E-mail address of submitting author (Strömbergsson): Astrombe@Princeton.edu

SEXTIC COVERINGS OF GENUS TWO WHICH ARE BRANCHED AT THREE POINTS

BJÖRN SELANDER
ANDREAS STRÖMBERGSSON

1. Introduction

Let $\mathcal{C}$ be the category whose objects are pairs (C, f) consisting of a smooth and proper $\overline{\mathbb{Q}}$-curve C and a finite morphism $f : C \to \mathbf{P}^1_{\overline{\mathbb{Q}}}$ which is branched only at $\{0, 1, \infty\}$. Since such a morphism f, which is called a Belyi map, is necessarily flat it is appropriate to refer to the objects of $\mathcal{C}$ as coverings. The morphisms in $\mathcal{C}$ are the $\mathbf{P}^1$-morphisms of the curves.

The category $\mathcal{C}$ has attracted considerable attention, particularly over the last 10–15 years. Cf., e.g., [27], [21]. The hope is that by studying the arithmetic of $\mathcal{C}$, one might find new connections between arithmetic geometry, algebraic number theory, pro-finite group theory and combinatorial topology. An important piece of motivation comes from the well-known result of Belyi [5], according to which the existence of a Belyi map is a necessary condition for a curve to be defined over the algebraic numbers.

There is an obvious action of $\mathrm{Gal}(\mathbb{Q})$ on $\mathcal{C}$, and a fundamental problem about the arithmetic of $\mathcal{C}$ is to find a complete set of invariants for the orbits of this action. Some well-known $\mathrm{Gal}(\mathbb{Q})$-invariants are the monodromy group, the ramification indices for the pre-image of each branch point, and the stabiliser group in $\mathcal{S}_{\{0,1,\infty\}}$. (We write $\mathcal{S}_{\{0,1,\infty\}} = \{\mathrm{Id}, (01), (01\infty), ...\}$ for the group of six automorphisms of $\mathbf{P}^1$ which permute the points $0, 1, \infty$, and define the action of $\mathcal{S}_{\{0,1,\infty\}}$ on $\mathcal{C}$ by composition in the target.)

While extensive computations of objects of $\mathcal{C}$ have been performed for the case of coverings of genus zero, attempts to find general computational techniques for coverings of higher genus are much more scarce. Most notable among the attempts in higher genus are the results of Richards [26] and Streit [31]. The technique in [26] builds on numerical computation of modular forms, using and extending the technique of Atkin and Swinnerton-Dyer from [3]. The technique in [31] computes Galois coverings, by means of finding the representation of the Galois group on the space of holomorphic differentials of the covering.

In the present paper we introduce a technique for computing hyperelliptic objects of $\mathcal{C}$. Our approach is quite close to that of Richards in [26]. We use the same basic idea of finding numerical approximations of modular forms in order to *guess* exact forms of the coverings. However, unlike [26], we retain the classical technique of viewing the coverings as solutions to a fixed set of polynomial equations. The advantage of this is that it makes us much less dependent on the accuracy to which the modular forms is obtained, since we may use the Newton algorithm to quickly compute arbitrarily close approximations of the coverings once we have obtained good initial values. Consequently, examples defined over more complicated number fields may be efficiently computed.

We illustrate our technique by means of examples of sextic coverings of genus two. These examples are computationally more complex than the ones considered

2000 *Mathematics Subject Classification.* Primary 14H30; Secondary 11F11, 14G20.

in [31] and [26]. The results are presented in Sections 6 and 7, cf. also Section 2. Our explicit computations make it possible to check the sizes of some orbits in $\mathcal{C}$ under the action of $\mathrm{Gal}(\mathbb{Q})$, and we find that the invariants already mentioned suffice to separate these orbits. We also find that the moduli fields of our examples are special in the sense that the Galois groups of their normal closures are imprimitive. This fact may also be combinatorially explained, in terms of the action of $\mathcal{S}_{\{0,1,\infty\}}$ (cf. Section 6). In the last section, we use one of our computed examples to deduce the existence of a tame Galois covering defined over a quadratic extension of $\mathbb{F}_5$ (the field with five elements), with the symmetric group $\mathcal{S}_6$ as Galois group.

On a more detailed level our technique encompasses two innovations. The first of these is a new way to set up equations for hyperelliptic objects (C, f) of $\mathcal{C}$, which we present in Section 3. The basic idea is to investigate the properties of the quotient of the morphism

$$(f, f \circ \iota) : C \to \mathbf{P}^1 \times \mathbf{P}^1$$

by the action of the group of order two, ι denoting the hyperelliptic involution. The main computational advantage of the equations which we obtain is that the number of unknowns which have to be guessed from numerical approximations is quite small (just three unknowns for each covering in the examples we consider).

The second innovation is a new method for numerical computation of modular forms which we present in Section 4. This technique generalises a recent algorithm by Hejhal [18] to the case of general cofinite Fuchsian groups with $\kappa \geqq 1$ cusps. As in Atkin and Swinnerton-Dyer [3] and Richards [26], the method is based on forming a finite system of linear equations for the Fourier coefficients of the modular forms; however, by building on Hejhal's ideas from [18] we obtain a system which is well-conditioned: In Richards [26] it was often necessary to use internal precision of several hundreds of digits, still yielding numerical output correct only to 15 digits or less, and this eventually led to both time and memory requirements becoming unreasonably large (cf. [26, pp. 37, 49(bottom), 51, 145, 169(B.3)]). In contrast, with our algorithm we have consistently obtained the first several Fourier coefficients of each modular form to a precision of $10 \sim 12$ digits, using an internal precision of 16 digits. (In recent work, we have successfully applied the algorithm to those coverings of index 7 and 8 which were left unresolved in [26]; cf. [28] for a brief preliminary report.)

Our algorithm for computation of modular forms may be expected to be useful for numerical investigation of many other problems as well, both in algebraic geometry and number theory. In the context of the present paper, we remark that our algorithm for modular forms can also be used to find a good approximation to the equations of the canonical model of any *nonhyperelliptic* curve of genus $g \geqq 3$ given in the form $G\backslash\mathcal{H}$ where $\mathcal{H}$ is the Poincaré upper half-plane and G is a cofinite, non-cocompact Fuchsian group. Furthermore, the algorithm should after simple changes also apply to the computation of Maass waveforms. This would open the way to extending the investigations in [18] on value distribution and statistics of Fourier coefficients of Maass waveforms to cases of Fuchsian groups having more than one cusp. (For some recent results on this, cf. [32].)

We remark that another method for the numerical computation of modular forms on Riemann surfaces has been given in [11] (cf. also [29]). The method which we give in the present paper is significantly different, as we focus on non-compact Riemann surfaces, and as our method determines the modular forms in terms of their Fourier expansions at the cusps.

Acknowledgements

We are grateful to B. Birch for several valuable comments on an earlier version of this paper, and for drawing our attention to the thesis [26]. We have benefited from discussions with and ideas from T. Ekedahl. We are grateful to D. A. Hejhal for providing us with a copy of the program code used for the computations in [18], and for helpful discussions on matters relating to these.

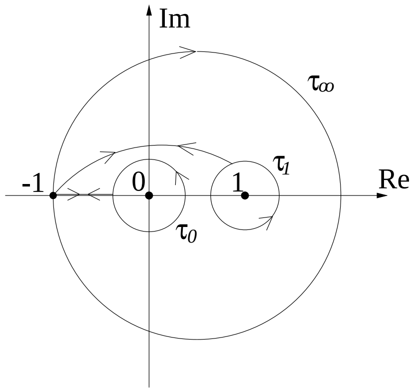
The work of the second author was partially supported by the European Commission under the Research Training Network (Mathematical Aspects of Quantum Chaos) n° HPRN-CT-2000-00103 of the IHP Programme.

2. Primitive sextic coverings of genus two

Throughout this paper, we will let $\overline{\mathbb{Q}}$ denote the subfield of algebraic numbers in the complex field $\mathbb{C}$.

The category $\mathcal{C}$ is by standard facts (see for example [30, Theorem 6.3.3] and [13, Théorème XII.5.1]) equivalent to the category of finite (unbranched) Riemann surface coverings of $\mathbf{P}^1_{\mathbb{C}} \setminus \{0,1,\infty\}$. Furthermore, this category is equivalent to the category of finite and transitive (right) $\pi_1(\mathbf{P}^1_{\mathbb{C}} \setminus \{0,1,\infty\})$-sets.

We choose -1 as base point in $\mathbf{P}^1_{\mathbb{C}} \setminus \{0,1,\infty\}$, and take $\tau_0, \tau_1, \tau_\infty$ to be the elements in $\pi_1(\mathbf{P}^1_{\mathbb{C}} \setminus \{0,1,\infty\}, -1)$ which are represented by the paths in the picture. Then $\tau_0\tau_1\tau_\infty = 1$, and $\pi_1(\mathbf{P}^1_{\mathbb{C}} \setminus \{0,1,\infty\}, -1)$ is the free group generated by τ_∞, τ_0.



We let $\mathcal{S}_n$ denote the symmetric group of order n. Now, if (C, f) is any object of $\mathcal{C}$ of degree n, and we fix a numbering $1, 2, ..., n$ of the points in the fibre $f^{-1}(-1)$, we obtain from τ_0, τ_1, τ_∞ a triple $(\sigma_0, \sigma_1, \sigma_\infty)$ of elements in $\mathcal{S}_n$ satisfying

(2.1) $\quad \sigma_\infty\sigma_1\sigma_0 = 1, \quad$ and

(2.2) $\quad \sigma_0, \sigma_1, \sigma_\infty$ generate a transitive group M (the monodromy group).

We say that two such triples $(\sigma_0, \sigma_1, \sigma_\infty)$ are equivalent if they only differ by a simultaneous conjugation by an element of $\mathcal{S}_n$. In this way we get a bijective correspondence between the isomorphism classes of objects of $\mathcal{C}$ of degree n, and equivalence classes of triples $(\sigma_0, \sigma_1, \sigma_\infty) \in \mathcal{S}_n^3$ satisfying (2.1), (2.2).

The action of $\mathcal{S}_{\{0,1,\infty\}}$ on $\mathcal{C}$ then corresponds to the action on triples $(\sigma_0, \sigma_1, \sigma_\infty)$ given by:

$$(01): \quad (\sigma_0, \sigma_1, \sigma_\infty) \mapsto (\sigma_1, \sigma_0, \sigma_0\sigma_\infty\sigma_0^{-1}). \tag{2.3}$$

$$(0\infty): \quad (\sigma_0, \sigma_1, \sigma_\infty) \mapsto (\sigma_\infty, \sigma_0^{-1}\sigma_1\sigma_0, \sigma_0) \tag{2.4}$$

Our aim now is to find a combinatorial description $(\sigma_0, \sigma_1, \sigma_\infty)$ as above for each object of $\mathcal{C}$ which has degree six and genus two and is primitive (i.e., the monodromy group M is primitive). Of course, we might program a computer to do this from scratch. But we may also proceed by hand, as follows.

First note that by Hurwitz formula, two of $\sigma_0, \sigma_1, \sigma_\infty$ must be six-cycles; we fix these to be σ_0 and σ_∞ (the other cases can easily be obtained via the action of $\mathcal{S}_{\{0,1,\infty\}}$). We may then assume that $\sigma_\infty = (123456)$. Now any six-cycle σ_0 determines a unique triple $(\sigma_0, \sigma_1, \sigma_\infty)$ satisfying (2.1) and (2.2), thus giving an object of $\mathcal{C}$; this object is primitive if and only if σ_0 does not share any block system with σ_∞. The centraliser of $\sigma_\infty = (123456)$ in $\mathcal{S}_6$ is the cyclic group $\langle\sigma_\infty\rangle$. Hence two six-cycles σ_0, σ_0' determine equivalent triples if and only if σ_0' is conjugate to σ_0 by means of an element of $\langle\sigma_\infty\rangle$.

Notice that $\sigma_\infty = (123456)$ has exactly two block systems; $\{1,4\},\{2,5\},\{3,6\}$ and $\{1,3,5\},\{2,4,6\}$. There are in total 12 six-cycles $\sigma_0 \in \mathcal{S}_6$ which respect the block system $\{1,4\},\{2,5\},\{3,6\}$, and 8 six-cycles which respect the block system $\{1,3,5\},\{2,4,6\}$; the only six-cycles which respect both block systems are σ_∞ and σ_∞^{-1}.

