2008

Number Fields Ramified at One Prime

John W. Jones
Arizona State University

David P. Roberts
University of Minnesota - Morris, roberts@morris.umn.edu

Number Fields Ramified at One Prime

John W. Jones[1] and David P. Roberts[2]

[1] Dept. of Mathematics and Statistics, Arizona State Univ., Tempe, AZ 85287
jj@asu.edu
[2] Div. of Science and Mathematics, Univ. of Minnesota–Morris, Morris, MN 56267
roberts@morris.umn.edu

Abstract. For G a finite group and p a prime, a G-p field is a Galois number field K with $\mathrm{Gal}(K/\mathbf{Q}) \cong G$ and $\mathrm{disc}(K) = \pm p^a$ for some a. We study the existence of G-p fields for fixed G and varying p.

For G a finite group and p a prime, we define a G-p field to be a Galois number field $K \subset \mathbf{C}$ satisfying $\mathrm{Gal}(K/\mathbf{Q}) \cong G$ and $\mathrm{disc}(K) = \pm p^a$ for some a. Let $\mathcal{K}_{G,p}$ denote the finite, and often empty, set of G-p fields.

The sets $\mathcal{K}_{G,p}$ have been studied mainly from the point of view of fixing p and varying G; see [Har94], for example. We take the opposite point of view, as we fix G and let p vary. Given a finite group G, we let $\mathcal{P}_G$ be the sequence of primes where each prime p is listed $|\mathcal{K}_{G,p}|$ times. We determine, for various groups G, the first few primes in $\mathcal{P}_G$ and their corresponding fields. Only the primes p dividing $|G|$ can be wildly ramified in a G-p field, and so the sequences $\mathcal{P}_G$ which are infinite are dominated by tamely ramified fields.

In Sections 1, 2, and 3, we consider the cases when G is solvable with length 1, 2, and ≥ 3 respectively, using mainly class field theory. Section 4 deals with the much more difficult case of non-solvable groups, with results obtained by complete computer searches for certain polynomials in degrees 5, 6, and 7.

In Section 5, we consider a remarkable $PGL_2(7)$-53 field given by an octic polynomial from the literature. We show that the generalized Riemann hypothesis implies that in fact $\mathcal{P}_{PGL_2(7)}$ begins with 53. Sections 6 and 7 construct fields for the first primes in $\mathcal{P}_G$ for more groups G by considering extensions of fields previously found. Finally in Section 8, we conjecture that $\mathcal{P}_G$ always has a density, and this density is positive if and only if G^{ab} is cyclic.

As a matter of notation, we present G-p fields as splitting fields of polynomials $f(x) \in \mathbf{Z}[x]$, with $f(x)$ chosen to have minimal degree. When $\mathcal{K}_{G,p}$ has exactly one element, we denote this element by $K_{G,p}$. To avoid a proliferation of subscripts, we impose the convention that m represents a cyclic group of order m. Finally, for odd primes p let $\hat{p} = (-1)^{(p-1)/4}p$, so that $K_{2,p}$ is $\mathbf{Q}(\sqrt{\hat{p}})$.

One reason that number fields ramified only at one prime are interesting is that general considerations simplify in this context. For example, the formalism of quadratic lifting as in Section 7 becomes near-trivial. A more specific reason is that algebraic automorphic forms ramified at no primes give rise to number fields ramified at one prime via associated p-adic Galois representations. For example, the fields $K_{S_3,23}$, $K_{S_3,31}$, $K_{\tilde{S}_4,59}$ and $K_{SL_2^{\pm}(11),11}$ here all arise in this way in the

context of classical modular forms of level one [SD73]. We expect that some of the other fields presented in this paper will likewise arise in similar studies of automorphic forms on larger groups.

Most of the computations carried out for this paper made use of pari/gp [PAR06], in both library and command line modes.

