J. Symbolic Computation (2000) **21**, 1–15
doi:10.1006/jsco.2000.0379
Available online at http://www.idealibrary.com on IDEAL®

Multi-parameter Polynomials with Given Galois Group

GUNTER MALLE

FB Mathematik, Universität Kassel, Heinrich-Plett-Str. 40, 34132 Kassel, Germany

We present a collection of multi-parameter polynomials for several mostly non-solvable permutation groups of small degree and describe their construction. As an application we are able to obtain totally real number fields with these Galois groups over the rationals, for example for the two small Mathieu groups M_{11} and M_{12}.

© 2000 Academic Press

1. Introduction

The non-Abelian finite simple groups and their automorphism groups play a crucial role in an inductive approach to the inverse problem of Galois theory. The rigidity method (see, for example, Malle and Matzat, 1999) has proved very efficient for deducing the existence of Galois extensions with such groups, as well as for the construction of polynomials generating such extensions. Nevertheless, the effective construction requires the solution of a nonlinear system of equations, a problem which is known to be very hard from a complexity point of view. Thus, in practice, the computation of polynomials is restricted to rather small degree, to the case of stem fields of genus zero and also to few (mostly three) ramification points. For several applications, for example for the solution of embedding problems, it is sometimes necessary to find Galois extensions of the rationals with given group and with complex conjugation lying in a prescribed conjugacy class. But it is well known (see, for example, Malle and Matzat, 1999, Example I.10.2) that three-point ramified Galois extensions almost never have totally real specializations, for example.

In this paper we give two-, three- and four-parameter polynomials for certain (mostly non-solvable) groups which, from a certain point of view, correspond to Galois extensions ramified in at least four points, with the property that these admit (infinitely many) totally real, Galois group preserving specializations. For example we obtain a two-parameter polynomial for the sporadic simple Mathieu group M_{12} over $\mathbb{Q}$. Suitable specializations then yield totally real number fields with groups M_{11} and M_{12}.

2. Background Results

We review some results on rigidity for Galois extensions with many ramification points, as explained for example in Malle and Matzat (1999). Let G be a finite group with trivial centre and $\mathbf{C} = (C_1, \ldots, C_r)$ a tuple of conjugacy classes of G. We write

$$\bar{\Sigma}(\mathbf{C}) := \{(\sigma_1, \ldots, \sigma_r) \mid \sigma_i \in C_i \, (1 \le i \le r), \, \sigma_1 \cdots \sigma_r = \iota\}$$

0747–7171/00/000001 + 15 $35.00/0 © 2000 Academic Press

and

$$\Sigma(\mathbf{C}) := \{(\sigma_1, \ldots, \sigma_r) \in \bar{\Sigma}(\mathbf{C}) \mid \langle \sigma_1, \ldots, \sigma_r \rangle = G\}.$$

By the Hurwitz classification for fields of characteristic zero, which derives from the Riemann existence theorem, for any choice of r distinct ramification points in $\mathbb{C} \cup \{\infty\}$ and any $(\sigma_1, \ldots, \sigma_r) \in \Sigma(\mathbf{C})$ there exists a Galois extension $N/\mathbb{C}(t)$ with group G and $(\sigma_1, \ldots, \sigma_r)$ as inertia group generators. The collection of all these extensions naturally carries an algebraic structure, called the Hurwitz space $\mathcal{H}$ attached to the tuple $\mathbf{C}$. The braid orbit theorems (see, for example, Malle and Matzat, 1999, Chapter III) give sufficient criteria for a field of definition of such an extension being contained in the field generated by the branch points.

In the case of four branch points (three of which we may assume to be algebraic over $\mathbb{Q}$ via the action of $\mathrm{PGL}_2(\mathbb{Q})$) the Hurwitz space $\mathcal{H}$ is a curve. Its number of components and their genera can be deduced by group-theoretical computations from the branch cycle description. More precisely, the number of components equals the number of orbits of the braid group on $\Sigma(\mathbf{C})$ and the genera are invariants of this action.

Conversely, assume given a Galois extension $N/k(t_1, \ldots, t_n)$ of a purely transcendental extension $k(t_1, \ldots, t_n)$ over a field k of characteristic zero. A partial description of such extensions can be obtained via a reduction to the one-dimensional case as follows. We view N as a function field in one variable over $K(t_n)$, where $K := k(t_1, \ldots, t_{n-1})$. This can be described by the Hurwitz classification. In particular, $N/K(t_n)$ has a branch cycle description in terms of generators of inertia groups at ramified points. These ramification points will in general depend on the parameters $t_1, \ldots, t_{n-1}$. Clearly this description is not unique but depends on the choice of field of constants K.

3. How the Polynomials were Found

Most of the polynomials given in this paper generate regular field extensions of a function field of genus zero, whose existence can be deduced from the braid orbit rationality criteria sketched in the previous section. Thus, at least in principle, they could be computed by solving a suitable system of nonlinear equations which can be deduced mechanically from the ramification data (see Malle and Matzat, 1999, Chapter I.9). But it turns out that in practice the resulting systems of equations are much to complicated and possess too many complex solutions (belonging to different Galois groups) to be solved on present-day computers.

Thus we used the rationality criteria just as an indication that extensions with certain properties exist, and constructed the polynomials in a different way.

3.1. Interpolation in the Hurwitz space

The first method used was what could be called *interpolation in the Hurwitz space*. Assume that a regular Galois extension $N/k(t)$ has a rational stem field $k(x)$, i.e. the Galois closure of $k(x)/k(t)$ equals N. Then there exists a generating polynomial of the form $f(t, X) = f_1(X) + tf_2(X)$ with $f_1, f_2 \in k[X]$. If, moreover, $N/k(t)$ has a rational ramification point, which, without loss we may assume to lie at $t = \infty$, then $f_2(X)$ is inseparable (or has degree $\deg(f_2) \leq \deg(f_1) - 2$). In particular, for any two specializations $f(t_i, X)$, $t_i \in k$ for $i = 1, 2$, the difference $f(t_1, X) - f(t_2, X)$ is inseparable, and moreover the degrees of all of its factors are determined by the ramification behaviour at $t = \infty$.

This can be used in the following way. Assume the rationality criteria predict the existence of a Galois extension $N/k(t)$ with group G having a rational stem field and a rational ramification point. Given "many" polynomials $g_i(X) \in \mathbb{Q}[X]$ with this Galois group we can search for cases where $g_i(X) - g_j(X)$ is inseparable with the right factorization behaviour. For each such pair, it can be tested whether the polynomial

$$g_{ij}(t, X) := g_i(X) + t(g_i(X) - g_j(X))$$

has Galois group G. In practice this turned out to be true in an overwhelming number of cases.

The one-parameter polynomials found in this way should then be transformed into a suitable normal form, usually by fixing branch points and certain points lying above branch points. Having done this, the resulting polynomials can again interpolated in order to try and add a further parameter, and so on.

