involve
a journal of mathematics

Degree 14 2-adic fields

Chad Awtrey, Nicole Miles, Jonathan Milstead,
Christopher Shill and Erin Strosnider

msp

2015 vol. 8, no. 2

INVOLVE 8:2 (2015)
dx.doi.org/10.2140/involve.2015.8.329

Degree 14 2-adic fields

Chad Awtrey, Nicole Miles, Jonathan Milstead,
Christopher Shill and Erin Strosnider

(Communicated by Nigel Boston)

We study the 590 nonisomorphic degree 14 extensions of the 2-adic numbers by computing defining polynomials for each extension as well as basic invariant data for each polynomial, including the ramification index, residue degree, discriminant exponent, and Galois group. Our study of the Galois groups of these extensions shows that only 10 of the 63 transitive subgroups of S_{14} occur as a Galois group. We end by describing our implementation for computing Galois groups in this setting, which is of interest since it uses subfield information, the discriminant, and only one other resolvent polynomial.

1. Introduction

Hensel's p-adic numbers are a foundational tool in 21st century number theory, with applications to such areas as number fields, elliptic curves, and representation theory (among others). They are also the subject of much current research themselves, with several studies aimed at classifying arithmetic invariants of finite extensions of the p-adic numbers. Among the most useful invariants to identify are the ramification index, residue degree, discriminant, and Galois group (of the normal closure) of each extension. For such a pursuit, we can take the following classical result as motivation [Lang 1994, p. 54].

Theorem 1.1. *For a fixed prime number p and positive integer n, there are only finitely many nonisomorphic extensions of the p-adic numbers of degree n.*

When $p \nmid n$, all extensions are tamely ramified and are well understood [Jones and Roberts 2006]. Likewise, when $p = n$, the situation has been solved since the early 1970s [Amano 1971; Jones and Roberts 2006]. The difficult cases where $p \mid n$ and n is composite have been dealt with on a case-by-case basis for low degrees n and small primes p. Jones and Roberts [2004; 2006; 2008] have classified the cases where $n \leq 10$, and the case of degree 12 is dealt with in [Awtrey 2012; Awtrey and Shill 2013; Awtrey et al. $\geq$ 2015a; $\geq$ 2015b].

MSC2010: 11S15, 11S20.
Keywords: 2-adic, extension fields, Galois group, local field.

In this paper, we are concerned with classifying degree 14 extensions of the 2-adic numbers. In particular, we focus on computing defining polynomials for each field as well as the Galois group for each of these polynomials. The other invariants are straightforward to compute using basic number field commands in [PARI 2012]. In Section 2, we lay the theoretical groundwork for computing Galois groups of p-adic fields using the theory of ramification groups. A consequence of this section is that every degree 14 extension of $\mathbb{Q}_2$ has a unique septic 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 show that every degree 14 2-adic field has a unique septic subfield. To accomplish this, we introduce the basic properties of ramification groups and use those properties to deduce structural information about degree 14 extensions of $\mathbb{Q}_2$. For a more detailed exposition of ramification group theory, see [Serre 1979].

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

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

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. For example, the following result is useful for determining possible Galois groups of p-adic fields. A proof can be found in [Serre 1979, Chapter 4].

Lemma 2.2. *Let $L/\mathbb{Q}_p$ 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 $\mathbb{Z}_L$ 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 semidirect 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.*

Suppose f is an irreducible polynomial of degree 14 defined over $\mathbb{Q}_2$ and let G be its Galois group. From Lemma 2.2, we see that G is a solvable transitive subgroup of S_{14}. 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). Moreover, G_0/G_1 is cyclic of order dividing $2^{[G:G_0]}-1$. Direct computation on the 63 transitive subgroups of S_{14} (using [GAP 2008], for example) shows that only 15 of the 63 are possibilities for the Galois group of f. Using the transitive group notation in [GAP 2008], these 15 groups are `TransitiveGroup(14,n)`, where n is one of the following possibilities:

$$\{1, 4, 5, 6, 7, 9, 11, 18, 21, 29, 35, 40, 41, 44, 48\}.$$

Showing that every degree 14 extension of $\mathbb{Q}_2$ has a unique septic subfield amounts to showing that each of the above 15 groups possesses the corresponding group-theoretic property. In particular, let $K/\mathbb{Q}_2$ be a degree 14 extension defined by an irreducible polynomial f, and consider the subfields of K 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 $\operatorname{sgg}(K)$.

