MATHEMATICS OF COMPUTATION
Volume 69, Number 230, Pages 775–796
S 0025-5718(99)01160-6
Article electronically published on August 19, 1999

SOME POLYNOMIALS OVER $\mathbb{Q}(t)$ AND THEIR GALOIS GROUPS

GENE WARD SMITH

Abstract. Examples of polynomials with Galois group over $\mathbb{Q}(t)$ corresponding to every transitive group through degree eight are calculated, constructively demonstrating the existence of an infinity of extensions with each Galois group over $\mathbb{Q}$ through degree eight. The methods used, which for the most part have not appeared in print, are briefly discussed.

1. Introduction

For each transitive group G of degree ≤ 8 we give a polynomial over $\mathbb{Q}(t)$ with Galois group G. Taken in conjunction with [9], to which this may be regarded as a companion piece, we have both a method for computing the Galois group of function fields over $\mathbb{Q}(t)$ and examples of such function fields through degree eight.

I used the Maple routines described in [9], which were written by Mattman as an extension of previous code by Sommeling, in determining Galois groups over $\mathbb{Q}(t)$ and $\mathbb{Q}$. This is due to appear as a part of the next Maple release, and should be available to those who have the most recent version of Maple by the time this sees print. I also used a C program by Helmut Geyer, which implemented the Staduhauer floating-point approach to determining Galois groups over $\mathbb{Q}$. In addition, I used the Pari package for various purposes, and a Maple program written by David Ford to compute the discriminant or p-discriminant of number fields.

The computations were done on a variety of Sparc stations, principally a SparcServer 10 with four sporty Ross HyperSparc processors and 128MB of RAM.

We will use the notation T_i to denote the ith transitive group of degree n (with n understood from context) in the tables of [1], but also what will probably become the new standard: a naming scheme for permutation groups given in [2]. This should be consulted for information about the meaning of these names.

A polynomial over $\mathbb{Q}(t)$ can define a splitting field extension which is $\mathbb{Q}(t)$ together with an algebraic extension of $\mathbb{Q}$ even when it has coefficients which are in $\mathbb{Q}(t)$ but not in $\mathbb{Q}$. For example, $x^2 - 2tx + t^2 - 2$, which has roots $t + \sqrt{2}$ and $t - \sqrt{2}$. However, if a polynomial over $\mathbb{Q}(t)$ is not reducible in this way, it will define an infinity of Galois extensions of $\mathbb{Q}$ with the Galois group of the polynomial over $\mathbb{Q}(t)$ by Hilbert's irreducibility theorem. The following definition is variously named, but is standard when discussing this situation:

Received by the editor October 19, 1993 and, in revised form, September 8, 1997.
1991 *Mathematics Subject Classification.* Primary 12F12.

Definition 1. A finite Galois extension of the field $F(t_1, \ldots, t_n)$, where the t_i are indeterminates, is *geometric for F* if it contains no nontrivial algebraic subextension K/F. We will call it geometric without qualification if it is geometric for $\mathbb{Q}$.

The polynomials we construct will, with one exception, have splitting fields which define geometric extensions. Since these polynomials are geometric over $\mathbb{Q}$, they will in each case, by Hilbert irreducibility, give for any number field an infinity of extensions with Galois group G.

In statements such as the one above, the usual convention is to take "Galois group" to refer to the group of automorphisms of a Galois extension over a base field. In what I write below, "Galois group" will refer to the permutation representation of the abstract Galois group on the roots of a polynomial giving a Galois extension with that group, up to relabeling of the roots—that is, up to conjugacy in S_n. Thus, while there are, in the sense of representation theory, two permutation representations of degree seven with group $L(3, 2)$, we will count this as one Galois group, since while there are two up to conjugacy in $L(3, 2)$, there is only one up to conjugacy in S_7. This also means that two polynomials of the same degree giving the same Galois extension may have in this sense *different* "Galois groups". In constructing "Galois groups", I will then construct an example of both types.

2. Direct and wreath products

It is often possible to construct a polynomial with a given Galois group by descent from a larger group. By substituting a suitable rational function of t in place of t into a polynomial over $\mathbb{Q}(t)$, we may specialize to another polynomial over $\mathbb{Q}(t)$ with the Galois group contained in the previous group.

To get a starting "top" polynomial for this process, we can do a number of things. When the group we wish to construct is imprimative, it is often the case that a wreath product gives us a suitable starting point. Because the direct product is analogous and simpler, and gives us certain groups which we will wish to construct, we will begin by considering it.

Definition 2. If G is a permutation group acting on a set S, and H is a permutation group acting on a set T, then the *direct product* of G and H, $G \times H$, is a permutation group acting on the cartesian product of S and T. The action is given by

$$[g, h](s, t) = (gs, ht),$$

where $g \in G$, $h \in H$, $s \in S$, and $t \in T$.

Theorem 1. *Let P and Q be polynomials of degree n and m, respectively, with coefficients in $F(t)$ and defining Galois extensions geometric for F with permutation groups G and H. If these two Galois extensions are disjoint over $F(t)$, then we can construct a polynomial of degree nm over $F(t)$, geometric for F, and defining a Galois extension with permutation group $G \times H$.*

Proof. This result is trivial, since the sum of a root from the first polynomial and a root from the second polynomial will have a minimal polynomial which gives the desired construction. □

The computation presents no difficulty as we can, for example, use the resultant to find the sum or product of the roots of two polynomials.

Definition 3. If G is a permutation group acting on a set S, and H is a permutation group acting on a set T, then the *wreath product* of G and H, $G \wr H$, is a permutation group acting on the cartesian product of S and T.

The elements of $G \wr H$ as an abstract group correspond with pairs $[f, h]$, where f is a function from T to G, and $h \in H$. This has a faithful permutation representation on the cartesian product of S and T, where the action of $[f, h]$ on a pair (s, t), with $s \in S$ and $t \in T$ is given by

$$[f, h](s, t) = (f(t)s, ht).$$

Theorem 2. *Let P and Q be polynomials of degree n and m, respectively, with coefficients in $F(t)$ and defining Galois extensions geometric for Hilbertian* ([6]) *F with permutation groups G and H. We can construct from these a polynomial of degree nm over $F(t)$, geometric for F, and defining a Galois extension with permutation group $G \wr H$.*

Proof. Suppose we have a polynomial h of degree m with Galois group H over F, and another polynomial g of degree n with Galois group G over $F(r)$, where r is a root of the polynomial h. Suppose also that the coefficients of g generate $F(r)$ over F. By taking the product of g together with its conjugate polynomials over F, we obtain a polynomial of degree nm with Galois group $G \wr H$ over F.

Now substitute for t in the polynomial P in the statement of the theorem the value

$$a_0 + a_1 r + \cdots + a_{m-1} r^{m-1},$$

where r is a root of the polynomial Q in the statement of the theorem, and the a_i are indeterminates. Then starting from a base field $F(t, a_0, \ldots, a_{m-1})$, we have the situation of the previous paragraph, and hence we obtain by that construction a polynomial with Galois group $G \wr H$ over $F(t, a_0, \ldots, a_{m-1})$. Since F is Hilbertian, so is any finitely generated extension, and so for most specializations of the a_i to values in $F(t)$, we will now obtain a polynomial over $F(t)$ with Galois group $G \wr H$, and hence we have the theorem. □

It should be noted that we may use resultants as a handy way to compute polynomials which exploit Theorem 2. If we have a polynomial in z over $F(t)$, and another in x over $F(z)$, then eliminating z gives us a polynomial in x over $F(t)$, which is the corresponding specialization from the theorem. For instance, suppose we eliminate z between $x^3 + zx + 1$ and $z^2 + tz + 1$; we get $T_{13} = F_{36}(6)\colon 2 = S(3) \wr 2$ as the Galois group for the polynomial $x^6 - tx^4 + 2x^2 - tx + 1$. Taking it in reverse order (that is, eliminating z between $x^2 + zx + 1$ and $z^3 + tz + 1$) gives us

$$(x^2 - x + 1)(x^4 + x^3 + 3x^2 + x + 1) + tx^2(x^2 + 1),$$

with Galois group $T_{11} = 2S_4(6) = 2 \wr S(3)$. These are typical examples of the wreath product construction.