Let us illustrate this on a particular example: for the group $G = \mathrm{L}_3(2)$ we consider the ramification type $(2^2, 2^2, 2^2, 2^2, 3^2)$. Assume that $f(t, X)$ generates a stem field K of degree 7 for a regular Galois extension of $\mathbb{Q}(t)$ with this branch cycle description. We may replace t via a linear fractional transformation so that its denominator divisor has ramification order 3. Since K is a rational function field (by the Hurwitz relative genus formula) there exists a generating element x of K whose numerator and denominator divisor both lie over the denominator divisor of t. It can thus easily be seen that f can be taken to have the form $g(X) + tX^3(X - 2)$, where $g(X) \in \mathbb{Q}[X]$ is monic of degree 7 and with vanishing coefficient at X^4.

Starting from roughly 2000 polynomials $g_i(X)$ over $\mathbb{Q}$, more than 150 different polynomials $g_{ij}(t, X)$ of that shape were found. Interpolating these yielded several dozen two-parameter polynomials with the right Galois group. For $\mathrm{L}_3(2)$ this procedure could be repeated three times, so as to yield a four-parameter polynomial (see Theorem 4.3). Theory shows that with the ramification types considered, this is the maximal number of independent parameters possible.

3.2. Hensel lifting

A more conceptual approach is by Hensel lifting. For the larger groups treated in this paper, only relatively few polynomials $f(X) \in \mathbb{Q}[X]$ (with reasonably sized coefficients) could be found. The interpolation method then only yielded a few (or just one) one-parameter polynomial with the right ramification type. Let us denote by S the nonlinear system of (algebraic) equations describing all polynomials defining extensions with the given ramification type. This system can be computed from the ramification data. Clearly the coefficients of our polynomial $f(t, X)$ are a solution to S. More precisely, they correspond to one particular choice $a_1, \ldots, a_r \in \overline{\mathbb{Q}}$ of the four (or more) branch points. Thus $f(t, X)$ may be considered as the reduction of a polynomial $h(u, t, X)$ modulo the ideal (u) of $\mathbb{Q}((u))$ which is the solution of S for the choice $a_1 + u, a_2, \ldots, a_r$ of branch points. Hence $h(u, t, X) \in \mathbb{Q}((u))(t)[X]$ may be approximated from the specialization $h(0, t, X) = f(t, X)$ via Hensel lifting modulo increasing powers of u.

Since the coefficients of h solve an algebraic system of equations, they are algebraic over $\mathbb{Q}(u)$. Let $a(u) \in \mathbb{Q}((u))$ be such a coefficient. Then there exists a polynomial $r(U, V) \in \mathbb{Q}[U, V]$ such that $r(u, a(u)) = 0$ identically. This polynomial $r(U, V)$ can be found by plugging the (first few terms of the) power series $a(u)$ into the general polynomial of degree d. Its unknown coefficients can then be found by solving the linear

system of equations obtained by comparing coefficients at powers of u. (If d was chosen too small, no solution will exist, but after increasing d, a solution will eventually be found.) If the Hurwitz space for the chosen ramification type is rational, there will exist a rational parametrization of all these algebraic equations $r(U, V)$, by u_1 say, thus yielding a two-parameter polynomial $\tilde{f}(u_1, t, X)$ for G.

Note that for this to work we have to assume that the starting polynomial $f(t, X)$ corresponds to a simple solution of the system of equations, since otherwise the Hensel method fails.

Hensel lifting as described above has already been used by Granboulan (1996) to find a polynomial with group M_{24}; see also Couveignes (1999).

3.3. Verification of the Galois groups

We verify the Galois group of the given polynomials by two standard techniques. First, lower bounds for the group are obtained by factoring (specializations of) the polynomial modulo various primes. By the Dedekind criterion this exhibits cycle types occurring in the Galois group. On the other hand, we prove upper bounds for the group by computing resolvent polynomials of suitable degrees which split off a nontrivial factor.

We also make use of the following consequence of the Hurwitz classification for algebraically closed fields of characteristic zero (see Malle and Matzat, 1999, Theorem III.6.4).

Lemma 3.1. *Let k be a field of characteristic zero and $f(t_1, \ldots, t_n)(X) \in k(t_1, \ldots, t_n)[X]$ absolutely irreducible. Assume that $k(t_1, \ldots, t_{n-1})$ is algebraically closed in the splitting field of f. Let $v_1, \ldots, v_{n-1} \in k$ such that the stem fields of $f(t_1, \ldots, t_n)(X)$ over $k(t_1, \ldots, t_n)$ and of $f(v_1, \ldots, v_{n-1}, t_n)(X)$ over $k(t_n)$ have the same number of ramification points with respect to t_n. Then the Galois groups of*

$$f(t_1, \ldots, t_n)(X) \qquad \textit{and} \qquad f(v_1, \ldots, v_{n-1}, t_n)(X)$$

coincide.

Indeed, under the assumption on the branch points, both extensions have the same branch cycle description.

4. The Group $\mathrm{L}_3(2)$

The group $G := \mathrm{GL}_3(2) = \mathrm{L}_3(2)$ is the second smallest non-Abelian simple group. It has a faithful permutation representation on the seven projective lines of the three-dimensional projective space over $\mathbb{F}_2$. LaMacchia (1980) gives a two-parameter family $f(a, t)(X)$ of polynomials over $\mathbb{Q}(a, t)$ with this Galois group. It can be verified that the ramification over $\mathbb{Q}(a)$ (that is, with respect to the parameter t) is $(2^2, 2^2, 2^2, 2^2, 3^2)$.

We give two three-parameter polynomials with group G, one of which has the LaMacchia family as a specialization:

Theorem 4.1. *The polynomial*

$$\begin{aligned} f_1(a, b, t, X) := {} & (X^4 + 2\,a\,X^3 + 2\,(a^2 + a\,b - 1)\,X^2 + 4\,b\,X + 2\,b^2) \\ & \cdot (X^3 - (a + b + 3)\,X^2 + 2\,(b + a + 1)\,X + b) + t\,X^3\,(X - 2) \end{aligned}$$

has Galois group $\mathrm{L}_3(2)$ *over* $\mathbb{Q}(a,b,t)$*. The branch cycle description with respect to* t *is of type* $(2^2,2^2,2^2,2^2,3^2)$*.*

Proof. The polynomial f_1 is irreducible, as can be seen by specializing $a=b=t=1$ and noting that the resulting polynomial is irreducible modulo 3. Upon replacing t by

$$\begin{aligned}&(Y^6-(3b+3c-4)Y^5+c(7b+4c-12)Y^4+2(b^3+4b^2-4b-2cb-2c^2b-c^3+4c^2)Y^3\\&\quad-bc(4b^2+cb+16b-16-4c)Y^2+b^2c^2(b+c+8)Y+b^3c^3)(Y+c)/(8Y^3(Y-c))\end{aligned}$$

(where $c:=2\,a+b+2$) the polynomial f_1 splits into two irreducible factors of degrees 3 and 4. Thus the Galois group of f_1 has a subgroup of index seven which has orbits of lengths 3 and 4 on the seven points. Its order must hence be divisible by 3, 4, and 7. On the other hand, it cannot be the alternating or the symmetric group, since these do not possess such a subgroup. The only remaining transitive subgroup of $\mathfrak{S}_7$ is $\mathrm{L}_3(2)$. □

Replacing a by $-2-3b/2$ in f_1 yields a field extension isomorphic to the one generated by the polynomial of LaMacchia.

