International Journal of Pure and Applied Mathematics
Volume 103 No. 4 2015, 781-795
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: http://dx.doi.org/10.12732/ijpam.v103i4.13

ijpam.eu

GROUPS OF ORDER 16 AS GALOIS GROUPS OVER THE 2-ADIC NUMBERS

Chad Awtrey[1 §], John Johnson[2], Jonathan Milstead[3], Brian Sinclair[4]

[1,2]Department of Mathematics and Statistics
Elon University
Campus Box 2320
Elon, NC 27244, USA

[3]Department of Mathematics and Statistics
University of North Carolina
116 Petty Building, 317 College Ave
Greensboro, NC 27412, USA

Abstract: Let K be a Galois extension of the 2-adic numbers $\mathbf{Q}_2$ of degree 16 and let G be the Galois group of $K/\mathbf{Q}_2$. We show that G can be determined by the Galois groups of the octic subfields of K. We also show that all 14 groups of order 16 occur as the Galois group of some Galois extension $K/\mathbf{Q}_2$ except for E_{16}, the elementary abelian group of order 2^4. For the other 13 groups G, we give a degree 16 polynomial $f(x)$ such that the Galois group of f over $\mathbf{Q}_2$ is G.

AMS Subject Classification: 20B35, 12F10, 11S20
Key Words: groups of order 16, extension fields, Galois group, 2-adic

1. Introduction

Two important problems in Galois theory are the following.

Received: August 8, 2015

§Correspondence author

(P1) Given an irreducible polynomial $f(x)$ of degree n defined over a field F, identify the Galois group of f as a transitive subgroup of S_n (the symmetric group on n letters).

(P2) Given a field F and a transitive subgroup G of S_n, find an irreducible polynomial f of degree n whose Galois group over F is G, if such a polynomial exists.

If we restrict to the case where $F = \mathbf{Q}_p$, the field of p-adic numbers, then no general methods are known for either problem. However, partial results do exist. For example, Galois groups of over the p-adic numbers must be solvable (cf. [18]). Therefore problem **(P2)** is impossible to answer for nonsolvable groups.

Since the number of degree n extensions of $\mathbf{Q}_p$ is finite [14], it is possible to determine defining polynomials for all extensions along with their corresponding Galois groups. If we tabulate these results, we effectively provide an answer for **(P2)** in the cases where a solution exists. Furthermore, the task of resolving **(P1)** for a given polynomial f amounts to determining which of the pre-tabulated fields is isomorphic to the stem field of f. Note that the p-adic root-finding algorithm in [15, 16] can determine when two polynomials define isomorphic fields.

Consequently, current research on solving problems **(P1)** and **(P2)** focuses on classifying degree n extensions of $\mathbf{Q}_p$ by computing a defining polynomial for each extension as well as the polynomial's Galois group. When $p \nmid n$, then all extensions are tamely ramified and are well understood in principle. The situation is similar when $p = n$, with [1] providing all pertinent theory. In both cases, explicit methods for the computation of defining polynomials and Galois groups can be found in [12].

The situation is more difficult when $p \mid n$ and n is composite. In this case, no general results are known. However, some progress has been made on individual cases up to $n = 15$. Table 1 gives data on the number of degree n extensions of $\mathbf{Q}_p$, sorted by pairs (p, n). The column # gives the number of nonisomorphic extensions. Though there is no general formula which counts such extension, this number can be calculated by first computing defining polynomials using [16]. Sources which contain methods for computing Galois groups are listed in the column **References**

This paper focuses on solving problems **(P1)** and **(P2)** for the case of Galois extensions of degree 16 defined over the 2-adic numbers. As Table 1 shows, our work fills a gap in the literature. In Section 2, we solve problem **(P1)**. In particular, we develop a method for computing the Galois group of a Galois

Table 1: For a given pair $(\mathbf{p}, \mathbf{n})$, the number of nonisomorphic degree n extensions of $\mathbf{Q}_p$ is given in column #. Sources which contain methods for computing Galois groups are listed in the column **References**.

