A linear resolvent for degree 14 polynomials

Chad Awtrey and Erin Strosnider

Abstract We discuss the construction and factorization pattern of a linear resolvent polynomial that is useful for computing Galois groups of degree 14 polynomials. As an application, we develop an algorithm for computing the Galois group of a degree 14 polynomial defined over the 7-adic numbers. This algorithm is of interest since it only makes use of the aforementioned linear resolvent, the polynomial's discriminant, and subfield information of the polynomial's stem field.

1 Introduction

Let p be a prime number. An important problem in computational number theory is to determine the Galois group of an irreducible polynomial f defined over the field of p-adic numbers $\mathbf{Q}_p$. If the degree of f is either equal to p or is not a multiple of p, then it is straightforward to compute the Galois group of f (see for example [1, 11]). Otherwise, the situation is more complicated, with no practical general algorithm currently available. However, several researchers have developed ad hoc techniques that depend on both the degree of f and the prime p ([2, 3, 4, 5, 6, 7, 10, 11, 12]).

In this paper, we focus on determining the Galois group G when the degree of f is 14 and $p = 7$ (lower degrees have already been treated). Since the elements of G act as permutations on the roots of f, once we fix an ordering on the roots, G can be be considered as a subgroup of S_{14}, well-defined up to conjugation (different orderings correspond to conjugates of G). Since f is irreducible, G is a transitive subgroup of S_{14}; i.e., there is a single orbit for the action of G on the roots of f (each orbit corresponds to an irreducible factor of f). Therefore our aim is to identify G

Chad Awtrey
Elon University, Campus Box 2320, Elon, NC 27244 e-mail: cawtrey@elon.edu

Erin Strosnider
Elon University, Campus Box 2320, Elon, NC 27244 e-mail: estrosnider@elon.edu

among the 63 transitive subgroups of S_{14}, following the naming convention that is implemented in [9].

All permutation group computations described in this paper were performed with [9], making extensive use of its transitive group data library. In particular, GAP contains all relevant data concerning transitive groups of S_{14} needed for our work. The reliability of GAP in this context is supported by the fact that its transitive group data library was authored by Alexander Hulpke, a leading researcher in computational group theory.

The remainder of the paper is structured as follows. Section 2 introduces the basic properties of ramification groups to give structural information on possible Galois groups over $\mathbf{Q}_p$. As a consequence of this section, we will show that only 14 of the 63 transitive subgroups of S_{14} are candidates for Galois groups of degree 14 polynomials over $\mathbf{Q}_7$. The goal then becomes to compute enough invariants to uniquely identify the Galois group from among these 14 possibilities. In Section 3, we introduce three invariants associated to a polynomial's stem field; namely, the size of its automorphism group, its discriminant, and the Galois groups of its proper, nontrivial subfields. These invariants are enough to distinguish 5 of the 14 possible cases. In the final section, we introduce a linear resolvent polynomial that is able to distinguish the remaining 9 cases. Since the number of isomorphism classes of degree 14 extensions of $\mathbf{Q}_7$ is finite [13, p.54], it is possible to compute a defining polynomial for each extension and implement our algorithm to compute the polynomial's Galois group. We have carried out this computation, and our results are summarized in Table 1; the final column lists the number of extensions by Galois group.

2 Ramification Groups

The aim of this section is to introduce the basic properties of ramification groups (over general p-adic fields) and use those to deduce structural information about degree 14 extensions of $\mathbf{Q}_7$. A more detailed exposition can be found in [17].

Definition 1. Let $L/\mathbf{Q}_p$ be a Galois extension with Galois group G. Let v be the discrete valuation on L and let $\mathbf{Z}_L$ denote the corresponding discrete valuation ring. For an integer $i \geq -1$, we define the **i-th ramification group** of G to be the following set

$$G_i = \{\sigma \in G : v(\sigma(x) - x) \geq i + 1 \text{ for all } x \in \mathbf{Z}_L\}.$$

The ramification groups define a sequence of decreasing normal subgroups which are eventually trivial and which give structural information about the Galois group of a p-adic field.

Lemma 1. *Let $L/\mathbf{Q}_p$ be a Galois extension with Galois group G, and let G_i denote the i-th ramification group. Let $\mathfrak{p}$ denote the unique maximal ideal of $\mathbf{Z}_L$ and U_0 the units in L. For $i \geq 1$, let $U_i = 1 + \mathfrak{p}^i$.*

(a) For $i \geq 0$, G_i/G_{i+1} is isomorphic to a subgroup of U_i/U_{i+1}.
(b) The group G_0/G_1 is cyclic and isomorphic to a subgroup of the group of roots of unity in the residue field of L. Its order is prime to p.
(c) The quotients G_i/G_{i+1} for $i \geq 1$ are abelian groups and are direct products of cyclic groups of order p. The group G_1 is a p-group.
(d) The group G_0 is the semi-direct product of a cyclic group of order prime to p with a normal subgroup whose order is a power of p.
(e) The groups G_0 and G are both solvable.

