

ON GALOIS GROUPS OF DEGREE 15 POLYNOMIALS

Chad Awtrey¹ §Mazur², Sara Rodgers³, Nicole Soltz⁴, Jesi Weed⁵

^{1,2,3,4,5}Department of Mathematics and Statistics

Elon University

Campus Box 2320, Elon, NC 27244, USA

Abstract: We discuss the construction and factorization pattern of several resolvent polynomials that are useful for computing Galois groups of degree 15 polynomials. As an application, we develop an algorithm for computing the Galois group of a degree 15 polynomial defined over the 5-adic numbers. This algorithm is of interest since it uses substantially fewer resolvents than the traditional method for computing Galois groups.

AMS Subject Classification: 11S15, 11S20

Key Words: 5-adic, extension fields, Galois group, local 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, 12]). 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, 11, 12, 13]).

Received: July 19, 2015

© 2015 Academic Publications, Ltd.
url: www.acadpubl.eu

§Correspondence author

In this paper, we focus on determining the Galois group G when the degree of f is 15 and $p = 5$ (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 considered a subgroup of S_{15} , well-defined up to conjugation (different orderings correspond to conjugates of G). Since f is irreducible, G is a transitive subgroup of S_{15} ; 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 among the 104 transitive subgroups of S_{15} , 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_{15} needed for our work.

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 24 of the 104 transitive subgroups of S_{15} are candidates for Galois groups of degree 15 polynomials over \mathbf{Q}_5 . These groups are listed in Table 1. The goal then becomes to compute enough invariants to uniquely identify the Galois group from among these 24 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 6 of the 24 possible cases. In the next section, we introduce three resolvent polynomials that are able to distinguish the remaining 18 cases. Table 2 contains information about these invariants.

Since the number of isomorphism classes of degree 15 extensions of \mathbf{Q}_5 is finite [14, p.54], it is possible to compute a defining polynomial for each extension and implement our algorithm to compute the polynomial's Galois group. In the final section, we have included such data in the cases where the Galois group is among the set $\{T1, T2, T3, T4, T6, T7, T8\}$ (see Table ?? for a summary). These results comprise 39 of the 1012 extensions and are contained in Tables 3 and 4. Data for the remaining cases is available by emailing the first author.

Table 1: The 24 transitive subgroups of S_{15} that are possible Galois groups of degree 15 polynomials defined over \mathbf{Q}_5 . The groups are ordered by **Size**. Included are their transitive number **T** and descriptive name **Name** (as listed in **GAP**).

T	Name	Size
1	$C(15) = 5[x]3$	15
2	$D(15)$	30
3	$D(5)[x]3$	30
4	$5[x]S(3)$	30
6	$F(5)[1/2]S(3)$	60
7	$D(5)[x]S(3)$	60
8	$F(5)[x]3$	60
9	$[5^2]3$	75
11	$F(5)[x]S(3)$	120
12	$[5^2 : 2]3$	150
13	$[5^2]S(3)$	150
14	$5^2 : 2[1/2]S(3)$	150
17	$1/2[5^2 : 4]S(3)$	300
18	$[5^2 : 2]S(3)$	300
19	$[5^2 : 4]3$	300
25	$[5^3]3 = 5wr3$	375
27	$[5^2 : 4]S(3)$	600
30	$[5^3 : 2]3$	750
31	$1/2[5^3 : 2]S(3)$	750
32	$[5^3]S(3)$	750
37	$1/2[5^3 : 4]S(3)$	1500
40	$[5^3 : 2]S(3)$	1500
49	$[5^3 : 4]S(3)$	3000

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 15 extensions of \mathbf{Q}_5 . A more detailed exposition can be found in [18].

Definition 2.1. 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

Table 2: Invariant data for transitive subgroups of S_{15} that can occur as the Galois group of a degree 15 polynomial defined over \mathbf{Q}_5 . The column $[\mathbf{N}(\mathbf{H}) : \mathbf{H}]$ gives the index of a point stabilizer of the group inside its normalizer; this quantity corresponds to the size of the automorphism group of the defining polynomial’s stem field. **Parity** indicates whether the group is even (+) or not (–), and **SGG** gives the *sgg* content of the group. The columns **F₁₀₅**, **F₄₅₅**, and **F₂₁₀** give the degrees of the irreducible factors of the corresponding resolvent polynomials; degrees occurring more than once are listed with superscripts (so an entry including 15^2 means the resolvent has two factors of degree 15). Resolvent data that is not needed is not included.