Theorem 4.2. *The polynomial*

$$\begin{aligned}f_2(a,b,t,X):=&\,(X^4-2\,(b+2)\,X^2+4\,b\,X-a)\\&\cdot(X^3+2\,(b-1)\,X^2+(a+b^2-4\,b)\,X-2\,a)+t\,X^2\,(X-2)\end{aligned}$$

has Galois group $\mathrm{L}_3(2)$ *over* $\mathbb{Q}(a,b,t)$*. The branch cycle description with respect to* t *is of type* $(2^2,2^2,2^2,2^2,4.2)$*.*

Proof. First, the polynomial f_2 is irreducible, as can be seen by specializing $a=b=2$, $t=1$ and noting that the resulting polynomial is irreducible modulo 3. Upon replacing t by

$$\begin{aligned}&(Y+b)(Y^6-2(b-4)Y^5+(2a+b^2-20b+16)Y^4-4b(a-5b+12)Y^3\\&\quad+(a^2+(2b^2+4b+4)a-8b^3+32b^2)Y^2-2ba(a+2b+4)Y+b^2a^2)/(4Y^2(Y-b))\end{aligned}$$

the polynomial f_2 splits into two irreducible factors of degrees 3 and 4. We can now repeat the argument from the proof of Theorem 4.1 to conclude that $\mathrm{Gal}(f)=\mathrm{L}_3(2)$. □

We end this section by giving a four-parameter polynomial with group $\mathrm{L}_3(2)$:

Theorem 4.3. *The polynomial*

$$\begin{aligned}f_3(a,b,c,t,X):=&\,X^7-((c-2)a+2b+c)X^6+(-(b-4)(c-1)a^2+((c-2)b^2\\&+(2c^2-5c+4)b-2c^2)a+b(2bc+2c^2+b^2))X^4\\&+((2c^2-1)(b-4)a^2+((-2c^2+c+2)b^2+(5c^2+2c-4)b-4c^2)a\\&-(c+1)b^3-c(2c+3)b^2+c^2b)X^3+((c^2+3c-1)(4-b)\cdot a^2\\&+((3c-2)b^2-2(c^2+4c-2)b+4c^2)a+b(b^2+3bc-c^2))cX^2\\&+(2abc-8ac+ab-4a-b^2+2bc)ac^2X-a^2(b-4)c^3\\&+t\,X^2(X-c)(X^2-bX+b)\end{aligned}$$

has Galois group $\mathrm{L}_3(2)$ *over* $\mathbb{Q}(a,b,c,t)$*. The branch cycle description with respect to* t *is of type* $(2^2,2^2,2^2,2^2,2^2,2^2)$*.*

The proof is as in the previous cases by exhibiting a factorization. In fact, it is sufficient to do this for some specialization of a, b, c which does not change the ramification with respect to t.

For an application of these polynomials see Section 12.

5. The Group $\mathbf{PGL_2(7)}$

THEOREM 5.1. *The polynomial*

$$\begin{aligned} f(a,t,X) :=& X(X^7 + X^6 + 14aX^5 + 7aX^4 + 49a^2X^3 + 14a^2X^2 + 49a^3X + 7a^3) \\ &+ t\,(7X^2 + X + 1) \end{aligned}$$

has Galois group $\mathrm{PGL}_2(7)$ *over* $\mathbb{Q}(a,t)$. *The branch cycle description with respect to* t *is of type* $(2^3, 2^3, 2^3, 6)$.

PROOF. By looking at the factorization of specializations modulo various primes one proves that the Galois group is twofold transitive. Moreover the discriminant is not a square. Thus either $\mathrm{Gal}(f) = \mathrm{PGL}_2(7)$ or $\mathrm{Gal}(f) = \mathfrak{S}_8$. The ramification with respect to t can be read off from the discriminant.

Let us consider the Hurwitz space of extensions of degree 8 with ramification of type $(2^3, 2^3, 2^3, 6)$. Since the number of ramification points is four, the Hurwitz space is one-dimensional. The braid orbit criteria give that this space has two absolutely irreducible components, one for $\mathrm{PGL}_2(7)$ of genus 0, one for $\mathfrak{S}_8$ of genus 31. Since the polynomial $f(a,t,X)$ corresponds to an irreducible component of genus 0, its geometric Galois group has to be $\mathrm{PGL}_2(7)$. Finally, $\mathrm{PGL}_2(7)$ is self-normalizing in $\mathfrak{S}_8$, so it is also equal to the arithmetic Galois group. □

REMARK. The polynomial f in Theorem 5.1 has totally real specializations: for example, if $a = -2$ and $-1 \le t \le 6$. One example of a totally real $\mathrm{PGL}_2(7)$ polynomial is given by

$$X^8 - 2\,X^7 - 35\,X^6 + 308\,X^4 + 308\,X^3 - 462\,X^2 - 556\,X + 6.$$

The field extension with group $\mathrm{L}_3(2)$ constructed by LaMacchia (1980) is embeddable into a $\mathrm{PGL}_2(7)$ field. Since $\mathrm{PGL}_2(7)$ does not have a faithful permutation representation of degree 7, a stem field of that Galois extension will have degree 8. A generating polynomial is given by the following theorem.

THEOREM 5.2. *The polynomial*

$$\begin{aligned} f(a,t,X) :=& \left(X^2 - 4\,(16\,a - 3)\,b\right)\left(X^3 + 4\,b\,X^2 - 2\,X\,(16\,a - 3)b - 4\,(16\,a - 3)\,b^2\right)^2 \\ &- t(2X^5 + (8\,a^2 - 24\,a - 31)X^4 - 4(40\,a + 17)bX^3 - 4(16\,a - 3) \\ &(6\,a^2 - 20\,a - 29)bX^2 + 32\,(88\,a^6 - 497\,a^5 - 302\,a^4 + 114\,a^3 \\ &+ 854\,a^2 - 9\,a - 18)\,X + 16\,(64\,a^8 - 2672\,a^7 + 2906\,a^6 + 550\,a^5 \\ &+ 3466\,a^4 - 118\,a^3 - 2731\,a^2 + 366\,a - 90)) + t^2\,(X^2 - 4\,(2\,a - 1)X \\ &+ 4\,(31\,a^2 - 4\,a + 1)) \end{aligned}$$

(where $b := a^2 - 2\,a - 1$*) has Galois group* $\mathrm{PGL}_2(7)$ *over* $\mathbb{Q}(a,t)$. *The branch cycle description with respect to* t *is of type* $(2^4, 2^4, 2^3, 6)$.

The polynomial $f(a,t^2,X)$ has Galois group $\mathrm{L}_2(7)$ over $\mathbb{Q}(a,t)$, with branch cycle description of type $(2^4,2^4,2^4,2^4,3^2)$ with respect to t.

