DODECIC 3-ADIC FIELDS

CHAD AWTREY

ABSTRACT. Let n be an integer and p a prime number. An important problem in number theory is to classify the degree n extensions of the p-adic numbers through their arithmetic invariants. The most difficult cases arise when p divides n and n is composite. In this paper, we consider the case $n = 12$ and $p = 3$; the degrees $n < 12$ having previously been determined.

1. INTRODUCTION

First introduced by Hensel near the end of the 19th century, the p-adic numbers $\mathbf{Q}_p$ have become an essential tool in many areas of mathematics as well as mathematical physics. Of particular interest to number theorists is the connection between the p-adic numbers, the rational numbers, and their respective field extensions of finite degree. Specifically, let $K/\mathbf{Q}$ be a finite extension defined by adjoining to $\mathbf{Q}$ a root of the polynomial $f(x) \in \mathbf{Q}[x]$. Then for each prime number p, we can factor f over $\mathbf{Q}_p$ to obtain

$$K \otimes \mathbf{Q}_p \simeq \prod_{j=1}^{m} K_j$$

where each K_j is a finite extension of $\mathbf{Q}_p$ defined by the corresponding irreducible factor of f.

To study the number field K, we are led to the problem of determining the arithmetic invariants of the polynomials defining the fields K_j; the most important of which are the discriminant, ramification index, residue degree, polynomials defining subfields, and Galois group. If K_j is unramified, tamely ramified, or a degree p extension of $\mathbf{Q}_p$, then the situation is well-understood [7], [1]. For degree n extensions of $\mathbf{Q}_p$ where $p \mid n$ and n is composite, the situation is more complicated.

Suppose we have an irreducible monic polynomial of degree n with integer coefficients defining the extension $K/\mathbf{Q}$. To compute the arithmetic invariants of the p-adic fields K_j, Jones and Roberts propose the following [9]:

(1) Classify the degree m extensions of $\mathbf{Q}_p$ for all $m \mid n$ and store the invariants.
(2) Factor the polynomial over the p-adic numbers.
(3) Use Panayi's p-adic root finding algorithm [13] on each irreducible factor to identify an isomorphic representative.

Item (1) is clearly the most interesting and the most difficult. The work done by Jones and Roberts classifies degree n extensions of $\mathbf{Q}_p$ where $p \mid n$ and $n \leq 10$ is composite. Their approach for $n = 4$, 6, and 10 is described in [9], while the difficult cases of $(n, p) = \{(8, 2), (9, 3)\}$ are described in [10] and [8], respectively.

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

In this paper, we are concerned with item (1) when $n = 12$ and $p = 3$. In particular, we focus on computing defining polynomials for each field as well as the Galois group (over $\mathbf{Q}_p$) for each of these polynomials. The other invariants are straightforward to compute using basic number field commands in [14] and Panayi's algorithm. In section 2, we lay the theoretical groundwork for computing Galois groups of p-adic fields using the notion of ramification group. A consequence of this section is that every degree 12 extension of $\mathbf{Q}_3$ has a unique quartic subfield. In section 3, we use the result of section 2 to compute defining polynomials. In the final section, we discuss our method of determining the Galois groups of the polynomials found in section 3.

2. Ramification Groups

The aim of this section is to introduce the basic properties of ramification groups and use those to deduce structural information about degree 12 extensions of $\mathbf{Q}_3$. A more detailed exposition can be found in [16].

Definition 2.1. Let $L/\mathbf{Q}_p$ be a Galois extension with Galois group G. Let v be the discrete valuation on L and let $\mathbf{Z}_L$ denote the corresponding discrete valuation ring. For an integer $i \geq -1$, we define the **i-th ramification group** of G to be the following set

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

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

Lemma 2.2. *Let $L/\mathbf{Q}_p$ be a Galois extension with Galois group G, and let G_i denote the i-th ramification group. Let $\mathfrak{p}$ denote the unique maximal ideal of $\mathbf{Z}_L$ and U_0 the units in L. For $i \geq 1$, let $U_i = 1 + \mathfrak{p}^i$.*

