LMS J. Comput. Math. 17 (1) (2014) 595–618
doi:10.1112/S1461157014000424

A database of number fields

John W. Jones and David P. Roberts

Abstract

We describe an online database of number fields which accompanies this paper. The database centers on complete lists of number fields with prescribed invariants. Our description here focuses on summarizing tables and connections to theoretical issues of current interest.

1. *Introduction*

A natural computational problem is to completely determine the set $\mathcal{K}(G, D)$ of all degree-n number fields K with a given Galois group $G \subseteq S_n$ and a given discriminant D. Many papers have solved instances of this problem, some relatively early contributions being [**3**, **16**, **32**, **36**].

This paper describes our online database of number fields at http://hobbes.la.asu.edu/NFDB/. This database gives many complete determinations of $\mathcal{K}(G, D)$ in small degrees n, collecting previous results and going well beyond them. Our database complements the Klüners–Malle online database [**25**], which covers more groups and signatures, but is not as focused on completeness results and the behavior of primes. Like the Klüners–Malle database, our database is searchable and intralinked.

Section 2 explains in practical terms how one can use the database. Section 3 explains some of the internal workings of the database, including how it keeps track of completeness. Section 4 presents tables summarizing the contents of the database in degrees $n \leqslant 11$, which is the setting of most of our completeness results. The section also briefly indicates how fields are chosen for inclusion in the database and describes connections with previous work.

The remaining sections each summarize an aspect of the database, and explain how the tabulated fields shed some light on theoretical issues of current interest. As a matter of terminology, we incorporate the signature of a field into our notion of discriminant, considering the formal product $D = -^s|D|$ to be the discriminant of a field with s complex places and absolute discriminant $|D|$.

Section 5 focuses on the complete list of all 11 279 quintic fields with Galois group $G = S_5$ and discriminant of the form $-^s 2^a 3^b 5^c 7^d$. The summarizing table here shows that the distribution of discriminants conforms moderately well to the mass heuristic of [**5**]. Section 6 summarizes lists of fields for more nonsolvable groups, but now with attention restricted to discriminants of the form $-^s p^a q^b$ with $p < q$ primes.

Sections 7 and 8 continue to pursue cases with $D = -^s p^a q^b$, but now for octic groups G of 2-power order. Section 7 treats the cases $p > 2$ and discusses connections to tame maximal nilpotent extensions as studied in [**9**, **10**]. Section 8 treats the case $p = 2$ and takes a first step towards understanding wild ramification in some of the nilpotent extensions studied in [**26**].

Sections 9 and 10 illustrate progress in the database on a large project initiated in [**21**]. The project is to completely classify Galois number fields with root discriminant $|D|^{1/n}$ at most the

Received 1 April 2014.

2010 Mathematics Subject Classification 11R21, 11R32 (primary).

This work was partially supported by a grant from the Simons Foundation (#209472 to David Roberts).

Serre–Odlyzko constant $\Omega := 8\pi e^{\gamma} \approx 44.76$. Upper bounds on degrees coming from analysis of Dedekind zeta functions [29, 30] play a prominent role. The database gives many solvable fields satisfying the root discriminant bound. In this paper, for brevity, we restrict attention to nonsolvable fields, where, among other interesting things, modular forms [8, 35] sometimes point the way to explicit polynomials.

The database we are presenting here has its origin in posted versions of the complete tables of our earlier work [18]. Other complete lists of fields were posted sporadically in the next ten years, while most fields and the new interface are recent additions. Results from the predecessors of the present database have occasionally been used as ingredients of formal arguments, as in for example [12, 15, 31]. The more common use of our computational results has been to guide investigations into number fields in a more general way. With our recent enhancements and this accompanying paper, we aim to increase the usefulness of our work to the mathematical community.

2. *Using the database*

A simple way to use the database is to request $\mathcal{K}(G, D)$ for a particular (G, D). A related but more common way is to request the union of these sets for varying G and/or D. Implicit throughout this paper and the database is that fields are always considered up to isomorphism. As a very simple example, asking for quartic fields with any Galois group G and discriminant D satisfying $|D| \leqslant 250$ returns Table 2.1.

In general, the monic polynomial $f(x) \in \mathbb{Z}[x]$ in the last column defines the field of its line, via $K = \mathbb{Q}[x]/f(x)$. It is standardized by requiring the sum of the absolute squares of its complex roots to be minimal, with ties broken according to the conventions of Pari's *polredabs*. Note that the database, like its local analog [20], is organized around non-Galois fields. However, on a given line, some of the information refers to a Galois closure K^g.

The Galois group $G = \mathrm{Gal}(K^g/\mathbb{Q})$ is given by its common name, as in Table 2.1, or its T-name, as in [11, 37, 38], if it does not have a very widely accepted common name. Information about the group, essential for intelligibility in higher degrees, is obtainable by clicking on the group. For example, the database reports $10T42$ as having structure $A_5^2.4$ and hence order $60^2 4 = 14\,400$; moreover, it is isomorphic to $12T278$, $20T457$, and $20T461$.

Continuing to explain Table 2.1, the column D prints $-^s|D|$, where s is the number of complex places and $|D|$ is given in factored form. This format treats the infinite completion $\mathbb{Q}_\infty = \mathbb{R}$ on a parallel footing with the p-adic completions $\mathbb{Q}_p$. If $n \leqslant 11$, then clicking on any appearing prime p links into the local database of [20], thereby giving a detailed description

TABLE 2.1. *Results of a query for quartic fields with absolute discriminant less than or equal to 250, sorted by root discriminant.*

Results below are proven complete					
rd(K)	grd(K)	D	h	G	Polynomial
3.29	6.24	$-^2 3^2 13^1$	1	D_4	$x^4 - x^3 - x^2 + x + 1$
3.34	3.34	$-^2 5^3$	1	C_4	$x^4 - x^3 + x^2 - x + 1$
3.46	3.46	$-^2 2^4 3^2$	1	V_4	$x^4 - x^2 + 1$
3.71	6.03	$-^2 3^3 7^1$	1	D_4	$x^4 - x^3 + 2x + 1$
3.87	3.87	$-^2 3^2 5^2$	1	V_4	$x^4 - x^3 + 2x^2 + x + 1$
3.89	15.13	$-^2 229^1$	1	S_4	$x^4 - x + 1$

of the p-adic algebra $K_p = \mathbb{Q}_p[x]/f(x)$. This automatic p-adic analysis also often works in degrees $n > 11$.

The root discriminant $\mathrm{rd}(K) = |D|^{1/n}$ is placed in the first column, since one commonly wants to sort by root discriminant. Here and later we often round real numbers to the nearest hundredth without further comment. When it is implemented, our complete analysis at all ramifying primes p automatically determines the Galois root discriminant of K, meaning the root discriminant of a Galois closure K^g. The second column gives this more subtle invariant $\mathrm{grd}(K)$. Clicking on the entry gives the exact form and its source. Often it is better to sort by this column, as fields with the same Galois closure are then put next to each other. As an example, quartic fields with $G = D_4$ come in twin pairs with the same Galois closure. The twin K^t of the first listed field K in Table 2.1 is off the table because $|D(K^t)| = 3^1 13^2 = 507$; however, $\mathrm{grd}(K^t) = \mathrm{grd}(K) = 3^{1/2}13^{1/2} \approx 6.24$.

Class numbers are given in the column h, factored as $h_1 \ldots h_d$, where the class group is a product of cyclic groups of size h_i. There is a toggle button, so that one can alternatively receive narrow class numbers in the same format. To speed up the construction of the table, class numbers were computing assuming the generalized Riemann hypothesis (GRH); they constitute the only part of the database that is conditional. Theoretical facts about class groups can be seen repeatedly in various parts of the database. For example, let n be an odd positive integer and consider a degree-n field K with dihedral Galois group D_n. Let L be its Galois closure with unique quadratic subfield F. Let p be a prime not dividing $2n$ and consider the p-parts of all class groups in question. Then, decomposing via the natural D_n action on $\mathrm{Cl}_p(L)$ and using the triviality of $\mathrm{Cl}_p(\mathbb{Q})$, one gets

$$\mathrm{Cl}_p(L) \cong \mathrm{Cl}_p(K)^2 \times \mathrm{Cl}_p(F). \tag{2.1}$$

One explicit example comes from the unique D_7 field K with Galois root discriminant $1987^{1/2} \cong 44.58$. Illustrating (2.1), the database reports $\mathrm{Cl}(L) = 13 \cdot 13$, $\mathrm{Cl}(K) = 13$, and $\mathrm{Cl}(F) = 7$.

When the response to a query is known to be complete, the table is headed by the completeness statement shown in Table 2.1. As emphasized in the introduction, keeping track of completeness is one of the most important features of the database. The completeness statement often reflects a very long computational proof, even if the table returned is very short.

There are many other ways to search the database, mostly connected to the behavior of primes. For example, one can restrict the search to find fields with restrictions on $\mathrm{ord}_p(D)$ or one can search directly for fields with Galois root discriminant in a given range. On the other hand, there are some standard invariants of fields that the database does not return, such as Frobenius partitions and regulators. The database does allow users to download the list of polynomials returned, so that it can be used as a starting point for further investigation.

3. *Internal structure*

The website needs to be able to search and access a large amount of information. It uses a fairly standard architecture: data is stored in a MySQL database and web pages are generated by programs written in Perl.

A MySQL database consists of a collection of tables, where each table is analogous to a single spreadsheet with columns representing the types of data being stored. We use data types for integers, floating point numbers, and strings, all of which come in various sizes, that is, amount of memory devoted to a single entry. When searching, one can use equalities and inequalities where strings are ordered lexicographically.

https://doi.org/10.1112/S1461157014000424 Published online by Cambridge University Press

When a user requests number fields, the Perl program takes the following steps.

(1) Construct and execute a MySQL query to pull fields from the database.
(2) Filter out fields which satisfy all of the user's requirements when needed (see below).
(3) Check completeness results known to the database.
(4) Generate the output web page.

The main MySQL table has one row for each field. There are columns for each piece of information indicated by the input boxes in the top portion of the search screen, plus columns for the defining polynomial (as a string), and an internal identifier for the field. The only unusual aspect of this portion of the database is how discriminants are stored and searched. The difficulty stems from the fact that many number fields in the database have discriminants which are too large to store in MySQL as integers. An option would be to store the discriminants as strings, but then it would be difficult to search for ranges: string comparisons in MySQL are lexicographic, so '11' comes before '4'. Our solution is to store absolute discriminants $|D|$ as strings, but prepend the string with four digits which give $\lfloor \log_{10}(|D|) \rfloor$, padded on the left with zeros as needed. So, 4 is stored as '00004', 11 is '000111', etc. In this way we can use strings to store each discriminant in its entirety, but searches for ranges work correctly.

The MySQL table of number fields also has a column for the list of all primes which ramify in the field, stored as a string with a separator between primes. This is used to accelerate searches when it is clear from the search criteria that only a small finite list of possibilities can occur, for example when the user has checked the box that 'Only listed primes can ramify'.

Information on ramification of specific primes can be input in the bottom half of the search inputs. To aid in searches involving these inputs, we have a second MySQL table, the ramification table, which stores a list of triples. A triple (field identifier, p, e) indicates that p^e exactly divides the discriminant of the corresponding field. The most common inputs to the bottom half of the search page work well with this table, namely those which list specific primes and allowable discriminant exponents. However, the search boxes allow much more general inputs, that is, where a range of values is allowed for the prime and the discriminant exponent allows both 0 and positive values. It is possible to construct MySQL queries for inputs of this sort, but they are complicated, involve subqueries, and are relatively slow. Moreover, a search condition of this type typically rules out relatively few number fields. If a user does make such a query, we do not use the information at this stage. Instead, we invoke Step (2) above to select fields from the MySQL query which satisfy these additional requirements.

