MATHEMATICS OF COMPUTATION
Volume 81, Number 277, January 2012, Pages 555–567
S 0025-5718(2011)02511-1
Article electronically published on June 3, 2011

NUMBER FIELDS WITH SOLVABLE GALOIS GROUPS AND SMALL GALOIS ROOT DISCRIMINANTS

JOHN W. JONES AND RACHEL WALLINGTON

Abstract. We apply class field theory to compute complete tables of number fields with Galois root discriminant less than $8\pi e^{\gamma}$. This includes all solvable Galois groups which appear in degree less than 10, groups of order less than 24, and all dihedral groups D_p where p is prime.

Many people have studied questions of constructing complete lists of number fields subject to conditions on degree and possibly Galois group, with a goal of determining complete lists of such fields with discriminant less than a fixed bound. This study can be phrased in those terms, with the principle distinction being that our discriminant bounds apply to Galois fields, rather than to particular stem fields.

For a finite group G and bound $B > 0$, let $\mathcal{K}(G, B)$ be the set of number fields in $\mathbf{C}$ which are Galois over $\mathbf{Q}$ and which have root discriminant $\leq B$. It is a classical theorem that each set $\mathcal{K}(G, B)$ is finite. Jones and Roberts [JR07a] considered these sets with $B = \Omega = 8\pi e^{\gamma} \approx 44.7632$, a constant introduced by Serre [Ser86]. This number is the asymptotic limit for root discriminant bounds assuming the Generalized Riemann Hypothesis. Jones and Roberts conjecture that there are only finitely many such fields in the union of the $\mathcal{K}(G, \Omega)$, with G running through all finite groups. They determine all sets $\mathcal{K}(A, \Omega)$ where A is an abelian group, and most sets $\mathcal{K}(G, \Omega)$ for groups G which appear as Galois groups of irreducible polynomials of degree at most 6. Here we extend those results using class field theory. We complete their study of Galois groups which appear in degree 6, treat all solvable extensions in degrees 7–9, as well as for all groups G with $|G| \leq 23$. Finally, we determine the sets $\mathcal{K}(D_\ell, \Omega)$ where ℓ is an odd prime.

The primary theoretical difficulty in carrying out these computations is to deduce bounds which effectively screen out conductors for our extensions. Section 1 sets notation and describes some of the methods used before Section 2 addresses this question, and describes our overall process. Section 3 summarizes the results of our computations.

1. Notation and conventions

1.1. **Groups.** We let C_n denote the cyclic group of order n, and D_n the dihedral group of order $2n$. Direct products are indicated by juxtaposition, so $G_1 \times G_2$ will be denoted by simply G_1G_2, and $G_1 \times G_1$ will be written G_1^2. Many groups will be semidirect products, and $N : H$ will denote a semidirect product with normal subgroup N and complimentary subgroup H. We will write $G_1 : G_2 : G_3$ to mean

Received by the editor July 24, 2010 and, in revised form, December 15, 2010.
2010 *Mathematics Subject Classification.* Primary 11R21; Secondary 11R37.

$(G_1 : G_2) : G_3$. If $H \le S_n$, then the wreath product is denoted $G \wr H \cong G^n : H$. An extension of G_1 by G_2 will be denoted by $G_1.G_2$.

We always try to use notation which indicates the structure of the group. However, to avoid ambiguity, particularly for group extensions and semidirect products, we also make use of two standard group numberings. For Galois groups, we also use the notation nTd to denote the dth transitive subgroup of S_n in the numbering of [BM83, CHM98]. For small groups, at times we use the numbering system employed by the small group library of gap [GAP06]. In this case, a group denoted $[n, k]$ is produced in gap by `SmallGroup(n,k)`. So, $D_7 = C_7 : C_2 = 7T2 = [14, 1]$.

1.2. **Discriminants.** For an extension L/K of number fields, we write $D_{L/K}$ for the discriminant ideal of the relative extension. For absolute extensions $K/\mathbf{Q}$, we write d_K for a positive generator of $D_{K/\mathbf{Q}}$. If $[K : \mathbf{Q}] = n$, then $\mathrm{rd}(K) = d_K^{1/n}$ denotes the root discriminant of K. Finally, we let K^{gal} denote a normal closure for $K/\mathbf{Q}$, and define the Galois root discriminant for $K/\mathbf{Q}$ to be $\mathrm{grd}(K) = \mathrm{rd}(K^{gal})$. Finally, for a number field K, we will denote its ring of integers by $\mathcal{O}_K$.

1.3. **Sibling fields.** Number fields $F_1, F_2 \subseteq \mathbf{C}$ are *sibling* fields if they have the same Galois closure in $\mathbf{C}$. Sibling fields need not have the same degree. For example, any field is always a sibling of its own Galois closure. On the other hand, siblings might have the same degree and yet be non-isomorphic. The first case of this phenomenon occurs with quartic D_4 fields.

When we represent fields by irreducible polynomials, we can have sibling fields defined by polynomials f_1 and f_2 of the same degree, so $\mathrm{Gal}(f_1) \cong \mathrm{Gal}(f_2)$, but where the Galois groups do not necessarily have the same T-number. This first happens in degree 6 where $6T7 \cong 6T8 \cong S_4$.

2. Discriminant bounds

Let $\mathbf{Q} \subseteq K \subseteq L$, with $n = [L : K]$ and $m = [K : \mathbf{Q}]$. Then, as is well known,

$$D_{K/\mathbf{Q}}^n \mathcal{N}_{K/\mathbf{Q}}(D_{L/K}) = D_{L/\mathbf{Q}} \tag{1}$$

where $\mathcal{N}_{K/\mathbf{Q}}$ denotes the ideal norm. In particular,

$$\mathrm{rd}(K) \le \mathrm{rd}(K)\,\mathrm{Nm}(D_{L/K})^{1/(nm)} = \mathrm{rd}(L)\,. \tag{2}$$

Here, $\mathrm{Nm}(I)$ denotes the numeric norm of an ideal I. Applied to $K \subseteq K^{gal}$, we have $\mathrm{rd}(K) \le \mathrm{grd}(K)$, and when applied to $K^{gal} \subseteq L^{gal}$ gives $\mathrm{grd}(K) \le \mathrm{grd}(L)$.