Proof. The ramification with respect to t can be determined from the discriminant of f with respect to X. It turns out that this discriminant is of the form $t\,h(a,t)^2$ with a polynomial $h(a,t)\in\mathbb{Q}(a,t)$. Since in their degree 8 permutation representations $\mathrm{L}_2(7)$ consists of the even elements of $\mathrm{PGL}_2(7)$ the second assertion follows from the first.

As in the previous proof one checks that $\mathrm{Gal}(f)$ is (at least) twofold transitive, hence one of $\mathrm{PGL}_2(7)$ or $\mathfrak{S}_8$. But $\mathfrak{S}_8$ does not have generating systems of type $(2^4,2^4,2^3,6)$ (while $\mathrm{PGL}_2(7)$ has 12 such systems, and the corresponding Hurwitz curve has genus 0). □

Author: $2^3.\mathrm{L}_3(2)$ centered baseline dot correct as set?

6. The Group $2^3.\mathrm{L}_3(2)$

The affine group $\mathrm{AGL}(3,2)\cong 2^3.\mathrm{L}_3(2)$ has a primitive permutation representation on the points of the three-dimensional vector space over $\mathbb{F}_2$. A one-parameter polynomial for this group was first obtained by Malle (1987).

If we extract a square root from a sufficiently general element in a stem field of the four-parameter polynomial for $\mathrm{L}_3(2)$ in Theorem 4.3, this will generate a field extension of degree 14 over $\mathbb{Q}(a,b,c,t)$ with Galois closure the wreath product $2^7.\mathrm{L}_3(2)$. This has $2^3.\mathrm{L}_3(2)$ as a factor group. Thus there is a computational way to obtain a $2^3.\mathrm{L}_3(2)$-polynomial with at least four parameters. This will be quite complicated, though. Here, we content ourselves with presenting a reasonably short two-parameter polynomial.

Theorem 6.1. *The polynomial*

$$f(a,t,X):=X^4\,(X^2+a\,X+2\,a)\,(X-2)^2+t\,((a-5)\,(X^2+X)-2\,a-2)\,(X-1)^2$$

has Galois group $2^3.\mathrm{L}_3(2)$ over $\mathbb{Q}(a,t)$. The branch cycle description with respect to t is of type $(2^2,2^2,2^2,4.2,4.2)$ and with respect to a of type $(2^2,2^2,2^2,2^2,2^2,2^2,2^2)$.

Proof. The ramification can be determined from the discriminant of f. Furthermore, $\mathrm{Gal}(f)$ is at least twofold transitive, as follows by factoring a few specializations modulo several small primes. Since the discriminant is a square, and $\mathrm{L}_2(7)$ does not contain elements of cycle shape 2^2 in its degree 8 representation, $\mathrm{Gal}(f)$ is either $2^3.\mathrm{L}_3(2)$ or the alternating group $\mathfrak{A}_8$. The specialized polynomial $f(1,t,X)$ has the same ramification type with respect to t, thus its Galois group over $\mathbb{Q}(t)$ equals that of $f(a,t)$ over $\mathbb{Q}(a,t)$ by Lemma 3.1.

Now consider the irreducible polynomial

$$\begin{aligned}h(t,Y):=\,&Y\,(Y-1)\,(Y+1)^2\,(Y-2)^2\,(Y^2-Y+2)^4-4\,(2\,Y^{12}-12\,Y^{11}+38\,Y^{10}\\&-80\,Y^9+112\,Y^8-100\,Y^7+62\,Y^6-40\,Y^5+83\,Y^4-122\,Y^3\\&+67\,Y^2-10\,Y+1)t+16\,Y\,(Y-1)\,(Y^2-Y+1)^4\,t^2\end{aligned}$$

of degree 14 in Y. Write $f(1,t,X)=f_1(X)-t\,f_2(X)$. Then $h(f_1(X)/f_2(X),Y)$ splits into two factors of degree 7. Thus the Galois groups of $h(t,Y)$ and of $f(1,t,X)$ over $\mathbb{Q}(t)$ have a nontrivial common factor group. Since $\mathfrak{A}_8$ does not have a transitive degree 14 permutation representation, this only leaves the possibility $2^3.\mathrm{L}_3(2)$. □

The proof incidently shows that the polynomial $h(t, Y)$ also has group $2^3.\mathrm{L}_3(2)$ and generates the same splitting field as $f(1, t, X)$.

Let K be a number field whose discriminant is the square of a square-free odd integer and which is primitive over $\mathbb{Q}$. Kondo (1997) has shown that the Galois group of the Galois closure of $K/\mathbb{Q}$ is either the alternating group or one of D_5, $\mathrm{L}_2(5)$, $\mathrm{L}_3(2)$ or $2^3.\mathrm{L}_3(2)$. He gives examples for the occurrence of the second and third case, but states that he is not aware of an example with group $2^3.\mathrm{L}_3(2)$.

We take the opportunity to present a $2^3.\mathrm{L}_3(2)$-polynomial whose discriminant is the square of an odd prime: a stem field of

$$X^8 - 4\,X^7 + 8\,X^6 - 11\,X^5 + 12\,X^4 - 10\,X^3 + 6\,X^2 - 3\,X + 2$$

has discriminant 5717^2. Similar extensions with group D_5 have long been known; for example

$$X^5 - 2\,X^4 + 2\,X^3 - X^2 + 1$$

has Galois group D_5 and a stem field has discriminant 47^2.

7. The Group $3^2.\,\mathrm{GL}_2(3)$

The affine group $\mathrm{AGL}(2,3) \cong 3^2.\,\mathrm{GL}_2(3)$ has a primitive permutation representation on the points of the two-dimensional vector space over $\mathbb{F}_3$. We present two geometric two-parameter polynomials for this group.

Theorem 7.1. *The polynomial*

$$\begin{aligned} f(a,t,X) :=& (X^2 + (a-3)X - a)^3 (X^3 + (3a-12)X^2 + (3a^2 - 18a + 36)X - a^3) \\ &+ tX^2(X-3) \end{aligned}$$

has Galois group $3^2.\,\mathrm{GL}_2(3)$ *over* $\mathbb{Q}(a,t)$. *The branch cycle description with respect to* t *is of type* $(2^3, 2^3, 3^2, 6.2)$.

Proof. The Galois group $G = \mathrm{Gal}(f)$ is transitive since f is irreducible. The discriminant of $f(a+1, t, X)$ with respect to x equals

$$\begin{aligned} -2^8\,3^9\,t^4\,(a+1)^6\,(&a^{12} + 30\,a^{10} + 321\,a^8 + 1312\,a^6 + 384\,a^4 - 6144\,a^2 + 4096 \\ &-2\,t\,a^6 + 78\,t\,a^4 - 96\,t\,a^2 + 128\,t + t^2)^3. \end{aligned}$$

The statement about the ramification with respect to t can be deduced from this. In particular, the Galois group contains elements of cycle shapes 2^3, 3^2, 4^2. This leaves only the possibilities $3^2.\,\mathrm{GL}_2(3)$ or $\mathfrak{S}_9$ for G.