This construction is not the only way to obtain wreath products. However, it is the most general construction, and will give us all we need.

The above construction depends on the fact that we may specialize to values which give us the wreath product. However, with the correct choice of values for specialization, we may at times obtain values which are subgroups of this product.

For instance, if we eliminate z between $z^2 - az - t$ and $x^3 - x - z$ we obtain

$$x^6 - 2x^4 - ax^3 + x^2 + ax - t,$$

with Galois group $S(3) \wr 2$ over $\mathbb{Q}(a, t)$. However, the special value $a = 0$ leads to a Galois group $D(6)$ over $\mathbb{Q}(t)$ instead.

3. Semidirect products

Some of the groups for which we wish to construct associated polynomials are split extensions with an abelian kernel. There is a nice way of treating these which essentially is the construction in [12] in a more general form.

In [12] I discussed how to construct polynomials whose Galois group was a split abelian by abelian extension; which is to say $\mathbf{Hol}(Z_n)$ or a subgroup. We may obtain nonabelian analogues of this process by considering instead the holomorphs of noncyclic abelian groups.

When considering polynomials through degree eight, the most important example is the holomorph of the 2-elementary abelian group of order 8, $E(8)\colon L_7$. The roots of this we may take to be sums over the characters of the 2-elementary group of a function f on the group which is 0 at the identity, and equal to an indeterminate f_i at any nonidentity element i, so that a root is

$$r_\chi = \sum \chi(i) f_i,$$

where χ is a character on the 2-elementary group $E(8)$ of order 8, and the sum is over elements i of this group.

Expanding this out, we get a polynomial of degree eight, with 0 as the trace term. The coefficient of degree five has the form of the resolvent for $L(3, 2)$, which consists of the seven products of three roots, corresponding to the lines of the projective plane of order 2. If we label the nonzero elements of the 2-elementary group by integers from 1 to 7, then in one of the labelings we obtain

$$-16(f_1 f_2 f_4 + f_2 f_3 f_5 + f_3 f_4 f_6 + f_4 f_5 f_7 + f_5 f_6 f_1 + f_6 f_7 f_2 + f_7 f_1 f_3).$$

We now form a seven by seven matrix by putting 1 in the (i, j)th place when we have a term containing f_i in the jth "line" of the resolvent, and 0 otherwise. This is the matrix

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

It is the incidence matrix for the projective plane of degree two.

We invert this matrix, multiply by 2, and reduce mod 2, and obtain the matrix

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

We now set f_i equal to the product of seven new indeterminates c_j, where we have c_j in the product for f_i whenever we have a 1 in our new matrix. Thus, for example, we substitute $c_2c_3c_4c_6$ for f_1.

The product of these two matrices is

$$\begin{bmatrix} 0 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 0 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 0 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 0 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 0 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 0 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 0 \end{bmatrix}.$$

Hence, inserting the corresponding product of c_j's into the degree eight polynomial over the seven indeterminates f_i, we get a new polynomial over the seven indeterminates c_j such that each c_j appears only to square powers. Now by substituting $b_j = \sqrt{c_j}$ in this polynomial, we get another polynomial in seven indeterminates b_j, where the b_j all appear to integral powers.

If we now substitute for b_j the roots of a polynomial contained in $L(3,2)$, with the roots ordered according to the order determined by considering the degree six term of this new polynomial, we get a polynomial of degree eight which has roots that are sums of square roots of products of the roots b_j of our degree seven polynomial, and which gives the split extension of the degree seven group by the 2-elementary group of degree eight. (This polynomial is long and complicated, and so we do not give it here; however, it is not too difficult to compute using a computer algebra package.)

In particular, we can substitute roots which are roots of a polynomial of degree seven over $\mathbb{Q}(t)$ with Galois groups $L(3,2)$, $7\colon 3$, or $C(7)$. The last two can be constructed via a similar method, which in fact gives a generic construction of all such Galois extensions, but with the added complication of seventh roots of unity (see [12], [13]). We then get $E(8)\colon L_7$, $E(8)\colon F_{21}$, and $E(8)\colon 7$, respectively.

Representative polynomials for all of these groups were computed. The method was to use floating point computations for enough successive values of t that it was possible to obtain a polynomial over $\mathbb{Q}(t)$ by interpolation. This allows a provably correct result, since we can bound the degree of the result as a polynomial in t. For $T_{25} = E(8)\colon 7$ and $T_{36} = E(8)\colon F_{21}$ we obtained polynomials of degree 48 in t, each of which had over 200 terms. These are given in §12, below the table for degree eight polynomials. It would be interesting to see less complicated examples.

It is worth remarking that in many circumstances, such as this one, a floating point computation can accomplish what would be very difficult or impossible for a purely algebraic approach. In [5], it is estimated that using the methods of [13] to construct a geometric cyclic extension of $\mathbb{Q}(t)$ with Galois group $C(17)$ would take about a year on a SUN Sparcstation 2, using the purely algebraic approach of that paper. On the same computer, I easily computed an example in a few hours by floating point methods, and it is clear that this result could be pushed up to higher degrees.

We may also use nontransitive subgroups of $L(3,2)$. If we substitute the roots of an S_4 extension of degree four for one of the seven complements of a line, and put 1 for all three values of the line of which it is a complement, we get a polynomial of degree eight with $T_{41} = E(8)\colon S_4$ as a Galois group.

This example was relatively easy because the group was 2-elementary; additional complications occur otherwise.

4. Examples over $\mathbb{Q}$

Sometimes one can guess what a polynomial with a given group looks like by consideration of an example over $\mathbb{Q}$. For instance, over $\mathbb{Q}$ the table of [9] gives

$$x^8 - 24x^6 + 144x^4 - 288x^2 + 144$$

as an example of a polynomial with $T_5 = Q_8(8)$ (the quaternion group) as a Galois group.

We might guess that this is a specialization of

$$x^8 - 2tx^6 + t^2x^4 - 2t^2x^2 + t^2$$

for the value $t = 12$, and use this as a starting point. This polynomial has a Galois group $T_{29} = E(8)\colon D_8$ over $\mathbb{Q}(t)$, and is not a very good starting point since the order of $E(8)\colon D_8$ is 64 and the order of $Q_8(8)$ is 8. This extension also is not geometric, and finally it is obtained by substituting $z = x^2$ into

$$z^4 - 2tz^3 + t^2z^2 - 2t^2z + t^2,$$

which has $D(4)$ as a Galois group instead of $E(4)$. So let us look instead for polynomials of degree four with $E(4)$ as a Galois group and which specialize in the desired way.

Solving the example polynomial gives us roots which are the conjugates of

$$\sqrt{6 + 2\sqrt{3} + 3\sqrt{2} + \sqrt{6}} = \sqrt{(2 + \sqrt{2})(3 + \sqrt{3})}.$$

If we look instead at

$$\sqrt{(a + \sqrt{a})(b + \sqrt{b})},$$

we obtain

$$\begin{aligned} &x^8 - 4abx^6 + 2ab(3ab - a - b - 1)x^4 \\ &\quad - 4a^2b^2(a-1)(b-1)x^2 + a^2b^2(a-1)^2(b-1)^2, \end{aligned}$$

which is a much better starting point, since this polynomial has a geometric Galois group $T_{22} = E(8)\colon D_4$ over $\mathbb{Q}(a, b)$.

This now becomes a means to solve not just the problem we began with, but others as well. In various ways we can specialize it to produce a geometric polynomial for $\mathbb{Q}(t)$, for instance by setting $a = t-1$, $b = t+1$, which gives the polynomial for $E(8)\colon D_4$ in the table. As for several other groups, it seems to be a good deal easier to find a polynomial over $\mathbb{Q}(t)$ with this Galois group than to find one which is geometric, so we may regard this as a lucky break.

