CENTRALIZERS OF TRANSITIVE PERMUTATION GROUPS AND APPLICATIONS TO GALOIS THEORY

CHAD AWTREY, NAKHILA MISTRY, AND NICOLE SOLTZ

ABSTRACT. Let $f(x)$ be an irreducible polynomial of degree n defined over a field F, and let G be the Galois group of f, identified as a transitive subgroup of S_n. Let K/F be the stem field of f. We show the automorphism group of K/F is isomorphic to the centralizer of G in S_n. We include two applications to computing Galois groups; one in the case F is the rational numbers, the other when F is the 5-adic numbers.

1. INTRODUCTION

The work of 19th century mathematician Evariste Galois shows it is possible to associate a group structure to a polynomial's roots. This group, called the polynomial's Galois group, is a collection of permutations of the roots that encodes much arithmetic information concerning the polynomial. For example, the polynomial is solvable by radicals if and only if its Galois group is solvable (see for example [4, p. 628]). Recall that a polynomial is said to be solvable by radicals if its roots can be expressed using the following three items: (1) the polynomial's coefficients, (2) the four basic arithmetic operations $(+, -, \times, \div)$, and (3) radicals (square roots, cube roots, etc.).

An important problem in computational algebra therefore is to determine the Galois group of a polynomial $f(x)$ of degree n defined over a field F. Most practical methods for computing Galois groups focus on factoring what are known as resolvent polynomials [5, 13, 14]. These are polynomials that define subfields of the splitting field of f. But the resolvent method can be computationally expensive, since resolvent polynomials generally have large degree (which makes factoring difficult) and/or they are formed using complex or p-adic approximations (this requires high precision for proven results). Implementations of these methods over $\mathbf{Q}$ can be found in many software programs, including but not limited to GAP [6] and PARI/GP [11]. We note that no general implementations exist for computing Galois groups over the field of p-adic numbers $\mathbf{Q}_p$.

In this paper, we present a simple alternative to the resolvent method. Our approach is based on the centralizer of the Galois group in S_n (the symmetric group of degree n). After providing a brief overview in Section 2 of the basic notation and terminology related to the Fundamental Theorem of Galois Theory, Section 3 contains a proof that the centralizer of the Galois group in S_n of an irreducible polynomial of degree n is isomorphic to the automorphism group of the polynomial's stem field (cf. Theorem 3.6) .

2010 *Mathematics Subject Classification.* 20B35, 12Y05, 11R32, 11S20.

Key words and phrases. Galois group computation; centralizers; normalizers; p-adic fields; quartic extensions.

Our final two sections provide applications of Theorem 3.6 to computing Galois groups. Section 4 gives an algorithm for computing Galois groups of irreducible quartic polynomials over arbitrary base fields (of characteristic $\neq 2$). This algorithm is an improvement over the traditional methods that use resolvent polynomials [3,8]. Section 5 gives a complete classification of all isomorphism classes of degree 15 extensions of the 5-adic numbers whose Galois group is isomorphic to a direct product of the form $H \times C_3$ where H is a solvable transitive subgroup of S_5 and C_3 is the cyclic group of order 3. Note, there are only finitely many such isomorphism classes [9, p. 54]. This extends previous research on classifying finite extensions of $\mathbf{Q}_p$; see [1, 2] for the most recent results in this area.

2. Definitions

In this section we provide basic notation and terminology related to field extensions and their automorphism groups for the purpose of introducing the Fundamental Theorem of Galois Theory. Let F be a field and let $\overline{F}$ be a fixed algebraic closure. Let $f(x) \in F[x]$ be an irreducible polynomial of degree n with roots $\alpha_1, \ldots, \alpha_n \in \overline{F}$. Let K be the **stem field** of f; that is, $K = F(\alpha_1)$.

Then it is straight forward to verify that K is a vector space over F with the set $\{1, \alpha, \ldots, \alpha^{-1}\}$ serving as a basis. Since the dimension of K as an F-vector space is n, we say K/F is an extension field of **degree** n and we write $[K : F] = n$.

We are interested primarily in automorphisms of K/F, which are field isomorphisms from K to itself that restrict to the identity function on F.

Definition 2.1. An **automorphism** of K/F is a mapping $\sigma : K \to K$ such that,

(1) σ is bijective,
(2) $\sigma(x + y) = \sigma(x) + \sigma(y)$ for all $x, y \in K$,
(3) $\sigma(xy) = \sigma(x)\sigma(y)$ for all $x, y \in K$,
(4) $\sigma(a) = a$ for all $a \in F$.

The collection of all automorphisms of K/F is denoted $\mathrm{Aut}(K/F)$.

