International Journal of Pure and Applied Mathematics
Volume 100 No. 2 2015, 337-345
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: http://dx.doi.org/10.12732/ijpam.v100i2.12

DEGREE 14 EXTENSIONS OF $\mathbb{Q}_7$

Jim Brown[1] §, Robert Cass[2], Rodney Keaton[3],
Salvatore Parenti[4], Daniel Shankman[5]

[1]Department of Mathematical Sciences
Clemson University
Clemson, SC 29634, USA

[2]Department of Mathematics
University of Kentucky
Lexington, KY 40506, USA

[3]Department of Mathematics
University of Oklahoma
Norman, OK 73019, USA

[4]Department of Mathematics
University of Michigan
Ann Arbor, MI 48109, USA

[5]Department of Mathematics
University of Tennessee
Knoxville, TN 37996, USA

Abstract: We compute all degree 14 extensions of $\mathbb{Q}_7$ up to isomorphism, and find that there are 654 such extensions. Additionally, we compute several invariants of these extensions in order to classify the associated Galois group of the Galois closure of each extension.

AMS Subject Classification: 11S15, 11S20
Key Words: local fields, Galois groups

Received: January 5, 2015

§Correspondence author

1. Introduction

For a prime p and a positive integer n, it is well-known that there are only finitely many degree n field extensions of the field $\mathbb{Q}_p$ of p-adic numbers. When $p \nmid n$ or $p = n$, all of the extensions of $\mathbb{Q}_p$ have been classified and data associated to these extensions is stored in an online database of local fields created by Jones and Roberts [8]. When p properly divides n, the problem of classifying these extensions becomes much more complicated. In this case, such extensions have been classified completely for all $n \leq 12$.

In this paper, we focus on the case $n = 14$ and $p = 7$. We use methods established by S. Pauli and implemented in the computer algebra system MAGMA ([4]) to compute defining polynomials for each of these extensions up to isomorphism. Using ramification groups, we obtain a list which includes all possible Galois groups of an irreducible degree 14 polynomial over $\mathbb{Q}_7$. Employing computational methods motivated by those used in [3] to classify degree 12 extensions of $\mathbb{Q}_3$, we compute several invariants of these extensions to determine the Galois groups of their defining polynomials.

Throughout this paper we fix an algebraic closure $\overline{\mathbb{Q}}_7$ and work in this algebraic closure.

2. Defining Polynomials

In his thesis, Pauli developed methods to compute defining polynomials for extensions of local fields ([9]). Using the implementation of his techniques in MAGMA, we compute a list of defining polynomials for all extensions of $\mathbb{Q}_7$. We obtain 1158 such irreducible polynomials. Sorting the extensions defined by these polynomials into isomorphism classes can be done using Panayi's p-adic root finding algorithm, which is also implemented in MAGMA. Two degree n extensions of $\mathbb{Q}_p$ are isomorphic if and only if their defining polynomials share a common root. Table 1 gives the counts for the extensions of $\mathbb{Q}_7$. Here e is the ramification degree, c is the discriminant exponent, $\#\mathcal{K}_{e,c}$ is the total number of extensions as counted by Krasner's mass formula, and $\#\mathbb{Q}_7^{e,c}$ is the number of non-isomorphic extensions.

Some of the polynomials obtained have coefficients with many digits. In order to obtain polynomials with coefficients more amenable to computation, we randomly generated degree 14 polynomials with small integer coefficients. Each random polynomial was checked for irreducibility using Panayi's root finding algorithm. If the random polynomial was irreducible, we found the unique

Table 1: Counts for Extensions of $\mathbb{Q}_7$

e	c	# $\mathcal{K}_{e,c}$	# $\mathbb{Q}_7^{e,c}$
1	0	1	1
2	7	2	2
7	14	336	27
	16	336	27
	18	336	27
	20	336	27
	22	336	27
	24	336	54
	26	343	28
14	8	84	6
	9	84	12
	10	84	6
	11	84	12
	12	84	6
	13	84	18
	15	588	48
	16	588	42
	17	588	48
	18	588	42
	19	588	96
	20	588	42
	21	686	56
			=654

polynomial f in our list of 654 polynomials defining the same isomorphism class of extensions. If the random polynomial had coefficients with fewer digits, we let it replace f in our list of 654 polynomials. One can see [5] for the complete list of all 654 polynomials.

