GALOIS GROUPS OF DEGREE 12 2-ADIC FIELDS WITH TRIVIAL AUTOMORPHISM GROUP

CHAD AWTREY, NICOLE MILES, CHRISTOPER SHILL, AND ERIN STROSNIDER

Abstract. We classify all degree 12 extensions of the 2-adic numbers that have a trivial automorphism group. Up to isomorphism, we find that there are 111 such extensions. For each extension, we compute a defining polynomial, the ramification index, residue degree, discriminant, and the Galois group of the normal closure. These results extend previous work in the area of constructive local field theory recently initiated by Pauli-Roblot and Jones-Roberts.

1. Introduction

Let p be a prime number. The p-adic numbers $\mathbf{Q}_p$ and their finite extensions (referred to as p-adic fields) are a foundational tool in many areas of number theory — e.g., number fields, elliptic curves, L-functions, and Galois representations — and they are connected to practical applications in physics and cryptography. Of particular interest to number theorists is the role they play in computational attacks on certain unsolved questions in number theory, such as the Riemann Hypothesis and the Birch and Swinnerton-Dyer conjecture (among others). The task of classifying p-adic fields therefore has merit, since the outcomes of such a pursuit can provide computational support to the afore-mentioned problems as well as other number-theoretic investigations.

Let n be a positive integer. Classifying extensions of $\mathbf{Q}_p$ of degree n entails gathering explicit data that uniquely determine the extensions, including,

(1) the number of nonisomorphic extensions for a given prime p and degree n (necessarily finite [14, p. 54]),
(2) a defining polynomial for each extension, and
(3) the Galois group of the extension's polynomial (a difficult computational problem in general).

When $p \nmid n$, then all extensions are tamely ramified and are well understood; see [11] for an explicit description. Likewise, when $p = n$ the situation has been solved since the early 1970s [1, 11].

For example, there are 7 quadratic extensions of $\mathbf{Q}_2$, each with a cyclic Galois group (of order 2). For primes $p > 2$, there are $p^2 + 1$ degree p extensions of $\mathbf{Q}_p$. Of these, $p + 1$ are cyclic. The remaining $p(p - 1)$ extensions have a Galois group of the form $C_p \rtimes C_d$ where d is a non-trivial divisor of $p - 1$ (here C_n denotes the cyclic group of order n). If we let $J(d)$ denote the number of elements in $(\mathbf{Z}/d)^2$ of order d (this is a generalization of the Euler ϕ function), then the number of degree p extensions of $\mathbf{Q}_p$ whose Galois group is $C_p \rtimes C_d$ is $J(d)$. In other words, since

2000 *Mathematics Subject Classification.* Primary 11S15, 11S20.
Key words and phrases. 2-adic, extension fields, Galois group, local field.

$J(2) = 3$, this means that for any prime $p > 2$, there are three degree p extensions of $\mathbf{Q}_p$ whose Galois group is D_p, the dihedral group of order $2p$ [3].

The difficult cases where $p \mid n$ and n is composite have been dealt with on a case-by-case basis for low degrees. Jones and Roberts have classified the cases where $n \leq 10$ [10–12]. Awtrey et al. have classified degree 14 extensions of the 2-adic and 7-adic numbers [4, 7], degree 12 extensions of the 3-adic numbers [2], and degree 12 extensions of the 2-adic numbers with automorphism group of order greater than two [5, 6].

In this paper, we study degree 12 extensions of $\mathbf{Q}_2$ that have a trivial automorphism group. After describing the computation of defining polynomials of such extensions in the next section, we use the final sections of the paper to show that the Galois groups of these polynomials can be computed using subfield information, the discriminant, and an additional resolvent polynomial [9, 20, 21].

2. Defining Polynomials

In this section, we describe our approach for computing defining polynomials of degree 12 2-adic fields with trivial automorphism group. We begin by introducing some notation and terminology.