The automorphisms of K/F form a group under function composition. Since automorphisms are field isomorphisms and since a basis for K/F consists of powers of the one root α_1, it follows that each automorphism is completely determined by where it sends α_1. Furthermore, since automorphisms act like the identity function on F, we have $0 = \sigma(0) = \sigma(f(\alpha_1)) = f(\sigma(\alpha_1))$ for each $\sigma \in \mathrm{Aut}(K/F)$. This shows that automorphisms send α_1 to some other root of f that lies in K. Therefore, the automorphisms of K/F are in one-to-one correspondence to the roots of f that lie in K.

Definition 2.2. If K/F contains all n roots of f, then we say K/F is a **Galois extension**. In this case, we call $\mathrm{Aut}(K/F)$ the **Galois group** of f. If K/F contains fewer than n roots of f, the Galois group of f is defined to be $\mathrm{Aut}(K^g/F)$ where K^g is the splitting field of f, the smallest subfield of $\overline{F}$ that contains F and all n roots of f.

The next result is the Fundamental Theorem of Galois Theory, which gives a bijection between the subfields of K/F and the subgroups of $\mathrm{Aut}(K/F)$ when K/F is a Galois extension (see [4, p. 574]).

Theorem 2.3 (Fundamental Theorem of Galois Theory)**.** *Let K/F be a Galois extension with Galois group G. Let E be a subfield of K/F, H a subgroup of G,*

and K^H the collection of elements in K fixed by all the elements of H (called the ***fixed field*** *of H). That is, $K^H = \{k \in K : \sigma(k) = k \text{ for all } \sigma \in H\}$.*

(1) *K^H is a subfield of K/F.*
(2) *The maps $E \mapsto Aut(K/E)$ and $H \mapsto K^H$ are inverses of each other.*
(3) *$[K : E] = \#H$ and $[E : F] = [G : H]$ (the index of H in G).*
(4) *K/E is a Galois extension with Galois group H.*
(5) *E/F is a Galois extension if and only if H is normal in G. In this case, $Aut(E/F) \simeq G/H$.*

We now prove several facts about subfields of K and subgroups of $\mathrm{Aut}(K/F)$. The first considers conjugate fields of a subfield E of K/F. For $\sigma \in \mathrm{Aut}(K/F)$ a subfield E of K/F, the image $\sigma(E)$ of E under σ is called a **conjugate field** of E. The next result shows that conjugate fields correspond to conjugate subgroups.

Proposition 2.4. *Let K/F be a Galois extension with Galois group G. Let H be a subgroup of G and let E be the fixed field of H. For $\sigma \in G$, the subgroup fixing $\sigma(E)$ is $\sigma H \sigma^{-1}$.*

Proof. First we show $\sigma H \sigma^{-1}$ fixes $\sigma(E)$. Let $\sigma h \sigma^{-1} \in \sigma H \sigma^{-1}$ and let $\sigma(x) \in \sigma(E)$. Then $\sigma h \sigma^{-1}(\sigma(x)) = \sigma h(x) = \sigma(x)$, as desired.

Next we show that every element that fixes $\sigma(E)$ belongs to $\sigma H \sigma^{-1}$. Suppose $\tau \in G$ fixes $\sigma(E)$. Then for all $x \in E$, $\tau(\sigma(x)) = \sigma(x)$. Thus $\sigma^{-1}\tau\sigma(x) = x$. Thus $\sigma^{-1}\tau\sigma$ fixes E, which implies $\sigma^{-1}\tau\sigma \in H$. Thus $\tau \in \sigma H \sigma^{-1}$, as desired. □

Proposition 2.5. *Let K/F be a Galois extension with Galois group G. Let H be a subgroup of G and let E be the fixed field of H. Let $\sigma, \tau \in G$. Then $\sigma(x) = \tau(x)$ for all $x \in E$ if and only if $\tau \in \sigma H$.*

Proof. Let $\sigma, \tau \in G$ and suppose $\sigma(x) = \tau(x)$ for all $x \in E$. Then $x = \sigma^{-1}\tau(x)$ for all $x \in E$. Thus $\sigma^{-1}\tau$ fixes E, which is true if and only if $\sigma^{-1}\tau \in H$. This is true if and only if $\tau \in \sigma H$, as desired. □

Proposition 2.6. *Let K/F be a Galois extension with Galois group G. Let H be a subgroup of G and let E be the fixed field of H. Then $Aut(E/F) \simeq N(H)/H$, where $N(H)$ is the normalizer of H in G.*

Proof. First we note that every element in $\mathrm{Aut}(E/F)$ corresponds to some restriction to E of an element $\sigma \in G$ [4, p. 575]. Such an element σ will restrict to an automorphism of E/F precisely when $\sigma(E) = E$. By Proposition 2.4, these are restrictions of elements in the normalizer $N(H)$ of H in G. By Proposition 2.5, the elements in $N(H)$ that restrict to distinct functions on E correspond to the cosets of H in $N(H)$. Therefore $\mathrm{Aut}(E/F)$ is isomorphic to the quotient group $N(H)/H$, as desired. □

3. Centralizers and Automorphism Groups

In this section, we prove that the automorphism group of the stem field of an irreducible degree n polynomial $f(x)$ defined over a field F is isomorphic to the centralizer of its Galois group in S_n. Our proof involves analyzing two group actions on suitably chosen cosets of the Galois group. We begin with preliminary definitions and results.