The polynomial $f(a, u, X)$ with

$$u := \frac{(y^3 + 6\,y^2 + 6\,a\,y - 2\,a^2\,(a-3))^3\,(y^2 - (a-9)\,y - 2\,a^2)\,(y + a - 3)}{27\,y^3\,(y+a)^2\,(y - 2\,a + 6)}$$

splits into factors of degrees 3 and 6, thus G has a subgroup of index dividing 12 which acts intransitively on the nine points. This rules out the symmetric group $\mathfrak{S}_9$, proving the assertion. □

By forcing the discriminant to become a square, we may descend to the normal subgroup $3^2.\mathrm{SL}_2(3)$ of index 2:

Corollary 7.2. *The polynomial* $f(b+1,t,X)$, *with* $b = 2\,(3\,v^2-3\,u^2+1)/(3\,v^2+3\,u^2+1)$, $t = 6\,(b-2)^2\,(b+2)\,b^2/u+b^6-39\,b^4+48\,b^2-64$, *has Galois group* $3^2.\mathrm{SL}_2(3)$ *over* $\mathbb{Q}(u,v)$.

There exists a second class vector of length 4 for $3^2.\,\mathrm{GL}_2(3)$ with rational Hurwitz curve:

Theorem 7.3. *The polynomial*

$$f(a,t,X) := (X^2+2bX+a(a+2)b)^3(X^3-ab(3a^2+5a+1)X^2-a^2b(10a^3+18a^2 \\ +12a+5)X-3a^3(a^2+a+1)b^2)-t(X^2-a^2b)^4$$

(where $b := 3a^2+2a+1$*) has Galois group* $3^2.\,\mathrm{GL}_2(3)$ *over* $\mathbb{Q}(a,t)$. *The branch cycle description with respect to* t *is of type* $(2^3,2^3,3^2,4^2)$.

Proof. We proceed as in the case of $\mathrm{PGL}_2(7)$. First, the Galois group is twofold transitive and odd. The ramification with respect to t follows by computing the discriminant. The Hurwitz curve of degree 9 extensions with ramification $(2^3,2^3,3^2,4^2)$ turns out to have two components, one of genus 0 corresponding to $3^2.\,\mathrm{GL}_2(3)$ extensions, and another one of genus 128. Thus our polynomial has geometric (and arithmetic) Galois group $3^2.\,\mathrm{GL}_2(3)$. □

8. The Group $\mathrm{Aut}(\mathfrak{S}_6)$ and Some Normal Subgroups

The automorphism group of the symmetric group $\mathfrak{S}_6$ has a twofold transitive permutation representation on ten points. A polynomial with one parameter for this group and its four nontrivial normal subgroups was given by Matzat (1984). Here we exhibit two-parameter polynomials for $\mathrm{Aut}(\mathfrak{S}_6)$ and two of its nontrivial normal subgroups.

Theorem 8.1. *The polynomial*

$$f(a,t,X) := \left((X+8)\,(X-1)^4+4\,(X+2)\,(X-1)^2\,a+2\,X\,a^2\right)^2+t\,(X^2+8)$$

has Galois group $\mathrm{Aut}(\mathfrak{S}_6)$ *over* $\mathbb{Q}(a,t)$. *The branch cycle description with respect to* t *is of type* $(2^3,2^3,2^5,8)$.

Proof. The Galois group $G = \mathrm{Gal}(f)$ is transitive since f is irreducible. Write f as $f = g(a,X)+t\,(X^2+8)$. Then the one-point stabilizer of G is the Galois group of $f(a,u,X)$ with $u = -g(a,Y)/(Y^2+8)$. Since $f(a,u,X)$ has an irreducible factor of degree 9, G is at least twofold transitive. Moreover, the discriminant of f is not a square. This leaves only the groups $\mathrm{PGL}_2(9)$, $\mathfrak{S}_6$, $\mathrm{Aut}(\mathfrak{S}_6)$ and $\mathfrak{S}_{10}$ as candidates for G. The statement about the ramification with respect to t can be deduced from the discriminant of f with respect to x. Since $\mathfrak{S}_6$ does not contain elements of order 8 and $\mathrm{PGL}_2(9)$ does not contain involutions of cycle type 2^3, the ramification now rules out these two groups.

It follows from Lemma 3.1 that the Galois group of f is preserved under any specialization of a which does not change the ramification with respect to t. This is satisfied for example for $a = 1$, so we may now restrict ourselves to considering $f(1,t,X)$. It can be checked that the resultant of $f(1,-t^2,X)$ and

$$(Y^5-2Y^4-84Y^3+8Y^2+1116Y-1624)(Y^{10}-4Y^9-64Y^8+336Y^7+1100Y^6 \\ -9104Y^5+6256Y^4+52224Y^3-78848Y^2-83968Y+161792)$$

$$-8(Y-2)(Y^{10}-4Y^9-88Y^8+384Y^7+684Y^6-4432Y^5-1776Y^4$$
$$+29184Y^3-38272Y^2+10752Y-512)t+16Y^4(Y-2)^3t^2$$

with respect to t splits into factors of degrees 8 and 12 in X. This shows that G has a subgroup of index dividing $2\cdot 15$ which has orbits of lengths 4 and 6 on the ten points. The symmetric group $\mathfrak{S}_{10}$ does not have such a subgroup, so we conclude that $G = \mathrm{Aut}(\mathfrak{S}_6)$. □

The polynomial $f(a, -t^2, X)$ encountered in the above proof can easily be seen to have Galois group $\mathfrak{S}_6$ (in its permutation representation on ten points). We can also descend to one of the other two normal subgroups of index 2:

Corollary 8.2. *The polynomial $f(a,t,X)$, with $a = w^2 - 2\,v^2 - v + 10$,*

$$t = 2\,(8\,a-81)\,(2\,a-27)^2\,v - 4\,a^4 + 360\,a^3 - 8856\,a^2 + 86022\,a - 295245,$$

has Galois group $\mathrm{PGL}_2(9)$ *over* $\mathbb{Q}(u,v)$.

Remark. The polynomial f in Theorem 8.1 has totally real specializations; for example, if $a = -2$ all specializations with $-8 \le t < 0$ will do. One example of a totally real $\mathrm{Aut}(\mathfrak{S}_6)$ polynomial is given by

$$X^{10}-2X^9-103X^8+496X^7+1996X^6-20104X^5+54884X^4-60064X^3$$
$$+17620X^2+6264X-2268.$$

The polynomial

$$X^{10}-2X^9-535X^8+2224X^7+83644X^6-481480X^5-2892220X^4$$
$$+15578336X^3+25004806X^2-90370476X-6352506$$

generates a totally real $\mathrm{PGL}_2(9)$ extension of $\mathbb{Q}$.

