ON GALOIS REALIZATIONS OF THE 2-COVERABLE SYMMETRIC AND ALTERNATING GROUPS

DANIEL RABAYEV AND JACK SONN

Abstract. Let \( f(x) \) be a monic polynomial in \( \mathbb{Z}[x] \) with no rational roots but with roots in \( \mathbb{Q}_p \) for all \( p \), or equivalently, with roots mod \( n \) for all \( n \). It is known that \( f(x) \) cannot be irreducible but can be a product of two or more irreducible polynomials, and that if \( f(x) \) is a product of \( m > 1 \) irreducible polynomials, then its Galois group must be “\( m \)-coverable”, i.e. a union of conjugates of \( m \) proper subgroups, whose total intersection is trivial. We are thus led to a variant of the inverse Galois problem: given an \( m \)-coverable finite group \( G \), find a Galois realization of \( G \) over the rationals \( \mathbb{Q} \) by a polynomial \( f(x) \in \mathbb{Z}[x] \) which is a product of \( m \) nonlinear irreducible factors (in \( \mathbb{Q}[x] \)) such that \( f(x) \) has a root in \( \mathbb{Q}_p \) for all \( p \). The minimal value \( m = 2 \) is of special interest. It is known that the symmetric group \( S_n \) is 2-coverable if and only if \( 3 \leq n \leq 6 \), and the alternating group \( A_n \) is 2-coverable if and only if \( 4 \leq n \leq 8 \). In this paper we solve the above variant of the inverse Galois problem for the 2-coverable symmetric and alternating groups, and exhibit an explicit polynomial for each group, with the help of the software packages MAGMA, PARI and GAP.

1. Introduction

Let \( f(x) \) be a monic polynomial in \( \mathbb{Z}[x] \) with no rational roots but with roots in \( \mathbb{Q}_p \) for all \( p \), or equivalently, with roots mod \( n \) for all \( n \). It is known that \( f(x) \) cannot be irreducible but can be a product of two or more irreducible polynomials, and that if \( f(x) \) is a product of \( m > 1 \) irreducible polynomials, then its Galois group must be \( m \)-coverable, i.e. a union of conjugates of \( m \) proper subgroups, whose total intersection is trivial. We are thus led to a variant of the inverse Galois problem: given an \( m \)-coverable finite group \( G \), find a Galois realization of \( G \) over the rationals \( \mathbb{Q} \) by a polynomial \( f(x) \in \mathbb{Z}[x] \) which is a product of \( m \) nonlinear irreducible factors (in \( \mathbb{Q}[x] \)) such that \( f(x) \) has a root in \( \mathbb{Q}_p \) for all \( p \).

The existence of such a polynomial can be established by means of the following proposition.

Proposition 1.1. [6] Let \( K/\mathbb{Q} \) be a finite Galois extension with Galois group \( G \). The following are equivalent:

1. \( K \) is a splitting field of a product \( f(x) = g_1(x) \cdots g_m(x) \) of \( m \) irreducible polynomials of degree greater than one in \( \mathbb{Q}[x] \) and \( f(x) \) has a root in \( \mathbb{Q}_p \) for all primes \( p \).

---

Date: October 21, 2010.

2000 Mathematics Subject Classification. Primary 11R32, Secondary 11Y40; 11R09.

Key words and phrases. Galois group, symmetric group, alternating group, polynomial, roots modulo \( n \).
(2) $G$ is the union of conjugates of $m$ proper subgroups $A_1, \ldots, A_m$, the intersection of all these conjugates is trivial, and for all primes $p$ of $K$, the decomposition group $G(p)$ is contained in a conjugate of some $A_i$.

**Remark.** Condition (2) is evidently satisfied if $G$ is $m$-coverable and all its decomposition groups are cyclic. This last condition holds automatically at all unramified primes.

This remark is used in [6] to prove existence for any $m$-coverable finite solvable group.

The minimal value $m=2$ is of natural interest. All Frobenius groups are 2-coverable. In [6] it is proved that Galois realizations satisfying condition (2) of Prop. 1.1 exist for all nonsolvable Frobenius groups with $m=2$.

In this paper we focus on 2-coverable symmetric and alternating groups, which have been determined in [3] and [4]: $S_n$ is 2-coverable if and only if $3 \leq n \leq 6$, and $A_n$ is 2-coverable if and only if $4 \leq n \leq 8$.