This discriminant of this polynomial is $2^{32}a^{14}b^{14}(a-1)^6(b-1)^6(a-b)^4$. The $a - b$ term in this and the form of the example polynomial suggests setting $a = t$, $b = t+1$ in this polynomial, and obtaining

$$x^8 - 4t(t+1)x^6 + 2t(t+1)^2(3t-2)x^4 - 4t^3(t+1)(t^2-1)x^2 + t^4(t^2-1)^2,$$

with geometric Galois group $T_{11} = Q_8\colon 2$ over $\mathbb{Q}(t)$. This specializes to our original polynomial over $\mathbb{Q}$ with group $Q_8(8)$ when $t = 2$, and by trying values, it is not hard to guess that by setting $t = t^2 + 1$ we obtain a polynomial with Galois group $Q_8(8)$ over $\mathbb{Q}(t)$.

For another example, [9] gives us $x^8+4x^6+8x^4+8x^2+2$ as an example polynomial with Galois group $T_{28} = \frac{1}{2}[2^4]dD(4)$. Factoring this over $\mathbb{Q}(\sqrt{2})$ gives $(x^4+2x^2+2+\sqrt{2})(x^4-2x^2+2-\sqrt{2})$. This suggests among other possibilities that we consider the polynomial

$$(x^4+tx^2+t+\sqrt{t})(x^4+tx^2+t-\sqrt{t}) = (x^4+tx^2+t)^2-t,$$

with Galois group $T_{35} = [2^4]D(4) = 2 \wr 2 \wr 2$ (which is what we would generically expect for this wreath product type of construction). It is now now too hard once again to discover that substituting t^2+1 for t gives a Galois group which is $T_{28} = \frac{1}{2}[2^4]dD(4)$.

5. Using resultants and discriminants

Often, interesting polynomials over $\mathbb{Q}(t)$ can be constructed by first constructing polynomials over $\mathbb{Q}(t, \mathbf{c})$, where $\mathbf{c}$ are some further indeterminates. We write a form which has a desirable factorization at $t=0$ and $t=\infty$, corresponding to the group we are seeking. We then take the discriminant of this polynomial. We want to choose values of $\mathbf{c}$ which will collapse this discriminant into something simpler. We can do this by taking the further discriminants of the factors (first with respect to t), or by collapsing two factors together, by taking a resultant (especially with respect to t).

For instance, suppose we start with $(x^2-a)(x^2-b)^3+t$. This has Galois group $2\wr S(4)$ over $\mathbb{Q}(t,a,b)$; since it is a wreath product, this is an easy group to construct. The discriminant of this is

$$2^8t^4(t+ab^3)(256t-27a^4+108ab^3-162a^2b2^2+108a^3b-27b^4)^2.$$

We can collapse the terms $t+ab^3$ and

$$256t-27a^4+108ab^3-162a^2b^2+108a^3b-27b^4$$

by eliminating t (via resultant or substitution), and so get

$$(3a+b)(3a^2-14ab+27b^2)^2.$$

Setting $b=-3a$ in the original polynomial gives $(x^2-a)(x^2+3a)^3+t$, with Galois group $T_{40} = \frac{1}{2}[2^4]S(4)$ over $\mathbb{Q}(t,a)$.

For another example, consider the polynomial

$$(x^2-a)^4+t(x-1)^2,$$

This has Galois group $S(4) \wr 2$ over $\mathbb{Q}(a,t)$—once again a wreath product. The discriminant of this has a factor equal to

$$65536a^6-131072a^5+65536a^4-13824a^3t+96768a^2t-147456at+65536t+729t^2,$$

and taking the discriminant of this with respect to t gives us

$$2^{20}(9a-8)^2(4-3a)^3.$$

This suggests specializing a to either $9/8$ or $4/3$. When we do this, we find that we obtain

$$(x^2-4/3)^4+t(x-1)^2$$

with Galois group $T_{45} = [\frac{1}{2}S(4)^2]2$, and

$$(x^2-8/9)^4+t(x-1)^2$$

with Galois group $T_{41} = E(8){:}\, S(4)$. We may now transform these slightly and obtain the two polynomials listed in the table for these groups.

For a final example, let us go to an example where the group is not solvable.

We start with the polynomial

$$x(x^2 - a)^3 - t(x-1)^3(x-c).$$

This has Galois group S_7 over $\mathbb{Q}(a, c, t)$, but it has a factorization at $t = 0$ and $t = \infty$ which is consistent with $L(3, 2)$. If we take the discriminant of this with respect to x and factor it, we obtain a factor which has degree four in t, which is largest in the sense that it contains the greatest number of terms.

Taking the discriminant of this factor with respect to t and factoring, we obtain a factor which is of degree eight in a and degree ten in c, and which is largest. Taking the discriminant of this with respect to either a or c and factoring, we obtain $a - 49$ and $c - 9$, respectively, as factors. Substituting either of these into the polynomial we started with gives us a polynomial with Galois group S_7. Back-substituting $a = 49$ (resp. $c = 9$) into our expression in a and c, or simply repeating the process with our new and more simple polynomial, we obtain $c - 9$ (resp. $a - 49$) as a factor. We have now obtained

$$x(x^2 - 49)^3 - t(x-1)^3(x-9),$$

which has $L(3, 2)$ as Galois group over $\mathbb{Q}(t)$.

6. Modular functions

The theory of modular functions, and in particular the genus 0 functions of "moonshine theory", allows us to construct polynomials with Galois group $\mathrm{Pgl}_2(p)$ over $\mathbb{Q}(t)$, and in most cases to construct polynomials with Galois group $\mathrm{Psl}_2(p)$ as well.

For instance, if we take the modular functions

$$f_{21+3} = 1/q - q - q^2 + q^3 + 2q^4 - \cdots$$

and

$$f_{3-} = 1/q + 42 + 783q + 8672q^2 + 65367q^3 + 371520q^4 + \cdots$$

(see [3] for this notation), then the polynomial

$$x^6(x^2 - x + 7) - t(x-1)$$

has the property that substituting $x = f_{21+3}(q)$ and $t = f_{3-}(q^7)$ into it yields 0. It is a polynomial of degree eight with Galois group $T_{43} = \mathrm{Pgl}_2(7) = L(8){:}\, 2$, and moreover it is suited to the descent process described below for finding a polynomial of degree eight with Galois group $\mathrm{Psl}_2(7) = L(8)$ from it.

The approach via moonshine functions gives a very nice (and, to my mind, an easier) approach to the results of [8] and [11].

7. Rigidity

Another approach to constructing polynomials with a variety of Galois groups is the rigidity method, as explained in [10]. I constructed no polynomials via the rigidity method; however, the polynomial

$$(x^4 + 4x - 3)^2 + tx^4(4x - 3)$$

was constructed by Gunter Malle by the rigidity method, and has Galois group $T_{47} = S(4) \wr 2$. As a wreath product this is easy to construct; I mention it because I used it to construct a polynomial which appears in the table.

It is instructive to note that this could have been obtained by the method of using discriminants, if the right starting point had been tried.

Starting from

$$(x^4 + ax + b)^2 + tx^4(x - 1),$$

we take the discriminant with respect to x, factor, and find the largest factor. Taking the discriminant of this with respect to t, we find that we have two factors. In either factor, taking the discriminant with respect to either a or b and factoring finally leads us to consideration of $a = 256/27$, $b = -256/27$. Putting this into the above polynomial and transforming leads to

$$(x^4 + 4x - 3)^2 + tx^4(4x - 3)$$

with Galois group $S(4) \wr 2$.

Putting t^2 in the place of t leads to a polynomial with $T_{46} = \frac{1}{2}[S(4)^2]2$ as its Galois group, whereas putting $t^2 - 4$ in the place of t leads to $T_{45} = [\frac{1}{2}S(4)^2]2$ as its Galois group. The T_{46} polynomial appears in the table.

8. Quotient groups

By evaluating a resolvent (a rational function of the roots of a polynomial) over a suitably chosen set of cosets, we may create a polynomial whose Galois group may be abstractly the same but with a different permutation group, or may be a quotient group (in some permutation representation).

The easiest way to compute such maps is via the resolvent functions built into the Soicher/Mattman Maple program. There are several groups which are fairly easy, or even very easy, to construct via this method, but I did not end up using any of the polynomials I got this way.

9. Subgroups

Once we have obtained a polynomial (by this or other methods) we may use it to try to descend. Starting with a polynomial over $\mathbb{Q}(t)$ with Galois group G we can often find a rational function in t such that specializing (i.e., substituting) t into this rational function gives us a Galois group different from G. The trick is then to find such functions.