2.1. **Notation and Terminology.** Let F be a p-adic field and let K be a degree n extension of F. In this paper, we are mostly concerned with the case $F = \mathbf{Q}_2$, but we will proceed with the general scenario in this section. Let $\mathbf{Z}_K$ and $\mathbf{Z}_F$ denote the ring of integers of K and F, respectively. Then $\mathbf{Z}_K$ and $\mathbf{Z}_F$ each have a unique maximal ideal $\mathcal{P}_K$ and $\mathcal{P}_F$. The **ramification index** of K/F is the integer $e_{K/F}$ such that $P_F\mathbf{Z}_K = \mathcal{P}_K^{e_{K/F}}$, as ideals. The **residue degree** of K/F is the integer $f_{K/F} = n/e_{K/F}$. Equivalently, the quotient $\mathbf{Z}_K/\mathcal{P}$ is a finite field with $p^{f_{K/F}}$ elements. If $f_{K/F} = n$, the extension K/F is called **unramified**. If $n = e_{K/F}$, the extension is called **totally ramified**. The discriminant of K/F is $\mathcal{P}_F^c$ for some integer c called the **discriminant exponent** of K/F. For example, in the case where $F = \mathbf{Q}_p$ and K is the stem field of the irreducible Eisenstein polynomial $f(x)$, then c is equal to the highest power of p dividing the discriminant of the polynomial f.

2.2. **Mass Formulas.** Formulas which count the number of extensions of p-adic fields have received much attention in the literature. Some authors have developed what are known as "mass" formulas [13, 16, 18], where the mass of an extension K/F takes into account the degree of the extension as well as its automorphism group. The mass is defined as:

$$\text{mass}(K/F) = \frac{[K : F]}{|\text{Aut}(K/F)|}.$$

The mass formulas previously mentioned compute the total mass for all extensions of F of a given degree, ramification index, residue degree, and discriminant exponent. As such, different embeddings are counted separately. Therefore these formulas do not give the number of nonisomorphic absolute extensions. Since there is currently no known formula for computing the number of nonisomorphic extensions of $\mathbf{Q}_p$ for a given degree, the approach taken in the literature is to resolve Item (1) of Section 1 by first completing Item (2).

TABLE 1. Cubic Extensions of $\mathbf{Q}_2$, including the ramification index **e**, the Galois group **G** of the defining polynomial **poly**, and the number **#K** of totally ramified quartic extensions of the stem field of **poly**.

e	**G**	**poly**	**#K**
1	C_3	$x^3 - x + 1$	27
3	S_3	$x^3 - 2$	84

2.3. **Defining Polynomials.** The most general reference for the computation of defining polynomials of p-adic fields is [16]. Using the methods of Krasner [13], Pauli-Roblot develop an algorithm for computing extensions of a p-adic field of a given degree by providing a generating set of polynomials to cover all possible extensions. Essential to their method is Panayi's root-finding algorithm [15], which can be used to determine whether two polynomials define isomorphic p-adic fields. The root-finding algorithm can also be used to determine the mass of an extension.

Our method for computing defining polynomials makes use of the Pauli-Roblot algorithm. We note that every degree 12 2-adic field with trivial automorphism group has a unique cubic subfield, which we prove in Corollary 4.2. Therefore, every such extension can be realized as a quartic extension of a cubic 2-adic field. Our strategy proceeds as follows.

First, we compute all cubic 2-adic fields. Such fields are tamely ramified (since the prime 2 does not divide the degree 3) and are therefore easy to classify using [11]. Table 1 shows the two nonisomorphic cubic 2-adic fields, the unramified extension (with cyclic Galois group) and the totally ramified extension (with S_3 as its Galois group).

Next, for each cubic 2-adic field, we compute all of its quartic extensions using the Pauli-Roblot algorithm. Using Panayi's algorithm, we extract only those extensions with trivial automorphism group, and we discard isomorphic extensions. Using this approach, we found 111 nonisomorphic degree 12 2-adic fields with trivial automorphism group. It turns out that such extensions occur as totally ramified quartic extensions of the cubic 2-adic fields. Of these, 27 have ramification index 4 and the other 84 are totally ramified. For convenience, Tables 2–4 give sample defining polynomials for these two cases, along with the discriminant exponent and the Galois group of the polynomial. This content is summarized in Table 5, where data are organized by Galois group and discriminant exponent.

3. Possible Galois Groups

Having computed a defining polynomial for each extension under consideration, we now turn our attention to determining the Galois group of each polynomial.

Given one of our defining polynomials f, let K denote the corresponding extension defined by adjoining to $\mathbf{Q}_2$ a root of f. We wish to compute the Galois group G of f, or equivalently the Galois group of the normal closure of K. Since the elements of G act as permutations on the roots of f, once we fix an ordering on the roots, G can be be considered as a subgroup of S_{12}, well-defined up to conjugation. Since the polynomial f is irreducible, G is a transitive subgroup of S_{12}; i.e., there is a single orbit for the action of G on the roots of f. Therefore G must be a

TABLE 2. Polynomials for degree 12 2-adic fields with trivial automorphism group and ramification index $e = 4$. Also included are the extension's discriminant exponent **c** and the Galois group **G** of its normal closure.