$(\mathbf{p}, \mathbf{n})$	#	**References**
(2,4)	59	[12]
(2,6)	47	[12]
(3,6)	75	[12]
(2,8)	1823	[13]
(3,9)	795	[11]
(2,10)	158	[12]
(5,10)	258	[12]
(2,12)	5493	[8, 7, 6]
(3,12)	785	[2]
(2,14)	590	[5]
(7,14)	654	[9]
(3,15)	1172	[3]
(5,15)	1012	[4]

2-adic field of degree 16. However our method does not follow the traditional approach [19], which relies on factoring resolvent polynomials. Instead, we only need to compute octic subfields and the Galois groups of their normal closures. This is a straightforward computation thanks to the complete list of octic 2-adic fields in [13] and the p-adic root finding algorithm [15, 16]. As a corollary of our work in this section, we prove that the group E_{16} does not occur as the Galois group of a degree 16 2-adic field.

In the final section, we solve problem **(P2)**. Again our methods differ from the traditional approach [16], which constructs a large generating set of polynomials (with redundancies) and discards isomorphic extensions using [15]. Instead, we use our results from Section 2 to prove that every Galois 2-adic field of degree 16 has an octic subfield. Consequently, each such field can be realized as a quadratic extension of an octic 2-adic field. We then give an algorithm for constructing quadratic extensions of 2-adic fields in general and use our method to produce polynomials whose Galois groups correspond to the remaining 13 transitive subgroups of S_{16} of order 16.

2. Computing Galois Groups

In this section, we describe our approach for computing Galois groups of Galois extensions of degree 16. We note that our method works over arbitrary base

fields. Though for Corollary 2.3 we do specialize to the case where the base field is the 2-adic numbers.

Groups of order 16

Up to isomorphism, there are 14 groups of order 16. Since this paper deals with computing Galois groups of degree 16 polynomials, it is beneficial to identify these groups as transitive subgroups of S_{16}. Such information is well known and is readily accessed in the computer software program `GAP` [10]. For example, Table 2 lists defining characteristics for the 14 groups. Each group is identified in two ways: (1) by its T-number, and (2) by a more descriptive name that indicates its structure. The T-numbering system is implemented in `GAP`.

For the descriptive name, C_n denotes the cyclic group of order n, E_n the elementary abelian group of order n, D_n the dihedral group of order $2n$, Q_n the generalized quaternion group of order n, $\times$ a direct product, and $\rtimes$ a semidirect product. In the case of $C_8 \rtimes C_2$, there are different mappings from C_2 into $\mathrm{Aut}(C_8)$. These give rise to two distinct groups of order 16 (other than D_8). One is defined by the mapping $x \mapsto x^3$, and the other is given by $x \mapsto x^5$. We distinguish these two cases in the obvious way: by $C_8 \rtimes_3 C_2$ and $C_8 \rtimes_5 C_2$, respectively.

Galois Groups of Subfields

Let K/F be a Galois extension of fields, and let G be the Galois group of K/F. Then under the Galois correspondence, the nonisomorphic subfields of K/F correspond to conjugacy classes of subgroups of G. For each such subfield, we can compute the Galois group of its normal closure. Theorem 2.1 shows that the list of all such Galois groups is an invariant of G.

Theorem 2.1. *Let K/F be a Galois extension of fields, and let G be the Galois group of K/F. The list of the Galois groups of the normal closures of all proper, nontrivial subfields of K/F is an invariant of G. That is, any two extensions that have the same Galois group must have the same list of Galois groups of subfields.*

Proof. Let E/F be a subfield of K/F, and let $H \leq G$ be the subgroup that corresponds to E under the Galois correspondence. Let E^g be the normal closure of E and let $N \leq G$ be the subgroup that corresponds to E^g. Then E^g is the smallest subfield of K containing E that is normal over F. Consequently, N is the largest normal subgroup of G that is contained inside H; i.e., N is the

Table 2: The 14 groups of order 16. Each is identified by their transitive number **T** (as implemented in [10]) as well as a more descriptive name. The final column lists the Galois groups of all proper, nontrivial **Subfields** (as defined in Theorem 2.1), also identified by T numbers. A more descriptive name for each subfield can be found in Table 3.