Therefore, there are $120-(12+8-2) = 102$ six-cycles $\sigma_0 \in \mathcal{S}_6$ which do not share any block system with σ_∞. Note that for any such σ_0, the centralisers of σ_0 and σ_∞ (i.e., $\langle\sigma_0\rangle$ and $\langle\sigma_\infty\rangle$) necessarily have trivial intersection; hence these six-cycles σ_0 determine exactly $102/6 = 17$ non-isomorphic objects of $\mathcal{C}$. By examining all six-cycles σ_0 in lexicographic order, we can fairly quickly find a set of representatives:

$$\begin{aligned} S := \{&(123465),(123564),(123645),(124365),(124635),(124653),(125364),\\ &(125463),(125643),(126354),(126435),(126543),(132654),(135264),\\ &(136254),(136542),(142653)\}. \end{aligned}$$

All the corresponding objects of $\mathcal{C}$ have branching index six over the points $0,\infty \in \mathbf{P}^1$, and the branching type over $1 \in \mathbf{P}^1$ is determined by the cycle decomposition of $\sigma_1 = \sigma_\infty^{-1}\sigma_0^{-1}$. In particular, by Hurwitz formula, the covering has genus two if and only if σ_1 has exactly two cycles in its decomposition. Using this, we find that 13 of the elements in S correspond to genus two coverings. We sort these according to the branching type over the point $1 \in \mathbf{P}^1$:

$$\text{type } 5,1: \quad \{(123465),(124653),(125463),(125643),(126354),(126435),(136254),(142653)\}; \tag{2.5}$$

$$\text{type } 4,2: \quad \{(123564),(123645),(124635),(125364)\}; \tag{2.6}$$

$$\text{type } 3,3: \quad \{(135264)\}. \tag{2.7}$$

If we consider the $\mathcal{S}_{\{0,1,\infty\}}$-action on the coverings corresponding to these six-cycles, we find that the stabiliser group is $\langle(0\infty)\rangle$ for the first and the fourth six-cycle in (2.5) and for the six-cycle in (2.7). The remaining genus two coverings have trivial stabiliser in $\mathcal{S}_{\{0,1,\infty\}}$.

We next consider the monodromy groups. We recall that the only primitive proper subgroups of $\mathcal{S}_6$ are $\mathcal{A}_6$, H_1, H_2, where H_1, H_2 are isomorphic to $\mathcal{A}_5$ and $\mathcal{S}_5$ respectively, and are determined up to conjugation in $\mathcal{S}_6$ (see for example [19, Satz II.4.7)]). But no group isomorphic to $\mathcal{A}_5$ or $\mathcal{A}_6$ contains an element of order six. Hence each covering corresponding to a six-cycle in the set S has monodromy group $\mathcal{S}_6$ or H_2.

One easily verifies that there is a unique conjugate of H_2 which contains $\sigma_\infty = (123456)$; this is the group generated by σ_∞ and (say) $(26345) \in \mathcal{S}_6$. Notice that $\mathcal{S}_5$ contains 20 elements of order six, namely, all the elements conjugate to $(12)(345) \in \mathcal{S}_5$. Note also that any two such elements generate $\mathcal{S}_5$, unless they are equal or inverse to each other (if we use that the maximal subgroups of $\mathcal{S}_5$ are known, then this is immediate). Using the isomorphism $H_2 \cong \mathcal{S}_5$ it follows that there are exactly 18 six-cycles $\sigma_0 \in \mathcal{S}_6$ such that $\langle\sigma_\infty,\sigma_0\rangle = H_2$. Hence exactly $18/6 = 3$ of the six-cycles in S yield monodromy group H_2; a quick computation shows that these are $(124365),(125643),(135264)$.

In view of this, the coverings corresponding to the fourth six-cycle in (2.5) and to the six-cycle in (2.7) have monodromy group H_2; for all other cases in (2.5) and (2.6) the monodromy group is $\mathcal{S}_6$.

It is easy to see that the only primitive coverings which have non-trivial automorphisms are cyclic Galois coverings of prime degree. Hence we see (and record for later use) that all objects of $\mathcal{C}$ obtained above have trivial automorphism group.

3. A hyperelliptic model

In this section we will show how to find a convenient set of equations for an algebraic model of a given hyperelliptic object of $\mathcal{C}$. For maximal clarity we will formulate the result (Proposition 3.2) in the particular case of a sextic covering of branching type (6,5,6), but the same basic technique can be applied to treat the case of an arbitrary hyperelliptic object of $\mathcal{C}$.

In the proof of Proposition 3.2 below, we will use the following well-known result:

Proposition 3.1. *Let X be a scheme such that 2 is invertible in $\mathcal{O}_X$. Then there is a bijection between the set of isomorphism classes of (branched) double coverings of X and the set of equivalence classes of pairs $(\mathcal{L}, d)$, where $\mathcal{L}$ is an invertible sheaf on X and $d \in H^0(X, \mathcal{L}^{\otimes -2})$. Here $(\mathcal{L}_1, d_1) \sim (\mathcal{L}_2, d_2)$ if and only if there is an isomorphism $\xi : \mathcal{L}_1 \to \mathcal{L}_2$ such that $\xi^{\otimes -2}(d_1) = d_2$. Furthermore, if X is a non-singular variety and if the divisor corresponding to d is non-singular, then the double covering is a non-singular variety as well.*

We will call a section d of $\mathcal{L}^{\otimes -2}$ a *branch section* of the double covering. For a proof of the proposition see for example [25, appendix to §2]. Let us just remark that given such a pair $(\mathcal{L}, d)$, then the corresponding double covering may be given either as $\operatorname{Spec} \mathcal{O}_X \oplus \mathcal{L}$ with the algebra structure given by d in the natural fashion, or as the Cartier divisor on $\mathbf{V}(\mathcal{L})$ (the line bundle corresponding to $\mathcal{L}$) which is given by $(\gamma^* \mathcal{L}^{\otimes -2}, z^2 - \gamma^* d)$. Here γ is the affine map $\mathbf{V}(\mathcal{L}) \to X$ and z is the global section of $\gamma^* \mathcal{L}^{-1}$ which comes from the canonical homomorphism $\mathcal{L} \to \mathbf{S}(\mathcal{L})$ by the standard identifications $\operatorname{Hom}_{\mathcal{O}_X}(\mathcal{L}, \mathbf{S}(\mathcal{L})) = \operatorname{Hom}_{\mathcal{O}_{\mathbf{V}(\mathcal{L})}}(\gamma^* \mathcal{L}, \mathcal{O}_{\mathbf{V}(\mathcal{L})}) = H^0(\mathbf{V}(\mathcal{L}), \gamma^* \mathcal{L}^{-1})$.

Also recall the following terminology. Given an object (C, f) of $\mathcal{C}$, the corresponding *field of moduli* is the fixed field of the stabiliser in $\operatorname{Gal}(\mathbb{Q})$ of the isomorphism class of (C, f). A *field of definition* of (C, f) is a number field k, such that there exists a k-curve C_k and a morphism $f_k : C_k \to \mathbf{P}^1_k$ so that after fibration with $\operatorname{Spec} \overline{\mathbb{Q}}$ the pair becomes isomorphic with (C, f). Such a pair (C_k, f_k) is called a *k-model* of the object of $\mathcal{C}$. Note that tautologically the field of moduli is contained in any field of definition, and if (C, f) is without automorphisms, then a standard application of descent gives that the field of moduli is a field of definition.

Throughout this section we will for any field k let $\mathbf{P}^1_k := \operatorname{Proj} k[y_0, y_1]$ and let $\mathbf{P}^2_k := \operatorname{Proj} k[x_0, x_1, x_2]$. When convenient, we will (by abuse of notation) let $s_1 \otimes s_2$ denote the element of $\mathcal{O}_{\mathbf{P}^d}(n+m)(U)$ if $s_1 \in \mathcal{O}_{\mathbf{P}^d}(m)(U)$ and $s_2 \in \mathcal{O}_{\mathbf{P}^d}(n)(U)$. Also let Ξ_k be the image of the map of sets

$$
\begin{aligned}
&(k^\times)^2 \to \Gamma(\mathbf{P}^2, \mathcal{O}_{\mathbf{P}^2}(2)) \\
&(a, b) \mapsto a^2 x_0^2 + b^2 x_1^2 + x_2^2 - 2ab x_0 x_1 - 2a x_0 x_2 - 2b x_1 x_2,
\end{aligned}
$$

and for an object (C, f) of $\mathcal{C}$ with C hyperelliptic define the following genericity assumption:

($*$) No point in the inverse image of $\{0, 1, \infty\}$ under f is mapped to another or itself by the hyperelliptic involution.

Proposition 3.2. *Let ψ_Λ be the family of morphisms $\mathbf{P}^1 \to \mathbf{P}^2$ which is determined by the homogeneous ring homomorphisms given by*

$$
\begin{aligned}
x_0 &\mapsto y_0^6 \\
x_1 &\mapsto (y_0 - y_1)^5 (y_0 - \Lambda y_1) \\
x_2 &\mapsto y_1^6.
\end{aligned}
$$

Then for any subfield k of $\overline{\mathbb{Q}}$ there is a bijection

$$\left\{\begin{array}{l}\textit{Isomorphism classes in } \mathcal{C} \textit{ such that}\\ \textit{representatives:}\\ \quad\bullet\ \textit{Have ramification indices } (6,5,6)\\ \quad\bullet\ \textit{Satisfy the } (*) \textit{ assumption.}\\ \quad\bullet\ \textit{Have } k \textit{ as a field of definition.}\end{array}\right\} \leftrightarrow \left\{\begin{array}{l}\textit{Pairs } (\Lambda, d) \in k^\times \times \Xi_k \textit{ such that}\\ \quad (3.1)\ \psi_\Lambda^* d = d_1 \otimes d_2^{\otimes 2} \textit{ with } d_1 \in \mathcal{O}_{\mathbf{P}^1_k}(6) \textit{ without multiple zeros and } d_2 \in \mathcal{O}_{\mathbf{P}^1_k}(3).\\ \quad (3.2)\ \textit{Neither } 0, 1 \textit{ nor } \infty \textit{ maps to the support of } d \textit{ by } \psi_\Lambda.\end{array}\right\}$$

This bijection commutes with the action of $\mathrm{Gal}(\mathbb{Q})$.

Proof. We start with a k-model (C, f) of an object of $\mathcal{C}$ which fulfils the conditions, and try to construct a pair (Λ, d). All varieties in the rest of the proof will be k-varieties unless otherwise indicated. The following diagram might be useful to keep track of the notation introduced below:

$$\begin{tikzcd} C \arrow[r, "\phi"] \arrow[d, "\Psi"'] & \mathbf{P}^1 \arrow[d, "\psi_\Lambda"] \\ \mathbf{P}^1 \times \mathbf{P}^1 \arrow[r, "\tilde{\Phi}, \Phi"'] & \mathbf{P}^2 \end{tikzcd} \tag{3.3}$$

Also let ι denote the hyperelliptic involution of C.

By a descent argument we may find Weil divisors $P_1, \ldots, P_4$ of C (of degree one as zero-cycles) such that $f^*(0) = 6P_1$, $f^*(1) = 5P_2 + P_3$ and $f^*(\infty) = 6P_4$. Since $H^0(C, \Omega_C)$ has dimension two we may find global sections l_0, l_1 of Ω_C such that (Ω_C, l_0) corresponds to $P_1 + \iota^*(P_1)$, $(\Omega_C, l_0 - l_1)$ corresponds to $P_2 + \iota^*(P_2)$ and (Ω_C, l_1) corresponds to $P_4 + \iota^*(P_4)$. Let $\phi : C \to \mathbf{P}^1$ be the degree two morphism which is determined by l_0 and l_1. Also let Λ be the unique element of k such that $(\Omega_C, \phi^*(y_0 - \Lambda y_1))$ corresponds to $P_3 + \iota^* P_3$. Then the composition $\psi_\Lambda \circ \phi$ is determined by the three sections $l_0^{\otimes 6}$, $(l_0 - l_1)^{\otimes 5} \otimes (l_0 - \Lambda l_1)$ and $l_1^{\otimes 6}$ of $\Omega_C^{\otimes 6}$.

Let Ψ be the morphism $C \to \mathbf{P}^1 \times \mathbf{P}^1$ which is given by $(f, f \circ \iota)$, and consider the invertible sheaf $\mathcal{L} := p_1^* \mathcal{O}_{\mathbf{P}^1}(1) \otimes p_2^* \mathcal{O}_{\mathbf{P}^1}(1)$ on $\mathbf{P}^1 \times \mathbf{P}^1$. Let Φ be the morphism $\mathbf{P}^1 \times \mathbf{P}^1 \to \mathbf{P}^2$ which is determined by the sections $y_0 \otimes y_0$, $(y_0 - y_1) \otimes (y_0 - y_1)$ and $y_1 \otimes y_1$ of $\mathcal{L}$. Then the composition $\Phi \circ \Psi$ is determined by the sections $f^*(y_0) \otimes (f \circ \iota)^*(y_0)$, $f^*(y_0 - y_1) \otimes (f \circ \iota)^*(y_0 - y_1)$ and $f^*(y_1) \otimes (f \circ \iota)^*(y_1)$ of $\Psi^* \mathcal{L}$.