The sgg content of an extension is an invariant of its Galois group. Indeed, suppose the normal closure of $K/\mathbb{Q}_2$ has Galois group G and let E be the subgroup fixing K. By Galois theory, the nonisomorphic subfields of K correspond to the intermediate subgroups F, up to conjugation, such that $E \le F \le G$. 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 these 15 groups, we used [GAP 2008] to compute their sgg content. We found that 5 of these groups — 4, 7, 40, 41, 48 — had 7T4 in their sgg content. This means that polynomials whose Galois group is one of these 5 possibilities must define an extension with a septic subfield whose normal closure has Galois group 7T4. But as we will see in the next section, the only possible Galois groups of degree 7 polynomials over $\mathbb{Q}_2$ are either 7T1 or 7T3. This means that these 5 groups cannot occur as the Galois group of a degree 14 2-adic field.

Therefore, there are only 10 possible Galois groups of degree 14 extensions of $\mathbb{Q}_2$. For each of these possible Galois groups, Table 3 shows their respective sgg contents. Notice that each group has exactly one entry of the form 7Tj. This shows that degree 14 extensions of $\mathbb{Q}_2$ have a unique septic subfield.

3. Defining polynomials

As a consequence of Section 2, every degree 14 extension of $\mathbb{Q}_2$ can be realized uniquely as a quadratic extension of a septic 2-adic field. Defining polynomials for degree 14 2-adic fields are therefore straightforward to compute.

e	G	poly
1	7T1	$u7 = x^7 - x + 1$
7	7T3	$t7 = x^7 - 2$

Table 1. Septic extensions of $\mathbb{Q}_2$, including the ramification index e and Galois group G of a defining polynomial poly.

First, we compute all septic 2-adic fields. Such fields are tamely ramified and are therefore easy to classify using [Jones and Roberts 2006]. Table 1 shows that there are two septic 2-adic fields, the unramified extension (with cyclic Galois group) and a totally ramified extension (with 7T3 $= C_7 : C_3$ as its Galois group). Next, for each septic 2-adic field, we compute all of its quadratic extensions using [Awtrey 2010]. In each case, there are 511 such quadratic extensions. But some of these 1022 extensions are isomorphic. Using Panayi's algorithm [Pauli and Roblot 2001], we discard isomorphic extensions to find a total of 590 nonisomorphic degree 14 extensions of $\mathbb{Q}_2$. Polynomials are available on request by emailing the first author.

Table 2 contains numerical data on the numbers of these extensions, excluding the unramified extensions of the two septic 2-adic fields. The "base" column references the two polynomials in Table 1. The column c is the discriminant exponent, G is the Galois group of the defining polynomial, and $\#\mathbb{Q}_2^{14}$ is the number of nonisomorphic extensions over $\mathbb{Q}_2$. Notice that there are 78 extensions that are ramified quadratic extensions of the unramified septic 2-adic field. There are 510 ramified quadratic extensions of the unique totally ramified septic 7-adic field. These 588 extensions plus the unramified extensions of the two septic 2-adic fields give 590 total degree 14 extensions of $\mathbb{Q}_2$. Krasner's mass formula [1966] verifies that these are all such extensions. We note that the number of extensions can also be verified using an implementation of [Pauli and Roblot 2001] in [PARI 2012].

4. Galois groups

It remains to identify the Galois group over $\mathbb{Q}_2$ for each of the 590 polynomials. We follow the standard approach for determining Galois groups [Hulpke 1999]. 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 10 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 the centralizer in S_{14} 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 $G \subseteq A_{14}$ and -1 otherwise. Likewise, the parity

base	c	G	$\#\mathbb{Q}_2^{14}$
$u7$	14	14T1	2
$u7$	14	14T6	2
$u7$	14	14T9	6
$u7$	14	14T21	7
$u7$	14	14T29	21
$u7$	21	14T1	4
$u7$	21	14T9	8
$u7$	21	14T29	28
$t7$	14	14T11	1
$t7$	14	14T18	1
$t7$	16	14T11	1
$t7$	16	14T18	1
$t7$	16	14T35	1
$t7$	16	14T44	1
$t7$	18	14T11	2
$t7$	18	14T18	2
$t7$	18	14T35	2
$t7$	18	14T44	2

base	c	G	$\#\mathbb{Q}_2^{14}$
$t7$	20	14T5	2
$t7$	20	14T18	8
$t7$	20	14T44	6
$t7$	22	14T11	2
$t7$	22	14T18	6
$t7$	22	14T35	6
$t7$	22	14T44	18
$t7$	24	14T11	4
$t7$	24	14T18	12
$t7$	24	14T35	12
$t7$	24	14T44	36
$t7$	26	14T11	4
$t7$	26	14T18	12
$t7$	26	14T35	28
$t7$	26	14T44	84
$t7$	27	14T5	4
$t7$	27	14T18	56
$t7$	27	14T44	196

Table 2. Ramified quadratic extensions of septic 2-adic fields.

