2,3)_approx.txt`". For the function field extension $\mathbb{C}(X)|\mathbb{C}(t)$ corresponding to this cover, we made the following assumptions:

- The inertia group generator belonging to the infinite place in t is of class $3A$.
- The unique place over $t \mapsto \infty$ which is fixed by the normalizer in M_{23} of this inertia group is $X \mapsto \infty$.
- Normalization of the ramification locus: the finite ramification locus is the set of zeroes of a polynomial $x^4 + a_1 x^2 + a_2 x + a_2$, with some $a_1, a_2 \in \mathbb{C}$.

By varying the parameters a_1 and a_2, one can therefore study a surface on the Hurwitz space. Note that the above assumptions about ramified places can be made without affecting the field of definition of the covers belonging to this surface.

5.5 Summary

We have applied various methods outlined in the previous chapters to obtain algebraic models of Hurwitz curves for class tuples with groups M_{24} and M_{23}. Although it could not be decided whether these curves may lead to regular M_{23}-realizations over $\mathbb{Q}$ (and although stronger number-theoretic tools may be necessary to decide this question), they do provide concrete data for further study. We have furthermore provided complex approximations of covers for the majority of rational class 4- and 5-tuples of genus zero in M_{24} and M_{23}. These approximations can be used to obtain further algebraic models for Hurwitz spaces, by applying the same methods as before.

Chapter 6

A family of polynomials with Galois group $PSL_5(2)$ over $\mathbb{Q}(t)$

We compute a family of coverings with four ramification points, defined over $\mathbb{Q}$, with regular Galois group $PSL_5(2)$.
This is (to my knowledge) the first explicit polynomial with group $PSL_5(2)$ over $\mathbb{Q}(t)$.

6.1 A theoretical existence argument

The group $PSL_5(2)$ does not have any rigid triples of rational conjugacy classes, and among the genus zero systems of rational class 4-tuples, there is only one with a Hurwitz curve of genus zero. This curve will turn out to be rational in the course of the explicit computations, but this does not seem to be immediately clear by the standard braid orbit criteria (see below). So in order to obtain $PSL_5(2)$ as a monodromy group of a rational function $t = \frac{f(x)}{g(x)} \in \mathbb{Q}(x)$ (or even as a Galois group over $\mathbb{Q}(t)$ at all) via theoretical arguments, one may have to look at class 5-tuples.
Indeed one can show, by arguments as developed by Dettweiler in [12], that there is a rational curve on the Hurwitz space for the 5-tuple $(2A, 2A, 2B, 2B, 3B)$ of $PSL_5(2)$ (which also is a genus zero tuple). The "natural" explanation for the existence of this rational curve is the fact that this 5-tuple of classes arises as a rational translate of a 4-tuple of classes in $Aut(PSL_5(2))$. This 4-tuple (of classes $(2A, 2B, 2C, 6)$) has a single braid orbit of length 46; its Hurwitz curve is of genus zero, and the images of the braids in the action on this orbit fulfill an oddness condition to guarantee the rationality of this genus zero curve.
This realizes $Aut(PSL_5(2))$ regularly over $\mathbb{Q}$, and as the $PSL_5(2)$-fixed field of such a realization is a rational function field (of degree 2 over the base field), one also obtains $PSL_5(2)$.[1]

[1] I have not seen this (or any) theoretical argument for the occurrence of $PSL_5(2)$ as a regular Galois group over $\mathbb{Q}$ in the literature, although the necessary criteria are well known.

6.2 Explicit computations

Let $G = PSL_5(2)$, and denote by $2A$ the class of involutions of cycle type $(2^8.1^{15})$, by $3B$ the class of elements of order 3 with cycle type $(3^{10}.1)$ in G, and by $8A$ the unique class of elements of order 8 in G (of cycle type $(8^2.4^3.2.1)$).

We consider the straight Nielsen class $SNi(C)$ of class tuples of length 4, of type $(2A, 2A, 3B, 8A)$ in $G = PSL(5, 2)$, generating G and having product 1, i.e.

$$SNi(C) := \{(\sigma_1, ..., \sigma_4) \in G \mid \sigma_1, \sigma_2 \in 2A, \sigma_3 \in 3B, \sigma_4 \in 8A, \langle\sigma_1, ..., \sigma_4\rangle = G, \sigma_1 \cdots \sigma_4 = 1\}$$

The action of the braid group on $SNi^{in}(C)$ yields the following:

There is a family of covers $\mathcal{T} \mapsto \mathcal{C} \times \mathbb{P}^1\mathbb{C}$, where $\mathcal{C}$ (the C_2-symmetrized reduced Hurwitz space) is an absolutely irreducible curve of genus zero and for every $h \in \mathcal{C}$ the corresponding fiber cover is a Galois cover of $\mathbb{P}^1\mathbb{C}$ with Galois group $PSL_5(2)$.

Although the usual braid genus criteria yield that the C_2-symmetrized Hurwitz space for this family is a genus-zero curve, it does not seem clear via standard theoretical considerations (e.g. odd cycle argument for the braid group generators, as in [39, Chapter III. 7.4.]) whether it can also be defined as a rational curve over $\mathbb{Q}$.

In particular, the cycle structure of the braid orbit generators acting on the Nielsen class does not yield any places of odd degree. More precisely, the image of the braid group is imprimitive on then 24 points, with 12 blocks of length 2 (i.e. if $F|\mathbb{Q}(t)$ is the corresponding function field extension, of degree 24, we have an inclusion $\mathbb{Q}(t) \subset E \subset F$, with $[E : \mathbb{Q}(t)] = 12$ and $[F : E] = 2$). As the images in the action on the blocks of the three braids defining the ramification structure of these fields have cycle structure $(4^2.3.1)$, $(7.3.2)$ and $(2^5.1^2)$ respectively, it is clear that E is still a rational function field; however the cycle structure of the latter involution in the action on 24 points is (2^{12}), so it is possible that a degree-2 place of E ramifies in F, in which case the rationality of F is not guaranteed.[2]

We therefore clarify the rationality of this curve by explicit computation. We start with a degenerate cover with ramification structure $(2A, 21A, 8)$, with group $PSL_5(2)$. We solve the corresponding system of equations for the three-point cover modulo a suitable prime, and then lift and retrieve algebraic numbers from the p-adic expansions.

The triple is rigid, but as the conjugacy class of the element of order 21 is not rational, we obtain

[2] Closer group theoretic examination yields some evidence for prime divisors of odd degree: namely, the two 3-cycles of the braid group generator of cycle structure $(7^2.3^2.2^2)$ correspond to degenerate covers with three ramification points, generating two isomorphic, but *non-conjugate* (in $PSL_5(2)$) subgroups. The same holds for the two 2-cycles of this braid group generator. The explicit computations show, that the corresponding prime divisors of ramification index 3 and 2 respectively are indeed of degree 1.

a solution over a quadratic number field, namely

$$0 = x^{21} \cdot (x-1)^7 \cdot (x-a_1)^3 - t \cdot (x^2 - 2 \cdot x + a_2)^8 \cdot (x^3 - 2 \cdot x^2 + a_3 \cdot x + a_4)^4 \cdot (x - a_5),$$

where $(a_1, ..., a_5) := (\frac{1}{8}(-\sqrt{-7}+11), \frac{1}{16}(-\sqrt{-7}+11), \frac{1}{16}(\sqrt{-7}+21), \frac{1}{128}(-3\sqrt{-7}-31), \frac{1}{8}(-\sqrt{-7}+3))$.

From this degenerate cover, we develop complex approximations for a cover branched in four points, using Puiseux expansions as in the previous chapters.

Let $\mathbb{C}(x)|\mathbb{C}(t)$ be the corresponding field extension of rational function fields for the cover with four branch points. Via Moebius transformations (in x and in t) it is possible to assume a defining polynomial

$$f := f_0(x)^3 \cdot (x-3) - t \cdot g_0(x)^8 \cdot g_1(x)^4 \cdot x,$$

where $deg(f_0) = 10$, $deg(g_0) = 2$ and $deg(g_1) = 3$.
(So we have e.g. assumed the element of order 8 to be the inertia group generator over infinity, and the element of order 3 the one over zero).
Also, assume that for some $\lambda \in \mathbb{C}$ the polynomials

$$f_a := f_0(x)^3 \cdot (x-3) - a \cdot g_0(x)^8 \cdot g_1(x)^4 \cdot x$$

and

$$f_b := f_0(x)^3 \cdot (x-3) - b \cdot g_0(x)^8 \cdot g_1(x)^4 \cdot x$$

(where a and b shall denote the complex zeroes of $x^2 + x + \lambda$) become inseparable in accordance with the elements in the conjugacy class $2A$.

Once we have obtained a complex approximation of such a polynomial f, we now slowly move the coefficient at x^2 of the above polynomial g_1 to a fixed rational value, and apply Newton iteration to expand the other coefficients with sufficient precision to then retrieve them as algebraic numbers (using the LLL-algorithm). One finds that all the remaining coefficients come to lie in a cubic number field. This already indicates that there is a rational function field of index 3 in the (genus-zero) function field of the Hurwitz space, which would enforce the latter function field to be rational over $\mathbb{Q}$ as well. This will be confirmed by the remaining computations.

We now choose a prime p such that the above solution, found over a cubic number field, reduces to an $\mathbb{F}_p$-point. Then we lift this point to sufficiently many p-adic solutions (all coalescing modulo p), in order to obtain algebraic dependencies between the coefficients[3]. These dependencies are all of

[3] Alternatively, one could just repeat the process of rational specialization and Newton iteration, as above, sufficiently often, obtaining cubic minimal polynomials for the other coefficients in each case, and then interpolate.

genus zero, and luckily some of them are of very small degree, e.g. if c_2 and c_1 are the coefficients at x^2 resp. x of the polynomial g_1, one obtains an equation of degrees 2 and 3 respectively.
One can easily find a parameter α for the rational function field defined by this equation, using Riemann-Roch spaces.

Now, we can express all coefficients as rational functions in α, and obtain the following result:

Theorem 6.1. *Let α, t be algebraically independent transcendentals over $\mathbb{Q}$.*
Define elements $a_1, ..., a_{14}$ as follows:

$$
\begin{aligned}
a_1 &:= \frac{2\alpha^4 - 37\alpha^3 - 6\alpha^2 - 109\alpha + 182}{(\alpha - 2) \cdot (\alpha + 1)^2}, \\
a_2 &:= -12 \cdot \frac{(\alpha^2 - 5/2 \cdot \alpha - 8) \cdot (\alpha^3 + 10 \cdot \alpha^2 + 17 \cdot \alpha + 44)}{(\alpha - 2) \cdot (\alpha + 1) \cdot (\alpha + 4)}, \\
a_3 &:= \frac{-8\alpha^6 + 372\alpha^5 + 1044\alpha^4 + 5372\alpha^3 + 2028\alpha^2 + 7704\alpha - 24608}{(\alpha - 2) \cdot (\alpha + 1) \cdot (\alpha + 4)}, \\
a_4 &:= \frac{62\alpha^9 + 318\alpha^8 - 2820\alpha^7 - 7668\alpha^6 - 61194\alpha^5 - 105810\alpha^4 - 144960\alpha^3 - 100392\alpha^2 + 512448\alpha - 112768}{(\alpha - 2)^2 \cdot (\alpha + 1) \cdot (\alpha + 4)^2}, \\
a_5 &:= \frac{-36\alpha^9 - 1446\alpha^8 - 2712\alpha^7 - 6252\alpha^6 - 17796\alpha^5 + 115914\alpha^4 + 154464\alpha^3 + 698232\alpha^2 + 616128\alpha - 371328}{(\alpha - 2)^2 \cdot (\alpha + 4)^2}, \\
a_6 &:= \frac{(\alpha + 1)^2 \cdot (-92\alpha^7 + 1348\alpha^6 + 948\alpha^5 + 8300\alpha^4 + 30896\alpha^3 - 8664\alpha^2 + 142960\alpha - 176192)}{(\alpha - 2)^2 \cdot (\alpha + 4)}, \\
a_7 &:= \frac{(\alpha + 1)^3 \cdot (152\alpha^7 + 20\alpha^6 - 1956\alpha^5 - 1628\alpha^4 - 17468\alpha^3 - 30144\alpha^2 - 23056\alpha - 185536)}{(\alpha - 2)^2 \cdot (\alpha + 4)}, \\
a_8 &:= \frac{(\alpha + 1)^4 \cdot (-87\alpha^6 - 288\alpha^5 - 198\alpha^4 - 1596\alpha^3 + 9\alpha^2 - 900\alpha - 14172)}{(\alpha - 2)^2}, \\
a_9 &:= \frac{(\alpha + 1)^6 \cdot (18\alpha^5 + 159\alpha^4 + 420\alpha^3 + 999\alpha^2 + 2256\alpha + 564)}{(\alpha - 2)^2}, \\
a_{10} &:= -6 \cdot \frac{(\alpha + 1)^9 \cdot (\alpha + 4)}{\alpha - 2}, \\
a_{11} &:= -(\alpha + 1)^2, \\
a_{12} &:= \frac{(\alpha + 1) \cdot (\alpha^2 - 16 \cdot \alpha - 8)}{(\alpha - 2) \cdot (\alpha + 4)}, \\
a_{13} &:= -3(\alpha + 1)^2, \\
a_{14} &:= \frac{(\alpha + 1)^3 \cdot (\alpha + 4)}{\alpha - 2}.
\end{aligned}
$$

and set

$$f_0 := x^{10} + a_1 x^9 + ... + a_{10},$$

$$g_0 := x^2 - 6x + a_{11},$$

$$g_1 := x^3 + a_{12} x^2 + a_{13} x + a_{14}.$$

Then the polynomial $f(x, \alpha, t) := f_0^3 \cdot (x-3) - t \cdot g_0^8 \cdot g_1^4 \cdot x$, of degree 31 in x, has Galois group $PSL_5(2)$ over $\mathbb{Q}(\alpha, t)$.

Proof. Dedekind reduction, together with the list of primitive groups of degree 31, shows that $PSL_5(2)$ must be a subgroup of the Galois group. It therefore suffices to exclude the possibilities A_{31} and S_{31}.
Multiplying t appropriately, we can assume the covers to be ramified in $t = 0, t = \infty$ and the zeroes of $t^2 + t + \lambda$, with some parameter λ. Interpolating through sufficiently many values of α one finds the degree-24 rational function $\lambda = \frac{h_1(\alpha)}{h_2(\alpha)}$ parameterizing the Hurwitz curve. As e.g. $\alpha = 0$ and $\alpha = 1/2$ yield the same value for λ, we set $t = C \cdot (\frac{f_0^3 \cdot (x-3)}{g_0^8 \cdot g_1^4 \cdot x})(s, 0)$ (evaluating x to a parameter s of a rational function field, as well as α to 0, and multiplying with a suitable constant C to obtain the above condition on the branch points). Then one can check that over $\mathbb{Q}(s)$, the polynomial $f(x, 1/2, C_2 \cdot t)$ (again for suitable constant C_2 to obtain the branch point conditions) splits into two factors of degrees 15 and 16. This means that for this particular point of the family, there is an index-31 subgroup of the Galois group that acts intransitively on the roots. As $PSL_5(2)$ has such a subgroup and A_{31} and S_{31} don't, the Galois group for this particular specialization is $PSL_5(2)$. This specialization corresponds to an unramified point on the (irreducible) Hurwitz space, therefore the entire family must belong to the same Hurwitz space and therefore have Galois group $PSL_5(2)$ over $\mathbb{Q}(\alpha, t)$. □

We can now specialize α to any value that does not let two or more ramification points coalesce, to obtain polynomials with nice coefficients with group $PSL_5(2)$ over $\mathbb{Q}(t)$.
e.g. $\alpha \mapsto 0$ leads to

$$\tilde{f}(x, t) := (x^5 - 95 \cdot x^4 - 110 \cdot x^3 - 150 \cdot x^2 - 75 \cdot x - 3)^3 \cdot (x^5 + 4 \cdot x^4 - 38 \cdot x^3 + 56 \cdot x^2 + 53 \cdot x - 4)^3 \cdot (x - 3)$$

$$-t \cdot (x^2 - 6x - 1)^8 \cdot (x^2 - x - 1)^4 \cdot (x + 2)^4 \cdot x.$$

In fact it can be seen from $\lambda = \frac{h_1(\alpha)}{h_2(\alpha)}$ (as in the proof above) that the only specialized rational values for α that lead to degenerate covers (with two branch points coalescing) are $\alpha \mapsto -4$, $\alpha \mapsto -1$ and $\alpha \mapsto 2$.

Remarks:

a) The above proof essentially uses the fact that $PSL_5(2)$ has two non-conjugate actions on 31 points inducing the same permutation character. This can of course be applied to other linear groups, and has e.g. been used in [35] to verify $PSL_2(11)$ (and others) as the Galois group of a family of polynomials. Cf. also the Galois group verifications in the following chapters.

b) In fact, the polynomials f_0 and g_1 given above are still reducible (compare the specialized polynomial $\tilde{f}(x, t)$!). This is because of the action of the decomposition groups. E.g., the

normalizer in $PSL_5(2)$ of a subgroup generated by an element of cycle structure $(3^{10}.1)$ does not permute the 10 orbits of lengths 3 transitively.
Therefore $f(x, \alpha, t)$ can be decomposed in the following way:

$$\begin{gathered}
f = (x-3) \cdot (x^5 - 2\frac{(\alpha+1)(\alpha+4)}{\alpha-2}x^4 - 2\frac{(\alpha+1)(\alpha^3-15\alpha^2-6\alpha-152)}{(\alpha-2)(\alpha+4)}x^3 \\
+8(\alpha+1)(\alpha^2-\alpha+7)x^2 - 7\frac{(\alpha+1)^2(\alpha^3+12/7\cdot\alpha^2+3/7\cdot\alpha+106/7)}{\alpha-2}x + 2\frac{(\alpha+1)^5(\alpha+4)}{\alpha-2})^3 \\
\cdot(x^5 + 4\frac{(\alpha-5)(\alpha^2+5/4\cdot\alpha+19/4)}{(\alpha+1)^2}x^4 - 2\frac{\alpha^3+42\alpha^2+45\alpha+220}{\alpha+4}x^3 \\
-12\frac{(\alpha+1)(\alpha^4-5/2\cdot\alpha^3-27/2\cdot\alpha^2-29\alpha-100)}{(\alpha-2)(\alpha+4)}x^2 + 9\frac{(\alpha+1)^2(\alpha^3+8/3\cdot\alpha^2+19/3\cdot\alpha+50/3)}{\alpha-2}x - 3(\alpha+1)^4)^3 \\
-t \cdot (x^2 - 6x - (\alpha+1)^2)^8 \cdot (x - \frac{(\alpha+1)(\alpha+4)}{\alpha-2})^4 \cdot (x^2 - 2\frac{(\alpha-2)(\alpha+1)}{\alpha+4}x - (\alpha+1)^2)^4 \cdot x
\end{gathered}$$

Chapter 7

Polynomials with Galois group $PSL_3(4) \leq G \leq P\Gamma L_3(4)$ over $\mathbb{Q}(t)$

We compute the Hurwitz space of a family of covers with Galois group $P\Gamma L_3(4)$, ramified over four places with monodromy $(2^8.1^5, 2^7.1^7, 3^5.1^6, 6^2.3^2.2.1)$. This Hurwitz space is a rational curve and therefore has many rational points. This will lead to polynomials with regular Galois group G for all $PSL_3(4) \leq G \leq P\Gamma L_3(4)$. For the groups $PSL_3(4)$, $PGL_3(4)$ and $P\Gamma L_3(4)$, these are, to my knowledge, the first explicit polynomials over $\mathbb{Q}(t)$. Malle gave a polynomial for $PSL_3(4).2$ in ([36]), but this does not yield a $PSL_3(4)$-polynomial, as the $PSL_3(4)$-fixed field does not have genus 0 (see however [57] for a way to obtain from Malle's polynomial a $PSL_3(4)$-polynomial over $\mathbb{Q}$ (not $\mathbb{Q}(t)$).

Theoretical arguments for all $PSL_3(4) \leq G \leq P\Gamma L_3(4)$ to be a regular Galois group over $\mathbb{Q}(t)$ have however been known for a long time (cf. [39], Example 4.2. in Chapter IV.4).

7.1 A theoretical existence argument

Let $G = P\Gamma L_3(4)$, acting on $21 = \frac{4^3-1}{4-1}$ points, C_1 be the unique class of involutions in G with 5 fixed points, C_2 the unique class of involutions with 7 fixed points, C_3 the class of elements of order 3 with 6 fixed points and C_4 the class of elements of order 6, with cycle structure $(6^2.3^2.2.1)$. Then there are, modulo simultaneous conjugacy in G, 54 tuples $(\sigma_1, ..., \sigma_4) \in C_1 \times ... \times C_4$ with product $\sigma_1 \cdot ... \cdot \sigma_4 = 1$ and $\langle \sigma_1, ...\sigma_4 \rangle = G$. They form a single orbit under the action of the Hurwitz braid group, and the braids β_{1i} have the cycle structures $(3^{12}.2^8.1^2)$, $(5^4.3^8.2^5)$ and $(4^{10}.2^7)$ (for $i = 2, 3, 4$ respectively).

Therefore the braid orbit genus is zero, and indeed the corresponding Hurwitz curve is a rational curve because the corresponding function field has places of odd degree over two of the ramified places. So there are many rational points on this curve, yielding many polynomials $f(X, t) \in$

$\mathbb{Q}(t)[X]$ with (regular) Galois group $P\Gamma L_3(4)$.
Let $E \supset \mathbb{Q}(t)$ be the fixed field of $PSL_3(4) \triangleleft G$ for such a polynomial. Then the extension $E \mid \mathbb{Q}(t)$ is ramified over at most four places (all of which are of degree 1), with ramification structure given by the cycle structure of the σ_i in the coset action on $G/PSL_3(4)$.
The image of σ_1 is the identity (as σ_1 lies in $PSL_3(4)$), the other elements have images of cycle structure (2^3), (3^2) and (2^3) respectively.
This means that the genus of E is zero, and E is a rational function field, as there are places of odd degree over two of the ramified places.
So there is $s \in E$ such that $E = \mathbb{Q}(s)$, and therefore the splitting field of $f(X,t)$ is a regular Galois extension of $\mathbb{Q}(s)$ with group $PSL_3(4)$.

7.2 A reducible three point cover

We start with a cover ramified over three points, with ramification structure of cycle type $(4^4.2.1^3, 3^5.1^6, 6^2.3^2.2.1)$. More precisely, let

$$\sigma_1 := (1,16)(4,20)(5,17)(6,13)(7,8)(9,19)(10,11)(12,18),$$

$$\sigma_2 := (2,12)(3,18)(4,14)(5,17)(7,16)(11,19)(20,21),$$

$$\tau := \sigma_1 \cdot \sigma_2 = (\sigma_3 \cdot \sigma_4)^{-1} = (1,7,8,16)(2,12,3,18)(4,21,20,14)(6,13)(9,11,10,19),$$

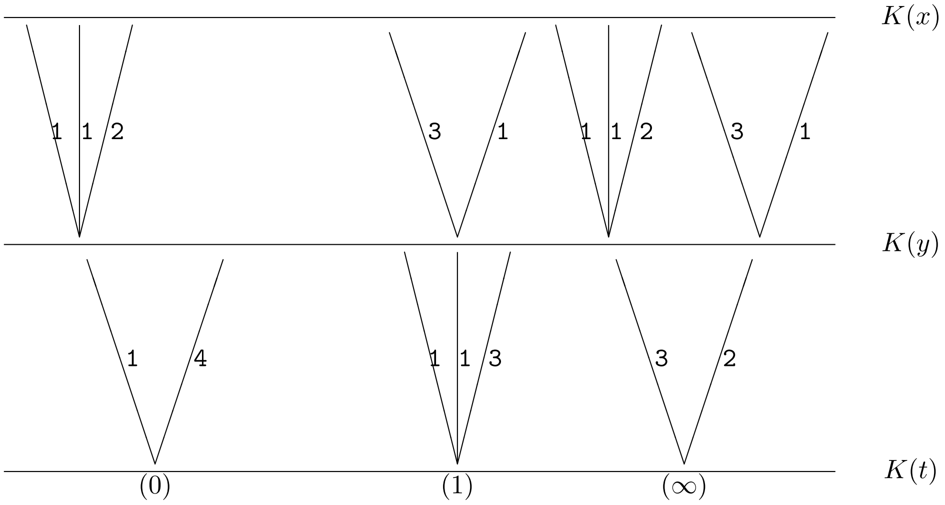
$$\sigma_3 := (1,17,11)(4,16,10)(6,8,18)(12,19,13)(14,21,15),$$

$$\sigma_4 := (1,9,19,2,18,7)(3,12,6)(4,11,17,16,14,15)(8,13,10)(20,21).$$

The group generated by σ_3 and σ_4 acts intransitively, with orbits of length 20 and 1, therefore the corresponding cover will be reducible with components of degree 20 and 1. Moreover the action on the orbit of length 20 is imprimitive, with five blocks of length 4. Observe also that the genus zero condition is fullfilled by the tuple $(\tau, \sigma_3, \sigma_4)$, restricted to this orbit. Therefore this component is given by an equation $t = \frac{p(y)}{q(y)}$, where $y = \frac{r(x)}{s(x)}$, with polynomials $p, q, r, s \in \overline{\mathbb{Q}}[X]$. Thus we are left with computing rational covers of degrees 4 and 5, given by the ramification structure depicted in Fig. 7.1.