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

Proof. We note that U_0/U_1 is isomorphic to the multiplicative group of the residue field of L. For $i \geq 1$, U_i/U_{i+1} is isomorphic to the additive group of the residue field. Let π be a uniformizer for L. Part (a) follows from considering the map $f : G_i/G_{i+1} \to U_i/U_{i+1}$ defined by $f(\sigma) = \sigma(\pi)/\pi$. It follows that f is an injective homomorphism, independent of choice of uniformizer. Part (b) follows from part (a). Since every subgroup of the residue field is a vector space over $\mathbf{Z}/p$, every subgroup of U_i/U_{i+1} is a direct sum of cyclic groups of order p. That G_1 is a p-group follows since

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

which proves part (c). Since G_0 and G_1 have relatively prime order, there exists a subgroup of G_0 that projects isomorphically onto G_0/G_1 ([5, p.230]), proving part (d). Since G/G_0 is isomorphic to the Galois group of the residue field, it is cyclic. Part (e) follows from general results on solvability. □

Specializing to the case when $[K : \mathbf{Q}_3] = 12$ and $G = \mathrm{Gal}(K^{\mathrm{gal}}/\mathbf{Q}_3)$, we see that G is a solvable transitive subgroup of S_{12}; of which there are 265 [15]. Furthermore, G contains a solvable normal subgroup G_0 such that G/G_0 is cyclic of order dividing 12. The group G_0 contains a normal subgroup G_1 such that G_1 is a 3-group (possibly trivial). Moreover, G_0/G_1 is cyclic of order dividing $3^{[G:G_0]} - 1$. Direct computation on the 265 candidates shows that only 45 are possible Galois groups of dodecic 3-adic fields. Using the transitive group notation in [4], these groups are `TransitiveGroup(12,n)`, where n is one of the following possibilities:

1, 2, 3, 5, 11, 12, 13, 14, 15, 16, 17, 18, 19, 34, 35, 36, 38, 39, 40,
41, 42, 46, 47, 70, 71, 72, 73, 84, 116, 118, 119, 120, 121, 130, 131,
167, 169, 170, 171, 172, 173, 174, 212, 215, 216

Showing that every degree 12 extension of $\mathbf{Q}_3$ has a unique quartic subfield amounts to showing that each of the above 45 groups possesses the corresponding group-theoretic property. In particular, consider the subfields of $K/\mathbf{Q}_3$ up to isomorphism. The list of the Galois groups of the Galois 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 $sgg(K)$.

The sgg content of an extension is an invariant of its Galois group. Indeed, suppose the normal closure of $K/\mathbf{Q}_3$ has Galois group G and let $E = G \cap S_{11}$. Then E is the subgroup fixing $\mathbf{Q}_3(\alpha)$ where α is a primitive element for K. By the fundamental theorem of Galois theory, the nonisomorphic subfields of $\mathbf{Q}_3(\alpha)/\mathbf{Q}_3$ correspond to the intermediate subgroups F, up to conjugation, such that $E \leq F \leq G$. Specifically, if K' is a subfield and F is its corresponding intermediate group, then the Galois group of the normal closure of K' is equal to the permutation representation of G acting on the cosets of F in G. Consequently, it makes sense to speak of the sgg content of a transitive subgroup as well.

For each of the 45 possible Galois groups of degree 12 extensions of $\mathbf{Q}_3$, Tables 3-8 show their respective sgg contents. Notice that each group has exactly one entry of the form 4Tj [2]. This shows that degree 12 extensions of $\mathbf{Q}_3$ have a unique quartic subfield.

3. Defining Polynomials

As a consequence of Section 2, every degree 12 extension of $\mathbf{Q}_3$ can be realized uniquely as a cubic extension of a quartic 3-adic field. Defining polynomials for dodecic 3-adic fields can therefore be computed by evaluating appropriate resultants [3, p.119].

3.1. Quartic 3-adic Fields.

Degree four extensions of $\mathbf{Q}_3$ are necessarily tamely ramified, and are therefore easily classified. In particular, each such extension is a totally and tamely ramified extension of an unramified extension of $\mathbf{Q}_3$. The unique unramified extension is obtained by extending the residue field [12, p.48]. For totally and tamely ramified extensions of unramified p-adic fields, we use the following well-known result [12, p.52].