The database supports a variety of different types of completeness results. Complicating matters is that these results can be interrelated. We use four MySQL tables for storing ways in which the data is complete. In describing them, G denotes the Galois group of a field, n is the degree, s is the number of complex places, and $|D|$ is the absolute discriminant, as above. The tables are:

(A) store (n, s, B) to indicate that the database is complete for fields with the given n and s such that $|D| \leqslant B$;
(B) store (n, s, G, B) to indicate that the database is complete for fields with the given n, s, and G such that $|D| \leqslant B$;
(C) store (n, S, L), where S is a list of primes and L is a list of Galois groups, to indicate that the database is complete for degree-n fields unramified outside S for each Galois group in L;
(D) store (n, G, B) to indicate that the database is complete for degree-n fields K with Galois group G such that $\mathrm{grd}(K) \leqslant B$.

In each case, database entries include the degree, so individual Galois groups can be stored by their T-number (a small integer). In the third case, we store the list L by an integer whose bits indicate which T-numbers are included in the set. For example, there are 50 T-numbers in degree 8, so a list of Galois groups in that degree is a subset of $S \subseteq \{1, \ldots, 50\}$, which we

https://doi.org/10.1112/S1461157014000424 Published online by Cambridge University Press

represent by the integer $\sum_{t\in S} 2^{t-1}$. These integers are too large to store in the database as integers, so they are stored as strings and converted to multiprecision integers in Perl. The list of primes in the third table is simply stored as a string consisting of the primes and separating characters.

To start checking for completeness, we first check that there are only finitely many degrees involved, and that the search request contains an upper bound on at least one of: $|D|$, $\mathrm{rd}(K)$, $\mathrm{grd}(K)$, or the largest ramifying prime. We then loop over the degrees in the user's search. We allow for the possibility that a search is known to be complete by some combination of completeness criteria. So, throughout the check, we maintain a list of Galois groups which need to be checked, and the discriminant values to check. If one check shows that some of the Galois groups for the search are known to be complete, they are removed from the list. If that list drops to being empty, then the search in that degree is known to be complete. Discriminant values are treated analogously.

For each degree, bounds on $|D|$ and $\mathrm{rd}(K)$ are clearly equivalent. Less obviously, bounds between $\mathrm{rd}(K)$ and $\mathrm{grd}(K)$ are related. In particular, we always have $\mathrm{rd}(K) \leqslant \mathrm{grd}(K)$, but also have, for each Galois group, $\mathrm{grd}(K) \leqslant \mathrm{rd}(K)^{\alpha(G)}$, where $\alpha(G)$ is a rational number depending only on G (see [**23**]).

We then perform the following checks.

- We compare the request with Tables A, B, and D for discriminant bound restrictions.
- Remove Galois groups from the list to be checked based on grd.
- If there are at most ten discriminants not accounted for, check each individually against Table C.
- If there is a bound on the set of ramifying primes, which could arise from the user checking 'Only these primes ramify', or from a bound on the maximum ramifying prime, check Table C.

4. *Summarizing tables*

The tables of this section summarize all fields in the database of degree less than or equal to eleven. Numbers in tables which are known to be correct are given in regular type. Numbers which are merely the bounds which come from perhaps incomplete lists of fields are given in italics. The table has a line for each group nTj, sorted by degree n and the index j. A more descriptive name is given in the second column.

The next four columns represent a main focus of the database, complete lists of fields ramified within a given set of primes. As a matter of notation, we write for example $\mathcal{K}(G, -^*p^*q^*)$ to denote the union of all $\mathcal{K}(G, -^s p^a q^b)$. The database contains completeness results for many other prime combinations beyond those given in the table; §§ 5–8 give examples of these further completeness results.

Degree 2									
T	G	$\{2,3\}$	$\{2,5\}$	$\{3,5\}$	$\{2,3,5\}$	$\mathrm{rd}(K)$	$\mathrm{grd}(K)$	$\lvert\mathcal{K}[G,\Omega]\rvert$	Tot
1	2	7	7	3	15	1.73	1.73	1220	1 216 009

Degree 3									
T	G	$\{2,3\}$	$\{2,5\}$	$\{3,5\}$	$\{2,3,5\}$	$\mathrm{rd}(K)$	$\mathrm{grd}(K)$	$\lvert\mathcal{K}[G,\Omega]\rvert$	Tot
1	3	1	0	1	1	3.66	3.66	47	1015
2	S_3	8	1	5	31	2.84	4.80	610	856 522

https://doi.org/10.1112/S1461157014000424 Published online by Cambridge University Press

Degree 4

T	G	$\{2,3\}$	$\{2,5\}$	$\{3,5\}$	$\{2,3,5\}$	$\mathrm{rd}(K)$	$\mathrm{grd}(K)$	$\lvert\mathcal{K}[G,\Omega]\rvert$	Tot
1	4	4	12	2	24	3.34	3.34	228	10 078
2	2^2	7	7	1	35	3.46	3.46	2421	52 559
3	D_4	28	24	0	176	3.29	6.03	2850	1 228 701
4	A_4	1	0	0	1	7.48	10.35	59	28 786
5	S_4	22	3	1	143	3.89	13.56	527	720 093

Degree 5

T	G	$\{2,3\}$	$\{2,5\}$	$\{3,5\}$	$\{2,3,5\}$	$\mathrm{rd}(K)$	$\mathrm{grd}(K)$	$\lvert\mathcal{K}[G,\Omega]\rvert$	Tot
1	5	0	1	1	1	6.81	6.81	7	181
2	D_5	0	4	2	8	4.66	6.86	146	11 595
3	F_5	1	19	7	82	8.11	11.08	102	1646
4	A_5	0	5	6	62	7.14	18.70	78	98 138
5	S_5	5	38	22	1353	4.38	24.18	192	898 183

Degree 6

T	G	$\{2,3\}$	$\{2,5\}$	$\{3,5\}$	$\{2,3,5\}$	$\mathrm{rd}(K)$	$\mathrm{grd}(K)$	$\lvert\mathcal{K}[G,\Omega]\rvert$	Tot
1	6	7	0	3	15	5.06	5.06	399	5291
2	S_3	8	1	5	31	4.80	4.80	610	8353
3	D_6	48	6	10	434	4.93	8.06	3590	149 303
4	A_4	1	0	0	1	7.32	10.35	59	5219
5	$3 \wr 2$	8	0	5	31	4.62	10.06	254	8207
6	$2 \wr 3$	7	0	0	15	5.61	12.31	243	176 809
7	S_4^+	22	3	1	143	5.69	13.56	527	242 007
8	S_4	22	3	1	143	6.63	13.56	527	43 944
9	S_3^2	22	0	4	375	7.89	15.53	445	49 242
10	$3^2:4$	4	0	2	44	8.98	23.57	34	829
11	$2 \wr S_3$	132	18	2	2002	4.65	16.13	2196	367 901
12	$\mathrm{PSL}_2(5)$	0	5	6	62	8.12	18.70	78	96 742
13	$3^2:D_4$	50	0	0	624	4.76	21.76	274	236 136
14	$\mathrm{PGL}_2(5)$	5	38	22	1353	11.01	24.18	192	898 183
15	A_6	8	2	4	*540*	8.12	31.66	10	901
16	S_6	54	30	42	*8334*	4.95	33.50	26	301 802

Degree 7

T	G	$\{2,3\}$	$\{2,5\}$	$\{3,5\}$	$\{2,3,5\}$	$\mathrm{rd}(K)$	$\mathrm{grd}(K)$	$\lvert\mathcal{K}[G,\Omega]\rvert$	Tot
1	7	0	0	0	0	17.93	17.93	4	117
2	D_7	0	0	0	0	6.21	8.43	80	496
3	$7:3$	0	0	0	0	21.03	31.64	2	56
4	$7:6$	0	0	1	5	12.10	15.99	94	189
5	$\mathrm{SL}_3(2)$	0	0	0		7.95	32.25	*36*	618
6	A_7	0	2	3	*204*	8.74	39.52	*1*	332
7	S_7	10	24	14	*4391*	5.65	*40.49*	*1*	13 827

https://doi.org/10.1112/S1461157014000424 Published online by Cambridge University Press

Degree 8									
T	G	$\{2,3\}$	$\{2,5\}$	$\{3,5\}$	$\{2,3,5\}$	rd(K)	grd(K)	$\lvert\mathcal{K}[G,\Omega]\rvert$	Tot
1	8	4	8	0	16	11.93	11.93	23	5817
2	4×2	6	18	1	84	5.79	5.79	581	15 523
3	2^3	1	1	0	15	6.93	6.93	908	10 687
4	D_4	14	12	0	88	6.03	6.03	1425	24 458
5	Q_8	2	0	0	8	18.24	18.24	7	788
6	D_8	20	20	0	104	6.71	9.75	708	29 794
7	$8:\{1,5\}$	6	20	1	88	9.32	9.32	55	8088
8	$8:\{1,3\}$	22	10	0	120	10.09	10.46	121	10 845
9	$D_4\times 2$	28	24	0	528	6.51	10.58	5908	175 572
10	$2^2:4$	8	24	0	160	6.09	9.46	620	29 745
11	$Q_8:2$	18	18	0	312	6.51	9.80	921	17 350
12	$\mathrm{SL}_2(3)$	0	0	0	0	12.77	29.84	4	681
13	$A_4\times 2$	7	0	0	15	8.06	12.31	243	26 637
14	S_4	22	3	1	143	9.40	13.56	527	7203
15	$8:8^\times$	42	42	0	928	8.65	13.79	818	60 490
16	$1/2[2^4]4$	8	24	0	176	7.45	13.56	76	15 571
17	$4\wr 2$	16	72	0	480	5.79	13.37	252	42 156
18	$2^2\wr 2$	24	8	0	608	7.04	16.40	2544	216 411
19	$E(8):4$	8	24	0	192	9.51	14.05	220	24 440
20	$[2^3]4$	4	12	0	96	8.46	14.05	110	13 661
21	$1/2[2^4]E(4)$	4	12	0	96	8.72	14.05	110	10 121
22	$E(8):D_4$	0	0	0	204	8.43	18.42	882	19 733
23	$\mathrm{GL}_2(3)$	128	24	4	912	8.31	16.52	388	6304
24	$S_4\times 2$	132	18	2	2002	6.04	16.13	2196	45 996
25	$2^3:7$	0	0	0	0	12.50	17.93	1	20
26	$1/2[2^4]eD(4)$	64	24	0	1872	7.23	20.37	840	135 840
27	$2\wr 4$	16	48	0	448	5.95	19.44	160	86 547
28	$1/2[2^4]dD(4)$	16	48	0	448	8.67	19.44	160	47 196
29	$E(8):D_8$	48	24	0	1296	6.58	19.41	1374	170 694
30	$1/2[2^4]cD(4)$	16	48	0	448	8.25	19.44	140	48 317
31	$2\wr 2^2$	16	8	0	432	5.92	19.41	458	54 843
32	$[2^3]A_4$	0	0	0	0	13.56	34.97	24	29 970
33	$E(8):A_4$	6	0	0	14	13.73	30.01	24	3240
34	$E(4)^2:D_6$	11	1	0	132	14.16	27.28	55	3907
35	$2\wr D(4)$	168	72	0	5568	5.83	22.91	1464	729 730
36	$2^3:7:3$	0	0	0	0	14.37	31.64	4	298
37	$\mathrm{PSL}_2(7)$	0	0			*21.00*	32.25	*18*	352
38	$2\wr A_4$	24	0	0	112	10.66	37.27	46	67 160
39	$[2^3]S_4$	168	24	0	2496	6.73	32.35	84	24 625
40	$1/2[2^4]S(4)$	216	24	0	3872	7.67	29.71	98	12 796
41	$E(8):S_4$	90	12	0	2282	8.38	28.11	222	11 950
42	$A_4\wr 2$	12	0	0	83	7.68	32.18	14	3550
43	$\mathrm{PGL}_2(7)$	*4*			*8*	*11.96*	*27.35*	*27*	1495
44	$2\wr S_4$	656	96	0	22944	5.84	31.38	336	440 683
45	$[1/2.S_4^2]2$	110	0	0	*836*	9.28	29.35	39	8028
46	$1/2[S(4)^2]2$	28	0	0	*54*	11.35	49.75	0	224
47	$S_4\wr 2$	542	0	0	*2185*	5.83	35.05	15	262 530
48	$2^3:\mathrm{SL}_3(2)$	0	0			*11.36*	*39.54*	*6*	495
49	A_8	*2*	*4*	*1*	*55*	*15.24*	*72.03*		90
50	S_8	*72*	*30*	*9*	*1728*	*11.33*	*43.99*	*1*	4026

https://doi.org/10.1112/S1461157014000424 Published online by Cambridge University Press