Throughout, we assume we have a fixed base field K, which may not be Galois over $\mathbf{Q}$, and a bound B such that $\mathrm{grd}(K) \le B$. We consider abelian extensions L/K such that $\mathrm{grd}(L) \le B$, and wish to determine restrictions on the conductors for L/K. We use the class field theory functions in gp [PAR08], and consequently, the extensions L/K are required to be not just abelian, but cyclic of prime order. This does not pose a serious problem for the computations. We now fix ℓ to be prime such that $\mathrm{Gal}(L/K) \cong C_\ell$.

2.1. **Root discriminants.** If $\mathfrak{f}$ is the conductor for L/K, we let $\mathfrak{f}_0$ denote its finite part. By the conductor-discriminant formula, $D_{L/K} = \mathfrak{f}_0^{\ell-1}$, and so by equation (2),

$$\mathrm{rd}(L) = \mathrm{rd}(K)(\mathcal{N}_{K/\mathbf{Q}}(\mathfrak{f}_0))^{\frac{\ell-1}{[L:\mathbf{Q}]}}.$$

This can be rephrased as bound on the conductor of an extension, which we will refer to this as the root discriminant test for conductors.

Proposition 2.1. *If K is a degree n number field, L/K is a C_ℓ extension with finite conductor $\mathfrak{f}_0$ and $\mathrm{rd}(L) \leq B$ for some bound B, then*

$$\mathcal{N}_{K/\mathbf{Q}}(\mathfrak{f}_0) \leq \left(\frac{B}{\mathrm{rd}(K)}\right)^{n\ell/(\ell-1)}.$$

2.2. **Galois root discriminants.** We have the stronger requirement $\mathrm{grd}(L) \leq B$ and use this to further restrict the list of conductors. For the base field K, we encode some basic information for computing $\mathrm{grd}(K)$, which we describe now.

For each prime p which ramifies in K, let F_p be the completion of K^{gal} at a prime above p; then $F_p/\mathbf{Q}_p$ is a Galois extension. Let $G = \mathrm{Gal}(F_p/\mathbf{Q}_p)$ and G^i denote its higher ramification groups with the standard upper numbering of [Ser79, Chap. IV]. For each $i \geq -1$, let $G^{i+} = \bigcup_{\epsilon>0} G^{i+\epsilon}$, so i is a jump in the filtration if and only if $G^i \neq G^{i+}$. Let $t = [G^0 : G^{0+}] = [G^0 : G^1]$, which is the degree of the maximal tame totally ramified subextension of $F_p/\mathbf{Q}_p$. If $i > 0$ is a jump in the filtration of higher ramification groups G^j, we refer to $s = i + 1$ as a wild slope and define its multiplicity m by $[G^{s-1} : G^{(s-1)+}] = p^m$. We then define the p-Galois slope content for K to be the slope content of $F_p/\mathbf{Q}_p$, which in turn is given by $\mathrm{GSC}_p(K) = [s_1, s_2, \ldots, s_k]_t$ where the s_i are wild slopes listed so that $s_i \leq s_{i+1}$ and each slope s is repeated m times where m is the multiplicity described above. Based on the factorization of the discriminant of K^{gal}, we have

$$\mathrm{grd}(K) = \prod_p p^{\alpha_p}$$

for rational numbers α_p. These can be computed from $\mathrm{GSC}_p(K)$ by the following formula (see [Jon, §1.1]).

$$\alpha_p = \frac{t-1}{p^k t} + \sum_{j=1}^{k} \left(\frac{1}{p^{k-j}} - \frac{1}{p^{k-j+1}}\right) s_j. \tag{3}$$

We first obtain a lower bound on tame degree of $\mathrm{GSC}_p(L)$ for a prime $p \neq \ell$. Here, if e is a positive integer and p is a prime with $e = p^j e'$ and $p \nmid e'$, then we refer to e' as the prime to p part of e.

Proposition 2.2. *Suppose K is a degree n number field, L/K is a C_ℓ extension, and p is a prime different from ℓ. Let t_K (resp. t_L) denote the tame degree for p of K^{gal} (resp. L^{gal}), let $\prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$ be the factorization of $p\mathcal{O}_K$, and for each e_i, let e_i' be its prime to p part. If $\mathfrak{p}_i$ divides the conductor for L/K, then*

$$\mathrm{lcm}(t_K, \ell e_i') \mid t_L\,.$$

Proof. Since $K^{gal} \subseteq L^{gal}$, we have $t_K \mid t_L$. Since $\mathfrak{p}_i$ divides the conductor and L/K is Galois of prime degree, $\mathfrak{p}_i$ is totally ramified in L/K. Thus, $e_i'\ell$ divides the ramification index of a prime in $\mathcal{O}_L$ above p, and consequently it divides the corresponding ramification index for a prime of $\mathcal{O}_{L^{gal}}$ above p. Since $e_i'\ell$ is prime to p, it divides t_L. □

If $p = \ell$, then the contribution of p to $\mathrm{grd}(L)$ is more subtle. Under certain conditions, we may be able to deduce that $\mathrm{GSC}_p(L)$ contains an additional wild slope when compared with $\mathrm{GSC}_p(K)$. We first define a partial ordering for slope contents from [Jon, Def. 2.3].

Definition 2.3. For two slope contents $\beta = [s_1, \ldots, s_k]_t$ and $\beta' = [s'_1, \ldots, s'_n]_{t'}$ associated to a prime p, then $\beta \leq \beta'$ if the following three conditions hold:

(1) $k \leq n$,
(2) $s_{k-i} \leq s'_{n-i}$ for $0 \leq i < k$,
(3) $t \leq p^{n-k} t'$.

It follows easily from equation (3) that $\beta \leq \beta'$ implies the corresponding inequality on Galois root discriminant exponents.

In general, if $E/\mathbf{Q}_p$ is a finite extension, its discriminant ideal is of the form (p^{c_E}) for some $c_E \geq 0$. If we embed E in a finite Galois extension $F/\mathbf{Q}_p$ with Galois group G, then $E = F^H$, the fixed field of H for some $H \leq G$, and

$$c_E = \sum_{i \geq -1} ([G : HG^{i+}] - [G : HG^i])(i+1) \tag{4}$$

(see [Jon, §1.2]). The non-zero terms of the sum come from the finitely many values i such that $HG^{i+} \neq HG^i$. In particular, for these values $G^{i+} \neq G^i$, so these are a subset of the jumps in the filtration of higher ramification groups. Those where $i > 0$ correspond to wild slopes. We note that the sum (4) is independent of whichever Galois field F is used, which is essentially a consequence of Herbrand's theorem.