If the discriminant of the polynomial in question is not a square, one way we can accomplish this is to find a rational function for which it is a square. For instance, consider the polynomial $x^n + t(x - n + 1)$. As a trinomial, the discriminant of this is easily evaluated, and turns out to be

$$\pm((n - 1)t)^{n-1}(t + n^n),$$

where the sign is positive if n is congruent to 0 or 1 mod 4, and negative if it is congruent to 2 or 3. For odd n, it is clear that we can obtain a square discriminant by means of substituting $t^2 - n^n$ for t if n is congruent to 1 mod 4, and $-t^2 - n^n$ if n is congruent to 3 mod 4. In this way we may easily find polynomials with Galois group A_n over $\mathbb{Q}(t)$ for odd n.

For even n, we can also find a rational function which produces a square discriminant. If our only interest is in polynomials with Galois group A_n, it is easier to perform a similar analysis with the general form $x^{n-1}(x-n)-t$, and discover

$$x^{n-1}(x-n)+t^2+(n-1)^{n-1},$$

when n is congruent to 0 mod 4, and

$$x^{n-1}(x-n)-t^2+(n-1)^{n-1}$$

when n is congruent to 2 mod 4 give a square discriminant.

We may perform such an analysis to obtain Galois groups contained in A_n as well. For instance, taking the polynomial

$$x^6(x^2-x+7)-t(x-1),$$

which we obtained from a pair of modular functions, we find that the discriminant is

$$-7^7t^5(t-108)^3.$$

If we wish to find values of t for which this is a square, we need to find rational points on the ellipse

$$\frac{y^2}{7}+t(t-108)=0.$$

Since $t=0, y=0$ is one such point, we may find the others by drawing a line through this point and intersecting with the ellipse. Setting $y=ut$ in the equation for the ellipse and factoring, we obtain

$$t(tu^2+7t-756)=0,$$

and solving for t in the second factor gives us

$$\frac{756}{u^2+7}.$$

Substituting this into the original polynomial gives us a square discriminant. Converting this into a monic polynomial and exchanging u for t gives us

$$x^8-(t^2+7)x^7+7(t^2+7)^2x^6-756(t^2+7)^6x+756(t^2+7)^7,$$

which has Galois group $\mathrm{Psl}_2(7)$, i.e., $L(8)$.

An entirely different approach to finding such a rational function is to find values of t which give us the Galois group we are looking for, and then to guess what rational function could be giving us these values. We may then test this guess and determine if it is correct.

This approach is not without its problems. Suppose we have a polynomial over $\mathbb{Q}(t)$ with group G, and a subgroup H of G. Suppose that z is a resolvent expression in the roots of our polynomial which reduces to an element of $\mathbb{Q}$ upon specializing t precisely when the Galois group is contained in H. If we now express the algebraic relation between z and t by means of a polynomial, we have a curve which has a rational point when we have descent to (at least) H.

This curve need not be of genus 0. Even when it is, finding it by the sort of method suggested above is easiest if it is a polynomial function, if it is either even or odd, and if it produces an infinity of integer values when evaluated at integers. None of these things need be true.

Consider what happens if we attempt to find the rational function which gave us $L(8)$ in degree 8 by this method. Searching integer values produces essentially nothing, since the only integer value produced by $756/(u^2+7)$ is 108. Searching the inverses of integer values gives us nothing. If we search over half-integer values, we find $27/2, 189/2, 216/2$. The common factor of 27 here might suggest to us that we should look at numbers of the form $27/i$. This nets us values of i equal to $2, 16, 44, 86, \ldots$, from which we can guess that $27/(7u^2+7u+2)$ produces acceptable values for t. This can easily be transformed to forms we might prefer, such as $189/(u^2+u+2)$ or (what we started with) $756/(u^2+7)$.

Examples more difficult than this appear in the list of polynomials computed—for instance, for the polynomial for $T_{23} = GL(2,3)$. This was obtained by descent from the polynomial listed for $T_{40} = \frac{1}{2}[2^4]S(4)$. A number of $GL(2,3)$ extensions can be found for various values of t: $t = 24, 11, -9, -216, \ldots$. However, a general pattern did not emerge. The values could be seen to cluster near the ramified point over $t = 27$, and to be less than 27. Looking at $t = 27 - 1/u$, we find values produced by a fourth-degree polynomial in u. Substituting this and transforming gives the polynomial listed.

Another interesting case is $T_{10} = [2^2]4$. This I had trouble finding by descent from the polynomials I had for $T_{18} = E(8)\colon E_4$, $T_{19} = E(8)\colon 4$ or $T_{20} = [2^3]4$. For example, the condition to get a $[2^2]4$ polynomial by specializing the $E(8)\colon E_4$ polynomial listed turns out to be an elliptic curve. Since the curve has positive rational rank, we obtain in this way an infinity of examples over $\mathbb{Q}$, but not a polynomial over $\mathbb{Q}(t)$.

Starting with an example over $\mathbb{Q}$, I was lead to consider the polynomial

$$x^4 - 4x^3a + (6a^2+4b^2-2b)x^2 - 4(a^2+2b^2+b)ax + (a^2+2b^2+b)^2,$$

with roots

$$\begin{aligned} &a - \sqrt{b} + \sqrt{-2b^2 - 2a\sqrt{b}}, && a + \sqrt{b} + \sqrt{-2b^2 + 2a\sqrt{b}}, \\ &a - \sqrt{b} - \sqrt{-2b^2 - 2a\sqrt{b}}, && a + \sqrt{b} - \sqrt{-2b^2 + 2a\sqrt{b}}. \end{aligned}$$

This has Galois group (in degree four) $D(4) = 2 \wr 2$ over $\mathbb{Q}(a,b)$. Substituting $x = x^2$ into this gives a polynomial $\mathcal{P}$ with geometric Galois group $T_{29} = E(8)\colon D_4$ over $\mathbb{Q}(a,b)$. (A similar polynomial with this property, which used to produce the polynomial in the table with this group, is

$$(x-a)^2(x-b)^2 - tx^2,$$

which has geometric Galois group $E(8)\colon D_4$ over $\mathbb{Q}(a,b,t)$ upon substituting x^2 for x.)

The example I began with was (up to a factor of 2) what one gets on substituting $a = 3$, $b = 5$ into $\mathcal{P}$, namely $x^8 - 3x^6 + 9x^4 - 12x + 16$. This has Galois group $[2^2]4$, and substituting $x = \sqrt{x}$ into it gives us a polynomial with Galois group $D(4)$.

However, $[2^2]4$ has the curious property that it can arise from substituting x^2 for x into a polynomial with cyclic Galois group $C(4)$ as well as one with dihedral Galois group $D(4)$. Substituting $a = t^2+1$, $b = t^2+1$ into the first polynomial gives us one with Galois group $C(4)$ over $\mathbb{Q}(t)$. Substituting $x = x^2$ into this then gives us a polynomial with Galois group $[2^3]4$. It no longer specializes to the polynomial we began with, but it turns out that does not matter!

We now may check to see which values of t lead to a $[2^2]4$ polynomial. One way to do this is to substitute $x = x+1$ into the polynomial, and then find the “2-set resolvent” which is th polynomial for products of distinct roots taken pairwise. This is of degree 28, and has a factor of degree 8. This factor is reducible if t leads to a polynomial with Galois group $[2^2]4$.

Checking for values of t leading to reducible polynomials, one find

$$0, 2, 8, 30, 112, 418, \ldots .$$

This appears to satisfy the recurrence relationship $a_i = 4a_{i-1} - a_{i-2}$. Hence we may suspect there is a Pell's equation involved, which is one form of a genus 0 condition. The Pell's equation corresponding to this recurrence is

$$x^2 - 3y^2 = 4,$$

where for x we get $2, 4, 14, 52, \ldots$ with the same recurrence relationship, and for y we get $0, 2, 8, 30, \ldots$, our desired values for t. Solving this Pell's equation, we find that

$$x = \frac{2t^2+3}{t^2-3}, \qquad y = \frac{4t}{t^2-3}.$$

Substituting the solution for y into our polynomial and transforming, we obtain the polynomial listed in the table.