Degree 9										
T	G	$\{2,3\}$	$\{2,5\}$	$\{3,5\}$	$\{2,3,5\}$	$\mathrm{rd}(K)$	$\mathrm{grd}(K)$	$\lvert\mathcal{K}[G,\Omega]\rvert$	Tot
1	9	1	0	1	1	13.70	13.70	3	52
2	3^2	0	0	0	0	15.83	15.83	9	189
3	D_9	6	0	4	20	9.72	12.19	105	705
4	$S_3 \times 3$	8	0	5	31	8.38	10.06	254	10 139
5	$3^2:2$	1	0	1	15	14.29	15.19	48	373
6	$1/3[3^3]3$	0	0	0	0	17.63	31.18	2	85
7	$3^2:3$	0	0	0	0	26.09	50.20	0	90
8	$S_3 \times S_3$	22	0	4	375	8.93	15.53	445	7055
9	$E(9):4$	2	0	1	22	19.92	23.57	17	142
10	$[3^2]S(3)_6$	22	0	17	171	9.57	17.01	69	1066
11	$E(9):6$	6	0	4	20	14.67	16.83	64	880
12	$[3^2]S(3)$	12	0	12	180	8.92	16.72	148	13 929
13	$E(9):D_6$	6	0	4	20	10.98	16.83	64	642
14	$3^2:Q_8$	4	0	0	19	21.52	29.72	2	47
15	$E(9):8$	5	1	0	18	17.74	25.41	3	40
16	$E(9):D_8$	25	0	0	312	9.19	21.76	137	434
17	$3 \wr 3$	0	0	0	0	14.93	75.41	0	1274
18	$E(9):D_{12}$	80	0	8	1380	8.53	22.06	290	9260
19	$E(9):2D_8$	60	1	0	*124*	17.89	23.41	33	624
20	$3 \wr S_3$	18	0	12	60	7.83	29.89	30	7989
21	$1/2.[3^3:2]S_3$	54	0	54	1296	9.82	24.90	126	4282
22	$[3^3:2]3$	18	0	12	60	10.27	26.46	51	784
23	$E(9):2A_4$	0	0	0	0	16.48	49.57	0	40
24	$[3^3:2]S(3)$	321	0	48	8307	9.15	30.64	111	17 973
25	$[1/2.S(3)^3]3$	4	0	0	4	12.89	29.96	4	303
26	$E(9):2S_4$	250	2	10	*362*	12.79	27.88	51	866
27	$\mathrm{PSL}_2(8)$	*4*			*4*	*16.25*	*30.31*	*15*	19
28	$S_3 \wr 3$	28	0	0	90	8.18	33.56	7	6738
29	$[1/2.S(3)^3]S(3)$	45	0	1	512	9.38	40.81	2	1255
30	$1/2[S(3)^3]S(3)$	232	1	40	*1637*	6.86	30.37	35	5026
31	$S_3 \wr S_3$	616	0	5	19 865	6.83	36.26	15	112 887
32	$\Sigma L_2(8)$	*64*			*240*	*16.09*	*34.36*	*15*	1141
33	A_9	*13*		*2*	*314*	*14.17*	*62.12*		627
34	S_9	*46*	*1*	*1*	*1507*	*7.84*	*53.19*		3189

https://doi.org/10.1112/S1461157014000424 Published online by Cambridge University Press

Degree 10									
T	G	$\{2,3\}$	$\{2,5\}$	$\{3,5\}$	$\{2,3,5\}$	$\mathrm{rd}(K)$	$\mathrm{grd}(K)$	$\lvert\mathcal{K}[G,\Omega]\rvert$	Tot
1	10	0	7	3	15	8.65	8.65	69	360
2	D_5	0	4	2	8	6.86	6.86	146	822
3	D_{10}	0	24	4	112	8.08	10.91	768	857
4	$1/2[F(5)]2$	1	19	7	82	10.23	11.08	102	698
5	$F_5 \times 2$	6	114	14	1148	9.48	14.50	584	1611
6	$[5^2]2$	0	8	4	16	6.84	18.02	32	175
7	A_5	0	5	6	62	12.35	18.70	78	1417
8	$[2^4]5$	0	3	0	3	12.75	24.98	18	36
9	$[1/2.D(5)^2]2$	0	12	2	56	*12.71*	24.72	34	87
10	$1/2[D(5)^2]2$	0	22	12	126	*14.02*	24.00	22	144
11	$A_5 \times 2$	0	35	18	930	9.42	22.24	179	1177
12	$S_5(10a)$	5	38	22	1353	12.04	24.18	192	1560
13	$S_5(10d)$	5	38	22	1353	9.16	24.18	192	2083
14	$2 \wr 5$	0	21	0	45	9.32	26.08	45	2050
15	$[2^4]D(5)$	0	60	0	360	9.33	25.15	72	620
16	$1/2[2^5]D(5)$	0	60	0	360	9.46	25.15	72	509
17	$[5^2:4]2$	0	65	0	922	*17.46*	26.65	34	1100
18	$[5^2:4]2_2$	0	*16*	0	*17*	*19.75*	35.98	3	22
19	$[5^2:4_2]2$	0	17	0	*63*	*16.96*	28.08	18	111
20	$[5^2:4_2]2_2$	0	0	0	*31*	*27.36*	48.25	0	43
21	$D_5 \wr 2$	0	34	0	*118*	7.54	28.08	36	235
22	$S_5 \times 2$	30	228	44	18 942	7.06	26.99	570	26 851
23	$2 \wr D_5$	0	360	0	5040	7.26	26.26	240	24 024
24	$[2^4]F(5)$	7	173	0	1250	14.13	27.62	30	1491
25	$1/2[2^5]F(5)$	7	173	0	1250	13.84	27.62	30	1491
26	$\mathrm{PSL}_2(9)$	4	1	2	*270*	20.20	31.66	5	334
27	$[1/2.F_5^2]2$	0	*56*	0	*652*	*13.40*	40.43	18	1052
28	$1/2[F_5^2]2$	*1*	*37*	*2*	*70*	*15.16*	*32.71*	*8*	72
29	$2 \wr F_5$	42	1038	0	17 500	11.44	32.17	90	19 112
30	$\mathrm{PGL}_2(9)$	*11*	*5*	*1*	*55*	*22.64*	*34.42*	*6*	149
31	M_{10}	*20*	*4*	*13*	*83*	*27.73*	*53.50*		198
32	S_6	27	15	21	*4166*	*14.74*	33.50	13	6913
33	$F_5 \wr 2$	0	*177*	0	*484*	9.93	*35.41*	*3*	485
34	$[2^4]A_5$	0	35	0	1322	10.82	35.81	5	1388
35	$\mathrm{P\Gamma L}_2(9)$	*100*	*32*	*15*	*1666*	*17.98*	*38.61*	*15*	3531
36	$2 \wr A_5$	0	245	0	19 830	10.39	36.60	8	20 660
37	$[2^4]S_5$	91	450	8	42 059	7.80	38.11	17	60 029
38	$1/2[2^5]S_5$	91	450	8	42 059	9.41	38.11	17	42 851
39	$2 \wr S_5$	546	2700	16	588 826	6.79	38.11	30	1 095 840
40	$A_5 \wr 2$	*12*	*68*	*29*	*1098*	9.48	*41.90*	*1*	1129
41	$[A_5:2]2$	*28*	*148*	*11*	*9444*	9.30	*43.89*	*1*	9686
42	$1/2[S_5^2]2$	*18*	*84*	*31*	*866*	*14.35*	*45.93*		898
43	$S_5 \wr 2$	*185*	*471*		*20 792*	6.82	*48.97*		31 896
44	A_{10}	*23*	*16*	*6*	*801*	*19.37*	*51.68*		1201
45	S_{10}	*1*	*12*	*3*	*2585*	*7.77*	*70.36*		4944

https://doi.org/10.1112/S1461157014000424 Published online by Cambridge University Press

Degree 11									
T	G	$\{2,3\}$	$\{2,5\}$	$\{3,5\}$	$\{2,3,5\}$	$\mathrm{rd}(K)$	$\mathrm{grd}(K)$	$\lvert\mathcal{K}[G,\Omega]\rvert$	Tot
1	11	0	0	0	0	17.30	17.30	1	18
2	D_{11}	0	0	0	0	10.24	12.92	32	55
3	$11:5$	0	0	0	0	*88.82*	*105.74*	0	2
4	$11:10$					*17.01*	20.70	*4*	56
5	$\mathrm{PSL}_2(11)$					*15.36*	*42.79*	*2*	91
6	M_{11}				*1*	*96.24*	*270.83*		10
7	A_{11}				*4*	*21.15*	*146.24*		71
8	S_{11}	*5*	*4*	*1*	*123*	*7.72*	*91.50*		931

The next column gives minimal values of root discriminants. More refined minima can easily be obtained from the database. For example, for S_5, minimal discriminants for $s = 0$, 1, and 2 complex places are respectively $(61 \cdot 131)^{1/5} \approx 7.53$, $(13 \cdot 347)^{1/5} \approx 5.38$, and $1609^{1/5} \approx 4.38$. Completeness is typically known well past the minimum.

In understanding root discriminants, the Serre–Odlyzko constant $\Omega = 8\pi e^{\gamma} \approx 44.76$ mentioned in the introduction plays an important role, as follows. First, if K has root discriminant $< \Omega/2$, then its maximal unramified extension K' has finite degree over K. Second, if $\mathrm{rd}(K) < \Omega$, then the GRH implies the same conclusion $[K' : K] < \infty$. Third, suggesting that there is a modestly sharp qualitative transition associated with Ω, the field $\mathbb{Q}(e^{2\pi i/81})$ with root discriminant $3^{3.5} \approx 46.77$ has $[K' : K] = \infty$ by [**14**].

The next two columns of the tables again represent a main focus of the database, complete lists of fields with small Galois root discriminant. We write $\mathcal{K}[G, B]$ for the set of all fields with Galois group G and $\mathrm{grd}(K) \leqslant B$. The tables give first the minimal Galois root discriminant. They next give $|\mathcal{K}[G, \Omega]|$. For many groups, the database is complete for cutoffs well past Ω. For example, the set $\mathcal{K}[9T17, \Omega]$ is empty and not adequate for the purposes of [**17**]. However, the database identifies $|\mathcal{K}[9T17, 200]| = 36$ and this result is adequate for the application.

The last column in a table gives the total number of fields in the database for the given group. Over time, the number of fields in the database will increase as results from new searches are added. Note that one could easily make this number much larger in any case. For example, a regular family over $\mathbb{Q}(t)$ for each group is given in [**28**, Appendix 1], and one could simply specialize at many rational numbers t. However, we do not do this: all the fields in our database are there only because discriminants met one criterion or another for being small. The fluctuations in this column should not be viewed as significant, as the criteria depend on the group in ways driven erratically by applications.