A proof can be found in [17, §IV].

Specializing to the case where L is the splitting field of an irreducible degree 14 polynomial defined over $\mathbf{Q}_7$, we see that G is a solvable transitive subgroup of S_{14}; of which there are 36. Furthermore, G contains a solvable normal subgroup G_0 such that G/G_0 is cyclic. The group G_0 contains a normal subgroup G_1 such that G_1 is a 7-group (possibly trivial). Moreover, G_0/G_1 is cyclic of order dividing $7^{[G:G_0]} - 1$. Direct computation on the 36 candidates shows that only 20 are possible Galois groups.

For each of these 20 groups, consider all index 3 subgroups (if there are any); the index 3 subgroups correspond to cubic subfields of L. Now for each such subgroup H, consider the permutation representation of G acting on the cosets of H in G, which is isomorphic to the Galois group of the corresponding cubic subfield. Since all cubic extensions of $\mathbf{Q}_7$ are cyclic (cf. [11]), we can rule out those groups from among the 20 that exhibit an S_3 permutation representation; there are 6 such groups.

Thus, there are 14 possible Galois groups of degree 14 polynomials over $\mathbf{Q}_7$. We identify these groups in the table below using the transitive numbering system in [9]. The second column gives an alternate naming scheme, which is also implemented in `GAP`. Later in the paper, we will reference these groups using only their first column identification.

14T1	C_{14}
14T2	D_7
14T3	D_7C_2
14T4	$2[1/2]F_{42}(7)$
14T5	$F_{21}C_2$
14T7	$F_{42}C_2$
14T8	$C_7 \wr C_2$
14T12	$1/2[D(7)^2]2$
14T13	$[1/2.D(7)^2]2$
14T14	$[7^2:3]2$
14T20	$D_7 \wr C_2$
14T23	$[1/6_+.F_{42}^2]2_2$
14T24	$[7^2:6]2$
14T32	$[D(7)^2:3]2$

3 Stem Field Invariants

As before, let f be a degree 14 polynomial defined over $\mathbf{Q}_7$, and let G be its Galois group. Our aim in this section is to introduce three field-theoretic invariants, related to the stem field of f, that will aid in our computation of G.

First, we consider the stem field of f and its corresponding subgroup H (under the Galois correspondence). Thus H is isomorphic to $G \cap S_{13}$, the point stabilizer of 1 in G. By Galois theory, the automorphism group of the stem field is therefore isomorphic to $N(H)/H$ (where $N(H)$ represents the normalizer of H in G), which is in turn isomorphic to the centralizer of G in S_{14}. In our work, we make use of the size of the automorphism group of the stem field of f, which is equal to the order of the centralizer in S_{14} of G.

Another invariant we employ is related to the discriminant of f. We say the parity of the polynomial f is $+1$ if the discriminant of f is a square in $\mathbf{Q}_7$; otherwise, the parity is -1. On the group theory side, the parity of a polynomial's Galois group is $+1$ if $G \subseteq A_{14}$ and -1 otherwise.

The third invariant we consider is related to the list of the Galois groups of the Galois closures of the proper nontrivial subfields (up to isomorphism) of the stem field of f. We call this the *subfield Galois group* content of f, and we denote it by $sgg(f)$.

Example 1. For example, consider the polynomial $x^{14}+2x^2-2x+3$, which defines the unique unramified degree 14 extension of $\mathbf{Q}_7$. Thus the Galois group G of this polynomial is cyclic of order 14. Since the transitive group notation in [9] lists cyclic groups first, the T-number of G is 14T1. By the fundamental theorem of Galois theory, since G has a unique cyclic subgroup for every divisor of its order, the stem field of f has unique subfields of degrees 2 and 7. These subfields define the unique unramified extensions of $\mathbf{Q}_7$ of their respective degrees, and therefore their Galois groups are also cyclic. Thus the *sgg* content of f is $\{2\text{T}1, 7\text{T}1\}$.

In general, to compute the *sgg* content of a polynomial f, we can make use of the complete lists of quadratic and septic 7-adic fields determined in [11] (these lists include defining polynomials along with their Galois groups). For each polynomial in these lists, we can use Panayi's p-adic root-finding algorithm [14, 16] to test if the polynomial has a root in the field defined by f. If it does, then this polynomial defines a subfield of the field defined by f. Continuing in this way, it is straightforward to compute the *sgg* content of f.