Proposition 3.1. *Let $K/\mathbf{Q}_p$ be the unramified extension of degree f and let ζ be a primitive $(p^f - 1)$-st root of unity in K. For an integer e with $p \nmid e$, let*

TABLE 1. Quartic Extensions of $\mathbf{Q}_3$

e	f	poly
1	4	$q_1 = x^4 - x + 2$
2	2	$q_2 = x^4 + 9x^2 + 36$
2	2	$q_3 = x^4 - 3x^2 + 18$
4	1	$q_4 = x^4 + 3$
4	1	$q_5 = x^4 - 3$

$g = \gcd(e, p^f - 1)$. *There are exactly g totally and tamely ramified extensions of K of degree e, up to K-isomorphism. All extensions can be generated over K by the roots of the polynomial*

$$x^e - \zeta^r p$$

where $r \in \{0, \dots, g-1\}$.

Corollary 3.2. *There are five quartic 3-adic fields, up to isomorphism; the unramified extension, two totally ramified extensions, and two with ramification index 2. Moreover, defining polynomials for these extensions can be chosen to be those given in Table 1.*

Proof. The only non-obvious statement is the fact that the norms of the polynomials defining the two totally ramified extensions of the unramified quadratic 3-adic field give two non-isomorphic extensions. To see this, let K be the unramified quadratic extension of $\mathbf{Q}_3$. By Proposition 3.1, there are two totally and tamely ramified quadratic extensions of K, generated by $x^2 - 3$ and $x^2 - 3\alpha$, where α is a primitive 8th root of unity. We note that $K/\mathbf{Q}_3$ is generated by a root of $x^2 - N(\alpha)$ where N represents the norm down to $\mathbf{Q}_3$. Let L_1/K be defined by the polynomial $N(x^2-3)$ and let L_2/K be defined by $N(x^2-3\alpha)$. Working up to multiplication by a square, the formula for the discriminant in towers gives

$$\operatorname{disc}(L_1/K) = \operatorname{disc}(N(x^2-3)) = N(\operatorname{disc}(x^2-3)) = N(12) = 144,$$

which is a square in K. Similarly, we have

$$\operatorname{disc}(L_2/K) = \operatorname{disc}(N(x^2-3\alpha)) = N(\operatorname{disc}(x^2-3\alpha)) = N(12\alpha) = 144 \cdot N(\alpha),$$

which is not a square in K since $N(\alpha)$ is not. Thus, $L_1/\mathbf{Q}_3$ and $L_2/\mathbf{Q}_3$ define non-isomorphic quartic extensions. □

3.2. **Amano Polynomials.** In [1], Amano studies totally ramified degree-p extensions of p-adic fields where p is an odd prime. He gives generating polynomials for all such extensions. In this section, we apply Amano's results to our setting to compute the cubic extensions of the quartic 3-adic fields.

Let K be a quartic 3-adic field. Let π be a uniformizer for K, let e, f denote the ramification index and residue field degree, let $\mathfrak{p}$ be the prime ideal of $\mathbf{Z}_K$, and let v be the corresponding valuation. Thus $v(\mathfrak{p}) = 1$. The polynomials obtained using Amano's method define totally ramified cubic extensions of K and are consequently Eisenstein. They are therefore of the following form,

$$f(x) = x^3 + a_2x^2 + a_1x + a_0\pi$$

where $v(a_0) = 0$ and $v(a_i) > 0$ for $i = 1, 2$. If L is a cubic extension of K, we define the *type* of L as follows:

- In the case where $m = \min(v(a_1), v(a_2)) \le e$, let λ denote the least integer such that $v(a_\lambda) = m$ and let $\omega \ne 0$ in $\mathbf{Z}_K/\mathfrak{p}$ be such that $a_\lambda \equiv \omega\pi^m$. In this case we say that L is of type $< \lambda, m, \omega >$.
- In the case where $v(a_i) > e$ for $i = 1, 2$. Let $\lambda = 0$ and $m = e + 1$. In this case we say that L is of type $< 0 >$.

We define $\mathcal{M}(\lambda, m)$ to be the set of one units in K of the form

$$1 + \sum_i a_i \pi^i$$

where each a_i is chosen from a complete set of representatives of $\mathbf{Z}_K/\mathfrak{p}$ and where the summation is taken over all integers i such that

$$1 \le i \le m - 1 + \left\lfloor \frac{m + \lambda + 1}{2} \right\rfloor \qquad \text{and } i \not\equiv -\lambda \pmod 3$$

The following result [1] completely characterizes the cubic extensions of K.