Proposition 2.4. *Let p be a prime and L/K is a C_p extension of number fields with conductor $\mathfrak{f}$. Suppose $\mathfrak{p}$ is a prime of K above p such that $\mathfrak{p} \mid \mathfrak{f}$. Let* $\mathrm{GSC}_p(K) = [s_1, \ldots, s_m]_t$*, $\mathcal{D}$ be the different for $K/\mathbf{Q}$, e the ramification index for $\mathfrak{p}$ for $K/\mathbf{Q}$, and $v_\mathfrak{p}$ the valuation for $\mathfrak{p}$. Finally, let*

$$s = \frac{v_\mathfrak{p}(\mathcal{D}) + v_\mathfrak{p}(\mathfrak{f})}{e}.$$

If $s > s_m$, then $[s_1, \ldots, s_m, s]_t \leq \mathrm{GSC}_p(L)$.

Proof. First we note that $K^{gal} \subseteq L^{gal}$ implies the corresponding inclusion for their completions with respect to a prime above p. So, $\mathrm{GSC}_p(K) \leq \mathrm{GSC}_p(L)$ where each wild slope for K is a wild slope for L whose multiplicity in $\mathrm{GSC}_p(K)$ is less than or equal to its multiplicity for $\mathrm{GSC}_p(L)$. So, it suffices to show that $\mathrm{GSC}_p(L)$ contains an additional slope $\geq s$.

Since L/K is Galois of prime order and $\mathfrak{p} \mid \mathfrak{f}$, $\mathfrak{p}$ is totally ramified in L/K. Let $\mathfrak{P}$ be the prime of $\mathcal{O}_L$ above $\mathfrak{p}$, E' the completion of L at $\mathfrak{P}$, and E the closure of K in E'. Let F be the Galois closure for $E'/\mathbf{Q}_p$, $G = \mathrm{Gal}(F/\mathbf{Q}_p)$, and let H and H' be the subgroups of G corresponding to E and E', respectively.

Let f be the residue class degree for $\mathfrak{p}$. Then, $c_E = f v_\mathfrak{p}(\mathcal{D})$, and from the local analog of equation (1) we have

$$c_{E'} = pc_E + f(p-1)v_\mathfrak{p}(\mathfrak{f}) = pfv_\mathfrak{p}(\mathcal{D}) + f(p-1)v_\mathfrak{p}(\mathfrak{f})\,.$$

So,

$$\begin{aligned}\frac{c_{E'}-c_E}{[E':\mathbf{Q}_p]-[E:\mathbf{Q}_p]} &= \frac{pfv_{\mathfrak{p}}(\mathcal{D})+f(p-1)v_{\mathfrak{p}}(\mathfrak{f})-fv_{\mathfrak{p}}(\mathcal{D})}{pef-ef}\\ &= \frac{f(p-1)v_{\mathfrak{p}}(\mathcal{D})+f(p-1)v_{\mathfrak{p}}(\mathfrak{f})}{f(p-1)e}\\ &= \frac{v_{\mathfrak{p}}(\mathcal{D})+v_{\mathfrak{p}}(\mathfrak{f})}{e}\\ &= s.\end{aligned}$$

Now we compute the same quantity in terms of higher ramification groups using equation (4). Note that since F is the Galois closure of $E'/\mathbf{Q}_p$ and E' is the completion of L at $\mathfrak{P}$, the jumps in the higher ramification groups G^i when $i>0$ correspond to the wild slopes in $\mathrm{GSC}_p(L)$:

$$\begin{aligned}s &= \frac{c_{E'}-c_E}{[E':\mathbf{Q}_p]-[E:\mathbf{Q}_p]}\\ &= \sum_{i\geq -1}\frac{[G:H'G^{i+}]-[G:H'G^{i}]-\big([G:HG^{i+}]-[G:HG^{i}]\big)}{[E':\mathbf{Q}_p]-[E:\mathbf{Q}_p]}(i+1)\\ &= \sum_{i\geq -1}\frac{[G:H'G^{i+}]-[G:HG^{i+}]-\big([G:H'G^{i}]-[G:HG^{i}]\big)}{[G:H']-[G:H]}(i+1)\\ &= \sum_{i\geq -1}\left(\frac{[G:H'G^{i+}]-[G:HG^{i+}]}{[G:H']-[G:H]}-\frac{[G:H'G^{i}]-[G:HG^{i}]}{[G:H']-[G:H]}\right)(i+1).\end{aligned}$$

Without the factors $i+1$ (but keeping it a finite sum over the higher ramification filtration jumps), the sum telescopes and reduces to 1, so this is a weighted average of the values $i+1$. So, if $s>s_m$, then $F=(E')^{gal}$ has a new slope greater than or equal to s. □

Applying the results of Propositions 2.2 and 2.4 to a modulus $\mathfrak{f}$, combined with information about the slope content for K, we obtain a lower bound on the slope content of L. Then, using equation (4), we can compute a lower bound for $\mathrm{grd}(L)$ and check if it is $\leq B$. We refer to this as the grd test for conductors.

2.3. **Galois subfields.** Finally, we consider the case where $L/\mathbf{Q}$ and $K/\mathbf{Q}$ are both Galois extensions. While this is not general by any means, it occurs frequently enough to warrant special attention since we get an easy restriction on the list of potential conductors.

For a number field $K/\mathbf{Q}$ and $\mathfrak{p}$, a non-zero prime ideal of $\mathcal{O}_K$, we define $\mathcal{N}'_{K/\mathbf{Q}}(\mathfrak{p})$ to be the product of the distinct primes of $\mathcal{O}_K$ above $\mathfrak{p}\cap\mathbf{Z}$.