Polynomials	**c**	**G**
$x^{12} + 6x^{11} - 4x^{10} - 2x^9 + 4x^8 - 8x^7 - 8x^6 - 8x^5 - 4x^4 - 8$	12	t129
$x^{12} + 4x^{11} - 6x^{10} + 8x^9 - 4x^8 + 8x^7 - 4x^6 + 4x^5 - 4x^4 + 8x + 8$	12	t205
$x^{12} - 2x^{11} + 4x^{10} - 4x^9 - 2x^8 - 4x^7 - 4x^6 + 8x^5 + 8x^3 + 8x^2 + 8$	18	t166
$x^{12} - 4x^{11} + 4x^{10} - 4x^9 - 2x^8 - 4x^7 + 4x^6 + 8x^3 + 8x^2 + 8$	18	t166
$x^{12} + 2x^{11} - 4x^9 + 8x^7 + 8x^5 - 4x^4 + 8x^2 + 8$	18	t166
$x^{12} - 4x^{11} - 2x^{10} - 4x^9 - 6x^8 + 8x^7 - 4x^6 + 8x^4 + 8x^3 + 8$	18	t166
$x^{12} - 6x^{11} + 8x^{10} + 6x^8 + 4x^6 + 8x^5 + 8x^4 + 8x^3 + 8$	18	t166
$x^{12} - 2x^{11} + 10x^{10} + 12x^9 - 14x^8 - 8x^7 + 8x^5 + 12x^4 - 8x^3 + 8x^2 - 8$	18	t166
$x^{12} + 4x^{11} + 6x^{10} - 4x^9 - 2x^8 + 4x^7 + 8x^5 + 8x^4 + 8x^2 + 8$	18	t166
$x^{12} - 12x^{11} + 4x^{10} - 10x^8 - 8x^7 + 16x^5 + 16x^3 + 16x^2 + 16x - 8$	24	t129
$x^{12} + 16x^6 + 16x^5 - 4x^4 + 16x - 8$	24	t129
$x^{12} + 28x^{11} - 12x^{10} + 8x^9 + 54x^8 - 32x^7 + 32x^6 - 16x^5 - 36x^4 - 48x^3 + 48x^2 + 64x + 40$	24	t129
$x^{12} + 28x^{11} - 36x^{10} + 8x^9 + 6x^8 - 32x^7 - 32x^6 - 4x^4 - 48x^3 - 48x^2 + 32x + 40$	24	t129
$x^{12} + 8x^{11} + 8x^{10} - 4x^9 - 10x^8 + 16x^7 - 8x^6 - 8x^5 + 16x^2 + 8$	24	t205
$x^{12} + 36x^{11} - 96x^{10} - 60x^9 + 94x^8 + 16x^7 + 96x^6 - 48x^5 - 52x^4 - 48x^3 + 64x^2 + 16x - 88$	24	t205
$x^{12} - 4x^{11} + 8x^{10} + 4x^9 + 2x^8 + 8x^6 + 8x^4 + 8$	24	t205
$x^{12} + 4x^{11} + 16x^{10} + 12x^9 + 16x^8 + 8x^6 + 8x^5 - 4x^4 + 16x^3 + 16x^2 - 8$	24	t205
$x^{12} + 36x^{11} - 48x^{10} - 12x^9 - 58x^8 - 32x^6 + 48x^5 + 60x^4 - 16x^3 + 64x^2 - 48x + 40$	24	t205
$x^{12} - 4x^{10} + 4x^9 - 8x^7 - 8x^6 - 4x^4 - 8$	24	t205
$x^{12} - 8x^{10} - 12x^8 - 8x^7 - 8x^6 - 8x^5 - 12x^4 + 16x^3 + 16x - 8$	24	t205
$x^{12} + 24x^{11} + 8x^{10} - 44x^9 - 14x^8 - 16x^6 - 48x^5 + 28x^4 - 32x^3 + 64x^2 + 16x + 56$	24	t205
$x^{12} - 12x^{11} - 12x^{10} + 4x^9 + 12x^8 - 8x^7 - 12x^4 + 16x^3 + 16x^2 + 16x - 8$	24	t205
$x^{12} + 20x^{10} - 4x^9 + 2x^8 - 16x^7 + 48x^5 + 60x^4 - 32x^3 + 48x^2 + 48x + 56$	24	t205
$x^{12} + 8x^{10} + 12x^9 - 12x^8 + 8x^5 + 12x^4 + 16x^3 + 16x^2 - 8$	24	t205
$x^{12} - 4x^{11} - 4x^{10} + 8x^9 - 2x^8 + 8x^6 + 8x^5 + 8$	24	t205
$x^{12} - 12x^{11} - 8x^{10} + 16x^9 - 4x^8 - 8x^7 - 8x^5 - 4x^4 + 16x^3 + 16x^2 + 16x - 8$	24	t205
$x^{12} + 24x^{11} - 52x^{10} + 16x^9 - 18x^8 - 16x^7 + 16x^5 - 36x^4 + 64x^3 - 48x^2 - 32x - 56$	24	t205