Theorem 3.3 (Amano)**.** *Each extension L of type $< 0 >$ is given by a polynomial of the form*

$$x^3 - a\pi$$

where $a \in K^*/K^{*3}$. Thus there is a one-to-one correspondence between the set K^*/K^{*3} and cubic extensions of K of type $< 0 >$.

For integers λ, m such that

$$1 \le \lambda \le 2 \qquad 1 \le m \le e$$

and $\omega \ne 0 \in K/\mathfrak{p}$, each extension L of type $< \lambda, m, \omega >$ is given by a polynomial of the form

$$x^3 - \omega\pi^m x^\lambda - a\pi$$

where $a \in \mathcal{M}(\lambda, m)$. Thus there is a one-to-one correspondence between the set $\mathcal{M}(\lambda, m)$ and the cubic extensions of K of type $< \lambda, m, \omega >$.

3.3. **Data Tables.** For each quartic extension of $\mathbf{Q}_3$, we compute all cubic extensions using Theorem 3.3. Taking the norms of these polynomials down to $\mathbf{Q}_3$, we produce a list of degree 12 polynomials. If at any time we obtain a non-separable polynomial, we apply a suitable Tschirnhausen transformation [3, p.324]. Using Panayi's algorithm, we discard isomorphic extensions. Table 2 contains numerical data on the numbers of these extensions. The **Base** column references polynomials in Table 1. The column **c** is the discriminant exponent, $\sum \mathbf{m(K)}$ is the total mass as in [11], and $\#\mathbf{Q}_3^{12}$ is the number of non-isomorphic extensions over $\mathbf{Q}_3$.

Using this approach, we found 785 degree 12 extensions of $\mathbf{Q}_3$; 780 correspond to totally ramified extensions of the five quartic 3-adic fields and 5 correspond to the unramified extensions of these fields. Krasner's mass formula [11] proves that these are all such extensions.

4. Galois Groups

It remains to identify the Galois group over $\mathbf{Q}_3$ for each of the 785 polynomials. We follow the standard approach for determining Galois groups [6]. We compute enough group-theoretic and field-theoretic invariants so as to uniquely identify a polynomial with its corresponding Galois group. Our strategy is to divide the above list of 45 groups into smaller pieces that are easily distinguished from each other. Our first division will be at the level of centralizer order. The order of

Table 2. Ramified Cubic Extensions of Quartic 3-adic Fields

Base	c	$\sum \mathbf{m(K)}$	$\#\mathbf{Q}_3^{12}$
q_1	12	240	23
q_1	16	240	46
q_1	20	243	24
q_2	12	24	3
q_2	14	24	8
q_2	18	216	46
q_2	20	216	21
q_2	22	243	72
q_3	12	24	2
q_3	14	24	7
q_3	18	216	42
q_3	20	216	18
q_3	22	243	24

Base	c	$\sum \mathbf{m(K)}$	$\#\mathbf{Q}_3^{12}$
q_4	12	6	1
q_4	13	6	3
q_4	15	18	8
q_4	16	18	3
q_4	18	54	9
q_4	19	54	24
q_4	21	162	57
q_4	22	162	27
q_4	23	243	135
q_5	12	6	1
q_5	13	6	3
q_5	15	18	8
q_5	16	18	3
q_5	18	54	9
q_5	19	54	24
q_5	21	162	57
q_5	22	162	27
q_5	23	243	45

the centralizer in S_{12} of the Galois group is useful as it corresponds to the size of the automorphism group of the stem field defined by the polynomial. We divide these smaller sets even further based on their *sgg* content and their parity. The parity of a group G is $+1$ if $G \subseteq A_{12}$ and -1 otherwise. Likewise, the parity of a polynomial f is $+1$ if its discriminant is a square in $\mathbf{Q}_3$ and -1 otherwise. When this information is not enough, we introduce various resolvent polynomials [18], [3, p.322] and use information about how these resolvents factor. For each scenario, we provide summary tables. As before, we include the column $\#\mathbf{Q}_3^{12}$, which represents the number of non-isomorphic extensions over $\mathbf{Q}_3$ with the corresponding Galois group.