Since the three-tuple of global sections of $\Psi^* \mathcal{L}$ describes the same three-tuple of Cartier divisors as the three-tuple of sections of $\Omega_C^{\otimes 6}$ above, there exists a unique isomorphism $\nu : \Psi^* \mathcal{L} \to \Omega_C^{\otimes 6}$ and constants $a, b \in k^\times$ such that ν maps

$$\begin{gathered} f^*(y_0) \otimes (f \circ \iota)^*(y_0)/a \mapsto l_0^{\otimes 6} \\ f^*(y_0 - y_1) \otimes (f \circ \iota)^*(y_0 - y_1)/b \mapsto (l_0 - l_1)^{\otimes 5} \otimes (l_0 - \Lambda l_1) \\ f^*(y_1) \otimes (f \circ \iota)^*(y_1) \mapsto l_1^{\otimes 6}. \end{gathered}$$

This means that if we let $\tilde{\Phi}$ be the modification of Φ given by

$$\begin{aligned} x_0 &\mapsto y_0 \otimes y_0/a \\ x_1 &\mapsto (y_0 - y_1) \otimes (y_0 - y_1)/b \\ x_2 &\mapsto y_1 \otimes y_1, \end{aligned} \tag{3.4}$$

then $\tilde{\Phi}$ makes diagram (3.3) commutative.

Note that Φ is a double covering. An easy computation shows that the section

$$x_0^2 + x_1^2 + x_2^2 - 2x_0 x_1 - 2x_0 x_2 - 2x_1 x_2$$

of $\mathcal{O}_{\mathbf{P}^2}(2)$ is a branch section of Φ. Hence an element $d \in \Xi_k$ (with the same a, b as above) is a branch section of $\tilde{\Phi}$. Let $d_1 \in H^0(\mathbf{P}^1, \mathcal{O}_{\mathbf{P}^1}(6))$ be a branch section of ϕ.

Then since ψ_Λ is affine, we get from Ψ an $\mathcal{O}_{\mathbf{P}^1}$-algebra homomorphism

$$\mathcal{A}(\Psi) : {\psi_\Lambda}^*(\mathcal{O}_{\mathbf{P}^2} \oplus \mathcal{O}_{\mathbf{P}^2}(-1)) = \mathcal{O}_{\mathbf{P}^1} \oplus \mathcal{O}_{\mathbf{P}^1}(-6) \to \mathcal{O}_{\mathbf{P}^1} \oplus \mathcal{O}_{\mathbf{P}^1}(-3).$$

Let us use standard multiplicative notation for products in these algebras. Clearly, the restriction of $\mathcal{A}(\Psi)$ to $\mathcal{O}_{\mathbf{P}^1}(-6)$ is given by a section e of $\mathcal{O}_{\mathbf{P}^1}(6)$ and a section d_2 of $\mathcal{O}_{\mathbf{P}^1}(3)$. Now let U be an open subset of $\mathbf{P}^1$ such that $\mathcal{O}_{\mathbf{P}^1}(-6)$ trivialises, and let v be a $\mathcal{O}_{\mathbf{P}^1}(U)$-generator of $\Gamma(U, \mathcal{O}_{\mathbf{P}^1}(-6))$. Evaluating $\mathcal{A}(\Psi)(0, v)^2$ in two ways, we obtain the following identity in $\Gamma(U, \mathcal{O}_{\mathbf{P}^1} \oplus \mathcal{O}_{\mathbf{P}^1}(-3))$:

$$(v^{\otimes 2} \otimes (e^{\otimes 2} + d_1 \otimes d_2^{\otimes 2}), 2(v^{\otimes 2} \otimes e \otimes d_2)) = (v^{\otimes 2} \otimes \psi_\Lambda^*(d), 0). \tag{3.5}$$

In particular, since char $k = 0 \neq 2$, either d_2 or e is equal to 0. But if $d_2 = 0$, then Ψ would factor through ϕ, and this would make the object of $\mathcal{C}$ obtained from (C, f) an imprimitive covering. Since no imprimitive subgroup of $\mathcal{S}_6$ contains an element of order five, this would contradict our assumptions. Hence $e = 0$, and from (3.5) we now obtain $\psi_\Lambda^*(d) = d_1 \otimes d_2^{\otimes 2}$, i.e. (3.1) holds. That the condition (3.2) is fulfilled is an easy consequence of the $(*)$-assumption.

We also wish to make certain that the pair (Λ, d) is independent of our choice of model (C, f). Hence let (C', f') be another model over a number field such that we have a $\mathcal{C}$-isomorphism $\pi : C_{\overline{\mathbb{Q}}} \to C'_{\overline{\mathbb{Q}}}$. Here the subscript $\overline{\mathbb{Q}}$ denotes tensorisation with $\overline{\mathbb{Q}}$. Let ϕ' and $\tilde{\Phi}'$ be the analogues of ϕ and $\tilde{\Phi}$ for (C', f'). Clearly, $\phi'_{\overline{\mathbb{Q}}} \circ \pi$ is a hyperelliptic quotient and hence differs from $\phi_{\overline{\mathbb{Q}}}$ by a linear fractional transformation. But P_1, P_2, P_4 get mapped to the same points by $\phi_{\overline{\mathbb{Q}}}$ and $\phi'_{\overline{\mathbb{Q}}} \circ \pi$; hence $\phi_{\overline{\mathbb{Q}}} = \phi'_{\overline{\mathbb{Q}}} \circ \pi$. This means that (C, f) and (C', f') give the same Λ. To see that they also give the same d it suffices to note that both $\tilde{\Phi}'$ and $\tilde{\Phi}''$ make the base extended version of diagram (3.3) (with $C_{\overline{\mathbb{Q}}}$ and $\phi_{\overline{\mathbb{Q}}}$) commutative.

Now consider the other direction. That is, we consider a pair $(\Lambda, d) \in k^\times \times \Xi_k$ such that $\psi_\Lambda^* d = d_1 \otimes d_2^{\otimes 2}$ for some global sections $d_1 \in \mathcal{O}_{\mathbf{P}^1_k}(6)$ and $d_2 \in \mathcal{O}_{\mathbf{P}^1_k}(3)$. Let C be the Spec of the $\mathcal{O}_{\mathbf{P}^1}$-algebra $\mathcal{O}_{\mathbf{P}^1} \oplus \mathcal{O}_{\mathbf{P}^1}(-3)$ (the algebra structure is given by d_1). Note that C is regular by the assumption on d_1. Then there is an $\mathcal{O}_{\mathbf{P}^1}$-algebra homomorphism

$$\begin{gathered} \mathcal{O}_{\mathbf{P}^1} \oplus \mathcal{O}_{\mathbf{P}^1}(-6) \to \mathcal{O}_{\mathbf{P}^1} \oplus \mathcal{O}_{\mathbf{P}^1}(-3) \\ (a, b) \mapsto (a, b \otimes d_2), \end{gathered}$$

where the algebra structure on the first algebra is determined by $\psi^*(d)$. This means that we get a commutative diagram

$$\begin{tikzcd} C \arrow[r] \arrow[d, "\Psi"'] & \mathbf{P}^1 \arrow[d, "\psi_\Lambda"] \\ \operatorname{Spec} \mathcal{O}_{\mathbf{P}^2} \oplus \mathcal{O}_{\mathbf{P}^2}(-1) \arrow[r] & \mathbf{P}^2. \end{tikzcd}$$

As we have already found out, there is a commutative diagram

$$\begin{tikzcd} \operatorname{Spec} \mathcal{O}_{\mathbf{P}^2} \oplus \mathcal{O}_{\mathbf{P}^2}(-1) \arrow[rr, "\Omega"] \arrow[dr] & & \mathbf{P}^1 \times \mathbf{P}^1 \arrow[dl, "\tilde{\Phi}"] \\ & \mathbf{P}^2 & \end{tikzcd}$$

where Ω is an isomorphism of coverings (and hence unique up to composition by permutation of the factors), and $\tilde{\Phi}$ is still defined by (3.4). Our claim now is that after tensorisation with $\overline{\mathbb{Q}}$ the pair $(C, \mathrm{pr}_1 \circ \Omega \circ \Psi)$ is an object of $\mathcal{C}$ with the right ramification behaviour. When we check this below we work with the tensorisation, but use the same notation as for the k-objects.

Since $\mathrm{pr}_1 \circ \Omega \circ \Psi$ is a dominant morphism of proper curves it is finite and flat, and we wish to verify that it has the right ramification behaviour. Note that by condition (3.2) it follows that the inverse image of $\psi_\Lambda(0)$ under $\tilde{\Phi}$ consists of two points, say Q_1 and Q_2. Furthermore, since $\psi_\Lambda(0)$ lies in the support of the divisor x_0, in a Zariski neighbourhood of (say) Q_1 we have that $\mathrm{pr}_1^*(y_0) = \tilde{\Phi}^*(x_0)$ as divisors. From the explicit form of ψ_Λ we then get the right ramification behaviour of $\mathrm{pr}_1 \circ \Omega \circ \Psi$ above zero (furthermore this shows that the degree of $\mathrm{pr}_1 \circ \Omega \circ \Psi$ is six). The remaining ramification may be checked in the same manner.

It certainly remains to check that our construction (it suffices to check one direction) is compatible with the Galois action. We leave that to the reader. □

Now let (Λ, d) be a pair as in Proposition 3.2. We write

$$d = a^2x_0^2 + b^2x_1^2 + x_2^2 - 2abx_0x_1 - 2ax_0x_2 - 2bx_1x_2, \qquad a, b \in k^\times$$

as before, and impose the restriction that d_2 (in $\psi_\Lambda^* d = d_1 \otimes d_2^{\otimes 2}$) should have no multiple zeros. Notice that

$$\psi_\Lambda^* d = \left(ay_0^6 - b(y_0 - y_1)^5(y_0 - \Lambda y_1) + y_1^6\right)^2 - 4ay_0^6y_1^6.$$

From (3.2) in Proposition 3.2 it follows that $\psi_\Lambda^* d$ contains no factor y_1. Since d_2 has no multiple zeros, we get that the polynomial

$$P(y) = \left(ay^6 - b(y-1)^5(y - \Lambda) + 1\right)^2 - 4ay^6 \tag{3.6}$$

has three distinct double roots $y^{(j)} \in \overline{\mathbb{Q}}$, $j = 1, 2, 3$. Hence:

$$P(y^{(1)}) = P'(y^{(1)}) = P(y^{(2)}) = P'(y^{(2)}) = P(y^{(3)}) = P'(y^{(3)}) = 0. \tag{3.7}$$

This gives us a system of six polynomial equations for the six indeterminates $\Lambda, a, b, y^{(1)}, y^{(2)}, y^{(3)}$. (It is also possible to reduce to only three indeterminates Λ, a, b, at the price of having to deal with *much* more complicated equations. Cf., e.g., [10, Thm. 8.4.3].)

The modifications needed to cover the cases where d_2 has multiple zeros are of course trivial, and lead to systems with fewer indeterminates.

4. Numerical computation of modular forms

Starting with an analytic description of an object (C, f) in $\mathcal{C}$ as a covering $G\backslash\mathcal{H} \to \Gamma(2)\backslash\mathcal{H} \cong \mathbf{P}^1$, where G is a finite index subgroup of $\Gamma(2)$, we will be able to recover an algebraic description of (C, f) (over $\mathbb{C}$) by finding an explicit basis for the space of holomorphic cusp forms of weight 2 with respect to G.

In this section, we will discuss a general algorithm for the computation of cusp forms on an arbitrary cofinite Fuchsian group Γ having at least one cusp.

A few years ago, in [18], Hejhal presented a new, robust algorithm for the computation of both holomorphic cusp forms and Maass waveforms on certain cofinite Fuchsian groups. (For the case of modular forms, see also [33].) This elegant algorithm represents a major step forward compared to earlier existing methods, regarding both numerical stability and range of applicability.

The essential restriction on Γ in [18] is that $\Gamma\backslash\mathcal{H}$ should have exactly one cusp. We will show how to generalise the algorithm in [18] to the case where Γ has $\kappa \geqq 1$ cusps. We will follow the discussion in [18, §4] as closely as possible; the main new difficulty is one of bookkeeping, as we have to make simultaneous use of all the κ distinct Fourier expansions of our searched-for modular form when building the appropriate system of equations.

In view of the application which we have in mind, we will restrict our presentation to the case of holomorphic cusp forms.

Let Γ be a cofinite Fuchsian group having $\kappa \geqq 1$ inequivalent cusps. We let $\mathbf{F} \subset \mathcal{H}$ be a nice fundamental domain for $\Gamma \backslash \mathcal{H}$. Here "nice" means that the boundary of $\mathbf{F}$ should be a finite union of geodesic arcs, but we do *not* assume that $\mathbf{F}$ is canonical in the sense of [17, p. 5]. In particular, $\mathbf{F}$ may have vertices at infinity which are equivalent under Γ. The reason to accept such non-canonical fundamental domains is that they often appear as the most natural choices for many cases of arithmetic groups Γ.

We let $\eta_1, ..., \eta_\kappa \in \mathbb{R} \cup \{\infty\}$ be representatives for the inequivalent cusp classes of Γ. For each $j \in \{1, ..., \kappa\}$ we take $N_j \in \mathrm{PSL}(2, \mathbb{R})$ to be a cusp normalising map such that

(A) $N_j(\eta_j) = \infty$;

(B) The stabiliser Γ_{η_j} is generated by $N_j^{-1} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} N_j$.