of a polynomial f is $+1$ if its discriminant is a square in $\mathbb{Q}_2$ and -1 otherwise. When this information is not enough, we introduce a single resolvent polynomial [Stauduhar 1973] and use information about its irreducible factors over $\mathbb{Q}_2$. This resolvent, denoted as f_{364}, has degree 364. It corresponds to the subgroup $S_{11} \times S_3$ of S_{14} and can be computed as a linear resolvent on 3-sets [Soicher and McKay 1985], i.e., as a resultant. It can also be computed in the following way. Let $f(x)$ define a degree 14 extension over $\mathbb{Q}_2$, and let $r_1, r_2, \ldots, r_{14}$ be the roots of f. Then,

$$f_{364}(x) = \prod_{i=1}^{12} \prod_{j=i+1}^{13} \prod_{k=j+1}^{14} (x - r_i - r_j - r_k).$$

We note that in our search for suitable resolvent polynomials, we also looked at a lower degree linear resolvent (corresponding to the group $S_2 \times S_{12}$), subfields of the field defined by this lower degree resolvent, and other subfield information of f_{364}. In order to keep the computational difficulty of our algorithm as low as possible, we focused on subfields of degree less than 12, with a preference toward quadratic subfields of the fields defined by the irreducible factors of the linear resolvents.

G	parity	$\lvert C_{S_{14}}(G)\rvert$	sgg	f_{364}	quad subs	$\#\mathbb{Q}_2^{14}$
14T1	-1	14	2T1, 7T1			7
14T5	-1	2	2T1, 7T3			7
14T6	$+1$	2	7T1	$14^6, 28^2, 56^4$		2
14T21	$+1$	2	7T1	$14^6, 56^5$		7
14T9	-1	2	7T1	$14^6, 56^5$	one	14
14T29	-1	2	7T1	$14^6, 56^5$	none	49
14T11	$+1$	2	7T3	$28^2, 42^2, 56, 168$		14
14T35	$+1$	2	7T3	$42^2, 56^2, 168$		49
14T18	-1	2	7T3	$42^2, 56^2, 168$	one	98
14T44	-1	2	7T3	$42^2, 56^2, 168$	none	343

Table 3. Invariant data for possible Galois groups of degree 14 2-adic fields.

Under these constraints, we found the degree 56 factors of f_{364} to be the smallest degree factors that accomplished our needs.

Table 3 contains all pertinent invariant data for each Galois group. Notice that all groups can be distinguished using parity, centralizer order, sgg content, and the degrees of the factors of f_{364} except for two sets: 14T9/14T29 and 14T18/14T44. But in both cases, the groups can be distinguished by counting quadratic subfields of the fields defined by the degree 56 factors of f_{364}. In these two cases, we have also verified Galois group computations with [Milstead et al. 2015] by computing sizes of splitting fields. As before, we include the column $\#\mathbb{Q}_2^{14}$, which represents the number of nonisomorphic extensions over $\mathbb{Q}_2$ with the corresponding Galois group (which can also be inferred from Table 2). The other columns are defined as follows: $\lvert C_{S_{14}}(G)\rvert$ gives the size of the centralizer of the group in S_{14}, sgg gives the sgg content of the group, f_{364} gives the degrees of the irreducible factors of f_{364}, and "quad subs" gives the number of quadratic subfields of the fields defined by the degree 56 factors of f_{364}.

On our workstation — two quad-core Intel Xeon processors (2.4GHz) — our Galois group computations finished in just over 4 months (125 days). The most difficult cases (where the Galois group was either 14T9/14T29 or 14T18/14T44) took on average 20–25 hours per polynomial.

Acknowledgements

The authors wish to thank the anonymous referee for their careful reading and useful comments, Sebastian Pauli for helpful discussions, Elon University for supporting this project through internal grants, and the Center for Undergraduate Research in Mathematics for their support.

This research was partially funded by NSF grant #DMS-1148695.

References

[Amano 1971] S. 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 46 #7201 Zbl 0231.12019

[Awtrey 2010] C. Awtrey, *Dodecic local fields*, Ph.D. thesis, Arizona State University, Tempe, AZ, 2010, available at http://search.proquest.com/docview/305184993. MR 2736787

[Awtrey 2012] C. Awtrey, "Dodecic 3-adic fields", *Int. J. Number Theory* **8**:4 (2012), 933–944. MR 2926553 Zbl 1257.11101

[Awtrey and Shill 2013] C. Awtrey and C. R. Shill, "Galois groups of degree 12 2-adic fields with automorphism group of order 6 and 12", pp. 55–66 in *Topics from the 8th Annual UNCG Regional Mathematics and Statistics Conference* (Greensboro, NC, 2012), edited by J. Rychtář et al., Springer Proceedings in Mathematics and Statistics **64**, Springer, Heidelberg, 2013.