The degree-5 cover corresponds to a (non-rigid) triple in S_5 and can be easily computed over a quadratic number field.
The degree-4 cover with four branch points (whose position is determined by the degree-5 cover) belongs to a family of S_4-covers of length 6. This still can be easily computed with the standard Groebner basis approach. One can then compute the monodromy numerically for each of the six covers, to find out which one belongs to the monodromy we are looking for.
Next, after applying suitable Moebius transformations in x (to fix three points via $PGL_2(\mathbb{C})$-action),

Figure 7.1: Ramification structure corresponding to the orbit of length 20



develop a polynomial equation $f(X) - tg(X) = 0$ for a cover ramified over four points.
The cycle structure of the inertia group generators and the orbits of their normalizers in $P\Gamma L_3(4)$ tell us that we can w.l.o.g. set

$$f(X) = \alpha \cdot f_1(X)^2 \cdot f_2(X),$$

with a leading coefficient α and monic polynomials f_1, f_2 of degree 7, as well as

$$g(X) = (X + a_1)^6 \cdot (X + a_2)^6 \cdot (X + a_3)^3 \cdot (X - 1)^3 \cdot X,$$

with coefficients a_1, a_2, a_3.
Furthermore, as the ramification index in the Hurwitz space (at the degenerate cover we started with) is $e = 4$, assume that

$$f(X) - \mu^4 g(X) = \alpha \cdot h_1(X)^2 \cdot h_2(X) \cdot h_3$$

and

$$f(X) - g(X) = \alpha \cdot h_4(X)^3 \cdot h_5(X) \cdot h_6(X)$$

with monic polynomials h_i of degrees 8, 4, 1, 5, 5 and 1 respectively (again, compare the orbit lengths of the normalizers $N_{P\Gamma L_3(4)}(\langle \sigma_i \rangle)$!).
Now, observe the cycle structure more closely:
The group $\langle \sigma_1, \sigma_2 \rangle$ has four orbits of length 4, two of length 2, and one fixed point.

All but one of these orbits (namely the orbit $\{5, 17\}$) are contained in the length 20 orbit of the group $\langle \sigma_1\sigma_2, \sigma_3, \sigma_4 \rangle$.
For these orbits, we can introduce parameter transformations, i.e. introduce coordinates

$$Y_i := \mu^{-4/f_i} \cdot (X - \zeta_i)$$

where $x \mapsto \zeta_i$ is a place of ramification index f_i over $t \mapsto 0$ of the degenerate cover computed above, just as in Section 3.3.1.
This yields approximations for all but one of the roots of $f(X)$ (and of $f(X) - \mu^4 g(X)$). We are left with the last orbit $\{5, 17\}$. As 5 is a fixed point of $\sigma_1\sigma_2$, the corresponding place $x \mapsto \zeta_0$ of the degenerate cover is unramified, so the corresponding root ζ (of multiplicity 2) of the polynomial $f(X)$ for the non-degenerate cover should be expected to be developed as a power series in μ^4, i.e. in particular:

$$\zeta = \zeta_0 + O(\mu^4),$$

and analogously for the corresponding root of $f(X) - \mu^4 g(X)$.
Therefore, introduce a coordinate $Y_0 := \mu^{-4} \cdot (X - \zeta_0)$. By the cycle structures of σ_1 and σ_2, we know that for $\mu \to 0$, the function $s := \mu^{-4} t = \mu^{-4} \frac{f(X)}{g(X)}$, seen as a function in Y_0, converges w.l.o.g. to a function s_0 of the form $s_0 = \alpha \frac{(Y_0 - \beta)^2}{Y_0}$ (with some $\alpha, \beta \in \mathbb{C}$).
This yields the missing component for the cover with group $\langle \sigma_1\sigma_2, \sigma_3, \sigma_4 \rangle$. Namely set

$$\tilde{X} := \mu^{-4} Y_0 = \mu^{-8}(X - \zeta_0)$$

Then $t = \frac{f(X)}{g(X)}$, seen as a function in $\tilde{X}$, should converge to a fractional linear function as μ tends to zero.
Therefore, the missing root of the polynomial $g(X)$ (of multiplicity 1, corresponding to the orbit $\{5\}$ of $\langle \sigma_3, \sigma_4 \rangle$) must be of the form $(X - \zeta_0 + O(\mu^8))$, and analogously for the missing root of the polynomial $f(X) - g(X)$.

Now we have approximated the four point cover with sufficient precision to again start Newton iteration.

7.3 Hurwitz space and braid group action

Once we have obtained a complex approximation of a four point cover, we look for algebraic relations: By letting one of the branch points move, we move the above coefficient $-a_1$ (6-fold root of the polynomial $g(X)$) to a rational value, and develop the remaining coefficients with sufficient precision to recognize them as algebraic numbers with the help of the LLL-algorithm.
In this case we obtain polynomials of degree 5 (which suggests that the function field $K|\mathbb{Q}$ corre-

sponding to the Hurwitz curve has degree 5 over the field generated by a_1). Now we look for a prime p such that all these polynomials have a root modulo p, and ideally only one root, so that there is no need to guess how to combine the roots of the different polynomials. This worked in our case for $p = 17$, and we hence obtained an $\mathbb{F}_{17}$-cover ramified over 4 points with the prescribed ramification structure.

Lifting this cover (ramified over, say $t \in \{0, 1, \infty, a\}$ with $a \in \mathbb{F}_{17}$) to many different 17-adic approximations (e.g. ramified over $t \in \{0, 1, \infty, a + k \cdot 17\}$ for many $k \in \mathbb{Z}$) allows us to obtain algebraic dependencies between pairs of coefficients of the above model. As all of these dependencies define a rational curve, there exists a parameter α such that all of these coefficients are rational functions in α.

We find α e.g. by first finding an equation $F(a_1, a_2) = 0$ over $\mathbb{Q}$ for the coefficients a_1 and a_2 (this works with relative degrees 5 and 7), and then computing elements in Riemann-Roch spaces as in Lemma 3.16.

Once the parameter α is found, we can express all the coefficients of the model as rational functions in α to obtain a family of polynomials $f_\alpha(X) - t \cdot g_\alpha(X)$, with $f_\alpha, g_\alpha \in \mathbb{Q}(\alpha)[X]$.

As the polynomials f_α and g_α are not very nice (particularly because large degrees in α occur), we only include them in plain text format, in the file "pgammal34_family.txt".

In particular, the value of the fourth (moving) branch point can be expressed as a rational function of degree 54 in α. The ramification behaviour of this function is given by the braid group action, so one can double-check with the group theoretical information already known.

7.4 Rational points

While it seems that the whole family $f_\alpha - t \cdot g_\alpha$ can only be parameterized with rather large coefficients, certain specializations of small values of α lead to relatively small coefficients, and also allow for a nice verification that the Galois group is indeed $P\Gamma L_3(4)$, without computing monodromy.

E.g. in our model, the values $-\frac{1}{7}$ and $-\frac{5}{3}$ for α lead to the same branch points (i.e. they lie in the same fiber of the cover $\mathcal{C} \to \mathbb{P}^1$ of the Hurwitz curve).

Theorem 7.1. *The polynomial $F_\alpha(X, t) := f_\alpha(X) - t \cdot g_\alpha(X)$ given in the file "pgammal34_family.txt" has regular Galois group $P\Gamma L_3(4)$ over $\mathbb{Q}(\alpha, t)$.*

Proof. Specializing in appropriate finite fields, one sees that the Galois group is either $P\Gamma L_3(4)$ or S_{21}.

Now $P\Gamma L_3(4)$ has two non-conjugate subgroups U and V of index 21. If one considers the action of $P\Gamma L_3(4)$ on the right cosets of U, then V is intransitive with orbits of length 5 and 16. The images of the desired inertia subgroup generators $\sigma_1, ..., \sigma_4$ in the action on the cosets of V are still of the

same cycle type, and therefore belong to the same family of covers, but not to the same cover. We use this to show that the group belonging to our polynomial is indeed $P\Gamma L_3(4)$:
Let

$$\begin{aligned}\widehat{F}(X,s) := &-\frac{2582417876931378942785781 76}{230141841324943480613305664 0625}\cdot(s^5+\frac{889225}{17248}\cdot s^4-\frac{5839592406875}{1969626736}\cdot s^3+\frac{1005374606421875}{96511710064}\cdot s^2\\ &-\frac{14538493015527734375}{747193659315488}\cdot s+\frac{2558247783203125}{2364536896568})^3\cdot(s^5+\frac{1448962213075}{4616461696}\cdot s^4+\frac{8598644802030578125}{383399661922816}\cdot s^3\\ &-\frac{4538461492895816100734375}{13225754737689460736}\cdot s^2+\frac{6906167545351709822253906 25}{6480619821467835760 64}\cdot s-\frac{691752662812901016601562 5}{6612877368844730368})\\ &\cdot(s+\frac{3950}{343})\cdot(x+\frac{433}{392})^6(x-\frac{866}{2891})^6(x-\frac{433}{1225})^3(x-1)^3\cdot x+\frac{1261480906940392369068457984}{3682269461199095689812890625}\\ &\cdot(x^5+\frac{31775}{20384}\cdot x^4-\frac{1661535745}{2327740688}\cdot x^3+\frac{44439580225}{114059293712}\cdot x^2-\frac{354236407848965}{659490836242784}\cdot x+\frac{386673376331}{2794452695944})^3\\ &\cdot(x^5+\frac{2346471805}{5690968192}\cdot x^4-\frac{3494659178827295}{2599509068805376}\cdot x^3-\frac{4851810841101758405}{1630412087954731827 2}\cdot x^2\\ &+\frac{3836442063408152449 75}{7989019230978185953 28}\cdot x-\frac{708354726720410641}{8152060439773659136})\cdot(x-\frac{118}{343})\cdot(s+\frac{1675}{392})^6(s-\frac{16750}{3871})^6(s+\frac{8375}{49})^3(s-1)^3\cdot s.\end{aligned}$$

(As mentioned above, this essentially corresponds to considering the algebraic dependencies $F_{-5/3}(X,t)=0$ and $F_{-1/7}(s,t)=0$.)
Then $\widehat{F}$ is reducible with factors of degrees 5 and 16. This shows that there is an index-21 subgroup in $Gal(F_{-5/3}|\mathbb{Q}(t))$, acting intransitively. As S_{21} does not have such a subgroup, the Galois group must be $P\Gamma L_3(4)$. This is therefore the Galois group of F_α over $\mathbb{Q}(\alpha,t)$ as well.
So we know F_α has arithmetic monodromy group $P\Gamma L_3(4)$, and the geometric monodromy group is a normal subgroup of it. However, the ramification type $(2^8.1^5, 2^7.1^7, 3^5.1^6, 6^2.3^2.2.1)$ is not possible for any proper normal subgroups, so $P\Gamma L_3(4)$ is also the geometric monodromy group, and therefore regular. □

Upon some further Moebius transformations in X and t, the above polynomial $F_{-5/3}(X,t)$ can be simplified somewhat more to obtain

$$\begin{aligned}\tilde{F}(X,t) := (X^5+\frac{5131}{320}\cdot X^4-\frac{38139}{500}\cdot X^3+\frac{18762}{3125}\cdot X^2-\frac{216664}{15625}\cdot X+\frac{27136}{15625})^3\cdot\\ (X^5+\frac{12301781}{622080}\cdot X^4+\frac{326413663}{3779136}\cdot X^3-\frac{285841817}{2460375}\cdot X^2-\frac{68955968}{12301875}\cdot X-\frac{11505664}{36905625})\cdot(X+\frac{424}{9})\\ -t\cdot X^6\cdot(X+8)^6\cdot(X-1)^3\cdot(X-\frac{192}{625})^2\cdot(X+\frac{24}{25})\end{aligned}$$

with Galois group $P\Gamma L_3(4)$ over $\mathbb{Q}(t)$.

7.5 Descent to proper normal subgroups of $P\Gamma L_3(4)$

As the ramification structure shows, the fixed fields of the above polynomial $\tilde{F}$ (and more generally, of the entire family of polynomials) under action of $PSL_3(4)$ is still a rational function field over $\mathbb{Q}$. If s is a parameter of this field, t can be expressed as a rational function in s, and plugging this into the equation $\tilde{F}(X, t(s)) = 0$ then yields a polynomial with (regular) Galois group $PSL_3(4)$ over $\mathbb{Q}(s)$.
Analogously one also obtains a polynomial with group $PGL_3(4)$.

Applying a suitable Moebius transformation to the parameter t, we can shift the ramification locus such that the $PSL_3(4)$-fixed field $E \mid \mathbb{Q}(t)$ is ramified over $(0, 1, \infty)$. In our concrete example, this can be done by replacing $\tilde{F}$ with $\tilde{F}(X, (-12930877668957043849/3249918613389312) \cdot (t-1))$. So we only need to find the defining equation $t = \frac{a(s)}{b(s)}$ for the $PSL_3(4)$-fixed field $E = \mathbb{Q}(s)$. It holds that $Gal(E \mid \mathbb{Q}(t)) = S_3$, acting regularly (and therefore imprimitively) on six points. After the above shift of the ramification locus, the branch cycles of $E \mid \mathbb{Q}(t)$ over $t \mapsto 0$, $t \mapsto 1$ and $t \mapsto \infty$ are of cycle type (2^3), (3^2) and (2^3) respectively.
Again by choosing suitable parameters, we can w.l.o.g. assume that $t = -\frac{1}{27}\frac{(as^2-9)^2 \cdot as^2}{(as^2-1)^2}$, with some $a \in \mathbb{Q}$. To find the correct a, we look at the decomposition group of a place of E over $t \mapsto \infty$. This group contains the inertia group as a normal subgroup. However the inertia subgroup is generated by an involution in S_3 and is therefore self-normalizing, so the decomposition group is equal to it. Therefore, all three places of E over the infinite place must be of degree one, i.e. they correspond to rational values $s \mapsto s_i \in \mathbb{Q}$. In particular, a must be a rational square, and in fact (again by a suitable Moebius transformation) it may be chosen as any rational non-zero square, so we can set $a = 1$, and finally obtain the following polynomial, having regular Galois group $PSL_3(4)$ over $\mathbb{Q}(s)$:

$$g(X, s) := \tilde{F}(X, (-12930877668957043849/3249918613389312) \cdot (t(s) - 1)),$$

with $t(s) = -\frac{1}{27}\frac{(s^2-9)^2 \cdot s^2}{(s^2-1)^2}$.

Similarly the fixed field of $PGL_3(4)$ is a rational extension of degree 2 over $\mathbb{Q}(t)$, ramified only over 0 and ∞. By the previous definition of the parameter s for the PSL-fixed field, $\tilde{s} := \frac{1}{9}\frac{(s^2-9)\cdot s}{s^2-1}$ is a parameter for the PGL-fixed field, and $t := t(\tilde{s}) := -3\tilde{s}^2$. We thus obtain the Galois group $PGL_3(4)$ over $\mathbb{Q}(\tilde{s})$.

7.6 Totally real specializations

Reality arguments show that some of the members of the above family of polynomials have totally real fibers. Suitable specialization of the parameters α and t yields totally real polynomials with Galois group $P\Gamma L_(3, 4)$ over $\mathbb{Q}$. Rational translates as above then lead to totally real polynomials

for $PSL_3(4)$ and $PGL_3(4)$ as well.
The polynomial $F_{-\frac{1}{4}}(X,t)$ (as defined in the file "`pgammal34_family.txt`") is one possible example for a $P\Gamma L_(3,4)$-polynomial with real fibers; these fibers occur in the interval $(-360318.9..., -267577.8...)$, the interval between the only two negative real branch points. By a suitable version of Hilbert's irreducibility theorem, the set of specializations $t \mapsto t_0 \in \mathbb{Q}$ that preserve the Galois group is dense, yielding many totally real $P\Gamma L_3(4)$-polynomials $f(X,t_0)$ over $\mathbb{Q}$.
Similarly, suitable rational functions $t(s)$ lead to polynomials $F_{-\frac{1}{4}}(X,t(s))$ with groups $PGL_3(4)$ resp. $PSL_3(4)$ over $\mathbb{Q}(s)$, and real fibers in appropriate open intervals (namely in any connected component of the preimage of $(-360318.9..., -267577.8...)$ under $s \mapsto t(s)$, which is automatically real as $\mathbb{Q}(s)$ is contained in the Galois closure of $F_{-\frac{1}{4}}$ over $\mathbb{Q}(t)$).

Chapter 8

Totally real extensions with groups $PGL_2(11)$ and $PSL_3(3)$

Here we compute explicit totally real polynomials with Galois groups $PGL_2(11)$ and $PGL_3(3)$ over $\mathbb{Q}$.[1]

As these groups are the smallest (with respect to minimal faithful permutation degree) that have not been previously realized as the Galois group of a totally real extension of $\mathbb{Q}$, this means that explicit totally real polynomials are now known for every transitive permutation group of degree at most 13 (cf. [30]).

8.1 The case $G = PGL_2(11)$

The problem for the group $PGL_2(11)$ is that, on the one hand, to obtain totally real fibers (i.e. a complex conjugation acting as the identity) one needs to compute polynomials with at least four branch points. On the other hand $PGL_2(11)$ in its natural action has no generating genus zero tuples of length $r \geq 4$.
There are however genus zero tuples in the imprimitive action on 22 points, which stems from the exceptional action of $PSL_2(11)$ on 11 points.
Below are explicit computations for two such class tuples:

a) Let $C = (2A, 2B, 2B, 3A)$ the quadruple of classes of $PGL_2(11)$, where $3A$ is the unique class of elements of order 3, $2A$ is the class of involutions inside $PSL_2(11)$, and $2B$ the class of involutions outside $PSL_2(11)$. This is a genus zero tuple in the imprimitive action on 22 points, so for a degree-22 cover of $\mathbb{P}^1(\mathbb{C})$ with this ramification type, we get the following

[1] I am indebted to J. Klüners who mentioned these open cases to me.

inclusion of function fields: $\mathbb{C}(t) \subseteq \mathbb{C}(s) \subseteq \mathbb{C}(x)$, where exactly two places of $\mathbb{C}(t)$ ramify in $\mathbb{C}(s)$ (namely the ones with inertia group generator not contained in $PSL_2(11)$), and exactly four places of $\mathbb{C}(s)$ ramify in $\mathbb{C}(x)$ (namely two places lying over the ramified place of $\mathbb{C}(t)$ with inertia group generator in $2A$, and two lying over the place of $\mathbb{C}(t)$ with inertia group generator $3A$).

The essential task is therefore to compute the extension $\mathbb{C}(x)|\mathbb{C}(s)$, i.e. to compute polynomials with $PSL_2(11)$-monodromy, defined over $\mathbb{Q}$ if possible, and ramification type $(2A, 2A, 3A, 3A)$. The straight inner Nielsen class of these tuples in $PSL_2(11)$ is of length $|SNi^{in}| = 54$, with transitive braid group action and symmetrized braid orbit genus $g_{12} = 1$.[2]
Via Moebius transformations, we therefore assume that the two places of $\mathbb{C}(s)$ with inertia group generator of order 3 are $s \mapsto 0$ and $s \mapsto \infty$, and also fix the sum of the other two branch points.
As the cycle structure of an element σ in the class $3A$ of $PSL_2(11)$ in the action on 11 points is $(3^3.1^2)$, and one of the 3-cycles remains fixed under conjugation with $N_{PSL_2(11)}(\langle\sigma\rangle)$ (and therefore under the action of the decomposition subgroup), one can assume w.l.o.g. for a model over $\mathbb{Q}$ that the place $x \mapsto 0$ lies over $s \mapsto 0$ (with ramification index 3), and the same for $x \mapsto \infty$ and $s \mapsto \infty$.
I.e. we may w.l.o.g. look for polynomial equations $x^3 \cdot f_1(x)^3 \cdot f_2(x) - s \cdot g_1(x)^3 \cdot g_2(x) = 0$, with quadratic polynomials f_i, g_i.

Now we searched for a mod-p reduced polynomial with the above restrictions on places and the correct ramification: there is a solution over $\mathbb{F}_7$. (Alternatively, start with a three point cover, as in previous sections.)

Now lift this solution to many approximate $\mathbb{Q}_7$-solutions, with the set of zeroes of $s\cdot(s^2+4s+\lambda)$ as the finite ramification locus (for many different values of λ).
Interpolation then yields an algebraic dependency between the coefficients at x^1 of the above polynomials g_1 and g_2, namely:
$(88/19 \cdot \beta^2 - 112/19 \cdot \beta + 32/19) \cdot \alpha^4 + (178/19 \cdot \beta^3 - 524/19 \cdot \beta^2 + 446/19 \cdot \beta - 112/19) \cdot \alpha^3 + (287/38 \cdot \beta^4 - 650/19 \cdot \beta^3 + 2051/38 \cdot \beta^2 - 662/19 \cdot \beta + 295/38) \cdot \alpha^2 + (59/19 \cdot \beta^5 - 687/38 \cdot \beta^4 + 773/19 \cdot \beta^3 - 1675/38 \cdot \beta^2 + 435/19 \cdot \beta - 173/38) \cdot \alpha + 10/19 \cdot \beta^6 - 70/19 \cdot \beta^5 + 21/2 \cdot \beta^4 - 595/38 \cdot \beta^3 + 491/38 \cdot \beta^2 - 213/38 \cdot \beta + 1 = 0$,
(with α the coefficient of g_1 and β the one of g_2).

Computation with Magma confirms that this defines (the affine part of) an elliptic curve of rank 1, which therefore has infinitely many points. Furthermore all other coefficients of the

[2] Additional symmetrization of the branch points 3 and 4 does not decrease this genus.

model can be expressed as polynomials in α and β, therefore this curve is already a model of the reduced Hurwitz curve of the $PSL_2(11)$-family. So there are infinitely many equivalence classes of covers defined over $\mathbb{Q}$ with this monodromy.

However, as we are interested in totally real polynomials, we need to choose a point on the curve in such a way, that complex conjugation on a fiber of the corresponding $PSL_2(11)$-cover is trivial in at least one segment of the punctured projective line.

Monodromy computations show that $\alpha = -\frac{3}{121}$ and $\beta = \frac{41}{55}$ yields such a point.
This leads to the polynomial

$$\begin{aligned} f(s,x) := x^3 \cdot (x^2 + x - \frac{413}{4114})^3 \cdot (x^2 - \frac{23}{726}x + \frac{63}{181016}) \\ -s \cdot (x^2 - \frac{3}{121}x + \frac{567}{1131350})^3 \cdot (x^2 + \frac{41}{55}x - \frac{413}{102850}), \end{aligned} \tag{8.1}$$

where specializations of s in the real interval $[-0.623.., -0.619..]$ (between the two algebraically conjugate branch points) lead to totally real fibers.

Now all that is left is to parameterize the above extension $\mathbb{C}(s)|\mathbb{C}(t)$ over $\mathbb{Q}$ to fit the positions of the branch points. This is fulfilled by

$$t := (s^2 + \frac{27280791476537}{21954955473000}s + \frac{7663094829906 25}{1985274409206528})/s$$

Plugging this into the above representation of s as a rational function in x, one obtains a degree 22 polynomial with regular Galois group $PGL_2(11)$.
Again, suitable specialization of t allows for totally real fibers: specialize $t \in \mathbb{R}$ larger than the largest real branch point; we did this for $t = 2^{18}$, and then used the routine "**GaloisSubgroup**" in Magma (and some linear transformations) to obtain a polynomial of degree 12, corresponding to the fixed field of the point stabilizer in the natural action of $PGL_2(11)$:

$$\begin{gathered} f_0(x) := x^{12} + 216250195584 \cdot x^{11} + 21291817873540566002688 \cdot x^{10} + 1262778206854960806932246495923934 \cdot x^9 + \\ 50268664952573858629713482778423482951953488 \cdot x^8 + 1415634612352514779876789551323009883253639347560868864 \cdot x^7 + \\ 28930440059668616621092488467714110337841840975066915742747362505 \cdot x^6 + \\ 432463499487244750087709846142904361549647160003627991051838740695470469544 \cdot x^5 + \\ 4694620331855344345697091125213620342007841178231718510259463495172530644610804866432 \cdot x^4 + \\ 144414375914674665850818303317771415765854765270144727335507532785335507793456483417088521151159/4 \cdot x^3 + \\ 186760350241708855747507113602327125632668246408881045492092681347492984320340391570231157016944534249662 \cdot x^2 + \\ 583610553971532074637919858762791632050935970469123629320074075277206737826393018985878957918138702221579477288704 \cdot x + \\ 11150929421926344628282210656174738743774808172811362367187099388952171216782841343130052732488366064124105178461056929 \cdot 3^{14}/64 \end{gathered}$$

b) The family computed above led to polynomials with rather large coefficients. This is because it seemed that all points on the Hurwitz curve allowing for totally real fibers give rise to covers with two branch points very close to each other.

