A ONE-PARAMETER FAMILY OF DEGREE 36
POLYNOMIALS WITH \( PSp_6(2) \) AS GALOIS GROUP OVER
\( \mathbb{Q}(t) \)

DOMINIK BARTH AND ANDREAS WENZ

Abstract. We present a one-parameter family of degree 36 polynomials with the symplectic 2-transitive group \( PSp_6(2) \) as Galois group over \( \mathbb{Q}(t) \).

In the following we will refer to well known facts about covers of the Riemann sphere \( \mathbb{P}^1 \mathbb{C} \) and Hurwitz spaces appearing in e.g. [4], [6] and [7].

Let \( \vec{C} = (C_1, C_2, C_3) \) be the class vector of the group \( PSp_6(2) \hookrightarrow S_{36} \), where the conjugacy classes \( \{C_i\}_{i=1,2,3} \) are unique of type \((3^{12})\), \((1^{12}.2^{12})\), and \((1^6.2^4)\), and \( H \) the associated \((2,3)\)-symmetrized Hurwitz curve\(^1\). The corresponding straight inner Nielsen class is of length 2 and forms a single orbit under the braid group action. Therefore, the branch point reference map \( H \to \mathbb{P}^1 \mathbb{C} \) is of degree 2, and ramified over two rational points. Combining this observation with the rationality of all classes in \( \vec{C} \) yields that \( H \) is a rational genus-0 curve over \( \mathbb{Q} \). This implies that \( PSp_6(2) \) occurs as a Galois group over \( \mathbb{Q}(a, t) \) where the ramification with respect to \( t \) is described by \( \vec{C} \).

In order to obtain an explicit polynomial with \( PSp_6(2) \) as Galois group we follow the method described in [1] by computing a four-branch point cover \( f \) corresponding to \( \vec{C} \). Assume \( f \) has the ramification locus consisting of 0, 1, \(-1, \infty \), then \( f^2 \) turns out to be a Belyi map ramified over 0, 1, \( \infty \), and its (transitive) monodromy group is contained in the wreath product \( PSp_6(2) \wr C_2 \hookrightarrow S_{72} \). The corresponding ramification has to be of type \((6^{12})\), \((1^{24}.2^{24})\) and \((2^6.4.8^7)\). Now, \( PSp_6(2) \wr C_2 \) contains exactly one triple \((x, y, z)\) (up to simultaneous conjugation) which satisfies \( xyz = 1 \) and the above conditions describing the monodromy of \( f^2 \). It is given by

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

\(^1\)\( H \) can be interpreted as the family of four-branch-point covers of \( \mathbb{P}^1 \mathbb{C} \) ramified over 0, 1 \( \pm \sqrt{\lambda} \), \( \infty \) with ramification data \( \vec{C} \).
and
\[ z = (1, 71, 35, 40, 4, 52, 16, 37)(2, 46, 10, 67, 31, 65, 29, 38) \]
\[ (3, 49, 13, 56, 20, 68, 32, 39)(5, 64, 28, 59, 23, 72, 36, 41)(6, 42) \]
\[ (7, 43)(8, 54, 18, 66, 30, 50, 14, 44)(9, 45)(11, 57, 21, 47) \]
\[ (12, 51, 15, 55, 19, 69, 33, 48)(17, 53)(22, 63, 23, 61, 25, 62, 26, 58) \]
\[ (24, 60)(34, 70). \]

Applying the method explained in [2] and [1] we compute the desired Belyi map:
\[ f^2(X) = -2^{-4} \cdot 3^{-8} \cdot \frac{p(X)}{q(X)} \in \mathbb{Q}(X) \]
where
\[ p(X) = (X^{12} + 8X^{11} - 10X^{10} - 40X^9 - 69X^8 - 96X^7 - 84X^6 \]
\[ -48X^5 - 21X^4 - 40X^3 - 26X^2 - 8X + 1)^6, \]
\[ q(X) = (X^3 + 3X + 2)^8 \left( X^4 + \frac{4}{3}X^3 - \frac{1}{3} \right)^8 \left( X^6 + \frac{3}{2}X^4 + \frac{1}{2} \right)^2. \]