T	Parity	$[\mathbf{N}(\mathbf{H}) : \mathbf{H}]$	sgg	F ₁₀₅	F ₄₅₅	F ₂₁₀
1	+	15	3T1,5T1			
4	–	5	3T2,5T1			
9	+	5	3T1	$15^2, 75$	$15^2, 25^5, 75^4$	
25	+	5	3T1	$15^2, 75$	$15^2, 75^4, 125$	
13	–	5	3T2	$15^2, 75$	$15^2, 25^5, 150^2$	
32	–	5	3T2	$15^2, 75$	$15^2, 125, 150^2$	
3	+	3	3T1,5T2			
8	–	3	3T1,5T3			
6	+	1	3T2,5T3			
12	+	1	3T1	$15^2, 75$	$15^2, 25, 50^2, 75^4$	
30	+	1	3T1	$15^2, 75$	$15^2, 75^4, 125$	
17	+	1	3T1	30, 75	25, 30, 100, 150^2	
37	+	1	3T1	30, 75	30, 125, 150^2	
11	–	1	3T2,5T3			
2	–	1	3T2,5T2	15^7		
7	–	1	3T2,5T2	$15^3, 30^2$		
19	–	1	3T1	30, 75	25, 30, 100, 150^2	
38	–	1	3T1	30, 75	30, 125, 150^2	
27	–	1	3T2	30, 75	25, 30, 100, 150^2	
49	–	1	3T2	30, 75	30, 125, 150^2	
14	–	1	3T2	$15^2, 75$	$15^2, 25, 50^2, 150^2$	$15^4, 75^2$
18	–	1	3T2	$15^2, 75$	$15^2, 25, 50^2, 150^2$	$30^2, 75^2$
31	–	1	3T2	$15^2, 75$	$15^2, 125, 150^2$	$15^4, 75^2$
40	–	1	3T2	$15^2, 75$	$15^2, 125, 150^2$	$30^2, 75^2$

which are eventually trivial and which give structural information about the Galois group of a p -adic field, as the following result shows.

Proposition 2.2. *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.

Proof. We note that U_0/U_1 is isomorphic to the multiplicative group of the residue field of L . For $i \geq 1$, U_i/U_{i+1} is isomorphic to the additive group of the residue field.

Part (a) follows from Proposition 4.2.7 in [18]. Part (b) follows from part (a). Since every subgroup of the residue field is a vector space over \mathbf{Z}/p , every subgroup of U_i/U_{i+1} is a direct sum of cyclic groups of order p . That G_1 is a p -group follows since

$$|G_1| = \prod_{i=1} |G_i/G_{i+1}|,$$

which proves part (c). Since G_0 and G_1 have relatively prime order, there exists a subgroup of G_0 that projects isomorphically onto G_0/G_1 [10, Theorem 15.2.2], proving part (d). Since G/G_0 is isomorphic to the Galois group of the residue field, it is cyclic. Part (e) follows from general results on solvability. \square

Specializing to the case where L is the splitting field of an irreducible degree 15 polynomial defined over \mathbf{Q}_5 , we see that G is a solvable transitive subgroup of S_{15} ; of which there are 64. 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 5-group (possibly trivial). Moreover, G_0/G_1 is cyclic of order dividing $5^{[G:G_0]} - 1$. Direct computation on the 64 candidates shows that only 24 are possible Galois groups.

We identify these groups in Table 1 using the transitive numbering system in [9] (see the \mathbf{T} column). The table also includes a few additional defining characteristics of each group. Later in the paper, we will reference these groups using only their \mathbf{T} number.

3. Stem Field Invariants

As before, let f be a degree 15 polynomial defined over \mathbf{Q}_5 , 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). In this case, H is isomorphic to the point stabilizer of 1 in G . Our next results relates the automorphism group of f 's stem field to the normalizer of H in G .

