Resolvents, masses, and Galois groups of irreducible quartic polynomials

Chad Awtrey Brett Barkley Jeremy Guinn
Mackenzie McCraw

April 25, 2013

Abstract

Let F be a field and $f(x) \in F[x]$ an irreducible polynomial of degree four. An important problem in computational algebra is to determine the Galois group of $f(x)$ as a transitive subgroup of S_4 (the symmetric group on four letters). In the case where F is the set of rational numbers, several methods appear in the literature, most of which rely on factoring the cubic resolvent as well as several other polynomials. We place this approach in the context of absolute resolvents and extend it by introducing a single degree twelve resolvent polynomial construction, the degrees of whose irreducible factors completely determine the Galois group of $f(x)$ over F. We also offer another approach, which does not rely on factoring resolvent polynomials of degree greater than two, but rather considers the discriminant of $f(x)$ along with the subfields and the size of the automorphism group of $F[x]/(f(x))$. We show that this alternative method is particularly effective in the case where F is a finite extension of the p-adic numbers.

1 Introduction

Considered by some to be one of the most beautiful areas of pure mathematics, Galois theory stands at the intersection of two of the most foundational topics in algebra; namely, group theory and field theory. Specifically, we can consider field extensions obtained by adjoining to a given base field the roots of monic irreducible polynomials. We are often interested in the arithmetic structure of these field extensions, since this information is related to how the roots of these polynomials interact via the algebraic operations of the base field. Galois theory is important because it associates to each polynomial a group (called its Galois group) that encodes this arithmetic structure.

Therefore, an important problem in computational algebra is to determine the Galois group of an irreducible polynomial defined over a field. Algorithms for accomplishing this task have been in existence for more than a century. Indeed, the original definition of the Galois group implicitly contained a technique for

its determination. For an explicit description of this method, see [vdW91, p. 189].

For this paper, we focus on quartic polynomials. Most modern treatments employ the so-called "cubic resolvent polynomial" to determine the Galois group [DF04, Hun80]. In short, this method involves taking the original quartic polynomial f, forming a degree three polynomial (the cubic resolvent) from the roots of f, and then factoring both the cubic resolvent and the discriminant of f over the base field. In one case, we also factor f over the base field adjoin the square root of the discriminant of f. An alternative (and more elementary) version of this technique can be found in [KW89], where the authors remove the need to factor the original quartic over extension fields and instead factor two additional quadratic polynomials over the base.

This paper offers two additional methods for computing Galois groups of quartic polynomials. The first is an improvement of the cubic resolvent method. The second incorporates what we call the mass of a polynomial, and it is especially useful over finite extensions of the p-adic numbers.

While our results can be applied to any field of characteristic different from 2, we are mostly interested in applications to p-adic fields (which are finite extensions of the p-adic numbers). Consequently, Section 2 provides a brief overview of p-adic fields. After this, we use Section 3 to improve upon the results found in [KW89] by situating the cubic resolvent method in the larger framework of what has become known as the absolute resolvent method. In this context, we determine all possible absolute resolvent polynomials as well as their factorizations (which depend on the Galois group of the original quartic). In particular, we prove that there is a unique absolute resolvent polynomial of degree 12 the degrees of whose irreducible factors completely determine the Galois group of the original quartic polynomial (i.e., no lower degree resolvent polynomial can accomplish this). Lastly, Section 4 introduces a new technique for computing quartic Galois groups based on the notion of the mass of the polynomial, following [Awt12b, Awt11, Awt12a, AE12]. To provide an example of the versatility of this method, we end the paper by examining Galois groups of totally ramified quartic extensions of p-adic fields for odd primes p.

2 Background on p-adic Fields

In this section, we give a brief overview of p-adic numbers and their extensions, introducing only those definitions and results that are used later in the paper. For more details, we refer the reader to [Gou97], which contains a good elementary account of p-adic numbers. More advanced treatments can be found in [Lan94] and [Ser79].