Proposition 2.5. *Let $\mathfrak{f}$ be the conductor of L/K and p a prime number. Suppose $K/\mathbf{Q}$ is a Galois extension, L/K is Abelian and $L/\mathbf{Q}$ is Galois. If there exists a prime ideal $\mathfrak{p}$ over p such that $\mathfrak{p}^j\mid\mathfrak{f}$ for some $j>0$, then $\mathcal{N}'_{K/\mathbf{Q}}(\mathfrak{p})^j\mid\mathfrak{f}$.*

Proof. Since $L/\mathbf{Q}$ and $K/\mathbf{Q}$ are Galois, $\mathfrak{f}_0$ is stable under the action of $\mathrm{Gal}(L/\mathbf{Q})$; but $\mathrm{Gal}(L/\mathbf{Q})$ acts through $\mathrm{Gal}(K/\mathbf{Q})$. So, if $\mathfrak{p}^j\mid\mathfrak{f}$ for some prime $\mathfrak{p}$ of $\mathcal{O}_K$, then $\sigma(\mathfrak{p})^j\mid\mathfrak{f}$ for all $\sigma\in\mathrm{Gal}(K/\mathbf{Q})$. Since $\mathrm{Gal}(K/\mathbf{Q})$ acts transitively on primes above $\mathfrak{p}\cap\mathbf{Z}$, $\mathcal{N}'_{K/\mathbf{Q}}(\mathfrak{p})^j\mid\mathfrak{f}$. □

When Proposition 2.5 applies, the grd test for conductors is of no use. Since K and L are both Galois over $\mathbf{Q}$, their root discriminants coincide with their Galois root discriminants. In this sense, Proposition 2.5 and the grd test for conductors are complementary.

2.4. **Procedure.** Here we outline the procedure used in the computations below. Let G be a finite group, and $B > 0$. We wish to determine $\mathcal{K}(G, B)$. By the Galois correspondence, we can describe what is needed in group theoretic language. We need subgroups $H_1 \leq H_2 \leq G$ where $\operatorname{Core}(H_1) = \langle e \rangle$, $H_1 \lhd H_2$, $H_2/H_1 \cong C_\ell$ for some prime ℓ. Here, the core of a subgroup is the intersection of its conjugates. Then, for each field K which is a sibling of $K^{gal} \in \mathcal{K}(G/\operatorname{Core}(H_2), B)$, we find all C_ℓ extensions L. This list will include a complete list of sibling fields for $\mathcal{K}(G, B)$.

So, let K be a number field with $\operatorname{grd}(K) \leq B$, and ℓ a prime. We wish to find all C_ℓ extensions L/K such that $\operatorname{grd}(L) \leq B$ and $\operatorname{Gal}(L^{gal}/\mathbf{Q}) \cong G$. We do this in six stages:

(1) generate a list of possible moduli $\mathfrak{f}$,
(2) compute the field for each congruence subgroup with modulus $\mathfrak{f}$ corresponding to a C_ℓ extension,
(3) use Frobenius filtering to remove some polynomials with the wrong Galois group,
(4) compute low degree siblings L' for the fields L,
(5) filter out fields L' which fail the conditions on their Galois root discriminants or Galois groups,
(6) remove duplicates.

Everything except stages (1) and (3) is fairly straightforward. In particular, stage (2) uses class field theory commands built into `gp`. Stage (4) involves computing resolvents and subfields, with the details varying from case to case. In stage (5), we compute Galois groups with `gp`. Galois root discriminants are computed using programs of Jones developed for [JR07a]. Finally, stage (6) is straightforward using `gp`. We note that while by default, `gp` makes assumptions in doing some class field computations, one can have it do the extra computations necessary to remove these assumptions (with the command `bnfcertify`). In all cases, we had `gp` do the extra computations.

Frobenius filtering is discussed below. For stage (1), we note that if p ramifies in L, then the minimum contribution of p to $\operatorname{grd}(L)$ is $\sqrt{p}$. Thus, we start with the following set of primes:

$$S_{\mathbf{Q}} = \left\{ p \;\middle|\; p \leq \left(\frac{B}{\operatorname{grd}(K)}\right)^2 \text{ or } p \mid d_K \right\}.$$

For prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$, we let

$$S_K = \begin{cases} \{\mathcal{N}'(\mathfrak{p}) \mid \mathfrak{p} \cap \mathbf{Z} \in S_{\mathbf{Q}}\} & \text{if } L/\mathbf{Q} \text{ and} K/\mathbf{Q} \text{ are Galois,} \\ \{\mathfrak{p} \mid \mathfrak{p} \cap \mathbf{Z} \in S_{\mathbf{Q}}\} & \text{otherwise.} \end{cases}$$

We build a list of potential conductors, starting with the one element list $\mathcal{L} = (\mathcal{O}_K)$. For each ideal $I \in S_K$ and each ideal J from the list $\mathcal{L}$, we consider the products $I^k J$ where $k = 1$ if the prime $p \in I$ is different from ℓ, and $2 \leq k \leq \lfloor \ell e(\mathfrak{p}/\ell)/(\ell - 1) \rfloor + 1$ otherwise. If the ideal $I^k J$ passes both the root discriminant test and the Galois root discriminant tests, it is appended to $\mathcal{L}$.

Once we have exhausted S_K, we test each potential conductor $\mathfrak{f} \in \mathcal{L}$ and ramification type at infinity and keep only those for which there exists a congruence subgroup C with conductor $\mathfrak{f}$ corresponding to at least one C_ℓ extension of K. This completes stage (1).

We note that the definition of the set S_K makes use of $\mathrm{grd}(K)$. So, in cases where K is not Galois over $\mathbf{Q}$, the use of Galois root discriminants is utilized at an early stage of the computation.

2.5. **Frobenius filtering.** In stage (3), we want to quickly filter out polynomials which have the wrong Galois group. We employed the following well-known technique, which we refer to as Frobenius filtering.

Given a separable degree n monic polynomial $f \in \mathbf{Z}[x]$, one can factor f over $\mathbf{F}_p$. If $p \nmid \mathrm{disc}(f)$, then the degrees of the irreducible factors give the cycle type for the Frobenius automorphism in $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$ acting on the roots of f. This lifts to an element $\mathrm{Frob}_p \in \mathrm{Gal}(f)$ with the same cycle type. The lifting is defined up to conjugation, hence its cycle type is well defined. So, one can often quickly prove that $\mathrm{Gal}(f)$ is not conjugate to some fixed group $G \leq S_n$ if the factorization of f over $\mathbf{F}_p$ (for some $p \nmid \mathrm{disc}(f)$) does not yield a cycle type of an element of G.