Definition 3.1. Let G be a group with identity element e, and let X be a set. A **group action** of G on X is a function from $G \times X$ to X where the image of (g, x), denoted by $g \cdot x$, satisfies the following two properties:

(1) $e \cdot x = x$ for all $x \in X$
(2) $g \cdot (h \cdot x) = (gh) \cdot x$ for all $x \in X$ and all $g, h \in G$

For each $g \in G$, we can define a function $\sigma_g : X \to X$ by $\sigma_g(x) = g \cdot x$. It is straightforward to verify that each σ_g has the following properties.

- σ_g is a permutation, hence $\sigma_g \in S_X$.
- $\sigma_g \sigma_h = \sigma_{gh}$.
- $\sigma_e = \mathrm{id}_X$.
- $\sigma_g^{-1} = \sigma_{g^{-1}}$.
- The function $\phi : G \to S_X$ defined by $\phi(g) = \sigma_g$ is a homomorphism.

The function ϕ is called the **permutation representation** of G acting on X.

Now we consider a group G acting on left cosets of some subgroup $H \leq G$.

Proposition 3.2. *Let G be a group with identity element e, and let H be a subgroup of G. Let L be the set of left cosets of H in G. Then G acts on L by left multiplication; i.e., for each $a \in G$,*

$$g \cdot (aH) = (ga)H,$$

defines a group action of G on L. Let $\lambda : G \to S_L$ be the permutation representation of this action. Then

$$Ker\ \lambda = \bigcap_{g \in G} gHg^{-1}.$$

Proof. That G defines a group action on L follows directly from the two defining properties of group actions. Let $\lambda : G \to S_L$ be the permutation representation of this action, so that $\lambda(g) = \sigma_g$ where $\sigma_g(aH) = gaH$. Then we have,

$$\begin{aligned}
\text{Ker } \lambda &= \{g \in G : \sigma_g = \mathrm{id}_L\} \\
&= \{g \in G : \sigma_g(aH) = aH \text{ for all } a \in G\} \\
&= \{g \in G : gaH = aH \text{ for all } a \in G\} \\
&= \{g \in G : a^{-1}ga \in H \text{ for all } a \in G\} \\
&= \{g \in G : g \in aHa^{-1} \text{ for all } a \in G\} \\
&= \bigcap_{g \in G} gHg^{-1}.
\end{aligned}$$

□

We now give two consequences of Proposition 3.2 that will be useful in our proof of Theorem 3.6. For $G \leq S_n$, let G_i denote the **point stabilizer** of i in G; that is, $G_i = \{g \in G : g(i) = i\}$.

Corollary 3.3. *Let G be a transitive subgroup of S_n, G_1 the point stabilizer of 1 in G, L the left cosets of G_1 in G, and λ the permutation representation of G acting on L by left multiplication. Then we have the following isomorphisms:*

(1) $S_L \simeq S_n$, *and*
(2) $\lambda(G) \simeq G$.

Proof. To prove item (1), we show there is a well-defined bijection from L to the set $\{1, \ldots, n\}$. Toward that end, let $\sigma \in G$ and suppose $\sigma(1) = i$. Then for every $a \in G_1$, we have $\sigma a(1) = i$, since $a(1) = 1$. Thus every element in the coset σG_1 sends 1 to i. Moreover, if $\tau \in G$ is any other element such that $\tau(1) = i$, then $\sigma^{-1}\tau(1) = \sigma^{-1}(i) = 1$. This shows that $\sigma^{-1}\tau \in G_1$; i.e., that $\tau \in \sigma G_1$. Thus the map from L to the set $\{1, \ldots, n\}$ is a well-defined injection. The map is surjective because G is transitive. Therefore $[G : G_1] = n$, and it follows that S_L is isomorphic to S_n in a natural way.

To prove item (2), we show that Ker λ is trivial. By Proposition 3.2, we have

$$\text{Ker } \lambda = \bigcap_{g \in G} gG_1g^{-1}.$$

For $g \in G$, if $g(1) = i$, then $gG_1g^{-1} = G_i$. Thus Ker λ consists of those elements $g \in G$ such that $g(i) = i$ for every $i \in \{1, \ldots, n\}$. The only such element is the identity. This proves Ker λ is trivial, and therefore $\lambda(G) \simeq G$ by the First Isomorphism Theorem. □

We now introduce another action on the left cosets of H. This action involves the normalizer $N(H)$ of H in G.