There are a number of patterns in the summarizing tables which hold because of relations between transitive groups. For example, the groups $5T4 = A_5$, $6T12 = \mathrm{PSL}_2(5)$, and $10T7$ are all isomorphic. Most of the corresponding lines necessarily agree. Similarly, A_5 is a quotient of $10T11$, $10T34$, and $10T36$. Thus, the fact that $\mathcal{K}(A_5, -^*2^*3^*) = \emptyset$ immediately implies that also $\mathcal{K}(10Tj, -^*2^*3^*) = \emptyset$ for $j \in \{11, 34, 36\}$.

Almost all fields in the database come from complete searches of number fields carried out by the authors. In a few cases, we obtained polynomials from other sources, notably for number fields of small discriminant: those compiled by the Bordeaux group [**7**], which in turn were computed by several authors, and the tables of totally real fields of Voight [**39**, **40**]. In addition, we include fields found by the authors in joint work with others [**13**, **24**].

To compute cubic fields, we used the program of Belabas [**1**, **2**]. Otherwise, we obtained complete lists by using traditional and targeted Hunter searches [**18**, **19**] or the class field

https://doi.org/10.1112/S1461157014000424 Published online by Cambridge University Press

theory functions in Pari/gp [38]. For larger nonsolvable groups where completeness results are currently out of reach, we obtained most of our fields by specializations of families at carefully chosen points to keep ramification small in various senses.

5. S_5 *quintics with discriminant* $-^s2^a3^b5^c7^d$

One of our longest searches determined $\mathcal{K}(S_5, -^*2^*3^*5^*7^*)$, finding it to consist of 11 279 fields. In this section, we consider how this set interacts with mass heuristics.

In general, mass heuristics [5, 27] give one expectations as to the sizes $|\mathcal{K}(G, D)|$ of the sets contained in the database. Here we consider these heuristics only in the most studied case $G = S_n$. The mass of a $\mathbb{Q}_v$-algebra K_v is by definition $1/|\mathrm{Aut}(K_v)|$. Thus, the mass of $\mathbb{R}^{n-2s}\mathbb{C}^s$ is

$$\mu_{n,-^s} = \frac{1}{(n-2s)!s!2^s}. \tag{5.1}$$

For p a prime, similarly let μ_{n,p^c} be the total mass of all p-adic algebras with degree n and discriminant p^c. For $n < p$, all algebras involved are tame and

$$\mu_{n,p^c} = |\{\text{Partitions of } n \text{ having } n-c \text{ parts}\}|. \tag{5.2}$$

For $n \geqslant p$, wild algebras are involved. General formulas for μ_{n,p^c} are given in [34].

The mass heuristic says that if the discriminant $D = -^s \prod_p p^{c_p}$ in question is a nonsquare, then

$$\left|\mathcal{K}\left(S_n, -^s \prod_p p^{c_p}\right)\right| \approx \delta_n \mu_{n,-^s} \prod_p \mu_{n,p^{c_p}}. \tag{5.3}$$

Here $\delta_n = 1/2$, except for the special cases $\delta_1 = \delta_2 = 1$, which require adjustment for simple reasons. The left-hand side is an integer and the right-hand side is often close to zero because of (5.1) and (5.2). So, (5.3) is intended only to be used in suitable averages.

For $n \leqslant 5$ fixed and $|D| \to \infty$, the heuristics are exactly right on average, the case $n = 3$ being the Davenport–Heilbronn theorem and the cases $n = 4$ and 5 more recent results of Bhargava [4, 6]. For a fixed set of ramifying primes S and $n \to \infty$, the mass heuristic predicts no fields after a fairly sharp cutoff $N(S)$, while in fact there can be many fields in degrees well past this cutoff [33]. Thus, the regime of applicability of the mass heuristic is not clear.

To get a better understanding of this regime, it is of interest to consider other limits. Let μ_{n,p^*} be the total mass of all $\mathbb{Q}_p$-algebras of degree n. Thus, μ_{n,p^*} is the number of partitions of n if $n < p$. Then, for $k \to \infty$, the mass heuristic predicts the asymptotic equivalence

$$|\mathcal{K}(S_n, -^*2^* \dots p_k^*\})| \sim \delta_n \mu_{n,-^*} \prod_{j=1}^{k} \mu_{n,p^*}. \tag{5.4}$$

Both sides of (5.4) are 1 for all k when $n = 1$. For $n = 2$ and $k \geqslant 1$, the statement becomes $2^{k+1} - 1 \sim 2^{k+1}$, which is true. Using the fields in the database as a starting point, we have carried out substantial calculations suggesting that, after removing fields with discriminants of the form $-3u^2$ from the count on the left, (5.4) holds also for $n = 3$ and $n = 4$.

In this section, we focus on the first nonsolvable case, $n = 5$. For $k \geqslant 3$, (5.4) becomes

$$|\mathcal{K}(S_5, -^*2^* \dots p_k^*)| \sim \tfrac{1}{2} \cdot \tfrac{26}{120} \cdot 40 \cdot 19 \cdot 27 \cdot 7^{k-3} \approx 6.48 \cdot 7^k. \tag{5.5}$$

Through the cutoff $k = 4$, there are fewer fields than predicted by the mass heuristic:

p_k	2	3	5	7
$\lvert\mathcal{K}(S_5, -^*2^* \dots p_k^*)\rvert$	0	5	1353	11 279
	0%	6%	61%	72%

https://doi.org/10.1112/S1461157014000424 Published online by Cambridge University Press

TABLE 5.1. *Local masses* $120\mu_{5,-^c}$ *and* μ_{5,p^c}*, compared with frequencies of local discriminants from* $\mathcal{K}(S_5, -^*2^*3^*5^*7^*)$.

$v \setminus c$	0	1	2	3	4	5	6	7	8	9	10	11	Total
∞	1	10	15										26
	0.71	9.52	15.77										
2	1		2	2	5	4	6		4	4	4	8	40
	0.73		1.66	1.48	4.71	3.83	5.66		4.47	4.37	4.15	8.94	
3	1	1	1	3	5	5	3						19
	0.76	0.85	0.78	2.89	5.24	5.13	3.43						
5	1	1	2	2		4	4	4	4	5			27
	0.37	0.39	0.96	1.32		4.07	4.17	4.70	4.65	6.38			
7	1	1	2	2	1								7
	0.84	0.88	1.92	2.12	1.24								

For comparison, the ratio $11\,279/(6.48 \cdot 7^4) \approx 72\%$ is actually larger than the ratios at $k = 4$ for cubic and quartic fields with discriminant $-3u^2$ removed, these being respectively $64/(1.33 \cdot 3^4) \approx 47\%$ and $740/(3.30 \cdot 5^k) \approx 36\%$. As remarked above, these other cases experimentally approach 100% as k increases. This experimental finding lets one reasonably argue that (5.5) may hold too, with the small percentage 72% being a consequence of a small discriminant effect.

Table 5.1 compares local masses with frequencies of actually occurring local discriminants, inflated by the ratio $(6.58 \cdot 7^4)/11\,279$ to facilitate direct comparison. Thus, for example, the 7-adic discriminants $(7^0, 7^1, 7^2, 7^3, 7^4)$ are predicted by the mass heuristic to occur with relatively frequency $(1, 1, 2, 2, 1)$. They actually occur with relative frequency $(0.84, 0.88, 1.92, 2.12, 1.24)$. Here and for the other four places, trends away from the predicted asymptotic values are explained by consistent under-representation of fields with small discriminant. The consistency of the data with the mass heuristic on this refined level provides further support for (5.5).

6. *Low-degree nonsolvable fields with discriminant* $-^s p^a q^b$

Our earliest contributions to the general subject of number field tabulation were [**18**] and [**19**]. These papers respectively found that there are exactly 398 sextic and 10 septic fields with discriminant of the form $-^s2^a3^b$. In the lists from these papers, the nonsolvable groups $\mathrm{PSL}_2(5) \cong A_5$, $\mathrm{PGL}_2(5) \cong S_5$, A_6, S_6 and $\mathrm{SL}_3(2)$, A_7, S_7 respectively arise zero, five, eight, 54 and zero, zero, ten times. In this section, we summarize further results from the database of this form, identifying or providing lower bounds for $|\mathcal{K}(G, -^*p^*q^*)|$.

The format of our tables exploits the fact that in the range considered for a given group, there are no fields ramified at one prime only. In fact [**22**], the smallest prime p for which $\mathcal{K}(G, -^*p^*)$ is nonempty is as follows:

G	A_5	S_5	A_6	S_6	$\mathrm{SL}_3(2)$	A_7	S_7	$\mathrm{PGL}_2(7)$
p	653	101	1579	197	227	>227	191	53

Here $7T5 = \mathrm{SL}_3(2)$ is abstractly isomorphic to $8T37 = \mathrm{PSL}_2(7)$ and thus has index two in $8T43 = \mathrm{PGL}_2(7)$.

TABLE 6.1. $|\mathcal{K}(A_5, -^*p^*q^*)|$ *beneath the diagonal and* $|\mathcal{K}(S_5, -^*p^*q^*)|$ *above the diagonal. It is expected that* A_5 *totals are smaller for primes* $p \equiv 2, 3$ (5) *because in this case* p^4 *is not a possible local discriminant.*

	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97	T
2	•	5	38	2	2	4	3	2	5	6	3	6	9	14	10	11	8	13	13	8	5	11	10	13	4	205
3		•	22				1	4			1	2	2	6	3	5	3	3	2	8	3	2	4	3	2	81
5	5	6	•	4	5	9	12	8	8	8	9	13	12	11	8	14	8	15	13	14	9	14	11	11	14	290
7				•	1				1	2			2	2					1	3		1		1		20
11		2			•			1	1			1		1	1		1			1	1		1	1		18
13			1			•		1		2		3	2		1						1			1	1	25
17	1	1					•	1		3		3	4	1		1	1			1	2			1	3	37
19	1	3						•	2		3		1		1	1	1	1	3	2		1	1		2	36
23		1							•	1		1		2			1	1					2	1	2	28
29	2	3				1	2		2	•		2	3	1	1		2	3	3	1	4	2		2	2	48
31	1	3	1			2	1				•	1		4	1			2	2	1			2		1	30
37			1									•	2	3		2	2	2				3	4	1	1	52
41	2	2	2				1	1	1				•	1		2		3		1	1	2	1	3	5	56
43	1	3	1		1								1	•			2	1	1	2	2	4	1	2		61
47															•	1	4		3			1	3			38
53			2		1				1							•	3	3		1	2	1	3	2		52
59	1	3	2			1	2				1						•			1	1	2	1	3	1	45
61	1	1					1			1		1	1					•	2	3	2	1			1	56
67	2	1	1												1				•	4		2	2	1	2	54
71	1	2	1					1		1	4	2					2	1		•		4	1	3		59
73	1		1	1						1			2	1	1			1			•			2	3	38
79	4	4	2			1		2					3			1	1					•		2	1	54
83		1														1			1			2	•	4		51
89	1	3	2							1	1	1	2			2		1	1	1		2		•	1	58
97		1				1							1				1		1			1		1	•	46
T	24	40	28	1	4	7	9	8	5	14	14	5	19	8	2	8	14	9	8	16	9	23	5	19	7	

Restricting to the six groups G of the form A_n or S_n, our results on $|\mathcal{K}(G, -^*p^*q^*)|$ compare with the mass heuristic as follows. First, local masses μ_{n,v^*} are given in the middle six columns:

n	∞	2	3	5	7	Tame	μ
5	26/120	40	19	27		7	5.31
6	76/720	145	83	31		11	6.39
7	232/5040	180	99	55	57	15	5.18

(6.1)

The column μ contains the global mass $0.5\mu_{n,-^*}\mu_{n,p^*}\mu_{n,q^*}$ for two tame primes p and q. When one or both of the primes are wild, the corresponding global mass is substantially larger.