For each polynomial, we tested up to 1000 primes p such that $p \nmid \mathrm{disc}(f)$. Naturally, if we find one such prime which proves that f has the wrong Galois group, we do not need to test f any further. It is possible that a polynomial is not eliminated by Frobenius filtering and still have $\mathrm{Gal}(f)$ not conjugate to G. We eliminate such polynomials in stage (5).

In practice, this reduced the number of polynomials requiring further processing considerably. For example, for the sextic fields with Galois group $C_3^2 : C_4$, we first computed degree 12 extensions. Of the 293 dodecic polynomials, only 80 survived Frobenius filtering. The computation for octic fields $8T46$ also starts by computing degree 12 extensions. Here, Frobenius filtering reduced the number of polynomials under consideration from 483 to 40. Finally, we note that using 1000 primes for this stage is almost certainly overkill, the computation runs relatively quickly.

2.6. **Representing fields, siblings, and Frobenius elements.** For a given Galois field $K \in \mathcal{K}(G, \Omega)$ for some group G, we represent the field as the splitting field of an irreducible polynomial of as small degree n as possible. Sometimes, there will be several degree n siblings for a given field K, and so we find a representative polynomial for each. The website [JR07b] gives these polynomials, and for printable tables for the fields, sibling fields are grouped together.

In most cases, we generate sibling fields by means of resolvents. In a few cases, we did not find a convenient resolvent. Our computations would necessarily find complete sibling sets if one, hence all siblings, meet the grd bound. Matching siblings then becomes a process of elimination. For this, we use the discriminant of the Galois closure and Frobenius elements.

The use of discriminants is clear. For Frobenius elements, we observe that the cycle type of a Frobenius element Frob_p determines the order of Frob_p as a group element: it is the least common multiple of the cycle lengths. While the cycle types of Frob_p may vary for sibling fields, $|\mathrm{Frob}_p|$ does not. Hence, these orders match for sibling fields.

When matching siblings we compute the vector

$$(D_L^{gal}, |\mathrm{Frob}_2|, |\mathrm{Frob}_3|, \ldots, |\mathrm{Frob}_{541}|),$$

which uses the first 100 primes. If a prime p divides the polynomial discriminant but not the field discriminant, we use gp to compute residue class degrees, which in turn gives $|\mathrm{Frob}_p|$. If a prime p divides d_L, we use 0 in place of $|\mathrm{Frob}_p|$. The resulting vector then provides a reliable fingerprint of the splitting field of a polynomial where two polynomials with different fingerprints cannot be siblings. By the completeness of our search, and knowing how many siblings to expect, we can then match siblings by this method. In cases where 100 primes were insufficient, we simply repeated the computation using more Frobenius elements.

It is interesting to observe the connections between sibling fields, arithmetically equivalent fields, and Frobenius fingerprints. Arithmetically equivalent fields are non-isomorphic fields with the same Dedekind zeta functions. By [Per77, Th. 1], if L and M are arithmetically equivalent, then: (i) L and M have isomorphic normal closures; (ii) $[L : \mathbf{Q}] = [M : \mathbf{Q}]$; (iii) every prime p has the same splitting type in L and M; and (iv) $D_L = D_M$. From (i), we see that arithmetically equivalent fields are a special case of sibling fields. From (iii), we further see that the cycle type of Frob_p will be the same for L and M for each prime p. So, Frobenius fingerprints will match arithmetically equivalent fields. In fact, arithmetically equivalent fields would be matched with the more stringent test where one used the cycle types of the Frob_p instead of the orders of these group elements. Note, we want arithmetically equivalent fields to be matched since here we are trying to match sibling fields.

As noted above, sibling fields are guaranteed to have the same Frobenius fingerprint. Conversely, two fields which are not siblings must have different fingerprints if one checks a sufficient number of primes. This follows since we are interested in invariants of say the Galois closures of the two fields L and M, and $L^{gal} \cong M^{gal}$ if and only if L^{gal} and M^{gal} have the same sets of primes which split completely. Here, a prime p splits completely in L^{gal} if and only if $|\mathrm{Frob}_p| = 1$. So, the fingerprints for non-sibling fields are assured to differ eventually, with a bound on how far one must check deducible from the Tchebotarev density theorem. We did not need this bound since we only used these fingerprints to prove that pairs of fields were not siblings.

3. Results

We applied the procedure outlined above to determine $\mathcal{K}(G, \Omega)$ for many specific groups G and $\Omega = 8\pi e^\gamma \approx 44.7632$ as in [JR07a]. Below, we give the number of fields in each case, along with a few notes on the computations. Complete lists of fields are given at [JR07b].

3.1. **Sextics.** In [JR07a, Thm. 5.1], Jones and Roberts determined $\mathcal{K}(G, \Omega)$ for 14 of the 16 Galois groups in degree 6. For the remaining two groups they found fields with Galois groups $C_3^2 : C_4$ and $C_3^2 : D_4$; however, the methods employed did not prove that these two lists were complete. Here, we do so.

Proposition 3.1. *$|\mathcal{K}(C_3^2 : C_4, \Omega)| = 17$ and $|\mathcal{K}(C_3^2 : C_4, \Omega)| = 137$.*

Both computations involve $\ell = 3$ for a C_3 extension of a quartic field. For $G = C_3^2 : C_4$ (resp. $G = C_3^2 : D_4$), a Galois field has a degree 12 sibling which contains a sextic sibling as a subfield. We first compute the degree 12 fields as C_3 extensions of a quartic C_4 (resp. quartic D_4) field.

To get a feel for the steps in the computation, we give some details on determining $\mathcal{K}(C_3^2 : C_4, \Omega)$. There are 228 fields in $\mathcal{K}(C_4, \Omega)$. If we used only the root discriminant test to screen potential moduli, we found 335 moduli. When we used both the root discriminant test and the Galois root discriminant test, we found 133 moduli. From the 133 moduli, there are 293 modulus/congruence subgroup pairs. After computing polynomials, Frobenius filtering reduced the number to 80. Taking resolvents and removing duplicates, yielded 40 distinct sextic fields. All had the right Galois group, and 34 satisfied $\mathrm{grd}(L) \leq \Omega$. Each Galois field gives rise to two such (sibling) sextic fields, so the number of $C_3^2 : C_4$ Galois fields is 17.