[Awtrey et al. ≥ 2015a] C. Awtrey, B. Barkley, N. Miles, C. R. Shill, and E. Strosnider, "Computing Galois groups of degree 12 2-adic fields with trivial automorphism group". Submitted.

[Awtrey et al. ≥ 2015b] C. Awtrey, B. Barkley, N. Miles, C. R. Shill, and E. Strosnider, "Degree 12 2-adic fields with automorphism group of order 4". To appear in *Rocky Mountain J. Math.*

[GAP 2008] *GAP: groups, algorithms, and programming*, Version 4.4.12, The GAP Group, 2008, available at http://www.gap-system.org.

[Hulpke 1999] A. Hulpke, "Techniques for the computation of Galois groups", pp. 65–77 in *Algorithmic algebra and number theory* (Heidelberg, 1997), edited by B. H. Matzat et al., Springer, Berlin, 1999. MR 2000d:12001 Zbl 0959.12003

[Jones and Roberts 2004] J. W. Jones and D. P. Roberts, "Nonic 3-adic fields", pp. 293–308 in *Algorithmic number theory*, edited by D. Buell, Lecture Notes in Comput. Sci. **3076**, Springer, Berlin, 2004. MR 2006a:11156 Zbl 1125.11356

[Jones and Roberts 2006] J. W. Jones and D. P. Roberts, "A database of local fields", *J. Symbolic Comput.* **41**:1 (2006), 80–97. MR 2006k:11230 Zbl 1140.11350

[Jones and Roberts 2008] J. W. Jones and D. P. Roberts, "Octic 2-adic fields", *J. Number Theory* **128**:6 (2008), 1410–1429. MR 2009d:11163 Zbl 1140.11056

[Krasner 1966] M. Krasner, "Nombre des extensions d'un degré donné d'un corps $\mathfrak{p}$-adique", pp. 143–169 in *Les tendances géométriques en algèbre et théorie des nombres* (Clermont-Ferrand, 1964), edited by M. Krasner, Colloques Internationaux du Centre National de la Recherche Scientifique **143**, Éditions du CNRS, Paris, 1966. MR 37 #1349 Zbl 0143.06403

[Lang 1994] S. Lang, *Algebraic number theory*, 2nd ed., Graduate Texts in Mathematics **110**, Springer, New York, 1994. MR 95f:11085 Zbl 0811.11001

[Milstead et al. 2015] J. Milstead, S. Pauli, and B. Sinclair, "Constructing splitting fields of polynomials over local fields", pp. 101–124 in *Collaborative mathematics and statistics research* (Greensboro, NC, 2013), vol. 109, edited by J. Rychtář et al., Springer Proceedings in Mathematics and Statistics **64**, Springer, Cham, 2015.

[PARI 2012] *PARI/GP*, Version 2.5.3, The PARI Group, Bordeaux, 2012, available at http://pari.math.u-bordeaux.fr.

[Pauli and Roblot 2001] S. Pauli and X.-F. Roblot, "On the computation of all extensions of a p-adic field of a given degree", *Math. Comp.* **70**:236 (2001), 1641–1659. MR 2002e:11166 Zbl 0981.11038

[Serre 1979] J.-P. Serre, *Local fields*, Graduate Texts in Mathematics **67**, Springer, New York, 1979. MR 82e:12016 Zbl 0423.12016

[Soicher and McKay 1985] L. Soicher and J. McKay, "Computing Galois groups over the rationals", *J. Number Theory* **20**:3 (1985), 273–281. MR 87a:12002 Zbl 0579.12006

[Stauduhar 1973] R. P. Stauduhar, "The determination of Galois groups", *Math. Comp.* **27** (1973), 981–996. MR 48 #6054 Zbl 0282.12004

Received: 2013-08-11 Revised: 2013-08-28 Accepted: 2013-08-29

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

nmiles@elon.edu *Department of Mathematics and Statistics, Elon University, Campus Box 3753, Elon, NC 27244, United States*

jmmilste@uncg.edu *Department of Mathematics and Statistics, University of North Carolina, 116 Petty Building, 317 College Ave, Greensboro, NC 27412, United States*

cshill@elon.edu *Department of Mathematics and Statistics, Elon University, Campus Box 9017, Elon, NC 27244, United States*

estrosnider@elon.edu *Department of Mathematics and Statistics, Elon University, Campus Box 5470, Elon, NC 27244, United States*

involve

msp.org/involve

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2015 is US $140/year for the electronic version, and $190/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve

2015 vol. 8 no. 2

1944-4176(2015)8:2;1-5