Also, for each vertex at infinity P of $\mathbf{F}$ we fix a map $U_P \in \Gamma$ such that $U_P(P) \in \{\eta_1, ..., \eta_\kappa\}$.

For each point $w \in \mathbf{F}$ we fix, once and for all, a choice of an index $\mathfrak{J}(w) \in \{1, ..., \kappa\}$ and a map $U_w \in \Gamma$, subject to the conditions that the total set of maps $\{U_w \mid w \in \mathbf{F}\}$ is finite, and that for all $w \in \mathbf{F}$ lying sufficiently close to a vertex at infinity P of $\mathbf{F}$ with $U_P(P) = \eta_j$, we have $\mathfrak{J}(w) = j$ and $U_w = U_P$. (In practice, we choose the $\mathfrak{J}(w)$'s and U_w's by partitioning $\mathbf{F}$ into a finite number of subregions in a sensible way, and attaching a single choice of $\mathfrak{J}$ and U to each subregion.) Then, by a simple compactness argument, the quantity

$$Y_0 = \inf_{w \in \mathbf{F}} \mathrm{Im}\, N_{\mathfrak{J}(w)} U_w(w) \tag{4.4}$$

is *positive.* (And in practice, with a judicious choice of the $\mathfrak{J}(w)$'s and U_w's: Y_0 will not be too small.)

Let k be an even positive integer. We wish to construct an explicit linear basis for the space $\mathcal{C}_k(\Gamma)$ of holomorphic cusp forms on Γ of weight k.

Let us consider any fixed element $F \not\equiv 0$ of $\mathcal{C}_k(\Gamma)$. For numerical reasons, it is preferable to have automorphy factors of modulus one. To this end, we set $f(z) = y^{k/2} F(z)$ (where $z = x + iy$, as usual). The automorphy relation for f then reads $\left[f_{|k} T\right] = f$ for all $T \in \Gamma$, where we have defined

$$\left[f_{|k} T\right](z) = \frac{|cz + d|^k}{(cz + d)^k} f(Tz), \qquad \text{for } T = \begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \mathrm{PSL}(2, \mathbb{R}). \tag{4.5}$$

Notice that (4.5) defines a right action of the group $\mathrm{PSL}(2, \mathbb{R})$ on the set of functions $g : \mathcal{H} \to \mathbb{C}$, i.e. we have

$$\left[g_{|k} T_1 T_2\right] = \left[\left[g_{|k} T_1\right]_{|k} T_2\right] \qquad \text{for all } T_1, T_2 \in \mathrm{PSL}(2, \mathbb{R}).$$

For $j \in \{1, ..., \kappa\}$, the Fourier expansion of $f(z)$ with respect to the cusp η_j reads

$$\left[f_{|k} N_j^{-1}\right](z) = y^{k/2} \sum_{n=1}^{\infty} a_n^{(j)} e^{2\pi i n z}.$$

Here, it is easy to prove that the Fourier coefficients satisfy the bound

$$a_n^{(j)} = O\left(n^{k/2}\right),$$

cf., e.g., [22, Cor. 2.1.6]. (This estimate is not the best possible. In fact, for arbitrary Γ and $k \geqq 4$, one knows that $a_n^{(j)} = O\left(n^{k/2 - 1/6}\right)$. Cf. [12].) We make the assumption that these estimates carry modest implied constants for each j, and we can then select a sensible (monotonic decreasing) function $M(y)$ so that

$$\left[f_{|k} N_j^{-1}\right](z) = y^{k/2} \sum_{n=1}^{M(y)} a_n^{(j)} e^{2\pi i n z} + [[10^{-16}]] \tag{4.6}$$

for each $z = x + iy \in \mathcal{H}$ and each $j \in \{1, ..., \kappa\}$. Here $[[10^{-16}]]$ is shorthand for a quantity of absolute value less that 10^{-16}.

Now fix a positive constant Y so that $Y < Y_0$ (cf. (4.4)), and an integer Q satisfying $M(Y) < Q$. We write, as a matter of notation, $a_n^{(j)} = 0$ for $n \leqq 0$. We introduce the following $2Q$ points, evenly spaced along a horocycle:

$$z_m = x_m + iY = \frac{1}{2Q}\left(m - \frac{1}{2}\right) + iY \in \mathcal{H}, \qquad 1 - Q \leqq m \leqq Q. \tag{4.7}$$

By taking appropriate linear combinations of relation (4.6) over all these points, we obtain, for each $|n| \leqq M(Y)$:

$$a_n^{(j)} Y^{k/2} e^{-2\pi n Y} = \frac{1}{2Q} \sum_{m=1-Q}^{Q} \left[f_{|k} N_j^{-1}\right](z_m) \cdot e^{-2\pi i n x_m} + [[10^{-16}]]. \tag{4.8}$$

We will now utilise the fact that f is Γ-automorphic. For each j and m, we compute the **F**-pullback of $N_j^{-1}(z_m)$, that is, we find[1] a map $T_{mj} \in \Gamma$ such that $w = T_{mj} N_j^{-1}(z_m) \in \mathbf{F}$. Recall that we have made choices of $\mathfrak{J}(w) \in \{1, ..., \kappa\}$ and a map $U_w \in \Gamma$ (cf. (4.4) and above). We write

$$\begin{aligned} z_{mj}^* = x_{mj}^* + y_{mj}^* &= N_{\mathfrak{J}(w)} U_w(w) = N_{\mathfrak{J}(w)} U_w T_{mj} N_j^{-1}(z_m); \\ \begin{pmatrix} * & * \\ c_{mj} & d_{mj} \end{pmatrix} &= N_{\mathfrak{J}(w)} U_w T_{mj} N_j^{-1}. \end{aligned} \tag{4.9}$$

Making use of the automorphy relation $f = \left[f_{|k} U_w T_{mj}\right]$, we now have:

$$\begin{aligned} \left[f_{|k} N_j^{-1}\right](z_m) &= \left[\left[f_{|k} U_w T_{mj}\right]_{|k} N_j^{-1}\right](z_m) \\ &= \left[\left[f_{|k} N_{\mathfrak{J}(w)}^{-1}\right]_{|k} N_{\mathfrak{J}(w)} U_w T_{mj} N_j^{-1}\right](z_m). \\ &= \frac{|c_{mj} z_m + d_{mj}|^k}{(c_{mj} z_m + d_{mj})^k} \cdot \left[f_{|k} N_{\mathfrak{J}(w)}^{-1}\right]\left(z_{mj}^*\right). \\ &= \frac{|c_{mj} z_m + d_{mj}|^k}{(c_{mj} z_m + d_{mj})^k} \cdot \left(\left(y_{mj}^*\right)^{k/2} \sum_{l=1}^{M(Y_0)} a_l^{(\mathfrak{J}(w))} e^{2\pi i l z_{mj}^*} + [[10^{-16}]] \right). \end{aligned}$$

(In the last equality we used the fact $\operatorname{Im} z_{mj}^* \geqq Y_0$, cf. (4.4) and (4.9).) We write $M_0 = M(Y_0)$. Substituting our last relation into (4.8), we obtain:

$$a_n^{(j)} Y^{k/2} e^{-2\pi n Y} = \sum_{j'=1}^{\kappa} \sum_{l=1}^{M_0} a_l^{(j')} V_{nl}^{(jj')} + 2[[10^{-16}]] \tag{4.10}$$

with

$$V_{nl}^{(jj')} = \frac{1}{2Q} \sum_{m=1-Q}^{Q}{}^{*} \frac{|c_{mj} z_m + d_{mj}|^k}{(c_{mj} z_m + d_{mj})^k} \left(y_{mj}^*\right)^{k/2} e^{2\pi i l z_{mj}^*} e^{-2\pi i n x_m}, \tag{4.11}$$

where the asterisk denotes that the summation is restricted to those values of m for which $\mathfrak{J}(w) = \mathfrak{J}(T_{mj} N_j^{-1}(z_m))$ equals j'. Relation (4.10) holds for all $|n| \leqq M(Y)$ and all $j \in \{1, ..., \kappa\}$, and for any given holomorphic cusp form $F \in \mathcal{C}_k(\Gamma)$. It is

[1] We will show in the next section how to do this in practice in the special case that we are interested in. For a general group Γ, once the fundamental polygon **F** and the corresponding side-by-side identification maps for $\partial\mathbf{F}$ are known, an algorithm for finding the **F**-pullback of an arbitrary point can in theory be constructed by working explicitly through [20, Ch. VII, 1C-1E, especially 1E].

easy to see that each c_{mj} in (4.9) is nonzero[2], and hence the relations (4.10) are far from any tautology. The system (4.10), (4.11) is the analogue of [18, (16),(17)]. In contrast to the situation in [18], our constants $V_{nl}^{(jj')}$ will in general not be real.

In practice, we restrict (4.10) to $1 \leqq n \leqq M_0$, thus obtaining a system of linear equations for the κM_0 unknowns $a_n^{(j)}$. Notice that the dimension D of $\mathcal{C}_k(\Gamma)$ is known from Riemann-Roch; see [17, pp. 485, 494ff] or [22, Thm. 2.5.2]. One now expects that it should be possible to solve (4.10) with some well-conditioned matrix operations, so as to obtain D linearly independent lists of coefficients $\{a_n^{(j)} \mid 1 \leqq n \leqq M_0,\ 1 \leqq j \leqq \kappa\}$, corresponding to a basis $F_1, ..., F_D$ of $\mathcal{C}_k(\Gamma)$.

Assuming that we *do* obtain such lists of coefficients to reasonable accuracy, then, just as in [18, p. 299], the higher coefficients for each basis element F_h can be derived from

$$a_n^{(j)} = \frac{\sum_{j'=1}^{\kappa} \sum_{l=1}^{M_0} a_l^{(j')} V_{nl}^{(jj')}}{Y^{k/2} e^{-2\pi n Y}}$$

by an incremental process wherein Y is successively reduced in a judicious way as n grows.

The remarks in [18, pp. 299–300] regarding accuracy carry over to the present situation. Note that, as in [18], it is not evident *a priori* that the linear system will be well-conditioned as hoped, but it is possible to get a reassuring test on the overall accuracy by running the whole process again *using a different* Y*-value.*

So far, the algorithm has been found to work quite well. We have applied the algorithm not only to the cases needed for the computations presented in this paper, but also to certain other subgroups of $\Gamma(2)$, and other weights than 2. Using an internal precision of 16 digits, the $a_n^{(j)}$'s were consistently obtained to an accuracy of $10 \sim 12$ places for $n \leqq 100$, and to at least 9 places all the way up to $n = 1000$.

We remark that a very similar discussion applies to the case of Maass waveforms; a comparison with [18] will make it clear exactly which modifications are necessary. We certainly expect that the resulting algorithm should work as satisfactorily as in the holomorphic case.

5. Application of modular forms to the explicit computation of a covering

The congruence group $\Gamma(2)$ is defined as the kernel of the natural homomorphism $\mathrm{PSL}(2,\mathbb{Z}) \to \mathrm{PSL}(2,\mathbb{Z}/2\mathbb{Z})$. The Riemann surface $\Gamma(2)\backslash\mathcal{H}$ has genus zero and three punctures, and is thus isomorphic to $\mathbf{P}^1 \setminus \{0,1,\infty\}$. We identify $\Gamma(2)\backslash\mathcal{H}$ and $\mathbf{P}^1 \setminus \{0,1,\infty\}$ in such a way that $0,1,\infty \in \overline{\mathcal{H}}$ correspond to $0,1,\infty \in \mathbf{P}^1$, in this order. The identification map is then given by

$$\Gamma(2)\backslash\mathcal{H} \ni z \mapsto 1 - 1/\lambda(z) \in \mathbf{P}^1. \tag{5.1}$$

Cf. [1, §§3.4, 3.5] and [7, Ch. VII, §7] concerning the standard modular function $\lambda(z)$.

Since $\Gamma(2)$ contains no elliptic elements, the projection $\mathcal{H} \to \Gamma(2)\backslash\mathcal{H} = \mathbf{P}^1 \setminus \{0,1,\infty\}$ is in fact a universal covering, and the choice of the point $i \in \mathcal{H}$ in the fibre of -1 (we have $1 - 1/\lambda(i) = -1$, for [1, p. 271 (25)] implies $\lambda(i) = 1/2$) gives an isomorphism $\Gamma(2) \cong \pi_1 = \pi_1(\mathbf{P}^1 \setminus \{0,1,\infty\}, -1)$.

---

[2]For if $c_{mj} = 0$ for some m, j, then $N_{\mathfrak{J}(w)} U_w T_{mj} N_j^{-1}$ would fix ∞, hence $\eta_{\mathfrak{J}(w)}$ and η_j would be equivalent under Γ, i.e. $\mathfrak{J}(w) = j$. Also, $U_w T_{mj} \in \Gamma_{\eta_j} = N_j^{-1} \begin{pmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{pmatrix} N_j$, and we would then get $\mathrm{Im}\ z_{mj}^* = \mathrm{Im}\ N_{\mathfrak{J}(w)} U_w T_{mj} N_j^{-1}(z_m) = \mathrm{Im}\ z_m = Y$. This is a contradiction to the fact that $\mathrm{Im}\ z_{mj}^* \geqq Y_0 > Y$. This proves our claim.