4.1. **Centralizer Order 4, 6, and 12.** Only four of the above 45 groups have centralizer order equal to twelve: 12T1, 12T2, 12T3, 12T5. Eight groups have centralizer order equal to six: 12T14, 12T15, 12T16, 12T17, 12T18, 12T19, 12T35, and 12T42. There is a unique group that has centralizer order equal to four: 12T11. In each of these three cases, the *sgg* content is enough to distinguish between the Galois groups (Table 3).

4.2. **Centralizer Order Equals 3.** There are nine groups which have centralizer order equal to three: 12T70, 12T71, 12T72, 12T73, 12T116, 12T121, 12T130, 12T131, 12T167. In this case, *sgg* content is not enough to determine Galois groups. Additionally, we use a degree 66 absolute resolvent $f_{66}(x)$ corresponding to the group $S_{10} \times S_2$. We note that this polynomial can be computed as a linear resolvent on 2-sets [17], i.e. as a resultant. In particular, let

$$g(x) = \text{Resultant}_y(f(y), f(x+y))/x^{12}$$

TABLE 3. Galois groups with $|C_{S_{12}}(G)| = 4$, 6, or 12. These groups are distinguished by their *sgg* content.

T	$\lvert C_{S_{12}}(G)\rvert$	sgg	$\#\mathbf{Q}_3^{12}$
1	12	2T1, 3T1, 4T1, 6T1	8
2	12	2T1, 2T1, 2T1, 3T1, 4T2, 6T1, 6T1, 6T1	4
3	12	2T1, 2T1, 2T1, 3T2, 4T2, 6T2, 6T3, 6T3	6
5	12	2T1, 3T2, 4T1, 6T2	2
11	4	2T1, 3T2, 4T1, 6T3	10
14	6	2T1, 3T1, 4T3, 6T1	8
15	6	2T1, 3T2, 4T3, 6T2	5
16	6	2T1, 2T1, 2T1, 4T2, 6T9	9
17	6	2T1, 4T1, 6T10	4
18	6	2T1, 2T1, 2T1, 4T2, 6T5	24
19	6	2T1, 4T1, 6T5	8
35	6	2T1, 4T3, 6T13	8
42	6	2T1, 4T3, 6T5	40

TABLE 4. Galois groups G with $|C_{S_{12}}(G)| = 3$. These groups are distinguished by *sgg* content and knowledge of certain cubic subfields of the absolute resolvent corresponding to the group $S_{10} \times S_2$.

T	sgg	$\mathbf{f_{66}}$	Cubic Subs	$\#\mathbf{Q}_3^{12}$
70	2T1, 2T1, 2T1, 4T2	[12,18,18,18]	3T1, 3T2, 3T2	36
71	2T1, 2T1, 2T1, 4T2	[12,18,18,18]	3T2, 3T2, 3T2	4
130	2T1, 2T1, 2T1, 4T2	[12,18,18,18]	none	32
72	2T1, 4T1	[12,18,36]	3T2	4
73	2T1, 4T1	[12,18,36]	3T1	16
131	2T1, 4T1	[12,18,36]	none	32
116	2T1, 4T3	[12,18,36]	3T2	20
121	2T1, 4T3	[12,18,36]	3T1	32
167	2T1, 4T3	[12,18,36]	none	160

Then $f_{66}(x) = g(\sqrt{x})$. Factoring this polynomial over $\mathbf{Q}_3$, we obtain at least one degree 18 factor and at most three degree 18 factors. The Galois groups of the normal closures of the cubic subfields of the fields defined by the degree 18 factors distinguish between these nine groups. See column **Cubic Subs** in Table 4. The column $\mathbf{f_{66}}$ gives the degrees of the irreducible factors of f_{66}.

4.3. **Centralizer Order Equals 2.** There are eight groups which have centralizer order equal to 2: 12T12, 12T13, 12T34, 12T36, 12T38, 12T39, 12T40, 12T41. In this case all but the groups 12T12 and 12T13 can be distinguished by their subfield content. For these two groups, we make use of the fact that each has a unique cubic and quartic subfield, according to their *sgg* content. For the group 12T12, the discriminant of the cubic subfield times the discriminant of the quartic subfield is a not a square. For the group 12T13, this quantity is a square. See column $\mathbf{d_3 \cdot d_4 = \square}$ in Table 5.