10. A problem group

Quite a lot of attention has been devoted to the group $2A_4 = \mathrm{Sl}_2(3)$ (see [4] and [7].) Despite this, no explicit polynomial giving a geometric extension of $\mathbb{Q}(t)$ with Galois group $2A_4$ seems to be known.

This group is a double cover of the alternating group of degree 4, and has a faithful permutation representation of degree 8, which is $T_{12} = 4A_4(8)$ in the list of degree 8 permutation groups.

Polynomials of degree 8 giving this group can be constructed by substituting x^2 for x in a polynomial of degree 4 with norm term a square and with Galois group A_4, and such that the roots are real and either all positive or all negative. This will in general give an extension with group $T_{32} = [2^3]A(4)$, but in particular cases the extension can be $2A_4(8)$ or $T_{13} = A(4)[\times]2$ instead.

One example of such a polynomial is $x^4 - 22x^3 + 135x^2 - 150x + 1$. This has Galois group A_4, and all of its roots are real and positive. Substituting $x = x^2$ into this gives a polynomial with Galois group $2A_4(8)$.

If we do not require a geometric extension of $\mathbb{Q}(t)$, this can be used to give us a polynomial over $\mathbb{Q}(t)$ with Galois group T_{12}, since by substituting $x = x^2/t$ into it we obtain $x^8 - 22tx^6 + 135t^2x^4 - 150t^3x^2 + t^4$. Specializing t gives extensions which have the same A_4 subfield.

A polynomial over $\mathbb{Q}(a, b)$ with Galois group A_4 and with square norm term, and such that substituting x^2 for x gives a polynomial with Galois group T_{32}, is

$$\begin{aligned}
&x^4 - 200a(b^2-1)^2x^3 \\
&\quad + 1500(b^2-1)^3(10a^2b^2 - 10a^2b + 5a^2 - 294b^2 + 50a + 882b - 399)x^2 \\
&\quad - 50000(b^2-1)^5(10a^3b^2 - 30a^3b - 882ab^2 - 50a^2b \\
&\qquad\qquad\qquad + 35a^3 + 2646ab + 225a^2 + 4410b - 947a - 3465)x \\
&\quad + 250000(b^2-1)^6(5a^2b^2 - 15a^2b - 441b^2 - 50ba + 5a^2 + 693b - 441)^2.
\end{aligned}$$

This has a region where the roots are all real and positive, which contains the region $a \geq 12$, $b \geq 4$. We can find specializations which produce a $2A_4(8)$ polynomial, but the descent problem presents difficulties. Examples where a and b are both positive integers less than 50 are $a = 11$ and $b = 9, 13, 29, 49$; $a = 27$ and $b = 9, 29, 49$; and $a = 15$ and $b = 3$. It seems likely that there is a pattern of some sort.

11. Determination of Galois groups

In compiling our tables, two things needed to be determined and proven: that the Galois group is in fact the one listed, and that the extensions are in fact geometric. To accomplish the first, we for the most part used the Maple program of Sommeling/Mattman/McKay, with checks on its accuracy provided by testing specializations using other programs.

However, in some cases these Maple routines failed to provide an answer, because of the large space requirements that routinely result in computer algebra applications. In those cases, a moral certainty can be obtained by testing successive specializations; however, without a theorem telling us how many successive specializations will suffice for a given input polynomial (something which would be desirable to have), an actual proof requires that we do the polynomial "by hand", so to speak. By this I mean that we must direct the computations instead of letting the program do it for us.

The heavy lifting of this Maple program is accomplished by two routines named "rsetpol" and "twoseqpol". The first finds the minimal polynomial for the products of n of the roots, and the second does the same for $r_1 + 2r_2$, where r_1 and r_2 are any two roots. These routines do not use floating point methods, which is why the program could be extended to cover function fields (and might be extended to cover other possibilities, such as p-adic or number field base fields). Determining the degrees of the irreducible factors (provided they are distinct, which we can always assure) gives invariants which in most instances, together with the discriminant, allow a determination of the Galois group.

To take one example, the program is able to determine that the Galois group of (the splitting field for)

$$x^8 + tx^7 - 28x^6 - 7tx^5 + 70x^4 + 7tx^3 - 28x^2 - tx + 1$$

is $T_7 = \frac{1}{2}[2^3]4$. Alas, this elegant polynomial is not geometric, and the program as it was originally configured failed with the computers I used. However, a simple change of strategy made the same approach work. The program chooses to compute products of three roots before invoking "twoseqpol"; however, the factor type $8^3 16^2$ is in fact unique among groups not contained in A_8, and it is easily computed when invoked.

For the group $T_{15} = C(8)\colon E_4$ we once again have a nongeometric polynomial which the computer *can* handle, namely

$$(x^4 + 4x^2 + 2)^2 + t,$$

and a geometric polynomial it has trouble with. In this case, we have a number of possible groups with a nonsquare discriminant and the same 2-set and 2-sequence invariants. The computer program therefore attempts to find the 3-set invariant (which does distinguish the group), and this runs into space problems.

However, the polynomial in question was constructed using the split-extension method described in the section on semidirect products. Hence, it can be no larger than T_{15}, and simply checking a few factorizations at specializations to primes of $\mathbb{Z}[t]$ (which is to say, specializing t and reducing modulo a prime integer) suffices to show it must also be at least this large.

This also allows us to show that the polynomials for $E(8)\colon F_{21}$ and $E(8)\colon 7$, which are far too large for the computer to handle, in fact give the claimed groups.

This left me with a few cases where I still had no proof, but only a moral certainty. But in those cases one can convert the moral certainty *into* a proof. If it comes down to factoring the "twoseqpol" resolvent, then factor the resolvent for a number of successive specializations, and then reconstruct the factors by interpolation, and so factor the resolvent "by hand". Often a simple transformation of the polynomial must be effected first, to prevent repeated factors in the resolvent polynomial. Except in the case of the polynomial for $r_1 + r_2 + r_3 + r_4 - r_5 - r_6 - r_7 - r_8$ in degree eight, simply adding one to each root always sufficed.

One can work in a similar way if some factor of some resolvent must be factored over an extension field. In effect, I was doing "by hand" a factorization algorithm which could be coded, and whose principle merit is that it is economical of space. The polynomials in the table were sometimes right on the edge of what was possible with these methods, but were never so far over the edge that a different resolvent altogether had to be used.

My first version of these tables included many entries which were not geometric. I used a set of Maple routines written by David Ford to determine the discriminant of the ring of integers of successive specialization, since it seemed to be more efficient than what was in the Maple distribution. If the GCD of these discriminants was 1, I could conclude without further work that no algebraic subfield could exist.

In other cases, I would get a nontrivial GCD—most commonly, a power of two. I then made use of the fact that usually (and in all the cases for which a question remained) I had a maximal quotient group which was solvable, and hence any algebraic subextension would have to be solvable. Such an extension would have a maximal abelian subextension, and this in term would have maximal p-elementary subextensions for each prime p. By checking the (usually quadratic) factors of this subextension, one can determine if an algebraic subextension exits. This can be done using class field theory; one checks at primes where the polynomial factors into linear factors, to see if the cyclic extensions with the relevant discriminants sometimes do not factor. In practice, this most often amounted to checking the factorization of $x^2 + 1$, $x^2 + 2$, and $x^2 - 2$, after determining (using discriminants) that only the prime 2 need be considered.