Using our definitions of $\tau_0, \tau_1, \tau_\infty$ in Section 2 and the mapping properties of $\lambda(z)$, as analysed in [1, pp. 272–273], one easily checks that this isomorphism takes

$$\tau_0 \mapsto T_0, \qquad \tau_\infty \mapsto T_\infty, \qquad \text{where } T_0 = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}, \quad T_\infty = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix};$$
$$\tau_1 \mapsto (T_\infty T_0)^{-1} = \begin{pmatrix} 1 & -2 \\ 2 & -3 \end{pmatrix}.$$

Notice that T_0, $(T_\infty T_0)^{-1}$ and T_∞ are generators for the parabolic subgroups of $\Gamma(2)$ fixing the cusps 0, 1 and ∞ respectively.

To illustrate our method of computation, we will from now on consider the particular object of our category $\mathcal{C}$ which corresponds to case number seven in (2.5). That is, we consider the (right) action of $\Gamma(2) \cong \pi_1$ on the set $\{1, 2, ..., 6\}$ which is given by $T_\infty \mapsto (123456)$ and $T_0 \mapsto (136254)$. We know that the fibre functor from the category of coverings to the category of π_1-sets has a quasi-inverse given by $S \mapsto S \times^{\pi_1} \mathcal{H}$. Hence, if we let $G = \mathrm{Stab}_{\Gamma(2)}(1) \subset \Gamma(2)$ be the stabiliser subgroup of $1 \in \{1, 2, ..., 6\}$, then our selected object in $\mathcal{C}$ has an analytic model given by the covering $G\backslash\mathcal{H} \to \Gamma(2)\backslash\mathcal{H}$ (the map which is induced by the identity map on $\mathcal{H}$).

We now want to apply the numerical calculation of cusp forms described in the preceding section. To do this, we first have to specify a fundamental domain $\mathbf{F}$ for $G\backslash\mathcal{H}$, and give a method for finding the G-pullback into $\mathbf{F}$ of any given point $z_0 \in \mathcal{H}$.

A natural choice of a fundamental domain is furnished by

$$\mathbf{F} = \bigcup_{k=0}^{5} T_\infty^k \mathbf{F}_0, \tag{5.2}$$

where $\mathbf{F}_0$ is the standard fundamental domain for $\Gamma(2)$;

$$\mathbf{F}_0 = \left\{ z \in \mathcal{H} \;\middle|\; -1 \leqq \mathrm{Re}\ z \leqq 1, \;\; \left|z - \tfrac{1}{2}\right| \geqq \tfrac{1}{2}, \;\; \left|z + \tfrac{1}{2}\right| \geqq \tfrac{1}{2} \right\}.$$

The choice (5.2) is possible since the action of T_∞ on $\{1, 2, ..., 6\}$ is given by a 6-cycle, for this means that $(1)T_\infty^k$ runs through all distinct elements of $\{1, 2, ..., 6\}$ as $k = 0, 1, ..., 5$, and thus, $\{GT_\infty^k\}_{k=0}^5$ gives a complete set of left cosets in $\Gamma(2)$.

We next give a pullback algorithm for $\mathbf{F}$. Let $z_0 \in \mathcal{H}$ be a given point. First, by imitating the well-known procedure for the modular group (cf., e.g., [15, §2]), we show how to obtain the $\Gamma(2)$-pullback of z_0 into $\mathbf{F}_0$. We start by $z = z_0$:

- Replace z by $T_\infty^n(z) = z + 2n$, where $n \in \mathbb{Z}$ is chosen so as to make $|\mathrm{Re}\ z| \leqq 1$.
- If $|z + 1/2| \geqq 1/2$ and $|z - 1/2| \geqq 1/2$, then $z \in \mathbf{F}_0$, and we are done.
- If $|z + 1/2| < 1/2$, replace z by $T_0^{-1}(z) = z/(2z + 1)$.
- If $|z - 1/2| < 1/2$, replace z by $T_0(z) = z/(-2z + 1)$.
- Repeat from start.

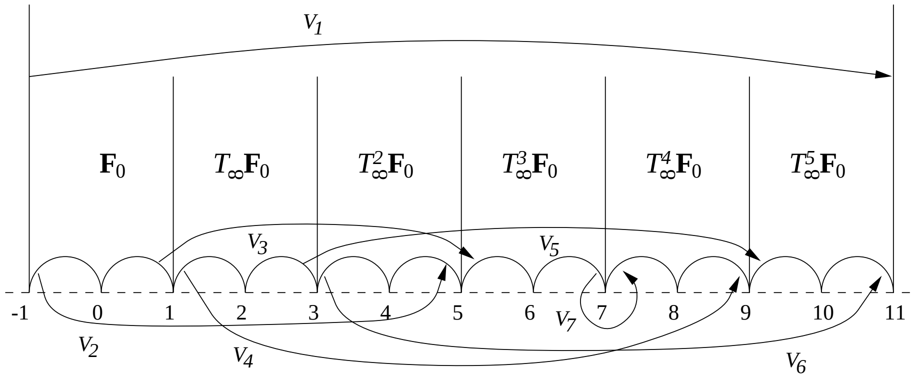
To show that we eventually end up with $z \in \mathbf{F}_0$, we notice that all points obtained in the above algorithm are of the form $T(z_0)$, for some $T = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(2)$. The height of $T(z_0)$ above the real axis is:

$$\mathrm{Im}\, T(z_0) = \frac{\mathrm{Im}\ z_0}{|cz_0 + d|^2},$$

Each time we apply the map T_0 or T_0^{-1} in the procedure, this height *increases*, for the map T_0^{-1} is nothing but an inversion in the circle $|z + 1/2| = 1/2$ followed by a reflexion in the imaginary axis, and similarly for the map T_0. It is easy to check that there are only finitely many pairs of integers c, d (with $2 \mid c$, $2 \nmid d$) such that $|cz_0 + d| < 1$ (cf. [15, §2, Lemma 1]). Hence the process cannot go on indefinitely; after a finite number of steps, we must end up with a point $T(z_0) \in \mathbf{F}_0$.

Once the $\Gamma(2)$-pullback has been calculated, it is easy to also find the *G-pullback* of z_0 *into* $\mathbf{F}$. For notice that in the above algorithm, the map $T \in \Gamma(2)$ which gives $T(z_0) \in \mathbf{F}_0$ is actually obtained as a product of T_∞'s and T_0's. Using this we can compute the action of T on $\{1,2,...,6\}$. We let $k=(1)T^{-1}\in\{1,2,...,6\}$. Then $(1)T_\infty^{k-1}T=1$, i.e. $T_\infty^{k-1}T\in G$, and $T_\infty^{k-1}T(z_0)\in\mathbf{F}$ is our searched-for pullback.

With the pullback algorithm in place, it is now easy to find all explicit "setup" data which we need for the group G; some of this data is shown in the following picture and tables. (To compute the $\partial\mathbf{F}$-identification map for a side s of $\mathbf{F}$, we simply choose one point z lying close to s, *outside* $\mathbf{F}$, and then determine its G-pullback into $\mathbf{F}$.)



Side-by-side identification maps for $\partial\mathbf{F}$:

V_1	V_2	V_3	V_4	V_5	V_6	V_7
$\begin{pmatrix}1&12\\0&1\end{pmatrix}$	$\begin{pmatrix}9&4\\2&1\end{pmatrix}$	$\begin{pmatrix}-11&6\\-2&1\end{pmatrix}$	$\begin{pmatrix}17&-26\\2&-3\end{pmatrix}$	$\begin{pmatrix}-19&48\\-2&5\end{pmatrix}$	$\begin{pmatrix}21&-74\\2&-7\end{pmatrix}$	$\begin{pmatrix}-15&98\\-2&13\end{pmatrix}$

(These maps all belong to G, and they identify the sides of $\mathbf{F}$ in pairs as indicated in the picture.)

Cusp-class of $\mathbf{F}$	$\{0,2,4,6,8,10\}$	$\{-1,1,3,5,9,11\}$	$\{7\}$	$\{\infty\}$
representative	$\eta_1=0$	$\eta_2=1$	$\eta_3=7$	$\eta_4=\infty$

(By numbering the cusp classes in this order we make $\eta_1,...,\eta_4$ correspond to the Weil divisors $P_1,...,P_4$ of C, in this order. Cf. the proof of Proposition 3.2, and our identification (5.1).)

Referring to the picture it is now easy to find, for each vertex at infinity P of $\mathbf{F}$, a map $U_P\in G$ such that $U_P(P)\in\{\eta_1,...,\eta_4\}$ (cf. Section 4):

$$U_\infty=U_0=U_1=U_7=\mathrm{Id},\quad U_{-1}=V_3^{-1}V_2,\quad U_2=V_2^{-1}V_6^{-1}V_5,\ \text{etc.}$$

Given $w\in\mathbf{F}$, a sensible choice of $\mathfrak{J}(w)$ and U_w (cf. (4.4) and above) can be made as follows. For $j=1,2,3,4$, we let P_j be the vertex in the η_j-class which lies "closest" to w. (In precise terms, we let $P_3=7$, $P_4=\infty$, and take $P_1\in\{0,2,4,6,8,10\}$ so as to minimize $|\mathrm{Re}\,w-P_1|$, and similarly for $P_2\in\{-1,1,3,5,9,11\}$.) We then choose that $j\in\{1,2,3,4\}$ for which Im $N_jU_{P_j}(w)$ takes its largest value, and set $\mathfrak{J}(w)=j$ and $U_w=U_{P_j}$.

The algorithm from Section 4 can now be applied. We used the specific settings as indicated above, and $M_0=100$, $Y=0.07$ (as well as $Y=0.06$). The output is a basis $\{F_0,F_1\}$ for the space $\mathcal{C}_2(G)$ of holomorphic cusp forms of weight 2 with respect to G. More precisely, we obtain good approximations to the Fourier coefficients $\{a_n^{(j)}\}$, $1\leqq n\leqq M_0$, of each basis element. In our case, once a first basis has been obtained, it turns out via some simple linear algebra that F_0,F_1 can be determined uniquely by the normalising conditions $\langle a_1^{(1)}, a_1^{(2)}\rangle = \langle 0,1\rangle$ for F_0, $\langle a_1^{(2)}, a_1^{(4)}\rangle = \langle 1,0\rangle$ for F_1.

We let $f : C_{\mathfrak{R}} \to \mathbf{P}^1$ denote the analytic map of compact Riemann surfaces obtained from our covering $G\backslash\mathcal{H} \to \Gamma(2)\backslash\mathcal{H} = \mathbf{P}^1 \setminus \{0,1,\infty\}$ by compactification of $G\backslash\mathcal{H}$, cf. [22, §1.7, §1.8]. In the following, we will use the letters $\tilde{\Phi}$, Ψ, ψ_Λ, ϕ, ι and l_0, l_1 to denote the *analytic* counterparts to the morphisms and sections defined in the proof of Proposition 3.2, starting from $(C_{\mathfrak{R}}, f)$. Recall that for each cusp form $F(z) \in \mathcal{C}_2(G)$ there is a corresponding holomorphic differential form $F(z)\,dz$ on $C_{\mathfrak{R}}$, cf. [22, Thm. 2.3.2]. Now, by virtue of our normalisation of F_0, F_1, and the fact that η_j corresponds to the divisor P_j for $j = 1,2,3,4$, we see that we may take $l_0 = F_0(z)\,dz$ and $l_1 = F_1(z)\,dz$. Hence the map $\phi : C_{\mathfrak{R}} \to \mathbf{P}^1$ is given by $\phi(z) = F_0(z)/F_1(z)$, for all $z \in G\backslash\mathcal{H}$.

We are now in a position to determine good floating point approximations to the algebraic numbers Λ, a, b in Proposition 3.2.

First of all, $\Lambda = \phi(P_3)$, and we obtain this number by computing the ratio between the $a_1^{(3)}$-coefficients for F_0 and F_1.