T	**Description**	**Subfields**
1	C_{16}	2T1, 4T1, 8T1
2	$E_4 \times C_4$	$(2T1)^7$, $(4T1)^4$, $(4T2)^7$, $(8T2)^6$, 8T3
3	E_{16}	$(2T1)^{15}$, $(4T2)^{35}$, $(8T3)^{15}$
4	$C_4 \times C_4$	$(2T1)^3$, $(4T1)^6$, 4T2, $(8T2)^3$
5	$C_8 \times C_2$	$(2T1)^3$, $(4T1)^2$, 4T2, $(8T1)^2$, 8T2
6	$C_8 \rtimes_5 C_2$	$(2T1)^3$, $(4T1)^2$, 4T2, 8T2, 8T7
7	$Q_8 \times C_2$	$(2T1)^7$, $(4T2)^7$, 8T3, $(8T5)^2$
8	$C_4 \rtimes C_4$	$(2T1)^3$, $(4T1)^2$, 4T2, $(4T3)^2$, 8T2, 8T4, 8T5
9	$D_4 \times C_2$	$(2T1)^7$, $(4T2)^7$, $(4T3)^4$, 8T3, $(8T4)^2$, $(8T9)^4$
10	$E_4 \rtimes C_4$	$(2T1)^3$, $(4T1)^2$, 4T2, $(4T3)^4$, 8T2, $(8T4)^2$, $(8T10)^2$
11	$Q_8 \rtimes C_2$	$(2T1)^7$, $(4T2)^7$, 8T3, $(8T11)^3$
12	$C_8 \rtimes_3 C_2$	$(2T1)^3$, 4T2, $(4T3)^2$, 8T4, 8T8
13	D_8	$(2T1)^3$, 4T2, $(4T3)^2$, 8T4, $(8T6)^2$
14	Q_{16}	$(2T1)^3$, 4T2, $(4T3)^2$, 8T4

intersection of all conjugates of H. Thus the Galois group of E^g/F is isomorphic to G/N.

We can identify G/N as a transitive subgroup of S_d where $d = [G : H]$ in the following way. Let ϕ be the permutation representation of G acting on the cosets G/H. Then it is straightforward to check that $\ker(\phi) = N$. And therefore G/N is isomorphic to $\phi(G)$. Note, computing images of permutation representations is a built-in command in [10]. □

The column **Subfields** in Table 2 gives the list of Galois groups of subfields for each of the 14 groups of order 16. Note, repetitions are included and are indicated via exponents. For example, the entry $(2T1)^{15}$, $(4T2)^{35}$, $(8T3)^{15}$ for the group 16T3 means that a degree 16 extension whose Galois group is E_{16} has 15 quadratic subfields, 35 quartic subfields whose normal closures all have Galois group 4T2, and 15 octic subfields whose normal closures all have Galois group 8T3.

All of the entries in Table 2 was computed with `GAP`. Notice that the Galois groups of the subfields are also identified by their T-number. For convenience, Table 3 gives more descriptive information on these groups. The column **Description** follows the same conventions as in Table 2.

Table 3: The sizes and descriptive names of the groups occurring in the **Subfields** column of Table 2.

G	Size	Description
2T1	2	C_2
4T1	4	C_4
4T2	4	E_4
4T3	8	D_4
8T1	8	C_8
8T2	8	$C_4 \times C_2$
8T3	8	E_8
8T4	8	D_4
8T5	8	Q_8
8T6	16	D_8
8T7	16	$C_8 \rtimes_5 C_2$
8T8	16	$C_8 \rtimes_3 C_2$
8T9	16	$D_4 \times C_2$
8T10	16	$E_4 \rtimes C_4$
8T11	16	$Q_8 \rtimes C_2$

Galois Group Algorithm

Using Theorem 2.1 and Table 2, we can develop an algorithm for computing the Galois group of a Galois 2-adic field of degree 16. The primary computation in our algorithm is compiling the list of the Galois groups of all proper nontrivial subfields of the field defined by f. This is a straightforward computation, thanks to the complete list of octic 2-adic fields in [13] and the p-adic root finding algorithm in [15, 16].

Algorithm 2.2. *Let $f(x)$ be an irreducible polynomial of degree 16 that defines a Galois extension over the 2-adic numbers, and let G be the Galois group of f. Let S be the list of the Galois groups of all nonisomorphic octic subfields of f's stem field, including repetitions. Then,*

- *If $\#S = 1$,*
  - *G is 16T1 if* 8T1 $\in S$.
  - *G is 16T14 otherwise.*
- *If $\#S = 2$,*
  - *G is 16T6 if* 8T2 $\in S$.