1 Abelian groups

For n a positive integer, set $\zeta_n = e^{2\pi i/n}$, a primitive n^{th} root of unity. The field $\mathbf{Q}(\zeta_n)$ is abelian over $\mathbf{Q}$, with Galois group $(\mathbf{Z}/n)^\times$, where $g \in (\mathbf{Z}/n)^\times$ sends ζ to ζ^g. The Kronecker-Weber theorem says that any finite abelian extension F of $\mathbf{Q}$ is contained in some $\mathbf{Q}(\zeta_n)$ with n divisible by exactly the set of primes ramifying in $F/\mathbf{Q}$. These classical facts let one quickly determine $\mathcal{K}_{G,p}$ for abelian G, and we record the results for future reference.

Proposition 1.1 *Let p be a prime and G a finite abelian group of order $d = p^a m$, with $\gcd(p, m) = 1$.*

1. *If p is odd, there exists a G-p field if and only if G is cyclic and $m \mid p-1$. In this case, $|\mathcal{K}_{G,p}| = 1$, and $K_{G,p}/\mathbf{Q}$ is tamely ramified if and only if $a = 0$.*
2. *There exists a G-2 field if and only if for some $j \geq 1$, $G \cong 2^j$ or $G \cong 2^j \times 2$. One has $|\mathcal{K}_{2^j \times 2,2}| = 1$, $|\mathcal{K}_{2,2}| = 3$, and, for $j \geq 2$, $|\mathcal{K}_{2^j,2}| = 2$. All fields in $\mathcal{K}_{G,2}$ are wildly ramified.*

For odd p, a defining polynomial for $K_{d,p}$ is given by the minimal polynomial of the trace $\mathrm{Tr}_{\mathbf{Q}(\zeta_{p^{a+1}})/K_{d,p}}(\zeta_{p^{a+1}})$. Explicitly,

$$f_{d,p}(x) = \prod_{u=1}^{d}(x - \sum_{j=1}^{(p-1)/m} e^{2\pi i g^{u+dj}/p^{a+1}}),$$

where g is a generator for the cyclic group $(\mathbf{Z}/p^{a+1})^\times$. For example,

$$f_{7,7}(x) = x^7 - 21x^5 - 21x^4 + 91x^3 + 112x^2 - 84x - 97,$$
$$f_{7,29}(x) = x^7 + x^6 - 12x^5 - 7x^4 + 28x^3 + 14x^2 - 9x + 1.$$

Irreducibility of $f_{d,p}(x)$ follows from the stronger fact that $f_{d,p}(x + (p-1)/m)$ is p-Eisenstein.

2 Length two solvable groups

The next case beyond abelian groups is solvable groups G of length two. This case also essentially reduces to a classical chapter in the theory of cyclotomic fields. Let K be a G-p field.

The case $p = 2$ needs to be treated separately; it doesn't yield any fields for the G considered explicitly below. We restrict to the case of odd p, in which case G^{ab} is necessarily cyclic and there is a unique field $K_{G^{\text{ab}},p} = K^{G'} \subseteq K$. The cyclicity of G^{ab} forces G to be a semidirect product $G'{:}G^{\text{ab}}$. The following is very similar to a statement discovered independently in [Hoe07].

Proposition 2.1 *Let K be a G-p field with $p \neq 2$, so that $G = G'{:}G^{\mathrm{ab}}$ as above. Then if p does not divide $|G'|$, the extension $K/K_{G^{\mathrm{ab}},p}$ is unramified.*

The proof considers the compositum $K\mathbf{Q}(\zeta_{p^k})$ where $K_{G^{\mathrm{ab}},p} \subseteq \mathbf{Q}(\zeta_{p^k})$ and then shows and uses that $\mathbf{Q}(\zeta_{p^k})$ has no tame totally ramified extensions.

Proposition 2.1 says that when p is odd and $|G'|$ is coprime to p the set $\mathcal{K}_{G,p}$ is indexed by G^{ab}-stable quotients of $\mathrm{Cl}(K_{G^{\mathrm{ab}},p})$ which are G^{ab}-equivariantly isomorphic to G'. Defining polynomials for fields in $\mathcal{K}_{G,p}$ can then often be computed using explicit class field theory functions in gp.