Polynomials for $S_3$ are exhibited in [1]. For $S_4$ and $A_4$ existence follows from the general theorem for solvable groups in [6]. For $S_5$, existence follows from a known quintic (see e.g. [5]). Until now, not even existence was known for $S_6$. In the present paper, with the help of the software packages MAGMA, GAP and PARI, we both prove existence and produce an explicit polynomial for each $S_n$ ($3 \leq n \leq 6$) and each $A_n$ ($4 \leq n \leq 8$):

**Theorem 1.2.** Let $G$ be a 2-coverable group which is either a symmetric group $S_n$ (i.e. $3 \leq n \leq 6$), or an alternating group $A_n$ (i.e. $4 \leq n \leq 8$). Then $G$ is realizable over $\mathbb{Q}$ as the Galois group of a polynomial $f(x)$ which is the product of two (nonlinear) irreducible polynomials in $\mathbb{Q}[x]$, such that $f(x)$ has a root in $\mathbb{Q}_p$ for all primes $p$.

In what follows, we take a group $G \in \{S_4, S_5, S_6, A_4, \ldots, A_8\}$, and a 2-covering of $G$ from [3] or [4], given by two subgroups $U_1, U_2$ of $G$. We then produce a polynomial $f(x) \in \mathbb{Q}[x]$ with Galois group $G$ over $\mathbb{Q}$ which satisfies the condition that for every prime $p$ of the splitting field $K$ of $f(x)$ over $\mathbb{Q}$, the decomposition group $G(p)$ is contained in a conjugate of $U_1$ or $U_2$. We then find two irreducible polynomials $g_1(x), g_2(x) \in \mathbb{Q}[x]$ whose splitting fields are contained in $K$, such that for each $i=1,2$, if $\eta_i \in K$ is a root of $g_i(x)$, then the Galois group of $K$ over $\mathbb{Q}(\eta_i)$ is $U_i$. It then follows that $h(x) = g_1(x)g_2(x)$ has the desired property. The software packages MAGMA, GAP and PARI are used in the searches for $f(x)$ and in the computation of $g_1(x), g_2(x)$.

2. The symmetric groups

$S_4$: The 2-covering of $S_4$ in [3] is given by $U_1 :=$ the stabilizer in $S_4$ of one point and $U_2 :=$ the 2-Sylow subgroup of $S_4$. $U_1$ contains permutations of type $1^2$ [2] and of type $[3]$, and $U_2$ contains permutations of types $[4]$ and $[2,2]$. Since two elements of $S_n$ are conjugate if and only if they are of the same type, $U_1, U_2$ is a 2-covering of $S_4$.

---

1. If $a_1, \ldots, a_k$ are natural numbers, and $\sigma$ is a permutation, then $\sigma$ is of type $[a_1, \ldots, a_k]$ if and only if $\sigma$ is the product of $k$ disjoint cycles of length $a_1, \ldots, a_k$ respectively. In particular, a permutation of type $[n]$ is an $n$-cycle.
Consider the polynomial
\[ f(x) = x^4 - 5x^2 + x + 4 \]
with prime discriminant \( p = 2777 \). \( f(x) \) is irreducible mod 3, factors into the product \((x + 4)(x^3 + 7x^2 + 1)\) of irreducible factors mod 11 and factors into the product \((x + 8)(x + 19)(x^2 + 19x + 20)\) mod 23. These factorizations imply that the Galois group of \( f(x) \) contains a 4-cycle, 3-cycle and a transposition. This implies that the Galois group of \( f(x) \) (over \( \mathbb{Q} \)), which is contained in \( S_4 \), is indeed \( S_4 \).

Let \( K \) be the splitting field of \( f(x) \) over \( \mathbb{Q} \). We will show that for all primes \( p \) of \( K \), the decomposition group \( G(p) \) is cyclic, hence contained in a conjugate of \( U_1 \) or \( U_2 \). The decomposition group of an unramified prime is cyclic, so it is enough to check the ramified primes. If the discriminant of the polynomial is squarefree then the ramified primes are exactly those primes dividing the discriminant of the polynomial, which in our case is a prime \( p = 2777 \).