  - *G is 16T12 otherwise.*

- *If $\#S = 3$,*
  - *G is 16T4 if $S = \{8\mathrm{T}2, 8\mathrm{T}2, 8\mathrm{T}2\}$.*
  - *G is 16T5 if $\{8\mathrm{T}1, 8\mathrm{T}1\} \subseteq S$.*
  - *G is 16T7 if $\{8\mathrm{T}5, 8\mathrm{T}5\} \subseteq S$.*
  - *G is 16T13 if $\{8\mathrm{T}6, 8\mathrm{T}6\} \subseteq S$.*
  - *G is 16T8 otherwise*
- *G is 16T11 if $\#S = 4$.*
- *G is 16T10 if $\#S = 5$.*
- *If $\#S = 7$,*
  - *G if $\{8\mathrm{T}4, 8\mathrm{T}4\} \subseteq S$.*
  - *G is 16T2 otherwise.*

Proof. By Theorem 2.1, the set S is an invariant of G. The algorithm's validity is therefore proved by consulting Table 4, which extracts the information from Table 2 concerning Galois groups of octic subfields and sorts it in decreasing order by the number of such subfields. The fact that the group $16\mathrm{T}3 = E_{16}$ does not appear in our algorithm is explained by Corollary 2.3. □

Corollary 2.3. *The group $16\mathrm{T}3 = E_{16}$ does not occur as the Galois group of a Galois 2-adic field of degree 16.*

Proof. According to Table 4, if K defines a Galois 2-adic field of degree 16 whose Galois group is E_{16}, then K must have 15 nonisomorphic octic subfields, each of whose normal closures has Galois group $8\mathrm{T}3 = E_8$. However, according to the complete list of octic 2-adic fields in [13], there is only one octic 2-adic field among the 1823 whose normal closure is 8T3. In fact, this field is defined by the polynomial $x^8 + 4x^6 + 8x^2 + 4$. Therefore, since there are not enough E_8 fields, E_{16} cannot occur as the Galois group of a Galois 2-adic field of degree 16. □

Table 4: The transitive subgroups of S_{16} of order 16, sorted by the number of octic subfields. The data for column **Galois groups** is extracted from Table 2.

T	**#Octic Subs**	**Galois Groups**
3	15	$(8T3)^{15}$
2	7	$(8T2)^6$, 8T3
9	7	8T3, $(8T4)^2$, $(8T9)^4$
10	5	8T2, $(8T4)^2$, $(8T10)^2$
11	4	8T3, $(8T11)^3$
4	3	$(8T2)^3$
5	3	$(8T1)^2$, 8T2
7	3	8T3, $(8T5)^2$
8	3	8T2, 8T4, 8T5
13	3	8T4, $(8T6)^2$
6	2	8T2, 8T7
12	2	8T4, 8T8
1	1	8T1
14	1	8T4

3. Defining Polynomials for Octic 2-adic Fields

In the previous section, we developed an algorithm for computing the Galois group of a Galois 2-adic field of degree 16 using only the list of Galois groups of the extension's octic subfields. We also proved that one of the groups of order 16 does not occur as the Galois group of such an extension; namely, $16T3 = E_{16}$. In this section, we show the other 13 groups of order 16 do indeed occur as the Galois group of a degree 16 2-adic field, and we produce a sample defining polynomial that realizes each group.

Our method for producing defining polynomials proceeds as follows. By Table 4, we note that every Galois 2-adic field of degree 16 has at least one octic subfield. Therefore, every such extension can be realized as a quadratic extension of an octic 2-adic field. But we do not have to consider quadratic extensions of all 1823 octic 2-adic fields. In fact, according to Table 4, we see that every Galois 2-adic field of degree 16 has an octic subfield whose normal closure has Galois group either 8T1, 8T2, 8T3, or 8T4. There are a total of 61 such fields: 24 of 8T1, 16 each of 8T2 and 8T4, and the unique 8T3 (which was mentioned in the proof of Corollary 2.3). For convenience, Table 5 contains polynomials defining these 61 fields, including their Galois groups.