3. Ramification Groups

In this section we introduce ramification groups and use them to gain information about the Galois groups of the Galois closures of degree 14 extensions of

$\mathbb{Q}_7$. For more facts about ramification groups one can see [2] or [10].

Let $L/\mathbb{Q}_p$ be a Galois extension and set $G = \mathrm{Gal}(L/\mathbb{Q}_p)$. Let ν_L be the discrete valuation on L and let $\mathcal{O}_L$ be the valuation ring. For each integer $i \geq -1$ we define the ith ramification group of G to be

$$G_i = \{\sigma \in G : \nu_L(\sigma(x) - x) \geq i + 1 \quad \text{for every } x \in \mathcal{O}_L\}.$$

Note that $G_{-1} = G$ and that the ramification groups form a decreasing filtration on G which is eventually trivial. Additionally, G/G_0 is isomorphic to the Galois group of the residue field extension. The following lemma gives some structural information about the ramification groups.

Lemma 3.1 (Corl. 4.1.3, [2])**.** *Let $L/\mathbb{Q}_p$ be a Galois extension with ϖ a uniformizer for L and let $G = \mathrm{Gal}(L/\mathbb{Q}_p)$. Let $U_i = \langle 1 + (\varpi^i) \rangle$ and let U_0 be the group of units of $\mathcal{O}_L$. Then*

1. *For $i \geq 0$, G_i/G_{i+1} is isomorphic to a subgroup of U_i/U_{i+1} and hence is abelian.*
2. *G_0/G_1 is cyclic with order coprime to p.*
3. *For $i \geq 0$, G_i/G_{i+1} is a direct product of cyclic groups of order p.*
4. *G_0 is the semi-direct product of a cyclic group of order coprime to p and a normal subgroup which is a p-group.*
5. *G and G_0 are solvable.*

In our case we have a degree 14 extension $K/\mathbb{Q}_7$ with $G = \mathrm{Gal}(K^{\mathrm{gal}}/\mathbb{Q}_7)$ and with K^{gal} the Galois closure of K in our chosen algebraic closure of $\mathbb{Q}_7$. Thus G is one of the 63 solvable transitive subgroups of S_{14}. Also, G must contain a solvable normal subgroup G_0 such that G/G_0 is cyclic and has order dividing 14 since G/G_0 is isomorphic to the Galois group of the residue field extension. Moreover, G_0/G_1 is cyclic and has order dividing $7^{[G:G_0]} - 1$. This last statement follows from part (1) of the lemma and the fact that U_0/U_1 is isomorphic to the multiplicative group of the residue field of L. Using GAP ([7]), computations on the 63 transitive subgroups of S_{14} show that there only 17 possible Galois groups that can be associated to a degree 14 extension of $\mathbb{Q}_7$. Listed using the T notation in the LMFDB ([1]), these 17 groups are given by $14Tn$ where n is one of

$$1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 15, 20, 22, 23, 24, 25, 32.$$

However, we can eliminate three of these groups. The groups $14T15$, $14T22$, and $14T25$ each have the low degree resolvent $3T2$. This means that any extension of $\mathbb{Q}_7$ whose Galois group is one of these three groups must contain a degree 3 subfield whose associated Galois group is $3T2$. This is impossible since none of the degree 3 extensions of $\mathbb{Q}_7$ have the associated Galois group $3T2$. Thus we can eliminate these three groups, leaving us with the following list of 14 possible Galois groups $14Tn$ where n is one of

$$1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 20, 23, 24, 32.$$

4. Galois groups

We now compute the Galois group of each of our 654 defining polynomials. To accomplish this task, we compute enough invariants to uniquely determine the Galois group of each polynomial. Following the approach used in [3], we first summarize three of the more basic invariants that we use.