3.2. **Septics.** There are four solvable Galois groups that appear in degree 7, viz. C_7, $D_7 = C_7 : C_2$, $C_7 : C_3$, and $F_7 = C_7 : C_6$. Naturally, the group C_7, being abelian, is handled by [JR07a, Prop. 3.1]. We treat the remaining three groups here.

Proposition 3.2. *$|\mathcal{K}(D_7, \Omega)| = 80$, $|\mathcal{K}(C_7 : C_3, \Omega)| = 2$, and $|\mathcal{K}(F_7, \Omega)| = 94$.*

Note, each group is of the form $C_7 : C_d$ where $d \mid 6$. We compute these fields by looking for C_7 extensions of a C_d field. Section 2.3 applies, which shortens the list of potential conductors. The sets $\mathcal{K}(C_d, \Omega)$ were known from [JR07b].

The resulting fields have degrees 14, 21, and 42. The greatest computational difficulties naturally arose for the $C_7 : C_6$ fields. Here, even computing the degree 42 polynomials seemed too slow. However, given a C_d field and a modulus $\mathfrak{f}$, we have enough information to specify ramification information for the corresponding degree 7 field. Since the groups $C_7 : C_d$ are Frobenius groups, we can apply the following proposition of Fieker and Klüners [FK03, Thm. 4]. We have specialized the notation to match the situation considered here.

Proposition 3.3 (Fieker, Klüners)**.** *Let ℓ be prime, $d \mid \ell - 1$, and K a C_d extension of $\mathbf{Q}$. Further, suppose L is a $C_\ell : C_d$ extension of $\mathbf{Q}$ containing K, and p a prime. Finally, let F be a degree ℓ extension of $\mathbf{Q}$ with L as its Galois closure. Then*

$$d_F = d_K^{(\ell-1)/d} \, \mathrm{Nm}(D_{L/K})^{1/d}.$$

In [JR03], Jones and Roberts describe targeted Hunter searches, a method for searching for primitive number fields with prescribed ramification. Using Proposition 3.3, we employed such searches to find some of the $C_7 : C_6$ septics.

We note that while Proposition 3.3 gives us discriminant information, one can determine more refined information for the local algebras $F \otimes \mathbf{Q}_p$. This information, in turn, could be fed into the machinery of the targeted Hunter search making it more efficient.

Finally, when conducting the targeted Hunter search, one need not wait for the search to complete. One knows beforehand how many fields to expect from class field theory.

3.3. **Octics.** Here we consider the solvable groups which appear as transitive subgroups of S_8, and represent corresponding Galois extensions as the splitting fields of irreducible degree 8 polynomials. We omit groups which appear as Galois groups of lower degree irreducible polynomials since they have already been treated in [JR07a].

Proposition 3.4. *For solvable groups which appear as Galois groups of irreducible octics, we have the following.*

G	$\lvert\mathcal{K}(G,\Omega)\rvert$	G	$\lvert\mathcal{K}(G,\Omega)\rvert$
$8T5 = Q_8$	7	$8T27 = C_2^4 : C_4$	80
$8T6 = D_8$	354	$8T29 = C_2^3 : D_4$	229
$8T7 = C_8 : C_2$	55	$8T30 = C_2^4 : C_4$	35
$8T8 = QD_{16}$	121	$8T32 = C_2^3 : A_4$	8
$8T9 = D_4C_2$	1477	$8T33 = C_2^3 : A_4$	12
$8T10 = (C_4C_2) : C_2$	310	$8T34 = C_2^4 : S_3$	55
$8T11 = (C_4C_2) : C_2$	307	$8T35 = D_4^2 : C_2$	183
$8T12 = SL_2(3)$	4	$8T36 = C_2^3 : (C_7 : C_3)$	4
$8T15 = (D_4C_2) : C_2$	818	$8T38 = C_2^4 : A_4$	23
$8T16 = 8T7 : C_2$	38	$8T39 = C_2^3 : S_4$	14
$8T17 = C_4^2 : C_2$	126	$8T40 = Q_8 : S_4$	49
$8T18 = C_2^4 : C_2$	318	$8T41 = C_3^2 : S_4$	111
$8T19 = C_2^3 : C_4$	110	$8T42 = A_4 \wr C_2$	9
$8T22 = (D_4C_2) : C_2$	147	$8T44 = C_2^4.S_4$	84
$8T23 = GL_2(3)$	194	$8T45 = A_4^2 : C_2^2$	39
$8T25 = C_2^3 : C_7$	1	$8T46 = A_4^2 : C_4$	0
$8T26 = C_4^2 : C_2 : C_2$	210	$8T47 = S_4^2 \wr C_2$	15

The simplest cases are when the octic field contains a quartic subfield. This accounts for most of the solvable octic groups. For octic fields which have a quadratic, but no quartic subfield, the octic has a degree 12 sibling, which in turn is a quadratic extension of a sextic field. Finally, there are two solvable primitive octic groups: $8T25 = C_2^3 : C_7$ and $8T36 = C_2^3 : (C_7 : C_3)$. In both cases, the octic field has a degree 14 sibling which is a quadratic extension of a septic field. The septic fields, having Galois groups C_7 or $C_7 : C_3$ have already been determined by [JR07b] and §3.2 above.

3.4. **Nonics.**

Proposition 3.5. *For solvable groups which appear as Galois groups of irreducible nonics, we have the following.*

G	$\lvert\mathcal{K}(G,\Omega)\rvert$	G	$\lvert\mathcal{K}(G,\Omega)\rvert$
$9T3 = D_9$	105	$9T20 = C_3 \wr S_3$	10
$9T5 = C_3^2 : C_2$	48	$9T21 = C_3^3 : S_3$	42
$9T6 = C_9 : C_3$	2	$9T22 = C_3^2 : C_3 : S_3$	17
$9T7 = C_3^2 : C_3$	0	$9T23 = C_3^2 : SL_2(\mathbf{F}_3)$	0
$9T10 = C_9 : C_6$	69	$9T24 = C_3^2 : C_3 : D_6$	37
$9T11 = C_3^2 : C_6 = 9T13$	64	$9T25 = C_3^3 : A_4$	4
$9T12 = C_3^2 : S_3$	37	$9T26 = C_3^2 : GL_2(\mathbf{F}_3)$	51
$9T14 = C_3^2 : Q_8$	2	$9T28 = S_3 \wr C_3$	7
$9T15 = C_3^2 : C_8$	3	$9T29 = C_3^3 : S_4$	2
$9T17 = C_3 \wr C_3$	0	$9T30 = C_3^3 : S_4$	35
$9T18 = C_3^2 : D_6$	145	$9T31 = S_3 \wr S_3$	15
$9T19 = C_3^2 : QD_{16}$	33		

The simplest case is where the nonic field has non-trivial automorphisms. Then it can be computed as the C_3 extension of a cubic field. If the nonic has a cubic subfield but no non-trivial automorphisms, it must be an S_3 cubic extension of the subfield. In this case, we can first find the C_3 extensions of the appropriate sextic fields. This gives a degree 18 field which has the desired nonic as a subfield.