Our strategy is as follows. For each of the 61 octic fields mentioned above, we compute all of its quadratic extensions following Theorem 4.3. The result-

ing fields are degree 16 extensions of $\mathbf{Q}_2$, but not all are necessarily Galois extensions. We use the p-adic root finding algorithm to discard non-Galois extensions. Then we use Algorithm 2.2 to compute the Galois groups of the remaining fields. Table 6 gives a sample defining polynomial for each of the 13 transitive subgroups of S_{16} of order 16.

4. Quadratic Extensions of Octic 2-adic Fields

Let K be a finite extension of $\mathbf{Q}_2$ of degree n, π a uniformizer of K, $|\ |$ the non-Archimedean absolute value on K that extends the 2-adic absolute value, $\mathcal{O}$ the ring of integers in K, $\mathcal{P}$ the unique maximal ideal of $\mathcal{O}$, e the ramification index and f the residual degree of K. We wish to study quadratic extensions of K, which are in one-to-one correspondence with non-trivial representatives of K^*/K^{*2}. Therefore we are led to consider the structure of the group K^*/K^{*2}. The group is isomorphic to an elementary abelian 2-group E_{2^m} for some integer m. This follows since there are only finitely many quadratic extensions of K and since every element in the group squares to give the identity. The aim of this section is to show $m = 2+n$. We also give a complete set of representatives for this group.

Proposition 4.1. *Let U_0 denote the units of $\mathcal{O}$. Then*

$$K^* = \pi^{\mathbf{Z}} \times U_0 \simeq \mathbf{Z} \times U_0.$$

Proof. The proof follows immediately since every $x \in K^*$ can be written in a unique way as $x = u\pi^k$ for some integer k where $u \in U_0$. □

We now study the structure of U_0 in more detail. Let $x \in U_0$ and let ω denote the Teichmüller character. That is, ω is characterized by the following two properties: $\omega(x) \equiv x \pmod{\mathcal{P}}$ and $\omega(x)^{2^f-1} = 1$. Then ω induces a canonical group isomorphism between $(\mathcal{O}/\mathcal{P})^*$ and μ_K, the (2^f-1)-st roots of unity in U_0. If we let U_1 denote the set of units in U_0 that are congruent to 1 mod $\mathcal{P}$, then it follows that $U_0 \simeq \mu_K \times U_1$, with ω inducing the isomorphism.

Proposition 4.2. *As abelian groups we have the isomorphism: $K^* \simeq \mu'_K \times \mathbf{Z} \times \mathbf{Z}_2^n$, where μ'_K is a cyclic group such that $|\mu'_K| = (2^f-1)2^k$ for some $1 \le k \le n$.*

Proof. For $i \ge 1$, let U_i be the set of units such that $x \equiv 1 \pmod{\mathcal{P}^i}$. The map $x \mapsto (x-1)/\pi^i$ induces an isomorphism from U_i/U_{i+1} to the additive group $\mathcal{O}/\mathcal{P}$ (i.e., C_{2^f}). Therefore U_i has a natural $\mathcal{O}$-module structure, being finitely

Table 5: Defining polynomials for the 61 octic 2-adic fields whose normal closures have Galois G from among: 8T1, 8T2, 8T3, or 8T4. These polynomials are taken from [13].