Proposition 3.4. *Let G be a group, $H \leq G$, $N(H)$ the normalizer of H in G, and L the left cosets of H in G. Then $N(H)$ acts on L by the following action:*

$$n \cdot (aH) = an^{-1}H.$$

Let $\rho : N(H) \to S_L$ be the permutation representation of this action. Then Ker $\rho = H$ and $\rho(N(H)) \simeq N(H)/H$.

Proof. First we show that $N(H)$ exhibits a well-defined action on L. Let $a, b \in G$ and suppose $aH = bH$. Then for all $n \in N(H)$,

$$\begin{aligned} n \cdot (aH) &= an^{-1}H \\ &= aHn^{-1} && \text{since } n \in N(H) \\ &= bHn^{-1} && \text{since } aH = bH \\ &= bn^{-1}H && \text{since } n \in N(H) \\ &= n \cdot (bH). \end{aligned}$$

Thus the action is well-defined. Next, we have

$$e \cdot (aH) = (ae^{-1})H = aH.$$

And if $x, y \in N(H)$, then we also have

$$\begin{aligned} x \cdot (y \cdot (aH)) &= x \cdot (ay^{-1}H) \\ &= ay^{-1}x^{-1}H \\ &= a(xy)^{-1}H \\ &= (xy) \cdot aH. \end{aligned}$$

So $N(H)$ does act on L. Let $\rho : N(H) \to S_L$ be the permutation representation of this action, so that $\rho(n) = \sigma_n$ where $\sigma_n(aH) = an^{-1}H$. Then we have,

$$\begin{aligned}\text{Ker } \rho &= \{n \in N(H) : \sigma_n = \text{id}_L\} \\ &= \{n \in N(H) : \sigma_n(aH) = aH \text{ for all } a \in G\} \\ &= \{n \in N(H) : an^{-1}H = aH \text{ for all } a \in G\} \\ &= \{n \in N(H) : n^{-1} \in H\} \\ &= H.\end{aligned}$$

The final statement in the proposition now follows from the First Isomorphism Theorem. □

Our next result proves an important relationship between the two permutation representations λ and ρ.

Proposition 3.5. *Let G be a group, $H \leq G$, $N(H)$ the normalizer of H in G, and L the left cosets of H in G. Let $\lambda : G \to S_L$ and $\rho : N(H) \to S_L$ be the permutation representations in Propositions 3.2 and 3.4, respectively. Thus for a coset aH of H, we have $\lambda(g)(aH) = gaH$ and $\rho(n)(aH) = an^{-1}H$ for all $g, a \in G$ and all $n \in N(H)$. Then*

$$C_{S_L}(\lambda(G)) = \rho(N(H)),$$

where $C_{S_L}(\lambda(G))$ is the centralizer of $\lambda(G)$ in S_L.

Proof. First we show that $\rho(N(H)) \subseteq C_{S_L}(\lambda(G))$. Let $n \in N(H)$ and let $g \in G$ be arbitrary. We will show that $\rho(n)\lambda(g)\rho(n)^{-1} = \lambda(g)$ as permutations of S_L. Note that $\rho(n)^{-1} = \rho(n^{-1})$ (see Definition 3.1). Then, for $aH \in L$, we have

$$\begin{aligned}\rho(n)\lambda(g)\rho(n^{-1})(aH) &= \rho(n)\lambda(g)(anH) \\ &= \rho(n)(ganH) \\ &= gann^{-1}H \\ &= gaH \\ &= \lambda(g)(aH).\end{aligned}$$

Thus $\rho(N(H)) \subseteq C_{S_L}(\lambda(G))$.

Conversely, let $\sigma \in C_{S_L}(\lambda(G))$ be arbitrary. Let $n \in G$ be defined by $\sigma(H) = nH$. Since $\sigma \in C_{S_L}(\lambda(G))$, this means $\sigma\lambda(a) = \lambda(a)\sigma$ for all $a \in G$. Evaluating both sides of the equation at H, we obtain:

$$\sigma(aH) = anH.$$

If we can show $n \in N(H)$, then we are done since this proves $\sigma = \rho(n^{-1}) \in \rho(N(H))$. Toward that end, let $h \in H$. Then we have

$$\begin{aligned}\sigma(nhn^{-1}H) &= nhn^{-1}nH \\ &= nhH \\ &= nH \\ &= \sigma(H).\end{aligned}$$

Since σ is a permutation, this implies $nhn^{-1}H = H$; i.e., $nhn^{-1} \in H$. Thus $n \in N(H)$, as desired. □

We are now able to prove our main result concerning automorphism groups of stem fields of polynomials.