transitive subgroup of S_{12}. Our method for computing Galois groups thus relies on the classification of the 301 transitive subgroups of S_{12} [17].

However, not all of these 301 groups can occur as the Galois group of a degree 12 2-adic field, as we show next.

Definition 3.1. 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

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

TABLE 3. Polynomials for totally ramified degree 12 2-adic fields with trivial automorphism group.

Polynomials	c	G
$x^{12}+2x^{11}+2x^9+2x^7+2x^5+2x^3+2x+2$	12	t254
$x^{12}+2x^3+2x^2+2$	14	t128
$x^{12}+2x^5+2$	16	t254
$x^{12}+2x^5+2x^4+2$	16	t254
$x^{12}+2x^9+2x^7+2x^6+2x^4+2$	18	t254
$x^{12}+2x^7+2$	18	t254
$x^{12}+2x^9+2x^7+2$	18	t254
$x^{12}+2x^9+2x^7+2x^6+2$	18	t254
$x^{12}+2x^{11}+2x^9+2x^6+2$	20	t206
$x^{12}+2x^{11}+2x^{10}+2x^9+2x^6+2$	20	t206
$x^{12}+2x^{11}+2x^{10}+2x^9+2x^6+2x^4+2$	20	t206
$x^{12}+2x^{10}+2x^9+2x^8+2x^6+2x^4+2$	20	t43
$x^{12}-2x^{11}+4x^{10}-2x^8+4x^6+4x+2$	22	t254
$x^{12}+2x^{11}+4x^9-2x^8+4x^7+4x^4+4x^3+4x-2$	22	t254
$x^{12}+2x^{11}+2x^{10}+2x^8+2$	22	t254
$x^{12}-2x^{11}+2x^{10}+4x^8+4x^7+2x^4+4x^2+4x-2$	22	t254
$x^{12}+2x^{11}+4x^{10}+4x^9-2x^8+4x^6+2x^4+4x^2+4x+2$	22	t254
$x^{12}+2x^{11}+2x^{10}-2x^8+4x^7+4x^6+4x^5-2x^4+4x^2+4x+2$	22	t254
$x^{12}+2x^{11}+2x^8+2$	22	t254
$x^{12}+2x^{11}+2x^{10}+2x^8+2x^4+2$	22	t254
$x^{12}+4x^{11}-2x^{10}+4x^9+4x^7+4x^6+4x^5+2x^4+4x^3+4x-2$	24	t254
$x^{12}+4x^{10}+4x^9+4x^8+4x^7+4x^6+4x^5+4x+2$	24	t254
$x^{12}+4x+2$	24	t254
$x^{12}+4x^8+4x^6-2x^4+4x^3+4x-2$	24	t254
$x^{12}-2x^{10}+4x^9+2x^8+4x^6+4x^4+4x^3+4x+2$	24	t254
$x^{12}+4x^{11}-2x^{10}+4x^7+4x^5+4x^3+4x-2$	24	t254
$x^{12}+4x^{11}+2x^{10}+4x^9-2x^8+4x^7+4x^6+4x^5-2x^4+4x^2+4x-2$	24	t254
$x^{12}+4x^{11}+4x^7+4x^6+4x^4+4x^2+4x-2$	24	t254
$x^{12}+4x^{11}+4x^{10}+4x^9+4x^7+4x^6+4x^5+4x^3+4x^2+4x+2$	24	t254
$x^{12}+4x^{10}+4x^6+4x^5+4x^4+4x^3+4x+2$	24	t254
$x^{12}+4x^8+4x^7+4x^6+2x^4+4x^2+4x+2$	24	t254
$x^{12}+4x^{11}-2x^{10}+4x^8+4x^6+2x^4+4x^3+4x^2+4x-2$	24	t254
$x^{12}+4x^{11}-2x^{10}+4x^9+4x^7+4x^6+2x^4+4x^2+4x+2$	24	t254
$x^{12}+2x^{10}+4x^9+4x^6-2x^4+4x+2$	24	t254
$x^{12}-2x^{10}-2x^8-2x^4+4x^3+4x-2$	24	t254
$x^{12}+4x^{10}-2x^8+4x^6-2x^4+4x^2+4x+2$	24	t254
$x^{12}+2x^{10}+2x^8+4x^7+4x^6+4x^5+6x^4+4x^3+4x^2+2$	26	t128
$x^{12}+2x^{10}+4x^7+4x^5+4x^4+4x^3+6$	26	t128
$x^{12}+2x^{10}+4x^7+4x^5+4x^3+6$	26	t128
$x^{12}+2x^{10}+4x^5+4x^4+4x^3+6$	26	t128
$x^{12}+2x^{10}+4x^7+4x^6+4x^4+4x^3+4x^2+2$	26	t206
$x^{12}+2x^{10}+4x^7+4x^3+2$	26	t206
$x^{12}+2x^{10}+6x^4+4x^3+4x^2+2$	26	t206
$x^{12}+2x^{10}+4x^6+4x^3+4x^2+2$	26	t206
$x^{12}+2x^{10}+2x^8+6x^4+4x^3+4x^2+2$	26	t206
$x^{12}+2x^{10}+2x^8+2x^4+4x^3+4x^2+2$	26	t206
$x^{12}+2x^{10}+2x^8+4x^7+4x^5+4x^3+2$	26	t206
$x^{12}+2x^{10}+4x^6+4x^3+4x^2+6$	26	t206