We consider another family, namely (in analogy to the above notation) the one associated to the class quadruple $(2A, 2A, 2B, 4A)$ in $PGL_2(11)$.

Again, looking at the imprimitive action of $PGL_2(11)$ on 22 points, this monodromy leads to function fields $\mathbb{C}(t) \subseteq \mathbb{C}(s) \subseteq \mathbb{C}(x)$. This time, the $PSL_2(11)$-part $\mathbb{C}(x)|\mathbb{C}(s)$ is ramified over 5 points, with monodromy of type $(2A, 2A, 2A, 2A, 2A)$.

We therefore look for points on a reduced Hurwitz space of dimension 2. However, we do not need to parameterize the whole surface.

Suitable choice of the branch points in $\mathbb{C}(t)$ and $\mathbb{C}(s)$ leads to a model for a one-dimensional family, corresponding to a curve on the Hurwitz space.

Firstly, we can map the branch points of $\mathbb{C}(t)$ to 0, ∞ and $-1 \pm \alpha$, with $\alpha^2 \in \mathbb{Q}$ (for a rational model) and only the places at zero and infinity ramifying in $\mathbb{C}(s)$. Therefore, by setting $t = s^2$, we may assume that the ramification locus is $\pm\sqrt{-1-\alpha}$, $\pm\sqrt{-1+\alpha}$, and therefore the set of zeroes of the polynomial $s^4 + 2s^2 + (1 - \alpha^2) =: s^4 + 2s^2 + \lambda$.

We can use the braid criteria exhibited in [12] to confirm the existence of a cover $\mathcal{C} \to \mathbb{P}^1$, where $\mathcal{C}$ is a curve of genus one, parameterizing the polynomials with the above monodromy and restrictions on branch points.

(Alternatively, observe that the 4-tuple in $PGL_2(11)$ with which we started to obtain the restrictions on the branch points has a Hurwitz curve of genus 1.)

As a starting point for the computations, we used a polynomial with 4 branch points and $PSL_2(11)$ monodromy, computed by Malle in [35].

Develop this into a cover with 5 branch points (as done in the previous examples), and observe that the normalizer of an involution in $PSL_2(11)$ fixes one of the 2-cycles, therefore we can assume a polynomial equation $f(x) - s \cdot g_1(x)^2 \cdot g_2(x) = 0$, with $deg(f) = 11$ and $deg(g_i) = 3$ (i.e. the infinite place of $\mathbb{C}(x)$ lies over the infinite place of $\mathbb{C}(s)$, with ramification index 2).

Specializing the coefficients of g_1 and g_2 at x^2 to sufficiently many rational values again allowed an interpolation polynomial (of degree 4 in both variables), and Magma computation again yields that this polynomial defines an elliptic curve of rank 1.

Now the procedure is the same as for the previous family: find a point on this curve that allows for a totally real fiber cover (one such point yields the polynomial

$$\begin{aligned} g(s,x) := (x-\frac{1}{4})\cdot(x^5+\frac{9}{4}x^4+\frac{11}{16}x^3-\frac{65}{64}x^2-\frac{11}{16}x-\frac{323}{2816}) \\ \cdot(x^5+\frac{7}{2}x^4-\frac{17}{32}x^3-\frac{9}{32}x^2+\frac{1}{512}x+\frac{5}{11264}) \\ -s\cdot(x^3+\frac{1}{16}x-\frac{7}{352})^2\cdot(x^3+x^2+\frac{5}{16}x+\frac{9}{352}). \end{aligned} \tag{8.2}$$

with Galois group $PSL_2(11)$) , and compose the resulting parameterization of s as a rational function in x with $t = s^2$.

In this case, we also computed a degree-12 polynomial defining the stem field of a stabilizer in $PGL_2(11)$ in its natural action on 12 points. This is the polynomial $\tilde{g}$ in Theorem 8.1 below.

It was found in the following way: Let E be the splitting field of the above polynomial g over $\mathbb{Q}(s)$. A primitive element of a subfield of E of degree 12 over $\mathbb{Q}(s)$ (corresponding to the stabilizer in $PSL_2(11)$ in its action on 12 points) can be computed with Magma. From this, one obtains a primitive element of the corresponding degree-12 extension of $\mathbb{Q}(s^2)$ as well.

By the Riemann-Hurwitz genus formula, this field is of genus 2. Therefore its gonality is 2. Via computation of Riemann-Roch spaces a rational subfield of index 2 can explicitly be parameterized. A few linear transformations then yielded the polynomial $\tilde{g}$ in Theorem 8.1.

We summarize the results of the above computations:

Theorem 8.1. *The polynomials*

$$\begin{gathered} \tilde{f} := x^3\cdot(x^2-\frac{3}{121}\cdot x+\frac{567}{1131350})^3\cdot(x^2+x-\frac{413}{4114})^3\cdot(x^2-\frac{23}{726}\cdot x+\frac{63}{181016})\cdot(x^2+\frac{41}{55}\cdot x-\frac{413}{102850}) \\ -t\cdot(x^2-\frac{166}{5445}\cdot x+\frac{413}{2036430})^2\cdot \\ (x^6+\frac{577}{605}\cdot x^5+\frac{1325977}{4525400}\cdot x^4+\frac{3899419}{124448500}\cdot x^3+\frac{2472141}{4654373900}\cdot x^2-\frac{20364939}{511981129000}\cdot x+\frac{132774957}{382961884492000})^2 \\ \cdot(x^6+\frac{22271}{5445}\cdot x^5+\frac{3418045129}{672021900}\cdot x^4+\frac{119086687367}{67762208250}\cdot x^3+\frac{113798082363}{2815896209500}\cdot x^2-\frac{21318225327}{7743714576125}\cdot x+\frac{462189625317}{23169194011766000}) \end{gathered}$$

(of degree 22), and

$$\begin{gathered} \tilde{g} = ((x^3+x^2+\frac{1}{4}x+\frac{1}{22})^4\cdot(t+1249)-364\cdot(x^2+\frac{5}{7}x-\frac{1}{44}) \\ \cdot(x^4-\frac{137}{110}x^2-\frac{3}{5}x-\frac{623}{9680})\cdot(x^6+\frac{36}{143}x^5-\frac{323}{143}x^4-\frac{6381}{3146}x^3-\frac{9671}{25168}x^2+\frac{5715}{138424}x-\frac{7035}{553696}))\cdot t \\ -\frac{3^3\cdot5^2\cdot7\cdot11}{4}\cdot(x^5+2x^4+\frac{321}{550}x^3-\frac{427}{550}x^2-\frac{2771}{9680}x+\frac{401}{5324})^2\cdot(x^2+\frac{632}{693}x-\frac{6914}{22869}) \end{gathered}$$

(of degree 12), have regular Galois group $PGL_2(11)$ over $\mathbb{Q}(t)$ and possess totally real specializations.

Proof. As mentioned above, $\tilde{f}$ is gained from the polynomial f in (8.1) by setting

$$t := (s^2 + \frac{27280791476537}{21954955473000}s + \frac{766309482990625}{1985274409206528})/s.$$

We therefore first prove that f has Galois group $PSL_2(11)$.
As in Chapter 7, we compute an explicit algebraic dependency for the natural (degree 54) cover of the reduced Hurwitz space over $\mathbb{P}^1$. We use this to find a second cover with the same ramification locus as the one given by f, and then make use of the fact that $PSL_2(11)$ has two non-conjugate subgroups of index 11. Set

$$\tilde{s} = -(\frac{295}{726})^3 \cdot \frac{s^3 \cdot (s^2 + s + 693/850)^3 \cdot (s^2 + 1107/295 \cdot s - 5103/50150)}{(s^2 + 297/1475 \cdot s - 5103/1253750)^3 \cdot (s^2 + 46/25 \cdot s + 12474/10625)}.$$

Then $f(\tilde{s}, x)$ splits over $\mathbb{Q}(s)$ into polynomials of degree 5 and 6. This shows that $Gal(f|\mathbb{Q}(s))$ has an intransitive index-11 subgroup, and so it cannot be equal to A_{11} or S_{11}. Dedekind reduction then leaves only $PSL_2(11)$. So f has Galois group $PSL_2(11)$ over $\mathbb{Q}(s)$, and regularity is obvious. Therefore $Gal(\tilde{f}|\mathbb{Q}(t))$ is a transitive subgroup of the wreath product $PSL_2(11) \wr C_2 < S_{22}$. Now one can check immediately that the only transitive subgroup of this wreath product with a generating 4-tuple (with product 1) of the necessary cycle structure is $PGL_2(11)$. So $PGL_2(11)$ is the geometric Galois group of $\tilde{f}$, and regularity follows because $PGL_2(11)$ is self-normalizing in S_{22}.

The same could be done for the polynomial g in (8.2).
Alternatively, one could start with the polynomial $\tilde{g}$ and retrieve a polynomial for the degree-22 extension of $\mathbb{Q}(t)$ corresponding to the point stabilizer in the imprimitive action on 22 points (i.e. invert the process that led to the polynomial $\tilde{g}$ in the first place), by taking the polynomial

$$(x - \frac{1}{4})^2 \cdot (x^5 + \frac{9}{4}x^4 + \frac{11}{16}x^3 - \frac{65}{64}x^2 - \frac{11}{16}x - \frac{323}{2816})^2$$

$$\cdot(x^5 + \frac{7}{2}x^4 - \frac{17}{32}x^3 - \frac{9}{32}x^2 + \frac{1}{512}x + \frac{5}{11264})^2 - t \cdot (x^3 + \frac{1}{16}x - \frac{7}{352})^4 \cdot (x^3 + x^2 + \frac{5}{16}x + \frac{9}{352})^2$$

arising from (8.2) after setting $t = s^2$, transforming its ramification locus (in t) to the one of $\tilde{g}$, and then, using Magma methods, confirming that the transformed polynomial has a root in the Galois closure of $\tilde{g}$.
The existence of this second permutation action on 22 points then also proves that the Galois group cannot be A_{12} or S_{12}.

Finally, the assertion about real specializations is easy to verify. □

Remark:
For the polynomial $\tilde{g}$ in Theorem 8.1, a nice totally real specialization can be obtained by specializing $t \mapsto 1$. Linear transformations yield the polynomial

$$g_0(x) := x^{12} - 4x^{11} - 1364x^{10} + 3168x^9 + 663982x^8 - 182072x^7 - 152003984x^6 - 288945448x^5$$

$$+16597479041x^4 + 67674606956x^3 - 657948054412x^2 - 4341773859112x - 5636722853708,$$

with Galois group $PGL_2(11)$ over $\mathbb{Q}$ and splitting field contained in $\mathbb{R}$.

Elliptic curves of positive rank

Theorem 8.1 provides, for both Hurwitz spaces, a single rational point. As mentioned above, Magma computation suggests that there are actually infinitely many rational points, as the curves are elliptic of rank $rk > 0$.
We give a proof for this that does not rely on deep calculations; instead it makes use of the Nagell-Lutz theorem (cf. [51, Chapter II.5]):

Theorem 8.2 (Nagell-Lutz Theorem)**.** *Let $Y^2 = f(X) := X^3 + aX^2 + bX + c$ $(a, b, c \in \mathbb{Z})$ be a non-singular cubic curve with integer coefficients and D the discriminant of f. Let $P = (x, y)$ be a rational point of finite order (in the Mordell-Weil group of the elliptic curve). Then $x, y \in \mathbb{Z}$ and either $y = 0$ or $y|D$.*

The obvious application of this theorem is to verify $rk > 0$ for an elliptic curve by first finding a cubic equation as in the theorem, and then finding a rational point that cannot have finite order. The Mordell-Weil group must therefore be infinite, i.e. the rank of the curve is > 0.

We do this for the genus one curve on the Hurwitz space for the $(2A, 2A, 2A, 2A, 2A)$-family in $PSL_2(11)$.
Beginning with the polynomial $g(s, x)$ in (8.2), we can easily develop a model for the whole family of covers ramified over $s \mapsto \infty$ and over the zeroes of $s^4 + 2s^2 + \lambda$, e.g. by interpolating through sufficiently many p-adic lifts.
We can then calculate algebraic dependencies between any two coefficients of this model, and confirm that they lie in the function field generated by two appropriate coefficients α and β.
After some some linear transformations in the variables, to obtain nicer coefficients, we find the following model:

$$F_{\alpha,\beta}(s, x) := f_0 \cdot f_1 \cdot f_2 - s \cdot r_1^2 \cdot r_2,$$

where

$$0 = \alpha^2 + (-\frac{1}{2}\beta^2 - 9\beta - \frac{11}{2}) \cdot \alpha - \beta \cdot (\beta + 4) \cdot (\beta + 22),$$

and

$f_0 := x + \alpha,$
$f_1 := x^5 + (\beta^2 + 4\beta) \cdot x^4 + ((-\frac{13}{4}\beta^2 - 5\beta + \frac{11}{4}) \cdot \alpha - \frac{17}{2}\beta^3 - 23\beta^2 + 44\beta) \cdot x^3$
$+ ((-2\beta^4 + \frac{31}{4}\beta^3 - 3\beta^2 - \frac{257}{4}\beta - 11) \cdot \alpha - 4\beta^5 - \frac{7}{2}\beta^4 - 9\beta^3 - 280\beta^2 - 176\beta) \cdot x^2$
$+ ((\frac{13}{16}\beta^6 + \frac{89}{4}\beta^5 + \frac{2125}{16}\beta^4 + \frac{983}{2}\beta^3 + \frac{12371}{16}\beta^2 + \frac{1177}{4}\beta + \frac{363}{16}) \cdot \alpha + (\frac{13}{8}\beta^7 + 51\beta^6 + \frac{1615}{4}\beta^5 + \frac{6677}{4}\beta^4 +$
$\frac{30669}{8}\beta^3 + \frac{12661}{4}\beta^2 + 363\beta)) \cdot x$
$+ (\frac{7}{16}\beta^8 + \frac{147}{16}\beta^7 - \frac{129}{2}\beta^6 - \frac{11729}{16}\beta^5 - \frac{18127}{8}\beta^4 - \frac{46243}{16}\beta^3 - \frac{2691}{2}\beta^2 - \frac{3047}{16}\beta - \frac{121}{16}) \cdot \alpha + \frac{7}{8}\beta^9 + \frac{175}{8}\beta^8 -$
$\frac{633}{8}\beta^7 - \frac{3909}{2}\beta^6 - \frac{69569}{8}\beta^5 - \frac{129797}{8}\beta^4 - \frac{99217}{8}\beta^3 - \frac{10131}{4}\beta^2 - 121\beta,$

$f_2 := x^5 + (-\alpha + 18\beta) \cdot x^4 + ((-\frac{5}{2}\beta^2 - 21\beta + \frac{11}{2}) \cdot \alpha - 8\beta^3 + 71\beta^2 + 88\beta) \cdot x^3$
$+ ((\frac{1}{4}\beta^4 - 17\beta^3 + 63\beta^2 + 34\beta - \frac{77}{4}) \cdot \alpha + (\frac{1}{2}\beta^5 - 68\beta^4 + \frac{405}{2}\beta^3 + 1853\beta^2 - 308\beta)) \cdot x^2$
$+ ((\beta^6 + \frac{79}{2}\beta^5 + 214\beta^4 + 261\beta^3 + 1301\beta^2 + \frac{4103}{2}\beta + 242) \cdot \alpha + (2\beta^7 + 87\beta^6 + 546\beta^5 + 877\beta^4 + 3678\beta^3 +$
$16368\beta^2 + 3872\beta)) \cdot x$
$+ (\frac{1}{4}\beta^8 + \frac{33}{2}\beta^7 + \frac{1065}{4}\beta^6 - 425\beta^5 - \frac{29973}{4}\beta^4 - \frac{38851}{2}\beta^3 - \frac{71277}{4}\beta^2 - 4158\beta - 242) \cdot \alpha + \frac{1}{2}\beta^9 + 35\beta^8 +$
$651\beta^7 + 494\beta^6 - \frac{42303}{2}\beta^5 - 87407\beta^4 - 124728\beta^3 - 50072\beta^2 - 3872\beta,$

$r_1 := x^3 + ((-\frac{3}{2}\beta^2 + \frac{3}{2}) \cdot \alpha - 3\beta^3 - 6\beta^2 + 24\beta) \cdot x$
$+ (-\frac{1}{2}\beta^4 - \frac{13}{2}\beta^3 - \frac{45}{2}\beta^2 - \frac{37}{2}\beta - 2) \cdot \alpha - \beta^5 - 17\beta^4 - 90\beta^3 - 160\beta^2 - 32\beta,$
$r_2 := x^3 + 9\beta \cdot x^2 + ((-\frac{3}{2}\beta^2 - 9\beta + \frac{3}{2}) \cdot \alpha - 3\beta^3 - 6\beta^2 + 24\beta) \cdot x$
$+ (-\frac{1}{2}\beta^4 - \frac{31}{2}\beta^3 - 63\beta^2 - \frac{181}{2}\beta - \frac{31}{2}) \cdot \alpha - \beta^5 - 35\beta^4 - 207\beta^3 - 394\beta^2 - 248\beta.$

Now it is not difficult to compute (with the help of some rational point) that the elliptic curve given by α and β can be defined by a (non-singular) cubic equation in the form $Y^2 = X^3 + 59X^2 - 77X + 121$.
This curve has a point at $(X, Y) = (-21, 136)$, and $136 = 8 \cdot 17$ does not divide the discriminant $disc(X^3 + 59X^2 - 77X + 121) = -2^{16} \cdot 11^3$.
Therefore, by Nagell-Lutz, this point is of infinite order, and the rank of the curve must be positive.

Furthermore, the existence of infinitely many rational points on the Hurwitz curve can be sharpened to obtain an infiniteness result for covers with real fibers. The main ingredient is the following theorem, known as the Poincaré-Hurwitz theorem (cf. [26, Satz 13]):

Theorem 8.3. *Let E be a non-singular cubic curve, defined over $\mathbb{Q}$, with infinitely many rational points. Let $P \in E(\mathbb{Q})$ be any rational point, and $U \ni P$ any real neighbourhood of P (in the topology of $\mathbb{P}^2\mathbb{R}$), then there are infinitely many points $P_i \in E(\mathbb{Q})$ such that $P_i \in U$.*

As a corollary, the Hurwitz curves of both families computed above contain infinitely many points with real fibers. This is because the property to possess real fibers is purely group theoretic (see Chapter 4) and invariant in a given connected component of the punctured real projective line ($\mathbb{P}^1\mathbb{R}$ minus the set of branch points).

8.2 The case $G = PSL_3(3)$

Computing totally real $PSL_3(3)$-extensions might be possible via covers with four branch points; however, there are no genus zero 4-tuples with a Hurwitz curve of genus zero in $PSL_3(3)$. We therefore solve the problem via a family of covers with five branch points, with branch cycle structure $(2^4.1^5, 2^4.1^5, 2^4.1^5, 3^3.1^4, 3^3.1^4)$. The reason is that theoretical arguments show that there is a rational curve on the corresponding Hurwitz space.

This can be seen in different ways:

- The group generated by the braids $B_0 := \beta_2\beta_3\beta_2$ and $B_1 := \beta_1^2\beta_4^2$ acts intransitively on the 120 $PSL_3(3)$-generating elements of the straight inner Nielsen class $SNi^{in}((C_1, C_2, C_1, C_2, C_1))$, where C_1 is the class of involutions of cycle type $2^4.1^5$ and C_2 is the class of elements of cycle type $3^3.1^4$.

  This braiding action corresponds to curve no. (26) given on p.51 in Dettweiler's list of curves on Hurwitz spaces in [12]. The orbits under this action are of lengths 12, 48 and 60; and the cycle structure of the braids in the action of the orbit of length 12 yields a (rational) genus zero curve on the Hurwitz space.

- Alternatively, observe that the 4-tuple of classes in $Aut(PSL_3(3))$ (as an imprimitive permutation group on 26 points) with cycle structures $(2^8.1^{10}, 2^{13}, 3^6.1^8, 4^4.2^5)$ has braid orbit genus $g = 0$. Our $PSL_3(3)$-5-tuple becomes a rational translate of this 4-tuple in a natural way, via ascending to the $PSL_3(3)$-fixed field. Therefore every rational point on the genus zero Hurwitz curve for the 4-tuple also yields a regular realization of $PSL_3(3)$ with the desired monodromy.

As a starting point for the computations, we used a 4-point cover with group $PSL_3(3)$, as computed by Malle in [35].

From this, the usual deformation process led to a 5-point cover with the above cycle structure.

We now consider those covers ramified over $t \mapsto -1, 1, \infty$ (each with an involution as inertia group generator), and the roots of $t^2 - \lambda$ (each with an element of order 3 as inertia group generator). For given $\lambda \in \mathbb{C} \setminus \{0, 1\}$, there are still 120 equivalence classes of such covers (as $|SNi^{in}(C)| = 120$), so the next step is to obtain, by applying appropriate braids (as outlined in Section 3.3.4), a cover with monodromy belonging to the orbit of length 12 under the action of the braid group $\langle B_0, B_1 \rangle$ as defined above.

