DEGREE 12 2-ADIC FIELDS WITH AUTOMORPHISM GROUP OF ORDER 4

CHAD AWTREY, BRETT BARKLEY, NICOLE E. MILES, CHRISTOPHER SHILL AND ERIN STROSNIDER

ABSTRACT. This paper is concerned with the 513 isomorphism classes of degree 12 2-adic fields whose automorphism groups have order 4. For each extension, we identify a defining polynomial, the extension's ramification index, residue degree, discriminant, and the Galois group of the extension's normal closure. These results extend previous work of Jones and Roberts, Awtrey and Shill.

1. Introduction. Let p be a prime number and n a positive integer. A standard result in number theory states that there are only finitely many nonisomorphic degree n extensions of the p-adic numbers [13, page 54]. It is therefore theoretically possible to classify all such extensions. Early research into this problem has produced mass formulas; formulas for the number of extensions of a local field which count subfields of an algebraic closure. For example, Krasner [12] gives a formula for the number of totally ramified extensions of a local field of specified degree. The main tool used is his well-known lemma. As another example, Serre [18] computes the number of extensions in two different ways, one using Eisenstein polynomials, the other applying Weyl's integration formula to the multiplicative group of a division algebra.

Current research is focused on determining arithmetic invariants for each isomorphism class of extensions, including the ramification index, residue degree, discriminant and Galois group (of the normal closure). Only certain cases have been completely determined. For example, if $p \nmid n$, then each extension is tamely ramified and is therefore well understood [10]. If p = n, then the situation has also been solved [1, 10]. If $p \mid n$ and n is composite, then the situation is more complicated, and researchers have dealt with these extensions on a

```
DOI:10.1216/RMJ-2015-45-6-1755 Copyright ©2015 Rocky Mountain Mathematics Consortium
```

²⁰¹⁰ AMS Mathematics subject classification. Primary 11S15, 11S20.

Keywords and phrases. 2-adic, extension fields, Galois group, local field.

Received by the editors on August 12, 2013, and in revised form on December 24, 2013.

case-by-case basis. Jones and Roberts have studied all *p*-adic fields of degree $n \leq 10$ in [9, 10, 11]. Awtrey and his coauthors have classified degree 12 extensions of the 3-adic numbers [3] and 2-adic numbers [5, 6], as well as degree 14 extensions of the 2-adic numbers [4].

In this paper, we focus on degree 12 2-adic fields with mass equal to 3, i.e., those extensions whose automorphism group has order 4. 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 [8, 20, 21].

2. Defining polynomials. In this section, we outline our method for determining defining polynomials of degree 12 2-adic fields with automorphism group of order 4.

We employ a strategy that is similar in spirit to the algorithms in [16, 14], by realizing our fields as towers of extensions. In both cases, the authors focus on enumerating totally ramified extensions of a general *p*-adic field, though their respective methods for identifying one polynomial per isomorphism class are slightly different. However, when taking norms of polynomials defining these relative extensions to produce polynomials defining absolute extensions (over the base field \mathbf{Q}_p), there can remain a necessity to discard isomorphic extensions. In this case, the standard approach is to employ Panayi's root-finding algorithm [15], which can determine whether two polynomials define isomorphic *p*-adic fields.

Our approach is similar. We first note that every degree 12 2-adic field with automorphism group of order 4 has a degree 6 subfield (take the fixed field of an element of order two in the automorphism group, or see Corollary 4.2). This result then implies that each of our extensions can be realized as a quadratic extension of a sextic 2-adic field. Using the complete list of sectic 2-adic fields in [10], we construct all quadratic extensions of these fields using [2]. Using Panayi's algorithm, we extract only those extensions with automorphism group of order 4, and we discard isomorphic extensions. In this way, we found 513 nonisomorphic degree 12 2-adic fields with automorphism group of order 4. Table 4 in Section 5 shows defining polynomials, their Galois group, the extension's residue degree and the discriminant exponent for a sampling of the extensions (the complete data set is available from the first author).

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 considered as a subgroup of S_{12} , well-defined up to conjugation (different orderings correspond to conjugates of G). 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 (each orbit corresponds to an irreducible factor of f). Therefore, G must be a 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:

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

The ramification groups define a sequence of decreasing normal subgroups 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, Chapter 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 $i \ge 1$, let $U_i = 1 + \mathfrak{p}^i$.

(i) For $i \ge 0$, G_i/G_{i+1} is isomorphic to a subgroup of U_i/U_{i+1} .