TABLE 4. Polynomials for totally ramified degree 12 2-adic fields with trivial automorphism group (continued).

Polynomials	c	G
$x^{12}+2x^{10}+2x^8+4x^7+6x^4+4x^3+4x^2+2$	26	t206
$x^{12}+2x^{10}+2x^8+4x^7+4x^5+2x^4+4x^3+2$	26	t206
$x^{12}+2x^{10}+4x^6+4x^5+4x^3+4x^2+2$	26	t206
$x^{12}+2x^{10}+2x^8+4x^7+4x^6+4x^3+2$	26	t206
$x^{12}+4x^{11}-2x^8+4x^7+4x^5+4x^2+2$	28	t254
$x^{12}+4x^9+4x^8+4x^7+4x^6+4x^5-2$	28	t254
$x^{12}+4x^{10}+4x^9-2x^8+4x^6+4x^5+4x^4+2$	28	t254
$x^{12}+4x^5+2$	28	t254
$x^{12}+4x^8+4x^7+4x^6+4x^5+2x^4+2$	28	t254
$x^{12}+4x^9+4x^5-2x^4+2$	28	t254
$x^{12}+4x^{10}+4x^9-2x^8+4x^7+4x^5+2x^4+4x^2-2$	28	t254
$x^{12}-2x^8+4x^6+4x^5+4x^2+2$	28	t254
$x^{12}+4x^{10}+4x^9+4x^8+4x^6+4x^5-2x^4-2$	28	t254
$x^{12}+4x^{10}+2x^8+4x^7+4x^5+2x^4+4x^2-2$	28	t254
$x^{12}+4x^{10}+4x^5-2x^4-2$	28	t254
$x^{12}+4x^{11}+4x^{10}+4x^6+4x^5-2$	28	t254
$x^{12}+4x^{11}+4x^5+4x^4+2$	28	t254
$x^{12}+4x^7+4x^5+4x^2-2$	28	t254
$x^{12}+4x^{11}+4x^{10}+4x^9+2x^8+4x^6+4x^5+2x^4+4x^2+2$	28	t254
$x^{12}+4x^{11}+4x^9-2x^8+4x^5-2x^4+4x^2+2$	28	t254
$x^{12}+4x^{11}+4x^{10}-2x^8+4x^7+4x^5-2x^4+4x^2+2$	28	t254
$x^{12}+4x^9+2x^8+4x^6+4x^5+4x^4+2$	28	t254
$x^{12}+4x^{10}+4x^8+4x^5-2x^4+4x^2+2$	28	t254
$x^{12}+4x^9+2x^8+4x^7+4x^6+4x^5+4x^4+4x^2+2$	28	t254
$x^{12}+4x^{10}+4x^8+4x^7+4x^5+2$	28	t254
$x^{12}+4x^{11}+4x^8+4x^5+4x^2-2$	28	t254
$x^{12}+4x^8+4x^7+4x^6+4x^5-2x^4+4x^2+2$	28	t254
$x^{12}+4x^{11}+4x^9+4x^7+4x^5-2x^4-2$	28	t254
$x^{12}+4x^{11}+4x^{10}+4x^9-2x^8+4x^7+4x^5+2x^4-2$	28	t254
$x^{12}+4x^{11}+4x^9+4x^8+4x^5-2$	28	t254
$x^{12}+4x^9+4x^6+4x^5+4x^4+4x^2-2$	28	t254
$x^{12}+4x^{11}+4x^9+2x^8+4x^5+4x^4+4x^2-2$	28	t254
$x^{12}+4x^{11}+4x^8+4x^7+4x^6+4x^5-2x^4-2$	28	t254
$x^{12}+4x^{11}+4x^9+2x^8+4x^6+4x^5+2x^4-2$	28	t254
$x^{12}+4x^9+2x^8+4x^5+4x^2+2$	28	t254
$x^{12}+4x^{10}+4x^8+4x^7+4x^5-2x^4+4x^2+2$	28	t254