2.1 The p-adic Numbers

The p-adic numbers are constructed from the rationals in much the same way the reals are constructed. In particular, consider the map $v_p : \mathbf{Q} \to \mathbf{Z} \cup \{\infty\}$

defined by

$$v_p(x) = \begin{cases} n & \text{if } x = p^n a/b \text{ with } p \nmid ab \\ \infty & \text{if } x = 0 \end{cases}$$

The function v_p is called the *p-adic valuation* and it gives rise to the *p-adic absolute value* $|\cdot|_p$ in the following way,

$$|x|_p = \frac{1}{p^{v_p(x)}} \qquad \text{for all } x \in \mathbf{Q}$$

The p-adic numbers are defined as the completion of $\mathbf{Q}$ with respect to this absolute value. The field $\mathbf{Q}_p$ has characteristic 0 and is a locally compact, totally disconnected Hausdorff topological space [Gou97, p.63].

The ring of *p-adic integers* $\mathbf{Z}_p$ is defined as

$$\mathbf{Z}_p = \{x \in \mathbf{Q}_p : |x|_p \leq 1\}$$

The ring $\mathbf{Z}_p$ is compact and has a unique maximal ideal; namely $p\mathbf{Z}_p$. The *residue field* is defined as $\mathbf{Z}_p/p\mathbf{Z}_p$ and is isomorphic to the finite field with p elements $\mathbf{F}_p$. Every element of $\mathbf{Q}_p$ can be written in the form x/p^n for some $x \in \mathbf{Z}_p$ and some nonnegative integer n. Moreover, every element of $\mathbf{Z}_p$ can be represented uniquely as an infinite sum in "base p" [Gou97, p.68]

$$\mathbf{Z}_p = \left\{ \sum_{k=0}^{\infty} a_k p^k : a_k \in \mathbf{Z} \text{ with } 0 \leq a_k \leq p-1 \right\}$$

2.2 Extensions of $\mathbf{Q}_p$

By an *extension field* of $\mathbf{Q}_p$, we mean any field K containing $\mathbf{Q}_p$. Notice that this implies K is a vector space over $\mathbf{Q}_p$, and we say K is a *finite extension* if its dimension as a $\mathbf{Q}_p$ vector space is finite. We write

$$[K : \mathbf{Q}_p] = \dim_{\mathbf{Q}_p} K$$

and call this number the *degree* of the extension.

Let $K/\mathbf{Q}_p$ be a finite extension. The set of all automorphisms on K which induce the identity on $\mathbf{Q}_p$ forms a group under function composition, called the *automorphism group* of K. The *mass* of $K/\mathbf{Q}_p$ is defined as the degree of the extension divided by the size of its automorphism group,

$$m(K) = [K : \mathbf{Q}_p]/|\mathrm{Aut}(K/\mathbf{Q}_p)|$$

If $m(K) = 1$, then K is called a *Galois extension* and $\mathrm{Aut}(K/\mathbf{Q}_p)$ is called the *Galois group* of K.

Since $\mathbf{Q}_p$ has characteristic 0, an extension field arises by adjoining to $\mathbf{Q}_p$ the root of some monic irreducible polynomial over $\mathbf{Z}_p$. By Krasner's Lemma [Lan94, p.43], this polynomial can be chosen to have integer coefficients. For an extension $K/\mathbf{Q}_p$ with $n = [K : \mathbf{Q}_p]$ and an element $x \in K$, let $f(y) =$

$y^d + a_{d-1}y^{d-1} + \cdots + a_1 y + a_0$ be its minimal polynomial. We define the *norm* of x from K down to $\mathbf{Q}_p$ as,

$$N_{K/\mathbf{Q}_p}(x) = (-1)^n f(0)^{n/d}$$

The norm is used to define the p-adic absolute value on K that extends the p-adic absolute value on $\mathbf{Q}_p$ [Gou97, p.151]. For $x \in K$, we define

$$|x|_p = \sqrt[n]{\left|N_{K/\mathbf{Q}_p}(x)\right|_p}$$

The p-adic absolute value on an extension K gives rise to the corresponding p-adic valuation v_p on K by using the equation

$$|x|_p = \frac{1}{p^{v_p(x)}}$$

where $v_p(0) = \infty$.