This, obviously, gives us \( f \in \mathbb{C}(X) \) ramified over 0, 1, −1, and \( \infty \). Finally, we follow the approach in [1] to find a one-parameter family of polynomials with Galois group \( PSp_6(2) \) over \( \mathbb{Q}(t) \) corresponding to \( \mathcal{H} \):

**Theorem.** Let \( f(a, t, X) = p(a, X) - tq(a, X) \in \mathbb{Q}(a, t)[X] \) where
\[ p(a, X) = \left( X^{12} + X^{11} + \left( 144a + \frac{1}{8} \right)X^{10} + 40aX^9 + \left( -1728a^2 + \frac{21}{4}a \right)X^8 \right. \]
\[ + \left. \left( -576a^2 + \frac{3}{8}a \right)X^7 - 84a^2X^6 - 6a^2X^5 + \left( 144a^3 - \frac{3}{64}a^2 \right)X^4 \right. \]
\[ + \left. 40a^3X^3 + \frac{13}{4}a^3X^2 + \frac{1}{8}a^3X + a^4 \right)^3, \]

and
\[ q(a, X) = \left( X^6 - 12aX^4 + \frac{1}{2}a^2 \right) \cdot \left( X^3 - 24aX - 2a \right)^4 \]
\[ \cdot \left( X^4 + \frac{1}{6}X^3 + \frac{1}{24}a \right)^4. \]

Then the Galois group of \( f \) over \( \mathbb{Q}(a, t) \) is isomorphic to \( PSp_6(2) \) \( \hookrightarrow \) \( S_{16} \), and the branch cycle structure of \( f \) with respect to \( t \) is given by \( (3^{12}, 1^{12}2^{12}, 1^{12}2^{12}, 1^62^47) \).

The polynomial is also contained in the ancillary Magma-readable [3] file. Another polynomial with \( PSp_6(2) \) as Galois group of degree 28 (associated to a different class vector) that possesses infinitely many totally real specializations was found recently by the two authors and J. König, see [1].

In order to prove the theorem we require the following observation:
Lemma. Let $K$ be an arbitrary field, $p(X), q(X) \in K[X]$ be coprime and $G := \text{Gal}(p(X) - tq(X) \mid K(t))$. Further assume there exists an irreducible polynomial $r(X) \in K(t)[X]$ of degree $n$ such that $r(X) \in K(s)[X]$ becomes reducible where $t = \frac{p(s)}{q(s)}$. Then there exists a divisor $d \neq 1$ of $n$ such that $G$ possesses an index $d$ subgroup.

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

![Diagram showing the relationships between $K(t)$, $L$, and $p(X) - tq(X)$]

Thanks to the assumption that $r(X)$ splits nontrivially over $K(s)$, the polynomial $p(X) - tq(X)$ is reducible over $K(t, y)$, thus $K(t, y) \subseteq L \cap K(t, y)$. Via Galois correspondence $G = \text{Gal}(L \mid K(t))$ must contain an index $d$ subgroup where $d \neq 1$ is a divisor of $n$.

Proof of the theorem. Let $f_1, p_1, q_1 \in \mathbb{Q}(t)[X]$ denote the specializations of $f, p, q$ at the place $a \mapsto 1$, and $\tilde{f}_1, \tilde{p}_1, \tilde{q}_1$ their images in $\mathbb{F}_{37}(t)[X]$ under the canonical projection.

Using Magma the discriminant of $f$ turns out to be

$$
\Delta = 2^{732} \cdot 3^{108} \cdot \left(a - \frac{1}{512}\right)^{154} \cdot a^{290} \cdot t^{24} \cdot \left(t^2 + \left(-2592a - \frac{81}{16}\right) t + 1679616a^2 - 6561a + \frac{6561}{1024}\right)^{12}.
$$

With this formula we see that $f$ and $f_1$ have exactly four branch points with respect to $t$. Furthermore the branch cycle structure of $f$ can be derived by inspecting the inseparability behaviour of $f$ evaluated at the places $t \mapsto 0$, $t \mapsto \infty$, and $t \mapsto r_i$ for $i = 1, 2$ where $r_1$ and $r_2$ denote the non-zero roots of $\Delta \in \mathbb{Q}(a)[t]$.

By a theorem of Malle (see [3]), the two Galois groups $\text{Gal}(f \mid \mathbb{Q}(a, t))$ and $\text{Gal}(f_1 \mid \mathbb{Q}(t))$ coincide. It remains to show that $\text{Gal}(f_1 \mid \mathbb{Q}(t))$ is isomorphic to $\text{PSp}_6(2)$.