The ramification groups define a sequence of decreasing normal sugroups which are eventually trivial and which give structural information about the Galois group of a p-adic field. A proof of the following result can be found in [19, Ch. IV].

Lemma 3.2. *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.*

TABLE 5. Summary data for the number of degree 12 2-adic fields with trivial automorphism group, organized by Galois group and discriminant exponent. Cases with 0 extensions have blank entries. The $\mathbf{e = 4}$ table summarizes data in Table 2. The $\mathbf{e = 12}$ table summarizes data in Tables 3 and 4.

e = 4				
c	**t129**	**t166**	**t205**	**Total**
12	1		1	2
18		7		7
24	4		14	18
Total	5	7	15	**27**

e = 12					
c	**t143**	**t128**	**t206**	**t254**	**Total**
12				1	1
14		1			1
16				2	2
18				4	4
20	1		3		4
22				8	8
24				16	16
26		4	12		16
28				32	32
Total	1	5	15	63	**84**

(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.*

Applying this lemma to our scenario, where $K/\mathbf{Q}_2$ is the extension defined by f, and G is the Galois group of f, we see that G is a solvable transitive subgroup of S_{12}. 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 2-group (possibly trivial), and G_0/G_1 is cyclic of order dividing $2^{[G:G_0]} - 1$. Moreover, since the automorphism group of $K/\mathbf{Q}_2$ is isomorphic to the centralizer of G in S_{12}, we need only consider those subgroups whose centralizer is trivial.

Direct computation on the 301 transitive subgroups of S_{12} shows that only 7 groups can occur as the Galois group of f. Using the transitive group notation in [8], these groups are `TransitiveGroup(12,n)`, where n is one of the following possibilities:

$$43, 128, 129, 166, 205, 206, 254.$$

Table 6 gives the size and generators for each one of these groups.

4. Computation of Galois Groups

In this section, we describe our approach for computing the Galois group of the normal closure of a degree 12 2-adic field with trivial automorphism group. We follow the standard approach for determining Galois groups [9]; we compute enough group-theoretic and field-theoretic invariants so as to uniquely identify a polynomial with its corresponding Galois group. However, our method is of interest since we use only three invariants: Galois groups of subfields, the discriminant, and a linear resolvent polynomial.

First, we focus on subfield information. Toward that end, let $K/\mathbf{Q}_2$ be a degree 12 extension defined by an irreducible polynomial f from Tables 2–4, and consider the subfields of K up to isomorphism. The list of the Galois groups of the normal closures of the proper nontrivial subfields of K is important for our work. We call this the *subfield Galois group* content of K, and we denote it by $sgg(K)$. When

TABLE 6. Possible Galois groups of polynomials defining degree 12 2-adic fields with trivial automorphism group. The size and a minimal set of two generators are given for each group in columns **#G** and **Generators**, respectively.