The p-adic valuation is a homomorphism from the multiplicative group K^* to the addivite group $\mathbf{Q}$. Its image is of the form $(1/e)\mathbf{Z}$ where $e \mid [K : \mathbf{Q}_p]$ [Gou97, p.159]. We call e the *ramification index* of $K/\mathbf{Q}_p$. Let $f = [K : \mathbf{Q}_p]/e$. We call f the *residue degree* of $K/\mathbf{Q}_p$. Any element in K whose p-adic valuation equals e is called a *uniformizer*. If $e = 1$, the extension is called *unramified*. If $e = [K : \mathbf{Q}_p]$, the extension is called *totally ramified*. If $p \nmid e$, the extension is called *tamely ramified*.

The ring of integers in $K/\mathbf{Q}_p$ is defined as

$$\mathcal{O}_K = \{x \in K : |x|_p \leq 1\} = \{x \in K : v_p(x) \geq 0\}$$

It is compact with a unique maximal ideal, given by

$$\mathcal{P}_K = \{x \in K : |x|_p < 1\} = \{x \in K : v_p(x) > 0\}$$

The *residue field* of $K/\mathbf{Q}_p$ is equal to $\mathcal{O}_K/\mathcal{P}_K$ and is isomorphic to the finite field with p^f elements $\mathbf{F}_{p^f}$, where f is the residue degree of K. Moreover, $p\mathcal{O}_K = \pi^e \mathcal{O}_k = \mathcal{P}_K^e$, where π is any uniformizer and e is the ramification index of K.

3 Absolute Resolvents

Now that we have given an overview of p-adic fields, we use the following sections to discuss techniques for computing Galois groups of polynomials over $\mathbf{Q}_p$. We point out that while the results in this section apply to arbitrary fields of characterstic different from 2, our focus will be on p-adic fields.

Toward that end, let $F/\mathbf{Q}_p$ be a finite extension and let K/F be a quartic extension, defined by the monic irreducible polynomial $f(x)$. Let α_1, α_2, α_3, and α_4 be the roots of f in some fixed algebraic closure $\overline{\mathbf{Q}_p}$ of $\mathbf{Q}_p$, and let G denote the Galois group of f; i.e., the Galois group of the splitting field of f, or

Table 1: Conjugacy classes of nontrivial subgroups of S_4.

Name	Transitive ?	Size	Generators
C_2	no	2	$(12)(34)$
C_2^*	no	2	(12)
C_3	no	3	(123)
V_4^*	no	4	$(12), (12)(34)$
V_4	yes	4	$(12)(34), (13)(24)$
C_4	yes	4	(1234)
S_3	no	6	$(12), (123)$
D_4	yes	8	$(13), (1234)$
A_4	yes	12	$(123), (234)$
S_4	yes	24	$(1234), (12)$

equivalently of the Galois closure of K in $\overline{\mathbf{Q}_p}$. Since the elements of G act as permutations on the roots α_i of f, once we fix an ordering of the roots, G can be viewed as a subgroup of S_4 (the symmetric group on 4 letters). Changing the ordering of the roots corresponds to conjugating G in S_4. Since the polynomial f is irreducible, G is a transitive subgroup of S_4; i.e., there is a single orbit for the action of G on the roots α_i of f (each orbit corresponds to an irreducible factor of f).

Therefore, in order to determine the group structure of G, we first identify the conjugacy classes of transitive subgroups of S_4. This information is well known. In fact, the transitive subgroups of S_n are known up to and including $n = 32$ (see [BM83, CHM98, CH08]).

Since we will make use of all conjugacy classes of subgroups of S_4 (not just the transitive subgroups), we include Table 1 for convenience, which gives information on these classes. This information can easily be computed with [GAP08].

Most of the group names in the table are standard. For example, A_4 represents the alternating group on 4 letters, D_4 represents the dihedral group of order 8, C_n represents the cyclic group of order n, and V_4 represents the Klein-four group (i.e., $C_2 \times C_2$). There are two different conjugacy classes of V_4 subgroups in S_4 (only one of which is transitive). There are also two different conjugacy classes of C_2 in S_4. In each case, we label one group with an asterisk so as to distinguish the conjugacy classes.

3.1 Definition of Resolvents

The usual technique for computing Galois groups involves the notion of absolute resolvent polynomial, which we now define.