Once such a cover is obtained, it is not difficult anymore to find algebraic dependencies between two coefficients. As these algebraic dependencies are expected to define a rational function field (assuming "good" choice of a model), find a parameter a for this function field, and subsequently develop all coefficients in the model as rational functions in a. This leads (after suitable linear transformations of the variables) to the following polynomial:

$$f_\alpha(x, t) := f_1(x) \cdot f_2(x) \cdot f_3(x) - t \cdot g_1(x)^2 \cdot g_2(x), \quad \text{with}$$

$$f_1 := x^3+(-\frac{29821}{62424}\cdot a^2+\frac{419}{2601}\cdot a-\frac{8}{867})\cdot x^2+(-\frac{34873085}{3896755776}\cdot a^3-\frac{533}{9020268}\cdot a^2+\frac{1625}{2255067}\cdot a-\frac{104}{2255067})\cdot a\cdot x$$
$$+(\frac{2373356737921}{243251082561024}\cdot a^5-\frac{77148169501}{10135461773376}\cdot a^4+\frac{13855907}{6210454518}\cdot a^3-\frac{5320666}{17596287801}\cdot a^2+\frac{6448}{345025251}\cdot a-\frac{832}{1955143089})\cdot a,$$

$$f_2 := x^4+(a^2-\frac{890}{2601}\cdot a+\frac{16}{867})\cdot x^3+(\frac{8411611}{38203488}\cdot a^3-\frac{2349737}{27060804}\cdot a^2+\frac{20228}{2255067}\cdot a-\frac{208}{751689})\cdot a\cdot x^2$$
$$+(-\frac{21042796489}{950199541254}\cdot a^4+\frac{8744166457}{563081209632}\cdot a^3-\frac{187946941}{52788863403}\cdot a^2+\frac{5221658}{17596287801}\cdot a-\frac{47632}{5865429267})\cdot a\cdot(a-\frac{24}{229})\cdot x$$
$$+(\frac{7432196318289301}{15184705577789362176}\cdot a^6-\frac{144913019054401}{316348032870611712}\cdot a^5+\frac{1111328385245}{6590584018137744}\cdot a^4-\frac{4187601652}{137303833711203}\cdot a^3+$$
$$\frac{127801349}{45767944570401}\cdot a^2-\frac{1892800}{15255981523467}\cdot a+\frac{10816}{5085327174489})\cdot a^2,$$

$$f_3 := x^6+(\frac{28235}{41616}\cdot a^2-\frac{72}{289}\cdot a+\frac{4}{289})\cdot x^5$$
$$+(-\frac{1448052449}{7793511552}\cdot a^4+\frac{787249}{19101744}\cdot a^3+\frac{248}{44217}\cdot a^2-\frac{2572}{2255067}\cdot a+\frac{32}{751689})\cdot x^4$$
$$+(-\frac{38143481476139}{243251082561024}\cdot a^5+\frac{523172167843}{5067730886688}\cdot a^4-\frac{2650094785}{105577726806}\cdot a^3+\frac{49731227}{17596287801}\cdot a^2-\frac{874120}{5865429267}\cdot a+$$
$$\frac{5824}{1955143089})\cdot a\cdot x^3$$
$$+(-\frac{10066362783339473}{1898088197223670272}\cdot a^7+\frac{3371688276738535}{632696065741223424}\cdot a^6-\frac{19857185160995}{8787445357516992}\cdot a^5+\frac{34140023593}{64613568805272}\cdot a^4-$$
$$\frac{3335319689}{45767944570401}\cdot a^3+\frac{29234920}{5085327174489}\cdot a^2-\frac{1203904}{5085327174489}\cdot a+\frac{6656}{1695109058163})\cdot a\cdot x^2$$
$$+(\frac{43944033385895261671}{371721592544283586068 48}\cdot a^8-\frac{30966451222875342317}{19747709603915065509888}\cdot a^7+\frac{2830703634223390757}{3291284933985844251648}\cdot a^6-\frac{5765876939279587}{2285614537490169619 2}\cdot$$
$$a^5+\frac{245579679980323}{5714036343725424048}\cdot a^4-\frac{517738531076}{119042423827613001}\cdot a^3+\frac{377464880}{1469659553427321}\cdot a^2-\frac{107997760}{13226935980845889}\cdot a+$$
$$\frac{475904}{4408978660281963})\cdot a^2\cdot x$$
$$+(-\frac{44967290507979730711584 01}{1183421783342202287413678571 52}\cdot a^{10}+\frac{20457661279785206660755}{16436413657530587325189980 16}\cdot a^9+\frac{16835262443096510700 17}{1027275853595661707824373 76}\cdot$$
$$a^8-\frac{1291371636087176632 3}{9511813459219089887262 72}\cdot a^7+\frac{816227378397985697}{178346502360357935386176}\cdot a^6-\frac{12928448962175591}{148622085300298279488 48}\cdot a^5+\frac{20979020447047}{2064195629170809437 34}\cdot$$
$$a^4-\frac{768779250512}{10320978145854047186 7}\cdot a^3+\frac{676210912}{2023721205069421017}\cdot a^2-\frac{96262400}{1146775349539338576 3}\cdot a+\frac{346112}{3822584498464461921})\cdot a^2,$$

$$g_1 := x^4+(\frac{10784735}{649459296}\cdot a^2-\frac{38701}{6765201}\cdot a+\frac{676}{2255067})\cdot a^2\cdot x^2$$
$$+(\frac{61351108559}{30406385320128}\cdot a^2-\frac{806490139}{1266932721672}\cdot a+\frac{3521791}{105577726806})\cdot a^3\cdot(a-\frac{24}{229})\cdot x$$
$$+(-\frac{9025766663839939}{15184705577789362176}\cdot a^6+\frac{90237380155}{172302850147392}\cdot a^5-\frac{198120745069}{1098430669689624}\cdot a^4+\frac{497656159}{16153392201318}\cdot a^3-\frac{1550237}{565036352721}\cdot$$
$$a^2+\frac{619216}{5085327174489}\cdot a-\frac{10816}{5085327174489})\cdot a^2,$$

$g_2 := x^4 + (a^2 - \frac{890}{2601} \cdot a + \frac{16}{867}) \cdot x^3$
$+(\frac{172433164037}{446178536352} \cdot a^5 - \frac{1144124578}{4647693087} \cdot a^4 + \frac{93064996}{1549231029} \cdot a^3 - \frac{3710744}{516410343} \cdot a^2 + \frac{70784}{172136781} \cdot a - \frac{512}{57378927})/(a - \frac{24}{229}) \cdot x^2$
$+(-\frac{17010954592385}{217595694947166} \cdot a^6 + \frac{278722741765}{4015606827168} \cdot a^5 - \frac{96448763320}{4029549906429} \cdot a^4 + \frac{16378199006}{4029549906429} \cdot a^3 - \frac{480248080}{1343183302143} \cdot a^2 +$
$\frac{2329600}{149242589127} \cdot a - \frac{13312}{49747529709}) \cdot a/(a - \frac{24}{229}) \cdot x$
$+(-\frac{34769884385426337719}{34772975773137639338304} \cdot a^8 + \frac{1626950136997162081}{1448873990547401640 96} \cdot a^7 - \frac{332432058136321}{62885155839730974} \cdot a^6 + \frac{341481778769807}{251540623358923896} \cdot a^5 -$
$\frac{2173533434761}{10480859306621829} \cdot a^4 + \frac{3961349704}{205507045227879} \cdot a^3 - \frac{138072064}{129393324773109} \cdot a^2 + \frac{4179968}{129393324773109} \cdot a - \frac{53248}{129393324773109}) \cdot$
$a/(a - \frac{24}{229})$.
One can show in a similar way as in the previous cases (using the fact that $PSL_3(3)$ has two non-conjugate subgroups of index 13), that $Gal(f|\mathbb{Q}(a,t)) \cong PSL_3(3)$.
Furthermore, suitable specializations of a and t lead to totally real $PSL_3(3)$-extensions. One possible way to reach this is $a \mapsto -\frac{24}{473}$, $t \mapsto \frac{73008}{3803393}$. With the help of Magma, one then obtains the following nice representation:

$$\widehat{f}(x) := x^{13} - 6x^{12} - 4368x^{11} + 224320x^{10} - 5117352x^9 + 65111472x^8 - 497820672x^7 + 2356418304x^6$$

$$-6896458080x^5 + 11993480256x^4 - 11036102400x^3 + 3485514240x^2 + 1133736960x - 458496000,$$

with all real roots and $Gal(\widehat{f}|\mathbb{Q}) \cong PSL_3(3)$.

A two-dimensional family

In the above computations, we used theoretical criteria to find a rational curve on the Hurwitz space $\mathcal{H}$ of the $(2A, 2A, 2A, 3A, 3A)$-family in $PSL_3(3)$, and thus a one-parameter family of polynomials over $\mathbb{Q}(t)$. It is even possible to find a two-parameter family over $\mathbb{Q}(t)$ for the same Hurwitz space. More precisely, explicit computations show that the surface on $\mathcal{H}$, consisting of equivalence classes of covers with partially ordered branch point set $(\{\text{ zeroes of } t^3 + t^2 + at + b\}, 0, \infty)$ (with parameters a, b) is a rational surface. We found suitable parameters α and β, such that $\mathbb{Q}(\alpha, \beta)$ is the corresponding rational function field of two variables.
An explicit (and very nice, compared with the above one-dimensional version) parameterization of the two-dimensional family is given by

$$f_{\alpha,\beta}(t,x) := f_0^3 \cdot f_1 \cdot x - t \cdot g_0^3 \cdot g_1, \text{ with}$$

$$f_0 := x^3 + \beta \cdot x^2 + (\beta - 3) \cdot x - \frac{1}{9}\alpha\beta^2 + \frac{4}{9}\alpha\beta - \frac{4}{3}\alpha,$$

$$f_1 := x^3 + \frac{\alpha\beta^2 - 4\alpha\beta + 12\alpha - 3\beta^2 - 9}{(\beta - 3)^2} \cdot x^2 + \frac{\alpha\beta^2 - 4\alpha\beta + 12\alpha - 9\beta - 9}{3(\beta - 3)} \cdot x - 1,$$

$$g_0 := x^3 + \alpha \cdot x^2 + \frac{1}{3}\alpha\beta \cdot x + \frac{1}{9}\alpha\beta - \frac{1}{3}\alpha,$$

$$g_1 := \alpha \cdot x^3 + \frac{4\alpha\beta - 3\alpha + 9}{3} \cdot x^2 + \frac{4\alpha\beta^2 - 6\alpha\beta + 9\alpha + 9\beta - 27}{9} \cdot x - \alpha.$$

In particular, suitable specializations yield further totally real $PSL_3(3)$-extensions.

It is worth noting that $f_{\alpha,\beta}$ (as a polynomial in x) also defines a genus zero extension with respect to α (not just with respect to t!), although not in rational parameterization. The branch cycle structure with respect to α consists of six involutions (all of cycle structure $(2^4.1^5)$).

Remark:

The next open cases with regard to totally real Galois extensions occur for the permutation degree $n = 14$: there are no explicitly known totally real Galois extensions of $\mathbb{Q}$ with Galois group $PSL_2(13)$ or $PGL_2(13)$.

For these groups, the genus zero approach will no longer work. This is obvious for $PGL_2(13)$, as this group does not possess any generating genus zero tuples of length ≥ 4. For $PSL_2(13)$, there is just one rational genus zero 4-tuple (of cycle type $(2A, 2A, 2A, 3A)$), with a Hurwitz curve of genus $g = 1$.

One might therefore hope for an elliptic curve of rank ≥ 1, as in the above $PGL_2(11)$-cases. However, explicit computation showed that this is an elliptic curve of rank zero (and more precisely, can be defined by $y^2 = x^3 - 25x^2 + 136x - 180$), with no rational points leading to covers with real fibers.

Chapter 9

Survey of almost simple groups as monodromy groups of rational functions over $\mathbb{Q}$

By the Guralnick-Thompson conjecture, as phrased in [21] and answered positively in [17], there are only finitely many non-abelian, non-alternating simple groups occurring as composition factors of monodromy groups of $f(X) - tg(X)$ with $f, g \in \mathbb{C}[X]$.
The question which of these groups are also monodromy groups of rational functions over $\mathbb{Q}$ cannot be definitely answered unless one finds methods to decide the existence of rational points on arbitrary curves (and varieties of higher dimensions!). Nevertheless, it is useful to summarize partial existence results.

Proposition 9.1. *Let G be an almost simple, primitive permutation group of degree at most 120, with a generating genus zero system of length at least 4 which gives rise to a rational function $t = \frac{f(X)}{g(X)}$ defined over $\mathbb{Q}$, i.e. $G = Gal(f(X) - tg(X) \mid \mathbb{Q}(t))$.*[1] *Assume also that the socle $soc(G)$ is non-abelian, non-alternating.*
Then $soc(G)$ is isomorphic to one of the following:

- *$PSL_n(q)$, for $(n, q) \in \{(2, 7), (2, 8), (2, 11), (2, 13), (3, 3), (3, 4), (4, 3), (5, 2), (6, 2)\}$.*
- *$PSp_4(3)$ or $PSp_6(2)$.*
- *$PSU_3(3)$ or $PSU_3(5)$.*
- *One of the five Mathieu groups $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$.*

[1] The primitivity of G therefore means that the rational function t is functionally indecomposable over $\mathbb{Q}$.

Proof. Extensive computation yields the genus zero systems of length ≥ 4 generating an almost simple primitive permutation group of degree at most 120, with a socle not isomorphic to a cyclic or alternating group.
The list is somewhat lengthy. We therefore only give the permutation groups that occur. In the Magma database of primitive groups these are exactly PrimitiveGroup(n,k), with $(n,k) \in \{(7,5),(8,5),(9,9),(11,5),(11,6),(12,3),(12,4),(13,7),(14,1),(21,1),(21,4),(21,5),(21,6),(21,7),(22,1),(22,2),(23,5),(24,3),(27,12),(27,13),(28,1),(28,2),(28,6),(28,12),(31,9),(31,10),(36,16),(36,17),(36,20),(40,3),(40,4),(40,5),(40,6),(45,5),(50,7),(52,1),(56,3),(57,2),(63,5),(63,6),(66,3)\}$.

The only isomorphism types of socles that occur in this list but can be excluded to yield a rational function with four or more branch points defined over $\mathbb{Q}$ are $PSL_3(5)$ (there are only non-rational 4-tuples of permutation degree 31 in this group, and as $PSL_3(5)$ is self-normalizing in S_{31}, it cannot be the geometric monodromy group of a rational function over $\mathbb{Q}$ either) and $PSL_3(7)$ (there is exactly one family of generating genus zero 4-tuples in $PSL_3(7)$ in its action on 57 points, namely the class tuple $(2A,2A,2A,4A)$. However, regardless of the choice of branch points, there never exists a complex conjugation in $N_{S_{57}}(PSL_3(7))$ for any of those tuples. Thus, $\mathbb{R}$ is not a field of definition).
Furthermore, the complete list of primitive genus zero systems of length ≥ 5 is given in [33]. This yields only composition factors contained in the statement of the proposition. □

Remark: The above proposition does not cover all primitive genus zero systems in groups of the described type. Namely, as we are interested in realizations over $\mathbb{Q}$, tuples that violate rationality conditions are neglected. Also, some genus zero systems can be excluded as they cannot yield a rational function over $\mathbb{Q}$ by a reality argument.
Still, the remaining cases do not automatically yield a rational function defined over $\mathbb{Q}$ - they only do if the corresponding Hurwitz space[2] has a rational point.
We therefore summarize the cases that are certain to occur over $\mathbb{Q}$, and describe the open cases somewhat closer.

Proposition 9.2. *The following non-abelian, non-alternating simple groups occur as the socle of an almost simple primitive monodromy group $G = Gal(f(X) - tg(X) \mid \mathbb{Q}(t))$ of a rational function $t = \frac{f(X)}{g(X)}$ over $\mathbb{Q}$:*

- *Groups that occur as a composition factor of a group with an r-tuple of branch cycles, $r \geq 4$:* $soc(G) \in \{PSL_2(7), PSL_2(8), PSL_2(11), PSL_2(13), PSL_3(3), PSL_3(4), PSL_4(3), PSL_5(2),$
$PSp_4(3), PSp_6(2),$
$M_{11}, M_{12}, M_{22}\}$.

[2] Note that, unlike in the previous chapters, we do not require regular Galois extensions here, so the Hurwitz spaces in question are the *absolute* Hurwitz spaces, for given permutation degrees.

- *Groups that are not included in the first case, but occur as a composition factor of a group with a triple of branch cycles:*
  $soc(G) \in \{PSL_2(16), PSL_2(25), PSU_3(3), PSU_3(5), PSp_4(4), HS\}$.

Proof. The following groups have a genus-zero 4-tuple satisfying a rationality condition, with a rational Hurwitz curve:
$PGL_4(3)$ (the 4-tuple of classes $(2A, 2A, 2C, 12A)$ has a single braid orbit of length 8, with a rational Hurwitz curve; it is also a *rational* genus zero tuple in the action on 40 points, as the elements of class $12A$ have three 12-cycles),
$PSL_5(2)$ (as shown in Chapter 6), $P\Gamma L_3(4)$ (cf. Chapter 7), $PSL_3(3)$ and $PSL_2(11)$ (see [35] for both groups; compare also Chapter 8), $PSL_2(8)$ (the class tuple $(2A, 2A, 2A, 3A)$ has a rational Hurwitz curve, and the corresponding family of degree-9 polynomials with group $PSL_2(8)$ was explicitly computed in [22]. This class tuple has genus 1 in the action on 9 points; note however that it is a rational genus zero tuple in the action on 28 points!), $PSL_3(2)$ (e.g. [35]), $Aut(M_{22})$ (e.g. with the class tuple $(2A, 2A, 2B, 11A)$, which has a rational Hurwitz curve even in the unsymmetrized case, and the class $2A$ has an odd number of transpositions), M_{12} (once again, cf. [35]), M_{11} (see the table in Appendix A), $PSp_4(3).2$ and $PSp_6(2)$ (in the actions on 27 and 28 points respectively, the tuples $(2A, 2A, 4B, 6A)$ and $(2A, 3A, 3B, 4A)$ in the respective groups are actually *rigid* genus zero tuples!).

The only remaining group for the case of four branch points is $PSL_2(13)$. There is only one genus zero 4-tuple in $PSL_2(13)$, namely the class tuple $(2A, 2A, 2A, 3A)$, with a Hurwitz curve of genus 1. Explicit computations show that this curve is of rank zero (cf. Chapter 8). There are, however, rational points on this curve, which means that there is a regular $PSL_2(13)$-extension over $\mathbb{Q}$ in this family; and it can even be defined via a rational function as the normalizer of an involution in $PSL_2(13)$ acts intransitively on its six transpositions, with two orbits of length 3.
An explicit example is $t = \frac{f(x)}{g(x)}$, with

$$\begin{aligned} f(x) = {} & 71621 \cdot x^{14} + 72813748 \cdot x^{13} + \frac{5838562093}{2} \cdot x^{12} + \frac{52600723539}{2} \cdot x^{11} + \frac{8439608322509}{16} \cdot x^{10} \\ & + \frac{29564258518249}{8} \cdot x^{9} + \frac{173259713244345}{4} \cdot x^{8} + \frac{3732178629141755}{16} \cdot x^{7} + \frac{123705336708929885}{64} \cdot x^{6} \\ & + \frac{117292753322586205}{16} \cdot x^{5} + \frac{1534815319893954371}{32} \cdot x^{4} + \frac{1808975171989429353}{16} \cdot x^{3} \\ & + \frac{3984034942550 6009289}{64} \cdot x^{2} + \frac{1095985028928 5242821}{16} \cdot x + \frac{5291112344202886 6197}{16}, \end{aligned}$$

$$g(x) = (x^2 + 27) \cdot (x^2 + 23 \cdot x - 27)^3 \cdot (x^2 + 1/4 \cdot x + 239/8)^3.$$

For the case of only three branch points, we only included socles of groups that have a rigid class triple of conjugacy classes which are rational at least in the symmetric normalizer. Note especially the Higman-Sims group HS. Its automorphism group $Aut(HS)$ is generated in two different ways by rational rigid genus zero triples (satisfying also an oddness condition for rationality of the stabilizer stem field) in the primitive action on 100 points, therefore it is the monodromy group of rational functions over $\mathbb{Q}$. This case is missing in the classification of sporadic monodromy groups in [34]. □

Remarks:

- It should be noted that several of the above composition factors occur in different permutation degrees.
  A notable example is the group M_{12}. It occurs as the monodromy group of a rational function over $\mathbb{Q}$ with four branch points in permutation degree 12 (e.g. [35]), but it can also be shown to occur in permutation degree 66, in the following way:
  The generating 4-tuples of conjugacy classes $(2A, 2B, 2B, 3B)$ in M_{12} yield a single braid orbit of length 32. The corresponding (C_2-symmetrized) Hurwitz curve has genus 1, and explicit computations of the corresponding family of degree-12 covers yield that this is an elliptic curve of positive rank, and more precisely can be defined by $y^2 = x^3 - 48x^2 + 525x + 9998$. This yields infinitely many equivalence classes of M_{12}-Galois extensions of $\mathbb{Q}(t)$; these cannot be the Galois closure of rational functions of degree 12 over $\mathbb{Q}$, as reality arguments show. However, the class tuple $(2A, 2B, 2B, 3B)$ is also a genus zero tuple in the action of M_{12} on 66 points, and this time the fixed field of a point stabilizer is necessarily a rational field, over any field of definition. This is because the class $2A$ has cycle type $2^{30}.1^6$ in this action, and the centralizer in M_{12} of this involution acts intransitively on the 30 2-cycles, with two orbits of length 15. By Lemma 3.7, this yields a place of odd degree in the fixed field of a point stabilizer, thereby forcing this field to be a rational function field.

  Similarly, M_{11} is the monodromy group of rational functions over $\mathbb{Q}$ of degree 11 as well as 12. For degree 12, this can be seen immediately by the standard braid genus criterion, as the class four tuple with cycle structures $(2^4.1^4, 3^3.1^3, 3^3.1^3, 3^3.1^3)$ yields a single braid orbit of length 63, and the (S_3-symmetrized) Hurwitz curve is a rational genus zero curve.
  For degree 11 however, there are no genus zero four tuples with a Hurwitz curve of genus zero. Instead, the tuple of classes with cycle structures $(2^4.1^3, 2^4.1^3, 3^3.1^2, 4^2.1^3)$ has a Hurwitz curve of genus 2. Explicit computations of this curve yielded a "good" rational point, allowing a non-degenerate cover of this family defined over $\mathbb{Q}$. A possible parameterization is given in Appendix A.

- In addition to the above results on almost simple groups, compare also the list of genus zero tuples in groups of affine type given in [56]. This list yields only a few genus zero tuples of length > 3 with a non-abelian, non-alternating composition factor.

- Among the open cases (groups with rational genus zero 4-tuples, but no obvious rational points on the corresponding Hurwitz space), the group $PSL_6(2)$ might be of special interest. It has one (and only one) rational genus zero 4-tuple, of elements of orders $(2, 2, 3, 3)$, with a single braid orbit of length 48. The corresponding Hurwitz curve has genus 3, and the imprimitive action of the braid group on the Nielsen class shows that this is a hyperelliptic curve. It would be interesting to find out whether this curve has a "good" rational point, leading to a $PSL_6(2)$-realization over $\mathbb{Q}(t)$. The only way to find out seems to be explicit computation.

  Furthermore, a major reason for the degree restrictions in the previous propositions is the group $PSL_7(2)$.

  Question: Are there any rational genus zero 4-tuples generating $PSL_7(2)$?

- The only other open cases (with our degree restriction) for the existence of rational functions over $\mathbb{Q}$ with ≥ 4 branch points are for the socles $PSU_3(3)$, $PSU_3(5)$, M_{23} and M_{24}. For the first two socles, there is just one 4-point genus zero family each (in $PSU_3(3).2$ resp. $PSU_3(5).2$). The corresponding Hurwitz curves are of genus 0 resp. 5. The first curve is even a rational curve, i.e. leads to genus zero covers defined over $\mathbb{Q}$, but it is not clear by the standard arguments whether these covers can be defined by rational functions over $\mathbb{Q}$. However, rational functions over $\mathbb{Q}$ with three branch points do exist for both groups.

  For M_{23} and M_{24}, existence of rational functions defined over $\mathbb{Q}$ is still open for any number of branch points, cf. Chapter 5.

As one more special application, we classify the monodromy groups of rational functions, defined over $\mathbb{Q}$, with exactly two places over infinity, i.e. either of the form $t = \frac{f(X)}{X^k}$, $0 \leq k \leq deg(f)$ (i.e. Laurent polynomials), or of the form $t = \frac{f(X)}{(X^2-a)^k}$ with $a \in \mathbb{Q} \setminus \{0\}$.

This uses Müller's classification of genus zero systems in primitive groups involving an element with two cycles (in [45]), as well as results about complex conjugation (cf. Chapter 4) and about minimal fields of definition of some 3-point covers (as in [38]).

Proposition 9.3. *Let the primitive group G of degree $2k$ be the arithmetic monodromy group of a rational function $p(X) \in \mathbb{Q}(X)$. Furthermore assume that p has denominator $(X^2-a)^k$, $a \in \mathbb{Q} \setminus \{0\}$. Then one of the following holds*

1. *G is also the monodromy group of a rational Siegel function, in particular the poles of p can be chosen real and algebraically conjugate.*[3] *More precisely, one of the following holds:*
   - *$G = A_n$ or S_n in the natural action.*

[3] Note that this does not mean that we can choose the poles real and conjugate for *any* ramification type fulfilling the assumptions, but just for at least one.

- *$G = PGL_2(5)$, acting on 6 points*
- *$G = AGL_3(2)$, acting on 8 points*
- *$A_n \leq G \leq Aut(A_n)$, for $n \in \{5, 6\}$, in the action on 10 points*
- *$G = S_4 \wr C_2$ in the (diagonal) action on 16 points*
- *$G = C_2^4 \rtimes S_5$, acting on 16 points.*

2. *$G \in \{PGL_2(7), Aut(M_{22})\}$.*

Proof. [45, Th. 4.8.] classifies the genus zero systems, in primitive groups of degree $2n$, containing and element with two n-cycles.
Theorem 5.2 of [45] then deals with the case of Siegel functions. There remains a finite list of cases. $Aut(M_{22})$ has been realized by Malle in [36] with a polynomial of the above form, so exclude this group, as well as the groups that occur in the Siegel case. This leaves only two groups with 4-tuples, namely M_{12} and M_{24}, with the 4-tuples discussed in Chapter 4.
In $PGL_2(7)$, the class tuple $(6.1^2, 2^3.1^2, 4^2)$ can easily be confirmed to give rise to a rational function over $\mathbb{Q}$ with denominator $(X^2 + 7)^4$. For the remaining triples, in most cases the degree is small enough to confirm via the Groebner basis approach that $\mathbb{Q}$ is not a field of definition.
The only groups of "larger" degrees are M_{24} (degree 24), $PSL_4(3)$, and $PGL_4(3)$ (both of degree 40).
M_{24} has three genus zero triples with an element with two 12-cycles, with element orders $(2, 5, 12)$, $(2, 6, 12)$ and $(3, 3, 12)$ respectively. In all cases, direct computation shows that complex conjugation is always a fixed point free involution in M_{24}.
For the degree-40 cases, it suffices to note that the elements of order 20 do not form a rational class in $PGL_4(3)$, so $\mathbb{Q}$ cannot be a field of definition by the branch cycle argument. □

Corollary 9.4. *The non-abelian, non-alternating composition factors of monodromy groups of rational functions $p(X) \in \mathbb{Q}(X)$ of even degree $2k$ with denominator $(X^2 - a)^k$ are exactly $PSL_2(7)$ and M_{22}.*

Proposition 9.5. *Let the primitive group G of degree n be the arithmetic monodromy group of a Laurent polynomial $t = \frac{f(X)}{X^k} \in \mathbb{Q}(X)$, i.e. $G = Gal(f(X) - t \cdot X^k | \mathbb{Q}(t))$. Assume furthermore that G has a non-abelian, non-alternating composition factor. Then one of the following holds:*

1. *$k \in \{0, deg(f)\}$, and $G = P\Gamma L_2(8)$, of permutation degree 9.*
2. *$0 < k < deg(f)$, and*
   - *either G almost-simple, $G \in \{PGL_2(7), M_{12}, PGL_2(13)\}$, of permutation degree 8, 12 and 14 respectively.*
   - *or $G = AGL_3(2)$, acting as an affine group of degree 8.*

Proof. In the first case, $k = 0$ can be assumed w.l.o.g., so G is the monodromy group of a polynomial over $\mathbb{Q}$. These were classified in [46]. $P\Gamma L_2(8)$ is the only group that fulfills all the requirements.
In the second case, G must contain a genus zero system involving an element with two cycles; also, there must be an involution in G, representing complex conjugation in a connected component of the punctured $\mathbb{P}^1\mathbb{R}$ next to the point with the two-cycle inertia group generator (without restriction the point at infinity), and this element must not switch the two cycles (otherwise the two places over $t \mapsto \infty$ would be complex conjugate, contradicting the representation $t = \frac{f(X)}{X^k}$).