We shall show that \( G(p) \) is cyclic by showing that the Galois group of \( f(x) \) over \( \mathbb{Q}_p \), which is isomorphic to \( G(p) \), is of order 2. We have the following factorization of \( f(x) \) modulo \( p = 2777 \):
\[
 f(x) \equiv (x + 787)(x + 929)(x + 1919)^2 \pmod{2777}
\]
Applying Hensel’s Lemma we conclude that \( f(x) \) factors into two relatively prime linear factors and one irreducible factor of degree 2 over \( \mathbb{Q}_p \). Indeed, Hensel’s Lemma tells us that \( f(x) \) will factor into two relatively prime linear factors and one factor of degree 2, which must be irreducible since \( f(x) \) is separable over \( \mathbb{Q}_p \) and \( p \) is ramified. This implies that the Galois group of \( f(x) \) over \( \mathbb{Q}_p \) is of order 2.

We now find two irreducible polynomials \( g_1(x), g_2(x) \) of degree greater than 1, such that \( K \) is the splitting field of their product and the groups \( U_1 \) and \( U_2 \) are the Galois groups of \( K \) over the root fields of \( g_1(x) \) and \( g_2(x) \) respectively. Moreover, the polynomial \( g_1(x)g_2(x) \) has a root in \( \mathbb{Q}_p \) for all prime \( p \).

Since \( U_1 \) is the stabilizer of one point, we may take \( g_1(x) := f(x) \).

Since \( U_2 \) is a 2-sylow subgroup of \( S_4 \), we may take \( g_2(x) \) to be the cubic resolvent
\[ g_2(x) = x^3 + 10x^2 + 9x + 1 \]

of \( f(x) \).

In conclusion, the product:
\[
 g_1(x) \cdot g_2(x) = (x^4 - 5x^2 + x + 4)(x^3 + 10x^2 + 9x + 1)
\]
has Galois group \( S_4 \) and has a root in \( \mathbb{Q}_p \) for all prime \( p \).
S_5: The 2-covering of S_5 in [3] is given by U_1 := the stabilizer in S_5 of the set \{1,2\}, and U_2 := the normalizer N_{S_5}(\langle (1,2,3,4,5) \rangle) of \langle (1,2,3,4,5) \rangle in S_5.

\[ f(x) = x^5 - 9x^3 - 9x^2 + 3x + 1 \]

has prime discriminant \( p = 36497 \).

Factoring \( f(x) \) mod 3, mod 17, and mod 103 yields the Galois group S_5.

The factorization of \( f(x) \) modulo \( p \) is

\[ f(x) \equiv (x + 8522)(x + 18488)(x + 19525)(x + 31478)^2 \pmod{36497} \]

so (as in the preceding case) the decomposition group at \( p \) is cyclic.

We now find the desired polynomials \( g_1(x), g_2(x) \). We start with the polynomial \( g_1(x) \) corresponding to the group \( U_1 \), which is the stabilizer in \( S_5 \) of the set \{1,2\}. It is easy to see that \( U_1 = C_2 \times S_3 \), and furthermore, all of the subgroups of \( S_5 \) which are isomorphic to \( C_2 \times S_3 \) are conjugates. Hence we need only find a polynomial whose roots lie in \( K \) and with Galois group \( U_1 \) over its root field. That polynomial is the polynomial whose roots are the sums of pairs of roots of \( f(x) \), namely (using GAP),

\[ g_1(x) = x^{10} - 27x^8 - 9x^7 + 234x^6 + 151x^5 - 756x^4 - 585x^3 + 873x^2 + 660x - 163 \]

Indeed, it is an irreducible polynomial of degree 10 (\( [S_5 : U_1] \)) and according to the previous discussion, it is clear that it has Galois group \( C_2 \times S_3 \) over its root field.

We turn next to the polynomial \( g_2(x) \) corresponding to the group \( U_2 = N_{S_5}(\langle (1,2,3,4,5) \rangle) \). The order of \( U_2 \) is 20, so \( g_2(x) \) will be of degree 6. First, let us notice that up to conjugation, there is only one subgroup of order 20 in \( S_5 \), since every subgroup of order 20 is the normalizer of a 5-cycle. Thus we need only find an irreducible polynomial of degree 6 whose splitting field is contained in \( K \). Our method is ad hoc. Consider the action of \( S_5 \) on the set \( A \) of the ten 2-subsets of \{1,2,3,4,5\}, which is equivalent to its action on the roots of \( g_1(x) \). Then consider the action of \( S_5 \) on the set \( B \) of 252 5-subsets of \( A \). This latter action has an orbit of length 12 (MAGMA). We wish to produce a separable polynomial of degree 252 with splitting field \( K \) such that the action of \( G(K/\mathbb{Q}) \cong S_5 \) on its roots is equivalent to its action on \( B \). We start with