Definition 3.1. Let $T(x_1, \ldots, x_4)$ be a polynomial with coefficients in $\mathbf{Z}_p$. Let

H be the stabilizer of T in S_4. That is,

$$H = \left\{\sigma \in S_4 \colon T(x_{\sigma(1)}, \ldots, x_{\sigma(4)}) = T(x_1, \ldots, x_4)\right\}.$$

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

$$R_{f,T}(x) = \prod_{\sigma \in S_4/H} \left(x - T(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(4)})\right),$$

where S_4/H is a complete set of right coset representatives of S_4 modulo H and where $\alpha_1, \ldots, \alpha_4$ are the roots of $f(x)$. By Galois theory, $R_{f,T}(x)$ also has coefficients in $\mathbf{Z}_p$.

3.2 Example: Discriminant

Perhaps the most well known example of a resolvent polynomial is the discriminant [DF04, p. 610]. Recall that the discriminant of a quartic polynomial $f(x)$ is given by

$$\operatorname{disc}(f) = \prod_{1 \le i < j \le 4} (\alpha_i - \alpha_j)^2,$$

where α_i are the roots of f. In particular, let

$$T = \prod_{1 \le i < j \le 4} (x_i - x_j),$$

and let $H = A_4$. Notice that a complete set of right coset representatives of S_4/A_4 is $\{(1), (12)\}$. Also notice that applying the permutation (12) to the subscripts of T results in $-T$. In this case, we can form the resolvent polynomial as follows,

$$R_{f,T}(x) = \prod_{\sigma \in S_4/A_4} (x - \sigma(T)) = x^2 - T^2 = x^2 - \operatorname{disc}(f).$$

As a concrete example, consider the polynomial $f(x) = x^4 + ap \in \mathbf{Z}_p[x]$. Its discriminant is given by: $\operatorname{disc}(x^4 + ap) = 256a^3p^3$.

3.3 Example: Cubic Resolvent

As another example, consider the cubic resolvent [DF04, p. 614]. In this case, we let $T = x_1x_2 + x_3x_4$. The stabilizer of T in S_4 is a dihedral group D_4 of order 8. In particular, the elements of this particular D_4 are,

$$D_4 = \{(1), (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\}.$$

A complete set of right coset representatives for S_4/D_4 is given by: $\{(1), (13), (14)\}$. We can form the cubic resolvent for $f(x)$ by computing $R_{f,T}$:

$$R_{f,T}(x) = (x - (\alpha_1\alpha_2 + \alpha_3\alpha_4))\,(x - (\alpha_3\alpha_2 + \alpha_1\alpha_4))\,(x - (\alpha_4\alpha_2 + \alpha_3\alpha_1)).$$

For example, if $f(x) = x^4 + 2x^2 + 2 \in \mathbf{Z}_p[x]$, then the cubic resolvent of f is $x^3 - 2x^2 - 8x + 16$.

3.4 Main Theorem on Resolvents

The main theorem concerning resolvent polynomials is the following. A proof can be found in [SM85].

Theorem 3.2. *With the notation of the preceding definition, set* $m = [S_4 \colon H] = deg(R_{f,T})$. *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_4 *to* S_m *given by the natural right action of* S_4 *on* S_4/H. *Note that we can always ensure* R *is squarefree by taking a suitable Tschirnhaus transformation of* f *[Coh93, p. 324].*

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, $R_{f,T}$ has a root in $\mathbf{Z}_p$ if and only if G is conjugate under S_4 to a subgroup of H. This remark leads to the following well-known result on discriminants of polynomials.

Corollary 3.3. *For any irreducible quartic polynomial* $f(x) \in \mathbf{Z}_p[x]$, *its Galois group is a subgroup of* A_4 *if and only if* $disc(f)$ *is a square in* $\mathbf{Z}_p$.

