Journal of Symbolic Computation ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

On rational functions with monodromy group M_{11}

Joachim König

Universität Würzburg, Emil-Fischer-Str. 30, 97074 Würzburg, Germany

ARTICLE INFO

Article history:
Received 2 May 2015
Accepted 8 February 2016
Available online xxxx

Keywords:
Galois theory
Number fields
Moduli spaces
Monodromy groups

ABSTRACT

We compute new polynomials with Galois group M_{11} over $\mathbb{Q}(t)$. These polynomials stem from various families of covers of $\mathbb{P}^1\mathbb{C}$ ramified over at least 4 points. Each of these families has features that make a detailed study interesting. Some of the polynomials lead, via specialization, to number fields with very small discriminant or few ramified primes.

1. Theoretical background

As the following sections make use of Hurwitz spaces as moduli spaces for families of covers of the projective line, I will begin with a very brief outline of the theory. More thorough introductions may be found e.g. in Debes and Fried (1994) or Völklein (1996).

Let G be a finite group and $C = (C_1, \dots, C_r)$ be an r-tuple of conjugacy classes of G, all $\neq \{1\}$. The Nielsen class of the class tuple C is defined as

$$Ni(C) = \{(\sigma_1, \dots, \sigma_r) \in G^r \mid \langle \sigma_1, \dots, \sigma_r \rangle = G, \sigma_1 \cdots \sigma_r = 1, \exists_{\pi \in S_r} : \sigma_i \in C_{\pi(i)} (i = 1, \dots, r)\}.$$

The inner Nielsen class $Ni^{in}(C)$ is defined as the quotient of $Ni(C)$ by the diagonal action of $Inn(G)$. The analogous sets with the additional requirement $\pi = id$ are called the straight Nielsen classes $SNi(C)$ resp. $SNi^{in}(C)$.

It is well known that the elements of $Ni^{in}(C)$ parametrize branched Galois covers of $\mathbb{P}^1\mathbb{C}$ in the following way:

E-mail address: joachim.koenig@mathematik.uni-wuerzburg.de.

http://dx.doi.org/10.1016/j.jsc.2016.02.014
0747-7171/© 2016 Published by Elsevier Ltd.

Let $\{p_1, \ldots, p_r\}$ be a fixed subset of $\mathbb{P}^1\mathbb{C}$ of cardinality r, $p_0 \in \mathbb{P}^1\mathbb{C} \setminus \{p_1, \ldots, p_r\}$ and $f : \pi_1(\mathbb{P}^1\mathbb{C} \setminus \{p_1, \ldots, p_r\}, p_0) \to G$ an epimorphism (which, by Riemann's existence theorem, induces a Galois cover) mapping the r-tuple of standard fundamental group generators to an element of $Ni(C)$.

Now f and f' (with same branch point sets and same base point) are defined to by equivalent if for some $\gamma \in \pi_1(\mathbb{P}^1\mathbb{C} \setminus \{p_1, \ldots, p_r\}, p_0)$: $f(\gamma\delta\gamma^{-1}) = f'(\delta)$ for all $\delta \in \pi_1(\mathbb{P}^1\mathbb{C} \setminus \{p_1, \ldots, p_r\}, p_0)$.

Letting the branch points vary over all r-sets in $\mathbb{P}^1\mathbb{C}$, the set of these equivalence classes forms a (not necessarily connected) algebraic variety (for non-empty $Ni(C)$, of course), known as the inner Hurwitz space $\mathcal{H}^{in}(C)$. This variety comes with a natural morphism $\Psi : \mathcal{H}^{in}(C) \to \mathcal{U}_r$ to the space $\mathcal{U}_r$ of r-subsets of $\mathbb{P}^1\mathbb{C}$, mapping (an equivalence class of) a cover to the set of its branch points.

The elements of a given fiber of Ψ correspond one-to-one to the elements of $Ni^{in}(C)$.