Tables 6.1, 6.2, and 6.3 clearly show that there tend to be more fields when one or more of the primes p, q allow wild ramification, as one would expect from (6.1). To make plausible conjectures about the asymptotic behavior of the numbers $|\mathcal{K}(G, -^*p^*q^*)|$, one would have

https://doi.org/10.1112/S1461157014000424 Published online by Cambridge University Press

TABLE 6.2. *$|\mathcal{K}(A_6, -^*p^*q^*)|$ beneath the diagonal and $|\mathcal{K}(S_6, -^*p^*q^*)|$ above the diagonal. All entries are even because contributing fields come in twin pairs.*

	2	3	5	7	11	13	17	19	23	29	31	T
2	•	54	30			2	2	2	4	4	6	104
3	8	•	42		4		8		2	12	2	124
5	2	4	•	2	2	2		6	8	2	4	98
7		2		•								2
11					•							6
13		2				•						4
17			2				•		2			12
19		2				2		•				8
23	2	2							•			16
29		4						2		•		18
31	4	6								2	•	12
T	16	30	8	2		4	2	6	4	8	12	

TABLE 6.3. *Determinations or lower bounds for $|\mathcal{K}(G, -^*p^*q^*)|$ for four G. The entries $|\mathcal{K}(\mathrm{SL}_3(2), -^*p^*q^*)|$ are all even because contributing fields come in twin pairs.*

$\mathrm{SL}_3(2)$ and $\mathrm{PGL}_2(7)$						
	2	3	5	7	11	13
2	•	*4*	*0*	*51*	*0*	*0*
3	0	•	*0*	*28*	*0*	*0*
5	0	0	•	*4*	*0*	*0*
7	*44*	*12*	*4*	•	*4*	*6*
11	4	0	*0*	*6*	•	*0*
13	0	*0*	*0*	*0*	0	•

A_7 and S_7						
	2	3	5	7	11	13
2	•	10	24	*55*	0	0
3	0	•	14	*44*	2	*0*
5	2	3	•	*18*	*0*	*0*
7	*0*	*7*	*5*	•	*5*	*0*
11	0	0	*1*	*0*	•	0
13	0	*0*	*0*	*0*	0	•

to do more complicated local calculations than those summarized in (6.1). These calculations would have to take into account various secondary phenomena, such as the fact that s is forced to be even if $p \equiv q \equiv 1$ (4). Tables 6.1, 6.2, and 6.3 each reflect substantial computation, but the amount of evidence is too small to warrant making formal conjectures in this setting.

7. *Nilpotent octic fields with odd discriminant $-^s p^a q^b$*

The database has all octic fields with Galois group a 2-group and discriminant of the form $-^s p^a q^b$ with p and q odd primes $<$250. There are $\binom{52}{2} = 1326$ pairs $\{p, q\}$ and the average size of $\mathcal{K}(\mathrm{NilOct}, -^*p^*q^*)$ in this range is about 12.01. In comparison with the nonsolvable cases discussed in the previous two sections, there is much greater regularity in this setting. We exhibit some of the greater regularity and explain how it makes some of the abstract considerations of [**9**, **10**] more concrete.

https://doi.org/10.1112/S1461157014000424 Published online by Cambridge University Press

TABLE 7.1. *Nonzero cardinalities* $|\mathcal{K}(8Tj, -^*p^*q^*)|$ *for* $8Tj$ *an octic group of* 2*-power order.*

p	q	1	2	4	5	6	7	8	10	16	17	19	20	21	27	28	30	s_3	#	ν	T	s
3,7	3,7																			1/4		
7_2	3_1			1				1										4	193	1/8	○	4
11_2	7_1			1		2												4	185	1/8	•	⩾ 5
3,7	5																			1/4		
3_1	5_1		1				1											4	219	1/8	*i*	4
11_4	5_2		1	2					2	2	4							6	87	1/16	*ii*	6
19_2	5_2		1	2		2		1	2		2	2	1	1	2	2	4	7	86	1/16	*iii*	19
3,7	1																			1/4		
3_1	17_1	2	1															4	162	1/8		
19_2	17_2	2	1	2		2	1	1	2		2							6	66	1/16		
23_4	41_2	2	1	2		4	1	2	2	2	4	2	1	1	4	4	4	8	52	1/16		
5	5																			1/16		
5_1	13_1		3				2											5	42	1/32	*I*	6
5_2	29_2		3	3	1				6		8	4	2	2	4	4		9	11	1/128	*II*	27
13_4	53_4		3	3	1	2		2	6		8	12	6	6	12	12	16	11	13	1/128	*III*	⩾17
13_2	29_4		3	3	1				6	2	12	4	2	2	2	2	4	9	25	1/64	*IV*	⩾30
5	1																			1/8		
5_1	17_1	4	3															5	76	1/16		
13_4	17_2	4	3	3	1		2		6	2	8	4	2	2	4	4		9	17	1/64		
5_2	41_4	4	3	3	1		2		6		4	4	2	2	2	2	4	9	22	1/64		
53_2	17_2	4	3	3	1	2	2	2	6		12	4	2	2	2	2	4	9	18	1/64		
109_4	73_4	4	3	3	1	4	2	4	6	2	16	12	6	6	12	12	16	11	6	1/128		
101_4	97_4	4	3	3	1	4	2	4	6	2	16	12	6	6	16	16	24	12	1	1/128		
1	1																			1/16		
17_1	41_1	12	3															6	27	1/32		
41_4	73_2	12	3	3	1		6		6	2		4	2	2	4	4		9	12	1/64		
41_2	241_2	12	3	3	1	4	6	4	6	2	16	4	2	2	4	4	4	10	2	1/128		
73_4	89_4	12	3	3	1	6	6	6	6	6	24	12	6	6	16	16	16	12	2	1/256		
73_4	137_4	12	3	3	1	6	6	6	6	6	24	12	6	6	24	24	24	13	2	1/256		

https://doi.org/10.1112/S1461157014000424 Published online by Cambridge University Press

Twenty-six of the 50 octic groups have 2-power order. Table 7.1 presents the nonzero cardinalities, so that for example $|\mathcal{K}(8Tj, -^*5^*29^*)| = 4, 2, 2$ for $j = 19, 20, 21$. The repeated proportion $(2, 1, 1)$ for these groups and other similar patterns are due to the sibling phenomenon discussed in § 4. Only the sixteen 2-groups generated by two elements actually occur. Columns s_3, #, ν, T, and s are all explained later in this section.

The main phenomenon presented in Table 7.1 is that the multiplicities presented are highly repetitious, with for example the multiplicities presented for $(5, 29)$ occurring for altogether eleven pairs (p, q), as indicated in the # column. The repetition is even greater than indicated by the table itself. Namely, if (p_1, q_1) and (p_2, q_2) correspond to the same line, then not only are the numbers $\mathcal{K}(8Tj, -^*p_i^*q_i^*)$ independent of i, but the individual $\mathcal{K}(8Tj, -^*p_i^aq_i^b)$ and even further refinements are also independent of i.

The line corresponding to a given pair (p, q) is almost determined by elementary considerations, as follows. Let U be the order of q in $(\mathbb{Z}/p)^\times$ and let V be the order of p in $(\mathbb{Z}/q)^\times$. Let $u = \gcd(U, 4)$ and $v = \gcd(V, 4)$. Then all (p, q) on a given line have the same u, v, and a representative is written (p_u, q_v) in the leftmost two columns. Almost all lines are determined by their datum $\{[p]_u, [q]_v\}$, with $[\cdot]$ indicating reduction modulo eight. The only exceptions are $\{[p]_u, [q]_v\} = \{5_4, 1_4\}$ and $\{[p]_u, [q]_v\} = \{1_4, 1_4\}$, which have two lines each. The column headed by # gives the number of occurrences in our setting $p, q < 250$. In the five cases where this number is less than ten, we continued the computation up through $p, q < 500$ assuming the GRH. We expect that all possibilities are accounted for by the table, and they occur with asymptotic frequencies given in the column headed by ν. Assuming that these frequencies are correct, the average size of $\mathcal{K}(\mathrm{NilOct}, -^*p^*q^*)$ is exactly 15.875, substantially larger than the observed 12.01 in the $p, q < 250$ setting.

The connection with [**9**, **10**] is as follows. Let $L(p, q)_k \subset \mathbb{C}$ be the splitting field of all degree-2^k fields with Galois group a 2-group and discriminant $-^*p^*q^*$. The Galois group $\mathrm{Gal}(L(p, q)_k/\mathbb{Q})$ is a 2-group and so all ramification at the odd primes p and q is tame. Let $L(p, q)$ be the union of these $L(p, q)_k$. The group $\mathrm{Gal}(L(p, q)/\mathbb{Q})$ is a pro-2-group generated by the tame ramification elements τ_p and τ_q. The central question pursued in [**9**, **10**] is the distribution of the $\mathrm{Gal}(L(p, q)/\mathbb{Q})$ as abstract groups.

Table 7.1 corresponds to working at the level of the quotient $\mathrm{Gal}(L(p, q)_3/\mathbb{Q})$. The fact that this group has just the two generators τ_p and τ_q explains why only the sixteen 2-groups having one or two generators appear. One has $|\mathrm{Gal}(L(p, q)_3/\mathbb{Q})| = 2^{s_3}$, where s_3 is as in Table 7.1. The lines with an entry under T are pursued theoretically in [**9**]. The cases marked by ◦–•, *i–iii*, and *I–IV* are respectively treated in §§ 5.2, 5.3, and 5.4 there. The entire group $\mathrm{Gal}(L(p, q), \mathbb{Q})$ has order 2^s, with $s = \infty$ being expected sometimes in Case *IV*.

Some of the behavior for $k > 3$ is previewed by 2-parts of class groups of octic fields. For example, in Case *ii* all 87 instances behave the same: the unique fields in $\mathcal{K}(8T2, -^4p^3q^7)$, $\mathcal{K}(8T4, -^4p^4q^6)$, $\mathcal{K}(8T17, -^4p^6q^5)$ and the two fields in $\mathcal{K}(8T17, -^4p^6q^7)$ all have 2 exactly dividing the class number; the remaining six fields all have odd class number. In contrast, in Case *iii* the 86 instances break into two types of behaviors, represented by $(p, q) = (19, 5)$ and $(p, q) = (11, 37)$. These patterns in the database reflect the fact [**9**, § 5.3] that in Case *ii* there is just one possibility for $(\mathrm{Gal}(L(p, q)/\mathbb{Q}); \tau_p, \tau_q)$, while in Case *iii* there are two.

8. *Nilpotent octic fields with discriminant* $-^s2^aq^b$

The database has all octic fields with Galois group a 2-group and discriminant of the form $-^s2^aq^b$ with $q < 2500$. The sets $\mathcal{K}(\mathrm{NilOct}, -^*2^*q^*)$ average 1711 fields, the great increase from the previous section being due to the fact that now there are many possibilities for wild ramification at 2. As in the previous section, there is great regularity explained by identifications of relevant absolute Galois groups [**26**]. Again, even more so this time, there is further regularity not explained by theoretical results.

https://doi.org/10.1112/S1461157014000424 Published online by Cambridge University Press

Continuing with the notation of the previous section, consider the Galois extensions $L(2,q) = \bigcup_{k=1}^{\infty} L(2,q)_k$ and their associated Galois groups $\mathrm{Gal}(L(2,q)/\mathbb{Q}) = \varprojlim \mathrm{Gal}(L(2,q)_k/\mathbb{Q})$. As before, octic fields with Galois group a 2-group let one study $\mathrm{Gal}(L(2,q)_3/\mathbb{Q})$. Table 8.1 presents summarizing data for $q < 2500$ in a format parallel to Table 7.1 but more condensed. Here the main entries count Galois extensions of $\mathbb{Q}$. Thus, an entry m in the 19^2 20 21 column corresponds to m Galois extensions of $\mathbb{Q}$ having degree 32. Each of these Galois extensions corresponds to four fields in our database, of types $8T19$, $8T19$, $8T20$, and $8T21$.