3.5 Example: Degree 12 Resolvent

As proven in Theorem 3.2, we can use information on how resolvent polynomials factor to determine the Galois group of $f(x)$. Given a transitive subgroup G of S_4, the first step is to determine the factorizations of all possible resolvents arising from a quartic polynomial whose Galois group is G. This is a purely group-theoretic problem. In particular, the function `resfactors` below will perform such a task. It is written for the program GAP [GAP08].

```
resfactors := function(h, g)
  local s4, cosets, index, permrep;
    s4      := SymmetricGroup(4);
    cosets  := RightCosets(s4,h);
    index   := Size(cosets);
    permrep := Group(List(GeneratorsOfGroup(g),
                 j->Permutation(j, cosets, OnRight)));
  return(List(Orbits(permrep, [1..index]), Size));
end;
```

Table 2 shows for each conjugacy class of subgroups of S_4 the degrees of the irreducible factors of the corresponding resolvent polynomial according to the Galois group of f.

We can use the information in Table 2 to develop algorithms for computing Galois groups of irreducible quartic polynomials. For example, let f be an irreducible quartic polynomial, G the Galois group of f, and g the resolvent for D_4. This resolvent is the well-known cubic resolvent. We see that:

Table 2: The top row contains the transitive subgroups G of S_4. The left column contains representatives H of conjugacy classes of subgroups of S_4, as in Table 1. For a particular pair (H, G), the entry in the table gives the output of the function `resfactors(H,G)`. In particular, this list is equivalent to the list of irreducible factors of the resolvent polynomial $R(T, f)$ where T is stabilized by H and G is the Galois group of the irreducible quartic polynomial f.

H/G	C_4	V_4	D_4	A_4	S_4
C_2	2,2,4,4	2,2,2,2,2,2	4,4,4	6,6	12
C_2^*	4,4,4	4,4,4	4,8	12	12
C_3	4,4	4,4	8	4,4	8
V_4	2,2,2	1,1,1,1,1,1	2,2,2	3,3	6
V_4^*	2,4	2,2,2	2,4	6	6
C_4	1,1,4	2,2,2	2,4	6	6
S_3	4	4	4	4	4
D_4	1,2	1,1,1	1,2	3	3
A_4	2	1,1	2	1,1	2

1. if g factors as three linear polynomials, then $G = V_4$.
2. if g factors as a linear times a quadratic, then $G = C_4$ or D_4.
3. if g remains irreducible, then $G = A_4$ or S_4.

The standard procedure for remedying the situation in item (3) is to use the discriminant of f (i.e., the resolvent corresponding to A_4). If this resolvent factors as two linears, then $G = A_4$; otherwise, $G = S_4$. The resolve item (2), Kappe-Warren make use of the linear factor of g. See their paper for details [KW89].

As another example, we could use the resolvent corresponding to the group C_4, which is a degree 6 polynomial. In this case, there is no discrepancy between distinguishing C_4 from D_4. However, we still must distinguish between A_4 and S_4. The approach taken in [Coh93] is to use the discriminant for this latter computation. Again letting f denote the quartic polynomial, G its Galois group, and g the degree 6 resolvent corresponding to C_4, we have:

1. if g factors as two linears times a quartic, then $G = C_4$.
2. if g factors as three quadratics, then $G = V_4$.
3. if g factors as a quadratic times a quartic, then $G = D_4$.
4. if g remains irreducible, then $G = A_4$ if the discriminant of f is a square; $G = S_4$ otherwise.

The C_4 resolvent method mentioned above can be considered an improvement over the cubic resolvent method, since it completely determines the Galois group of the polynomial using only two resolvents (and nothing else).

We now point out our new method for computing Galois groups of quartics using absolute resolvent polynomials. Notice that there is one line in Table 2 which only requires one resolvent to uniquely identify the Galois group. This is the resolvent corresponding to the group C_2. In this case the resolvent will have degree 12, and here is a method to construct it.

Since $C_2 = \{(1), (12)(34)\}$, a complete set of right coset representatives for S_4/C_2 is

$$\{(1), (12), (13), (14), (23), (24), (123), (124), (132), (142), (13)(24), (1324)\}.$$

A form which is stabilized by C_2 is

$$T(x_1, x_2, x_3, x_4) = x_1x_2^2x_3^3x_4^4 + x_2x_1^2x_4^3x_3^4.$$

An algorithm for determing quartic Galois groups based on the degree 12 resolvent proceeds as follows. Letting f denote the quartic polynomial, G its Galois group, and g the degree 12 resolvent corresponding to C_2, we have:

1. if g factors as two quadratics times two quartics, then $G = C_4$.
2. if g factors as six quadratics, then $G = V_4$.
3. if g factors as three quartics, then $G = D_4$.
4. if g factors as two sextics, then $G = A_4$.
5. if g remains irreducible, then $G = S_4$.