Proposition 3.1. *Let K/\mathbf{Q}_5 be the stem field of f , G the Galois group of f , and $H \leq G$ the subgroup of G corresponding to K under the Galois correspondence. Then the automorphism group of K/\mathbf{Q}_5 is isomorphic to $N(H)/H$, where $N(H)$ is the normalizer of H in G . In particular, $\#\text{Aut}(K/\mathbf{Q}_5) = [N(H) : H]$.*

Proof. Each $\sigma \in G$ restricts to an automorphism of K if and only if $\sigma K = K$. This in turn is true if and only if the subgroup fixing K equals the subgroup fixing σK . Now the subgroup fixing σK is equal to the collection of elements $\tau \in G$ such that $\tau \sigma k = \sigma k$ for all $k \in K$; i.e., all $\tau \in G$ such that $\sigma^{-1} \tau \sigma k = k$ for all $k \in K$. This means $\sigma^{-1} \tau \sigma$ fixes K . Since H is the subgroup that fixes K , $\sigma^{-1} \tau \sigma \in H$; i.e., $\tau \in \sigma H \sigma^{-1}$. Therefore, the subgroup fixing σK is $\sigma H \sigma^{-1}$. So the automorphisms of K are precisely the elements of $N(H)$, the normalizer of H in G .

But two such elements of the normalizer might restrict to the same automorphism. Specifically, let $\alpha, \beta \in N(H)$. Then $\alpha k = \beta k$ for all $k \in K$ if and only if $\alpha^{-1} \beta k = k$ for all $k \in K$. As before, this means $\alpha^{-1} \beta$ fixes K . So $\alpha^{-1} \beta \in H$; i.e., $\beta \in \alpha H$. Thus the elements in G that restrict to distinct automorphisms of K correspond precisely to the cosets of H in $N(H)$. The last sentence in the statement of the proposition now follows immediately. \square

Another invariant we employ is related to the discriminant of f . We say the parity of the polynomial f is $+$ if the discriminant of f is a square in \mathbf{Q}_5 ; otherwise, the parity is $-$. On the group theory side, the parity of a polynomial's Galois group is $+$ if $G \subseteq A_{15}$ and $-$ 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 $sgg(f)$.

Table 3: Polynomials defining degree 15 5-adic fields whose normal closure has Galois group \mathbf{G} which is either T1, T2, T3, T4, or T6. Also included are the extension's ramification index \mathbf{e} and discriminant exponent \mathbf{c} . The table is sorted first by Galois group, then by ramification index, then by discriminant exponent.