The third normal subgroup of $\mathrm{Aut}(\mathfrak{S}_6)$ of index 2 is the point stabilizer M_{10} of the Mathieu group M_{11} in its natural permutation representation. Although $f(a,t,X)$ does not have a two-parameter specialization with group M_{10}, it nevertheless admits some specializations with this group. An example of a totally real one is

$$X^{10}-2\,X^9-129\,X^8-60\,X^7+5397\,X^6+15186\,X^5-50757\,X^4$$
$$-316260\,X^3-605514\,X^2-517760\,X-168650.$$

The two remaining nontrivial normal subgroups of $\mathrm{Aut}(\mathfrak{S}_6)$ are $\mathfrak{S}_6$ and the alternating group $\mathfrak{A}_6$. Totally real extensions for these can easily be constructed via their permutation representations on six points.

9. The Group $\mathrm{L}_2(11)$

It was first shown by Galois that the minimal degree of a faithful permutation representation of $\mathrm{L}_2(p)$ is at least $p+1$ except for the cases $p = 5, 7, 11$. We have already considered the degree 7 representation of $\mathrm{L}_2(7)$. Here we look at the largest case $p = 11$. The group $\mathrm{L}_2(11)$ has two non-conjugate subgroups $\mathfrak{A}_5$ which give rise to the primitive permutation representations of degree 11. In the representation on the cosets of one of these, the other has orbits of lengths 5 and 6. As we did similarly for $\mathrm{L}_2(7)$ we will

use this fact to identify $\mathrm{L}_2(11)$ as the Galois group of a two-parameter polynomial. The first (one-parameter) polynomial for $\mathrm{L}_2(11)$ over $\mathbb{Q}$ was computed by Malle and Matzat (1985). Earlier, LaMacchia (1981) found such a polynomial over $\mathbb{Q}(\sqrt{5})$.

THEOREM 9.1. *The polynomial*

$$\begin{aligned} f(a,t,X) := {} & (X^5 + 2\,(a-4)\,X^4 - 4\,(a-5)\,X^3 - 2\,(a^2 - 3\,a + 8)\,X^2 \\ & +(2\,a-1)^2\,X - 2\,a^2) \cdot (X^6 + 2\,(-3+5\,a)\,X^5 + (32\,a^2 - 24\,a + 11)\,X^4 \\ & +2\,(16\,a^3 + 15\,a^2 + 9\,a - 4)\,X^3 + 2\,(2\,a+1)\,(20\,a^2 - 4\,a + 1) \\ & X^2 - 16\,a^2\,(2\,a^2 + 7\,a + 2)\,X + 32\,a^4) + t\,X^3\,(X-1)^2 \end{aligned}$$

has Galois group $\mathrm{L}_2(11)$ *over* $\mathbb{Q}(a,t)$. *The branch cycle description with respect to* t *is of type* $(2^4, 2^4, 2^4, 6.3.2)$.

PROOF. The polynomial f is irreducible, as can be seen by specializing $a = 2$, $t = 1$ and noting that the resulting polynomial is irreducible modulo 5. Upon replacing t by

$$\begin{aligned} & (Y-3)(64a^6Y^{10} - 64(11a-9)a^5Y^9 + 16(184a^2 - 252a + 117)a^4Y^8 - 32(188a^3 \\ & -315a^2 + 180a - 81)a^3Y^7 + 8(808a^4 - 1548a^3 + 684a^2 + 81a + 162)a^2Y^6 \\ & -8(440a^4 - 828a^3 - 36a^2 - 567a - 324)a^2Y^5 + 6(128a^6 + 48a^5 - 210a^4 \\ & -3438a^3 - 1566a^2 + 54a - 9)Y^4 - 18(64a^5 - 50a^4 - 726a^3 - 252a^2 + 63a + 3)Y^3 \\ & +27(16a^4 - 8a^3 + 60a^2 + 48a + 19)Y^2 - 162(4a^2 + 3a + 4)Y \\ & +243)/(27Y^3(Y-1)^2) \end{aligned}$$

the polynomial f splits into two irreducible factors of degrees 5 and 6. Thus the Galois group of f has a subgroup of index 11 which has orbits of lengths 5 and 6 on the 11 points. Its order must hence be divisible by 5, 6, and 11. On the other hand, it cannot be the alternating group, the symmetric group or the Mathieu group M_{11}, since these do not possess such a subgroup. The only remaining transitive subgroup of $\mathfrak{S}_{11}$ is $\mathrm{L}_2(11)$. □

REMARK. The polynomial f in Theorem 9.1 has totally real specializations: for example, if $a = -5$ all specializations with $-716550 \le t \le -715599$ will do. One example of a totally real $\mathrm{L}_2(11)$ polynomial is given by

$$\begin{aligned} & X^{11} - 4X^{10} - 25X^9 + 81X^8 + 237X^7 - 562X^6 - 1010X^5 + 1574X^4 + 1805X^3 \\ & -1586X^2 - 847X + 579. \end{aligned}$$

10. The Mathieu Groups M_{11} and M_{12}

The Mathieu groups M_{11} and M_{12} possess sharply fourfold respectively fivefold transitive permutation representations on 11 respectively 12 points. The first regular extensions over $\mathbb{Q}(t)$ with these Galois groups were computed by Matzat and Zeh-Marschke (1986). We construct a two-parameter polynomial of degree 12 for M_{12} admitting totally real specializations, and such that the fixed field of M_{11} has genus 0 (with respect to one of the parameters).

THEOREM 10.1. *The polynomial* $f(a,t,X) := p^2 - t\,X^2\,q \in \mathbb{Q}(a,t)[X]$ *where*

$$\begin{aligned} :=\ & pX^6 + 288a^2(a+2)X^5 - 36(a^8 + 8a^7 - 792a^6 - 3136a^5 - 3320a^4 + 288a^3 + 864a^2 \\ & +384a - 48)X^4 + 288(a+2)(3a^{11} + 19a^{10} - 14a^9 + 3930a^8 + 14584a^7 + 18184a^6 \\ & -5424a^5 - 15056a^4 - 4880a^3 + 1968a^2 - 96a - 96)X^3 - 54(19a^{16} - 960a^{15} \\ & -16048a^{14} - 79968a^{13} - 416496a^{12} - 1894272a^{11} - 5779776a^{10} - 9006720a^9 \\ & -2619360a^8 + 8744960a^7 + 5260032a^6 - 5167616a^5 - 5662464a^4 - 1431552a^3 \\ & +95232a^2 + 92160a - 48384)X^2 + 864(a+2)(7a^2 + 4a - 2)(a^{13} + 35a^{12} + 396a^{11} \\ & +2200a^{10} + 5996a^9 + 4188a^8 - 16352a^7 + 17408a^6 + 121200a^5 + 117264a^4 \\ & -10560a^3 - 49536a^2 - 15552a - 1728)(a^2+2)^2X + 5832(7a^2 + 4a - 2)(a^2 \\ & +4a - 14)^2(a^2 + 4a + 2)^3(a^2+2)^6, := q3X^2 - 32X(a-1)(2a+1)(2a^2 + 8a - 1) \\ & +216(2a^2+1)^4, \end{aligned}$$

has Galois group M_{12} *over* $\mathbb{Q}(a,t)$. *The branch cycle description with respect to* t *is of type* $(2^4, 2^4, 2^6, 8.2)$.