The last case consists of primitive nonics. In each case here, one computes degree 24 fields as C_3 extensions of the appropriate octic field. This has a degree 12 subfield which is a sibling of the desired field. We then use resolvents to go from the dodecic sibling to the nonic field.

3.5. **Small groups.** Combining previous results above with those of [JR07a], the sets $\mathcal{K}(G,\Omega)$ are classified for all finite groups G with $|G| \leq 11$. Here we extend the list to all groups G with $|G| \leq 23$. The results are given in Table 1.

Table 1. Sizes $|\mathcal{K}(G,\Omega)|$ for all groups with $|G| \leq 23$. Groups are listed by a descriptive name, and by their small group number from gap.

G		#	G		#	G		#	G		#
C_2	$[2,1]$	1220	D_5	$[10,1]$	146	$C_4:C_4$	$[16,4]$	11	$C_3^2:C_2$	$[18,4]$	48
C_3	$[3,1]$	47	C_{10}	$[10,2]$	69	C_8C_2	$[16,5]$	30	C_6C_3	$[18,5]$	19
C_4	$[4,1]$	228	C_{11}	$[11,1]$	1	$C_8:C_2$	$[16,6]$	55	C_{19}	$[19,1]$	0
C_2^2	$[4,2]$	2421	$C_3:C_4$	$[12,1]$	15	D_8	$[16,7]$	354	$C_{10}.C_2$	$[20,1]$	0
C_5	$[5,1]$	7	C_{12}	$[12,2]$	66	QD_{16}	$[16,8]$	121	C_{20}	$[20,2]$	8
S_3	$[6,1]$	610	A_4	$[12,3]$	59	Q_{16}	$[16,9]$	0	$C_5:C_4$	$[20,3]$	102
C_6	$[6,2]$	399	D_6	$[12,4]$	1795	$C_4C_2^2$	$[16,10]$	195	D_{10}	$[20,4]$	384
C_7	$[7,1]$	4	C_6C_2	$[12,5]$	391	D_4C_2	$[16,11]$	1477	$C_{10}C_2$	$[20,5]$	56
C_8	$[8,1]$	23	C_{13}	$[13,1]$	1	Q_8C_2	$[16,12]$	7	$C_7:C_3$	$[21,1]$	2
C_4C_2	$[8,2]$	581	D_7	$[14,1]$	80	$Q_8:C_2$	$[16,13]$	307	C_{21}	$[21,2]$	2
D_4	$[8,3]$	1425	C_{14}	$[14,2]$	8	C_2^4	$[16,14]$	16	D_{11}	$[22,1]$	32
Q_8	$[8,4]$	7	C_{15}	$[15,1]$	4	C_{17}	$[17,1]$	0	C_{22}	$[22,2]$	7
C_2^3	$[8,5]$	908	C_{16}	$[16,1]$	9	D_9	$[18,1]$	105	C_{23}	$[23,1]$	1
C_9	$[9,1]$	3	C_4^2	$[16,2]$	16	C_{18}	$[18,2]$	24			
C_3^2	$[9,2]$	9	$C_2^2:C_4$	$[16,3]$	310	S_3C_3	$[18,3]$	254			

Most of these computations are straightforward since in most cases, we are computing the full Galois field (since groups with faithful transitive permutation representations of degree < 10 have already been dealt with).

It is interesting to look a little more closely at cases where $\mathcal{K}(G,\Omega) = \emptyset$. The smallest such group is the generalized quaternion group of order 16, Q_{16}. This group has a D_4 quotient, and $|\mathcal{K}(D_4,\Omega)| = 1408$ which is fairly large. Thus, it is at first a bit surprising that $\mathcal{K}(Q_{16},\Omega) = \emptyset$. However, the obstructions to an octic D_4 field being embedded in a Q_{16} are fairly restrictive [Sch89, Thm. 2], with only 31 base fields passing the lifting criterion. Of those, none of the lifts fit under the root discriminant bound Ω.

The groups C_{17} and C_{19} are less surprising since the fields are cyclotomic, and C_p fields are highly ramified, and ramified at primes $\geq p$.

The last group in Table 1 for which $\mathcal{K}(G,\Omega)$ is empty is $G = C_{10}.C_2$. Such a field is a compositum of a C_4 field and a D_5 field which share a common quadratic field. There are only a few such pairs to start with, and none lead to a field which fit under our chosen root discriminant bound.

3.6. **Dihedral fields.** In [JR07a, Prop. 3.1], Jones and Roberts determine all abelian groups A such that $\mathcal{K}(A,\Omega)$ is non-empty. Here, we consider the analogous question for the most accessible non-abelian groups, the dihedral groups D_ℓ where ℓ is an odd prime. We show that $\bigcup_\ell \mathcal{K}(D_\ell,\Omega)$ is a finite set, and exactly which primes ℓ contribute.