TABLE 5. Galois groups G with $|C_{S_{12}}(G)| = 2$. These groups are distinguished by *sgg* content with the exception of two groups. These groups are distinguished by the product of the discriminants of their cubic and quartic subfields.

T	**sgg**	$\mathbf{d_3} \cdot \mathbf{d_4} = \square$	$\#\mathbf{Q}_3^{12}$
12	2T1, 3T2, 4T3, 6T3	no	2
13	2T1, 3T2, 4T3, 6T3	yes	5
34	2T1, 2T1, 2T1, 4T2, 6T13		8
36	2T1, 4T3, 6T13		8
38	2T1, 4T3, 6T9		10
39	2T1, 4T1, 6T9		8
40	2T1, 2T1, 2T1, 4T2, 6T10		4
41	2T1, 4T1, 6T10		4

4.4. **Centralizer Order Equals 1.** There are 15 groups which have centralizer order equal to 1: 12T46, 12T47, 12T84, 12T118, 12T119, 12T120, 12T169, 12T170, 12T171, 12T172, 12T173, 12T174, 12T212, 12T215, 12T216. The *sgg* contents of these groups either have size two or size four. We first divide the 15 candidates into three sets: those with *sgg* content of size 2 which are subgroups of A_{12} (Table 6), those with *sgg* content of size 2 which are not subgroups of A_{12} (Table 7), and those with *sgg* content of size 4 (Table 8).

The groups in the first set are: 12T46, 12T84, 12T173, 12T212, 12T215, 12T216. They are subgroups of A_{12} and have *sgg* content equal to either {2T1, 4T1} or {2T1, 4T3}. To distinguish between these groups, we use the *sgg* content and two resolvents. One is a degree 220 absolute resolvent $f_{220}(x)$ corresponding to the group $S_9 \times S_3$. It can be computed in a manner similar to $f_{66}(x)$, i.e., using resultants. It can also be computed in the following way. Let $f(x)$ define a degree 12 extension over $\mathbf{Q}_3$, and let $r_1, r_2, \ldots, r_{12}$ be the roots of f. Then,

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

The other resolvent we use is a degree 8 relative resolvent $f_8(x)$ that makes use of the unique quartic subfield. To compute this resolvent, let f define a degree 12 extension $F/\mathbf{Q}_3$ and let K be the unique quartic subfield of F. Let g be a cubic polynomial obtained by factoring f over K. Then $f_8(x)$ is equal to the norm of $x^2 - \mathrm{disc}(g(x))$ down to $\mathbf{Q}_3$. We make use of the Galois group of $f_8(x)$, which is easy to compute since the polynomial defines a tamely ramified extension of $\mathbf{Q}_3$ [7], [9]. See column $\mathbf{f_8}$ in Table 6. The column $\mathbf{f_{220}}$ gives the degrees of the irreducible factors of f_{220}.

The groups in the second set are: 12T118, 12T119, 12T120, 12T169, 12T170. They are not subgroups of A_{12} and have *sgg* content equal to either {2T1, 4T1} or {2T1, 4T3}. To distinguish between these groups, we use *sgg* content and the absolute resolvent f_{66} introduced earlier. Factoring f_{66} over $\mathbf{Q}_3$, we obtain three factors of degrees 12, 18, and 36, respectively. The Galois groups of the normal closures of the sextic subfields of the field defined by the degree 18 factor of f_{66} are useful for distinguishing between these five groups. See column **Sextic Subs** in Table 7. The column $\mathbf{f_{66}}$ gives the degrees of the irreducible factors of f_{66}.

TABLE 6. Galois groups G with $|C_{S_{12}}(G)| = 1$, $G \subseteq A_{12}$, and $|sgg(G)| = 2$. These groups are distinguished by their *sgg* content, by the degrees of the irreducible factors of an absolute resolvent corresponding to $S_3 \times S_9$, and by the Galois group of the norm of the discriminant polynomial over the unique quartic subfield.