- (ii) The group G₀/G₁ 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.
- (iii) The quotients G_i/G_{i+1} for $i \ge 1$ are abelian groups and are direct products of cyclic groups of order p. The group G_1 is a p-group.
- (iv) 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.
- (v) 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} , of which there are 265 [17]. 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 $2^{[G:G_0]}-1$. Only 134 subgroups have the correct filtration. By Galois theory, it follows that the automorphism group of K/\mathbf{Q}_2 is isomorphic to the centralizer of G in S_{12} . Therefore, we need only consider those subgroups whose centralizer order is 4.

Direct computation on the 134 candidates shows that only 27 groups can occur as the Galois group of f. Using the transitive group notation in [7], these groups are TransitiveGroup(12,n), where n is one of the following possibilities:

6, 7, 9, 10, 11, 21, 23, 24, 25, 26, 29, 30, 31, 48, 53, 55, 62, 63, 67, 68, 94, 95, 98, 101, 103, 139, 150.

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 automorphism group of order 4. We follow the standard approach for determining Galois groups [8]; 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 Table 4, and consider the subfields of K up to isomorphism. The list

TABLE 1. Subfield content for transitive subgroups of S_{12} with centralizer order 4 that are subgroups of A_{12} and can be distinguished by their sgg content. The last column gives the number of extensions with the corresponding Galois group.

G	Subfields	$\#\mathbf{Q}_2^{12}$
12T6	3T1, 6T4, 6T6	7
12T7	2T1, 3T1, 6T1, 6T4, 6T6	7
12T9	2T1, 3T2, 6T2, 6T7, 6T8	3
12T10	2T1, 2T1, 2T1, 3T2, 4T2, 6T3, 6T3, 6T3	4
12T21	2T1, 3T2, 6T2, 6T11, 6T11	9
12T23	2T1, 3T2, 6T3, 6T7, 6T11	18
12T24	2T1, 3T2, 6T3, 6T8, 6T11	18
12T25	2T1, 3T1, 6T1, 6T6, 6T6	21
12T26	3T1, 6T6, 6T6, 6T6	14
12T48	2T1, 3T2, 6T3, 6T11, 6T11	36
12T67	3T2, 6T7, 6T7, 6T7	1
12T68	3T2, 6T7, 6T8, 6T8	3
12T101	3T2, 6T7, 6T11, 6T11	18
12T103	3T2, 6T8, 6T11, 6T11	18
12T139	3T2, 6T11, 6T11, 6T11	24

TABLE 2. Subfield content for transitive subgroups of S_{12} with centralizer order 4 that are subgroups of A_{12} and cannot be distinguished by their sgg content. The last column gives the number of extensions with the corresponding Galois group.

G	Subfields	f ₂₂₀	Octic Subs	$\# \mathbf{Q}_{2}^{12}$
12T31	3T1, 6T4	$12, 16^4, 24^2, 48^2$		2
12T55	3T1, 6T4	$12, 24^2, 32^2, 48^2$		14
12T62	3T2, 6T7	$12, 16^4, 48, 96$		6
12T63	3T2, 6T7	$12, 32^2, 48, 96$	8T14	6
12T95	3T2, 6T7	$12, 32^2, 48, 96$	8T24	36

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).

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 be the subgroup fixing K, arising from the Galois correspondence. 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 Galois group of the normal closure of K' is isomorphic to the image of the permutation representation of G acting on the cosets of F in G. 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.

For each possible Galois group of a degree 12 2-adic field with automorphism group of order 4 (listed in Section 2), Tables 1–3 list the sgg content. Using this data, we have an alternative proof that every extension under consideration has a sextic subfield.

TABLE 3. Subfield content for transitive subgroups of S_{12} with centralizer order 4 that are not subgroups of A_{12} . The last column gives the number of extensions with the corresponding Galois group.

G	Subfields	$\#\mathbf{Q}_2^{12}$
12T11	2T1, 3T2, 4T1, 6T3	8
12T29	2T1, 3T1, 6T1	12
12T30	2T1, 3T2, 6T2	12
12T53	2T1, 3T2, 6T3	24
12T94	3T1, 6T6	48
12T98	3T2, 6T8	48
12T150	3T2, 6T11	96

Corollary 4.2. Let K/\mathbf{Q}_2 be a degree 12 extension and suppose that the automorphism group of K has order 4. Then K has a sextic 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 Tables 1–3. We see that each possible group has an sgg content that contains an element of the form 6Tj. Moreover, if the automorphism group is cyclic, there is a unique such sextic subfield. Otherwise, there are three, since, in this case, the automorphism group is the Klein 4-group (which has three elements of order 2). In particular, this proves that every extension K has a sextic 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 Tables 1 and 3 show, the sgg content and

TABLE 4. Defining polynomials and invariants for some of the degree 12 2-adic fields with automorphism group of order 4. The column \mathbf{e} gives the ramification index, \mathbf{c} gives the discriminant exponent, and \mathbf{G} gives the Galois group as a transitive subgroup of S_{12} (using the numbering system of [7]).