For example, consider the Eisenstein polynomial x^4+2x+2, which defines a totally ramified quartic extension of $\mathbf{Q}_2$ (since all Eisenstein polynomials define totally ramified extensions [Gou97, p. 164]). Forming the degree 12 resolvent polynomial corresponding to the group C_2, we obtain

$$\begin{aligned} g =& x^{12} + 24x^{11} - 128x^{10} - 2560x^9 + 49152x^8 + 327680x^7 - 5898240x^6 \\ & - 19398656x^5 + 339738624x^4 + 2348810240x^3 + 6174015488x^2 \\ & + 8589934592x + 4294967296, \end{aligned}$$

which remains irreducible when factored over $\mathbf{Q}_2$ (using [PAR08] for example). Thus the Galois group of $x^4 + 2x + 2$ over $\mathbf{Q}_2$ is S_4.

4 The Mass of a Polynomial

In the previous section, we situated the standard approach for computing Galois groups of quartic polynomials (the cubic resolvent method) into the larger framework of the absolute resolvent method. We completely determined all possible resolvent polynomials along with their factorizations. We then used this information to develop an algorithm to compute Galois groups of quartic polynomials that only relied on factoring a single degree 12 resolvent polynomial.

In this section, we offer a different approach to computing Galois groups of quartic polynomials. In particular, the aim of this section is to prove the following theorem.

Theorem 4.1. *Let $p > 2$ be a prime number and $F/\mathbf{Q}_p$ a finite extension. Let f be the residue degree of F.*

1. *If $p \equiv -1 \pmod 4$ and f is odd, then there are two nonisomorphic totally ramified quartic extensions of F. The Galois closure of each extension has Galois group D_4.*

2. *Otherwise, there are four nonisomorphic totally ramified quartic extensions of F. Each extension is Galois with cyclic Galois group.*

Notice that this theorem proves the Galois group of an Eisenstein quartic polynomial defined over the p-adic field F depends only on the odd prime p and the residue degree of F. Specifically, if $p \equiv -1 \pmod 4$ and f is odd, then the Galois group is D_4; otherwise, the Galois group is C_4. Our approach for proving this theorem is to determine the Galois groups of all possible quartic polynomials of a p-adic field simultaneously, rather than focusing on one polynomial at a time.

Toward that end, we fix a prime $p > 2$, an algebraic closure $\overline{\mathbf{Q}}_p$ of the p-adic numbers, and a finite extension $F/\mathbf{Q}_p$. We let e be the ramification index of F and let f be its residue degree. Thus $ef = [F : \mathbf{Q}_p]$. For a finite extension K/F, we let K^{gal}/F denote its Galois closure, G the Galois group of K^{gal}/F, and $m(K/F)$ the mass of K/F.

4.1 Two Lemmas

In this subsection, we formulate two technical lemmas and describe how they fit together to yield a proof of Theorem 4.1. First, we focus on the invariants that distinguish between the possible Galois groups for quartic polynomials. One invariant is the discriminant of the polynomial, mentioned previously. If the Galois group G of the polynomial is a subgroup of A_4, then we say the **parity** of G is $+$. As we saw in the previous section, this occurs precisely when the discriminant of the polynomial is a square in F. Otherwise, we say the parity of G is $-$.

Another invariant we use is the centralizer of G in S_4. This quantity is useful for computing Galois groups since it is isomorphic to the automorphism group of the stem field $F[x]/(f(x))$.

A third invariant is the list of the proper, nontrivial, nonisomorphic subfields of $F[x]/(f(x))$. To see that this quantity is an invariant of G, let $E \leq G$ be the subgroup which fixes $F[x]/(f(x))$, according to the Galois correspondence. In particular, E is isomorphic to $G \cap S_3$, where S_3 is generated by the permutation $(234) \in S_4$. The proper, nontrivial, nonisomorphic subfields of $F[x]/(f(x))$ correspond to conjugacy classes of intermediate groups E' such that $E < E' < G$. Direct computation shows that A_4 and S_4 have no such intermediate subgroups.