12. Tables

Group	Name	Polynomial
1	S_2	$x^2 - tx + 1$

Group	Name	Polynomial
1	A_3	$x^3 + tx^2 + (t-3)x - 1$
2	S_3	$x^3 - 3x - t$

Group	Name	Polynomial
1	$C(4)$	$x^4 + tx^3 - 6x^2 - tx + 1$
2	$E(4)$	$x^4 + tx^2 + 1$
3	$D(4) = 2 \wr 2$	$x^4 + tx^3 + tx + 1$
4	A_4	$x^4 + 18tx^3 + (81t^2 + 2)x^2 + 2(54t^2 + 1)tx + 1$
5	S_4	$x^4 + tx + 1$

Group	Name	Polynomial
T_1	$C(5)$	$x^5 + x^4t^2 - (2t^3 + 6t^2 + 10t + 10)x^3$ $+(t^4 + 5t^3 + 11t^2 + 15t + 5)x^2$ $+(t^3 + 4t^2 + 10t + 10)x + 1$
T_2	$D(5) = 5\colon 2$	$x(x^2 - 25)^2 - t(x - 1)^2(x + 3)$
T_3	$F(5) = 5\colon 4$	$x^5 + 10x^3 + 5tx^2 - 15x + t^2 - t + 16$
T_4	A_5	$x^5 + (t^2 - 3125)(x - 4)$
T_5	S_5	$x^5 + tx + 1$

Group	Name	Polynomial
T_1	$C(6)$	$x^6 + 2tx^5 + 5(t + 3)x^4 + 20x^3 + 5tx^2 - 2(t + 3)x + 1$
T_2	$D_6(6)$	$(x^2 + 4)(x^2 + 1)^2 + 3t^2$
T_3	$D(6)$	$x^2(x^2 + 3)^2 - t$
T_4	$A_4(6)$	$x^6 + tx^4 + (t - 3)x^2 - 1$
T_5	$F_{18}(6) = 3 \wr 2$	$(x^3 - 3x - 1)^2 + tx^2(x + 1)^2$
T_6	$2 \wr 3$	$x^6 - 4t^2(t^2 + 3)(3x^2 - 4t^2)$
T_7	$S_4(6d) = [2^2]S(3)$	$x^6 + tx^2 - 1$
T_8	$S_4(6c) = \frac{1}{2}[2^3]S(3)$	$(x^2 + 1)(x^2 - 2)^2 + 3t^2$
T_9	$F_{18}(6)\colon 2$	$x^4(x - 6)^2 - t^2 - 1024$
T_{10}	$F_{36}(6)$	$(x + 2)^2(x - 1)^4 + t^2x^3(3x - 2)$
T_{11}	$2 \wr S(3)$	$(x^2 + 1)(x^2 - 2)^2 + t$
T_{12}	$L(6)$	$x^6 + (10t^2 - 50)x^5 + 55(t^2 - 5)^2x^4 + 140(t^2 - 5)^3x^3$ $+175(t^2 - 5)^4x^2 + 2(53t^2 + 375)(t^2 - 5)^4x + 25(t^2 - 5)^6$
T_{13}	$S(3) \wr 2$	$x^4(x - 1)^2 - t$
T_{14}	$L(6)\colon 2 = PGL(2, 5)$	$x^4(x^2 + 4x + 20) - t(x - 1)$
T_{15}	A_6	$x^5(x - 6) - t^2 + 3125$
T_{16}	S_6	$x^6 + tx + 1$

Group	Name	Polynomial
T_1	$C(7)$	$x^7 + (t^3 + 2t^2 - t + 13)x^6 + 3(t^2 - t + 2)(t^3 + t + 9)x^5$ $+ (3t^7 - 9t^6 + 27t^5 - 22t^4 + 6t^3 + 84t^2 - 121t + 75)x^4$ $+ (t^2 - t + 2)(t^7 - 5t^6 + 15t^5 - 32t^4 + 20t^3 + 14t^2 - 113t - 1)x^3$ $- (t^{10} - 5t^9 + 25t^8 - 61t^7 + 126t^6 - 117t^5$ $+ 58t^4 + 155t^3 - 168t^2 + 80t + 44)x^2$ $- (t^{10} - 8t^9 + 30t^8 - 75t^7 + 102t^6 - 89t^5$ $- 34t^4 + 56t^3 - 113t^2 - 42t + 17)x$ $+ t^9 - 7t^8 + 23t^7 - 42t^6 + 28t^5 + 19t^4 - 60t^3 - 2t^2 + 16t - 1$
T_2	$D(7) = 7\colon 2$	$x^7 - (7t^3 + 35t^2 + 21t + 1)(21x^5 + (98t + 70)x^4$ $- (1029t^3 + 4557t^2 + 343t - 105)x^3$ $- 28(7t + 1)(49t^3 + 147t^2 + 63t - 3)x^2$ $+ 7(7t^2 + 42t - 1)(7t^2 + 14t - 5)(7t + 1)^2x$ $+ 235298t^7 + 1236858t^6 + 1138074t^5$ $+ 562226t^4 + 11270t^3 - 4914t^2 - 322t + 6)$
T_3	$F_{21}(7) = 7\colon 3$	$x^7 - (t^6 + 56t^4 - 7t^3 + 980t^2 - 189t + 5103)$ $(21x^5 + (21t^3 - 49t^2 + 539t - 1323)x^4$ $- (91t^6 + 98t^5 + 4753t^4 + 3822t^3 + 72471t^2 + 31752t + 250047)x^3$ $- (112t^9 - 49t^8 + 8379t^7 - 7154t^6 + 221186t^5 - 293265t^4$ $+ 2343033t^3 - 4167450t^2 + 7501410t - 13502538)x^2$ $+ 7(12t^{11} + 14t^{10} + 1456t^9 + 1687t^8 + 67816t^7 + 79786t^6 + 1492540t^5$ $+ 1847888t^4 + 15067647t^3 + 20994687t^2 + 51902613t + 94517766)tx$ $+ 97t^{15} + 14t^{14} + 14371t^{13} + 798t^{12} + 865494t^{11}$ $- 24087t^{10} + 26944169t^9 - 2680790t^8 + 451657745t^7$ $- 66683316t^6 + 3747134223t^5 - 557965989t^4 + 10380951252t^3$ $- 573857865t^2 - 14765025303t - 4921675101)$
T_4	$F_{42}(7) = 7\colon 6$	$x(x^2 + 7x + 28)(x^2 + 7)^2 + 28(x - 7)(x^2 + 7)t$ $- 7(x^4 + 16x^2 - x + 84)t^2 - 7(5x^2 + 37)t^3 - 30t^4 - t^5$
T_5	$L(7) = L(3, 2)$	$x(x^2 - 49)^3 - t(x - 1)^3(x - 9)$
T_6	A_7	$x(x^2 - 49)^3 - t(x^2 - 25)^3$
T_7	S_7	$x^7 - t(x - 6)$