Polynomial	е	с	G
$x^{12} - 6x^{10} - 73x^8 + 140x^6 + 79x^4 - 6x^2 + 57$		12	12T7
$x^{12} + 66x^{10} - 93x^8 - 68x^6 - 41x^4 + 66x^2 - 123$			12T29
$x^{12} + 22x^{10} + 75x^8 - 12x^6 - 89x^4 + 54x^2 - 115$	2	12	12T29
$x^{12} - 2x^{10} - 65x^8 + 100x^6 - 97x^4 - 98x^2 + 97$	2	12	12T25
$x^{12} + 132x^{10} - 4468x^8 - 4640x^6 - 4752x^4 + 2112x^2 - 7872$	2	18	12T29
$x^{12} - 4x^{10} - 260x^8 - 3296x^6 + 2544x^4 + 5056x^2 + 6208$	2	18	12T25
$x^{12} + 44x^{10} + 1324x^8 - 6240x^6 - 5520x^4 - 6464x^2 - 7360$	2	18	12T29
$x^{12} - 12x^{10} - 2340x^8 + 1120x^6 + 1264x^4 - 192x^2 + 3648$	2	18	12T25
$x^{12} - 18x^{10} + 171x^8 + 116x^6 - 313x^4 + 190x^2 + 877$	6	12	12T30
$x^{12} - x^{10} + 2x^8 - x^6 - 2x^4 + 3x^2 + 1$	6	12	12T9
$x^{12} - 54x^{10} - 509x^8 - 964x^6 - 777x^4 - 934x^2 + 357$	6	16	12T30
$x^{12} + x^{10} - 2x^8 - 3x^6 + 2x^4 - 3x^2 + 1$	6	16	12T21
$x^{12} + 14x^{10} - 5x^8 - 12x^6 - 5x^4 + 14x^2 - 11$	6	20	12T30
$x^{12} + x^{10} + x^6 + x^2 + 1$	6	20	12T21
$x^{12} - 14x^{10} + 19x^8 + 24x^6 + 3x^4 - 26x^2 + 13$	6	20	12T30
$x^{12} + 14x^{10} + 16x^8 - 8x^6 - 8x^4 + 16x^2 + 16$	6	20	12T9
$x^{12} - 18x^{10} - 21x^8 - 8x^6 + 19x^4 - 6x^2 + 21$	6	20	12T30
$x^{12} - 6x^{10} - x^8 + 4x^6 + 3x^4 + 2x^2 - 7$	6	20	12T9
$x^{12} - 26x^{10} - 5x^8 + 8x^6 + 19x^4 + 2x^2 + 21$	6	20	12T30
$x^{12} - 5x^8 + 4x^6 + 3x^4 + 8x^2 - 7$	6	20	12T21
$x^{12} - 2x^{10} + 4x^8 + 4x^6 + 4x^4 + 4$	6	22	12T21
$x^{12} - 28x^{10} + 64x^8 - 20x^6 - 36x^4 + 24x^2 + 36$	6	22	12T21
$x^{12} + 2x^{10} + 4x^6 + 4x^4 + 8x^2 + 4$	6	22	12T21
$x^{12} + 36x^8 - 52x^6 + 4x^4 + 24x^2 - 44$	6	22	12T30
$x^{12} + 40x^{10} + 4x^8 + 20x^6 - 12x^4 + 40x^2 + 52$	6	22	12T30
$x^{12} - 6x^{10} + 6x^8 + 8x^4 - 4x^2 + 4$	6	22	12T21
$x^{12} + 56x^{10} + 48x^8 - 60x^6 + 48x^4 + 64x^2 + 52$	6	22	12T30
$x^{12} - 4x^{10} + 6x^8 + 4x^4 - 4x^2 + 4$		22	12T21
$x^{12} - 14x^{10} - 10x^8 - 8x^6 + 8x^4 - 4x^2 - 12$	6	22	12T30
$x^{12} - 2x^{10} - 2x^8 + 8x^4 + 4x^2 + 4$	6	22	12T21
$x^{12} + 56x^{10} - 28x^8 - 4x^6 + 52x^4 + 56x^2 - 44$	6	22	12T30
$x^{12} - 24x^{10} - 16x^8 - 20x^6 - 16x^4 + 20$	6	22	12T30

parity are enough to determine Galois groups in all but 5 of the 27 cases.