The first of these invariants is the subfield content of an extension $K/\mathbb{Q}_7$, which is the list of the Galois groups of the Galois closures of the proper nontrivial subfields of K. On the group theory side, the subfield content for a degree 14 field extension associated with any of our 14 possible Galois groups has been computed and is listed in the LMFDB. We list the subfield content associated to these Galois groups in Table 2, and immediately notice that all degree 14 extensions of $\mathbb{Q}_7$ must have a unique quadratic subfield. In order to compute the subfield content of a degree 14 extension $K/\mathbb{Q}_7$, we must only check if any of the finitely many degree 2 extensions of $\mathbb{Q}_7$ or degree 7 extensions of $\mathbb{Q}_7$, which have been completely classified, are subfields of K. Such a degree 2 or degree 7 extension of $\mathbb{Q}_7$ is a subfield of K if and only if the defining polynomial of the degree 2 or 7 extension has a root in K. We already know that K must have a unique quadratic subfield, but we will make use of the defining polynomial of that subfield later so we still determine the quadratic subfield here.

We also make use of the order of the centralizer of the Galois group in S_{14}, which is equal to the order of the automorphism group $\mathrm{Aut}(K/\mathbb{Q}_7)$. This automorphism group can be computed easily as MAGMA has built-in functionality for computing $\mathrm{Aut}(K/\mathbb{Q}_7)$. The centralizer order of our 14 possible Galois groups is listed in Table 2 under the heading C.O.

Additionally, we use the parity of the the Galois groups, which is +1 if $G \subseteq A_{14}$ and -1 otherwise. The parity of a defining polynomial f is +1 if its discriminant is a square in $\mathbb{Q}_7$ and -1 otherwise. To compute the parity of the

defining polynomials, we use the algorithm outlined in [2]. We list the parity of each possible Galois group in Table 2.

As these invariants are not enough to distinguish all the groups, it is necessary to use two resolvent polynomials to uniquely determine each Galois group. (For more on resolvent polynomials one can consult [6].) The first of these is the following degree 91 linear absolute resolvent

$$f_{91}(x) = \prod_{1 \le i < j \le 14} (x - (\alpha_i + \alpha_j))$$

where the α_i are the roots of the defining polynomial f. This can be computed in terms of resultants via the formula

$$f_{91}(x) = \left(\frac{\text{Resultant}_y(f(y), f(x-y))}{2^{14} f(x/2)} \right)^{1/2}.$$

If the resolvent polynomial $f_{91}(x)$ is square-free, then degrees of the irreducible factors of $f_{91}(x)$ factored over $\mathbb{Q}_7$ correspond to the orbit lengths of the componentwise action of G on ordered pairs (a_1, a_2) where $a_1 \neq a_2$ and $a_1, a_2 \in \{1, \ldots, 14\}$. These orbit lengths are listed for some of the Galois groups in Table 2 under the heading $O.L.$ If $f_{91}(x)$ is not square-free, we apply a Tschirnhausen transformation to the defining polynomial f to get a new irreducible polynomial defining the same extension as f. Eventually we get a resolvent that is square-free.