Next, recall from the proof of Proposition 3.2 that a, b are uniquely determined by the fact that we should have a commutative diagram

$$\psi_\Lambda \circ \phi = \tilde{\Phi} \circ \Psi : C_{\mathfrak{R}} \to \mathbf{P}^2, \tag{5.3}$$

where $\tilde{\Phi}$ is the morphism $\mathbf{P}^1 \times \mathbf{P}^1 \to \mathbf{P}^2$ which is defined by (3.4) ($\tilde{\Phi}$ depends on a, b). We pick an arbitrary point $z \in G\backslash\mathcal{H}$, and let P be the corresponding point on $C_{\mathfrak{R}}$. Also, let $z' \in G\backslash\mathcal{H}$ be a representative for $\iota(P)$ (we assume $\iota(P) \neq P$ and $P, \iota(P) \notin \{P_1, P_2, P_3, P_4\}$). Evaluating both sides of (5.3) at the point P, we see that (cf. (5.1))

$$\begin{aligned} &\Big(F_0(z)^6 : (F_0(z) - F_1(z))^5 (F_0(z) - \Lambda F_1(z)) : F_1(z)^6\Big) \\ &\quad = \left(\frac{1}{a}(\lambda(z)-1)(\lambda(z')-1) : \frac{1}{b} : \lambda(z)\lambda(z')\right) \in \mathbf{P}^2. \end{aligned} \tag{5.4}$$

Here $\lambda(z)$ can be evaluated using theta series: As long as $\operatorname{Im} z$ is not too small we can simply use

$$\lambda(z) = \frac{\left(2\sum_{k=0}^{\infty} \exp((k+\frac{1}{2})^2 \pi i z)\right)^4}{\left(1 + 2\sum_{k=1}^{\infty} \exp(k^2 \pi i z)\right)^4}.$$

Cf., e.g., [7, Ch. VII, (7.1)]. Eliminating $\lambda(z')$ in (5.4) we obtain a linear identity $a = c_1 b + c_2$, with known numerical values for $c_1, c_2 \in \mathbb{C}$. Repeating this with a different $z \in G\backslash\mathcal{H}$ gives a different identity, and both a and b can then be determined. (Of course, this procedure can be repeated for any number of different points $z \in G\backslash\mathcal{H}$; this gives a test on the accuracy of the values for a, b which we obtain.)

In our particular case, we obtain the following approximate values for Λ, a, b:

$$\Lambda = -5.312093199, \quad a = 8.76074563 \cdot 10^{-5}, \quad b = 8.74892022 \cdot 10^{-5}. \tag{5.5}$$

(All three values turn out to have imaginary part 0, within the limits of accuracy.)

We can now check that the polynomial $P(y)$ in (3.6) indeed has three distinct double roots (again, within the limits of accuracy). We thus obtain a first approximation of a solution $(\Lambda, a, b, y^{(1)}, y^{(2)}, y^{(3)})$ to the system (3.7). We are then in a position to apply the procedure which is outlined in e.g. [9, pp. 111–112], that is, we use ordinary multivariate Newton iteration in (3.7) to determine our solution to a very high accuracy, and then apply a lattice reduction algorithm to guess minimal polynomials for Λ, a, b over $\mathbb{Q}$. (We used the Maple commands “fsolve” and “minpoly” for these two steps.) In our case we know from the discussion in Section 2 that Λ, a and b will be algebraic numbers of degree at most six over $\mathbb{Q}$, but we can only guess the size of the coefficients of their minimal polynomials. Some trial and error may therefore be required at this point.

For the particular case at hand, an accuracy of 100 digits for Λ, a, b turned out to be more than sufficient, and the following irreducible polynomials were obtained:

for Λ: $$33875 + 217950X + 300765X^2 + 574436X^3 + 300765X^4 + 217950X^5 + 33875X^6;$$

for a: $$625 - 7131750X - 26774625X^2 - 39683924X^3 - 26774625X^4 - 7131750X^5 + 625X^6;$$

for b: $$-33875 + 387248300X - 659116640X^2 + 450431064X^3 - 125172000X^4 - 5832000X^5 + 7290000X^6.$$

Of course, it is now easy to identify the algebraic numbers given approximately by (5.5), and to verify, by means of exact computations, that we have indeed found a solution to the system (3.7).

6. Presentation of the result

Let (C, f) be the particular object of $\mathcal{C}$ which we studied in the last section, and let Λ be as obtained above. Since Λ is unique for an isomorphism class in $\mathcal{C}$ it follows that (C, f) has at least six non-isomorphic images under the Gal($\mathbb{Q}$)-action. On the other hand, we know from Section 2 that there are exactly six objects of $\mathcal{C}$ which have branching type $(6, 5, 6)$ and trivial stabiliser subgroup in $\mathcal{S}_{\{0,1,\infty\}}$. Hence all these six objects are in the same Galois orbit, and (C, f) has moduli field $\mathbb{Q}(\Lambda)$.

The topological origin of Λ gives some information on the Galois group of the splitting field K of Λ. Indeed, let H be the subgroup of $\mathcal{S}_{\{0,1,\infty\}}$ generated by (0∞). Then H acts freely on the six Gal($\mathbb{Q}$)-conjugates of (C, f). Since the Galois action commutes with the action of H, it follows that the set of roots of the minimal polynomial of Λ has a block system with three blocks under the action of $\mathrm{Gal}(K/\mathbb{Q})$. This may be confirmed by Maple's "galois" command, which in addition shows that $[K : \mathbb{Q}] = 24$.

For each block of roots $\{\Lambda_1, \Lambda_2\}$ the fixed field of $\{\sigma \in \mathrm{Gal}(\mathbb{Q}) \mid \Lambda_1^\sigma \in \{\Lambda_1, \Lambda_2\}\}$ is a cubic subfield of $\mathbb{Q}(\Lambda_1) = \mathbb{Q}(\Lambda_2)$. The cubic subfield of $\mathbb{Q}(\Lambda)$ determined in this way turns out to be $\mathbb{Q}(\sqrt[3]{10})$. Now the following proposition shows that the curve C can be defined over $\mathbb{Q}(\sqrt[3]{10})$.

Proposition 6.1. *Let (C, f) be an object of $\mathcal{C}$ with trivial automorphism group, and assume that H is a subgroup of $\mathcal{S}_{\{0,1,\infty\}}$ such that H acts freely on the H-orbit of (C, f). Let G be the subgroup of* Gal($\mathbb{Q}$) *consisting of elements which take (C, f) to an isomorphism class in the same H-orbit. Let k be the fixed field of G. Then k is a field of definition for C.*

Proof. Let l be a sufficiently large finite Galois extension of k. By abuse of notation we will let (C, f) denote what is really an l-model of (C, f).

Clearly the data given defines a group homomorphism $\mathrm{Gal}(l/k) \ni \sigma \mapsto \nu_\sigma \in H$. Then define descent data for C by means of letting $\tau_\sigma : C \to C^\sigma$ for each $\sigma \in \mathrm{Gal}(l/k)$ be the unique isomorphism such that $\sigma \circ f^\sigma \circ \tau_\sigma = \nu_\sigma \circ f$. We have to check that the cocycle condition is fulfilled. But the squares in the following diagram commute:

$$\begin{tikzcd} C \arrow[r, "\tau_{\sigma_1}"] \arrow[d, "f"'] & C^{\sigma_1} \arrow[r, "(\tau_{\sigma_2})^{\sigma_1}"] \arrow[d, "\sigma_1 \circ f^{\sigma_1}"] & C^{\sigma_2\sigma_1} \arrow[d, "\sigma_2 \circ \sigma_1 \circ f"] \\ \mathbf{P}^1 \arrow[r, "\nu_{\sigma_1}"'] & \mathbf{P}^1 \arrow[r, "\nu_{\sigma_2}"'] & \mathbf{P}^1 \end{tikzcd}$$

Hence $\tau_{\sigma_2\sigma_1} = (\tau_{\sigma_2})^{\sigma_1} \circ \tau_{\sigma_1}$. $\square$

We are now going to present an explicit model of (C, f). We are (ultimately) interested in the arithmetic of coverings, and hence find it convenient to give a model where all coefficients are algebraic integers, and the curve is defined over $\mathbb{Q}(\sqrt[3]{10})$. Hence we must perform the descent explicitly.

A computation using the mathematical software package Pari/GP shows that

$$\mathbb{Q}(\Lambda) = \mathbb{Q}(\sqrt[3]{10}, \beta), \quad \text{where } \beta = \sqrt{9 + 4\sqrt[3]{10} + 2\sqrt[3]{10}^2}.$$

(In fact, the number $9 + 4\sqrt[3]{10} + 2\sqrt[3]{10}^2$ is chosen as an integer of minimal norm in $\mathbb{Q}(\sqrt[3]{10})$ for which we have such a presentation of $\mathbb{Q}(\Lambda)$, and as such it is unique up to multiplication by squares of units. The identification of this element is made easy by the fact that $\mathbb{Q}(\sqrt[3]{10})$ has class number one.)

Since (C, f) has no non-trivial automorphisms, and moduli field $\mathbb{Q}(\Lambda)$, there is a unique (up to unique $\mathbb{Q}(\Lambda)$-isomorphism) $\mathbb{Q}(\Lambda)$-model for (C, f). We use the notation of Proposition 6.1, hence let $k = \mathbb{Q}(\sqrt[3]{10})$ and $l = \mathbb{Q}(\sqrt[3]{10}, \beta) = \mathbb{Q}(\Lambda)$, and let σ be the non-trivial element of $\mathrm{Gal}(l/k)$. From the proof of Proposition 6.1 and the construction of ϕ in Proposition 3.2 it follows that the diagram

$$\begin{array}{ccc} C_l & \xrightarrow{\tau_\sigma} & C_l^\sigma \\ {\scriptstyle\phi}\big\downarrow & & \big\downarrow{\scriptstyle\phi^\sigma} \\ \mathbf{P}^1_l & \xrightarrow[(0\infty)\circ\sigma^{-1}]{} & (\mathbf{P}^1_l)^\sigma \end{array}$$

commutes. Note that

$$\begin{pmatrix} \beta & -\beta \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} \beta^\sigma & -\beta^\sigma \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

and let η be the linear fractional transformation corresponding to the left hand side matrix. Then it follows that

$$\begin{array}{ccc} C_l & \xrightarrow{\tau_\sigma} & C_l^\sigma \\ {\scriptstyle\eta\circ\phi}\big\downarrow & & \big\downarrow{\scriptstyle\eta^\sigma\circ\phi^\sigma} \\ \mathbf{P}^1_l & \xrightarrow[\sigma^{-1}]{} & (\mathbf{P}^1_l)^\sigma \end{array}$$

also commutes. Hence the morphism $\eta \circ \phi$ descends to k, and this morphism then gives a hyperelliptic k-model of C.

Here follows a section of $\mathcal{O}_{\mathbf{P}^1}(6)$ which defines such a model:

$$\begin{aligned}
&(6832053\sqrt[3]{10}^2 + 14719212\sqrt[3]{10} + 31711581)y_1^6 \\
&\quad + (-8406000\sqrt[3]{10}^2 - 18110178\sqrt[3]{10} - 39017196)y_0y_1^5 \\
&\quad + (4328967\sqrt[3]{10}^2 + 9326478\sqrt[3]{10} + 20093286)y_0^2y_1^4 \\
&\quad + (-1196760\sqrt[3]{10}^2 - 2578344\sqrt[3]{10} - 5554872)y_0^3y_1^3 \\
&\quad + (187391\sqrt[3]{10}^2 + 403724\sqrt[3]{10} + 869789)y_0^4y_1^2 \\
&\quad + (-15856\sqrt[3]{10}^2 - 34166\sqrt[3]{10} - 73596)y_0^5y_1 \\
&\quad + (1735\sqrt[3]{10}^2/3 + 3694\sqrt[3]{10}/3 + 8032/3)y_0^6.
\end{aligned} \tag{6.1}$$

In these variables the covering map $f : C \to \mathbf{P}^1$ is given by the quotient of

$$
\begin{aligned}
&((-4251 \sqrt[3]{10}^2 - 9156 \sqrt[3]{10} - 19722)\beta - 22071 \sqrt[3]{10}^2 - 47550 \sqrt[3]{10} - 102450) y_1^3 z \\
&+ ((2303 \sqrt[3]{10}^2 + 4961 \sqrt[3]{10} + 10688)\beta + 11959 \sqrt[3]{10}^2 + 25765 \sqrt[3]{10} + 55510) y_0 y_1^2 z \\
&+ ((-415 \sqrt[3]{10}^2 - 864 \sqrt[3]{10} - 1934)\beta - 2127 \sqrt[3]{10}^2 - 4610 \sqrt[3]{10} - 9910) y_0^2 y_1 z \\
&+ ((15 \sqrt[3]{10}^2 + 75 \sqrt[3]{10} + 104)\beta + 401 \sqrt[3]{10}^2/3 + 785 \sqrt[3]{10}/3 + 1670/3) y_0^3 z \\
&+ ((41459904 \sqrt[3]{10}^2 + 178645311 \sqrt[3]{10}/2 + 192439827)\beta + 215314776 \sqrt[3]{10}^2 + 927763245 \sqrt[3]{10}/2 + 999402660) y_1^6 \\
&+ ((-47953458 \sqrt[3]{10}^2 - 103312584 \sqrt[3]{10} - 222580224)\beta - 249037902 \sqrt[3]{10}^2 - 536535900 \sqrt[3]{10} - 1155931560) y_0 y_1^5 \\
&+ ((23118120 \sqrt[3]{10}^2 + 99612945 \sqrt[3]{10}/2 + 107304795)\beta + 120059910 \sqrt[3]{10}^2 + 517322475 \sqrt[3]{10}/2 + 557268750) y_0^2 y_1^4 \\
&+ ((-5941980 \sqrt[3]{10}^2 - 12801600 \sqrt[3]{10} - 27580320)\beta - 30858660 \sqrt[3]{10}^2 - 66483000 \sqrt[3]{10} - 143233200) y_0^3 y_1^3 \\
&+ ((859380 \sqrt[3]{10}^2 + 3702945 \sqrt[3]{10}/2 + 3988905)\beta + 4463040 \sqrt[3]{10}^2 + 19230675 \sqrt[3]{10}/2 + 20715600) y_0^4 y_1^2 \\
&+ ((-66402 \sqrt[3]{10}^2 - 143304 \sqrt[3]{10} - 308496)\beta - 345198 \sqrt[3]{10}^2 - 743580 \sqrt[3]{10} - 1601880) y_0^5 y_1 \\
&+ ((6652 \sqrt[3]{10}^2/3 + 27437 \sqrt[3]{10}/6 + 29611/3)\beta + 33478 \sqrt[3]{10}^2/3 + 144575 \sqrt[3]{10}/6 + 156490/3) y_0^6
\end{aligned}
$$

with

$$((12787 \sqrt[3]{10}^2/3 + 55073 \sqrt[3]{10}/6 + 59359/3)\beta + 66311 \sqrt[3]{10}^2/3 + 285751 \sqrt[3]{10}/6 + 307802/3)(-y_0 + \beta y_1)^6,$$

where z is a square-root of the pull-back of (6.1) to C, as in the discussion following Proposition 3.1. (The covering map was obtained by using the fact that we have, in the notation of Proposition 3.2,

$$\frac{y_0 \otimes 1}{y_1 \otimes 1} = \frac{y_0 \otimes y_1}{y_1 \otimes y_1} = \frac{a\tilde{\Phi}^* x_0 + \tilde{\Phi}^* x_2 - b\tilde{\Phi}^* x_1 + t}{2\tilde{\Phi}^* x_2},$$

where t is a square-root of the $\tilde{\Phi}$-pullback of d.)