G	**Polynomial**
8T1	$x^8 + x^4 + x^3 + x + 1$
8T1	$x^8 + 2x^7 + 2x^6 + 8x^3 + 48$
8T1	$x^8 + 6x^6 + 8x^5 + 80$
8T1	$x^8 + 2x^6 + 8x^4 + 80$
8T1	$x^8 + 4x^6 + 24x^5 + 8x^2 + 48x + 12$
8T1	$x^8 + 2x^4 + 16x^3 + 16x + 52$
8T1	$x^8 + 12x^6 + 6x^4 + 8x^2 + 52$
8T1	$x^8 + 8x^7 + 2x^4 + 16x^3 + 16x + 20$
8T1	$x^8 + 8x^6 + 4x^4 + 16x^2 + 50$
8T1	$x^8 + 24x^6 + 4x^4 + 16x^2 + 34$
8T1	$x^8 + 8x^6 + 4x^4 + 16x^2 + 18$
8T1	$x^8 + 24x^4 + 8x^2 + 16x + 46$
8T1	$x^8 + 8x^6 + 4x^4 + 16x^2 + 34$
8T1	$x^8 + 16x^7 + 28x^4 + 16x^3 + 2$
8T1	$x^8 + 28x^4 + 16x^3 + 50$
8T1	$x^8 + 24x^6 + 4x^4 + 16x^2 + 2$
8T1	$x^8 + 24x^6 + 12x^4 + 10$
8T1	$x^8 + 8x^6 + 12x^4 + 26$
8T1	$x^8 + 8x^6 + 32x^3 + 24$
8T1	$x^8 + 8x^6 + 12x^4 + 42$
8T1	$x^8 + 24x^6 + 12x^4 + 26$
8T1	$x^8 + 24x^6 + 12x^4 + 42$
8T1	$x^8 + 8x^6 + 12x^4 + 58$
8T1	$x^8 + 24x^6 + 12x^4 + 58$
8T2	$x^8 + 28x^4 + 144$
8T2	$x^8 + 6x^6 + 8x^5 + 16$
8T2	$x^8 + 2x^6 + 8x^4 + 16$
8T2	$x^8 + 6x^6 + 2x^4 + 4x^2 + 8x + 12$
8T2	$x^8 + 2x^6 + 6x^4 + 4x^2 + 8x + 20$
8T2	$x^8 + 2x^6 + 6x^4 + 4x^2 + 8x + 28$
8T2	$x^8 + 10x^4 + 16x + 4$

generated of rank n. More precisely, $U_1 \simeq \mu_{K,1} \times \mathbf{Z}_2^n$ where $\mu_{K,1}$ is the finite

Table 5: Continuation

G	Polynomial
8T2	$x^8 + 10x^4 + 16x + 36$
8T2	$x^8 + 4x^6 + 6x^4 + 16x^3 + 24x^2 + 36$
8T2	$x^8 + 2x^4 + 16x + 4$
8T2	$x^8 + 14x^4 + 4x^2 + 8x + 22$
8T2	$x^8 + 14x^4 + 4x^2 + 8x + 6$
8T2	$x^8 - 15$
8T2	$x^8 + 8x^7 + 12x^6 + 10x^4 + 8x^3 + 4x^2 + 8x + 14$
8T2	$x^8 + 8x^7 + 14x^4 + 4x^2 + 8x + 30$
8T2	$x^8 + 16$
8T2	$x^8 + 8x^7 + 8x^5 + 2x^4 + 12x^2 + 8x + 26$
8T2	$x^8 + 28x^4 + 36$
8T3	$x^8 + 4x^6 + 8x^2 + 4$
8T4	$x^8 + 12x^4 + 16$
8T4	$x^8 + 12x^4 + 144$
8T4	$x^8 + 6x^6 + 6x^4 + 8x^3 + 4x^2 + 8x + 20$
8T4	$x^8 + 4x^6 + 40x^2 + 4$
8T4	$x^8 + 8x^5 + 6x^4 + 16x^3 + 8x^2 + 12$
8T4	$x^8 + 12x^6 + 10x^4 + 8x^2 + 36$
8T4	$x^8 + 4x^7 + 2x^4 + 4x^2 + 14$
8T4	$x^8 + 4x^7 + 10x^4 + 4x^2 + 14$
8T4	$x^8 + 4x^7 + 10x^4 + 4x^2 + 6$
8T4	$x^8 + 4x^7 + 14x^4 + 12x^2 + 10$
8T4	$x^8 + 4x^7 + 6x^4 + 12x^2 + 2$
8T4	$x^8 + 152x^4 + 16$
8T4	$x^8 + 4x^7 + 2x^4 + 4x^2 + 6$
8T4	$x^8 + 4x^7 + 14x^4 + 12x^2 + 2$
8T4	$x^8 + 2x^4 + 8x^3 + 12x^2 + 8x + 18$
8T4	$x^8 + 44x^4 + 100$
8T4	$x^8 + 12x^6 + 6x^4 + 4x^2 + 8x + 2$
8T4	$x^8 + 52x^4 + 36$

cyclic group of roots of unity in K congruent to 1 mod $\mathcal{P}$ and $|\mu_{K,1}| = 2^k$ for some $0 \leq k \leq n$.