Polynomials	\mathbf{e}	\mathbf{c}	\mathbf{G}
$x^{15} + x^2 + 2$	1	0	T1
$x^{15} + 585x^{14} + 505x^{13} + 370x^{12} + 165x^{11} + 378x^{10} + 395x^9 + 170x^8$ $+ 315x^7 + 95x^6 + 306x^5 + 315x^4 + 260x^3 + 5x^2 + 260x + 607$	5	24	T1
$x^{15} + 405x^{14} + 120x^{13} + 10x^{12} + 90x^{11} + 188x^{10} + 135x^9 + 395x^8$ $+ 505x^7 + 345x^6 + 341x^5 + 300x^4 + 95x^3 + 75x^2 + 470x + 457$	5	24	T1
$x^{15} + 380x^{14} + 555x^{13} + 575x^{12} + 160x^{11} + 43x^{10} + 70x^9 + 125x^8$ $+ 330x^7 + 170x^6 + 546x^5 + 305x^4 + 75x^3 + 95x^2 + 370x + 382$	5	24	T1
$x^{15} + 70x^{14} + 315x^{13} + 80x^{12} + 530x^{11} + 518x^{10} + 565x^9 + 425x^8$ $+ 480x^7 + 30x^6 + 386x^5 + 275x^4 + 5x^3 + 295x^2 + 100x + 132$	5	24	T1
$x^{15} + 315x^{14} + 285x^{13} + 45x^{12} + 425x^{11} + 133x^{10} + 620x^9 + 325x^8$ $+ 365x^7 + 365x^6 + 516x^5 + 35x^4 + 575x^3 + 275x^2 + 420x + 257$	5	24	T1
$x^{15} + 40x^{14} + 95x^{13} + 50x^{12} + 115x^{11} + 44x^{10} + 15x^9 + 95x^8 + 100x^7$ $+ 40x^6 + 47x^5 + 60x^4 + 80x^3 + 110x + 67$	15	26	T2
$x^{15} + 90x^{14} + 15x^{13} + 70x^{12} + 110x^{11} + 60x^{10} + 85x^9 + 110x^8 + 5x^7$ $+ 15x^6 + 14x^5 + 15x^4 + 75x^3 + 90x^2 + 20x + 43$	5	18	T3
$x^{15} + 70x^{14} + 100x^{13} + 85x^{12} + 70x^{11} + 30x^{10} + 85x^9 + 85x^8 + 80x^7$ $+ 20x^6 + 49x^5 + 105x^4 + 5x^3 + 115x^2 + 80x + 83$	5	18	T3
$x^{15} + 445x^{14} + 130x^{13} + 265x^{12} + 560x^{11} + 323x^{10} + 505x^9 + 545x^8$ $+ 280x^7 + 580x^6 + 306x^5 + 120x^4 + 75x^3 + 175x + 252$	5	24	T3
$x^{15} + 11x^{14} + 17x^{13} + 23x^{12} + 13x^{11} + 6x^{10} + 3x^9 + 11x^8 + 18x^7$ $+ 14x^6 + 8x^5 + 4x^4 + 11x^3 + 9x^2 + 22x + 12$	3	10	T4
$x^{15} + 65x^{14} + 15x^{13} + 20x^{12} + 20x^{11} + 4x^{10} + 65x^9 + 115x^8 + 70x^7$ $+ 20x^6 + 42x^5 + 110x^4 + 35x^3 + 55x^2 + 80x + 32$	15	26	T4
$x^{15} + 45x^{14} + 10x^{13} + 40x^{12} + 15x^{11} + 114x^{10} + 95x^9 + 110x^8$ $+ 115x^7 + 40x^6 + 92x^5 + 30x^4 + 15x^3 + 110x^2 + 60x + 32$	15	26	T4
$x^{15} + 40x^{14} + 90x^{13} + 80x^{12} + 105x^{11} + 44x^{10} + 90x^9 + 90x^8 + 5x^7$ $+ 30x^6 + 82x^5 + 85x^4 + 110x^3 + 45x^2 + 120x + 7$	15	26	T4
$x^{15} + 5x^{13} + 45x^{12} + 45x^{11} + 39x^{10} + 100x^9 + 30x^8 + 120x^7 + 120x^6$ $+ 7x^5 + 100x^4 + 20x^3 + 30x^2 + 80x + 57$	15	26	T4
$x^{15} + 20x^{14} + 115x^{13} + 55x^{12} + 120x^{11} + 54x^{10} + 70x^9 + 40x^8 + 30x^7$ $+ 20x^6 + 52x^5 + 5x^4 + 60x^3 + 70x^2 + 80x + 82$	15	26	T4

Proposition 3.2. *The set $s\text{gg}(f)$ is an invariant of G . In other words, if f_1 and f_2 have the same Galois group, then $s\text{gg}(f_1) = s\text{gg}(f_2)$.*

Table 3: Continuation

Polynomials	e	c	G
$x^{15} + 10x^{14} + 15x^{12} + 20x^{11} + 9x^{10} + 20x^9 + 15x^8 + 10x^7 + 5x^6$ $+ 22x^5 + 20x^4 + 20x^3 + 20x^2 + 10x + 22$	15	20	T6
$x^{15} + 10x^{13} + 20x^{12} + 15x^{11} + 4x^{10} + 10x^9 + 20x^8 + 10x^7 + 20x^6$ $+ 7x^5 + 5x^4 + 20x^3 + 7$	15	20	T6
Polynomials	e	c	G
$x^{15} + 115x^{14} + 10x^{13} + 110x^{12} + 95x^{11} + 69x^{10} + 40x^9 + 60x^8 + 60x^7$ $+ 70x^6 + 62x^5 + 10x^4 + 65x^3 + 90x^2 + 105x + 107$	15	26	T6
$x^{15} + 105x^{14} + 65x^{13} + 60x^{12} + 80x^{11} + 84x^{10} + 105x^9 + 15x^8$ $+ 110x^7 + 105x^6 + 77x^5 + 70x^4 + 10x^3 + 15x^2 + 120x + 32$	15	26	T6