Theorem 3.6. *Let $f(x)$ be an irreducible degree n polynomial defined over a field F. Let $\alpha_1, \ldots, \alpha_n$ be the roots of f in some algebraic closure of F. Let $K = F(\alpha_1)$ be the stem field of f, and let G be the Galois group of f over F. Then $Aut(K/F) \simeq C_{S_n}(G)$, where $C_{S_n}(G)$ is the centralizer of G in S_n. In particular, the order of the centralizer of G in S_n equals the number of roots of f in K.*

Proof. We first note that since f is irreducible, G is necessarily a transitive subgroup of S_n. Now let G_1 be the point stabilizer of 1 in G. Thus G_1 corresponds to K under the Galois correspondence of Theorem 2.3, since G_1 consists of those elements of G that fix α_1 (and hence fix all of K). Let L be the left cosets of G_1 in G, $N(G_1)$ the normalizer of G_1 in G, λ and ρ the permutation representations appearing in Propositions 3.2 and 3.4, respectively, and $C_{S_L}(\lambda(G))$ the centralizer of $\lambda(G)$ in S_L. Therefore, we have the following string of isomorphisms:

$$\begin{aligned} C_{S_n}(G) &\simeq C_{S_L}(\lambda(G)) && \text{Corollary 3.3} \\ &\simeq \rho(N(G_1)) && \text{Proposition 3.5} \\ &\simeq N(G_1)/G_1 && \text{Proposition 3.4} \\ &\simeq \mathrm{Aut}(K/F) && \text{Proposition 2.6.} \end{aligned}$$

The final sentence in the statement of the Theorem now follows, since the automorphisms of K/F are in one-to-one correspondence with the roots of f in K. □

4. Application: Quartic Galois groups

In this section, let $f(x)$ denote an irreducible quartic polynomial defined over the rational numbers and let G be the Galois group of f. We give an algorithm for determining G that does not involve factoring resolvent polynomials like the traditional approaches [3,8]. Though we are focusing on the case where f is defined over $\mathbf{Q}$, we point out that our method is valid over any field of characteristic different from two.

First we describe the possibilities for G. Since $f(x)$ is irreducible, G can be identified with a transitive subgroup of S_4, well defined up to conjugation (different orderings of the roots correspond to conjugate subgroups). There are five conjugacy classes of transitive subgroups of S_4. Table 1 contains information on one representative group from each of these conjugacy classes, including the representative's **Name**, **Size**, and **Generators**. The names are standard: C_4 is the cyclic group of order 4, E_4 is the elementary abelian group of order 4, $C_2 \times C_2$ (also called the Klein 4-group), D_4 is the dihedral group of order 8, and A_4 and S_4 are the alternating and symmetric groups, respectively. The table also gives the order of the centralizer in S_4 in column $|\mathbf{C}|$ and the **Parity** of the group. The parity of a transitive subgroup $G \leq S_n$ is $+$ if $G \leq A_n$ and $-$ otherwise.

There is something important to observe about Table 1. If we consider the two columns $|\mathbf{C}|$ and **Parity**, then no two groups have the same values for these two characteristics. This observation forms the core of our algorithm for computing the Galois group of an irreducible quartic polynomial (see Theorem 4.3). Before stating our algorithm, we introduce an important quantity associated to each polynomial.

TABLE 1. Possible Galois groups of irreducible quartic polynomials.

Name	Size	Generators	|C|	Parity
C_4	4	(1234)	4	−
E_4	4	(12)(34), (13)(24)	4	+
D_4	8	(13), (1234)	2	−
A_4	12	(123), (124)	1	+
S_4	24	(12), (1234)	1	−

Definition 4.1. Let $f(x)$ be a degree n polynomial defined over a field F, and let $\alpha_1, \ldots, \alpha_n$ be the roots of f in a fixed algebraic closure of F. The **discriminant** of f is defined as

$$\mathrm{Disc}(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

The discriminant of a polynomial is related to its Galois group in the following way. See [4, p. 610] for a proof.

Proposition 4.2. *If $f(x)$ is a degree n polynomial defined over a field F with Galois group G, then Disc(f) is a perfect square in F if and only if $G \leq A_n$.*

Furthermore, by the theory of elementary symmetric polynomials, it follows that $\mathrm{Disc}(f)$ can be expressed using only the coefficients of f [4, p. 611]. For example, in the case of quartic polynomials, [11] gives the following:

$$\begin{aligned}\mathrm{Disc}(x^4 + ax^3 + bx^2 + cx + d) = &-27a^4d^2 + 2a^3c(9bd - 2c^2) \\ &- a^2(4b^3d - b^2c^2 - 144bd^2 + 6c^2d) \\ &- 2ac(40b^2d - 9bc^2 + 96d^2) \\ &+ 4b(4b^3 - b^2c^2 - 32bd^2 + 36c^2d) \\ &- 27c^4 + 256d^3.\end{aligned}$$

The discriminant is used in the traditional approaches to computing Galois groups of quartic polynomials [3, 8]. We now give a brief description of each of these methods.