The process of employing the *sgg* content of a polynomial to identify its Galois group is justified by the following result.

Proposition 1. *The sgg content of a polynomial is an invariant of its Galois group (thus it makes sense to speak of the sgg content of a transitive group).*

Proof. Suppose the polynomial f defines an extension L/K of fields, and let G denote the Galois group of f. Let E be the subgroup fixing L/K, arising from the Galois correspondence. The nonisomorphic subfields of L/K correspond to the intermediate subgroups F, up to conjugation, such that $E \leq F \leq G$. Furthermore, if

K' is a subfield and F is its corresponding intermediate group, then the Galois group of the normal closure of K' is equal to the permutation representation of G acting on the cosets of F in G. Consequently, every polynomial with Galois group G must have the same subfield content, and this quantity can be determined by a purely group-theoretic computation. □

For each of the 14 possible Galois groups of degree 14 extensions of $\mathbf{Q}_7$, Table 1 shows their respective data for centralizer order, parity, and *sgg* content, with the groups sorted based on their corresponding characteristics. Notice that these three invariants are enough to uniquely identify the five Galois groups 14T1, 14T2, 14T3, 14T5, and 14T8. The final column in the table shows the number of isomorphism classes of degree 14 extensions of $\mathbf{Q}_7$ that have the corresponding group as the Galois group of their normal closure. Note, defining polynomials for these extensions can be computed with a built-in command in [15] (there are a total of 654 such extensions).

To distinguish between the remaining 9 Galois groups, we make use of a linear resolvent (in the sense of [18]).

4 A Linear Resolvent

We begin with a definition of a general resolvent polynomial.

Definition 2. Let $T(x_1,\ldots,x_{14})$ be a polynomial with integer coefficients. Let H be the stabilizer of T in S_{14}. That is,

$$H = \left\{\sigma \in S_{14} \colon T(x_{\sigma(1)},\ldots,x_{\sigma(14)}) = T(x_1,\ldots,x_{14})\right\}.$$

We define the **resolvent polynomial** $R_{f,T}(x)$ of the polynomial $f(x) \in \mathbf{Z}[x]$ by

$$R_{f,T}(x) = \prod_{\sigma \in S_{14}/H} \left(x - T(r_{\sigma(1)},\ldots,r_{\sigma(14)})\right),$$

where S_{14}/H is a complete set of right coset representatives of S_{14} modulo H and where $r_1,\ldots,r_{14}$ are the roots of $f(x)$. By Galois theory, $R_{f,T}(x)$ also has integer coefficients.

The main theorem concerning resolvent polynomials is the following. A proof can be found in [18].

Theorem 1. *With the notation of the preceding definition, set $m = [S_{14} \colon H] = deg(R_{f,T})$. If $R_{f,T}$ is squarefree, its Galois group (as a subgroup of S_m) is equal to $\phi(G)$, where ϕ is the natural group homomorphism from S_{14} to S_m given by the natural right action of S_{14} on S_{14}/H. Note that we can always ensure R is squarefree by taking a suitable Tschirnhaus transformation of f [8, p. 318].*

As a consequence, this theorem implies that the list of degrees of irreducible factors of $R_{f,T}$ is the same as the length of the orbits of the action of $\phi(G)$ on the set $[1,\ldots,m]$. In particular, the Galois group of an irreducible factor of $R_{f,T}$ can be determined by a purely group-theoretic computation.

Our linear resolvent is constructed as follows. Let $T(x_1,\ldots,x_{14}) = x_1+x_2$, which is stabilized by the subgroup $H \simeq S_2 \times S_{12}$ and which is generated by the following three permutations,

$$(1,2),(3,4),(3,4,5,6,7,8,9,10,11,12,13,14).$$

Since $[S_{14} : H] = 91$, the corresponding resolvent polynomial, which we denote by F_{91}, has degree 91, and it can be computed by,

$$F_{91}(x) = \prod_{i=1}^{13}\prod_{j=2}^{14}(x-r_i-r_j),$$

where r_i are the roots of the degree 14 polynomial f. However, since T is linear, it can also be computed as a resultant (as in [18]). In particular, let

$$g(x) = \text{Resultant}_y(f(y), f(x+y))/x^{14}.$$

Then $F_{91}(x) = g(\sqrt{x})$.

The list of the irreducible factors of F_{91} is enough to distinguish 4 of the 9 remaining Galois groups (14T4, 14T7, 14T12, and 14T23), as seen in Table 1. For the remaining 5 cases, we note that F_{91} has a unique irreducible factor of degree 49. It turns out that if we consider Galois groups of septic subfields of the stem field of this degree 49 factor, then this information is enough to distinguish between the remaining Galois groups.