If $Z(G) = \{1\}$, then by a famous theorem of Fried and Völklein (1991, Corollary 1), G occurs as the Galois group of a regular Galois extension of $\mathbb{Q}(t)$ iff the inner Hurwitz space $\mathcal{H}^{in}(C)$ contains a rational point for some class tuple C of G. In other words, inner Hurwitz spaces are fine moduli spaces under the assumption $Z(G) = \{1\}$.

Remark. We restrict here to the notion of inner Hurwitz spaces. In certain contexts, *absolute* Hurwitz spaces are more natural. However, for the purpose of this paper, there is no difference anyway, since the Mathieu group M_{11} has no outer automorphisms.

To find out about the existence of rational points, one needs to investigate the algebraic structure of the Hurwitz spaces. The dimension of the Hurwitz spaces can be reduced by 3 via the action of $PGL_2(\mathbb{C})$ on $\mathbb{P}^1\mathbb{C}$, which induces an equivalence relation on $\mathcal{U}_r$, and thereby also on $\mathcal{H}^{in}(C)$. Under relatively mild assumptions, rational points on the reduced Hurwitz spaces also lift to rational points on the non-reduced ones. Especially for $r = 4$, reduced Hurwitz spaces are curves. The genera of these curves, and more generally, of certain curves on Hurwitz spaces of higher dimension, can be computed from the action of the Hurwitz braid group $\mathcal{H}_r$ on $Ni^{in}(C)$, which acts on $Ni(C)$ via $(\sigma_1, \ldots, \sigma_r)^{B_i} = (\sigma_1, \ldots, \sigma_{i-1}, \sigma_i\sigma_{i+1}\sigma_i^{-1}, \sigma_i, \ldots, \sigma_r)$, $i = 1, \ldots, r-1$, where $B_1, \ldots, B_{r-1}$ are the standard generators of the braid group, as defined e.g. in Malle and Matzat (1999, Chapter III.1.2).

This action has an interpretation as a monodromy action on the fibers of the branch point reference cover $\Psi : \mathcal{H}^{in}(C) \to \mathcal{U}_r$.

Similarly, for different versions of covers of reduced Hurwitz spaces over suitable parameter spaces,[1] the appropriate choice of braids yields the monodromy action of the cover. Therefore, the cycle types of the monodromy group generators (which depend on the exact version of the parameter space, e.g. on symmetrization of branch points) yield explicit genus formulas for the Hurwitz curves. Cf. III. (5.11) and Theorem III.7.8 in Malle and Matzat (1999) for such formulas.

In particular, for *rational* class 4-tuples C, if $\mathcal{H}^{in}(C)$ is connected (or more generally, if there is a rigid orbit in the braid group action) and the braid genus is zero, with some oddness condition satisfied (assuring that the genus zero curve is actually a rational curve), then the existence of infinitely many rational points on $\mathcal{H}^{in}(C)$ follows.

For larger genus (or for varieties of dimension > 1), explicit computation may help to clarify the situation. Hopefully, this paper supports that there is some value in explicit computation of Hurwitz families.

2. Overview of known M_{11} extensions of $\mathbb{Q}(t)$

In the following, we consider Galois extensions with Galois group the Mathieu group M_{11}. This group is the smallest sporadic simple group (of order $7920 = 11 \cdot 10 \cdot 9 \cdot 8$) and has a sharply 4-transitive action on 11 points.

[1] If some of the classes $C_1, \ldots, C_r$ occur several times in the class tuple C, there are various ways to "symmetrize" the branch points, leading to different variants of reduced Hurwitz spaces. I will not elaborate on this here; for a detailed outline cf. e.g. Malle and Matzat (1999, Chapter III.7).

Please cite this article in press as: König, J. On rational functions with monodromy group M_{11}. J. Symb. Comput. (2016), http://dx.doi.org/10.1016/j.jsc.2016.02.014