By Proposition 4.1, we have $K^* \simeq \mu_K \times \mu_{K,1} \times \mathbf{Z} \times \mathbf{Z}_2^n$. Now, $|\mu_K| = 2^f - 1$

and $|\mu_{K,1}|$ divides 2^n. Since $\pi \mid 2$, it follows that $-1 \equiv 1 \pmod{\mathcal{P}}$. Thus $-1 \in \mu_{K,1}$. Therefore, $2 \mid |\mu_{K,1}| \mid |\mu'_K|$. This proves $k \geq 1$, as required. □

Theorem 4.3. *As groups, $K^*/K^{*2} \simeq E_{2^{2+n}}$, so that $|K^*/K^{*2}| = 2^{2+n}$. Moreover, a system of representatives is given by the set*

$$Q = \left\{ \pi^{\delta} (1 + \omega\pi^{2e})^{\gamma} \prod_{i=1}^{e} \prod_{j=0}^{f-1} \left[1 + t^j \pi^{2i-1}\right]^{\varepsilon_i} \right\}$$

where t is a root of the polynomial $h(x) \in \mathbf{Q}_2[x]$ that defines the maximal unramified subextension of K and where $u = 2/\pi^e$. In this case $\gamma, \delta, \varepsilon_i \in \{0, 1\}$, and $\omega \in \mathcal{O}/\mathcal{P}$ is not *a root of $x^2 + ux \pmod{\mathcal{P}}$.*

Proof. By Proposition 4.2, we have $K^* \simeq \mu'_K \times \mathbf{Z} \times \mathbf{Z}_2^n$, where μ'_K is a cyclic group of even order. It follows that $K^*/K^{*2} \simeq C_2^2 \times (\mathbf{Z}_2/2\mathbf{Z}_2)^n \simeq E_{2^{2+n}}$.

To construct the set Q, we first recall that the isomorphism $K^* \simeq \mu'_K \times \mathbf{Z} \times \mathbf{Z}_2^n$, comes from the fact that $K^* = U_0 \times \pi^{\mathbf{Z}}$. Thus we conclude that one representative of K^*/K^{*2} is π. Next, we recall that $U_0 \simeq (\mathcal{O}/\mathcal{P})^* \times U_1$. Since the multiplicative group $(\mathcal{O}/\mathcal{P})^*$ has odd order $2^f - 1$, this implies that $U_0/U_0^2 \simeq U_1/U_1^2$.

Thus, we are left to determining the structure of U_1/U_1^2. By Hensel's lemma, every element $x \in U_1$, such that $x \equiv 1 \pmod{\mathcal{P}^{2e}}$, is a square. The remaining structure of Q can be determined by systematically considering elements $(1 + a\pi^i)^2$ for $a \in \mathcal{O}/\mathcal{P}$, $1 \leq i \leq e$, knowing *a priori* how many elements Q should have. □

4.1. Polynomials

Using Theorem 4.3, we can construct all quadratic extensions of the 61 fields defined by the polynomials in Table 5. There are a total of $61 \cdot 1023 = 62403$ such extensions. Using the p-adic root-finding algorithm in [15, 16], we discard all non-Galois extensions. Using Algorithm 2.2, we compute the Galois group of each extension. For each of the 13 possible Galois groups G of Galois 2-adic fields of degree 16, Table 6 lists a polynomial whose Galois group over $\mathbf{Q}_2$ is G. Our polynomials were also checked using the methods in [17].

Table 6: For each transitive subgroup G of S_{16} with $|G| = 16$, a polynomial with Galois group G over $\mathbf{Q}_2$ is given in column **Polynomial**. The group 16T3 $= E_{16}$ is missing from the table, since it does not occur as a Galois group over $\mathbf{Q}_2$ (see Corollary 2.3).