For the other five cases, we introduce a resolvent polynomial [21] and use information about its irreducible factors over \mathbf{Q}_2 . This resolvent, denoted as f_{220} , has degree 220. It corresponds to the subgroup $S_9 \times S_3$ of S_{12} and can be computed as a linear resolvent on 3-sets [20], i.e., as a resultant. It can also be computed in the following way. 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,

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

As Table 2 shows, the groups 12T31, 12T55 and 12T62 can all be distinguished by the list of degrees of the irreducible factors of f_{220} . However, 12T63 and 12T95 cannot be distinguished by degree considerations alone. However, in this case, we see that f_{220} has a unique degree 48 factor. It turns out that the field defined by this degree 48 factor has a unique degree 8 subfield, and the Galois group of this degree 8 extension is enough to distinguish 12T63 and 12T95 (see the column **Octic Sub**). Note: to compute the Galois group of a degree 8 polynomial over \mathbf{Q}_2 , we can use [11].

In Tables 1–3, the final column $\#\mathbf{Q}_2^{12}$ gives the number of extensions with the corresponding Galois group.

5. Sample data table. As a sample, Table 4 gives polynomials and their associated invariants for some of the degree 12 2-adic fields that have an automorphism group of order 4. For each polynomial, the table also gives its Galois group, as well as the ramification index and discriminant exponent of its corresponding extension field. The entire list can be obtained by emailing the first author.

Acknowledgments. The authors would like to thank the anonymous referee for their comments. The authors would also like to thank Elon University for supporting this project through internal grants and the Center for Undergraduate Research in Mathematics for their support.

REFERENCES

 Shigeru Amano, Eisenstein equations of degree p in a p-adic field, J. Fac. Sci. Univ. Tokyo Math. 18 (1971), 1–21.

2. Chad Awtrey, *Dodecic local fields*, Ph.D. thesis, Arizona State University, Tempe, 2010.

3. _____, Dodecic 3-adic fields, Int. J. Num. Theor. 8 (2012), 933–944.

4. Chad Awtrey, Nicole Miles, Jonathan Milstead, Christopher R. Shill and Erin Strosnider, *Degree* 14 2-*adic fields*, Involve, to appear.

5. Chad Awtrey, Nicole Miles, Christopher R. Shill and Erin Strosnider, Computing Galois groups of degree 12 2-adic fields with trivial automorphism group, submitted.

6. Chad Awtrey and Christopher R. Shill, *Galois groups of degree* 12 2-adic fields with automorphism group of order 6 and 12, Springer Proc. Math. Stat. 64 (2013), 55–65.

7. The GAP Group, *GAP-Groups, algorithms, and programming*, Version 4.4.12, 2008.

8. Alexander Hulpke, *Techniques for the computation of Galois groups*, Algor. Alg. Num. Theor., Springer, Berlin, 1999.

9. John W. Jones and David P. Roberts, *Nonic 3-adic fields, Algorithmic number theory*, Lect. Notes Comp. Sci. **3076**, Springer, Berlin, 2004.

10. _____, A database of local fields, J. Symb. Comp. 41 (2006), 80–97.

11. _____, Octic 2-adic fields, J. Num. Theor. 128 (2008), 1410–1429.

12. Marc Krasner, Nombre des extensions d'un degré donné d'un corps p-adique, Les Tendances Géom. Alg. Theor. Nombr., Paris, 1966.

13. Serge Lang, *Algebraic number theory*, Second ed., Grad. Texts Math. 110, Springer-Verlag, New York, 1994.

14. Maurizio Monge, A family of Eisenstein polynomials generating totally ramified extensions, identification of extensions and construction of class fields, arxiv:math.NT-1109.4617v2.

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), 1641–1659 (electronic).

17. Gordon F. Royle, *The transitive groups of degree twelve*, J. Symb. Comp. 4 (1987), 255–268.

18. Jean-Pierre Serre, Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local, C.R. Acad. Sci. 286 (1978), A1031– A1036.

19. _____, *Local fields*, Grad. Texts Math. **67**, Springer-Verlag, New York, 1979.

20. Leonard Soicher and John McKay, *Computing Galois groups over the ratio*nals, J. Num. Theor. **20** (1985), 273–281.

21. Richard P. Stauduhar, *The determination of Galois groups*, Math. Comp. 27 (1973), 981–996.

Department of Mathematics and Statistics, Elon University, Campus Box 2320, Elon, NC 27244

Email address: cawtrey@elon.edu

UNIVERSITY OF MARYLAND, COLLEGE PARK, MD 20740 Email address: bbarkley@terpmail.umd.edu

DEPARTMENT OF MATHEMATICS AND STATISTICS, ELON UNIVERSITY, CAMPUS BOX 7599, ELON, NC 27244 Email address: nmiles@elon.edu

DEPARTMENT OF MATHEMATICS AND STATISTICS, ELON UNIVERSITY, CAMPUS BOX 9017, ELON, NC 27244 Email address: cshill@elon.edu

Department of Mathematics and Statistics, Elon University, Campus Box 9017, Elon, NC 27244

Email address: estrosnider@elon.edu