Pari/GP also tells us that the discriminant of $\mathbb{Q}(\Lambda)$ is $2^6 \times 3^4 \times 5^4$. This is of course consistent with [4, Theorem 5.5] (cf. also Propositions A.1 and A.2 below), which applied to our case implies that the field of moduli can only be ramified at the primes dividing the order of the monodromy subgroup, which is $\mathcal{S}_6$.

7. The other examples

By means of the technique described in Sections 3–6, we have found the following model for the object of $\mathcal{C}$ which is determined by the third element in (2.6). The curve is given by the section

$$
\begin{aligned}
&(22478148\sqrt{6} + 55059993) y_1^6 + (-38023236\sqrt{6} - 93137526) y_0 y_1^5 \\
&+ (23576472\sqrt{6} + 57750327) y_0^2 y_1^4 + (-9761544\sqrt{6} - 23910804) y_0^3 y_1^3 \\
&+ (1608372\sqrt{6} + 3939687) y_0^4 y_1^2 + (-3636\sqrt{6} - 8886) y_0^5 y_1 \\
&+ (-6416\sqrt{6} - 15735) y_0^6
\end{aligned}
\tag{7.1}
$$

of $\mathcal{O}_{\mathbf{P}^1}(6)$. If we let γ be a square-root of $9+4\sqrt{6}$ then the covering map is the quotient of

$$
\begin{aligned}
&((-63\sqrt{6}/2+126)\gamma-99\sqrt{6}/2+333)y_1^3z\\
&+((-231\sqrt{6}/2+252)\gamma-543\sqrt{6}/2+531)y_0y_1^2z\\
&+((1547\sqrt{6}/2-1890)\gamma+3463\sqrt{6}/2-4221)y_0^2y_1z\\
&+((-2149\sqrt{6}/2+2632)\gamma-4805\sqrt{6}/2+5885)y_0^3z\\
&+((-223641\sqrt{6}/2-273753)\gamma-969381\sqrt{6}/2-1187298)y_1^6\\
&+((144909\sqrt{6}+354294)\gamma+627669\sqrt{6}+1537704))y_0y_1^5\\
&+((-177255\sqrt{6}/2-219915)\gamma-773955\sqrt{6}/2-946890)y_0^2y_1^4\\
&+((25110\sqrt{6}+64260)\gamma+111510\sqrt{6}+272160)y_0^3y_1^3\\
&+((-15687\sqrt{6}/2+6129)\gamma-19467\sqrt{6}/2-32886)y_0^4y_1^2\\
&+((14685\sqrt{6}-36090)\gamma-5355\sqrt{6}+12600)y_0^5y_1\\
&+((-23481\sqrt{6}/2+28787)\gamma+8435\sqrt{6}/2-10206)y_0^6
\end{aligned}
\tag{7.2}
$$

with

$$((12\sqrt{6}-189)\gamma-198\sqrt{6}-207)(-y_0+\gamma y_1)^6, \tag{7.3}$$

where z is a square-root of the section (7.1). In particular, all objects coming from (2.6) belong to the same Galois orbit. The discriminant of the field of moduli is in this case $-2^6\times 3^3\times 5$.

We recall that the remaining three coverings from (2.5) and (2.7) have stabiliser subgroup $\langle(0\infty)\rangle$ for the $\mathcal{S}_{\{0,1,\infty\}}$-action. We have the following general proposition.

Proposition 7.1. *Assume that $G\subset\mathcal{S}_{\{0,1,\infty\}}$ stabilises the isomorphism class of an object (C,f) of $\mathcal{C}$. Assume furthermore that there is an action $G\times C\to C$ which makes f a G-morphism (this is immediate if (C,f) has no nontrivial automorphism). Then (C,f) can be recovered (up to isomorphism) from the induced morphism $G\backslash C\to G\backslash\mathbf{P}^1$ by means of the base extension $\mathbf{P}^1\to G\backslash\mathbf{P}^1$ followed by normalisation.*

Proof. Standard facts about quotients give that $G\backslash C$ and $G\backslash\mathbf{P}^1$ are non-singular and proper curves and that the quotient morphisms $C\to G\backslash C$ and $\mathbf{P}^1\to G\backslash\mathbf{P}^1$ must be finite. The universal property of quotients gives a morphism $G\backslash C\to G\backslash\mathbf{P}^1$ which must be finite as well.

Universal properties then give a morphism from C to the normalisation of $\mathbf{P}^1\times_{G\backslash\mathbf{P}^1} G\backslash C$. Hence some component of the normalisation must be isomorphic to $H\backslash C$ where H is a subgroup of G, and f then factors through $H\backslash C$. Since G acts faithfully on $\mathbf{P}^1$, it follows that H must be the trivial group. Hence some component of the normalisation must be isomorphic to C, and a comparison of degrees gives that this must be the only component of the normalisation. $\square$

Corollary 7.2. *Given two objects (C,f) and (C',f') of $\mathcal{C}$ with the same stabiliser subgroup G satisfying the condition in the proposition above, then these objects are in the same Galois orbit if and only if their quotients $G\backslash C\to G\backslash\mathbf{P}^1$ respectively $G\backslash C'\to G\backslash\mathbf{P}^1$ are in the same Galois orbit.*

The proposition makes it possible to find explicit forms for the remaining coverings from (2.5) and (2.7) in a simpler fashion than that used before: For $G=\langle(0\infty)\rangle$ we choose the quotient morphism $\mathbf{P}^1\to G\backslash\mathbf{P}^1\cong\mathbf{P}^1$ to be given explicitly by $y_0'\mapsto(y_0+y_1)^2$, $y_1'\mapsto 4y_0y_1$. Using the language introduced in Section 2, the three relevant coverings $G\backslash C\to G\backslash\mathbf{P}^1\cong\mathbf{P}^1$ are now determined by the triples $(\sigma_0,\sigma_1,\sigma_\infty)=\big((56),(15432),(123465)\big)$; $\big((15)(26)(34),(12536),(125643)\big)$ and $\big((15)(36),(132546),(135264)\big)$, respectively. The first of these is a $\mathbf{P}^1$-covering of $\mathbf{P}^1$, given explicitly by the map $z \mapsto 5(1-z)^6 - 6(1-z)^5 + 1$; the other two are coverings of genus one and models for these can be found in [26, pp. 66, 69]. Using this information, Proposition 7.1 now provides us with explicit forms of the coverings $C \to \mathbf{P}^1$.

For the sake of uniformity we give explicit models of the same form as used in (7.1), (7.2). The covering which comes from the first element in (2.5) is given by the section

$$y_1(y_1-y_0)(1296y_1^4 - 6048y_0y_1^3 + 10908y_0^2y_1^2 - 9156y_0^3y_1 + 3125y_0^4) \tag{7.4}$$

of $\mathcal{O}_{\mathbf{P}^1}(6)$ and the covering map

$$\frac{3125y_0^6 - 93312(y_0-y_1)^5y_1 + 432(y_0-y_1)^2(y_0-6y_1)z}{3125y_0^6}.$$

(Here z is a square-root of the section in (7.4).) A model for the fourth object from (2.5) is given by the section

$$(5y_1^2 - 6y_0y_1 + 5y_0^2)(5y_1^4 + 4y_0y_1^3 + 18y_0^2y_1^2 + 4y_0^3y_1 + 5y_0^4)$$

and the covering map

$$\frac{4y_0^6 + 4y_1^6 + (y_0-y_1)^6 + (y_0-y_1)(y_0^2+y_1^2)z}{8y_1^6}.$$

A model for the object from (2.7) is given by the section

$$(5y_1^2 + 2y_0y_1 + 5y_0^2)(5y_1^4 - 38y_0y_1^3 + 39y_0^2y_1^2 - 38y_0^3y_1 + 5y_0^4)$$

and the covering map

$$\frac{27y_0^6 + 27y_1^6 - 8(2y_0^2 - y_0y_1 + 2y_1^2)^3 + (y_0-y_1)(y_0^2 - 5y_0y_1 + y_1^2)z}{54y_1^6}.$$

8. Baby arithmetic

One of the main reasons for taking an interest in explicit algebraic forms for coverings of curves in characteristic zero, is to deduce results concerning the existence and behaviour of coverings of curves in characteristic p. In fact, the most general theorems concerning existence of coverings of curves in characteristic p are deduced by comparing with coverings of curves in characteristic zero. In the case of branched coverings, such a comparison gives more complete information if one restricts oneself to *tame* coverings. In the case of curves, tame coverings might of course be defined in classical terms, but to facilitate the comparison with the characteristic zero case one has to be more general. Hence we make the following definition:

Definition 8.1. Let X be a noetherian, irreducible and normal scheme, and let D be an effective divisor on X with normal crossings. Then a morphism $f : Y \to X$ is said to be a *tame covering* relative to D if f is finite, f is étale over the complement of the divisor D, the restriction of f to any irreducible component of Y is dominant, Y is normal and for any generic point x of the divisor D, Y is tamely ramified over $\mathcal{O}_{X,x}$. The category of tame coverings of X relative to D will be denoted $\mathrm{Rev}^D(X)$.

This is the definition given in [14, Definition 2.2.2], although we have allowed ourselves to be slightly more restrictive concerning X and D. We refer to (ibid.) for the definition of what normal crossings mean (in the case we consider D will have no crossings at all), as well as for an explication of the last condition (if needed). The main result about $\mathrm{Rev}^D(X)$ is now that it satisfies the axioms of a *Galois category* as defined by Grothendieck, see [14, Theorem 2.4.2].

Notice that in any Galois category $\mathcal{X}$ we may define the notion of a G-*object*; namely, a non-initial object X of $\mathcal{X}$ which is equipped with a right action by a finite group G such that $X \times G \cong X \times X$. A *Galois object* of the category is then a connected G-object.

Let (C, a) be a Galois object of $\mathcal{C}$ with Galois group G, where a now denotes the action $a : C \times G \to C$. Then if p does not divide the order of G, it follows from Grothendieck's specialisation theorem for the fundamental group that:

(8.1) *There exist a discrete valuation ring $R' \subset \overline{\mathbb{Q}_p}$ which is a finite and unramified extension of $\mathbb{Z}_p$ and a G-Galois object (C', a') in $Rev^{\{0,1,\infty\}}(\mathbf{P}^1_{R'})$ such that $(C' \otimes_{R'} \overline{\mathbb{Q}_p}, a' \otimes_{R'} \overline{\mathbb{Q}_p}) \cong (C \otimes_{\overline{\mathbb{Q}}} \overline{\mathbb{Q}_p}, a \otimes_{\overline{\mathbb{Q}}} \overline{\mathbb{Q}_p})$.*

(For a reasonably self-contained proof of the theorem which covers the stated result, cf. [23].)