T	sgg	$\mathbf{f_{220}}$	$\mathbf{f_8}$	$\#\mathbf{Q}_3^{12}$
46	2T1, 4T1	[4,36,36,36,36,72]	8T1	4
173	2T1, 4T1	[4,36,36,36,108]	8T1	16
215	2T1, 4T1	[4,36,36,36,108]	8T7	20
84	2T1, 4T3	[4,36,36,72,72]	8T8	16
212	2T1, 4T3	[4,36,72,108]	8T8	48
216	2T1, 4T3	[4,36,72,108]	8T6	16

TABLE 7. Galois groups G with $|C_{S_{12}}(G)| = 1$, $G \not\subseteq A_{12}$, and $|sgg(G)| = 2$. These groups are distinguished by their *sgg* content and by knowledge of certain sextic subfields of the absolute resolvent corresponding to the group $S_{10} \times S_2$.

T	sgg	$\mathbf{f_{66}}$	Sextic Subs	$\#\mathbf{Q}_3^{12}$
118	2T1, 4T3	[12,18,36]	6T3	8
120	2T1, 4T3	[12,18,36]	6T13	20
169	2T1, 4T3	[12,18,36]	6T9	40
119	2T1, 4T1	[12,18,36]	6T3	20
170	2T1, 4T1	[12,18,36]	6T9	32

Computing the Galois group of a sextic 3-adic polynomial is described in detail in [9].

The groups in the third and final set are: 12T47, 12T171, 12T172, 12T173. They are subgroups of A_{12} and have *sgg* content equal to {2T1, 2T1, 2T1, 4T2}. To distinguish between these groups, we use the two absolute resolvents from before, f_{66} and f_{220}. Factoring f_{66} over $\mathbf{Q}_3$, we obtain four factors of degrees 12, 18, 18, and 18, respectively. The Galois groups of the normal closures of the sextic subfields of the fields defined by the degree 18 factors of f_{66} uniquely determine the groups 12T171 and 12T172. See column **Sextic Subs** in Table 8. To distinguish between 12T47 and 12T174, we use the list of degrees of the irreducible factors f_{220}.

5. Acknowledgements

The author wishes to thank the anonymous reviewer for their helpful comments. The author also wishes to thank Elon university for supporting this project through an internal grant.

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. 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)

TABLE 8. Galois groups G with $|C_{S_{12}}(G)| = 1$, $G \subseteq A_{12}$, and $sgg(G) = \{2T1,2T1,2T1,4T2\}$. These groups are distinguished by knowledge of certain sextic subfields of the absolute resolvent corresponding to the group $S_{10} \times S_2$, as well as the degrees of the irreducible factors of the absolute resolvent corresponding to the group $S_9 \times S_3$.

T	$\mathbf{f_{66}}$	$\mathbf{f_{220}}$	**Sextic Subs**	$\#\mathbf{Q}_3^{12}$
47	[12,18,18,18]	[4,36,36,36,36,72]	none	4
171	[12,18,18,18]	[4,36,36,36,108]	6T10, 6T10	8
172	[12,18,18,18]	[4,36,36,36,108]	6T13, 6T13, 6T13, 6T13	6
174	[12,18,18,18]	[4,36,36,36,108]	none	6

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. The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, 2008.
5. Marshall Hall, Jr., *The theory of groups*, The Macmillan Co., New York, N.Y., 1959. MR 0103215 (21 #1996)
6. 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)
7. Kenkichi Iwasawa, *On Galois groups of local fields*, Trans. Amer. Math. Soc. **80** (1955), 448–469. MR 0075239 (17,714g)
8. 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)
9. ———, *A database of local fields*, J. Symbolic Comput. **41** (2006), no. 1, 80–97. MR 2194887 (2006k:11230)
10. ———, *Octic 2-adic fields*, J. Number Theory **128** (2008), no. 6, 1410–1429. MR MR2419170 (2009d:11163)
11. 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)
12. Serge Lang, *Algebraic number theory*, second ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994. MR 1282723 (95f:11085)
13. Peter Panayi, *Computation of leopoldt's p-adic regulator*, Ph.D. thesis, University of East Anglia, December 1995.
14. PARI Group, The, *PARI/GP – Computational Number Theory, version 2.3.4*, 2008, available from `http://pari.math.u-bordeaux.fr/`.
15. Gordon F. Royle, *The transitive groups of degree twelve*, J. Symbolic Comput. **4** (1987), no. 2, 255–268. MR MR922391 (89b:20010)
16. 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 MR554237 (82e:12016)
17. Leonard Soicher and John McKay, *Computing Galois groups over the rationals*, J. Number Theory **20** (1985), no. 3, 273–281. MR MR797178 (87a:12002)
18. 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`