The approach taken in [8] involves computing and factoring a cubic polynomial that is related to the original quartic f. If this cubic polynomial is irreducible, the Galois group of f is either A_4 or S_4, depending on whether the discriminant is a perfect square. In all other cases, the cubic polynomial has a rational root. If the cubic has three rational roots, then the Galois group is E_4. Otherwise, the cubic has an irreducible quadratic factor $g(x)$. The Galois group of f is C_4 if $g(x)$ factors into two linear factors over the stem field of $x^2 - \mathrm{Disc}(f)$, and it is D_4 otherwise.

The approach taken in [3] is more streamlined, as it involves only the discriminant of f as well as computing and factoring a degree 6 polynomial $g(x)$ that is related to f. Let L be the list of the degrees of the irreducible factors of $g(x)$. The Galois group of f is C_4 if $L = \{1, 1, 4\}$, E_4 if $L = \{2, 2, 2\}$, and D_4 if $L = \{2, 4\}$. If $g(x)$ is irreducible, then the Galois group of f is A_4 if $\mathrm{Disc}(f)$ is a perfect square and S_4 otherwise.

Our approach is similar to the one in [3]. We also make use of the discriminant of f, but instead of factoring a related degree 6 polynomial, we count the number of roots of f in its stem field (which is equivalent to factoring f over its stem field and counting linear factors).

Theorem 4.3. *Let $f(x) \in \mathbf{Z}[x]$ be an irreducible quartic polynomial, and let K be the stem field of f. Let $\#A$ be the number of roots of f in K, $D = Disc(f)$, and G the Galois group of f.*

(1) *If $\#A = 4$, then $G = E_4$ if D is a perfect square and C_4 otherwise.*
(2) *If $\#A = 2$, then $G = D_4$.*
(3) *If $\#A = 1$, then $G = A_4$ if D is a perfect square and S_4 otherwise.*

Proof. By Proposition 4.2, D is a perfect square if and only if the parity of G is $+$. Since the number of roots of f in K is equal to the size of $\mathrm{Aut}(K/\mathbf{Q})$, Theorem 3.6 therefore shows $\#A$ equals the order of the centralizer of G in S_4. The validity of our algorithm now follows by examining the columns $|\mathbf{C}|$ and **Parity** in Table 1. □

Examples. To illustrate our algorithm, we compute the Galois groups of the following three polynomials: $A(x) = x^4 + 3x + x$, $B(x) = x^4 + 5x + 5$, and $C(x) = x^4 + 7x + 7$. Let α, β, and γ denote a root of A, B, and C, respectively. Thus the stem field of A is $\mathbf{Q}(\alpha)$, the stem field of B is $\mathbf{Q}(\beta)$, and the stem field of C is $\mathbf{Q}(\gamma)$. Note that we can factor a polynomial over its stem field using Algorithm 3.6.4 in [3].

There are two roots of $A(x)$ in its stem field; these are α and $\frac{1}{5}(4\alpha^3 - 2\alpha^2 + \alpha + 9)$. According to Table 1, D_4 is the only group with centralizer order 2. Thus the Galois group of $A(x)$ is D_4.

There are four roots of $B(x)$ in its stem field; these are β, $-\frac{1}{11}(4\beta^3 + 2\beta^2 + 1\beta + 15)$, $-\frac{1}{11}(4\beta^3 - 9\beta^2 + 12\beta + 15)$, and $\frac{1}{11}(8\beta^3 - 7\beta^2 + 2\beta + 30)$. Therefore the Galois group is either C_4 or E_4. Factoring the discriminant, we see that $\mathrm{Disc}(B(x)) = 5^3 \cdot 11^2$, which is not a perfect square (because of the odd exponent of 5). Thus the Galois group of $B(x)$ is C_4.

There is only one root of $C(x)$ in its stem field; namely, γ. So the Galois group of $C(x)$ is either A_4 or S_4. Factoring the discriminant, we see that $\mathrm{Disc}(C(x)) = 7^3 \cdot 67$, which is also not a square. We conclude that the Galois group of $C(x)$ is S_4.

5. Application: Degree 15 5-adic Fields

Our final section deals with computing Galois groups of degree 15 polynomials defined over the field of 5-adic numbers. In the first subsection, we give a brief introduction to p-adic numbers $\mathbf{Q}_p$ and their extensions fields. Those interested in more details can find a good elementary account of p-adic numbers in [7]. Next, we describe the possible Galois groups of degree 15 polynomials defined over $\mathbf{Q}_5$ (see Table 2). For such a polynomial f, we then develop an algorithm for determining its Galois group G when G is a direct product of the form $H \times C_3$ where H is a solvable transitive subgroup of S_5. Since the number of isomorphism classes of degree n extensions of $\mathbf{Q}_p$ is finite [9, p. 54], we determine all isomorphism classes of degree 15 extensions of $\mathbf{Q}_5$ whose Galois group is of the form $H \times C_3$ (mentioned above). We find that there 26 such extensions. We end with Tables 3 and 4 which give a defining polynomial for each extension along with a few of the extension's invariants.