\[ g_1(x) = x^{10} - 27x^8 - 9x^7 + 234x^6 + 151x^5 - 756x^4 - 585x^3 + 873x^2 + 660x - 163 \]

as above which is an irreducible polynomial with Galois group \( S_5 \) over \( \mathbb{Q} \). Using a Tschirnau- sen algorithm\(^2\) in GAP, we obtain a degree 10 polynomial \( g(x) \) the sum of whose roots is zero.

\(^2\)We are grateful to Alexander Hulpke for introducing us to this algorithm in GAP.
and with the same root field (up to conjugacy) as \( g_1(x) \) and such that the polynomial \( h(x) \) of degree 252 whose roots are the sums of quintuples of distinct roots of \( g(x) \), is separable. We now observe that since the sum of the roots of \( g(x) \) is zero, the negative of any root of \( h(x) \) is also a root of \( h(x) \), so \( h(x) = r(t^2) \) for some \( r(t) \in \mathbb{Q}[t] \) of degree 126. \( r(t) \) has an irreducible factor of degree 6 with splitting field contained in \( K \), which is 

\[
g_2(x) = x^6 - \frac{1389834}{26569}x^5 + \frac{804440497905}{705911761}x^4 - \frac{248200341684305820}{18755369578009}x^3 \\
+ \frac{4305380914681123903578}{49831141431812112}x^2 - \frac{3981047272192561628884509657}{1323963596701816063849}x \\
+ \frac{153302536976991922308475759105476}{351763888007705494736404081}
\]

and is therefore a polynomial of the desired type.

\( S_6: \) The 2-covering of \( S_6 \) in [3] is given by \( U_1 := \) the stabilizer in \( S_6 \) of the partition \( \{1,2,3\}, \{4,5,6\} \) and \( U_2 = S_5 \). Note that \( U_1 \) is of order 72 and is also the normalizer of a 3-Sylow subgroup of \( S_6 \).

The polynomial 

\[
f(x) = x^6 - 10x^4 - 9x^3 + 5x^2 + 3x - 1
\]

has prime discriminant \( p = 33994921 \), and factoring mod 13, mod 37, and mod 263 yields the Galois group \( S_6 \).

\[
f(x) \equiv (x + 665896)(x + 3641312)(x + 15713959)(x + 25142575)(x + 11413050)^2 \pmod{p}
\]

so the decomposition group at \( p \) is cyclic (as in the preceding case for \( S_5 \)).

We will now find the polynomials \( g_1(x) \) and \( g_2(x) \). Let us notice that we already have a polynomial for one of the conjugates of the group \( U_2 \), namely \( g_2(x) := f(x) = x^6 - 10x^4 - 9x^3 + 5x^2 + 3x - 1 \), since the Galois group of \( f(x) \) over \( \mathbb{Q}(\theta) \), where \( \theta \) is a root of \( f(x) \), is \( S_5 \).

We now turn to the polynomial \( g_1(x) \) which corresponds to the group \( U_1 \), which is the stabilizer of the partition \( \{1,2,3\}, \{4,5,6\} \). Applying GAP we construct a polynomial \( h(x) \) whose roots are the sums of triples of distinct roots of \( f(x) \):

\[
h(x) = x^{20} - 60x^{18} + 1470x^{16} - 19209x^{14} + 146153x^{12} - 662097x^{10} \\
+ 1751524x^8 - 2532942x^6 + 1684385x^4 - 278413x^2 + 4096.
\]

Observe that \( h(x) = g_1(x^2) \), where

\[
g_1(x) = x^{10} - 60x^9 + 1470x^8 - 19209x^7 + 146153x^6 - 662097x^5 \\
+ 1751524x^4 - 2532942x^3 + 1684385x^2 - 278413x + 4096.
\]