Proof. Let K be the stem field of f , G the Galois group of f , and $H \leq G$ the subgroup of G that corresponds to K under the Galois correspondence. The non-isomorphic subfields of K correspond to subgroups F of G (up to conjugation) that contain H . Now let $g(x)$ define a subfield F of K and let $E \leq G$ be the subgroup that fixes F . Then the Galois group of $g(x)$ corresponds to the smallest field that contains F and all roots of g , which in turn corresponds to the largest normal subgroup of G contained in E . The largest normal subgroup of G that is contained in E is the normal core, $\text{Core}(E)$, of E in G . Alternatively $\text{Core}(E)$ is the intersection of all conjugates of G , or equivalently the kernel of the permutation representation of G acting on the cosets G/E . Therefore the Galois group of g is $G/\text{Core}(E)$, proving that $\text{sgg}(f)$ is an invariant of G . \square

For example, consider the polynomial $x^{15} + x^2 + 2$, which defines the unique unramified degree 15 extension of \mathbf{Q}_5 . Thus the Galois group G of this polynomial is cyclic of order 15. Since the transitive group notation in [9] lists cyclic groups first, the T -number of G is 15T1. 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 3 and 5. These subfields define the unique unramified extensions of \mathbf{Q}_5 of their respective degrees, and therefore their Galois groups are also cyclic. Thus $\text{sgg}(f)$ is $\{3\text{T1}, 5\text{T1}\}$.

In general, to compute $\text{sgg}(f)$, we can make use of the complete lists of cubic and quintic 5-adic fields determined in [12] (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 [15, 17] to test if the polynomial has a root in the field defined by f , which occurs if and only if this

polynomial defines a subfield of f 's stem field. Continuing in this way, it is straightforward to compute $sgg(f)$.

For each of the 24 possible Galois groups of degree 15 extensions of \mathbf{Q}_5 , Table 2 shows their respective data for $[N(H) : H]$, parity, and sgg content, with the groups sorted based on their corresponding characteristics. Notice that these three invariants are enough to uniquely identify the six Galois groups 15T1, 15T3, 15T4, 15T6, 15T8, and 15T11.

To distinguish between the remaining 18 Galois groups, we make use of three resolvent polynomials, two of which are linear resolvents (in the sense of [19]).

4. Three Resolvent Polynomials

We begin with a definition of a general resolvent for degree 15 polynomials.

Definition 4.1. Let $f(x)$ be an irreducible polynomial of degree 15 defined over \mathbf{Q}_5 , and let G be the Galois group of f . Let $T(x_1, \dots, x_{15})$ be a polynomial with integer coefficients. Let H be the stabilizer of T in S_{15} . That is,

$$H = \{ \sigma \in S_{15} : T(x_{\sigma(1)}, \dots, x_{\sigma(15)}) = T(x_1, \dots, x_{15}) \}.$$

We define the **resolvent polynomial** $R_T(x)$ by

$$R_T(x) = \prod_{\sigma \in S_{15}/H} (x - T(r_{\sigma(1)}, \dots, r_{\sigma(15)})),$$

where S_{15}/H is a complete set of right coset representatives of S_{15} modulo H and where r_1, \dots, r_{15} are the roots of $f(x)$.

The main theorem concerning resolvent polynomials is the following.