5.1. **Introduction to 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 [7, p. 63].

The ring of **p-adic integers** $\mathbf{Z}_p$ is defined as the set $\{x \in \mathbf{Q}_p : |x|_p \leq 1\}$. The ring $\mathbf{Z}_p$ has a unique maximal ideal; namely, $p\mathbf{Z}_p$. It follows that every ideal of $\mathbf{Z}_p$ is of the form $p^c\mathbf{Z}_p$ for some integer c. 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" [7, p. 68]

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

Since $\mathbf{Q}_p$ has characteristic 0, the Primitive Element Theorem shows that an extension field of $\mathbf{Q}_p$ arises by adjoining the root of some monic irreducible polynomial over $\mathbf{Z}_p$ [4, p. 595]. By Krasner's Lemma [9, 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 $g(y) = y^d + a_{d-1}y^{d-1} + \cdots + a_1 y + a_0$ be its minimal polynomial. We define the **norm** of x from K down to $\mathbf{Q}_p$ as,

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

The norm is used to define an absolute value on K that extends the p-adic absolute value on $\mathbf{Q}_p$ [7, p. 151]. For $x \in K$, we define

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

The absolute value on an extension K gives rise to the corresponding valuation v on K by using the equation: $|x| = p^{-v(x)}$, where $v(0) = \infty$.

The valuation on K 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 divides $[K : \mathbf{Q}_p]$ [7, p. 159]. We call e the **ramification index** of $K/\mathbf{Q}_p$. The discriminant of K, denoted by $\mathrm{Disc}(K)$, is an ideal of $\mathbf{Z}_p$. We define the **discriminant exponent** of K to be the integer c such that $\mathrm{Disc}(K) = p^c\mathbf{Z}_p$.

5.2. **Galois Groups of Degree 15 5-adic Fields.** If $f(x) \in \mathbf{Z}_5[x]$ is an irreducible polynomial of degree 15, then it follows that the Galois group G of f over $\mathbf{Q}_p$ is a transitive subgroup of S_{15}, of which there are 104. However, the arithmetic in extensions of $\mathbf{Q}_p$ is specialized, and this limits the possibility for what G can be.

For example, in [1, Lemma 2.2] it is shown that G must have the following properties:

- G contains a normal subgroup I such that G/I is cyclic.

TABLE 2. The 24 transitive subgroups of S_{15} that are possible Galois groups of degree 15 polynomials defined over $\mathbf{Q}_5$.

T	**Size**	**|C|**	**Parity**
1	15	15	+
2	30	1	−
3	30	3	+
4	30	5	−
6	60	1	+
7	60	1	−
8	60	3	−
9	75	5	+
11	120	1	−
12	150	1	+
13	150	5	−
14	150	1	−
17	300	1	+
18	300	1	−
19	300	1	−
25	375	5	+
27	600	1	−
30	750	1	+
31	750	1	−
32	750	5	−
37	1500	1	+
38	1500	1	−
40	1500	1	−
49	3000	1	−

- I contains a normal subgroup W such that W is a 5-group (possibly trivial).
- I/W is cyclic of order dividing $5^{[G:I]} - 1$.

Using the software GAP [6], direct computation on the 104 transitive subgroups of S_{15} shows that only 24 groups are possible Galois groups of degree 15 polynomials over $\mathbf{Q}_5$. We identify these groups in Table 2 using the transitive numbering system in [6]. Specifically, an entry of j in column **T** refers to the group `TransitiveGroup(15,`j`)` in GAP. The table also includes the **Size** of each group, the order of its centralizer in S_{15} (in column $|\mathbf{C}|$), and its **Parity**.

Notice that one group in Table 2 has a centralizer order of 15 and two have a centralizer order of 3. These three groups are T1 = C_{15}, T3 = $D_5 \times C_3$, and T8 = $F_5 \times C_3$. Here F_5 is the Frobenius group of order 20; it is a semidirect product $C_5 \rtimes C_4$, generated by (12345) and (2354). Note that these three groups are of the form $H \times C_3$ where H is a solvable transitive subgroup of S_5.

The group T1 is the only group among the 24 whose centralizer in S_{15} has 15 elements. Similarly, T3 and T8 are the only groups whose centralizers have 3 elements, and these two groups have different parities. We have therefore proven the following theorem, which determines when a degree 15 polynomial defined over $\mathbf{Q}_5$ has a Galois group among T1, T3, and T8.

Theorem 5.1. *Let f(x) be an irreducible degree 15 polynomial defined over the 5-adic numbers, and let K be the stem field of f. Let $\#A$ be the number of roots of f in K, $D = Disc(f)$, and G the Galois group of f.*

(1) *If $\#A = 15$, then $G = C_{15}$.*

TABLE 3. Polynomials over $\mathbf{Q}_5$ whose Galois group is T1 or T3. Also included are the extension's ramification index **e** and discriminant exponent **c**. The table is sorted first by Galois group, then by ramification index, then by discriminant exponent.