PROOF. The polynomial f is irreducible and has square discriminant. Moreover, $\mathrm{Gal}(f)$ is at least fourfold transitive, as can be seen by computing the factorization modulo various primes of some specializations. Thus $\mathrm{Gal}(f)$ is either M_{12} or $\mathfrak{A}_{12}$. But it can be checked that the alternating group $\mathfrak{A}_{12}$ does not have a Hurwitz curve of genus 0 for the branch cycle description $(2^4, 2^4, 2^6, 8.2)$. □

The polynomial was found as follows: first a polynomial $g(t,X) \in \mathbb{F}_{13}(t)[X]$ with the correct branch cycle description and the right Galois group was found by exhaustive search. Note that for this one may assume that g is of the form

$$g(t,X) = p_1(X)^2 - tX^2(X^2 + 2X + a_0)$$

for a suitable polynomial p_1 of degree 6 and some $a_0 \in \mathbb{F}_{13}$. For any choice $\tilde{a}_0 \equiv a_0 \pmod{13}$ of a preimage of a_0 in $\mathbb{Q}$ the Hensel method gives arbitrarily precise approximations to a polynomial $\tilde{g}(t,X) \in \mathbb{Q}_{13}(t)[X]$ over the 13-adic integers. Applying this to several choices for $\tilde{a}_0$ gives sets of (approximate) values for all coefficients of the desired polynomial over $\mathbb{Q}_{13}(t)$. The algebraic relations between these coefficients can now be deduced by interpolation, by solving a linear system of equations. These relations already hold over $\mathbb{Q}$, thus we finally obtain a polynomial $f(a,t,X) \in \mathbb{Q}(a,t)[X]$ with the right branch cycle description and whose reduction modulo 13 for a suitable specialization of a equals $g(t,X)$.

Since the stem field of the M_{12} extension in Theorem 10.1 is a rational function field (with respect to the field of constants $\mathbb{Q}(a)$), and the one-point stabilizer in M_{12} equals M_{11}, we also obtain a two-parameter family of M_{11} extensions:

COROLLARY 10.2. *Let* $f(a,t,X) = p(a,X)^2 - tX^2q(a,X)$ *as in Theorem* 10.1. *Then the polynomial*

$$g(a,t,X) := \frac{p(a,X)^2t^2q(a,t) - p(a,t)^2X^2q(a,X)}{X-t} \in \mathbb{Q}(a,t)[X]$$

has Galois group M_{11} *over* $\mathbb{Q}(a,t)$.

Both the M_{12} and the M_{11} polynomial allow for totally real specializations. For example

$$\begin{aligned}X^{12} - 968X^{10} + 346060X^8 - 56221440X^6 + 4128059232X^4 - 247374336X^3\\ -114286943232X^2 + 19295198208X + 632319724608\end{aligned}$$

is a totally real M_{12} polynomial, while

$$\begin{aligned}X^{11} - 4X^{10} - 5541X^9 - 17700X^8 + 8989656X^7 + 88565592X^6\\ -3982035456X^5 - 53992425120X^4 + 177164975493X^3 + 3011149862548X^2\\ -789230330881X - 3422014984884\end{aligned}$$

defines a totally real M_{11} polynomial.

11. The Group $\mathrm{L}_3(3)$

The simple group $\mathrm{L}_3(3)$ has a primitive permutation representation on the 13 cosets of the normalizer of its Borel subgroup. A regular extension of $\mathbb{Q}(t)$ with this group, ramified in three points, was first explicitly constructed in Malle (1987).

We construct a two-parameter polynomial for $G = \mathrm{L}_3(3)$ as follows. The group G has a semi-rational rigid class vector $(3^3, 4^2 2^2, 8.4)$ (where we identify the conjugacy classes by the cycle shapes of their elements in the degree 13 permutation representation). The corresponding stem field has genus 0 and thus a generating polynomial over $\mathbb{Q}(\sqrt{-2})(t)$, ramified in $1, \infty, 0$ can be computed with the standard methods (as in Malle, 1987, for example). Galois translation with the degree 2 extension $\mathbb{Q}(\sqrt{t})/\mathbb{Q}(t)$ produces an extension with ramification type $(3^3, 3^3, 2^4, 4^2 2^2)$. This corresponds to a regular point on the genus 0 Hurwitz curve for extensions with this branch cycle description. The latter can be constructed from this known point by the Hensel method described in Section 3.2 above. We obtain the following theorem.

Theorem 11.1. *The polynomial* $f(a,t,X) := x\,p_1^2\,p_2 - t\,q_1^4\,q_2^2$ *where*

$$\begin{aligned}&:= p_1x^4 + 3(a+1)bx^3 + 6a(a^2+11)bx^2 + 4(10a^2 - 5a + 9)b^2x + 72a(a^2 - 2a + 3)b^2,\\ &:= p_2 4x^4a^2 + (a+3)(3a^2 + 2a - 9)bx^3 + 12a(a^2 - 3)b^2x^2\\ &\quad +4a^2(3a^3 - 5a^2 + 13a - 27)b^2x + 32a^3(a-2)(a^2 - 2a + 3)b^2,\\ &:= q_1x^2 + 2bx + 4ab,\\ &:= q_2x^2 + (a-1)bx + 4a(a-2)b,\end{aligned}$$

with $b := a^2 - 2a + 9$ *has Galois group* $\mathrm{L}_3(3)$ *over* $\mathbb{Q}(a,t)$. *The branch cycle description with respect to* t *is of type* $(2^4, 3^3, 3^3, 4^2 2^2)$.

Proof. The polynomial f is irreducible and has square discriminant. Under the specialization $a \mapsto 1$ the ramification behaviour with respect to t does not change, hence by Lemma 3.1 the Galois groups $\mathrm{Gal}(f(a,t,X))$ and $\mathrm{Gal}(f(1,t,X))$ coincide. From factorizations modulo various primes it follows easily that $\mathrm{Gal}(f(1,t,X))$ is twofold transitive, hence contains $\mathrm{L}_3(3)$. In order to obtain an upper bound on the Galois group, we use the fact that $G = \mathrm{L}_3(3)$ has two classes of subgroups of index 13 (interchanged by the graph automorphism of G), and the second class has orbits of lengths 9 and 4 on the cosets of the first.

Write $f(1,t,X) = g(X) - th(X)$, and set $p(Y) := -g(Y)/h(Y)$. Then

$$f(1,p(Y),X) = g(X) + \frac{g(Y)}{h(Y)}h(X)$$

splits into two factors of degrees 9 and 4. This shows that $\mathrm{Gal}(f(1,t,X))$ is a subgroup of $\mathrm{L}_3(3)$, hence equal to that group. □

The degree 9 factor occurring in the factorization of $f(1,p(Y),X)$ above can be seen to have group $3^2.\,\mathrm{GL}_2(3)$. But its genus with respect to X and Y equals 24, and it is more complicated than the polynomials constructed in Section 7.