Theorem 4.2. *With the notation of the preceding definition, set $m = [S_{15} : H] = \deg(R_T)$. If R_T is squarefree, its Galois group (as a subgroup of S_m) is equal to the image of the permutation representation of G acting on S_{15}/H . Note that we can always ensure R is squarefree by taking a suitable Tschirnhaus transformation of f [8, p. 318].*

Proof. Let K be the stem field of $R_T(x)$. Then by construction, the subgroup that fixes R_T is H . Thus the splitting field of R_T corresponds to the kernel of the permutation representation of G acting on S_{15}/H . Therefore, the Galois group of R_T is isomorphic to G mod this kernel; i.e., to the image of the permutation representation. □

Table 4: Polynomials defining degree 15 5-adic fields whose normal closure has Galois group \mathbf{G} which is either T7 or T8. This is a continuation of Table 3.

Polynomials	e	c	\mathbf{G}
$x^{15} + 5x^{14} + 5x^{12} + 15x^{11} + 24x^{10} + 20x^9 + 20x^8 + 20x^6 + 2x^5 + 15x^4 + 10x^3 + 5x^2 + 2$	15	20	T7
$x^{15} + 5x^{14} + 10x^{13} + 10x^{12} + 10x^{11} + 9x^{10} + 15x^9 + 15x^8 + 15x^7 + 5x^6 + 17x^5 + 5x^3 + 5x^2 + 7$	15	20	T7
$x^{15} + 20x^{11} + 22x^{10} + 5x^9 + 15x^5 + 10x^4 + 10x^3 + 5x^2 + 15x + 3$	5	15	T8
$x^{15} + 15x^{13} + 10x^{12} + 5x^{11} + 12x^{10} + 5x^9 + 5x^7 + 10x^6 + 10x^5 + 10x^4 + 5x^3 + 20x^2 + 15x + 3$	5	15	T8
$x^{15} + 20x^{14} + 15x^{12} + 5x^{11} + 2x^{10} + 20x^9 + 10x^8 + 20x^7 + 20x^6 + 15x^5 + 15x^4 + 10x^3 + 5x^2 + 3$	5	15	T8
$x^{15} + 10x^{14} + 20x^{13} + 15x^{12} + 20x^{11} + 17x^{10} + 15x^8 + 20x^7 + 10x^6 + 20x^5 + 15x^4 + 15x^3 + 15x^2 + 20x + 18$	5	15	T8
$x^{15} + 90x^{14} + 100x^{13} + 80x^{12} + 110x^{11} + 15x^{10} + 5x^9 + 35x^8 + 45x^7 + 90x^6 + 34x^5 + 30x^4 + 100x^3 + 55x^2 + 60x + 38$	5	18	T8
$x^{15} + 85x^{14} + 90x^{13} + 85x^{11} + 115x^{10} + 10x^9 + 20x^8 + 40x^7 + 55x^6 + 99x^5 + 120x^4 + 120x^3 + 90x^2 + 75x + 8$	5	18	T8
$x^{15} + 95x^{14} + 75x^{13} + 65x^{12} + 45x^{11} + 60x^{10} + 25x^9 + 70x^8 + 65x^7 + 75x^6 + 23x^5 + 55x^3 + 60x^2 + 115x + 83$	5	21	T8
$x^{15} + 15x^{14} + 10x^{13} + 95x^{12} + 45x^{11} + 10x^{10} + 95x^9 + 95x^8 + 70x^7 + 30x^6 + 18x^5 + 110x^4 + 50x^3 + 35x^2 + 70x + 123$	5	21	T8
$x^{15} + 85x^{14} + 40x^{13} + 25x^{12} + 50x^{11} + 50x^{10} + 40x^9 + 95x^8 + 90x^7 + 105x^6 + 103x^5 + 70x^4 + 115x^3 + 100x^2 + 45x + 43$	5	21	T8
$x^{15} + 100x^{14} + 55x^{13} + 40x^{12} + 40x^{11} + 70x^{10} + 95x^9 + 5x^8 + 110x^7 + 45x^6 + 73x^5 + 10x^4 + 80x^3 + 55x^2 + 10x + 103$	5	21	T8
$x^{15} + 605x^{14} + 220x^{13} + 130x^{12} + 380x^{11} + 443x^{10} + 410x^8 + 235x^7 + 485x^6 + 171x^5 + 390x^4 + 150x^3 + 600x^2 + 60x + 522$	5	24	T8
$x^{15} + 130x^{14} + 605x^{12} + 200x^{11} + 213x^{10} + 140x^9 + 435x^8 + 305x^7 + 620x^6 + 131x^5 + 190x^4 + 560x^3 + 560x^2 + 445x + 512$	5	24	T8
$x^{15} + 570x^{14} + 530x^{13} + 620x^{12} + 70x^{11} + 549x^{10} + 460x^9 + 490x^8 + 615x^7 + 595x^6 + 34x^5 + 60x^4 + 100x^3 + 300x^2 + 620x + 537$	5	27	T8
$x^{15} + 470x^{14} + 555x^{13} + 595x^{12} + 370x^{11} + 54x^{10} + 335x^9 + 65x^8 + 440x^7 + 395x^6 + 449x^5 + 260x^4 + 575x^3 + 200x^2 + 20x + 7$	5	27	T8
$x^{15} + 420x^{14} + 305x^{13} + 45x^{12} + 170x^{11} + 594x^{10} + 160x^9 + 65x^8 + 190x^7 + 95x^6 + 194x^5 + 35x^4 + 375x^3 + 525x^2 + 495x + 367$	5	27	T8
$x^{15} + 170x^{14} + 430x^{13} + 320x^{12} + 420x^{11} + 519x^{10} + 10x^9 + 590x^8 + 290x^7 + 45x^6 + 514x^5 + 385x^4 + 300x^3 + 200x^2 + 420x + 202$	5	27	T8
$x^{15} + 620x^{14} + 455x^{13} + 95x^{12} + 320x^{11} + 4x^{10} + 210x^9 + 590x^8 + 490x^7 + 295x^6 + 489x^5 + 110x^4 + 225x^3 + 175x^2 + 495x + 192$	5	27	T8