We also use a quartic relative resolvent $f_4(x)$, analogous to one used in [3], which relies on the unique quadratic subfield. Let f define a degree 14 extension $K/\mathbb{Q}_7$ and let F be the unique quadratic subfield of K. Let g be any of the 7 quadratic polynomials obtained by factoring f over K. Then $f_4(x)$ is the norm of $x^2 - \text{disc}(g(x))$ down to $\mathbb{Q}_7$. That is,

$$f_4(x) = (x^2 - \text{disc}(g(x)))(x^2 - \sigma(\text{disc}(g(x))))$$

where $\sigma \in \text{Gal}(F/\mathbb{Q}_7)$ is the unique nontrivial automorphism. To aid in computation, note that the coefficients of $f_4(x)$ are symmetric polynomials in the roots of the defining polynomial of K. We are interested in the Galois group of $f_4(x)$, which can easily be computed using MAGMA as the degree is sufficiently small. Table 2 lists the Galois groups of $f_4(x)$ for extensions having some of our 14 possible Galois groups. These Galois groups were computed using polynomials with integer coefficients defining number fields and having the given Galois group. In one case $f_4(x)$ is not irreducible, which is why the Galois group has only two elements.

From Table 2 it is clear that the Galois groups $14T1, 14T2, 14T3, 14T5$, and $14T8$ are uniquely determined by their subfield content, centralizer order,

Table 2: Possible Galois Groups for $p = 7$

Label (14T)	Subfields	C.O.	Parity	O.L.	Gal(f_4)
1	7T1, 2T1	14	-1		
2	7T2, 2T1	14	-1		
3	7T2, 2T1	2	-1		
4	7T4, 2T1	2	-1	$[7, 21^2, 42]$	
5	7T3, 2T1	2	-1		
7	7T4, 2T1	2	-1	$[7, 42^2]$	
8	2T1	7	-1		
12	2T1	1	1	$[14^3, 49]$	
13	2T1	1	-1	$[14^3, 49]$	4T2
14	2T1	1	-1	[42,49]	2T1
20	2T1	1	-1	$[14^3, 49]$	4T3
23	2T1	1	1	[42,49]	4T1
24	2T1	1	-1	[42,49]	4T2
32	2T1	1	-1	[42,49]	4T3

and parity. By also making use of the degree 91 absolute resolvent, we are able to distinguish the Galois groups $14T4, 14T7$, and $14T12$. Finally, by using the resolvent $f_4(x)$ we are able to identify the remaining Galois groups $14T13, 14T14, 14T20, 14T23, 14T24$, and $14T32$. Note that we do not fill in the entire table; we only include enough information to distinguish the Galois groups.

We conclude by giving a count of the number of degree 14 extensions of $\mathbb{Q}_7$ having each of the 14 Galois groups. Table 3 gives this data.

Acknowledgments

The authors were supported by NSF DMS-1156734.

References

[1] Alderson, M. and et. al, LMFDB, http://www.lmfdb.org/, Accessed May 29, 2013.

Table 3: Counts for degree 14 extensions of $\mathbb{Q}_7$ by Galois group

Galois Group (14T)	Number of Extensions
1	24
2	3
3	6
4	31
5	24
7	62
8	72
12	8
13	9
14	93
20	16
23	64
24	114
32	128

[2] C.Awtrey, Dodecic local fields, PhD Thesis, Arizona State University, (2010).

[3] C. Awtrey, Dodecic 3-adic Fields, *Int. J. Num. Th.*, **8** (2012), 933-944.

[4] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.*, **24** (1997), 235–265.

[5] J. Brown,R. Cass, R. Keaton, S. Parenti, and D. Shankman, Data tables for degree 14 extensions of $\mathbb{Q}_7$, http://www.ces.clemson.edu/ jimlb/ResearchPapers/REU2013data.pdf, Accessed August 31, 2013.

[6] L. Cangelmi, Resolvents and Galois groups, *Rend. Sem. Mat. Univ. Pol. Torino*, **53**, No. 3 (1995), 208-222.

[7] GAP, GAP – Groups, Algorithms, and Programming, Version 4.5.5 (2012).

[8] J. Jones and D. Roberts, A database of local fields, *J. Symbolic Comput.*, **41** (2006), 80-97.

[9] S. Pauli, Efficient Enumeration of Extensions of Local Fields with Bounded Discriminant, PhD Thesis, Concordia University, (2001).

[10] J-P. Serre, Local Fields, Springer-Verlag, USA (1979).