Table 3: Invariant data for the possible Galois groups of irreducible quartic polynomials over $F/\mathbf{Q}_p$ where $p > 2$.

$\mathbf{G}$	**Parity**	$\lvert\mathbf{C}_{\mathbf{S}_4}(\mathbf{G})\rvert$
C_4	$-$	4
V_4	$+$	4
D_4	$-$	2

However, C_4 and D_4 each have a unique such subgroup, and V_4 has three. Note that in each case, these intermediate subgroups all have index two inside G, and they therefore correspond to quadratic subfields of $F[x]/(f(x))$. Since we are assuming $p > 2$, we know that $F[x]/(f(x))$ must have at least one quadratic subfield [Rep88]. Therefore, the only possible Galois groups are C_4, V_4, and D_4. For each of these possible Galois groups, Table 3 shows the parity and the order of the centralizer in S_4.

Our remaining lemmas describe how to compute the mass and centralizer order invariants on the field-theoretic side. The first is a standard result for p-adic fields [Lan94, p. 54].

Lemma 4.2. *Let $F/\mathbf{Q}_p$ be a finite extension and let n be an integer with $p \nmid n$. Let $g = \gcd(p^f - 1, n)$ and let $m = n/g$.*

(a) There are g nonisomorphic totally ramified extensions of F of degree n; each with mass m.

(b) Let ζ be a primitive $(p^f - 1)$-st root of unity and let π be a uniformizer for F. Each totally and tamely ramified extension of F of degree n is isomorphic to an extension that is generated by a root of the polynomial $x^n + \zeta^r\pi$, for some $0 \leq r < g$.

Lemma 4.3. *Let K/F be a totally ramified extension of degree n with $p \nmid n$ and let $g = \gcd(p^f - 1, n)$. Let $G = Gal(K^{gal}/F)$. Then*

$$g = |C_{S_n}(G)|.$$

Proof. From Galois theory, we know the automorphism group of K/F is isomorphic to the centralizer of G in S_n. Thus the size of $\mathrm{Aut}(L/K)$ is equal to the order of $C_{S_n}(G)$. Using this fact and the definition of the mass of K/F, we have

$$[K : F] = m(K/F) \cdot |\mathrm{Aut}(K/F)| = m(K/F) \cdot |C_{S_n}(G)|.$$

By Lemma 4.2, we also have

$$[K : F] = m(K/F) \cdot g.$$

These two equations combine to prove the lemma. □

4.2 Proof of Theorem 4.1

Proof. Let F be as in the statement of Theorem 4.1. Let K/F be a totally ramified quartic extension, and let K^{gal}/F denote the Galois closure of K/F. We know the Galois group $G = \text{Gal}(K^{\text{gal}}/F)$ must be either C_4, V_4, or D_4. Let $g = \gcd(p^f - 1, 4)$. Since p is odd, g is 2 or 4. Furthermore, $g = 2$ if and only if $p \equiv -1 \pmod 4$ and f is odd. Otherwise, we must have $g = 4$. Since $g = |C_{S_4}(G)|$, we see that $G = D_4$ if and only if $g = 2$; proving part (1).

If $g = 4$, then G is either C_4 or V_4. Since $V_4 \leq A_4$ and C_4 is not, we see that G is determined by the discriminant of K/F. By Lemma 4.2, the four totally ramified quartic extensions of F are generated by the polynomials $x^4 + \zeta^r\pi$ where ζ is a primitive $(p^f - 1)$-st root of unity, $0 \leq r < 4$, and π is a uniformizer for F. Computing the discriminants of these polynomials, we have

$$\text{disc}(K/F) = \text{disc}(x^4 + \zeta^r\pi) = 256\zeta^{3r}\pi^3,$$

which are clearly not squares in F (because of the odd exponent of π). Thus $G = C_4$ for all four of these extensions; proving part (2). □

Acknowledgements

The authors would like to thank the anonymous referee for their close reading of the paper and their helpful comments. The authors would also like to thank Elon Unversity for supporting this project through internal funding.