\( g_1(x) \) is irreducible over \( \mathbb{Q} \). It is evident that the splitting field of \( h(x) \) is contained in \( K \), and since \( g_1(x) \) is irreducible over \( \mathbb{Q} \), the splitting field of \( h(x) \) equals \( K \). It is evident that
$h(x)$ has Galois group $S_3 \times S_3$ over $\mathbb{Q}(\eta)$, where $\eta$ is a root of $h(x)$. The root field $\mathbb{Q}(\eta^2)$ of $g_1(x)$ is a subfield of $\mathbb{Q}(\eta)$ of degree 10 over $\mathbb{Q}$, so $\Gamma := G(K/\mathbb{Q}(\eta^2))$ is a subgroup of order 72 of $S_6$, containing $S_3 \times S_3$. $\Gamma$ contains a 3-Sylow subgroup of $S_6$ whose normalizer is of index 1 or 2 in $\Gamma$. It now follows from the Sylow theorems the index must be 1, so $\Gamma$ must be conjugate to $U_1$ in $S_6$. (In fact, every subgroup of $S_6$ of order 72 is conjugate to $U_1$.)

3. The alternating groups

$A_4$: A 2-covering of $A_4$ is given by $U_1 :=$ the stabilizer in $A_4$ of one point, namely, $U_1 = C_3$, and the group $U_2 :=$the 2-sylow subgroup of $A_4$ which is $C_2 \times C_2$. It is evident that this is indeed a 2-covering of $A_4$.

Let

$$f(x) = x^4 - 10x^3 - 7x^2 + 3x + 2.$$ 

The discriminant of $f(x)$ is $163^2$, a square (of a prime), hence the Galois group is contained in $A_4$. Factoring mod 3 and mod 5 gives the Galois group $A_4$.

We check that the Galois group of $f(x)$ over $\mathbb{Q}_p$ is of order 3. The factorization of $f(x)$ factors mod 163 is:

$$f(x) \equiv (x + 50)(x + 143)^3 \pmod{163}$$

By Hensel’s Lemma, $f(x)$ factors into a linear factor and a factor of degree 3 over $\mathbb{Q}_p$, which we claim must be irreducible over $\mathbb{Q}_p$. Indeed, $f(x)$ is separable over $\mathbb{Q}_p$ so this cubic factor is either irreducible as claimed or a product of a linear factor and an irreducible factor of degree 2. In the latter case, $f(x)$ has two relatively prime linear factors which implies that the local Galois group fixes exactly two roots, thus contains a transposition which contradicts the fact that this Galois group is contained in $A_4$. This proves the claim and implies that the Galois group of $f(x)$ over $\mathbb{Q}_p$ is either $S_3$ or $C_3$. The decomposition group cannot be $S_3$ since it is a subgroup of $A_4$ and $A_4$ does not contain a copy of $S_3$, hence we deduce that it is (the cyclic group) $C_3$.

For the polynomials $g_1(x), g_2(x)$, we argue as in the case of $S_4$. Since $U_1$ is the stabilizer of one point, we may take $g_1(x) := f(x)$. Since $U_2$ is a 2-sylow subgroup of $A_4$, we may take $g_2(x)$ to be the cubic resolvent

$$g_2(x) = x^3 + 89x^2 + 2586x + 24649$$

of $f(x)$.

$A_5$: A 2-covering of $A_5$ can be obtained from a 2-covering of $S_5$ and the following easy lemma.
Lemma 3.1. [4]. Let $G$ be a 2-coverable group which is covered by the conjugates of the subgroups $H$ and $K$. If $N \trianglelefteq G$ and $G = NH = NK$, then $N$ admits the covering $H \cap N$, $K \cap N$.

Applying the lemma to the 2-covering of $S_5$ which was given in a previous section, we take $U_1$ to be the intersection of $A_5$ with the stabilizer $\text{Stab}_{S_5}\{1, 2\}$ of the set $\{1, 2\}$ in $S_5$, and $U_2 = N_{S_5}\{(1, 2, 3, 4, 5)\} \cap A_5$. As $S_5 = N_{S_5}\{(1, 2, 3, 4, 5)\} \cdot A_5 = \text{Stab}_{S_5}\{1, 2\} \cdot A_5$, $\{U_1, U_2\}$ is a 2-covering of $A_6$.

$$f(x) = x^5 - 5x^4 - 7x^3 + 18x^2 - x - 1$$

with discriminant $15733^2$, the square of a prime.

Factoring mod 3, mod 5, and mod 7 yields the Galois group $A_5$, and factoring mod the discriminant $f(x) \equiv (x + 13759)(x + 4886)(x + 4272)^3 \pmod{15733}$, an argument similar to the case of $A_4$ yields cyclic decomposition groups.