In the range studied, there are thirteen different behaviors in terms of the cardinalities $|\mathcal{K}(8Tj, -^*2^*q^*)|$. As indicated by Table 7.1, these cardinalities depend mainly on the reduction of q modulo sixteen. However, classes 1, 9, and 15 are broken into subclasses. The biggest subclasses have size $|1A| = 23$, $|9A| = 24$, and $|15A| = 28$. The remaining subclasses are

$$\begin{aligned}
1B &= \{113, 337, 353, 593, 881, 1249, 1777, 2113, 2129, 2273\},\\
1C &= \{257, 1601\},\\
1D &= \{577, 1201, 1217, 1553, 1889\},\\
1E &= \{1153\},\\
9B &= \{73, 281, 617, 1033, 1049, 1289, 1753, 1801, 1913, 2281, 2393\},\\
9C &= \{137, 409, 809, 1129, 1321, 1657, 1993, 2137\},\\
15B &= \{31, 191, 383, 607, 719, 863, 911, 991, 1103, 1231, 1327, 1471,\\
&\qquad 1487, 1567, 1583, 2063, 2111, 2287, 2351, 2383\}.
\end{aligned}$$

TABLE 8.1. *The q–j entry gives the number of Galois extensions of $\mathbb{Q}$ with Galois group $8Tj$ and discriminant of the form $-^s2^aq^b$. The number of Galois extensions of $\mathbb{Q}_2$ with Galois group $8Tj$ is also given. Often a numerical entry in a given column persists for several more rows, and this repetition is indicated by ditto marks.*

	$\|G\|=8$					$\|G\|=16$						$\|G\|=32$				21	$\|G\|=64$					
																20		28^2	31^2			
q	1	2	3	4	5	6^2	7	8	9^4	10^2	11^3	15^2	16^2	17^2	18^8	19^2	26^4	27^2	29^6	30^4	35^8	Tot
$\mathbb{Q}_2$	24	18	1	18	6	16	36	36	9	12	16	38	12	48	4	24	24	48	16	24	48	1449
$1A$	24	18	1	30	2	42	36	44	15	36	12	64	36	96	16	48	80	104	32	52	72	2895
$1B$	″	″	″	″	″	54	36	60	″	″	″	84	60	144	″	96	144	256	80	128	312	6783
$1C$	″	″	″	″	″	″	″	″	″	″	″	″	″	″	″	″	″	272	″	136	336	7071
$1D$	″	″	″	″	″	″	″	″	″	″	″	″	″	″	″	″	″	336	″	168	384	7839
$1E$	″	″	″	″	″	″	″	″	″	″	″	″	″	″	″	″	″	″	″	″	240	6687
$9A$	24	18	1	30	2	44	36	48	15	36	12	68	36	112	16	48	96	104	48	52	156	3807
$9B$	″	″	″	″	″	″	″	″	″	″	″	″	″	″	″	″	″	″	″	″	132	3615
$9C$	″	″	″	″	″	″	″	″	″	″	″	″	″	″	″	″	″	72	″	36	156	3615
3, 11	4	6	1	14	2	10	6	22	7	4	6	21	4	8	3	4	16	8	8	4	21	579
5, 13	8	18	1	12	0	10	20	10	6	12	6	21	12	36	1	12	6	24	4	2	9	621
7	4	6	1	20	0	30	6	16	10	12	4	34	12	24	8	12	44	24	20	12	60	1401
$15A$	4	6	1	20	0	32	6	16	10	12	4	36	16	24	8	20	52	64	24	32	96	2041
$15B$	″	″	″	″	″	″	″	″	″	″	″	″	″	″	″	″	″	″	″	″	84	1945

https://doi.org/10.1112/S1461157014000424 Published online by Cambridge University Press

A prime $q \equiv 1$ (16) is in $1A$ if and only if $2 \notin \mathbb{F}_q^{\times 4}$. Otherwise, we do not have a concise description of these decompositions.

Let $D_\infty = \{1, c\}$, where c is complex conjugation. Let $D_q \subseteq \mathrm{Gal}(L(2,q)/\mathbb{Q})$ be a q-decomposition group. Then, working always in the category of pro-2-groups, one has the presentation $D_q = \langle \tau, \sigma | \sigma^{-1}\tau\sigma = \tau^q \rangle$; here τ is a ramification element and σ is a Frobenius element. Representing a more general theory, for $q \equiv 3, 5$ (8) one has two remarkable facts [**26**, Example 11.18]. First, the 2-decomposition group D_2 is all of $\mathrm{Gal}(L(2,q)/\mathbb{Q})$. Second, the global Galois group is a free product:

$$\mathrm{Gal}(L(2,q)/\mathbb{Q}) = D_\infty * D_q. \tag{8.1}$$

As a consequence, always for $q \equiv 3, 5$ (8), the quotients $\mathrm{Gal}(L(2,q)_k/\mathbb{Q})$ are computable as abstract finite groups and moreover depend only on q modulo eight. In particular, the counts in the lines 3,11 and 5,13 of Table 8.1 can be obtained purely group theoretically. The other lines of Table 8.1 are not covered by the theory in [**26**].

A important aspect of the situation is not understood theoretically, namely the wild ramification at 2. The database exhibits extraordinary regularity at the level $k = 3$, as follows. By 2-adically completing octic number fields $K \in \mathcal{K}(\mathrm{NilOct}, -^*2^*q^*)$, one gets 579 octic 2-adic fields if $q \equiv 3$ (8) and 621 octic 2-adic fields if $q \equiv 5$ (8). The regularity is that the subset of all 1499 nilpotent octic 2-adic fields which arise depends on q only modulo eight, at least in our range $q < 2500$. One can see some of this statement directly from the database: the cardinalities $|\mathcal{K}(8Tj, -^*2^aq^*)|$ for given (j, a) depend only on q modulo eight.

In the cases $q \equiv 3, 5$ (8), the group $\mathrm{Gal}(L(2,q)/\mathbb{Q}) = D_2$ has a filtration by higher ramification groups. From the group-theoretical description of $\mathrm{Gal}(L(2,q)/\mathbb{Q})$, one can calculate that the quotient group $\mathrm{Gal}(L(2,q)_3/\mathbb{Q})$ has size 2^{18}. The eighteen slopes measuring wildness of 2-adic ramification work out to be

3	0,	2, 2, $2\frac{1}{2}$	3, 3, $3\frac{1}{2}$, $3\frac{1}{2}$, $3\frac{5}{8}$, $3\frac{3}{4}$,	4, 4, $4\frac{1}{4}$, $4\frac{1}{4}$, $4\frac{3}{8}$, $4\frac{1}{2}$, $4\frac{3}{4}$	5
5	0, 0,	2, 2, 2, $2\frac{1}{2}$	3, 3, 3, $3\frac{1}{2}$, $3\frac{1}{2}$, $3\frac{3}{4}$,	4, $4\frac{1}{4}$, $4\frac{1}{2}$, $4\frac{3}{4}$, $4\frac{3}{4}$,	5.

Most of these slopes can be read off from the octic field part of the database directly, via the automatic 2-adic analysis of fields given there. For example, the first four slopes for $q = 3$ all arise already from $\mathbb{Q}[x]/(x^8 + 6x^4 - 3)$, the unique member of $\mathcal{K}(8T8, -^3 2^{16} 3^7)$. A few of the listed slopes can only be seen directly by working with degree-16 resolvents. A natural question, not addressed in the literature, is to similarly describe the slopes appearing in all of $\mathrm{Gal}(L(2,q)/\mathbb{Q})$.

9. *Minimal nonsolvable fields with* grd $\leqslant \Omega$

Our focus for the remainder of the paper is on Galois number fields, for which root discriminants and Galois root discriminants naturally coincide. As reviewed in the introduction, in [**21**] we raised the problem of completely understanding the set $\mathcal{K}[\Omega]$ of all Galois number fields $K \subset \mathbb{C}$ with grd at most the Serre–Odlyzko constant $\Omega = 8\pi e^\gamma \approx 44.76$. As in [**21**], we focus attention here on the interesting subproblem of identifying the subset $\mathcal{K}^{\mathrm{ns}}[\Omega]$ of K which are nonsolvable. Our last two sections explain how the database explicitly exhibits a substantial part of $\mathcal{K}^{\mathrm{ns}}[\Omega]$.

We say that a nonsolvable number field is *minimal* if it does not contain a strictly smaller nonsolvable number field. So, fields with Galois group say S_n are minimal, while fields with Galois group say $C_p \times S_n$ or $C_p^k : S_n$ are not. Figure 9.1 draws a dot for each minimal nonsolvable field $K_1 \in \mathcal{K}^{\mathrm{ns}}_{\mathrm{min}}[\Omega]$ coming from the degree less than or equal to eleven part of the

https://doi.org/10.1112/S1461157014000424 Published online by Cambridge University Press

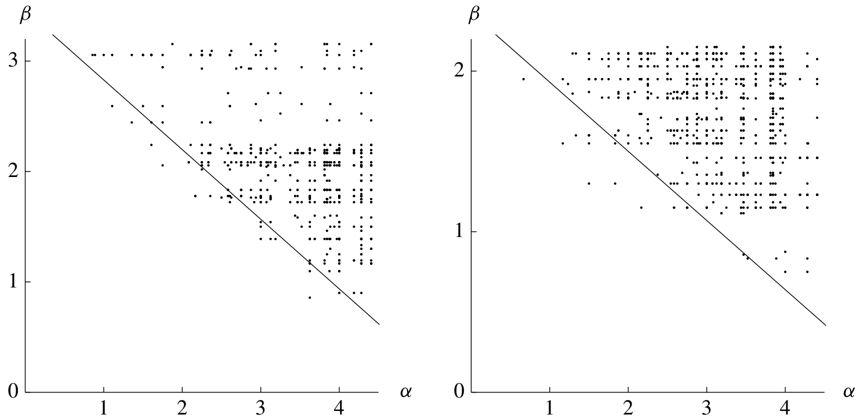

FIGURE 9.1. *Galois root discriminants $2^\alpha 3^\beta$ (left) and $2^\alpha 5^\beta$ (right) arising from minimal nonsolvable fields of degree less than or equal to eleven in the database. The lines have equation $2^\alpha q^\beta = \Omega$.*

database with grd of the form $2^\alpha 3^\beta$ or $2^\alpha 5^\beta$. There are 654 fields in the first case and 885 in the second. Of these fields, 24 and 17 have grd $\leqslant \Omega$. Figure 9.1 illustrates the extreme extent to which the low-grd problem is focused on the least ramified of all Galois number fields.