References

[AE12] Chad Awtrey and Trevor Edwards, *Dihedral p-adic fields of prime degree*, Int. J. Pure Appl. Math. **75** (2012), no. 2, 185–194.

[Awt11] Chad Awtrey, *On Galois groups of totally and tamely ramified sextic extension of local fields*, Int. J. Pure Appl. Math. **70** (2011), no. 6, 855–863.

[Awt12a] ———, *Dodecic 3-adic fields*, Int. J. Number Theory **8** (2012), no. 4, 933–944. MR 2926553

[Awt12b] ———, *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

[BM83] Gregory Butler and John McKay, *The transitive groups of degree up to eleven*, Comm. Algebra **11** (1983), no. 8, 863–911. MR MR695893 (84f:20005)

[CH08] John J. Cannon and Derek F. Holt, *The transitive permutation groups of degree 32*, Experiment. Math. **17** (2008), no. 3, 307–314. MR 2455702 (2009j:20003)

[CHM98] John H. Conway, Alexander Hulpke, and John McKay, *On transitive permutation groups*, LMS J. Comput. Math. **1** (1998), 1–8 (electronic). MR 1635715 (99g:20011)

[Coh93] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993. MR 1228206 (94i:11105)

[DF04] David S. Dummit and Richard M. Foote, *Abstract algebra*, third ed., John Wiley & Sons Inc., Hoboken, NJ, 2004. MR 2286236 (2007h:00003)

[GAP08] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, 2008.

[Gou97] Fernando Q. Gouvêa, *p-adic numbers*, second ed., Universitext, Springer-Verlag, Berlin, 1997, An introduction. MR 1488696 (98h:11155)

[Hun80] Thomas W. Hungerford, *Algebra*, Graduate Texts in Mathematics, vol. 73, Springer-Verlag, New York, 1980, Reprint of the 1974 original. MR 600654 (82a:00006)

[KW89] Luise-Charlotte Kappe and Bette Warren, *An elementary test for the Galois group of a quartic polynomial*, Amer. Math. Monthly **96** (1989), no. 2, 133–137. MR 992075 (90i:12006)

[Lan94] Serge Lang, *Algebraic number theory*, second ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994. MR 1282723 (95f:11085)

[PAR08] PARI Group, The, *PARI/GP – Computational Number Theory, version 2.3.4*, 2008, available from `http://pari.math.u-bordeaux.fr/`.

[Rep88] Joe Repka, *Quadratic subfields of quartic extensions of local fields*, Internat. J. Math. Math. Sci. **11** (1988), no. 1, 1–4. MR 918210 (89b:11096)

[Ser79] 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)

[SM85] Leonard Soicher and John McKay, *Computing Galois groups over the rationals*, J. Number Theory **20** (1985), no. 3, 273–281. MR MR797178 (87a:12002)

[vdW91] B. L. van der Waerden, *Algebra. Vol. I*, Springer-Verlag, New York, 1991, Based in part on lectures by E. Artin and E. Noether, Translated from the seventh German edition by Fred Blum and John R. Schulenberger. MR 1080172 (91h:00009a)

About the authors:

Chad Awtrey is an assistant professor of mathematics at Elon University. He is passionate about involving undergraduates in research, especially on problems related to p-adic numbers, their extensions, and computational Galois theory.

Brett Barkley, Jeremy Guinn, and Mackenzie McCraw are undergraduate students at Elon University. Brett is an engineering major with interests in aerospace engineering. Jeremy is a math and chemistry double major. Mackenzie is a math with teacher licensure (secondary) major. All three will graduate in 2014, and they plan to attend graduate and/or medical school in the future.

Chad Awtrey

Department of Mathematics and Statistics, Elon University, Campus Box 2320, Elon, NC 27244. cawtrey@elon.edu

Brett Barkley

Department of Mathematics and Statistics, Elon University, Campus Box 2320, Elon, NC 27244. bbarkley@elon.edu

Jeremy Guinn

Department of Mathematics and Statistics, Elon University, Campus Box 2320, Elon, NC 27244. jguinn@elon.edu

Mackenzie McCraw

Department of Mathematics and Statistics, Elon University, Campus Box 2320, Elon, NC 27244. mmccraw@elon.edu