G	#G	Generators
t43	72	(2,12,11,6,8,3)(4,7,10)(5,9) (1,11,9,7,5,3)(2,12,10,8,6,4)
t128	288	(1,5,9)(2,6,10)(3,7,11)(4,8,12) (2,9,5,3,8,12)(4,10,7)(6,11)
t129	288	(4,10,7)(5,8,11)(6,12,9) (1,5,9)(2,3,10,11,6,7)(4,8,12)
t166	576	(1,7)(4,10) (1,3,2)(4,12,5,10,9,8,7,6,11)
t205	1152	(4,7,10)(5,11,8)(6,9,12) (1,11,6,7,8,12,4,2,3,10,5,9)
t206	1152	(1,2)(4,8,10,11,7,5)(6,9,12) (1,11,9,7,5,3)(2,12,10,8,6,4)
t254	3456	(1,11)(2,10,5,7,8,4)(6,12) (1,5,6,10,8,12,4,11,9)(2,3,7)

computing $sgg(K)$, we identify the Galois group of each subfield as a transitive subgroup of S_d where d divides 12 (see Table 7). The next proposition shows that $sgg(K)$ is entirely determined by the Galois group of the normal closure of K.

Proposition 4.1. *The set $sgg(K)$ is an invariant of its Galois group (thus it makes sense to speak of the subfield content of a transitive group).*

Proof. Let G denote the Galois group of f (i.e., of the normal closure of $K/\mathbf{Q}_2$). Let $E \leq G$ be the subgroup fixing K, arising from the Galois correspondence. For example, we could take E to be the point stabilizer of 1 in G. The nonisomorphic subfields of K correspond to the intermediate subgroups F, up to conjugation, such that $E \leq F \leq G$. Furthermore, if K' is a subfield and F is its corresponding intermediate group, then the normal closure of K' is the smallest field K'' (inside a fixed algebraic closure of $\mathbf{Q}_2$) containing K' which is Galois over $\mathbf{Q}_2$. Thus K'' corresponds to the largest normal subgroup N of G contained inside of F; i.e., N is the normal core of F (the intersection of all conjugate subgroups of F). Thus the Galois group of K'' is isomorphic to G/N.

To identify the Galois group of K'' as a transitive subgroup of S_d where $d = [K' : \mathbf{Q}_2] = [G : F]$, we note that N is the kernel of the permutation representation of G acting on the cosets G/F. Therefore, the Galois group of K'' is isomorphic to the image of this permutation representation. Identifying the transitive subgroup structure of this action is a straightforward task in group theory software programs (such as [8]).

Consequently, every polynomial with Galois group G must have the same subfield content, and this quantity can be determined by a purely group-theoretic computation on G. □

To use the proposition in practice, we first fix one of our degree 12 polynomials. We then use Panayi's root-finding algorithm on the complete lists of 2-adic fields of degree d, where $d \in \{2, 3, 4, 6\}$ (these are referenced in [11]). A degree d polynomial has a root in the stem field of f if and only if it defines a subfield. We keep track

of all such polynomials defining subfields and their Galois groups (which are also readily available via [11]).

For each possible Galois group of a degree 12 2-adic field with trivial automorphism group, Table 7 lists the *sgg* content. Using this data, we can prove that every extension under consideration has a unique cubic subfield.

Corollary 4.2. *Let $K/\mathbf{Q}_2$ be a degree 12 extension with trivial automorphism group. Then K has a unique cubic subfield.*

Proof. Since $sgg(K)$ is an invariant of the Galois group of the normal closure of K, we need only analyze the *sgg* contents of the possible Galois groups in Table 7. We see that each possible group has an *sgg* content that contains exactly one element of the form 3Tj. This proves that every extension K has a unique cubic subfield. □

In addition to the *sgg* content, we also make use of the parity of the extension. The parity of a group G is $+1$ if $G \subseteq A_{12}$ and -1 otherwise. Likewise, the parity of an extension is $+1$ if its discriminant is a square in $\mathbf{Q}_2$ and -1 otherwise. As Table 7 shows, the *sgg* content and parity are enough to determine Galois groups in 3 of the 7 cases.

For the other 4 cases, we introduce a resolvent polynomial [21], which we call f_{220}, and we use information about its irreducible factors over $\mathbf{Q}_2$ to give us information about the Galois group of our degree 12 polynomial. The resolvent f_{220} has degree 220, and it can be computed as follows. Let $f(x)$ define a degree 12 extension over $\mathbf{Q}_2$, and let $r_1, r_2, \ldots, r_{12}$ be the roots of f. Then,

$$f_{220}(x) = \prod_{i=1}^{10} \prod_{j=i+1}^{11} \prod_{k=j+1}^{12} (x - r_i - r_j - r_k).$$

Just as in the case of *sgg* content, the degrees of the irreducible factors f_{220} are determined completely by the Galois group of f.