Since $\frac{1}{X - \tilde{q}_1} \cdot \tilde{f}_1 \left(\frac{\tilde{p}_1(t)}{\tilde{q}_1(t)}, X\right) \in \mathbb{F}_{37}(t)[X]$ is irreducible the Galois group of $\tilde{f}_1$ over $\mathbb{F}_{37}(t)$ must be 2-transitive of permutation degree 36, implying $\text{Gal}(\tilde{f}_1 \mid \mathbb{F}_{37}(t)) \in \{\text{PSp}_6(2), A_{36}, S_{36}\}$. Dedekind reduction yields $\text{Gal}(f_1 \mid \mathbb{Q}(t)) \in \text{PSp}_6(2)$.

\footnote{A well known result in field theory states: Let $K$ be a field, and $a, b$ algebraic over $K$ with minimal polynomials $\mu_a, \mu_b \in K[X]$. Then $\mu_a$ is irreducible over $K(b)$ if and only if $\mu_b$ is irreducible over $K(a)$.}
\{PSp_6(2), A_{36}, S_{36}\}. Since both discriminants of \( f_1 \) and \( \bar{f}_1 \) are squares, we can each exclude the group \( S_{36} \). In particular, \( \text{Gal}(f_1 \mid \mathbb{Q}(t)) \) is simple, and the corresponding function field extension must be regular, allowing us to apply a theorem of Beckmann, see \[ \text{Chapter I, Proposition 10.9} \], to obtain \( \text{Gal}(f_1 \mid \mathbb{Q}(t)) \cong \text{Gal}(\bar{f}_1 \mid \mathbb{F}_{37}(t)) \).

Let \( r(t, X) \in \mathbb{F}_{37}(t)[X] \) be the irreducible polynomial of degree 63 in the ancillary file, then \( r\left(\bar{f}_1(t), \frac{\bar{f}_1(t)}{\bar{q}_1(t)}, X\right) \) becomes reducible over \( \mathbb{F}_{37}(t) \). The previous lemma guarantees the existence of an index \( d \neq 1 \) subgroup of \( \text{Gal}(\bar{f}_1 \mid \mathbb{F}_{37}(t)) \) where \( d \) is a divisor of 63. Since \( A_{36} \) does not contain such a subgroup we end up with \( \text{Gal}(\bar{f}_1 \mid \mathbb{F}_{37}(t)) = PSp_6(2) \), completing the proof.

\[ \Box \]

\section*{Acknowledgements}

We would like to thank Peter Müller for some valuable suggestions regarding the proof of the theorem.

\section*{References}

[1] D. Barth, J. König and A. Wenz. An approach for computing families of multi-branch-point covers and applications for symplectic Galois groups. 2018, arxiv:1803.08778v1
[2] D. Barth and A. Wenz. Belyi map for the sporadic group J1. 2017, arXiv:1704.06419v1.
[3] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. \textit{J. Symbolic Comput.}, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
[4] M. D. Fried and H. Völklein. The inverse Galois problem and rational points on moduli spaces. \textit{Math. Ann.}, 290(4):771–800, 1991.
[5] G. Malle. Multi-parameter polynomials with given Galois group. \textit{J. Symbolic Comput.}, 30(6):717–731, 2000. Algorithmic methods in Galois theory.
[6] G. Malle and B. Matzat. \textit{Inverse Galois theory. 2nd edition}. Berlin: Springer, 2018.
[7] H. Völklein. \textit{Groups as Galois groups}, volume 53 of \textit{Cambridge Studies in Advanced Mathematics}. Cambridge University Press, Cambridge, 1996. An introduction.

\textbf{Institute of Mathematics, University of Würzburg, Emil-Fischer-Strasse 30, 97074 Würzburg, Germany}

\textit{E-mail address:} dominik.barth@mathematik.uni-wuerzburg.de
\textit{E-mail address:} andreas.wenz@mathematik.uni-wuerzburg.de

---

\(3\)The polynomial \( r \), which is a minimal polynomial of a primitive element of the fixed field of an index 63 subgroup of \( PSp(6,2) \), was obtained by using the \texttt{Magma} command \texttt{GaloisSubgroup}. 