In the affine case, the list in [46], together with the condition of a non-abelian non-alternating composition factor, only leaves the cases $G = AGL_3(2)$ and $AGL_5(2)$; however, in the latter case, the two-orbit element always belongs to a non-rational conjugacy class and therefore, as $AGL_5(2)$ is self-normalizing in S_{32}, by the branch cycle argument the corresponding rational function cannot be defined over $\mathbb{Q}$ (and in fact, not even over $\mathbb{R}$).

All other groups fulfilling the conditions of the propositions are almost simple, and more precisely one of $PSL_2(7), PGL_2(7), M_{11}, M_{12}, PGL_2(13), P\Sigma L_3(4), P\Gamma L_3(4), Aut(M_{22}), M_{24}$ and $PGL_4(3)$.

However, the branch cycle argument already excludes many possible class tuples, in particular all for the groups $M_{11}, P\Sigma L_3(4), P\Gamma L_3(4)$ and $PGL_4(3)$. In M_{24}, the only candidate left for a two-orbit element is an element consisting of two 12-cycles; this case has already been dealt with in Prop. 9.3.
Furthermore, regardless of the choice of branch points, none of the cases with (arithmetic) monodromy group $Aut(M_{22})$ has a complex conjugation fixing both cycles of the two-orbit element, which is always an element of order 11. Similarly, in $PSL_2(7)$, the only rational genus zero class tuple with a two-orbit element (classes $(3A, 3A, 4A)$) cannot be realized with a complex conjugation inside $PSL_2(7)$ fixing both cycles of the element of order 4. □

Remark: All the groups G in the above proposition do indeed occur as the Galois group of a Laurent polynomial over $\mathbb{Q}$; indeed all these groups have a rigid triple of rational conjugacy classes fulfilling the conditions of the proposition, and explicit polynomials were computed long ago.

Chapter 10

An algorithm for algebraic patching over complete valued fields

In the previous chapters we have only considered computational methods for genus zero covers. The goal of the following chapter is to give an algorithm for computing covers of higher genus from very simple starting covers, using the method of algebraic patching, as described e.g. in [27]. Cf. also [55, Chapter 11]. We should note that this algorithm may be applied for non-Galois covers, which is important for practical computations.

10.1 Theoretical background

Definition 10.1 (Patching Data)**.** Let I be a finite set of cardinality at least two.
A patching data is a tuple $(E, F_i, P_i, Q; G_i, G)_{i\in I}$, where $E \subseteq F_i, P_i \subseteq Q$ are fields and $G_i \leq G$ are subgroups of a finite group G, such that the following hold:

- $F_i|E$ is a Galois extension with Galois group G_i, for all $i \in I$.
- $F_i \subseteq P_i' := \cap_{j\neq i} P_j$, for all $i \in I$.
- $\cap_{i\in I} P_i = E$.
- G is generated by the union of the subgroups G_i.
- Set $n := |G|$. Then, for all $i \in I$ and all $m \leq n$, every $B \in GL_m(Q)$ can be written as a product $B = B_1 B_2$ with $B_1 \in GL_m(P_i)$ and $B_2 \in GL_m(P_i')$
(This is called a Cartan decomposition.[1])

[1] Cf. [27, Def. 1.1.1]. We demand Cartan decomposition for all $m \leq n$ (not just for n, as in [27]) in order to proceed to intermediate fields of Galois extensions as in Lemma 10.2.

The underlying idea is the following. Suppose the subgroups G_i have been realized as Galois groups over E according to the above setting. The goal is to "patch" from these subgroups the full group G as a Galois group over E. This will be achieved by constructing certain algebras over the fields P_i.
Of course the last condition in the above definition is quite restrictive and doesn't hold over arbitrary fields.
The method works over complete valued fields (and a descent argument can be used to generalize it to ample fields), so two typical situations would be fields of Laurent series or p-adic fields.

One can however combine the methods exhibited here with the investigation of Hurwitz spaces to proceed e.g. from p-adic integers to algebraic (or ideally rational) numbers, cf. Sections 10.2 and 10.3.

In our algorithm, for the sake of simplicity, we will always set $|I| = 2$. This somewhat simplifies the situation in the above definition and also shortens the computations.
So assume that the group G is generated by the two subgroups G_1 and G_2. As we want easy Galois extensions to start with, the groups G_i should be small and/or easy to handle. Ideally G_1 and G_2 are cyclic groups. If one works with simple groups G, this is not a strong restriction, as every finite simple group is generated by two elements, i.e. by two cyclic groups.

[27, Chapter 1.1] gives a construction to obtain from a patching data a field F with $Gal(F|E) = G$. The proof of this result also contains an explicit way[2] to obtain a vector space basis of F over E (we again restrict to the case $I = \{1, 2\}$):

Lemma 10.1. *Let $(E, F_i, P_i, Q; G_i, G)_{i\in\{1,2\}}$ be a patching data. Let $N := \{\sum_{\zeta\in G} a_\zeta \zeta \mid a_\zeta \in Q\}$, regarded as a $|G|$-dimensional Q-vector space, and turn N into a Q-algebra via componentwise multiplication.*
Set $Q_i := P_i F_i$ and

$$N_i := \{\sum_{\zeta\in G} a_\zeta \zeta \in N \mid a_\zeta \in Q_i, a_\zeta^\eta = a_{\zeta\eta} \text{ for all } \zeta \in G, \eta \in G_i\}, \quad \text{for } i \in \{1, 2\}.$$

Then the intersection $F := N_1 \cap N_2$ is a field which is Galois over E with group G.
A Q-basis of N which is contained in $N_1 \cap N_2$ can be obtained in the following way:

- *Firstly, choose $\{\lambda_1, ..., \lambda_m\}$ as a set of coset representatives of G/G_1 as well as $(\eta_1, ..., \eta_r)$ as some ordering of the elements of G_1, Then the following is a Q-basis of N inside N_1:*

$$v := (\sum_{\nu=1}^{n} (z^{j-1})^{\eta_\nu} \cdot \lambda_k \eta_\nu \mid j = 1, ..., r; k = 1, ..., m)$$

[2] (at least as far as Cartan decomposition can be done explicitly)

with z a primitive element of $Q_1|P_1$.

- *In the same way, obtain a basis u of N contained in N_2.*
- *Let $B \in GL_n(Q)$ be the transition matrix of these bases, i.e. $u = vB$. Use Cartan decomposition to write $B = B_1B_2$, with $B_1 \in GL_n(P_1)$, $B_2 \in GL_n(P_2)$. Then $uB_2^{-1} = vB_1$ is a Q-basis of N inside $N_1 \cap N_2$.*

Proof. See [27, Lemmas 1.1.2 and 1.1.3, as well as Remark 1.1.8]. □

As I learned from unpublished work of R. Schulze ([49]), this result can be generalized to arbitrary intermediate fields of $F|E$. To do this, one needs to define an appropriate subalgebra of the above algebra Q: Let $U \leq G$ be a subgroup and N^U the set of fixed points in N under the action of U given by

$$(\sum_{\zeta\in G} a_\zeta\zeta)^u := \sum_{\zeta\in G} a_{u\zeta}\zeta.$$

This is again a Q-vector space, of dimension $[G:U]$.
Analogously, define N_i^U, for the sub-algebras N_i defined in Lemma 10.1.

Lemma 10.2 (Generalization of Lemma 10.1 to arbitrary intermediate fields of $F|E$)**.**
Let $(E, F_i, P_i, Q; G_i, G)_{i\in\{1,2\}}$ be a patching data. Let $U \leq G$ be any subgroup; F, N, N_1 and N_2 as above, and denote by F^U the fixed field of U inside F and by N^U the set of fixed points under the action of U on N.
Then there is a Q-basis of N^U contained in $N_1^U \cap N_2^U = F^U$.

Proof. First, one constructs a basis of N^U contained in N_1^U.
Let $S := \{g^{(1)}, ..., g^{(l)}\}$ be a complete system of (U, G_1)-double coset representatives, i.e. the sets $Ug^{(i)}G_1$ form a partition of G. For each $g \in S$, fix a primitive element $z := z_g$ of the extension $Fix(U^g \cap G_1)|E$, with $Fix(U^g \cap G_1) \subseteq F_1$ the fixed field, of degree $[G_1 : (U^g \cap G_1)]$ over E. Then z is also a primitive element of the corresponding fixed field inside $Q_1 := P_1F_1|P_1$. As P_1 and F_1 are linearly disjoint, the degree of the latter field extension is still $[G_1 : (U^g \cap G_1)]$. Denote this degree by $r(= r_g)$.
Now for each $k = 0, ..., r-1$, define an element

$$a_k := a_k(g) := \sum_{\zeta\in UgG_1} a_\zeta \cdot \zeta,$$

with $a_{ugg_1} := (z_g^k)^{g_1}$ for $u \in U$ and $g_1 \in G_1$.
Then $a_k \in N_1$ and $a_k \in N^U$, as one easily verifies. Therefore $a_k \in N_1^U$.
Doing this for all $g \in S$, one obtains a total of $[G:U] = dim_Q N^U$ elements $a_k(g)$. It remains to show that these are linearly independent over Q.
Let $\{\zeta_1, ..., \zeta_m\}$ be a right transversal of U in G; then $s := (\sum_{\sigma\in U} 1 \cdot \sigma\zeta_k \mid k = 1, ..., m)$ is a Q-basis

of N^U. We need to show that the transformation matrix B such that $sB = (a_k(g) \mid g \in S, k = 0, ..., r_g - 1)$ is non-singular.
But upon permuting the basis s appropriately, this matrix becomes a block diagonal matrix, consisting of Vandermonde blocks of the form $\begin{pmatrix} 1 & z & \cdots & z^{r-1} \\ 1 & z^{g_1} & \cdots & (z^{g_1})^{r-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & z^{g_{r-1}} & \cdots & (z^{g_{r-1}})^{r-1} \end{pmatrix}$, with $\{id, g_1, ..., g_{r-1}\}$ a right transversal of $U^g \cap G_1$ in G_1.
As z is a primitive element of $Fix(U^g \cap G_1)|E$, the elements z, z^{g_1}, ..., z^{g_r} are pairwise different, so the Vandermonde block is invertible.
This proves that B is invertible as well, so $(a_k(g) \mid g \in S, k = 0, ..., r_g - 1)$ is a Q-basis of N^U.

In the same way, obtain a basis contained in N_2^U. A basis contained in the intersection $N_1^U \cap N_2^U$ is now obtained just as in the previous lemma, by applying Cartan decomposition. □

This result is quite important for explicit computations, as the degree of a faithful action of G is often dramatically smaller than the group order and therefore the size of the matrices involved in the computation will decrease correspondingly.

In particular, in the case that G is a primitive permutation group (with point stabilizer U), each of the basis vectors obtained via Lemma 10.2 is either contained in the base field E or already a primitive element of $F^U|E$.

We now turn to the explicit computation of extensions with given ramification.
Let G be a transitive permutation group of degree n and $U \leq G$ a point stabilizer. Let K be a complete valued field with ultrametric absolute value $|\cdot|$, e.g. a p-adic field or a Laurent series field, and $K(t)$ the rational function field.
Define two functions $w_1 := \frac{r}{t-c_1}$ and $w_2 := \frac{r}{t-c_2}$, where $|r| \leq |c_1 - c_2|$, $r, c_1, c_2 \in K$ and $r \neq 0$. Following [27, Chapter 3], we consider the rings of convergent power series $K\{w_i\} := \{f = \sum_{n=0}^{\infty} a_{i,n} w_i^n \mid a_{i,n} \in K, a_{i,n} \to 0 \text{ for } n \to \infty\}$ $(i = 1, 2)$, and their quotient fields.
The starting point of the computations will be the realization of the groups G_i (with prescribed ramification) within these fields.

To do this, choose the groups G_i and the inertia group generators for the G_i-extensions such that these extensions can easily be computed. Typically, $|G_i|$ will be prime to $char(K)$ (to ensure tame ramification), and generating systems $(\sigma_{1,i}, ..., \sigma_{r_i,i})$ of G_i will be chosen such that the image on each orbit of G_i is a genus zero system. A standard example would be to choose $G_1 = \langle\sigma_1\rangle$ and $G_2 = \langle\sigma_2\rangle$ to be cyclic groups with order prime to $char(K)$, and the generating systems to be $(\sigma_1, \sigma_1^{-1})$ and $(\sigma_2, \sigma_2^{-1})$.

Algorithmic patching of Galois groups from cyclic subgroups

So assume from now on that G_1 and G_2 are cyclic and $G = \langle G_1, G_2 \rangle$ (note however, that the following algorithm can be adapted to non-cyclic G_i as well).
Assuming that K contains the $|G_1|$-th roots of unity, and the characteristic is prime to $k_1 := |G_1|$, a genus zero G_1-extension of $K(t)$ is simply given by $K(x)|K(t)$ with $x^{k_1} = t$. However, for the patching algorithm one needs to construct a Galois extension of $K(t)$ with group G_1 within $Quot(K\{w_1\})$. To ensure this, points of $K(t)$ ramifying in $K(x)$ should be "close" to each other (in the ultrametric absolute value of K, extended to $K[t]$ via setting $||t|| := 1$).
For $K = \mathbb{Q}_p$, one can e.g. choose $w_1 \mapsto \infty$ and $w_1 \mapsto \frac{1}{p}$ as the ramified points; one possibility to obtain this would be to choose x such that $x^{k_1}(pw_1 - 1) = -1$.
For $K = K_0((z))$, for a base field K_0, one can similarly choose the points $w_1 \mapsto \infty$ and $w_1 \mapsto \frac{1}{z}$.
The element x can then be expanded as a power series in pw_1 (or zw_1 respectively), i.e. we can demand $x \in K\{w_1\}$.

Also, changing to t-coordinates, the branch points $\mathcal{P}_1$ and $\mathcal{P}_2$ fulfill $|\mathcal{P}_1 - \mathcal{P}_2| = |rp|$ resp. $|rz|$, i.e. $|\mathcal{P}_1 - \mathcal{P}_2| < |r|$ in all cases.
Repeat this for a G_2-extension within $K\{w_2\}$ (by choosing two branch points with "large" w_2-coordinates this time). In t-coordinates, one again gets $|\mathcal{P}_3 - \mathcal{P}_4| < |r|$, and apart from this, $\min_{i\in\{1,2\},j\in\{3,4\}} |\mathcal{P}_i - \mathcal{P}_j| = |c_1 - c_2| \geq |r|$, by the definition of w_1 and w_2.
This choice of branch points will help to control the ramification behaviour of the eventual Galois extension with group G.

Now, define $K\{w_1, w_2\} = \{z_1 + z_2 \mid z_i \in K\{w_i\}\}$ (this is a ring, and upon setting $||a_0 + \sum_{n\in\mathbb{N}} a_{1n}w_1^n + \sum_{n\in\mathbb{N}} a_{2n}w_2^n|| := \max(\{|a_0|\} \cup \{|a_{1n}| \mid n \in \mathbb{N}\} \cup \{|a_{2n}| \mid n \in \mathbb{N}\})$ for $a_0, a_{in} \in K$, $K\{w_1, w_2\}$ becomes the completion of $K[w_1, w_2]$ with respect to the norm $||\cdot||$, cf. [27, Chapter 3]).
Then the following yields a patching data $(E, F_i, P_i, Q; G_i, G)_{i\in\{1,2\}}$, as proven in [27, Prop. 4.4.2]:

$$E := K(t), P_1 := Quot(K\{w_2\}), P_2 := Quot(K\{w_1\}), Q := Quot(K\{w_1, w_2\}),$$

and $F_1 \subseteq P_2$ and $F_2 \subseteq P_1$ the two Galois extensions of E with groups $Gal(F_1|E) = G_1$ and $Gal(F_2|E) = G_2$.
With the above choices of defining equations for the G_i-extensions, it is easy, following the proof of Lemma 10.2, to obtain a basis of N^U contained in N_1^U, and more precisely a coordinate matrix (with regard to the standard basis s introduced in the proof of Lemma 10.2) with entries in $Quot(K\{w_1\})$; and analogously for N_2^U and $Quot(K\{w_2\})$.

Note that these matrices are of a special form, as the proof of Lemma 10.2 shows: they arise from block matrices with Vandermonde blocks after suitable permutations of rows, depending on the ordering of the standard basis s in the proof of Lemma 10.2. Therefore, their determinants, adjoint matrices etc. can be computed with comparatively little effort (cf. e.g. [54]).

To obtain from this a basis of the degree-n field extension $F^U|K(t)$ (U being a point stabilizer in G), and in particular a primitive element of this extension, we need an explicit realization of Cartan decomposition in $GL_n(Q)$. We do this by following the proof of [27, Lemma 3.4.3], adapted to our specific patching data.

Begin with matrices A_1 and A_2 parameterizing bases of N^U contained in N_2^U and N_1^U respectively. The proof of Lemma 10.2 outlined the construction of these matrices A_i. We give a more detailed description of this construction for the case of cyclic subgroups G_i:

Let $(a_{1,1}, ..., a_{1,r_1}) \cdots (a_{l,1}, ..., a_{l,r_l})$ be a cycle decomposition of σ_1 (the generator of G_1). As U is a point stabilizer of G, the (U, G_i)-double coset representatives can be identified naturally with the orbits of G_1, i.e. the cycles of σ_1. Furthermore, for each double coset representative g, one needs a right transversal of $U^g \cap G_1$ in G_1 to fill up Vandermonde blocks as in the proof of Lemma 10.2. The elements of this right transversal can be identified naturally with the elements of the respective orbit of G_1. Choosing such a right transversal for *each* double coset representative eventually yields a right transversal of U in G, to be identified with the tuple $t := (a_{1,1}, ..., a_{1,r_1}, ..., a_{l,1}, ..., a_{l,r_l})$. Each element of this right transversal yields a row of a representation matrix, and because of the ordering of this transversal, the resulting matrix will be a Vandermonde block matrix.

Now, the standard basis s in the proof of Lemma 10.2 also corresponds to a right transversal of U in G. However, this basis needs to be in a fixed order (not depending on G_1, G_2). We therefore choose the right transversal for the basis s such that it can be identified with the tuple $(1, ..., [G : U])$. The matrices A_i are coordinate matrices with regard to this standard basis. To proceed from the Vandermonde block matrix to the correct coordinate matrix A_i, one needs to observe that the first row of the block matrix should actually be row number $a_{1,1}$, the second one should be number $a_{1,2}$ etc.

Thus, permute the rows of the block matrix via the permutation $\tau : i \mapsto t_i$ (for $i = 1, ..., [G : U]$), with the above tuple t.

Now we have obtained the matrices A_1 and A_2. Furthermore, by the special choice of primitive elements described above, the entries of A_1 are elements of $K\{w_2\} \subseteq P_1$, and those of A_2 are in $K\{w_1\} \subseteq P_2$.

By the Weierstrass preparation theorem (e.g. [27, Cor. 2.2.5]), the determinants of A_1 and A_2 can be decomposed as $\det A_i = h_i \cdot u_i^{-1}$, with units $u_i \in K\{w_j\}^\times$ and polynomials $h_i \in K[w_j]$, $j \in \{1, 2\} \setminus \{i\}$ (and this decomposition can be explicitly obtained by a simple algorithm).

Let B_i be the adjoint matrix of A_i (i.e. $A_iB_i = \det(A_i)\cdot I$), and set $C_1 := u_1B_1A_2$ and $C_2 := u_2B_2A_1$.

Now, approximate the matrix C_2 in the norm $||\cdot||$ of $K\{w_1, w_2\}$ induced by the ultrametric absolute value of the field K. More precisely, using the Weierstrass division theorem, for each entry $(C_2)_{i,j}$ of C_2 write

$$(C_2)_{i,j} = c_{i,j} \cdot h_1h_2 + b_{i,j},$$

with $c_{i,j} \in K\{w_1, w_2\}$ and polynomials $b_{i,j} \in K[w_1, w_2]$ of degree less than the pseudo-degree of h_1h_2 (which is defined as the highest degree of a monomial with the maximal norm among all the monomials of the unique Mittag-Leffler expansion $(K\{w_1, w_2\} \ni)h_1h_2 = a_0 + \sum_{n\in\mathbb{N}} a_{1n}w_1^n + \sum_{n\in\mathbb{N}} a_{2n}w_2^n)$. Again the $c_{i,j}$ and $b_{i,j}$ can be explicitly determined by a simple algorithm.

Now for each $c_{i,j}$, find $(c_0)_{i,j} \in K[w_1, w_2]$, such that $||c_{i,j} - (c_0)_{i,j}|| < \frac{1}{||C_1||}$. For K a p-adic or a Laurent series field, this is simply achieved by truncating the expansion of $c_{i,j}$.
Then let $M \in M_n(K[w_1, w_2]) \subset M_n(K(t))$ be the matrix consisting of the entries $h_1h_2(c_0)_{i,j} + b_{i,j}$. Furthermore, set $\tilde{M} := I - C_1M_0$, where M_0 is the matrix consisting of the entries $c_{i,j} - (c_0)_{i,j}$. Then $||I - \tilde{M}|| = ||C_1M_0|| < 1$ by the definition of M_0, and this allows a Cartan decomposition for the matrix $\tilde{M}$ (cf. [27, Lemma 3.4.2]), i.e. $\tilde{M} = \tilde{M}_1 \cdot \tilde{M}_2$ with $\tilde{M}_i \in GL_n(P_i)$.

The columns of the matrix $V := A_2 \cdot M \cdot \tilde{M}_2^{-1}$ then yield a basis of N^U contained in $N_1^U \cap N_2^U$.
Here the matrix $\tilde{M}_2^{-1}$ is determined by an explicit implementation of Cartan decomposition (see Chapter 11 for a Magma implementation, and cf. again [27, Lemma 3.4.2] or [55, Lemma 11.14]).
Note especially that the whole algorithm works without explicit inversion of the occurring matrices over complete valued fields, which is important as in practice, p-adic or Laurent series expansions will only be given up to a fixed precision.

Once a vector space basis (and in particular a primitive element x for the extension $F^U|K(t)$) is found, one needs to retrieve the minimal polynomial of x over $K(t)$.
This is done by looking for algebraic dependencies between series expansions of sufficient precision for x and t, similarly as in previous chapters.
We know the x-degree of the dependency, as this is simply the permutation degree $[G : U]$; for the degree in t however, we have to guess.
(We noticed, however, that with our implementation, and with cyclic subgroups $G_1 = \langle\sigma_1\rangle$ and $G_2 = \langle\sigma_2\rangle$ such that $(\sigma_1, \sigma_1^{-1}, \sigma_2, \sigma_2^{-1})$ is a genus-g tuple of G, the t-degree $[G : U] + (g - 1)$ works in many examples.)