As a consequence, this theorem implies that the list of degrees of irreducible factors of R_T is the same as the length of the orbits of the action on the cosets. In particular, the degrees of the irreducible factors of R_T can be determined by a purely group-theoretic computation.

Our three resolvents are constructed as follows. First consider the following multivariable functions.

- Let $T_1 = x_1 + x_2$
- Let $T_2 = x_1 + x_2 + x_3$
- Let $T_3 = (x_8 - x_{10})(x_8 - x_5)(x_8 - x_6)(x_8 - x_7)(x_9 - x_{10})(x_9 - x_5)(x_9 - x_6)(x_9 - x_7)(x_5 - x_7)(x_6 - x_7)(x_{10} - x_5)(x_{10} - x_6)(x_{10} - x_7)(x_5 - x_6)(x_3 - x_4)(x_3 - x_{14})(x_3 - x_{15})(x_3 - x_{12})(x_3 - x_{11})(x_3 - x_{13})(x_3 - x_8)(x_3 - x_9)(x_3 - x_{10})(x_3 - x_5)(x_3 - x_6)(x_3 - x_7)(x_4 - x_{14})(x_4 - x_{15})(x_4 - x_{12})(x_4 - x_{11})(x_4 - x_{13})(x_4 - x_8)(x_4 - x_9)(x_4 - x_{10})(x_4 - x_5)(x_4 - x_6)(x_4 - x_7)(x_{14} - x_{15})(x_{14} - x_{12})(x_{14} - x_{11})(x_{14} - x_{13})(x_{14} - x_8)(x_{14} - x_9)(x_{14} - x_{10})(x_{14} - x_5)(x_{14} - x_6)(x_{14} - x_7)(x_{15} - x_{12})(x_{15} - x_{11})(x_{15} - x_{13})(x_{15} - x_8)(x_{15} - x_9)(x_{15} - x_{10})(x_{15} - x_5)(x_{15} - x_6)(x_{15} - x_7)(x_{12} - x_{11})(x_{12} - x_{13})(x_{12} - x_8)(x_{12} - x_9)(x_{12} - x_{10})(x_{12} - x_5)(x_{12} - x_6)(x_{12} - x_7)(x_{11} - x_{13})(x_{11} - x_8)(x_{11} - x_9)(x_{11} - x_{10})(x_{11} - x_5)(x_{11} - x_6)(x_{11} - x_7)(x_{13} - x_8)(x_{13} - x_9)(x_{13} - x_{10})(x_{13} - x_5)(x_{13} - x_6)(x_{13} - x_7)(x_8 - x_9)$