Group	Polynomial
T_1	$x^8 - (t^4 + 12t^2 + 4)x^6 + (3t^2 + 1)(t^4 + 12t^2 + 4)x^4$ $- (3t^2 + 2)(t^4 + 12t^2 + 4)t^2x^2 + (t^4 + 12t^2 + 4)t^6$
T_2	$x^8 - t^2x^7 - (7t^2 + 12)x^6 + (t^2 - 3)t^2x^5 + (2t^4 + 6t^2 + 38)x^4$ $+ (t^2 - 3)t^2x^3 - (7t^2 + 12)x^2 - t^2x + 1$
T_3	$x^8 - 12tx^6 + (30t^2 + 8)x^4 - 4(7t^2 - 4)tx^2 + (3t^2 - 4)^2$
T_4	$x^8 - 10(t - 2)(t + 2)x^6 + (33t^4 - 208t^2 + 472)x^4$ $- 40(t - 2)(t + 2)(t^4 - t^2 + 9)x^2 + 16(t^4 + 17t^2 - 9)^2$
T_5	$x^8 - 4(t^2 + 2)(t^2 + 1)x^6 + 2(3t^2 + 1)(t^2 + 1)(t^2 + 2)^2x^4$ $- 4t^2(t^2 + 2)^2(t^2 + 1)^3x^2 + t^4(t^2 + 2)^2(t^2 + 1)^4$
T_6	$x^8 - (t^2 + 12t + 4)x^6 + (3t + 1)(t^2 + 12t + 4)x^4$ $- (3t + 2)(t^2 + 12t + 4)tx^2 + t^3(t^2 + 12t + 4)$
T_7	$x^8 - 12(5t^2 - 6t + 2)(t^2 - 6t + 10)x^6$ $+ 6(5t^2 - 6t + 2)(t^2 - 6t + 10)(23t^4 - 140t^3 + 300t^2 - 224t + 64)x^4$ $-108(t^2-6t+10)(5t^2-6t+2)(3t^4-20t^3+44t^2-32t+8)(t^2-2t+2)^2x^2$ $+ 9(5t^2 - 6t + 2)(t^2 - 6t + 10)(t^2 - 2t + 2)^2(t^2 - 6t + 4)^4$
T_8	$x^8 - (16t^8 + 64t^6 + 96t^4 + 80t^2 + 36)x^6$ $+ 4(4t^6 + 20t^4 + 40t^2 + 31)(4t^8 + 16t^6 + 24t^4 + 20t^2 + 9)t^2x^4$ $- 32(4t^6 + 14t^4 + 16t^2 + 7)(4t^8 + 16t^6 + 24t^4 + 20t^2 + 9)(t^2 + 2)^2t^4x^2$ $- 64(t^2 + 1)(4t^8 + 16t^6 + 24t^4 + 20t^2 + 9)(t^2 + 2)^4t^6$
T_9	$x^8 + tx^6 + (2t - 1)x^4 + tx^2 + 1$
T_{10}	$x^8 + 2(t^2 + 1)(t^2 + 9)x^6 + 2(t^2 + 1)(t^2 + 9)(t^4 + 14t^2 + 9)x^4$ $+ 2(t^2 + 3)^2(t^2 + 1)^2(t^2 + 9)^2x^2 + (t^2 + 1)^2(t^2 + 9)^2(t^2 + 3)^4$
T_{11}	$x^8 - 4t(t + 1)x^6 + 2t(t + 1)(3t^2 + t - 2)x^4 - 4t^3(t^2 - 1)x^2 + t^4(t^2 - 1)^2$
T_{12}	$x^8 - 22tx^6 + 135t^2x^4 - 150t^3x^2 + t^4$
T_{13}	$x^8 + 18tx^6 + (81t^2 + 2)x^4 + 2(54t^2 + 1)tx^2 + 1$
T_{14}	$(x^4 - 42x^2 + 729)(x^2 + 3)^2 + 3t^2x^2$
T_{15}	$x^8 - (36t^2 - 4032)x^6 - 108(t^2 - 112)(t^2 + 88t + 820)x^4$ $-15552(t+11)(t^2-112)(t^2+52t+424)x^2-746496(t+29)(t^2-112)(t+11)^3$
T_{16}	$x^8 + 8(5t^2 + 6t + 5)^2(25t^2 + 14t + 25)^2x^6$ $+ 14(5t^2 + 6t + 5)^4(25t^2 + 14t + 25)^4x^4$ $- 8(5t^2 + 6t + 5)^6(25t^2 + 14t + 25)^6x^2$ $+ (5t^2 + 22t + 5)^2(5t^2 + 6t + 5)^7(25t^2 + 14t + 25)^7$
T_{17}	$x^8 - tx^7 - 11x^6 + 7tx^5 + 36x^4 - 7tx^3 - 11x^2 + tx + 1$

Group	Polynomial
T_{18}	$x^8 + tx^6 + tx^2 + 1$
T_{19}	$x^8 - (t^2+1)^2x^6 + 2(t^2+1)(t^2-t+1)(t^2+t+1)x^4$ $- (t^2+1)^3t^2x^2 + (t^2+1)^2t^4$
T_{20}	$x^8 - 4(t^2+1)x^6 + 2(t^2+1)(5t^2+4)x^4$ $- 4(3t^2+4)(t^2+1)^2x^2 + (3t^2+4)^2(t^2+1)^2$
T_{21}	$x^8 + 8x^6 - (16t^6 + 64t^4 + 80t^2 + 16)x^4$ $- 64(t^2+2)(t^2+1)^2x^2 + 64(t^2+1)^3t^2$
T_{22}	$x^8 - 4(t+1)(t-1)x^6 + 2(t+1)(t-1)(3t^2-2t-4)x^4$ $- 4(t+1)^2(t-1)^2t(t-2)x^2 + (t+1)^2(t-1)^2(t-2)^2t^2$
T_{23}	$(x^2+9)(x^2-3)^3 - t^3(t+4)(2x^4 - 8x^2 + 9)$
T_{24}	$(x^2-1)^4 + tx^2$
T_{25}	See below
T_{26}	$x^8 + 8(t^2-1)^2x^6 + 14(t^2-1)^4x^4$ $- 8(t^2-1)^6x^2 + 3(t+3)^2(t^2-1)^7$
T_{27}	$x^8 + tx^7 - 2x^6 + 2tx^5 - 5x^4 + 2tx^3 - 2x^2 + tx + 1$
T_{28}	$(x^4 + (t^2+1)x^2 + t^2 + 1)^2 - t^2 - 1$
T_{29}	$(x^2 - t - 1)^2(x^2 - t + 1)^2 - tx^4$
T_{30}	$x^2(x^2-4)(x^2-2)^2 - 2(x^2-1)(x^2-3)(2t^2+6) + (2t^2+6)^2$
T_{31}	$x^8 + 8x^6 - (16t^3 + 64t^2 + 80t + 16)x^4 - 64(t+2)(t+1)^2x^2 + 64t(t+1)^3$
T_{32}	$(x^2+1)(x^2-3)^3 + t^2 + 27$
T_{33}	$x^8 - 4(x^4 + 12x^3 + 82x^2 + 192x + 256)x^2(t^2+27)$ $+ (6x^4 + 96x^3 + 464x^2 + 960x + 1296)(t^2+27)^2$ $+ (4x^2 + 48x + 72)(t^2+27)^3 + (t^2+27)^4$
T_{34}	$(x^2-18)^4 + (2x-9)^2(3t^2 - 1728)$
T_{35}	$(x^4 + tx^2 + t)^2 - t$
T_{36}	See below
T_{37}	$x^8 + (t^2+7)x^7 + 7x^6(t^2+7)^2 - 756(t^2+7)^6x + 756(t^2+7)^7$
T_{38}	$x^6(x^2-4) + t^2 + 27$
T_{39}	$x^8 + tx^2 + 1$
T_{40}	$(x^2+1)(x^2-3)^3 + t$
T_{41}	$(x^2-2)^4 + t(2x-3)^2$
T_{42}	$(x^2-3)^4 + 3t^2(2x-3)^2$
T_{43}	$x^6(x^2 - x + 7) - t(x-1)$
T_{44}	$x^8 + tx^7 + tx + 1$

Group	Polynomial
T_{45}	$(x^2-3)^4+t(2x-3)^2$
T_{46}	$(x^4+4x-3)^2+t^2x^4(4x-3)$
T_{47}	$(x^4+x+1)^2+t(x+1)x^4$
T_{48}	$x(x^7-8x^6+16x^5+6x^4-18x^3-18x^2-7x-1)-t(2x+1)^2$
T_{49}	$x^7(x-8)+t^2+823543$
T_{50}	$x^7(x-8)+t$

Let $l=t^6+t^5+t^4+t^3+t^2+t+1$. Then a polynomial for T_{25} is

$$\begin{gathered}
x^8+l(84t^6+84t^5-112t^4-308t^3-700t^2-504t+84)x^6\\
+112l(t-1)(5t^{11}+15t^{10}-5t^9-62t^8-93t^7\\
-91t^6-126t^5-166t^4-113t^3-30t^2-8t-12)x^5\\
+98l^2(15t^{12}+30t^{11}+3t^{10}-122t^9-492t^8-274t^7\\
+1225t^6+2092t^5+2175t^4+2006t^3+906t^2+100t+127)x^4\\
+224l^2(9t^{18}+27t^{17}+138t^{16}+146t^{15}-1167t^{14}\\
-1547t^{13}+7049t^{12}+18959t^{11}+12770t^{10}-1200t^9+4097t^8\\
+9439t^7-12075t^6-28217t^5-13039t^4+2393t^3-212t^2-2430t+58)x^3\\
+28l^2(55t^{24}+220t^{23}+2153t^{22}+4691t^{21}-5418t^{20}\\
+23233t^{19}+228452t^{18}+475520t^{17}+287159t^{16}-600374t^{15}\\
-1984307t^{14}-3379523t^{13}-4660453t^{12}-5845875t^{11}\\
-6137953t^{10}-5782110t^9-5639153t^8-4845124t^7-3078208t^6\\
-2133257t^5-2075038t^4-1607507t^3-622674t^2+4721t+92679)x^2\\
+16l^2(39t^{30}+195t^{29}+2790t^{28}+8519t^{27}+16940t^{26}\\
+225855t^{25}+1104180t^{24}+2242889t^{23}+1399808t^{22}\\
-6020961t^{21}-25508840t^{20}-49019705t^{19}-58600367t^{18}\\
-69234886t^{17}-102278166t^{16}-112179983t^{15}-70498523t^{14}\\
-39241916t^{13}-35156807t^{12}+2191322t^{11}+57656039t^{10}\\
+74500144t^9+72804904t^8+79557490t^7+70533449t^6\\
+48000512t^5+34276466t^4+21509663t^3+5376298t^2-1410928t-610984)x\\
+7l^3(15t^{30}+75t^{29}+1597t^{28}+4837t^{27}+23884t^{26}+347732t^{25}\\
+2111634t^{24}+5807707t^{23}-871233t^{22}-50322479t^{21}-111635825t^{20}\\
-28345436t^{19}+193203437t^{18}+346778159t^{17}+656100311t^{16}\\
+1389057175t^{15}+2002720726t^{14}+2197415248t^{13}+2560304502t^{12}\\
+2936446653t^{11}+2672763639t^{10}+2134534195t^9+1835594167t^8\\
+1442639068t^7+890569771t^6+522893385t^5+352986417t^4\\
+187040567t^3+83103483t^2+52679639t+27709039).
\end{gathered}$$