Polynomial	**G**
$x^{16} + 8x^{12} + 32x^{11} + 16x^{10} + 32x^9 + 4x^8 + 32x^7 + 32x^5 + 2$	16T1
$x^{16} + 4x^{12} + 8x^{10} + 16x^9 - 8x^8 + 16x^6 + 32x^5 - 8x^4 + 64x^3 + 16x^2 - 96x + 228$	16T2
$x^{16} - 8x^{15} + 60x^{14} + 80x^{13} - 44x^{12} - 40x^{11} + 128x^{10} + 48x^9 - 20x^8 + 224x^7 + 296x^6 + 64x^4 + 176x^3 + 32x^2 - 64x + 124$	16T4
$x^{16} + 8x^{14} + 2x^8 + 16x^7 + 4x^4 + 8x^2 + 16x + 10$	16T5
$x^{16} + 2x^8 + 4x^4 + 8x^2 + 16x + 2$	16T6
$x^{16} + 4x^{12} + 16x^{11} + 8x^{10} + 16x^9 - 8x^8 + 32x^7 + 80x^6 + 96x^5 + 120x^4 - 32x^3 + 16x^2 - 96x + 228$	16T7
$x^{16} + 4x^{14} + 8x^{13} + 8x^9 + 2x^8 + 8x^7 + 8x^6 + 4x^4 + 6$	16T8
$x^{16} + 16x^{13} + 4x^{12} + 16x^{11} + 72x^{10} + 48x^9 + 120x^8 + 96x^7 + 208x^6 + 120x^4 - 32x^3 + 16x^2 - 96x + 228$	16T9
$x^{16} + 4x^{14} + 8x^{13} + 4x^{12} + 8x^{11} + 2x^8 + 8x^7 + 8x^6 + 4x^4 + 8x^2 + 10$	16T10
$x^{16} + 8x^{15} + 24x^{14} + 32x^{13} + 12x^{12} - 16x^{11} - 8x^{10} + 32x^9 + 88x^8 + 16x^7 + 8x^4 + 16x^2 + 4$	16T11
$x^{16} + 8x^{15} + 4x^{14} + 8x^{13} + 8x^{11} + 2x^8 + 16x^5 + 4x^4 + 6$	16T12
$x^{16} + 8x^{15} + 4x^{14} + 8x^{13} + 8x^{11} + 10x^8 + 16x^5 + 4x^4 + 6$	16T13
$x^{16} + 4x^{14} + 8x^{13} + 8x^{11} + 10x^8 + 4x^4 + 16x^3 + 16x + 6$	16T14

Acknowledgements

This work was supported in part by NSF grant #DMS-1148695. The authors would like to thank Sebastian Pauli for helpful conversations, Elon University for supporting this project, and the Center for Undergraduate Research in Mathematics for their support.

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. MR0308086 (46 #7201)

[2] Chad Awtrey, *Dodecic 3-adic fields*, Int. J. Number Theory **8** (2012), no. 4, 933–944. 2926553

[3] Chad Awtrey, Kristen Mazur, Sara Rodgers, Nicole Soltz, and Jesi Weed, *Degree 15 extensions of the 3-adic numbers*, (in preparation).

[4] Chad Awtrey, Kristen Mazur, Sara Rodgers, Nicole Soltz, and Jesi Weed, *On Galois groups of degree 15 polynomials*, (submitted).

[5] Chad Awtrey, Nicole Miles, Jonathan Milstead, Christopher Shill, and Erin Strosnider, *Degree 14 2-adic fields*, Involve **8** (2015), no. 2, 329–336. 3320863

[6] Chad Awtrey, Nicole Miles, Christopher Shill, and Erin Strosnider, *Computing Galois groups of degree 12 2-adic fields with trivial automorphism group*, (submitted).

[7] 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).

[8] 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.

[9] 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.

[10] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, 2008.

[11] 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. MR2137362 (2006a:11156)

[12] John W. Jones and David P. Roberts, *A database of local fields*, J. Symbolic Comput. **41** (2006), no. 1, 80–97. 2194887 (2006k:11230)

[13] John W. Jones and David P. Roberts, *Octic 2-adic fields*, J. Number Theory **128** (2008), no. 6, 1410–1429. MR2419170 (2009d:11163)

[14] 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. 0225756 (37 #1349)

[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). 1836924 (2002e:11166)

[17] Sebastian Pauli and Brian Sinclair, *Enumerating extensions of π-adic fields with given invariants*, arXiv:1504.06671 [math.NT].

[18] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg. 554237 (82e:12016)

[19] Richard P. Stauduhar, *The determination of Galois groups*, Math. Comp. **27** (1973), 981–996. 0327712 (48 #6054).