Proposition 3.6. *For all odd primes $\ell > 43$, $\mathcal{K}(D_\ell,\Omega) = \emptyset$. Moreover,*

$$\begin{array}{lll}
|\mathcal{K}(D_3,\Omega)| \ = 610 & |\mathcal{K}(D_5,\Omega)| \ = 146 & |\mathcal{K}(D_7,\Omega)| \ = 80 \\
|\mathcal{K}(D_{11},\Omega)| = \ \ 32 & |\mathcal{K}(D_{13},\Omega)| = \ \ 18 & |\mathcal{K}(D_{17},\Omega)| = 10 \\
|\mathcal{K}(D_{19},\Omega)| = \ \ \ \ 9 & |\mathcal{K}(D_{23},\Omega)| = \ \ \ \ 8 & |\mathcal{K}(D_{29},\Omega)| = \ \ 1 \\
|\mathcal{K}(D_{31},\Omega)| = \ \ \ \ 2 & |\mathcal{K}(D_{37},\Omega)| = \ \ \ \ 1 & |\mathcal{K}(D_{41},\Omega)| = \ \ 1 \\
|\mathcal{K}(D_{43},\Omega)| = \ \ \ \ 1 & &
\end{array}$$

Proof. If $L \in \mathcal{K}(D_\ell,\Omega)$, then L contains a quadratic field $K \in \mathcal{K}(C_2,\Omega)$, and $\mathrm{Gal}(L/K) \cong C_\ell$. If L/K is unramified, then ℓ divides the class number of K. There are finitely many fields $K \in \mathcal{K}(C_2,\Omega)$, so it is not hard to check that this happens exactly when $\ell \leq 43$ (for ℓ an odd prime). In each such case, the corresponding extension $L/\mathbf{Q}$ would have to be Galois of order 2ℓ, and not abelian. Hence it is dihedral. Since L/K is unramified, $\mathrm{rd}(L) = \mathrm{rd}(K) \leq \Omega$, so $L \in \mathcal{K}(D_\ell,\Omega)$. Moreover, we carried out the computation of the sets $\mathcal{K}(D_\ell,\Omega)$ for $\ell \leq 23$ (including cases of non-trivial conductors) to obtain the counts given.

It remains to show that $\mathcal{K}(D_\ell,\Omega) = \emptyset$ for $\ell \geq 47$, so we assume not and that $L \in \mathcal{K}(D_\ell,\Omega)$. With K as above, let $\mathfrak{f}$ be the conductor for L/K. By a theorem of Martinet [Coh00, Prop. 10.1.25], $\mathfrak{f} = m\mathcal{O}_K$ for some integer m. Since $\ell \geq 47$, the conductor is non-trivial, so m is divisible by some prime p.

Now $p^{\ell-1} \mid D_{L/K}$ by equation (1), and so $p^{2(\ell-1)}d_K^\ell \leq d_L$. Using that the smallest value for $d_K = 3$, we have

$$p^{(\ell-1)/\ell} \leq \frac{\mathrm{rd}(L)}{d_K^{1/2}} = \frac{\mathrm{grd}(L)}{\sqrt{d_K}} \leq \frac{\Omega}{\sqrt{3}}\,.$$

So,

$$p \leq \left(\frac{\Omega}{\sqrt{3}}\right)^{\ell/(\ell-1)} \leq \left(\frac{\Omega}{\sqrt{3}}\right)^{47/46} < 28\,.$$

Thus, $p \leq 23$.

Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ above p. If $\mathfrak{p}$ is wildly ramified in L/K, then $\ell = p \leq 23$, a contradiction to $\ell \geq 47$. So, $\mathfrak{p}$ must be tamely ramified, which implies $\ell \mid \mathrm{Nm}(\mathfrak{p})-1$, $\mathrm{Nm}(\mathfrak{p})$ being the numeric norm of the ideal for $K/\mathbf{Q}$. So, $47 \leq \ell \leq \mathrm{Nm}(\mathfrak{p})-1$. Since $p < \ell$, this forces $\mathfrak{p}$ to be inert, so $N(\mathfrak{p}) = p^2$. So, ℓ divides $p^2-1 = (p-1)(p+1)$, but with $p < \ell$, we cannot have $\ell \mid p-1$. Thus, $\ell \mid p+1$, which is a contradiction since otherwise $47 \leq \ell \leq p+1 \leq 24$. □

References

[BM83] Gregory Butler and John McKay, *The transitive groups of degree up to eleven*, Comm. Algebra **11** (1983), no. 8, 863–911. MR84f:20005

[CHM98] John H. Conway, Alexander Hulpke, and John McKay, *On transitive permutation groups*, LMS J. Comput. Math. **1** (1998), 1–8 (electronic). MR99g:20011

[Coh00] Henri Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York, 2000. MR2000k:11144

[FK03] Claus Fieker and Jürgen Klüners, *Minimal discriminants for fields with small Frobenius groups as Galois groups*, J. Number Theory **99** (2003), no. 2, 318–337. MR1968456 (2004f:11147)

[GAP06] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4*, 2006, (http://www.gap-system.org).

[Jon] John W. Jones, *Wild ramification bounds and simple group Galois extensions ramified only at* 2, Proc. Amer. Math. Soc. **139** (2011), no. 3, 807–821. MR2745634

[JR03] John W. Jones and David P. Roberts, *Septic fields with discriminant* $\pm 2^a 3^b$, Math. Comp. **72** (2003), no. 244, 1975–1985 (electronic). MR1986816 (2004e:11119)

[JR07a] ———, *Galois number fields with small root discriminant*, J. Number Theory **122** (2007), no. 2, 379–407. MR2292261 (2008e:11140)

[JR07b] ———, *Website: Number fields with small grd*, http://hobbes.la.asu.edu/lowgrd, 2007.

[PAR08] The PARI Group, Bordeaux, *Pari/gp, version 2.3.4*, 2008.

[Per77] Robert Perlis, *On the equation* $\zeta_K(s) = \zeta_{K'}(s)$, J. Number Theory **9** (1977), no. 3, 342–360. MR0447188 (56:5503)

[Sch89] Leila Schneps, $\tilde{D}_4$ *et* $\hat{D}_4$ *comme groupes de Galois*, C. R. Acad. Sci. Paris Sér. I Math. **308** (1989), no. 2, 33–36. MR980080 (90f:12004)

[Ser79] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg. MR82e:12016

[Ser86] ———, *Œuvres. Vol. III*, Springer-Verlag, Berlin, 1986, 1972–1984. MR926691 (89h:01109c)

School of Mathematical and Statistical Sciences, Arizona State University, P.O. Box 871804, Tempe, Arizona 85287

E-mail address: jj@asu.edu

School of Mathematical and Statistical Sciences, Arizona State University, P.O. Box 871804, Tempe, Arizona 85287

Current address: Faith Christian School, P.O. Box 31300, Mesa, Arizona 85275

E-mail address: rwallington@faith-christian.org