10.2 Connection with Hurwitz spaces

Under suitable normalization of the G_i-extensions, as outlined above, the set of places of $K(t)$ that ramify in $F|K(t)$ will be the union of the sets of places that ramify in $F_i|K(t)$. Furthermore, the inertia subgroups of places in $F_i|K(t)$ can be mapped isomorphically onto the corresponding inertia subgroups in $F|K(t)$ (e.g. [55, Remark 11.24]).
If $char(K) = 0$ and the extension $F|K(t)$ can be defined over $\tilde{K}(t)$ with some field $\tilde{K} \subseteq K \cap \mathbb{C}$, this observation can be made even more precise by means of the theory of covering spaces: If one begins with the above realizations of cyclic groups $G_1, G_2 \leq G$, the extension $\tilde{F}|\tilde{K}(t)$ arising via descent of the base field will have a branch cycle description of the form $(\sigma_1, \sigma_1^{-1}, \sigma_2, \sigma_2^{-1})$.

Especially for $K = \mathbb{Q}_p$ with a "good" prime p, this may be used to obtain information about the Hurwitz curve corresponding to a family with this branch cycle description.

I.e., the above algorithm will yield p-adic approximations of polynomials for function field extensions $F|\mathbb{Q}_p(t)$ with given ramification. It may not be immediately obvious that the extension $F|\mathbb{Q}_p(t)$ will in fact lead to a function field extension defined over a number field. However, for suitable choice of the prime p and the ramification locus, descent arguments yield that the corresponding Galois cover can be defined over $\mathbb{Q}_p \cap \overline{\mathbb{Q}}$, and therefore in fact over some number field, cf. [24, Th. 2.10 with Cor. 2.11].

If the Hurwitz space belonging to the ramification data has a rational point, then sometimes one can choose the branch points accordingly, in order to obtain rational polynomials (or polynomials over small number fields, which usually would not be the case for arbitrary choice of the ramification locus). Note however that there are restrictions arising from the conditions on the ramification loci in w_1 and w_2.
E.g., when working over a Laurent series field $K((z))$, with $K \subseteq \mathbb{C}$, the ramification locus $t \mapsto (0, z, 1, z+1)$ (corresponding to inertia group generators $(\sigma_1, \sigma_1^{-1}, \sigma_2, \sigma_2^{-1})$) fulfills the conditions on distance of branch points given in the previous section. PGL_2-action can map this ramification locus to $(0, z^2, 1, \infty)$. Set $\lambda := z^2$, then the reduced Hurwitz curve can be defined by some polynomial equation $h(\lambda, \alpha) = 0$.
Again by an algebraization theorem such as [24, Cor. 2.11], our Galois cover can in fact be defined over the field of algebraic Laurent series $K((z)) \cap \overline{K(z)}$, i.e. even over some function field extension of $K(z)$. However, the field of definition will certainly contain $K(\lambda, \alpha)$.
Therefore, in order to obtain, via specialization of z into K, a cover defined over K with the prescribed ramification type, it is necessary to find a K-rational point in $K(z, \alpha)$, which will usually be a degree 2 extension of the function field $K(\lambda, \alpha)$ of the Hurwitz curve. Compare the second computational example in the following section.

Another possibility is to repeat the algorithm several times with different sets of branch points and thereby obtain data for interpolation in the Hurwitz space. This has been done in the first computational example in the next section. In that concrete example, we were able to determine algebraic dependencies over $\mathbb{Q}$ for all coefficients in the model, and therefore obtain an explicit family of polynomials over $\mathbb{Q}(t)$. Although this may not always be possible, even an algebraic dependency between two coefficients may yield a defining equation for the Hurwitz curve, which then may be used to search for rational points.

10.3 Computational examples

We illustrate the algorithm with a simple computational example: we patch Galois extensions with group S_3, with four ramification points and branch cycles of cycle type $(3, 3, 2.1, 2.1)$. This is a genus-one tuple in the action on 3 points. The corresponding Nielsen class is especially short, namely of length 2, with transitive braid group action, and braid orbit genus zero (even in the unsymmetrized case).

We start with two cyclic genus zero Galois extensions over $\mathbb{Q}_p(t)$ with $p = 73$ (here the prime can be chosen arbitrarily, as long as the base field contains the sixth roots of unity), with groups $\langle(1, 2, 3)\rangle \cong C_3$ and $\langle(1, 2)\rangle \cong C_2$ respectively. We parameterized these with the following polynomials:

- $f_1 := x^3 \cdot (k \cdot p \cdot w_2 - 1) + 1$ for the group C_3,
- $f_2 := p \cdot w_1 \cdot (-(p + 2) + (p - 2) \cdot x^2) - (x^2 - 1)$ for the group C_2.

Here $w_1 := \frac{1}{t-1}$, $w_2 := \frac{1}{t}$, and $k \in \mathbb{N}$ some integer (as we will later iterate over k).

This leads to the following ramification points:

- $w_2 \mapsto \frac{1}{kp}$ and $w_2 \mapsto \infty$ for a root field of the polynomial f_1,
- $w_1 \mapsto \frac{1}{p(p-2)}$ and $w_1 \mapsto \frac{1}{p(p+2)}$ for a root field of the polynomial f_2.

In particular, the ramification loci fulfill the conditions described in the preceding section.

In the variable t, this will yield the ramification locus $\{0, kp, p(p - 2) + 1, p(p + 2) + 1\}$ for the "patched" S_3-extension.

We develop the occurring p-adic integers to a precision of p^{100} and apply the algorithm described above to obtain a basis (in the form of columns of a matrix) of a degree-3 extension of $\mathbb{Q}_p(t)$ with the above ramification structure. The first column vector turns out to be constant (i.e. an element of the base field), so we choose the second column vector as a primitive element x and search for minimal algebraic dependencies between x and w_1. We know that the degree in x must be 3; the degree in w_1 turns out to be 3 as well.

We repeat this procedure sufficiently often by moving one of the branch points (i.e. varying k in the above definition of f_1). So we obtain polynomial dependencies $p_i(w_1(i), x(i)) = 0$, all of degree 3 in each of the variables, and with coefficients in $\mathbb{Q}_p$. Now interpolate the values of coefficients of any two fixed monomials $w_1^{m_j} x^{n_j}$ $(j = 1, 2)$ to obtain algebraic dependencies describing the Hurwitz space. In our case, all the coefficients occurring in the model could be expressed as rational functions in one particular coefficient a (namely the coefficient at $x \cdot w_1$), which is not particular surprising, as the braid orbit is very short and the Hurwitz curve is rational.

The algebraic dependencies obtained in this way are still a priori over $\mathbb{Q}_p$, but by good choice of the model, we can expect their coefficients to actually be rational numbers.
This led to the following polynomial $f(a, w_1, x) \in \mathbb{Q}(a, w_1)[x]$ (with independent transcendentals a, w_1):

$$f(a,w_1,x) := 1+a_1w_1+a_2w_1^2+a_3w_1^3+73axw_1+a_4xw_1^2+a_5xw_1^3+1/8x^3+a_6x^3w_1+a_7x^3w_1^2+a_8x^3w_1^3,$$

with

$$a_1 := -8/27 \cdot a^3 - 5401,$$

$$a_2 := 64/3 \cdot a^3 - 10731,$$

$$a_3 := 584/27 \cdot a^3 - 5329,$$

$$a_4 := \frac{-584/27 \cdot a^6 - 388944a^3 - 10503459/8}{a^2},$$

$$a_5 := \frac{-584/27 \cdot a^6 - 389017a^3 - 10503459/8}{a^2},$$

$$a_6 := \frac{-2/27 \cdot a^6 - 15841/8 \cdot a^3 - 143883/32}{a^3},$$

$$a_7 := \frac{8/729 \cdot a^{12} + 2336/3 \cdot a^9 + 83649313/8 \cdot a^6 + 94531131/2 \cdot a^3 + 20702317689/512}{a^6},$$

$$a_8 := \frac{-41464/729 \cdot a^{12} - 55240414/27 \cdot a^9 - 147243323517/8 \cdot a^6 - 3974078243781/32 \cdot a^3 - 107300112582087/512}{a^6}.$$

Furthermore, after replacing x by x/a (with the above coefficient a), it actually turns out that all the coefficients in the model become rational functions in $s := a^3$. I.e., $f(a, w_1, x/a) =: g(s, w_1, x) \in \mathbb{Q}(s, w_1)[x]$. Now the model can be somewhat simplified by applying some more fractional linear transformations in the variables s, w_1 and x. In particular, the places of $\mathbb{Q}(s)(w_1)$ ramifying in $\mathbb{Q}(s, w_1)(x)$ can be transformed to $w_1 \mapsto 0$, $w_1 \mapsto 1$, $w_1 \mapsto \infty$ and $w_1 \mapsto s^2$.

This leads to the following, somewhat nicer polynomial:

$$\tilde{g}(s,w_1,x) := w_1\cdot(w_1-s^2)^2\cdot x^3-3(w_1-\frac{37^2}{36^2})(w_1-1)(w_1-s^2)x-2(w_1-1)(w_1^2+(-\frac{25}{12}s+\frac{37}{432})w_1+\frac{37^2\cdot 71}{2^6\cdot 3^6}s-\frac{37^3}{2^6\cdot 3^6}).$$

Compare the computations in [8], which feature the same class tuple as a computational example, although with a different approach.

We include another example to demonstrate some techniques over fields of Laurent series: We try to patch an A_4-extension with the (genus one) class tuple $(3A, 3A, 3B, 3B)$ as ramification type from two cyclic extensions with Galois group C_3, e.g. $G_1 = \langle(1,2,3)\rangle$ and $G_2 = \langle(1,2,4)\rangle$. As the base field we choose $\mathbb{F}_{13}((z))(t)$ (note again that the prime field contains the third roots of unity). We set $r := 5$, $w_1 := \frac{r}{t-1}$ and $w_2 := \frac{r}{t}$ and chose polynomials $f_1(x,w_2) := x^3\cdot(zw_2-r)+r$ and $f_2(x,w_1) = zw_1\cdot(3+2x^3)-(x^3-1)$ for the C_3-extensions. In w_1-coordinates, this will yield the ramification locus $(\frac{5}{z-1}, -5, \frac{7}{z}, \frac{4}{z})$. Applying the above patching algorithm, we obtain (a z-adic approximation of) an algebraic dependency between w_1 and a primitive element x of the desired degree-4 extension (of degree 4 in both variables):

$$f(x,w_1) := \sum_{i,j=0}^{4} \alpha_{i,j}\cdot w_1^i\cdot x^j = 0.$$

In our case, $\alpha_{0,0} = 0$ and $\alpha_{1,0} = z$.[3] Next, we try to find algebraic dependencies between all the power series $\alpha_{i,j}$. It turns out that $\alpha_{1,0}(= z)$ and $\alpha_{0,1}$ fulfill a polynomial equation of relative degrees 2 and 6. This equation generates a function field of genus zero, and all the other $\alpha_{i,j}$ lie in this field. To find the connection of this function field with the Hurwitz curve, observe that the above ramification locus can be mapped to $(1, 0, \infty, 5\frac{(z+3)(z+6)}{z^2})$ via PGL_2. So after setting $\lambda := 5\frac{(z+3)(z+6)}{z^2}$, the Hurwitz curve, reduced modulo 13, should yield a degree 3 extension of $\mathbb{F}_{13}(\lambda)$, as the corresponding braid orbit is of length 3. Indeed, one obtains a tower of genus zero function fields, as given in Fig. 10.1.

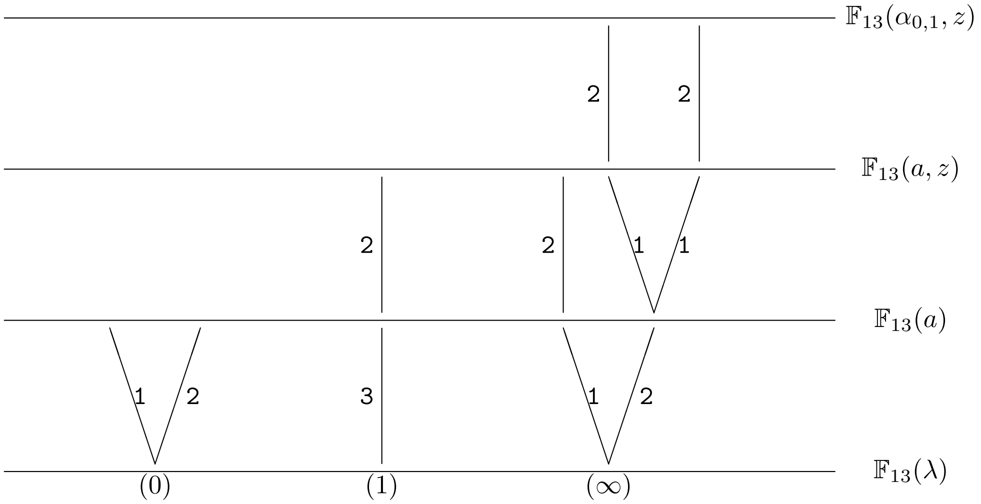
Here the extension $\mathbb{F}_{13}(a)|\mathbb{F}_{13}(\lambda)$ is ramified over $\lambda = 0, 1$ and ∞, with inertia group generators of cycle structure (2.1), (3) and (2.1). This corresponds exactly to the ramification given by the braid group action on the braid orbit of length 3.

All the other coefficients of our model lie in a degree-4 extension of $\mathbb{F}_{13}(a)$. It can therefore be expected that appropriate parameter changes will lead to a model with all the coefficients inside $\mathbb{F}_{13}(a)$.

Still, as the function field containing all our coefficients is of genus zero, specialization to appropriate

[3] The concrete coefficients, as well as the precise implementation in Magma, are included in a plain-text file.

Figure 10.1: Tower of function fields inside $\mathbb{F}_{13}((z))$ containing the coefficients of $f(x, w_1)$



values in $\mathbb{F}_{13}$ leads to polynomials over $\mathbb{F}_{13}(t)$ with the desired inertia groups, such as the following:

$$\tilde{f}(x, w_1) := (3w_1^4 + w_1^3 + 11w_1 + 12) \cdot x^4 + (7w_1^4 + 11w_1^3 + 4w_1 + 2) \cdot x^3$$

$$+(12w_1^4 + 8w_1^3 + 8w_1^2 + 4w_1 + 3) \cdot x^2 + (5w_1^4 + 7w_1^3 + 4w_1^2 + 10w_1 + 8) \cdot x + w_1^4 + 2w_1^3 + w_1^2 + 2w_1.$$

10.4 Proposals for further research

The above algorithm is very expensive because of the Cartan Decomposition of matrices with very big entries. It would be quite desirable to have an efficient algorithm for this decomposition. At the moment I cannot use it to compute covers of "interestingly" large degree.
With a faster algorithm, the following families, amongst others, deserve attention:

- $PSL_2(16)$, $(2A, 2A, 3A, 3A)$.
  $PSL_2(16)$ is the group of smallest permutation degree that has not yet been proven to be a regular Galois group over $\mathbb{Q}$ (for a non-regular realization, cf. [4]). The tuple proposed here is a genus-2 tuple in the action on 17 points, with a braid orbit of length 252. The reduced Hurwitz space is a curve of genus $g_{sym} = 31$.

- M_{24}, $(2B, 2B, 3A, 3A)$. This is a genus-1 tuple in the action on 24 points, with a braid orbit of length $l = 290$ and a reduced Hurwitz space of genus $g_{sym} = 14$.

If the Hurwitz space has a rational point, and in addition the genus-1-curve defined by the degree-24 polynomial at this point has suitable points, one would obtain M_{23}, not over $\mathbb{Q}(t)$, but at least over $\mathbb{Q}$.

The usual reality arguments at least assure the existence of real points for both the Hurwitz space and the genus-1 curve corresponding to the M_{23}-stem field.

Chapter 11

MAGMA programs

We give Magma implementations for the most important algorithms involved in the computations in the previous chapters.

11.1 Monodromy verification

The first algorithm computes the monodromy (in the form of a tuple of permutations) corresponding to a function field extension $\mathbb{C}(X,t)|\mathbb{C}(t)$.

```
monodromy:=function(f,ram,base, contr, sectors)
/*f in C[X][t]: a complex polynomial in 2 variables,
 ram: the list of finite ramification points (in t!),
 base (in C, not a ramification point): the base point
 Note that for this implementation the base point should NOT be collinear
(or too close to it) with any two finite ramification points
 contr: A contraction constant defining the stepsizes when moving from the
        base point towards a branch point.
 sectors: An integer defining the number of steps for a 360-degree turn
          around a branch point
*/

local f0, r0, r1, r, r_before, perm, mx, min, index, mindist_ram, m, t0;

/*Compute the roots of the specialized (by sending t to base) polynomial
*/
f0:=Evaluate(f,base);
 r0:=[root[1]: root in Roots(f0)];
```

```
/* A (somewhat arbitrary) constant to specify how close one should walk towards
   a branch point before circling around it
*/
mindist_ram:=1/4*Min([Abs(ram[i]-ram[j]): i,j in [1..#ram]| i ne j]);

/*perm will contain a sequence of permutations describing the monodromy
*/
perm:=[];

for i:=1 to #ram do
 r:=r0;
 t0:=base;

/*
walking on the line from the base point to the i-th ramification point,
until sufficiently close, and sort the roots of the new specialized polynomials
in accordance with the "old" roots
*/
 while Abs(t0-ram[i]) gt mindist_ram do
  t0+:=(ram[i]-t0)*contr;
  f0:=Evaluate(f,t0);
  r1:=[root[1]: root in Roots(f0)];
  m:=[];
  for j:=1 to #r0 do
   min,index:=Min([Abs(r[j]-r1[j2]): j2 in [1..#r0]]);
   m:=Append(m,r1[index]);
  end for;
  r:=m;
 end while;

r_before:=r; //The roots before turning around the ramification point

/*
circling around the ramification point (counter-clockwise)
*/
 for k:=1 to sectors do
  t0:=(t0-ram[i])*ComplexField()!(-1)^(2/sectors)+ram[i];
  f0:=Evaluate(f,t0);
  r1:=[root[1]: root in Roots(f0)];
  m:=[];
  for j:=1 to #r0 do
   min,index:=Min([Abs(r[j]-r1[j2]): j2 in [1..#r0]]);
   m:=Append(m,r1[index]);
  end for;
 r:=m;
 end for;

/*
creating the permutation induced by the monodromy action by comparing
the roots before and after the turn
*/
 mx:=[];
 for j:=1 to #r0 do
  min,index:=Min([Abs(r[j]-r_before[j2]): j2 in [1..#r]]);
  mx:=Append(mx,index);
 end for;

Append(~perm, Sym(#r0)!mx);
end for;

return perm;
end function;
```

11.2 p-adic lifting of solutions and algebraic dependencies

```
 /*
For a mod-p-reduction of a non-singular point on a Hurwitz space,
produce a sequence of lifts, with different ramification loci.
Special cases: a) For cover with 3 ramification points: apply just one lift.
       b) Works over a LaurentSeries-Ring K[[mu]] (instead of p-adic ring Z_p) as well.
          In this case, also apply just one lift, with branch locus depending on mu

pols: List of r monic polynomials f_1,...,f_r over a (r-2)*deg-dimensional polynomial ring
 (with deg as defined below). Each f_i is the specialization of f(X)-tg(X) at
```

```
  t-> ramified point. Here we demand that the last ramified point is infinity, i.e. f_r=g
 NOTE: f_r should be monic, while the other f_i should come with the correct leading
 coefficients!

ram_loci: a list of lists! Each element is a list of r-1 finite ramification points,
 corresponding to f_1,...,f_{r-1}
 (the r-th ramification point is demanded to be t -> infinity)
To allow p-adic lifting, all branch point tuples need to coincide modulo p!

v: Sequence of length (r-2)*deg; a mod-p-solution of the system of equations

deg: Degree of the polynomial f(X)-tg(X) in X.

steps: Number of Newton iterations that should be applied
*/
padiclifts:=function(pols, ram_loci, v, deg, steps)
 local lift, eqns, m, j, v1, v2;

 lift:=[];
for k:=1 to #ram_loci do

/*A set of equations that the lifted coefficients have to fulfill:*/
 eqns:=[];

 for i:=2 to #pols-1 do
  Append(~eqns, pols[1]-(ram_loci[k][i]-ram_loci[k][1])*pols[#pols]-pols[i]);
 end for;

 m:=[];
 for i:=1 to #eqns do for j:=0 to deg-1 do Append(~m,Coefficient(eqns[i],j));
 end for; end for;

 j:=JacobianMatrix(m);
 v1:=v;

 for i:=1 to steps do
  v2:=NewtonStep(v1,m,j); //to be defined: Newton step should return v1-j^-1(v1)*m
  v2[1]-v1[1]; //output for convenience/control
  v1:=v2;
 end for;

 Append(~lift,v2);
end for;

return lift;
end function;

/*
Function looking for algebraic dependencies of fixed degree between two coefficients
of a model, by interpolating through a sequence of p-adic lifts

a,b: Two sequences of the same length providing interpolation points
(should have length at least (deg_a+1)*(deg_b+1) in order to produce meaningful result)
deg_a,deg_b: intended relative degrees of the algebraic dependencies

(The goal is usually to find a dependency of minimal degree, i.e. d=1 below)
*/
algdep:=function(a,b, deg_a,deg_b)
local m, mat, ker, d, v, p, f;
m:=[];
for i:=0 to deg_a do
 for j:=0 to deg_b do
  for k:=1 to #a do
   Append(~m,a[k]^i*b[k]^j);
end for; end for; end for;

mat:=Matrix(Parent(a[1]),(deg_a+1)*(deg_b+1),#a,m);
ker:=Kernel(mat);
d:=Dimension(ker);


/*Case that no dependency is found:
*/
if d eq 0 then return d;
end if;
```

```
v:=Basis(ker)[1];
p<t,x>:=PolynomialRing(Parent(a[1]),2);
f:=p!0;
for i:=1 to (deg_a+1)*(deg_b+1) do
 f+:=v[i]*x^((i-1) mod (deg_b+1))*t^((i-1) div (deg_b+1));
end for;

return d,f;
end function;

/*
Analogon of algdep for Laurent-series-lifts
*/
algdep_laurent:=function(a,b, deg_a,deg_b, limit)
local m, mat, ker, d, v, p, f, z;
m:=[];
for i:=0 to deg_a do z:=a^i;
 for j:=0 to deg_b do
  if j ne 0 then z*:=b; end if;
  for k:=0 to limit-1 do
   Append(~m,Coefficient(z,k));
end for; end for; end for;

mat:=Matrix(CoefficientRing(Parent(a)),(deg_a+1)*(deg_b+1),limit,m);
ker:=Kernel(mat);
d:=Dimension(ker);

if d eq 0 then return d;
end if;

v:=Basis(ker)[1];
p<t,x>:=PolynomialRing(CoefficientRing(Parent(a)),2);
f:=p!0;
for i:=1 to (deg_a+1)*(deg_b+1) do
 f+:=v[i]*x^((i-1) mod (deg_b+1))*t^((i-1) div (deg_b+1));
end for;
```

```
return d,f;
end function;



/*
Function retrieving a rational number (with denominator not divisible by p)
 from its (sufficiently precise) development as a p-adic integer.
Typically, u is a p-adic integer computed to precision m (some power of p)
*/
padicToRational:=function(m,u)
local a1, a2, v1, v2, q, temp;
a1:=m;
a2:=Integers()!u; v1:=0; v2:=1;
for i:=1 to m do // Return will in fact be reached after much less than m steps

 if v2 ge (m/2)^(1/2) then return []; end if;
/*No rational number can be retrieved
*/

 if Abs(a2) lt (m/2)^(1/2) then return [a2,v2]; break i;
 else q:=Floor(a1/a2);
  a1:=a1-q*a2;
  v1:=v1-q*v2;
  temp:=a2;
  a2:=a1; a1:=temp;
  temp:=v2;
  v2:=v1; v1:=temp;
 end if;
end for;
end function;
```

11.3 Braid group action

```
/*
function checking whether two r-tuples of group elements are simultaneously
 conjugate via an element in a prescribed group
*/

isAllConjugate:=function(tup1,tup2,group)
local a, b, tup1_neu;
if #tup1 eq 0 then return true;
end if;

if not IsConjugate(group, tup1[1], tup2[1]) then return false;
end if;

a,b:=IsConjugate(group, tup1[1], tup2[1]);
tup1_neu:=[x^b: x in tup1];

return $$(Exclude(tup1_neu, tup1_neu[1]),Exclude(tup2, tup2[1]),
          Centralizer(group, tup2[1]));
end function;



/*
function receiving a tuple of elements of a finite group, applying to it
 the action of the braid beta_i.
If i is negative, the inverse of the |i|-th braid is applied
*/
braid:=function(m,i)
 local a;
 if i gt 0 then
  a:=m[i+1]; m[i+1]:=m[i+1]^-1*m[i]*m[i+1];
  m[i]:=a;
 else
  a:=m[-i]; m[-i]:=m[-i]*m[-i+1]*m[-i]^-1;
  m[-i+1]:=a;
 end if;
 return m; end function;
```

```
/*
A function finding a minimal (i.e. of cardinality one less than the length of the
braid orbit) sequence of braids which, when applied (in the given order) to a given
starting tuple, produce the whole braid orbit.
The length of the braid orbit is assumed to be known, in order to allow quicker
termination.

br is a list of the braids that should be applied.
Each braid is given as a sequence of non-zero integers i representing the product of the
respective braids beta_i.
*/
minimal_braidset:=function(tuple, length, group, br)
local m, braids, checked, new_tuple, is_contained;
m:=[tuple];

braids:=[];

/*
For every braid in br, keeping a list to which elements of m this braid has already
been applied.
*/
checked:=[];
for i:=1 to #br do Append(~checked,0); end for;

while #m lt length do
    for i:=1 to #checked do
        checked[i]+:=1;

/* Apply br[i]
*/
new_tuple:=m[checked[i]];
for j:=1 to #br[i] do
new_tuple:=braid(new_tuple,br[i][j]);
        end for;

is_contained:=false;
for tup in m do
if isAllConjugate(tup, new_tuple, group) then is_contained:=true; break tup; end if;
```

```
end for;

if not is_contained then
Append(~braids, [checked[i],i]);
Append(~m,new_tuple);
end if;
    end for;
end while;

return braids;
end function;
```

11.4 An algorithm to deform covers ramified over three points to such ramified over four points

We give an explicit algorithm to deform degenerate covers to non-degenerate ones, as described in Section 3.3.1. Here, we restrict to the case of gaining four point covers from three point covers, and also assume for simplicity that the starting cover belongs to a transitive subgroup of G.