We turn now to the polynomials $g_1(x), g_2(x)$. From here the proof is similar to the case of $S_5$. The indices of $U_1$ and $U_2$ in $A_5$ are 10 and 6 respectively. Furthermore, each $U_i$ is the unique subgroup of order $|U_i|$ in $A_5$ up to conjugacy, $i = 1, 2$. By the same method as in the case of $S_5$, starting with $f(x)$, we compute

$$g_1(x) = x^{10} - 20x^9 + 129x^8 - 167x^7 - 1160x^6 + 3139x^5 + 2214x^4 - 9559x^3 + 1089x^2 + 5486x - 461$$

and

$$g_2(x) = x^6 - \frac{42323896}{212521}x^5 + \frac{733217461235730}{45165175441}x^4 - \frac{6645087421265775407450}{9598548249896761}x^3 + \frac{86429398882716670964952901401177395}{433520115685490720702646601}x^2 - \frac{9171516822801665361140634800285822768801}{92132128505596173454447158291121}.$$ 

$A_6$: In contrast to the previous examples, in this example not all the decomposition groups turn out to be cyclic. The 2-covering of $A_6$ is given by applying the lemma from the previous section to the 2-covering of $S_6$ which was given earlier. Namely, $U_1 = H_1 \cap A_6$, where $H_1$ denotes the stabilizer in $S_6$ of the partition $\{1, 2, 3\}, \{4, 5, 6\}$ and $U_2 = H_2 \cap A_6 = A_5$ where $H_2 = S_5$. ($S_6 = A_6H_1 = A_6H_2$ because $U_1$ and $U_2$ each contains an odd permutation.)

$$f(x) = x^6 - 3x^5 - 4x^4 + 5x^3 + 3x^2 - 5x - 1,$$
with discriminant $14341^2$, the square of a prime. Factoring mod 3, mod 5, and mod 101 yields the Galois group $A_6$.

In order to verify that the requirements hold, we need the decomposition group of a prime above $p = 14341$ to be contained in a conjugate of $U_1$ or $U_2$.

We claim that the Galois group of $f(x)$ over $\mathbb{Q}_p$ is contained in a conjugate of $U_2$. $f(x)$ factors mod $p$ as a product of two distinct linear factors and the square of an irreducible quadratic factor:

$$f(x) \equiv (x + 5464)(x + 5605)(x^2 + 8805x + 9098)^2 \pmod{14341}$$

By Hensel’s Lemma, $f(x)$ factors into two relatively prime linear factors and one irreducible factor of degree 4 over $\mathbb{Q}_p$. This means that the decomposition group, which is contained in $A_6$, fixes two roots of $f(x)$, and is therefore contained in a conjugate of $A_6 = U_2$. Note that the decomposition group is noncyclic, since its order is divisible by 4 and is embedded in $A_4$.

We turn to the polynomials $g_1(x)$ and $g_2(x)$. First, as $U_2 = A_5$, we may take $g_2(x) = f(x) = x^6 - 3x^5 - 4x^4 + 5x^3 + 3x^2 - 5x - 1$. By the same method used for $S_6$, we arrive at the polynomial

$$g_1(x) = x^{10} - \frac{93}{2}x^9 + \frac{14253}{16}x^8 - \frac{75007}{8}x^7 + \frac{7698057}{128}x^6 - \frac{62688663}{256}x^5 + \frac{1276887561}{2048}x^4 - \frac{1886832143}{2048}x^3 + \frac{45377978093}{65536}x^2 - \frac{33044483389}{131072}x + \frac{1696039489}{1048576}$$

$A_7$: The 2-covering of $A_7$ given in [4] is $U_1 = N_{A_7}(\langle 123456 \rangle)$, of order 21, and $U_2 = (\text{Sym}\{1,2\} \times \text{Sym}\{3,4,5,6,7\})\cap A_7$, of order 120, where $\text{Sym}\{1,2\}$ is the symmetric group on $\{1,2\}$ and $\text{Sym}\{3,4,5,6,7\}$ is the symmetric group on $\{3,4,5,6,7\}$.

$$f(x) = x^7 - 2x^6 - 5x^5 - x^4 - 3x^3 - x^2 - x - 5$$

with discriminant $554293^2$, the square of a prime. The factorizations of $f(x)$ modulo 3, 5, 7, 23 show that the Galois group contains permutations of the types $[7],[5],[2,4],[3,3]$ respectively. As $A_7$ has no proper subgroup of order divisible by $3 \cdot 4 \cdot 5 \cdot 7$ (GAP), the Galois group is $A_7$.