Figure 9.1 also provides some context for the next section, as follows. Consider the compositum $K = K_1 K_2$ of distinct minimal fields K_1 and K_2 contributing to the same half of Figure 9.1. Let $2^{\alpha_i} q^{\beta_i}$ be the root discriminant of K_i. The root discriminant $2^\alpha q^\beta$ of K satisfies $\alpha \geqslant \max(\alpha_1, \alpha_2)$ and $\beta \geqslant \max(\beta_1, \beta_2)$. The figure makes it clear that one must have almost exact agreement $\alpha_1 \approx \alpha_2$ and $\beta_1 \approx \beta_2$ for K to even have a chance of lying in $\mathcal{K}^{\mathrm{ns}}[\Omega]$. As some examples where one has exact agreement, consider the respective splitting fields K_1, K_2, and K_3 of

$$f_1(x) = x^5 - 10x^3 - 20x^2 + 110x + 116,$$
$$f_2(x) = x^5 + 10x^3 - 10x^2 + 35x - 18,$$
$$f_3(x) = x^5 + 10x^3 - 40x^2 + 60x - 32.$$

TABLE 9.1. *Lower bounds on $|\mathcal{K}[G,\Omega]|$ for minimal nonsolvable groups G. Entries highlighted in bold are completeness results from [21]. Fields found since [21] are indicated by '.'.*

#	$\lvert H\rvert$	$G = H$	#	$G = H.Q$	#
1	60	A_5	**78**	S_5	**192**
2	168	$\mathrm{SL}_3(2)$	*.18*	$\mathrm{PGL}_2(7)$	*...23*
3	360	A_6	**5**	S_6, $\mathrm{PGL}_2(9)$, M_{10}, $\mathrm{P\Gamma L}_2(9)$	**13**, *....6*, *0*, *.15*
4	504	$\mathrm{SL}_2(8)$	*15*	$\Sigma L_2(8)$	*15*
5	660	$\mathrm{PSL}_2(11)$	*1*	$\mathrm{PGL}_2(11)$	*0*
8	2520	A_7	*1*	S_7	*1*
1^2	3600	A_5^2		$A_5^2.2$, $A_5^2.V$, $A_5^2.C_4$, $A_5^2.D_4$	*1*, *.1*, *0*, *0*
10	4080	$\mathrm{SL}_2(16)$	*.1*	$\mathrm{SL}_2(16).2, \mathrm{SL}_2(16).4$	*0*, *0*
12	6048	$G_2(2)'$	*0*	$G_2(2)$	*.1*
19	20 160	A_8	*0*	S_8	*.1*

https://doi.org/10.1112/S1461157014000424 Published online by Cambridge University Press

All three fields have Galois group A_5 and root discriminant $2^{3/2}5^{8/5} \approx 37.14$. The first two completely agree at 2, but differ at 5, so that K_1K_2 has root discriminant $2^{3/2}5^{48/25} \approx 62.17$. The other two composita also have root discriminant well over Ω, with $\mathrm{grd}(K_2K_3) = 2^{9/4}5^{8/5} \approx 62.47$ and $\mathrm{grd}(K_1K_3) = 2^{9/4}5^{48/25} \approx 104.55$. These computations, done automatically by entering $f_i(x)f_j(x)$ into the grd calculator of [**20**], are clear illustrations of the general difficulty of using known fields in $\mathcal{K}[\Omega]$ to obtain others.

In [**21**], we listed fields proving $|\mathcal{K}^{\mathrm{ns}}_{\mathrm{min}}[\Omega]| \geqslant 373$. Presently, the fields in the database show $|\mathcal{K}^{\mathrm{ns}}_{\mathrm{min}}[\Omega]| \geqslant 386$. In [**21**], we highlighted the fact that the only simple groups involved were the five smallest, A_5, $\mathrm{SL}_3(2)$, A_6, $\mathrm{SL}_2(8)$, and $\mathrm{PSL}_2(11)$ and the eighth, A_7. The new fields add $\mathrm{SL}_2(16)$, $G_2(2)'$, and A_8 to the list of simple groups involved. These groups are tenth, twelfth, and tied for nineteenth in the list of all non-abelian simple groups in increasing order of size.

Table 9.1 summarizes all fields in the database in $\mathcal{K}^{\mathrm{ns}}_{\mathrm{min}}[\Omega]$. It is organized by the socle $H \subseteq G$, which is a simple group except in the single case $H = A_5 \times A_5$. The '.' indicate that, for example, of the 23 known fields in $\mathcal{K}[\mathrm{PGL}_2(7), \Omega]$, twenty are listed in [**21**] and three are new. The polynomial for the $\mathrm{SL}_2(16)$ field was found by Bosman [**8**], starting from a classical modular form of weight two. We found polynomials for the new $\mathrm{SL}_3(2)$ field and the three new $\mathrm{PGL}_2(7)$ fields starting from Schaeffer's list [**35**, Appendix A] of ethereal modular forms of weight one. Polynomials for the other new fields were found by specializing families. All fields summarized by Table 9.1 come from the part of the database in degree less than or equal to eleven, except for Bosman's degree-17 polynomial and the degree-28 polynomial for $G_2(2)$. It would be of interest to pursue calculations with modular forms more systematically. They have the potential not only to yield new fields in $\mathcal{K}^{\mathrm{ns}}_{\mathrm{min}}[\Omega]$, but also to prove completeness for certain G.

10. *General nonsolvable fields with* grd $\leqslant \Omega$

We continue in the framework of the previous section, so that the focus remains on Galois number fields contained in $\mathbb{C}$. For $K_1 \in \mathcal{K}^{\mathrm{ns}}_{\mathrm{min}}[\Omega]$ such a Galois number field, let $\mathcal{K}[K_1; \Omega]$ be the subset of $\mathcal{K}^{\mathrm{ns}}[\Omega]$ consisting of fields containing K_1. Clearly,

$$\mathcal{K}^{\mathrm{ns}}[\Omega] = \bigcup_{K_1} \mathcal{K}[K_1; \Omega]. \tag{10.1}$$

So, a natural approach to studying all of $\mathcal{K}^{\mathrm{ns}}[\Omega]$ is to study each $\mathcal{K}[K_1; \Omega]$ separately.

The refined local information contained in the database can be used to find fields in $\mathcal{K}[K_1; \Omega]$. The set of fields so obtained is always very small, often just $\{K_1\}$. Usually it seems likely that the set of fields obtained is all of $\mathcal{K}[K_1; \Omega]$, and sometimes this expectation is provable under the GRH. We sketch such a proof for a particular K_1 in the first example below. In the remaining examples, we start from other K_1 and construct proper extensions $K \in \mathcal{K}[K_1; \Omega]$, illustrating several phenomena. Our examples are organized in terms of increasing degree $[K : \mathbb{Q}]$. The fields here are all extremely lightly ramified for their Galois group, and therefore worthy of individual attention.

Our local analysis of a Galois number field K centers on the notion of p-adic slope content described in [**20**, §3.4] and automated in the associated database. Thus, a p-adic slope content of $[s_1, \ldots, s_m]^u_t$ indicates a wild inertia group P of order p^m, a tame inertia group I/P of order t, and an unramified quotient D/I of order u. Wild slopes $s_i \in \mathbb{Q} \cap (1, \infty)$ are listed in weakly increasing order and from [**20**, equation (7)] the contribution p^α to the root discriminant of K is determined by

$$\alpha = \left(\sum_{i=1}^{m} \frac{p-1}{p^i} s_{n+1-i} \right) + \frac{1}{p^m} \frac{t-1}{t}.$$

The quantities t and u are omitted from presentations of slope content when they are 1.

https://doi.org/10.1112/S1461157014000424 Published online by Cambridge University Press

Degree 120 *and nothing more from* S_5. The polynomial

$$f_1(x) = x^5 + x^3 + x - 1$$

has splitting field K_1 with root discriminant $\Delta_1 = 11^{2/3}37^{1/2} \approx 30.09$. Since $\Delta_1 2^{2/3} \approx 47.76$, $\Delta_1 3^{1/2} \approx 52.11$, $\Delta_1 11^{1/6} \approx 44.87$, and $\Delta_1 37^{1/4} \approx 74.20$ are all more than Ω, any $K \in \mathcal{K}[K_1; \Omega]$ has to have root discriminant $\Delta = \Delta_1$. The GRH bounds say that a field with root discriminant 30.09 can have degree at most 2400 [**29**].

The main part of the argument is to use the database to show that most other *a priori* possible G in fact do not arise as $\mathrm{Gal}(K/\mathbb{Q})$ for $K \in \mathcal{K}[K_1; \Omega]$. For example, if there were an S_3 field K_2 with absolute discriminant $11^2 37$, then $K_1 K_2$ would be in $\mathcal{K}[K_1; \Omega]$; there is in fact an S_3 field with absolute discriminant $11 \cdot 37^2$, but not one with absolute discriminant $11^2 37$. As an example of a group that needs a supplementary argument to be eliminated, the central extension $G = 2.S_5$ does not appear because the degree-12 subfield of K_1 fixed by $D_5 \subset S_5$ has root discriminant Δ_1 and class number 1.

Degree 1920 *from* A_5. The smallest root discriminant of any nonsolvable Galois field is $2^{6/7}17^{2/3} \approx 18.70$ coming from a field K_1 with Galois group A_5. This case is complicated because one can add ramification in several incompatible directions, so that there are different maximal fields in $\mathcal{K}[K_1; \Omega]$. One overfield is the splitting field $\tilde{K}_1$ of $f_-(x)$, where

$$f_\pm(x) = x^{10} + 2x^6 \pm 4x^4 - 3x^2 \pm 4.$$

In this direction, ramification has been added at 2, making the slope content there $[2, 2, 2, 2, 4]^6$ and the root discriminant $2^{39/16}17^{2/3} \approx 35.81$. The only solvable field K_2 in the database which is not contained in $\tilde{K}_1$ but has $\mathrm{rd}(\tilde{K}_1 K_2) < \Omega$ is $\mathbb{Q}(i)$. The field $\tilde{K}_1 K_2$ is the splitting field of $f_+(x)$ with Galois group $10T36$. There is yet another wild slope of 2, making the root discriminant $2^{79/32}17^{2/3} \approx 36.60$.

Degree 25 080 *from* $\mathrm{PSL}_2(11)$. The only known field K_1 with Galois group $\mathrm{PSL}_2(11)$ and root discriminant less than Ω first appeared in [**25**] and is the splitting field of

$$f_1(x) = x^{11} - 2x^{10} + 3x^9 + 2x^8 - 5x^7 + 16x^6 - 10x^5 + 10x^4 + 2x^3 - 3x^2 + 4x - 1.$$

The root discriminant is $\Delta_1 = 1831^{1/2} \approx 42.79$, forcing all members of $\mathcal{K}[K_1; \Omega]$ to have root discriminant $1831^{1/2}$ as well.

The prime 1831 is congruent to 3 modulo 4, so that the associated quadratic field $\mathbb{Q}(\sqrt{-1831})$ is imaginary and its class number can be expected to be considerably larger than one. This class number is in fact nineteen, and the splitting field of a degree-19 polynomial in the database is the corresponding Hilbert class field K_2. The field $K_1 K_2 \in \mathcal{K}[K_1; \Omega]$ has degree $660 \cdot 38 = 25\,080$.

Degree 48 384 *from* $\mathrm{SL}_2(8).3$. The splitting field K_1 of

$$f_1(x) = x^9 - 3x^8 + 4x^7 + 16x^2 + 8x + 8$$

has Galois group $\mathrm{Gal}(K_1/\mathbb{Q}) = 9T32 = \mathrm{SL}_2(8).3$ and root discriminant $2^{73/28}7^{8/9} \approx 34.36$. This root discriminant is the smallest known from a field with Galois group $\mathrm{SL}_2(8).3$. In fact, it is small enough that it is possible to add ramification at both 2 and 7 and still keep the root discriminant less than Ω. Namely, let

$$f_2(x) = x^4 - 2x^3 + 2x^2 + 2,$$
$$f_3(x) = x^4 - x^3 + 3x^2 - 4x + 2.$$

The splitting fields K_2 and K_3 have Galois groups A_4 and D_4, respectively. Composing with K_2 increases degrees by four and adds wild slopes 2 and 2 to the original 2-adic slope content

https://doi.org/10.1112/S1461157014000424 Published online by Cambridge University Press

$[20/7, 20/7, 20/7]_7^3$. Composing with K_3 then increases degrees by eight, adding another wild slope of 2 to the 2-adic slope content and increasing the 7-adic tame degree from nine to 36. The root discriminant of $K_1K_2K_3$ is then $2^{153/56}7^{35/36} \approx 44.06$.

Degree 80 640 *from* S_8. The largest group in Table 9.1 is S_8, and the only known field in $\mathcal{K}[S_8, \Omega]$ is the splitting field K_1 of

$$f_1(x) = x^8 - 4x^7 + 4x^6 + 8x^3 - 32x^2 + 32x - 20.$$

Here Galois slope contents are $[15/4, 7/2, 7/2, 3, 2, 2]^3$ and $[\,]_7$ at 2 and 5, respectively, giving root discriminant $2^{111/32}5^{6/7} \approx 43.99$. The only field in the database which can be used to give a larger field in $\mathcal{K}[K_1; \Omega]$ is $K_2 = \mathbb{Q}(i)$. This field gives an extra wild slope of 2, raising the degree of K_1K_2 to 80 640 and the root discriminant to $2^{223/64}5^{6/7} \approx 44.47$.