Let $l = t^6 + 56t^4 - 7t^3 + 980t^2 - 189t + 5103$. Then a polynomial for T_{36} is

$$\begin{gathered}
x^8 + 84lt(t^5 + 7t^4 + 77t^3 + 413t^3 + 1260t + 6048)x^6 \\
+112lt(12t^{11} + 14t^{10} + 1456t^9 + 1687t^8 \\
+67816t^7 + 79786t^6 + 1492540t^5 + 1847888t^4 \\
+150676647t^3 + 20994687t^2 + 51902613t + 94517766)x^5 \\
+98l^2(127t^{12} + 98t^{11} + 14861t^{10} + 17024t^9 + 700637t^8 \\
+983066t^7 + 16546411t^6 + 23970996t^5 + 195888672t^4 + 226709280t^3 \\
+954750888t^2 + 354923856t + 416649744)x^4 \\
+224l^2(58t^{18} + 4746t^{17} + 11466t^{16} + 848533t^{15} + 956613t^{14} \\
+63940695t^{13} + 44653847t^{12} + 2622099564t^{11} + 1310602461t^{10} \\
+62800333736t^9 + 25896405969t^8 + 868595348565t^7 + 354357606708t^6 \\
+6267169256355t^5 + 3143228815944t^4 + 16609715039484t^3 \\
+13293262163538t^2 - 10542228066342t - 3720786376356)x^3 \\
+28l^2(92679t^{24} + 27251t^{23} + 22341494t^{22} + 1970703t^{21} \\
+2377821859t^{20} - 240284219t^{19} + 147080271408t^{18} \\
-40133661729t^{17} + 5850921810489t^{16} - 2479591212651t^{15} \\
+156245540841530t^{14} - 85460151822283t^{13} + 2833137718953549t^{12} \\
-1785942335328053t^{11} + 34407743050495192t^{10} - 22484916215014995t^9 \\
+267949508417695944t^8 - 155111569609853808t^7 + 1216946756938622976t^6 \\
-395161827317561304t^5 + 2582944198926978096t^4 + 1006961653695531744t^3 \\
+1207469594855049120t^2 + 5260150115982004320t + 1367076447255216096)x^2 \\
-16l^2(610984t^{30} - 1814358t^{29} + 173412876t^{28} - 559269767t^{27} \\
+22215296852t^{26} - 78272133695t^{25} + 1693448633947t^{24} \\
-6574758748187t^{23} + 85165722582185t^{22} - 369101044061057t^{21} \\
+2955182978201118t^{20} - 14590325493108141t^{19} + 71604511995708853t^{18} \\
-416655064165453477t^{17} + 1188305557133823772t^{16} \\
-8674662266588396099t^{15} + 12503079535353566551t^{14} \\
-131164617287149386157t^{13} + 60477161743382905710t^{12} \\
-1416213397101350695932t^{11} - 292455772615528882857t^{10} \\
-10557931743508007769876t^9 - 6515994233868926912595t^8 \\
-51084827821598387592258t^7 - 39552526739628735284088t^6 \\
-140788682522299613035836t^5 - 87194523110846975505108t^4 \\
-140691994656875937962064t^3 + 16720104436846434640800t^2 \\
+144009541799423532572760t + 62979503079488736522600)x \\
+7l^3(27709039t^{30} + 31223556t^{29} + 7833378014t^{28} + 8760462179t^{27}
\end{gathered}$$

$$
\begin{gathered}
+1006873891569t^{26}+1119419376019t^{25}+77741715374757t^{24}\\
+86111109399567t^{23}+4011691914670251t^{22}+4439407451249239t^{21}\\
+145581051354018525t^{20}+161498379453143537t^{19}\\
+3804201727782153131t^{18}+4247052560379095481t^{17}\\
+72008641447685051599t^{16}+81226343219113714293t^{15}\\
+978223087576340403546t^{14}+1118046058222551179673t^{13}\\
+9287040686789967525585t^{12}+10736207594262764690328t^{11}\\
+58484587187200337972928t^{10}+67268821419254486839248t^{9}\\
+220790751720343098064848t^{8}+235447728140821637919744t^{7}\\
+395798513988183140997792t^{6}+252982270940951430978624t^{5}\\
+117912897702128865103488t^{4}-479678343600685954894848t^{3}\\
+295571041739559421395584t^{2}+425691200757907229701248t\\
+327105849840544576154304).
\end{gathered}
$$

Acknowledgments

I wish to thank the IWR (Interdisziplinäres Zentrum für Wissenschaftliches Rechnen) of Heidelberg University and the funding agency Deutsche Forschungsgemeinschaft for support during my stay in Heidelberg, and CICMA (Centre Interuniversitaire en Calcul Mathématique Algébrique) and Concordia University for my stay in Montreal. They supported me in various projects, including this one.

References

[1] G. Butler and J. McKay, *The transitive groups of degree up to eleven*, Comm. Algebra **11** (1983), 863–911. MR **84f:**20005

[2] J. H. Conway, A. Hulpke, and J. McKay, *On transitive permutation groups*, J. Comput. Math. **1** (1998), 1–8. CMP 98:15

[3] J. H. Conway and S. P. Norton, *Monstrous moonshine*, Bull. London Math. Soc. **11** (1979), 308–339. MR **81j:**20028

[4] T. Crespo, *Explicit construction of $\widetilde{A}_n$ type fields*, J. Algebra **127** (1989), 452–461; **157** (1993), 283. MR **91a:**12006; MR **94c:**12005

[5] R. Dentzer, *Polynomials with cyclic Galois group*, Comm. Algebra **23** (1995), 1593–1603. MR **96a:**12006

[6] M. Fried and M. Jarden, *Field Arithmetic*, Springer-Verlag, 1986. MR **89b:**12010

[7] F. Heider and P. Kolvenbach, *The construction of $SL(2,3)$-polynomials*, J. Number Theory **19** (1984), 392–411. MR **86g:**11063

[8] G. Malle, *Polynome mit Galoisgruppen* $\mathrm{Pgl}_2(p)$ *und* $\mathrm{Psl}_2(p)$ *üper* $\mathbb{Q}(t)$, Comm. Algebra, **21** (1993), 511–526. MR **94c:**12007

[9] T. Mattman and J. McKay, *Computation of Galois groups over function fields*, Math. Comp., **66** (1997), 823–831. MR **97g:**12003

[10] B. H. Matzat, *Konstruktive Galoistheorie*, Lecture Notes in Math., vol. 1284, Springer-Verlag, 1987. MR **91a:**12007

[11] K.-Y. Shih, *On the construction of Galois extensions of function fields and number fields*, Math. Ann. **207** (1974), 99–120. MR **48:**11051

[12] G. W. Smith, *Generic cyclic polynomials of odd degree*, Comm. Algebra **19** (1991), 3367–3391. MR **93d:**12004

[13] ———, *Generic cyclic polynomials and some applications*, PhD thesis, University of California at Berkeley, 1990.

4408 Upham Court, Ft. Collins, Colorado 80526