Acknowledgements The authors would like to thank Elon University for supporting this project through internal grants and the Center for Undergraduate Research in Mathematics for their grant support.

References

1. Shigeru Amano, *Eisenstein equations of degree p in a* $\mathfrak{p}$*-adic field*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **18** (1971), 1–21. MR MR0308086 (46 #7201)
2. Chad Awtrey, *Dodecic 3-adic fields*, Int. J. Number Theory **8** (2012), no. 4, 933–944. MR 2926553
3. _____, *Masses, discriminants, and Galois groups of tame quartic and quintic extensions of local fields*, Houston J. Math. **38** (2012), no. 2, 397–404. MR 2954644
4. Chad Awtrey, Nicole Miles, Jonathan Milstead, Christopher R. Shill, and Erin Strosnider, *Degree 14 2-adic fields*, Involve.
5. Chad Awtrey, Nicole Miles, Christopher R. Shill, and Erin Strosnider, *Computing Galois groups of degree 12 2-adic fields with trivial automorphism group*, submitted.
6. _____, *Degree 12 2-adic fields with automorphism group of order 4*, submitted.

Table 1 Invariant data for transitive subgroups of S_{14} that can occur as the Galois group of a degree 14 polynomial defined over $\mathbf{Q}_7$. The column **CentOrd** gives the order of the group's centralizer in S_{14}, **Parity** indicates whether the group is even $(+1)$ or not (-1), and **SGG** gives the *sgg* content of the group. The column $\mathbf{F_{91}}$ gives the degrees of the irreducible factors of the linear resolvent F_{91}. When F_{91} has a unique factor of degree 49, **Septics** gives the Galois groups of all septic subfields of the stem field of this degree 49 factor. The final column gives the number of isomorphism classes of degree 14 extensions of $\mathbf{Q}_7$ whose normal closures have the corresponding Galois group.

G	CentOrd	Parity	SGG	$\mathbf{F_{91}}$	Septics	#
14T1	14	-1	2T1,7T1	$7, 14^6$		24
14T2	14	-1	2T1,7T2	$7^7, 14^3$		3
14T8	7	-1	2T1	$14^3, 49$	7T1,7T2	72
14T3	2	-1	2T1,7T2	$7, 14^6$		6
14T5	2	-1	2T1,7T3	$7, 42^2$		24
14T4	2	-1	2T1,7T4	$7, 21^2, 42$		31
14T7	2	-1	2T1,7T4	$7, 42^2$		62
14T12	1	$+1$	2T1	$14^3, 49$	none	8
14T23	1	$+1$	2T1	$42, 49$	none	64
14T13	1	-1	2T1	$14^3, 49$	7T2,7T2	9
14T20	1	-1	2T1	$14^3, 49$	none	16
14T14	1	-1	2T1	42,49	7T3,7T4	93
14T24	1	-1	2T1	42,49	7T4,7T4	114
14T32	1	-1	2T1	42,49	none	128

7. Chad Awtrey and Christopher R. Shill, *Galois groups of degree 12 2-adic fields with automorphism group of order 6 and 12*, Topics from the 8th Annual UNCG Regional Mathematics and Statistics Conference **64** (2013), 55–65.
8. Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993. MR 1228206 (94i:11105)
9. The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, 2008.
10. John W. Jones and David P. Roberts, *Nonic 3-adic fields*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 293–308. MR MR2137362 (2006a:11156)
11. ———, *A database of local fields*, J. Symbolic Comput. **41** (2006), no. 1, 80–97. MR 2194887 (2006k:11230)
12. ———, *Octic 2-adic fields*, J. Number Theory **128** (2008), no. 6, 1410–1429. MR MR2419170 (2009d:11163)
13. Serge Lang, *Algebraic number theory*, second ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994. MR 1282723 (95f:11085)
14. Peter Panayi, *Computation of leopoldt's p-adic regulator*, Ph.D. thesis, University of East Anglia, December 1995.
15. PARI Group, The, *PARI/GP – Computational Number Theory, version 2.3.4*, 2008, available from `http://pari.math.u-bordeaux.fr/`.
16. Sebastian Pauli and Xavier-François Roblot, *On the computation of all extensions of a p-adic field of a given degree*, Math. Comp. **70** (2001), no. 236, 1641–1659 (electronic). MR 1836924 (2002e:11166)
17. Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg. MR 554237 (82e:12016)
18. Leonard Soicher and John McKay, *Computing Galois groups over the rationals*, J. Number Theory **20** (1985), no. 3, 273–281. MR MR797178 (87a:12002)