Note that the aim of this algorithm is mainly to demonstrate an explicit implementation of the considerations in Section 3.3.1 that can be reused in similar situations, but not an implementation that covers all possible cases. In particular, this implementation uses only complex approximations. Therefore in some cases, problems with convergence will arise. One can deal with this by first developping *formal* Laurent series up to a certain precision, and only then specializing to complex values. However, this would complicate the implementation considerably.

```
/*
zeroes1: List of length 3, each element is a list of zeroes of the
 specialized (in t) polynomial belonging to the 3-point cover.
 The ramification points of the 3-point cover are required to be 0,1 and infinity.

mult1: List of length 3, as above. Each element is a list of
 multiplicities of the above zeroes (in the correct order!)

LeadCoeff: Leading Coefficient of the polynomial corresponding
 to the above 3-point cover, specialized at 0.
```

```
ramifications: A LIST of lists of length 3: ramification[i] contains,
 for each cycle of the inertia group generator over zero
 (i.e. for each entries of mult1[1]!) the ramification structure of the
 "opposite" degenerate cover

zeroes2: A LIST of lists of length 2. Each element contains a list of roots
 over s->0 and one of roots over s->1 for one "opposite" degenerate cover.
 The ordering of this lists needs to to corresponds to the ordering
         of the list "ramifications"
**NOTE: In this implementation, we demand all the leading coefficients of the
**  polynomials parameterizing the "opposite" covers to be 1. I.e., one should multiply
**  the zeroes with approprate constants to norm these polynomials
**  before running the algorithm!

mu: Complex number of small absolute value
 (corresponding to a specialized Laurent series parameter)
ram_index: Ramification index in the Hurwitz space
degree: The permutation degree of the group, i.e. the degree
 of the polynomial to be computed
precision: Expected precision of approximation of the solution

infty: true or false, depending on whether the place x->infty should extend
 the place t->infty or not.
** NOTE: We do not allow x->infty to extend any finite ramified place in t.

fixplaces: List determining which coefficients should be fixed (via PGL_2) to their
 start values. If "infty=true", this list should be of length 2, otherwise of length 3.
 An element of fixplaces should be a list [i,j,k], meaning the coefficient at x^k of
element number j of the list pols"i" (see below) should be fixed; 0<= k<= deg(pols"i"[j])-1.
*/
complexlaurent:=function(zeroes1, mult1, ramifications, LeadCoeff,
                  mu, ram_index, zeroes2, degree, precision, infty, fixplaces)

local C, multa, multb, multc, multd, polsa, polsb, polsc, polsd,
index1, index2,cf,p,q,x,v,ff_a,ff_b,ff_c,ff_d,ff1,ff2,mm,j,v2,prec0;

cf:=Parent(zeroes1[1][1]);
p:=PolynomialRing(cf,2*degree);
```

```
q<x>:=PolynomialRing(cf);

/*
C is a list of leading coefficients that arise for the "opposite" degenerate covers
   upon the respective specializations
*/
C:=[];
v:=[];
multa:={}; multb:={};
polsa:=[];
polsb:=[];

for i:=1 to #ramifications do
multa:=multa join SequenceToSet(ramifications[i][1]);
multb:=multb join SequenceToSet(ramifications[i][2]);

c:=LeadCoeff;
for j:=1 to #zeroes1[1] do if j ne i then
c*:=(zeroes1[1][i]-zeroes1[1][j])^mult1[1][j];
end if; end for;
for j:=1 to #zeroes1[3] do
c/:=(zeroes1[1][i]-zeroes1[3][j])^mult1[3][j];
 end for;
C:=Append(C,c);
end for;

multa:=SetToIndexedSet(multa);
multb:=SetToIndexedSet(multb);
for i:=1 to #multa do polsa:=Append(polsa,q!1);end for;
for i:=1 to #multb do polsb:=Append(polsb,q!1);end for;

for i:=1 to #ramifications do
 for j:=1 to #ramifications[i][1] do
  index1:=ramifications[i][1][j];
  for k:=1 to #multa do if multa[k] eq index1 then
   polsa[k]*:=(x-(zeroes1[1][i]+mu^(ram_index/mult1[1][i])
              *zeroes2[i][1][j]/(C[i]^(1/mult1[1][i]))));
   break k; end if; end for;
 end for;
end for;

for i:=1 to #ramifications do
 for j:=1 to #ramifications[i][2] do
  index2:=ramifications[i][2][j];
  for k:=1 to #multb do if multb[k] eq index2 then
   polsb[k]*:=(x-(zeroes1[1][i]+mu^(ram_index/mult1[1][i])
               *zeroes2[i][2][j]/(C[i]^(1/mult1[1][i]))));
   break k; end if; end for;
 end for;
end for;

polsc:=[];
multc:=SequenceToSet(mult1[2]);

multc:=SetToIndexedSet(multc);
for i:=1 to #multc do polsc:=Append(polsc,q!1);end for;

for i:=1 to #zeroes1[2] do
index1:=mult1[2][i];

  for k:=1 to #multc do if multc[k] eq index1 then
polsc[k]*:=(x-zeroes1[2][i]); break k; end if; end for;

end for;

polsd:=[];
multd:= SequenceToSet(mult1[3]);

multd:=SetToIndexedSet(multd);
for i:=1 to #multd do polsd:=Append(polsd,q!1);end for;

for i:=1 to #zeroes1[3] do
index1:=mult1[3][i];

  for k:=1 to #multd do if multd[k] eq index1 then
polsd[k]*:=(x-zeroes1[3][i]); break k; end if; end for;
```

```
end for;

q<x>:=PolynomialRing(p);
varcount:=0;

pols1:=[];
for i:=1 to #polsa do
 pols1:=Append(pols1,x^(Degree(polsa[i])));
 for j:=1 to Degree(polsa[i]) do
  if not ([1,i,Degree(polsa[i])-j] in fixplaces) then
   varcount+:=1;
   pols1[i]+:=x^(Degree(polsa[i])-j)*Name(p,varcount);
   v:=Append(v,Coefficient(polsa[i],Degree(polsa[i])-j));
   else pols1[i]+:=x^(Degree(polsa[i])-j)*Coefficient(polsa[i],Degree(polsa[i])-j);
  end if;
 end for;
end for;

pols2:=[];
for i:=1 to #polsb do
 pols2:=Append(pols2,x^(Degree(polsb[i])));
 for j:=1 to Degree(polsb[i]) do
 if not ([2,i,Degree(polsb[i])-j] in fixplaces) then
   varcount+:=1;
   pols2[i]+:=x^(Degree(polsb[i])-j)*Name(p,varcount);
   v:=Append(v,Coefficient(polsb[i],Degree(polsb[i])-j));
   else pols2[i]+:=x^(Degree(polsb[i])-j)*Coefficient(polsb[i],Degree(polsb[i])-j);
  end if;
 end for;
end for;

pols3:=[];
for i:=1 to #polsc do
 pols3:=Append(pols3,x^(Degree(polsc[i])));
 for j:=1 to Degree(polsc[i]) do
  if not ([3,i,Degree(polsc[i])-j] in fixplaces) then
   varcount+:=1;
   pols3[i]+:=x^(Degree(polsc[i])-j)*Name(p,varcount);
   v:=Append(v,Coefficient(polsc[i],Degree(polsc[i])-j));
   else pols3[i]+:=x^(Degree(polsc[i])-j)*Coefficient(polsc[i],Degree(polsc[i])-j);
  end if;
 end for;
end for;

pols4:=[];
for i:=1 to #polsd do
 pols4:=Append(pols4,x^(Degree(polsd[i])));
 for j:=1 to Degree(polsd[i]) do
  if not ([4,i,Degree(polsd[i])-j] in fixplaces) then
   varcount+:=1;
   pols4[i]+:=x^(Degree(polsd[i])-j)*Name(p,varcount);
   v:=Append(v,Coefficient(polsd[i],Degree(polsd[i])-j));
   else pols4[i]+:=x^(Degree(polsd[i])-j)*Coefficient(polsd[i],Degree(polsd[i])-j);
  end if;
 end for;
end for;

v:=Append(v,LeadCoeff);

ff_a:=q!1;
ff_b:=q!1;
ff_c:=q!1;
ff_d:=q!1;
for i:=1 to #pols1 do ff_a*:=pols1[i]^multa[i]; end for;
for i:=1 to #pols2 do ff_b*:=pols2[i]^multb[i]; end for;
for i:=1 to #pols3 do ff_c*:=pols3[i]^multc[i]; end for;
for i:=1 to #pols4 do ff_d*:=pols4[i]^multd[i]; end for;

if infty eq false then
ff1:=Name(p,2*degree)*ff_a-mu^ram_index*ff_d-(Name(p,2*degree)-mu^ram_index)*ff_b;
ff2:=Name(p,2*degree)*ff_a-ff_d-(Name(p,2*degree)-1)*ff_c;
else
ff1:=Name(p,2*degree)*ff_a-mu^ram_index*ff_d-(Name(p,2*degree))*ff_b;
ff2:=Name(p,2*degree)*ff_a-ff_d-(Name(p,2*degree))*ff_c;
```

```
end if;

mm:=Coefficients(ff1) cat Coefficients(ff2);
j:=JacobianMatrix(mm);

prec0:=Infinity();
while prec0 gt precision do
 v2:=NewtonStep(v,mm,j);
 prec0:=Max([Abs(v2[i]-v[i]): i in [1..2*degree]]); prec0;
 v:=v2;
end while;

return v2, <ff_a,ff_b,ff_c,ff_d>;
end function;
```

11.5 Moving through the Hurwitz space via braid group action

```
/*
function receiving as an argument a complex approximation of a genus zero cover
(including a list v of values and a list of polynomial equations for all ramified places),
 its r branch points and an integer ii with 1 <= |ii| <=r-1, representing the |ii|-th
 braid group generator.
The output is the (approximate) cover obtained after applying the action of the braid
to the original cover. If ii<0, the inverse of the respective braid is applied.

As the braiding action is performed by moving two branch points along a circle,
the remaining branch points need to be outside this circle to obtain the correct
braiding action!

The variable stepsize indicates how far the branch points should be moved in each step.
If this step was too big it is continually diminished in the process.
The variable bound gives an abort condition if the stepsize is getting too small.
precision gives the necessary precision of approximation in each Newton step
*/
cover_braid:=function(v,f,ram,ii, stepsize, bound, precision)

local mid, ram_neu, angle, test, eqns, j, v1, v2, v_neu, maxx, N, cf, i;
```

```
i:=Abs(ii);
cf:=Parent(ram[1]); //Complex field with given precision
mid:=(ram[i]+ram[i+1])/2; //center of the turn, between i-th and (i+1)-th branch point

ram_neu:=ram;
v_neu:=v;  //variable for the last successful approximation vector

angle:=0;     // variable for the angle of the braiding turn

while angle lt 2 and stepsize gt bound do
angle+:=stepsize;
angle;

test:=true; //controls whether the Newton iteration below converges
 if ii gt 0 then
 ram_neu[i]:=((ram[i]-mid)*cf!(-1)^(angle))+mid;
 ram_neu[i+1]:=((ram[i+1]-mid)*cf!(-1)^(angle))+mid;
 else
 ram_neu[i]:=((ram[i]-mid)/cf!(-1)^(angle))+mid;
 ram_neu[i+1]:=((ram[i+1]-mid)/cf!(-1)^(angle))+mid;
 end if;

/*Set of equations to be fulfilled approximately after each Newton iteration step*/
eqns:=[];

for i:=1 to #f do eqns:=eqns cat Coefficients(Evaluate(f[i],ram_neu)); end for;
   j:=JacobianMatrix(eqns);

 maxx:=Infinity(); /*Max-Norm of the difference to the last approximation vector;
     loop aborts if this becomes too large*/
 N:=0; //counts the number of iteration step; loop aborts if N is too high
 v1:=v_neu;

while maxx gt precision and test eq true do
 N+:=1;
  v2:=NewtonStep(v1,eqns,j);
  maxx:=Max({@ Abs(v2[i]-v1[i]): i in [1..#eqns]@});
```

```
if maxx gt 10^50 or N gt 20 then test:=false;
end if; //(somewhat arbitrary) abort conditions
  v1:=v2;
end while;

if test eq true then
 v_neu:=v2; //update the approximation vector, if iteration was successful

else
 angle-:=stepsize; stepsize:=stepsize/2;  //try again with smaller step size
end if;

end while;


if test eq true then

/*after complete 360-degree turn, set ramification locus back to original
  and do one more iteration to double-check*/
ram_neu[i]:=ram[i];
ram_neu[i+1]:=ram[i+1];

  eqns:=[];
for i:=1 to #f do eqns:=eqns cat Coefficients(Evaluate(f[i],ram_neu)); end for;
   j:=JacobianMatrix(eqns);

v1:=v_neu;

  maxx:=Infinity();
N:=0;
 while maxx gt precision and test eq true do
N+:=1;
 v2:=NewtonStep(v1,eqns,j);
  maxx:=Max({@ Abs(v2[1]-v1[1]): i in [1..#eqns]@});
if maxx gt 10^50 or N gt 20 then test:=false;end if;
  v1:=v2;
  end while;
```

```
else false; return []; //no result if the approximation went wrong
end if;

if test eq true then
 v_neu:=v2;
 return v_neu;
else false; return []; end if;
end function;
```

11.6 Algebraic Patching

Firstly we give several auxiliary functions (such as Weierstrass decomposition for series in one as well as in two variables, and Cartan decomposition for matrices) that are needed for the computations.

Note that one can often force these decompositions to become trivial by choice of a good model for the G_1- and G_2-extensions (see Chapter 10 for notation)!

```
/*
The pseudo-degree of a power series over a complete valued field (with valuation Norm())
*/
pseudodeg:=function(f)
 local m, max_norm, index;
 m:=[Norm(a): a in Reverse(Coefficients(f))];
//Norms of the Coefficients (with monomials in descending order)

 max_norm, index:=Max(m); //finds the highest monomial with maximal norm
 return #m-index;
end function;

/*
A two-dimensional analogon of the above.
For f in a ring A{w_1, w_2} (A a complete normed ring) as described in the chapter on
 "Algebraic patching", this returns:
a) an i in {1, 2} such that the maximal norm of the coefficients of f is attained
   for a monomial in w_i;
b) the exponent of the highest monomial attaining this maximal norm
```

```
*/
pseudodeg_2dim:=function(f)
 local max,c;
 max:=Max([Norm(a): a in Coefficients(f)]);
 for i:=0 to Degree(f,2)-1 do
   c:=Coefficient(f,2,Degree(f,2)-i);
   for j:=0 to Degree(c) do
     if Norm(Coefficient(UnivariatePolynomial(c),j)) eq max then
       return 2, Degree(f,2)-i;
     end if;
   end for;
 end for;
 return 1, pseudodeg(UnivariatePolynomial(Coefficient(f,2,0)));
end function;

/*
Weierstrass division for a (expansion to fixed precision of a ) convergent
 power series f in A{x} and a polynomial g in A[x].
 The return values q0 in A{x}, r0 in A[x] fulfill f = q0*g + r0 and deg(r0)<deg(g)
*/
weierstrasspol:=function(f,g)
 local pp,phi;
 if f eq 0 then
   return Parent(f)!0,Parent(f)!0;
 end if;
 pp:=PolynomialRing(CoefficientRing(Parent(f)));
 phi:=hom<pp->Parent(f)|Name(Parent(f),1)>;

 return phi(pp!f div pp!g), phi(pp!f mod pp!g);
end function;

/*
Weierstrass division for two convergent power series f,g in A{x}
(generalization of the function weierstrasspol)
*/
weierstrass:=function(f,g)
 local f0,g0,r0,q0,i,q1,r1;
 g0:=0;
 for i:=0 to pseudodeg(g) do
   g0:=g0+Coefficient(g,i)*Monomials(g)[i+1];
 end for;
 q0,r0:=weierstrasspol(f,g0);
 f0:=-q0*(g-g0);
 while f0 ne 0 do
   q1,r1:=weierstrasspol(f0,g0);
   q0:=q0+q1;
   r0:=r0+r1;
   f0:=-q1*(g-g0);
 end while;
 return q0,r0;
end function;

/*
Series decomposition via Weierstrass preparation theorem
For a convergent power series f in A{x}, this returns a normed polynomial p in A[x]
(of degree pseudodeg(f)), and a unit q in A{x} such that f=p*q^-1
*/
series_decompose:=function(f)
 local d,q,r;
 d:=pseudodeg(f);
 q,r:=weierstrass(Name(Parent(f),1)^d, f);
 return Name(Parent(f),1)^d-r, q;
end function;


/*
Two-dimensional series decomposition
For f in K{w1, w2}, this returns a unit u in K{w1, w2} and a polynomial p in one
 variable w_i, such that f=p*u^-1. (cf. Lemma 3.2.6 in Jarden, "Algebraic Patching")
*/
series_decompose_2dim:=function(f)
 local i,d,p,f0,pp,qq,u1,u2,v,u,phi,wi,wj,p0,u0;
 i,d:=pseudodeg_2dim(f);
 if d eq 0 then
   p:=Evaluate(f,[0,0]);
   f0:=Invert(1/p*f); // Norm(1 - 1/p*f) < 1, as pseudodeg(f) = 0
   /* requires function Invert() for such 1/p*f!
         e.g.
         Invert:=function(f)
         local a,finv;
           a:=1-f;
           finv:=1;
           while a ne 0 do
            finv:=finv+a;
            a:=a*(1-f);
           end while;
           return finv;
         end function;
      */

   return Parent(f)!p, Parent(f)!f0;
      // In this case the polynomial p is actually a constant
 else

pp:=PolynomialRing(CoefficientRing(Parent(f)));
   qq<v>:=PolynomialRing(pp);
   wi:=Name(Parent(f),i);
   wj:=Name(Parent(f),(i mod 2)+1);
   gen:=Generators(DivisorIdeal(Parent(f)))[1];
/* This generator should be of the form (c1-c2)*w1*w2-r*(w1-w2); cf. the chapter
   on "Algebraic Patching"*/


   if i eq 1 then
     f0:=Evaluate(f,[v,Name(pp,1)]);
   else
     f0:=Evaluate(f,[Name(pp,1),v]);
   end if;
   p,u:=series_decompose(f0);
   qq2,phi:=ChangeRing(qq,Parent(f),hom<pp->Parent(f)|wj>);
   phi2:=hom<qq2 -> Parent(f)|wi>;
   p:=phi2(phi(p));
   u:=phi2(phi(u));
   p:=(1-(-1)^i*(Coefficients(gen)[1]/Coefficients(gen)[2])*wj)^d*p;
   u:=(1-(-1)^i*(Coefficients(gen)[1]/Coefficients(gen)[2])*wj)^d*u;

   i,d:=pseudodeg_2dim(p);
   if d eq 0 then
     p0:=Evaluate(p,[0,0]);
     f0:=Invert(1/p0*p);
     return Parent(f)!p0, Parent(f)!f0*u;
   else
     if i eq 1 then
       f0:=Evaluate(p,[v,Name(pp,1)]);
     else
       f0:=Evaluate(p,[Name(pp,1),v]);
     end if;
     p,u0:=series_decompose(f0);
     wi:=Name(Parent(f),i);
     wj:=Name(Parent(f),(i mod 2)+1);
   qq2,phi:=ChangeRing(qq,Parent(f),hom<pp->Parent(f)|wj>);
   phi2:=hom<qq2 -> Parent(f)|wi>;
   p:=phi2(phi(p));
   u:=u*phi2(phi(u0));

   return Parent(f)!p, Parent(f)!u;
   end if;
 end if;
end function;


/*
Two-dimensional analogue of weierstrasspol (cf. Cor.3.2.8 in Jarden, "Algebraic Patching")
For f in A{w1, w2} and g in A[w1, w2], this returns q0 and r0 such that f = q0*g + r0
*/
weierstrass_2dim:=function(f,g)
 local w1,w2,gen, h,u, h1,u1,h2,u2, pp, phi1,phi2, f1,f2, q1,r1,q2,r2;

 w1:=Name(Parent(g),1);
 w2:=Name(Parent(g),2);
 gen:=Generators(DivisorIdeal(Parent(g)))[1];
```

```
/* This generator should be of the form (c1-c2)*w1*w2-r*(w1-w2);
cf. the chapter on "Algebraic Patching"*/

 h,u:=series_decompose_2dim(g);

  h1:=(1-(Coefficients(gen)[1]/Coefficients(gen)[2])*w2)^Degree(h,2)*h;
  u1:=(1-(Coefficients(gen)[1]/Coefficients(gen)[2])*w2)^Degree(h,2)*u;
  h2:=(1+(Coefficients(gen)[1]/Coefficients(gen)[2])*w2)^Degree(h,1)*h;
  u2:=(1+(Coefficients(gen)[1]/Coefficients(gen)[2])*w2)^Degree(h,1)*u;
//one of Degree(h,2) and Degree(h,1) is =0

 pp:=PolynomialRing(CoefficientRing(Parent(g)));
 phi1:=hom<pp->Parent(f)|Name(Parent(f),1)>;
 phi2:=hom<pp->Parent(f)|Name(Parent(f),2)>;
 f1:=Coefficient(f,2,0);
 f2:=Coefficient(f,1,0)-Evaluate(f,[0,0]);
 q1,r1:=weierstrasspol(pp!UnivariatePolynomial(f1),pp!UnivariatePolynomial(h1));
 q2,r2:=weierstrasspol(pp!UnivariatePolynomial(f2),pp!UnivariatePolynomial(h2));
 return phi1(q1)*u1+
        phi2(q2)*u2 ,
        phi1(r1)+phi2(r2);
end function;


/*
Cartan decomposition for matrices over a ring A{w1, w2} of convergent power series
 in two variables.
For a non-singular square matrix f over the ring A{w1, w2}, compute square matrices a1b
(over A{w1}) and a2b (over A{w2}) such that f = a1b^{-1}*a2b^{-1}.
This function only returns a2b, as this is sufficient for the patching process
*/
CartanDecompose:=function(f)
 local a,a1,a2,a2b;
 a:=f-1;
 a1:=Parent(f)![Coefficient(a[i][j],2,0):
  j in [1..Degree(Parent(f))], i in [1..Degree(Parent(f))]];
 a2:=Parent(f)![Coefficient(a[i][j],1,0)-Evaluate(a[i][j],[0,0]):
  j in [1..Degree(Parent(f))], i in [1..Degree(Parent(f))]];
 a2b:=Parent(f)!(1-a2);
 while a ne 0 do
   a:=(1-a1)*(1+a)*(1-a2)-1;
   a1:=Parent(f)![Coefficient(a[i][j],2,0):
    j in [1..Degree(Parent(f))], i in [1..Degree(Parent(f))]];
   a2:=Parent(f)![Coefficient(a[i][j],1,0)-Evaluate(a[i][j],[0,0]):
    j in [1..Degree(Parent(f))], i in [1..Degree(Parent(f))]];
   a2b:=a2b*(1-a2);
 end while;
 return a2b;
end function;
```