We show next that the Galois group of $f(x)$ over $\mathbb{Q}_p$ is contained in a conjugate of $U_2$, where $p = 554293$ is the unique ramified prime. The factorization of $f(x)$ modulo $p$ is

$$f(x) \equiv (x + 521396)(x + 134869)(x + 281696)^2(x^2 + 308251x + 256808) \pmod{554293}.$$ 

Applying Hensel’s Lemma we conclude that $f(x)$ factors into a (separable) product of a linear factor and quadratic factors over $\mathbb{Q}_p$. It follows that the decomposition group $G(p)$ is a 2-group. But this means that the decomposition group is contained in a conjugate of $U_2$ since $U_2$ contains a 2-Sylow subgroup of $A_7$.

For the explicit polynomials $g_1(x), g_2(x)$, we start with $g_1(x)$ and observe first that $U_1$ is not a maximal subgroup of $A_7$. It is contained in a maximal subgroup of order 168, isomorphic to $GL_3(2)$. Although the unique conjugacy class of subgroups of order 168 in $S_7$ splits into
two conjugacy classes in $A_7$, each contains the unique conjugacy class of subgroups of order 21 in $A_7$. It follows that either of the two conjugacy classes of subgroups of order 168 in $A_7$ can replace the conjugacy class of $U_1$ in the given 2-covering of $A_7$. It is advantageous to do this in order to seek a $g_1(x)$ of smaller degree (15) than that of the $g_1(x)$ (120) that would correspond to the original $U_1$. The method for seeking the explicit $g_1(x)$ and $g_2(x)$ is similar to the preceding, except for a greater dependence on trial and error, and that in addition to the two algorithms in GAP used earlier, the Tschirnhausen algorithm and the algorithm that produces a polynomial whose roots are sums of roots of a given polynomial, an algorithm that produces a polynomial whose roots are products of roots of a given polynomial was pressed into service.

The polynomials corresponding to the groups $U_1$ and $U_2$ are:

$$g_1(x) = x^{15} + \frac{236441}{835}x^{14} - \frac{553005}{3796}x^{13} - \frac{142958}{2413}x^{12} + \frac{3151297}{45345}x^{11} - \frac{5686331}{48267}x^{10} + \frac{30589}{7924}x^9 + \frac{10004127}{37216}x^8 - \frac{255049}{586}x^7 - \frac{41630007}{36825}x^6 + \frac{72184440}{8779}x^5 - \frac{45952163}{3584}x^4 - \frac{1964679}{5883}x^3 + \frac{14351259}{5423}x^2 - \frac{3135356}{2567}x - \frac{791507}{457}$$

$$g_2(x) = x^{21} - 30x^{20} + 395x^{19} - 2937x^{18} + 12917x^{17} - 29077x^{16} - 6543x^{15} + 236441x^{14} - 553005x^{13} - 142958x^{12} + 3151297x^{11} - 5686331x^{10} + 305889x^9 + 10004127x^8 - 255049x^7 - 416300022x^6 + 72184440x^5 - 45952163x^4 - 1964679x^3 + 14351259x^2 - 3135356x - 791507$$

respectively.

$A_8$: The 2-covering of $A_8$ in [4] is given by $U_1$ := the affine linear group on $F_2^3$ acting as permutations on the 8 points of this space (shown to be embedded into $A_8$), isomorphic to $F_2^3 \times GL_3(F_2)$, of index 15, and $U_2 := [Sym\{1, 2, 3\} \times Sym\{4, 5, 6, 7, 8\}] \cap A_8$, of index 56.

$$f(x) = x^8 - x^7 - 2x^6 - x^5 + 3x^4 + 3x^3 + 2x^2 + x + 1$$

with discriminant 11489, the square of a prime. The factorizations of $f(x)$ modulo 3, 37, 41 show that the Galois group contains permutations of the types [7], [4,4], [3,5] respectively. As $A_8$ has no proper subgroup of order divisible by 3·4·5·7 (GAP), the Galois group is $A_8$.