It is straightforward to compute the stabilizers of these forms:

- T_1 is stabilized by the subgroup H_1 generated by $\{(1,2), (3,4), (3,4,5,6,7,8,9,10,11,12,13,14,15)\}$.
- T_2 is stabilized by the subgroup H_2 generated by $\{(1,2), (1,2,3), (4,5), (4,5,6,7,8,9,10,11,12,13,14,15)\}$.
- T_3 is stabilized by the subgroup H_3 generated by $\{(1,2), (3,4,5), (4,6,7,8,9,10,11,12,13,14,15), (3,6,7,8,9,10,11,12,13,14,15)\}$.

The index of each subgroup is as follows: $[S_{15} : H_1] = 105$, $[S_{15} : H_2] = 455$, and $[S_{15} : H_3] = 210$. Let F_{105} be the resolvent corresponding to H_1 , F_{455} the resolvent corresponding to H_2 , and F_{210} the resolvent corresponding to H_3 ; note, the subscript gives the degree of the resolvent polynomial. Table 2 gives the degrees of the irreducible factors for each resolvent, depending on the Galois group of f .

5. Sample Defining Polynomials

In this section, we give defining polynomials for all extensions whose Galois groups have order ≤ 60 . This corresponds to polynomials with Galois group equal to T1, T2, T3, T4, T6, T7, or T8. Note, defining polynomials for these extensions can be computed with a built-in command in [16] (there are a total of 1012 such extensions). Tables 3 and 4 give 39 polynomials defining the above-mentioned extensions. Also included are the ramification index \mathbf{e} of each extension and the discriminant exponent \mathbf{c} ; i.e, the integer c such that the extension's discriminant is (p^c) . The remaining data are available by emailing the first author.

Acknowledgements

The authors were supported in part by NSF grant #DMS-1148695. The authors would like to thank Elon University for supporting this project and the Center for Undergraduate Research in Mathematics for their 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] Chad Awtrey, *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 Shill, and Erin Strosnider, *Degree 14 2-adic fields*, Involve **8** (2015), no. 2, 329–336. **MR:** 3320863
- [5] Chad Awtrey, Nicole Miles, Christopher Shill, and Erin Strosnider, *Computing Galois groups of degree 12 2-adic fields with trivial automorphism group*, (submitted).

- [6] Chad Awtrey, Nicole Miles, Christopher Shill, and Erin Strosnider, *Degree 12 2-adic fields with automorphism group of order 4*, Rocky Mountain Journal of Mathematics (to appear).
- [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, Springer Proceedings in Mathematics & Statistics, vol. 64, Springer, New York, 2013, pp. 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] Marshall Hall, Jr., *The theory of groups*, The Macmillan Co., New York, N.Y., 1959. **MR:** 0103215 (21 #1996)
- [11] 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)
- [12] John W. Jones and David P. Roberts, *A database of local fields*, J. Symbolic Comput. **41** (2006), no. 1, 80–97. **MR:** 2194887 (2006k:11230)
- [13] John W. Jones and David P. Roberts, *Octic 2-adic fields*, J. Number Theory **128** (2008), no. 6, 1410–1429. **MR:** MR2419170 (2009d:11163)
- [14] Serge Lang, *Algebraic number theory*, second ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994. **MR:** 1282723 (95f:11085)
- [15] Peter Panayi, *Computation of leopoldt’s p-adic regulator*, Ph.D. thesis, University of East Anglia, December 1995.
- [16] PARI Group, The, *PARI/GP – Computational Number Theory, version 2.3.4*, 2008, available from <http://pari.math.u-bordeaux.fr/>.
- [17] 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)

- [18] 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)
- [19] Leonard Soicher and John McKay, *Computing Galois groups over the rationals*, J. Number Theory **20** (1985), no. 3, 273–281. **MR:** MR797178 (87a:12002)