Next, an algorithm realizing algebraic patching over $\mathbb{Q}_p(t)$ (the function field over a p-adic field), i.e. constructing (a p-adic expansion of) a vector space basis as in Lemma 10.2. The implementation only considers the case $G = \langle G_1, G_2 \rangle$, where G_1 and G_2 are cyclic, and begins with genus zero realizations with Galois groups G_1 and G_2 respectively.

```
/* Auxiliary function.
Computes the adjoint matrix of a given Vandermonde matrix.
(Cf. Turner, "Inverse of the Vandermonde matrix and applications").
*/
Adjugate_Vandermonde:=function(A)
local L,U;
L:=Parent(A)!0;
U:=Parent(A)!0;
for i:=1 to Degree(Parent(A)) do
 for j:=1 to Degree(Parent(A)) do
   if i ge j then
     L[i][j]:=(-1)^(i+j);
     for k1:=1 to Degree(Parent(A)) do
       for k2:=k1+1 to Degree(Parent(A)) do
         if not ((k1 eq j or k2 eq j) and k2 le i) then
           L[i][j]:=L[i][j]*(A[k2][2]-A[k1][2]);
         end if;
       end for;
     end for;
   end if;
 end for;
end for;
```

```
for i:=1 to Degree(Parent(A)) do
 for j:=1 to Degree(Parent(A)) do
   if i eq j then
     U[i][j]:=1;
   else
     if j ge 2 then
       U[i][j]:=-U[i][j-1]*A[j-1][2];
       if i ge 2 then
         U[i][j]:=U[i][j]+U[i-1][j-1];
       end if;
     end if;
   end if;
 end for;
end for;
return U*L;
end function;


/*
Choose a permutation group g, elements alpha1 and alpha 2 of g
(generating cyclic subgroups g1 resp. g2)
and parameters prime (=1 mod Lcm(#g1,#g2)), limit for precision of p-adic expansions
and  r,c1,c2 (for the rings of Mittag-Leffler series; with r,c1,c2 fulfilling
 conditions as described in the chapter "An algorithm for algebraic patching")

Also choose two ramified places for g1- and g2-extension respectively.
(Conditions on ramification locus need to be observed!)
The elements of ram_places"i" should be linear polynomials over Q of the form t-a;
 or =1 if the infinite place should ramify.
Polynomials for primitive elements x of (subfields of) g1- and g2-extensions
will then be created via the following conventions (which are not mandatory!):
 (i) The places x->0 and x->infty will extend the ramified places.
 (ii) x->1 will be an extension of the place at w1->0 resp. w2->0
      (which has to be unramified!).
*/

cyclic_patching:=function(
g,alpha1,alpha2, prime, limit, r,c1,c2, ram_places1, ram_places2)
```

```
local orb, s1,s2, ss1,ss2, p,w1,w2, ls, t, p_ls, x, pp,t0, phi1,phi2,
      U, AdjU, V, AdjV, detU, detV,
      zp, p0, zeta, f1, t1, xx, mat1, f2,t2,yy, mat2, cyc1,cyc2,
      h1,u1,h2,u2, C1,C2, m, m_tilde, c,b,c0, test, M, M_tilde, cd, V_neu;

/* Finding and sorting
double coset representatives for g1,g2
(here only for cyclic g1, g2!)
*/

orb:=Orbits(sub<g|alpha1>);
s1:=[IndexedSetToSequence(orb[i]): i in [1..#orb]];
orb:=Orbits(sub<g|alpha2>);
s2:=[IndexedSetToSequence(orb[i]): i in [1..#orb]];

ss1:=[];
for i:=1 to #s1 do for j:=1 to #s1[i] do ss1:=Append(ss1,s1[i][j]); end for; end for;
ss2:=[];
for i:=1 to #s2 do for j:=1 to #s2[i] do ss2:=Append(ss2,s2[i][j]); end for; end for;

p<w1,w2>:=PolynomialRing(Integers(prime^limit),2);
p<w1,w2>:=p/ideal<p|(c1-c2)*w1*w2-r*(w1-w2)>;
ls<t>:=LaurentSeriesRing(Rationals(),limit);
p_ls<x>:=PolynomialRing(ls);
pp<t0>:=PolynomialRing(Rationals());
phi1:=hom<pp->p | w1>;
phi2:=hom<pp->p | w2>;

U:=Matrix(p,0,0,[]);
AdjU:=Matrix(p,0,0,[]);

V:=Matrix(p,0,0,[]);
AdjV:=Matrix(p,0,0,[]);

detU:=1;
detV:=1;

zp:=pAdicRing(prime, limit);
```

```
p0:=PolynomialRing(zp);

/* Choosing polynomials f(x,t) for the extensions with groups g1,g2
and developping x as a power series
*/
for a in s1 do
 zeta:=Roots(p0!CyclotomicPolynomial(#a))[1][1];
 zeta:=Integers(prime^limit)!(Integers()!(zeta));
 f1:=Coefficient(ram_places1[1],0)/Coefficient(ram_places1[2],0)
 *x^#a*ls!(ram_places1[2]) - ls!(ram_places1[1]);
/*
Polynomials f1, f2 may be altered as long as constraints
   e.g. on ramification are observed.*/

 for root in Roots(f1) do if Evaluate(root[1],0) eq 1 then
  t1:=Evaluate(root[1],t0); break root;
 end if; end for;
 xx:=phi2(t1);

/* Filling up the representation matrices for the g_i-extensions
(as described in the chapter "An algorithm for algebraic patching")
*/
 mat1:=[];
 for i:=0 to #a-1 do
   for j:=0 to #a-1 do
     mat1:=Append(mat1, (zeta^i*xx)^j);
   end for;
 end for;
 U:=DiagonalJoin(U,Matrix(p,#a,#a,mat1));
 AdjU:=DiagonalJoin(Determinant(Matrix(p,#a,#a,mat1))*AdjU,
   detU*Adjugate_Vandermonde(Matrix(p,#a,#a,mat1)));
 detU:=detU*Determinant(Matrix(p,#a,#a,mat1));
end for;

for a in s2 do
 zeta:=Roots(p0!CyclotomicPolynomial(#a))[1][1];
 zeta:=Integers(prime^limit)!(Integers()!(zeta));
 f2:=Coefficient(ram_places2[1],0)/Coefficient(ram_places2[2],0)
 *x^#a*ls!(ram_places2[2]) - ls!(ram_places2[1]);

 for root in Roots(f2) do if Evaluate(root[1],0) eq 1 then
  t2:=Evaluate(root[1],t0); break root;
 end if; end for;
 yy:=phi1(t2);

 mat2:=[];
 for i:=0 to #a-1 do
   for j:=0 to #a-1 do
     mat2:=Append(mat2, (zeta^i*yy)^j);
   end for;
 end for;
 V:=DiagonalJoin(V,Matrix(p,#a,#a,mat2));
 AdjV:=DiagonalJoin(Determinant(Matrix(p,#a,#a,mat2))*AdjV,
   detV*Adjugate_Vandermonde(Matrix(p,#a,#a,mat2)));
 detV:=detV*Determinant(Matrix(p,#a,#a,mat2));
end for;

/*
Resorting the matrices appropriately, according to the sequence of double coset
representatives. Determinants and adjoint matrices are manipulated accordingly.
*/
cyc1:=CycleDecomposition(Sym(Degree(g))!ss1);
cyc2:=CycleDecomposition(Sym(Degree(g))!ss2);

for i:=1 to #cyc1 do
 for j:=2 to #cyc1[i] do
   U:=SwapRows(U,cyc1[i][1], cyc1[i][j]);
   AdjU:=-SwapColumns(AdjU,cyc1[i][1], cyc1[i][j]);
   detU:=-detU;
 end for;
end for;
for i:=1 to #cyc2 do
 for j:=2 to #cyc2[i] do
   V:=SwapRows(V,cyc2[i][1], cyc2[i][j]);
   AdjV:=-SwapColumns(AdjV,cyc2[i][1], cyc2[i][j]);
   detV:=-detV;
 end for;
end for;

/*
The actual patching step, obtaining from two vector space bases, contained in
different algebras, a base contained in the intersection (which is the
fixed field of a point stabilizer of G in a Galois extension with group G).
*/
h1, u1:=series_decompose_2dim(detU);
h2, u2:=series_decompose_2dim(detV);
C1:=u1*AdjU*V;
C2:=u2*AdjV*U;

m:=[];
m_tilde:=[];
for i:=1 to Degree(Parent(C2)) do
 for j:=1 to Degree(Parent(C2)) do
   c,b:=weierstrass_2dim(p!(C2[i][j]),p!(h1*h2));
   c0:=Evaluate(c,[0,0]);
   test:=1;
   while c ne c0 and Norm(c-c0) ge 1/Max([Norm(C1[i0][j0]):
    i0 in [1..Degree(Parent(C1))], j0 in [1..Degree(Parent(C1))]]) do
     c0+:=Coefficient(c,1,test)*w1^test+Coefficient(c,2,test)*w2^test;
     test:=test+1;
   end while;
   c0;
   Append(~m_tilde,c-c0);
   Append(~m,h1*h2*c0+b);
 end for;
end for;

M:=Parent(C1)!m;
M_tilde:=1-C1*Parent(C1)!m_tilde;

cd:=CartanDecompose(M_tilde);
V_neu:=V*M*cd; //The matrix containing the desired vector space basis
return V_neu;
end function;
```

Appendix A

New Mathieu group polynomials with $r \geq 4$ branch points

As many of our computations have been dealing with the Mathieu groups, it should be appropriate to summarize the polynomials obtained through these computations over various fields. These include new polynomials over $\mathbb{Q}$ (for the small Mathieu groups), over certain number fields, over certain finite fields as well as complex approximations for polynomials with 4 or 5 branch points. The complex approximations cover the majority of genus zero tuples of rational classes in M_{24} and M_{23}. As they are usually too lengthy to fit comfortably into a table, see the following plain-text files:

- "`M24_(2,2,2,8)_approx.txt`" (for the family with inertia group generators of classes $(2A, 2A, 2B, 8A)$ in M_{24}),
- "`M24_(2,2,2,8)_approx.txt`" (for the family with classes $(2A, 2A, 2B, 8A)$ in M_{24}),
- "`M24_(2,2,4a,4b).txt`" (for the $(2A, 2A, 4A, 4B)$-family in M_{24}),
- "`M24_(2,2,4b,6).txt`" (for the $(2A, 2A, 4B, 6A)$-family in M_{24}),
- "`M24_(2,2,4b,5).txt`" (for the $(2A, 2A, 4B, 5A)$-family in M_{24}),
- "`M24_(2,2,3,4).txt`" (for the $(2A, 2A, 3B, 4B)$-family in M_{24}),
- "`M24_(2,2,2,2,4)_approx.txt`" (for the $(2A, 2A, 2A, 2A, 4B)$-family in M_{24}),
- "`M23_(2,2,3,5)_approx.txt`" (for the $(2A, 2A, 3A, 5A)$-family in M_{23}),
- "`M23_(2,2,4,4).txt`" (for the $(2A, 2A, 4A, 4A)$-family in M_{23}),
- "`M23_(2,2,2,2,3)_approx.txt`" (for the $(2A, 2A, 2A, 2A, 3A)$-family in M_{23}).

In the following table we collect the other cases (polynomials over number fields or finite fields) with at least four branch points[1].

[1] Of course during the computations, polynomials with 3 branch points over certain number fields were obtained as well, see Chapters 5.1 and 5.3.

Group	Branch cycle structure	Field of definition	Polynomial
M_{11}	$(2^4.1^3, 2^4.1^3, 3^3.1^2, 4^2.1^3)$	$\mathbb{Q}$	$(77x^3+10989x^2+129816x+496368)^3\cdot(77x^2+2376x+15472)-t\cdot(11x^2-1296)^4\cdot(11x^2+143x+621)$.
M_{12}	$(2^4.1^4, 2^4.1^4, 2^4.1^4, 6^2)$	$\mathbb{Q}$	$(1+x^2)B^2+(t-A)^2$, with $A := -\frac{37040901254696641}{171619330843980000}x^6+\frac{33418800162487519439}{1121246294847336000}x^5-\frac{643838351275918002272217}{4688304507521660928000}x^4+\frac{81506169578192757684274951729795277}{318335564340980037304990890393600}x^3-\frac{1506221663493056801339570027722377061637021513009}{768532040995657748567302296663008952818073600}x^2-\frac{102109142900372062943594687109131533969014356304708283672663}{144953540235644427154530313893803793135770931415744512000}x-\frac{264437418140061448668509460089274099836762034357457529964169661}{1136435755447452308891517660927421738184444102299436974080000}$, and $B := \frac{161170153687309}{321504313934720}x^4+\frac{127423795320837923833}{567133609780846080}x^3-\frac{340397859783855225607653198324901}{136918522297195714969888555500080}x^2+\frac{382035203164320375297138535897341995679707107}{5738739852118113415227765058714224558080}x-\frac{1364346105683398322045488674317573232548120754570946621}{3711048137113272584601390524674956301479030502195200}$.
M_{12}	$(2^4.1^4, 2^4.1^4, 2^6, 5^2.1^2)$	$\mathbb{Q}$	$(x^6+1/3\cdot x^4-175/1728\cdot x^3+689/9216\cdot x^2-4333/165888\cdot x+15731/5971968)^2-237/3125\cdot t\cdot(x^7-26/237\cdot x^6-443/3792\cdot x^5+30605/273024\cdot x^4-1735175/19657728\cdot x^3+58925/1638144\cdot x^2-2367125/314523648\cdot x+6687625/11322851328)+9/6250\cdot t^2\cdot(x^2-7/24\cdot x+533/10368)$
M_{23}	$(2^8.1^7, 2^8.1^7, 3^6.1^5, 5^4.1^3)$	$\mathbb{F}_{19}$	$x^3\cdot(x^5+x^4-x^3-x^2+7)^3\cdot(x^5+6x^4+x^3+4x^2+12x+1)-t\cdot(x^3+2x^2+13x+5)^5\cdot(x^3+x^2+2x+6)$
M_{24}	$(2^8.1^8, 2^8.1^8, 2^8.1^8, 23.1)$	$\mathbb{Q}(\sqrt{-23})$	$(x^8+4x^7+(-\alpha+7)x^6+(6\alpha+30)x^5+(26\alpha+82)x^4+(16\alpha+272)x^3+(44\alpha+252)x^2+(80\alpha-240)x+40\alpha+8)^2\cdot(x^8-8x^7+(2\alpha+34)x^6+1/2(-3\alpha-135)x^5-(34\alpha+74)x^4+(238\alpha+470)x^3-(736\alpha+1248)x^2+(1082\alpha+1074)x-(920\alpha+184))-t\cdot x$, with $\alpha := \sqrt{-23}$.
M_{24}	$(2^8.1^8, 2^8.1^8, 2^{12}, 8^2.4.2.1^2)$	$\mathbb{F}_{17}$	$(x^{12}+x^{11}+2\cdot x^9+11\cdot x^8+9\cdot x^7+4\cdot x^6+15\cdot x^5+14\cdot x^4+15\cdot x^3+2\cdot x+15)^2-t\cdot(x^2+16\cdot x+10)^8\cdot(x+11)^2\cdot(x^2+4\cdot x+11)$
M_{24}	$(2^8.1^8, 2^8.1^8, 2^8.1^8, 2^8.1^8, 4^4.2^2.1^4)$	$\mathbb{F}_{17}$	$(16x^{24}+10x^{23}+12x^{21}+10x^{20}+15x^{19}+6x^{18}+3x^{17}+4x^{16}+8x^{14}+14x^{13}+12x^{12}+16x^{11}+16x^{10}+16x^8+4x^7+14x^6+6x^5+7x^4+13x^3+16x+4)-t\cdot(x^4+3x^3+13x^2+x+2)^4\cdot x^2\cdot(x^4+15x^3+12x+15)$

Table A.1: New Mathieu group polynomials

Bibliography

[1] A.O.L. Atkin, H.P.F. Swinnerton-Dyer, *Modular forms on noncongruence subgroups.* Combinatorics (Proc. Sympos. Pure Math., Vol. XIX, Univ. California, Los Angeles, Calif., 1968), Amer. Math. Soc., Providence, R.I. (1971), 1-25.

[2] P. Bailey, M. Fried, *Hurwitz monodromy, spin separation and higher levels of a modular tower.* Proc. Sympos. Pure Math 70, Amer. Math. Soc. (2002), 79-220.

[3] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system I: The user language.* J. Symb. Comput. 24 (1997), 235-265.

[4] J.G. Bosman, *A polynomial with Galois group* $SL_2(F_{16})$. LMS J. Comput. Math. 10 (2007), 378-388.

[5] A. Cadoret, *Lifting results for rational points on Hurwitz spaces.* Israel Journal of Mathematics, vol. 164 (2008), 19-61.

[6] G. Chèze, *Absolute irreducibility, Newton polytopes and modular computations.* Preprint, available at `www.math.univ-toulouse.fr/~cheze/cheze_eaca.ps`.

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

[8] J.-M. Couveignes, *Boundary of Hurwitz spaces and explicit patching.* J. Symb. Comput. 30 (2000), 739-759.

[9] J.-M. Couveignes, L. Granboulan, *Dessins from a geometric point of view.* Leila Schneps (editor), The theory of Grothendieck's dessins d'enfants, Cambridge University Press (1994), 79-113.

[10] P. Debes, M. Fried, *Rigidity and real residue class fields.* Acta Arithmetica 56.4 (1990), 291-323.

[11] P. Debes, M. Fried, *Non-rigid constructions in Galois theory.* Pacific J. Math. 163, No. 1 (1994), 81-122.

[12] M. Dettweiler, *Kurven auf Hurwitzräumen und ihre Anwendungen in der Galoistheorie.* PhD Thesis, Erlangen (1999).

[13] M. Deuring, *Reduktion algebraischer Funktionenkörper nach Primdivisoren des Konstantenkörpers.* Mathematische Zeitschrift 47 (1942), 643-654.

[14] N. Elkies, *The complex polynomials* $P(x)$ *with* $Gal(P(x)-t) \cong M_{23}$. Proceedings of the Tenth Algorithmic Number Theory Symposium (2013), 359-367.

[15] W. Feit, R. Lyndon, L.L. Scott, *A remark about permutations.* J. Comb. Theory, Ser. A 18 (1975), 234-235.

[16] M. Fried, H. Völklein, *The inverse Galois problem and rational points on moduli spaces.* Math. Ann. 290 (1991), no. 4, 771-800.

[17] D. Frohardt, K. Magaard, *Composition factors of monodromy groups.* Annals of Mathematics. Second Series, 154 (2001), 327-345.

[18] L. Gerritzen, F. Herrlich, M. van der Put, *Stable* n*-pointed trees of projective lines.* Indag. math. 50 (1988), 131-163.

[19] L. Granboulan, *Construction d'une extension reguliere de* $\mathbb{Q}(T)$ *de groupe de Galois* M_{24}. Experiment. Math. 5 (1996), no. 1, 3-14.

[20] B. Green, M. Matignon, F. Pop, *On valued function fields I.* Manuscr. Math. 65 (1989) 357-376.

[21] R. Guralnick, J. Thompson, *Finite groups of genus zero.* J. Alg. 131 (1990), 303-341.

[22] E. Hallouin, *Study and computation of a Hurwitz space and totally real* $PSL_2(\mathbb{F}_8)$*-extensions of* $\mathbb{Q}$. J. Alg. 321 (2009), 558-566.

[23] E. Hallouin, E. Riboulet-Deyris, *Computation of some moduli spaces of covers and explicit* S_n *and* A_n *regular* $\mathbb{Q}(t)$*-extensions with totally real fibers.* Pacific Journal of Math. 211, No. 1 (2003), 81-99.

[24] D. Harbater, *Galois coverings of the arithmetic line.* "Number Theory: New York, 1984-85". Springer LNM, vol. 1240 (1987), 165-195.

[25] W.J. Harvey, *Cyclic groups of automorphisms of a compact Riemann surface.* Quart. J. Math. 17 (1966), 86-97.

[26] A. Hurwitz, *Über ternäre diophantische Gleichungen dritten Grades.* Vierteljahrschr. d. Naturf. Ges. in Zürich 62 (1917), 207-229.

[27] M. Jarden, *Algebraic Patching.* Springer Monographs in Mathematics, Berlin-Heidelberg (2011).

[28] M. Klug, M. Musty, S. Schiavone, J. Voight, *Numerical calculation of three-point branched covers of the projective line*. Preprint (2013), available at `http://arxiv.org/abs/1311.2081`.

[29] J. Klüners, G. Malle, *Explicit Galois realization of transitive groups of degree up to 15*. J. Symb. Comput. 30 (2000), 675-716.

[30] J. Klüners, G. Malle, *A database for field extensions of the rationals*. LMS Journal of Computation and Mathematics 4 (2001), 182-196.

[31] S. Lang, *Algebra*. Graduate Texts in Mathematics, Vol. 211, Springer (2002).

[32] A.K. Lenstra, H.W. Lenstra, L. Lovasz, *Factoring polynomials with rational coefficients*. Mathematische Annalen 261 (1982), 513-534.

[33] K. Magaard, S. Shpectorov, H. Völklein, *A GAP package for braid orbit computation and applications*. Experimental Math. Vol. 12 (2003), No. 4, 385-393.

[34] K. Magaard, *Monodromy and sporadic groups*. Comm. Algebra 21 (1993), 4271-4297.

[35] G. Malle, *Multi-parameter polynomials with given Galois group*. J. Symb. Comput. 21 (2000), 1-15.

[36] G. Malle, *Polynomials with Galois groups* $\mathrm{Aut}(M_{22})$*,* M_{22}*, and* $\mathrm{PSL}_3(\mathbb{F}_4)\cdot 2_2$ *over* $\mathbb{Q}$. Math. Comp. 51 (1988), 761-768.

[37] G. Malle, *Polynomials for primitive nonsolvable permutation groups of degree* $d \leq 15$. J. Symb. Comput. 4 (1987), 83-92.

[38] G. Malle, *Fields of definition of some three point ramified field extensions*. Leila Schneps (editor), The theory of Grothendieck's dessins d'enfants, Cambridge University Press (1994), 115-145.

[39] G. Malle, B.H. Matzat, *Inverse Galois Theory*. Springer Monographs in Mathematics, Berlin-Heidelberg (1999).

[40] H. Mathieu, *Das Verhalten des Geschlechts bei Konstantenreduktion algebraischer Funktionenkörper*. Archiv der Mathematik 20 (1969), 597-611.

[41] B.H. Matzat, *Rationality criteria for Galois extensions*. Math. Sci. Res. Inst. 16 (1989), 361-383.

[42] B.H. Matzat, *Zöpfe und Galoissche Gruppen*. J. reine angew. Math. 420 (1991), 99-159.

[43] P. Müller, *A one-parameter family of polynomials with Galois group* M_{24} *over* $Q(t)$. Preprint (2012), available at `http://arxiv.org/abs/1204.1328`.

[44] P. Müller, *Finiteness results for Hilbert's irreducibility theorem.* Annales de l'Institut Fourier 52 (2002), 983-1015.

[45] P. Müller, *Permutation groups with a cyclic two-orbits subgroup and monodromy groups of Laurent polynomials.* Ann. Sc. Norm. Super. Pisa, Cl. Sci. (5) 12, No. 2 (2013), 369-438.

[46] P. Müller, *Primitive monodromy groups of polynomials.* M. Fried (editor), Recent developments in the inverse Galois problem, Contemp. Math. 186 (1995), 385-401.

[47] R. Ree, *A theorem on permutations.* J. Combinatorial Theory Ser. A 10 (1971), 174-175.

[48] M. Romagny, S. Wewers, *Hurwitz spaces.* Groupes de Galois arithmétiques et différentiels, Sémin. Congr., vol. 13, Soc. Math. France, Paris (2006), 313-341.

[49] R. Schulze, *Algebraic patching.* Unpublished manuscript (2011).

[50] J.-P. Serre, *Local Fields.* Springer Verlag, GTM 67 (1979).

[51] J. H. Silverman, J. Tate, *Rational Points on Elliptic Curves.* Springer Verlag (1992).

[52] W. A. Stein et al., *Sage Mathematics Software (Version 5.8)* . The Sage Development Team, 2013.

[53] H. Stichtenoth, *Algebraic Function Fields and Codes.* Springer Verlag, GTM 254 (2008).

[54] L.R. Turner, *Inverse of the Vandermonde matrix with applications.* NASA Technical Note (1966).

[55] H. Völklein, *Groups as Galois Groups. An Introduction.* Cambridge Studies in Advanced Mathematics 53, Cambridge Univ. Press, New York (1996).

[56] G. Wang, *Genus zero systems for primitive groups of affine type.* PhD thesis, Birmingham (2011).

[57] D. Zywina, *Inverse Galois problem for small simple groups.* Preprint (2013), available at `http://www.math.cornell.edu/~zywina/papers/smallGalois.pdf`.