Polynomials	**e**	**c**	**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
$x^{15} + 90x^{14} + 15x^{13} + 70x^{12} + 110x^{11} + 60x^{10} + 85x^9 + 110x^8 + 5x^7$ $+15x^6 + 14x^5 + 15x^4 + 75x^3 + 90x^2 + 20x + 43$	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

(2) *If $\#A = 3$, then $G = D_5 \times C_3$ if D is a perfect square and $F_5 \times C_3$ otherwise.*

Since the number of degree 15 extensions of $\mathbf{Q}_5$ is finite [9, p. 54], we can count how many extensions have Galois group C_{15}, $D_5 \times C_3$, and $F_5 \times C_3$. First, we use [12] to compute polynomials defining all nonisomorphic degree 15 extension of $\mathbf{Q}_5$. There are 1012 such polynomials. For each polynomial, we compute the number of roots of that polynomial in its stem field. This is possible using the p-adic root-finding algorithm in [10]. We extract those polynomials whose stem field contains either 15 roots or 3 roots. If the stem field contains 15 roots, then the Galois group is C_{15}.

Otherwise, we compute the polynomial's discriminant and determine if it is a perfect square in $\mathbf{Q}_5$. This is a straightforward task due to Hensel's Lemma [7, p. 71]. In particular, we write $D = p^k u$ where $\gcd(p, u) = 1$. Then D is a perfect square in $\mathbf{Q}_5$ if and only if k is even and u is a quadratic residue modulo 5. If the discriminant is a perfect square, then $G = D_5 \times C_3$. Otherwise $G = F_5 \times C_3$.

Of the 1012 polynomials defining nonisomorphic degree 15 extensions of $\mathbf{Q}_5$, six have C_{15} as Galois group, three have $D_5 \times C_3$ as Galois group, and 17 have $F_5 \times C_3$ as Galois group. Tables 3 and 4 list these 26 polynomials, their Galois group, and the ramification index e and discriminant exponent c of their stem field.

ACKNOWLEDGEMENTS

The authors were supported in part by NSF grant #DMS-1148695. The authors would like to thank the anonymous reviewer for their close reading and helpful comments, Elon University for supporting this project, and the Center for Undergraduate Research in Mathematics for their support.

TABLE 4. Polynomials over $\mathbf{Q}_5$ whose Galois group is T8. This is a continuation of Table 3.

Polynomials	e	c	G
$x^{15} + 20x^{11} + 22x^{10} + 5x^9 + 15x^5 + 10x^4 + 10x^3 + 5x^2 + 15x + 3$	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

REFERENCES

1. 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
2. Chad Awtrey and Erin Strosnider, *A linear resolvent for degree 14 polynomials*, Collaborative Mathematics and Statistics Research: Topics from the 9th Annual UNCG Regional Mathematics in Statistics Conference, Springer Proceedings of Mathematics & Statistics, vol. 109, Springer, New York, 2015, pp. 43–50.
3. Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993. MR 1228206 (94i:11105)
4. David S. Dummit and Richard M. Foote, *Abstract algebra*, third ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004. MR 2286236 (2007h:00003)
5. Claus Fieker and Jürgen Klüners, *Computation of Galois groups of rational polynomials*, LMS J. Comput. Math. **17** (2014), no. 1, 141–158. MR 3230862
6. The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, 2008.
7. Fernando Q. Gouvêa, *p-adic numbers*, second ed., Universitext, Springer-Verlag, Berlin, 1997, An introduction. MR 1488696 (98h:11155)

8. 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)
9. Serge Lang, *Algebraic number theory*, second ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994. MR 1282723 (95f:11085)
10. Peter Panayi, *Computation of leopoldt's p-adic regulator*, Ph.D. thesis, University of East Anglia, December 1995.
11. PARI Group, The, *PARI/GP – Computational Number Theory, version 2.3.4*, 2008, available from `http://pari.math.u-bordeaux.fr/`.
12. 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)
13. Leonard Soicher and John McKay, *Computing Galois groups over the rationals*, J. Number Theory **20** (1985), no. 3, 273–281. MR MR797178 (87a:12002)
14. Richard P. Stauduhar, *The determination of Galois groups*, Math. Comp. **27** (1973), 981–996. MR 0327712 (48 #6054)

Elon University, Campus Box 2320, Elon, NC 27244
E-mail address: `cawtrey@elon.edu`

Department of Mathematics, Mathematics Building, University of Maryland, College Park, MD 20742
E-mail address: `nmistry@elon.edu`

Department of Mathematics and Statistics, Elon University, Campus Box 5814, Elon, NC 27244
E-mail address: `nsoltz@elon.edu`