Now $f(x)$ factors modulo $p$ as:

$$f(x) \equiv (x + 1440)^3(x^2 + 10435x + 8884)(x^3 + 8222x^2 + 9218x + 10584) \pmod{11489}$$

Hensel's Lemma yields a corresponding factorization $f(x) = a(x)b(x)c(x)$ over $\mathbb{Q}_p$ with $a(x), c(x)$ of degree 3 and $b(x)$ of degree 2. The splitting field $K_p$ of $f(x)$ over $\mathbb{Q}_p$ is the composite of the splitting fields $K_a, K_b, K_c$ of these three factors, the first of which is ramified and the others unramified. $a(x)$ cannot be a product of linear factors since $p$ ramifies in the splitting field of $f(x)$. Thus $a(x)$ is either an irreducible cubic or a product of a linear and a quadratic polynomial. $b(x)$ and $c(x)$ are irreducible. If $a(x)$ is a product of a linear and a quadratic polynomial, then $K_a/\mathbb{Q}_p$ is a ramified quadratic extension and
G(K_p/Q_p) \cong C_2 \times C_2 \times C_3, and contains transpositions, contrary to the fact that it is contained in A_8. Therefore a(x) is an irreducible cubic. It follows that G(K_a/Q_p) is C_3 or S_3. C_3 is not possible because K_a/Q_p would then be totally and tamely ramified, but p \equiv 2 (mod 3) hence Q_p does not contain the cube roots of unity. Hence G(K_a/Q_p) is S_3. The only way that G(K_p/Q_p) can be contained in A_8 is if K_a is contained in K as the unramified quadratic subfield, and the action of G(K_a/Q_p) on the roots of a(x)b(x) is the representation of S_3 as \langle (123), (12)(45) \rangle. Furthermore, since K_c/Q is unramified of degree 3, K_a \cap K_c = Q_p, so G(K_p/Q_p) acts on the roots of f(x) as \langle (123), (12)(45), (678) \rangle, which is contained in U_2.

A trial and error search similar to that in the preceding section yields the following polynomials corresponding to the groups U_1 and U_2:

\[ g_1(x) = x^{15} - \frac{95}{2}x^{14} + \frac{3197}{4}x^{13} - \frac{21045}{32}x^{12} + \frac{743376}{296}x^{11} + \frac{22263473}{296}x^{10} - \frac{104363621}{512}x^9 \]
\[ -\frac{11710437647}{4096}x^8 + \frac{91829493277}{65536}x^7 + \frac{5512442410853}{131072}x^6 - \frac{21829527485865}{2048}x^5 + \frac{41094846145887}{32768}x^4 \]
\[ -\frac{1473790323407302}{16777216}x^3 + \frac{27794916917292379}{8388608}x^2 - \frac{3186512611918869}{491520}x - \frac{1256672780150964253}{134217728} \]

and

\[ g_2(x) = x^{56} - 21x^{55} + 180x^{54} - 735x^{53} + 783x^{52} + 5407x^{51} - 21690x^{50} + 6260x^{49} + 134354x^{48} \]
\[ -256270x^{47} + 304036x^{46} + 1275397x^{45} + 942277x^{44} - 6877457x^{43} - 2069019x^{42} + 42340751x^{41} \]
\[ -37776712x^{40} + 158592858x^{39} + 37918883x^{38} + 107601914x^{37} + 145543481x^{36} + 1392744196x^{35} \]
\[ +285490625x^{34} - 7385711268x^{33} + 817821146x^{32} + 17194579246x^{31} - 19188201050x^{30} \]
\[ -18578454420x^{29} + 56645526134x^{28} - 18919098068x^{27} - 77381156815x^{26} + 94740276783x^{25} \]
\[ +3058706228x^{24} - 150642640537x^{23} + 94400959739x^{22} + 77653585985x^{21} - 155812844138x^{20} \]
\[ +65943540240x^{19} + 68936866008x^{18} - 12163433784x^{17} + 85946585602x^{16} - 14385996295x^{15} \]
\[ -5212160988x^{14} + 76576460155x^{13} - 37676127233x^{12} - 34141244957x^{11} + 8269230483x^{10} \]
\[ -86059996214x^9 + 64840424670x^8 - 43929749632x^7 + 29390580877x^6 - 17890022300x^5 \]
\[ +8764351999x^4 - 3189669694x^3 + 811672328x^2 - 129075408x + 9546832 \]

respectively.

**References**