It can be checked that the polynomial in Theorem 11.1 does not allow for totally real specializations.

12. Applications

The polynomials computed in this paper can be used so show the solvability of certain embedding problems and hence to realize further groups as Galois groups over $\mathbb{Q}$.

The Schur multiplier of the simple group $\mathrm{L}_2(11)$ has order 2, and the corresponding non-split central extension is

$$1 \longrightarrow Z_2 \longrightarrow \mathrm{SL}_2(11) \longrightarrow \mathrm{L}_2(11) \longrightarrow 1\,.$$

The only involution in $\mathrm{SL}_2(11)$ is the central one, so all involutions of $\mathrm{L}_2(11)$ lift to elements of order 4 in $\mathrm{SL}_2(11)$. Thus an $\mathrm{L}_2(11)$ extension $N/\mathbb{Q}$ embeddable into an $\mathrm{SL}_2(11)$ extension necessarily has to be totally real. It has recently been shown by Klüners (2000) that Serre's criterion (see, for example, Malle and Matzat, 1999, IV.6.3) applies to one of the totally real specializations of the polynomial $f(a,t,X)$ in Theorem 9.1.

The group $\mathrm{PGL}_2(7)$ has two non-isomorphic non-split central extensions of degree 2. One of these was the smallest finite group not known to occur as Galois group over $\mathbb{Q}$ (Porat, 1994). As pointed out by Jack Sonn, a criterion of his implies that the corresponding embedding problem for $\mathrm{PGL}_2(7)$ can be solved for any totally real $\mathrm{PGL}_2(7)$ extension in which only one prime is ramified. The polynomials constructed in Section 5 have such specializations, for example

$$X^8 - X^7 - 29\,X^6 + 111\,X^5 - 139\,X^4 + 37\,X^3 + 32\,X^2 - 10\,X - 1$$

with discriminant 107509^3, so they lead to realizations of this covering group.

We finally use the $\mathrm{L}_3(2)$ polynomials from Section 4 to study the moduli spaces of Riemann surfaces of genus 3 and 4. Let M be a Riemann surface and $\phi : M \to \hat{\mathbb{C}}$ a meromorphic function. Then the monodromy group G of ϕ is by definition the Galois group of the Galois closure of the corresponding extension of fields of meromorphic functions. We then also say that M *admits* G *as a monodromy group.*

The polynomial $f_2(a,b,t,x)$ in Theorem 4.2 defines a regular extension K of $\mathbb{Q}(a,b,t)$ of degree 7 with Galois closure $\mathrm{L}_3(2)$. Consider K as a function field in one variable with field of constants $\mathbb{Q}(b,t)$. With respect to a the ramification is of type $(9 \cdot 2^2)$, hence K has genus 3. Since $K/\mathbb{Q}(x,b,t)$ has degree 2, K is hyperelliptic, and $\mathbb{Q}(x,b,t)$ is its only rational subfield. Thus its isomorphism type is determined by the set of eight ramification points in $K/\mathbb{Q}(x,b,t)$. Calculation shows that varying b,t gives a two-dimensional family of genus 3 extensions.

Similarly, the polynomial $f_3(a,b,c,t,x)$ in Theorem 4.3 defines a regular extension

K' of $\mathbb{Q}(a,b,c,t)$ with Galois closure $\mathrm{L}_3(2)$. Again considered as a function field in one variable over $\mathbb{Q}(b,c,t)$, K' has genus 4 and $K'/\mathbb{Q}(x,b,c,t)$ has degree 2. Thus K is hyperelliptic with unique rational subfield $\mathbb{Q}(x,b,c,t)$. We may now argue as above to obtain:

THEOREM 12.1. *(a) There exists a two-dimensional family of Riemann surfaces of genus* 3 *with monodromy group* $\mathrm{L}_3(2)$.
(b) There exists a three-dimensional family of Riemann surfaces of genus 4 *with monodromy group* $\mathrm{L}_3(2)$.

These seem to be the first results asserting a dimension at least two for a proper subgroup of S_n. The moduli space of Riemann surfaces of genus 3 respectively 4 is of dimension six respectively nine.

The polynomial $f_2(a,b,-16b^2-8b-1,x)$ defines a genus 1 extension (with respect to a) of $\mathbb{Q}(a,b)$, with j-invariant

$$-\frac{(16b^2-216b+9)^3}{b(4b+9)^2(4b+1)^2}\,.$$

Clearly, for b varying in $\mathbb{C}$ this j-invariant takes on all complex values, hence we deduce:

THEOREM 12.2. *Let M be a Riemann surface of genus* 1. *Then it admits* $\mathrm{L}_3(2)$ *as monodromy group.*

That is, for any M of genus 1 there exists a covering $\phi : M \to \hat{\mathbb{C}}$ such that the Galois closure of the corresponding extension of fields of meromorphic functions has group $\mathrm{L}_3(2)$.

Acknowledgement

I would like to thank Peter Müller for very useful conversations on the topic of this paper.

References

Couveignes, J. M. (1999). Tools for the computation of families of coverings. In *Aspects of Galois Theory*. Cambridge, Cambridge University Press.
Granboulan, L. (1996). Construction d'une extension régulière de $\mathbb{Q}(t)$ de groupe de Galois M_{24}. *Exp. Math.*, **5**, 3–14.
Klüners, J. (2000). A polynomial with $\mathrm{SL}_2(11)$ as Galois group. *J. Symb. Comput.* (This issue) *Editor: please update*
Kondo, T. (1997). Some examples of unramified extensions over quadratic fields. In *Proceedings of the 14th Algebraic Combinatorics Symposium*, International Christian University, Tokyo.
LaMacchia, S. (1980). Polynomials with Galois group $\mathrm{PSL}(2,7)$. *Commun. in Algebra*, **8**, 983–992.
LaMacchia, S. (1981). Polynomials with Galois group $\mathrm{PSL}(2,11)$. *Commun. in Algebra*, **9**, 613–625.
Malle, G. (1987). Polynomials for primitive nonsolvable permutation groups of degree $d \le 15$. *J. Symb. Comput.*, **4**, 83–92.
Malle, G., Matzat, B. H. (1985). Realisierung von Gruppen $\mathrm{PSL}_2(\mathbb{F}_p)$ als Galoisgruppen über $\mathbb{Q}$. *Math. Ann.*, **272**, 549–565.
Malle, G., Matzat, B. H. (1999). *Inverse Galois Theory*. Heidelberg, Springer-Verlag.
Matzat, B. H. (1984). Konstruktion von Zahl- und Funktionenkörpern mit vorgegebener Galoisgruppe. *J. Reine Angew. Math.*, **349**, 179–220.
Matzat, B. H., Zeh-Marschke, A. (1986). Realisierung der Mathieugruppen M_{11} und M_{12} als Galoisgruppen über $\mathbb{Q}$. *J. Number Theory*, **23**, 195–202.
Porat, H. (1994). Galois groups of small order. Thesis, Technion.

Originally Received 17 September 1999
Accepted 8 March 2000