Specifically, consider the group $H \leq S_{12}$ that is generated by the following elements:

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

In this case, notice that $H \simeq S_3 \times S_9$ and that $[S_{12} : H] = 220$. Notice also that H is the stabilizer of $r_1 + r_2 + r_3$ (where the action is on subscripts). It follows that f_{220} is a product of factors of the form $(x - \sigma(r_1 + r_2 + r_3))$ as σ ranges over a complete set of coset representatives of S_{12}/H. Therefore, the field defined by f_{220} corresponds to H, under the Galois correspondence. Thus the Galois group of f_{220} is isomorphic to the image of the permutation representation of G acting on the cosets of G/H. The degrees of the irreducible factors of f_{220} therefore correspond precisely with the orbit lengths of this action.

As Table 7 shows, the remaining 4 groups are distinguished by the degrees of the irreducible factors of f_{220}. The final column $\#\mathbf{Q}_2^{12}$ gives the number of extensions with the corresponding Galois group.

Acknowledgements

This work was 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.

TABLE 7. Subfield content for transitive subgroups of S_{12} with trivial centralizer.

G	**Parity**	**Subfields**	$\mathbf{f_{220}}$	$\#\mathbf{Q}_2^{12}$
t43	+1	3T2, 4T4		1
t166	+1	3T1		7
t128	+1	3T2	$12, 16, 48, 144$	5
t206	+1	3T2	$12, 64, 144$	15
t129	−1	3T1	$12, 16, 48, 72^2$	5
t205	−1	3T1	$12, 64, 72^2$	15
t254	−1	3T2		63

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 and Trevor Edwards, *Dihedral p-adic fields of prime degree*, Int. J. Pure Appl. Math. **75** (2012), no. 2, 185–194.
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, *Degree 12 2-adic fields with automorphism group of order 4*, Rocky Mountain Journal of Mathematics (to appear).
6. 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.
7. 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.
8. The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, 2008.
9. Alexander Hulpke, *Techniques for the computation of Galois groups*, Algorithmic algebra and number theory (Heidelberg, 1997), Springer, Berlin, 1999, pp. 65–77. MR 1672101 (2000d:12001)
10. John W. Jones and David P. Roberts, *Nonic 3-adic fields*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 293–308. MR MR2137362 (2006a:11156)
11. ———, *A database of local fields*, J. Symbolic Comput. **41** (2006), no. 1, 80–97. MR 2194887 (2006k:11230)
12. ———, *Octic 2-adic fields*, J. Number Theory **128** (2008), no. 6, 1410–1429. MR MR2419170 (2009d:11163)
13. Marc Krasner, *Nombre des extensions d'un degré donné d'un corps* $\mathfrak{p}$*-adique*, Les Tendances Géom. en Algèbre et Théorie des Nombres, Editions du Centre National de la Recherche Scientifique, Paris, 1966, pp. 143–169. MR 0225756 (37 #1349)
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. Sebastian Pauli and Xavier-François Roblot, *On the computation of all extensions of a p-adic field of a given degree*, Math. Comp. **70** (2001), no. 236, 1641–1659 (electronic). MR 1836924 (2002e:11166)
17. Gordon F. Royle, *The transitive groups of degree twelve*, J. Symbolic Comput. **4** (1987), no. 2, 255–268. MR MR922391 (89b:20010)

18. Jean-Pierre Serre, *Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local*, C. R. Acad. Sci. Paris Sér. A-B **286** (1978), no. 22, A1031–A1036. MR 500361 (80a:12018)
19. ———, *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)
20. Leonard Soicher and John McKay, *Computing Galois groups over the rationals*, J. Number Theory **20** (1985), no. 3, 273–281. MR MR797178 (87a:12002)
21. Richard P. Stauduhar, *The determination of Galois groups*, Math. Comp. **27** (1973), 981–996. MR 0327712 (48 #6054)

Department of Mathematics and Statistics, Elon University, Campus Box 2320, Elon, NC 27244
E-mail address: cawtrey@elon.edu

35 Stonegate Circle, Wilbraham, Ma 01095
E-mail address: nmiles@elon.edu

Department of Physics and Astronomy, University of North Carolina at Chapel Hill, 120 E. Cameron Ave., Chapel Hill, NC 27599
E-mail address: crshill@live.unc.edu

Applied Physics Laboratory, Johns Hopkins University, 11100 Johns Hopkins Road, Laurel, Maryland 20723
E-mail address: erin.strosnider@gmail.com