We next turn to the case where p divides $|G|$. In this case, (8.1) is in general false. However, Raynaud has recently obtained a partial result [24, Theorem 0]. Let (C, a) be a K-model (where K is a number field) of a Galois object of $\mathcal{C}$ with Galois group G. Let R denote the ring of integers of K, and let $\mathfrak{p}$ be a maximal ideal in R. We write $R_{\mathfrak{p}}$ for the completion of R with respect to $\mathfrak{p}$, and $K_{\mathfrak{p}}$ for its field of fractions. Also, we let $p > 0$ be the characteristic of the residue field $R/\mathfrak{p}$. Now *if* the following conditions are fulfilled:

(1) (C, a) is branched over *each* of $0, 1, \infty \in \mathbf{P}^1_K$;
(2) G has trivial centre and admits a Sylow p-group Q of order p (i.e., $p^2 \nmid |G|$);
(3) $e < (p-1)/|N/Z|$, where e is the absolute ramification index of $R_{\mathfrak{p}}$, and N (Z) is the normaliser (centraliser) of Q in G;

then the following result holds:

(8.2) *There exist a discrete valuation ring $R' \subset \overline{K_{\mathfrak{p}}}$ which is a finite and unramified extension of $R_{\mathfrak{p}}$ and a G-Galois object (C', a') in $Rev^{\{0,1,\infty\}}(\mathbf{P}^1_{R'})$ such that $(C' \otimes_{R'} \overline{K_{\mathfrak{p}}}, a' \otimes_{R'} \overline{K_{\mathfrak{p}}}) \cong (C \otimes_K \overline{K_{\mathfrak{p}}}, a \otimes_K \overline{K_{\mathfrak{p}}})$.*

A naïve way to study the existence of tame coverings in characteristic p is to consider the coverings we have computed as defined over a ring of integers, pull back to the completion at a prime ideal (or possibly a discrete valuation ring which is a tamely ramified extension of the completion at the prime ideal), and find out whether the morphism is tamely ramified with respect to $\{0, 1, \infty\}$. In view of (8.1) (and the propositions of the appendix) this is interesting only at the prime ideals which divide the order of the monodromy group. Let us consider the first explicit example in Section 7 in this light. Let R be the completion of the ring of integers of $\mathbb{Q}(\sqrt{6}, \gamma)$ at the prime ideal generated by $\sqrt{6} - 1$, and let (C, f) now denote the pull-back to this ring of the model given by (7.1) and (7.2),(7.3). Then we have:

Assertion. *(C, f) is a tame covering of $\mathbf{P}^1_R$ relative to $\{0, 1, \infty\}$.*

Proof. Note that C is locally the Spec of $R[X, Y]/(Y^2 - h(X))$, and that no element in such a ring is annihilated by a non-zero element of R. Hence we can deduce the fact that C is integral from the fact that the generic fibre is integral. It is easy to see that f must be proper and surjective. We have to check that the restriction of f to the inverse image of the complement of $\{0, 1, \infty\}$ is finite and étale, and that C is normal.

C is flat over $\operatorname{Spec} R$. A local description of C as above, immediately gives that C is flat over $\operatorname{Spec} R$.

The special fibre of C is integral and f is flat. Over the residue field $\mathbb{F}_5(\sqrt{3})$ of R, the section (7.1) is

$$\begin{aligned} &y_1^6 - 2y_0y_1^5 - y_0^2y_1^4 + 2y_0^3y_1^3 - y_0^4y_1^2 - 2y_0^5y_1 - 1 \\ &\quad = (y_1 + y_0)(y_1 + 2y_0)(y_0^2 + y_0y_1 + y_1^2)(y_0^2 - y_0y_1 + 2y_1^2). \end{aligned}$$

In particular, there are no double roots, and hence the special fibre of C is integral (and in fact smooth). The map f is flat if and only if its restriction to the special fibre is flat. It is then enough to check that the image of the special fibre in $\mathbf{P}^1_k$ is not a point. But this is clearly immediate, since we already know that f is surjective.

The ramification locus of f has pure codimension one. The map f is proper and quasi-finite, hence finite. Since the map is finite and faithfully flat we get the result from the purity theorem (cf. [2, Theorem VI.6.8]).

The restriction of f to the inverse image of the complement of $\{0, 1, \infty\}$ is unramified. All primitive divisors of C except the special fibre correspond to divisors of the generic fibre. Hence for all primitive divisors except the special fibre (and except $\{0, 1, \infty\}$) unbranchedness follows from the corresponding result for the generic fibre. To check that the special fibre is unbranched amounts to checking that a field extension of the form $\mathbb{F}_5(\sqrt{3}, X) \to \mathbb{F}_5(\sqrt{3}, X)[Y]/(Y^2 - h(X))$ is separable, but this is obvious since the degree of the field extension is two whereas the characteristic is five.

C is normal. C is normal at each point in the generic fibre since this fibre is a regular curve. C is normal at the generic point of the special fibre since f is étale at this point. At the closed points of C we may note that the integrality of the special fibre means that the S_2-condition is fulfilled. □

Let us now view (C, f) above as a ramified covering of $\mathbf{P}^1_{\mathbb{Q}(\sqrt{6},\gamma)}$, and consider the corresponding $\mathcal{S}_6$-Galois covering (cf. the appendix). Obviously the Sylow five-subgroup of $\mathcal{S}_6$ has order five. The ramification index of R is one, whereas the order of N/Z is four. Hence the inequality $e < (p-1)/|N/Z|$ does not hold. However, in view of the results in the appendix, the conclusion in (8.2) still holds for our particular example.

Other non-trivial examples of non-abelian tame $\mathbf{P}^1$-coverings in mixed characteristics may be found in [24, §6.4] and [6, Proposition 8.7]. However, in all these examples, the inequality $e < (p-1)/|N/Z|$ holds.

Appendix

The following propositions are certainly well-known. However, for the sake of completeness and in ignorance of suitable references we state and prove them.

Proposition A.1. *Let $\mathcal{G}$ be a Galois category. Then for all positive integers n there is a category equivalence between the groupoid of objects of $\mathcal{G}$ of degree n, and the groupoid of $\mathcal{S}_n$-objects in $\mathcal{G}$. Furthermore, in the case that the object of degree n is connected, then the number of components of the corresponding $\mathcal{S}_n$-object is equal to the index of the monodromy group in $\mathcal{S}_n$.*

Proof. It is enough that for any pro-finite group π_1 establish a category equivalence between the groupoid of objects with n elements in π_1-sets (the category of finite sets with a continuous right action of π_1) and the groupoid of objects in π_1-sets on which S_n acts freely and transitively. Now it is easy to check that

$$F \mapsto \mathrm{Isom}_{\mathrm{Sets}}(\{1, 2, \ldots, n\}, F)$$

defines such an equivalence with

$$P \mapsto P \times^{\mathcal{S}_n} \{1, 2, \ldots, n\}$$

as its quasi-inverse. □

Proposition A.2. *Let $\mathcal{G}, \mathcal{G}'$ be Galois categories, and assume that $\varphi : \mathcal{G} \to \mathcal{G}'$ is an exact functor. Then the category equivalence of Proposition A.1 commutes with φ.*

Proof. After the choice of a fibre functor of $\mathcal{G}'$, φ translates to the restriction of the action of fundamental groups. Then the statement is obvious. □

Consider now the situation when (X, D) is as in Definition 8.1, Y is a noetherian, irreducible and normal scheme, and $g : Y \to X$ is a morphism such that $g^*(D)$ is defined and is a divisor with normal crossings. Then $X' \mapsto X' \times_X Y$ defines a functor φ from $\mathrm{Rev}^D(X)$ to $\mathrm{Rev}^{g^*(D)}(Y)$ (cf. [14, Corollary 2.3.6]). If a' is a geometric point in $Y \setminus g^*(D)$ and $a = g(a')$, and if F_a respectively $F_{a'}$ are the corresponding fibre functors, then $F_a \simeq F_{a'} \circ \varphi$. Hence φ is exact (cf. [13, Proposition V.6.1]). This means that the propositions above apply to this situation.

References

[1] L. Ahlfors, *Complex analysis*, 2nd edition, McGraw-Hill, 1966.

[2] A. Altman and S. Kleiman, *Introduction to Grothendieck Duality Theory*, Lecture Notes in Math. **146**, Springer-Verlag, 1970.

[3] A. O. L. Atkin and H. P. F. Swinnerton-Dyer, Modular forms on noncongruence subgroups, Proc. Sump. Pure Math. A.M.S. XIX, 1–25 (1971).

[4] S. Beckmann, Ramified Primes in the Field of Moduli of Branched Coverings of Curves, J. Algebra **125** (1989), pp. 236–255.

[5] Г.Б. Белый (G.B. Belyi), О расширениях Галуа максимального кругового поля, Изв. Акад. Наук СССР Сер. Мат. **43** (1979), 267–276, translated as Galois extensions of a maximal cyclotomic field, Math USSR Izv. **14**, No. 2 (1980), pp. 247–256.

[6] I. I. Bouw, Reduction of the Hurwitz space of metacyclic covers. Available at arXiv:math.AG/0204043, 2002.

[7] K. Chandrasekharan, *Elliptic Functions*, Springer-Verlag, 1985.

[8] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, 1993.

[9] J.-M. Couveignes and L. Granboulan, Dessins from a geometric point of view, in [27], pp. 79–113.

[10] P. A. Fuhrmann, *A Polynomial Approach to Linear Algebra*, Springer-Verlag, 1996.

[11] P. Gianni, M. Seppälä, R. Silhol and B. Trager, Riemann surfaces, plane algebraic curves and their period matrices, J. Symbolic Comput. **26** (1998), pp. 789–803.

[12] A. Good, Cusp forms and eigenfunctions of the Laplacian, Math. Ann. **255** (1981), pp. 523 – 548.

[13] A. Grothendieck, *Revêtements Etales et Groupe Fondamental*, Lecture Notes in Math. **224**, Springer-Verlag, 1971.

[14] A. Grothendieck and J. P. Murre, *The Tame Fundamental Group of a Formal Neighbourhood of a Divisor with Normal Crossings on a Scheme*, Lecture Notes in Math. **208**, Springer-Verlag, 1971.

[15] R. C. Gunning *Lectures on Modular Forms*, Annals of Math. Studies No. 48, Princeton University Press, 1962.

[16] R. C. Gunning *Lectures on Riemann Surfaces*, Princeton Mathematical Notes, Princeton University Press, 1966.

[17] D. A. Hejhal, *The Selberg Trace Formula for PSL(2,**R**)*, Vol. 2, Lecture Notes in Math. **1001**, Springer-Verlag, 1983.

[18] D. A. Hejhal, On eigenfunctions of the Laplacian for Hecke triangle groups, in *Emerging Applications of Number Theory* (edited by D. Hejhal, J. Friedman, M. Gutzwiller, A. Odlyzko), IMA Series No. 109, Springer-Verlag, 1999, pp. 291–315.

[19] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, 1967.

[20] J. Lehner, *Discontinuous Groups and Automorphic Functions*, AMS Math. Surveys No. 8, 1964.

[21] P. Lochak and L. Schneps (editors), *Geometric Galois Actions*, volumes 1 and 2, LMS Lecture Note Series **242**, **243**, Cambridge University Press, 1997.

[22] T. Miyake, *Modular Forms*, Springer-Verlag, 1989.

[23] F. Orgogozo and I. Vidal, Le théorème de spécialisation du groupe fondamental, in *Courbes semi-stables et groupe fondamental en géométrie algébrique*, (edited by J.-B. Bost, F. Loeser, M. Raynaud), Progr. Math. 187, Birkhäuser, 2000, pp. 169–184.

[24] M. Raynaud, Spécialisation des Revêtements en Caractéristique $p > 0$, Ann. scient. Éc. Norm. Sup., 4^e série, t. 32, 1999, pp. 87–126.

[25] M. Reid, Hyperelliptic Linear Systems on a K3 Surface, J. London Math. Soc. (2) **13** (1976), pp. 427–437.

[26] M. J. Richards, *Computing Covering Maps for subgroups of* $\Gamma(1)$ *with genus* ≥ 1, Thesis, University of Oxford, 1996.

[27] L. Schneps (editor), *The Grothendieck Theory of Dessins d'Enfants* LMS Lecture Note Series **200**, Cambridge University Press, 1994.

[28] B. Selander and A. Strömbergsson, Some explicit covering maps, preliminary note (2003) available from www.math.princeton.edu/∼astrombe/papers.html.

[29] M. Seppälä, Computation of period matrices of real algebraic curves, Discrete Comput. Geom. **11** (1994), pp. 65–81.

[30] J.-P. Serre, *Topics in Galois Theory*, Research Notes in Mathematics, vol. **1**, Jones and Bartlett Publishers, Boston, London, 1992.

[31] M. Streit, Homology, Belyi functions and canonical curves, Manuscripta Math. **90** (1996), pp. 489–509.

[32] F. Strömberg, Computation of eigenvalues of the Laplacian and Maass waveforms for Hecke congruence subgroups, research announcement, 2002. [Available electronically at: www.math.uu.se/~fredrik]

[33] Z. Wang, Analytic number theory, complex variable, and supercomputers, Undergraduate thesis, Univ. of Minnesota, 1994.

(B.S.) Department of Mathematics, Box 480, Uppsala University, S-75106 Uppsala, Sweden
bjorn@math.uu.se

(A.S.) Department of Mathematics, Princeton University, Princeton, NJ 08544, U.S.A.
Astrombe@Princeton.edu