Degree 86 400 *from* $A_5^2.V$. Another new field K_1 in Table 9.1, found by Driver, is the splitting field of

$$f_1(x) = x^{10} - 2x^9 + 5x^8 - 10x^6 + 28x^5 - 26x^4 - 5x^2 + 50x - 25.$$

As in the previous example, this field K_1 is wildly ramified at 2 and tamely ramified at 5. Slope contents are $[23/6, 23/6, 3, 8/3, 8/3]_3$ and $[\,]_6$ for a root discriminant of $2^{169/48}5^{5/6} \approx 43.89$. The splitting field K_2 of $x^3 - x^2 + 2x + 2$ has Galois group S_3, with 2-adic slope content [3] and 5-adic slope content $[\,]_3$. In the compositum K_1K_2, the extra slope is in fact 2, giving a root discriminant of $2^{85/24}5^{5/6} \approx 44.53$.

Degree 172 800 *from* S_5 *and* S_6. Consider the $\binom{386}{2} = 74\,305$ composita K_1K_2, as K_1 and K_2 vary over distinct known fields in $\mathcal{K}_{\min}^{\rm ns}[\Omega]$. From our discussion of Figure 9.1, one would expect that very few of these composita would have root discriminant less than Ω. In fact, calculation shows that exactly one of these composita has $\mathrm{rd}(K_1K_2) \leqslant \Omega$, namely the joint splitting field of

$$f_1(x) = x^5 - x^4 - x^3 + 3x^2 - x - 19,$$
$$f_2(x) = x^6 - 2x^5 + 4x^4 - 8x^3 + 2x^2 + 24x - 20.$$

Here $\mathrm{Gal}(K_1/\mathbb{Q}) = S_5$ and $\mathrm{Gal}(K_2/\mathbb{Q}) = S_6$. Both fields have tame ramification of order two at 3 and order five at 7. Both are otherwise ramified only at 2, with K_1 having slope content $[2, 3]^2$ and K_2 having slope content $[2, 2, 3]^3$. In the compositum K_1K_2, there is partial cancellation between the two wild slopes of 3, and the slope content is $[2, 2, 2, 2, 3]^6$. The root discriminant of K_1K_2 then works out to be $2^{39/16}3^{1/2}7^{4/5} \approx 44.50$. The existence of this remarkable compositum contradicts [**21**, Corollary 12.1] and is the only error we have found in [**21**].

The field discriminants of f_1 and f_2 are respectively $-^2 2^6 3^1 7^4$ and $-^2 2^9 3^1 7^4$. The splitting fields K_1 and K_2 thus contain distinct quadratic fields, $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{6})$, respectively. The compositum therefore has Galois group all of $S_5 \times S_6$, and so the degree $[K_1K_2 : \mathbb{Q}] = 120 \cdot 720 = 86\,400$ ties with that of the previous example. But, moreover, $K_3 = \mathbb{Q}(\sqrt{-3})$ is disjoint from $\mathbb{Q}(\sqrt{3}, \sqrt{6})$ and does not introduce more ramification. So, $K = K_1K_2K_3$ has the same root discriminant $2^{39/16}3^{1/2}7^{4/5} \approx 44.50$, but the larger degree $2 \cdot 86\,400 = 172\,800$.

The GRH upper bound on degree for a given root discriminant $\delta \in [1, \Omega)$ increases to infinity as δ increases to Ω (as illustrated by [**21**, Figure 4.1]). However, we have only exhibited fields K here of degree less than or equal to 172 800. Dropping the restriction that K is Galois and nonsolvable may let one obtain somewhat larger degrees, but there remains a substantial and intriguing gap between degrees of known fields and analytic upper bounds on degree.

References

1. K. Belabas, 'cubic v. 1.2', http://www.math.u-bordeaux1.fr/~kbelabas/research/software/cubic-1.2.tgz.
2. K. Belabas, 'On quadratic fields with large 3-rank', *Math. Comp.* 73 (2004) no. 248, 2061–2074 (electronic); MR 2059751 (2005c:11132).
3. A.-M. Bergé, J. Martinet and M. Olivier, 'The computation of sextic fields with a quadratic subfield', *Math. Comp.* 54 (1990) no. 190, 869–884; MR 1011438 (90k:11169).
4. M. Bhargava, 'The density of discriminants of quartic rings and fields', *Ann. of Math.* (2) 162 (2005) no. 2, 1031–1063; MR 2183288 (2006m:11163).
5. M. Bhargava, 'Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants', *Int. Math. Res. Not. IMRN* 2007 (2007), doi:10.1093/imrn/rnm052; MR 2354798 (2009e:11220).
6. M. Bhargava, 'The density of discriminants of quintic rings and fields', *Ann. of Math.* (2) 172 (2010) no. 3, 1559–1591; MR 2745272 (2011k:11152).
7. Bordeaux tables of number fields, http://pari.math.u-bordeaux.fr/pub/pari/packages/nftables/.
8. J. Bosman, 'A polynomial with Galois group $SL_2(\mathbb{F}_{16})$', *LMS J. Comput. Math.* 10 (2007) 1461–1570 (electronic); MR 2365691 (2008k:12008).
9. N. Boston and J. S. Ellenberg, 'Random pro-p groups, braid groups, and random tame Galois groups', *Groups Geom. Dyn.* 5 (2011) no. 2, 265–280; MR 2782173 (2012b:11172).
10. N. Boston and D. Perry, 'Maximal 2-extensions with restricted ramification', *J. Algebra* 232 (2000) no. 2, 664–672; MR 1792749 (2001k:12005).
11. G. Butler and J. McKay, 'The transitive groups of degree up to eleven', *Comm. Algebra* 11 (1983) no. 8, 863–911.
12. S. R. Dahmen, 'Classical and modular methods applied to diophantine equations', PhD Thesis, University of Utrecht, 2008.
13. E. D. Driver and J. W. Jones, 'Minimum discriminants of imprimitive decic fields', *Exp. Math.* 19 (2010) no. 4, 475–479; MR 2778659 (2012a:11169).
14. J. L. Hoelscher, 'Infinite class field towers', *Math. Ann.* 344 (2009) no. 4, 923–928; MR 2507631 (2010h:11185).
15. K. Hulek, R. Kloosterman and M. Schütt, 'Modularity of Calabi–Yau varieties', *Global aspects of complex geometry* (Springer, Berlin, 2006) 271–309; MR 2264114 (2007g:11052).
16. J. Hunter, 'The minimum discriminants of quintic fields', *Proc. Glasgow Math. Assoc.* 3 (1957) 57–67; MR 0091309 (19,944b).
17. J. W. Jones and D. P. Roberts, 'Artin L-functions with small conductor', in preparation.
18. J. W. Jones and D. P. Roberts, 'Sextic number fields with discriminant $(-1)^j 2^a 3^b$', *Number theory (Ottawa, ON, 1996)*, CRM Proceedings & Lecture Notes 19 (American Mathematical Society, Providence, RI, 1999) 141–172; MR 2000b:11142.
19. J. W. Jones and D. P. Roberts, 'Septic fields with discriminant $\pm 2^a 3^b$', *Math. Comp.* 72 (2003) no. 244, 1975–1985 (electronic); MR 1986816 (2004e:11119).
20. J. W. Jones and D. P. Roberts, 'A database of local fields', *J. Symbolic Comput.* 41 (2006) no. 1, 80–97; website: http://math.asu.edu/~jj/localfields.
21. J. W. Jones and D. P. Roberts, 'Galois number fields with small root discriminant', *J. Number Theory* 122 (2007) no. 2, 379–407; MR 2292261 (2008e:11140).
22. J. W. Jones and D. P. Roberts, 'Number fields ramified at one prime', *Algorithmic number theory*, Lecture Notes in Computational Science 5011 (Springer, Berlin, 2008) 226–239; MR 2467849 (2010b:11152).
23. J. W. Jones and D. P. Roberts, 'The tame–wild principle for discriminant relations for number fields', *Algebra Number Theory* 8 (2014) no. 3, 609–645.
24. J. W. Jones and R. Wallington, 'Number fields with solvable Galois groups and small Galois root discriminants', *Math. Comp.* 81 (2012) no. 277, 555–567.
25. J. Klüners and G. Malle, 'A database for field extensions of the rationals', *LMS J. Comput. Math.* 4 (2001) 182–196 (electronic); MR 2003i:11184.
26. H. Koch, *Galois theory of p-extensions*, Springer Monographs in Mathematics (Springer, Berlin, 2002). With a foreword by I. R. Shafarevich, translated from the 1970 German original by Franz Lemmermeyer, with a postscript by the author and Lemmermeyer; MR 1930372 (2003f:11181).
27. G. Malle, 'On the distribution of Galois groups', *J. Number Theory* 92 (2002) no. 2, 315–329; MR 1884706 (2002k:12010).
28. G. Malle and B. H. Matzat, *Inverse Galois theory*, Springer Monographs in Mathematics (Springer, Berlin, 1999); MR 1711577 (2000k:12004).
29. J. Martinet, 'Petits discriminants des corps de nombres', *Number theory days, 1980 (Exeter, 1980)*, London Mathematical Society Lecture Note Series 56 (Cambridge University Press, Cambridge, 1982) 151–193; MR 84g:12009.

30. A. M. Odlyzko, 'Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results', *Sém. Théor. Nombres Bordeaux* (2) 2 (1990) no. 1, 119–141; MR 1061762 (91i:11154).
31. K. Ono and Y. Taguchi, '2-adic properties of certain modular forms and their applications to arithmetic functions', *Int. J. Number Theory* 1 (2005) no. 1, 75–101; MR 2172333 (2006e:11057).
32. M. Pohst, 'On the computation of number fields of small discriminants including the minimum discriminants of sixth degree fields', *J. Number Theory* 14 (1982) no. 1, 99–117; MR 644904 (83g:12009).
33. D. P. Roberts, 'Chebyshev covers and exceptional number fields', in preparation. http://facultypages.morris.umn.edu/∼roberts/.
34. D. P. Roberts, 'Wild partitions and number theory', *J. Integer Seq.* 10 (2007) no. 6, Article 07.6.6; MR 2335791 (2009b:11206).
35. G. J. Schaeffer, 'The Hecke stability method and ethereal forms', PhD Thesis, University of California, Berkeley, CA (ProQuest, UMI Dissertations Publishing, Ann Arbor, MI, 2012); MR 3093915.
36. A. Schwarz, M. Pohst and F. Diaz y Diaz, 'A table of quintic number fields', *Math. Comp.* 63 (1994) no. 207, 361–376; MR 1219705 (94i:11108).
37. The GAP Group, GAP—Groups, Algorithms, and Programming, version 4.4, 2006 (http://www.gap-system.org).
38. The PARI Group, Bordeaux, Pari/gp, version 2.6.2, 2013.
39. J. Voight, 'Tables of totally real number fields', http://www.math.dartmouth.edu/∼jvoight/nf-tables/index.html.
40. J. Voight, 'Enumeration of totally real number fields of bounded root discriminant', *Algorithmic number theory*, Lecture Notes in Computer Science 5011 (Springer, Berlin, 2008) 268–281; MR 2467853 (2010a:11228).

John W. Jones
School of Mathematical and Statistical Sciences
Arizona State University
PO Box 871804
Tempe, AZ 85287
USA
jj@asu.edu

David P. Roberts
Division of Science and Mathematics
University of Minnesota Morris
Morris, MN 56267
USA
roberts@morris.umn.edu

https://doi.org/10.1112/S1461157014000424 Published online by Cambridge University Press