The simplest case is this setting is dihedral groups $D_\ell = \ell{:}2$ with ℓ and p different odd primes. The group 2 must act on $\mathrm{Cl}(K_{2,p})$ by negation. If the quotient by multiples of ℓ, $\mathrm{Cl}(K_{2,p})/\ell$, is isomorphic to ℓ^r, then $\mathcal{K}_{D_\ell,p}$ has the structure of an $(r-1)$-dimensional projective space over $\mathbf{F}_\ell$ and thus $|\mathcal{K}_{D_\ell,p}| = (\ell^r-1)/(\ell-1)$. The general case is similar, but group-theoretically more complicated. In particular, one has to keep careful track of how G^{ab} acts.

In the table below, we present some cases where G is a length two solvable group with G^{ab} acting faithfully and indecomposably on G'. In this setting, $|G^{\mathrm{ab}}|$ and $|G'|$ are forced to be coprime. We list the first few primes p for which there is a tame G-p extension. If there happens to be a wildly ramified G-p extension as well, we record the prime in the column p_w. A prime listed as $p^{(j)}$ signifies that there are j different G-p fields.

G	G^{ab}	p_w	**Tame Primes**
S_3	2	3	$23, 31, 59, 83, 107, 139, 199, 211, 229, 239, 257, 283, 307, 331, 367$
D_5	2		$47, 79, 103, 127, 131, 179, 227, 239, 347, 401, 439, 443, 479, 523$
D_7	2	7	$71, 151, 223, 251, 431, 463, 467, 487, 503, 577, 587, 743, 811, 827$
D_{11}	2	11	$167, 271, 659, 839, 967, 1283, 1297, 1303, 1307, 1459, 1531, 1583$
D_{13}	2		$191, 263, 607, 631, 727, 1019, 1439, 1451, 1499, 1667, 1907, 2131$
A_4	3		$163, 277, 349, 397, 547, 607, 709, 853, 937, 1009, 1399, 1699, 1777$
7:3	3		$313, 877, 1129, 1567, 1831, 1987, 2437, 2557, 3217, 3571, 4219$
F_5	4	$5^{(2)}$	$101, 157, 173, 181, 197, 349, 373, 421, 457, 461, 613, 641, 653^{(2)}$
3^2:4	4		$149, 293, 661, 733, 1373, 1381, 1613, 1621, 1733, 1973, 2861, 3109$
F_7	6	7	$211, 463, 487, 619, 877, 907, 991, 1069, 1171, 1231, 1303, 1381$

Sample defining polynomials are

$$f_{7:3,313}(x) = x^7 - x^6 - 15x^5 + 20x^4 + 33x^3 - 22x^2 - 32x - 8,$$
$$f_{3^2:4,149}(x) = x^6 - 5x^4 - 9x^3 - 31x^2 - 52x - 17.$$

Note that direct application of class field theory would give defining polynomials of degree 21 and 12 respectively.

Suppose G is such that the action of G^{ab} on G' is faithful and decomposes G' as $N_1 \times N_2$. Suppose G^{ab} acts on N_i through a faithful action of its quotient $Q_i \cong G^{\mathrm{ab}}/H_i$. Put $G_i = N_i{:}Q_i$. Then $\mathcal{K}_{G,p}$ can be constructed directly from $\mathcal{K}_{G_1,p}$ and $\mathcal{K}_{G_2,p}$ by taking compositа. The simplest case is when $|N_1|$ and $|N_2|$

are coprime. Then $\mathcal{K}_{G,p}$ consists of the composita K_1K_2 as K_i runs over $\mathcal{K}_{G_i,p}$. In particular, $|\mathcal{K}_{G,p}| = |\mathcal{K}_{G_1,p}| \cdot |\mathcal{K}_{G_2,p}|$. Similarly, if G^{ab} acts on G' through a faithful action of its quotient Q, then $\mathcal{K}_{G,p}$ is empty if $\mathcal{K}_{G^{\mathrm{ab}},p}$ is empty, and otherwise consists of $K_{G^{\mathrm{ab}},p}K$ with K running over $\mathcal{K}_{G':Q,p}$. First primes for some groups of these composed types are

G	3^2:2	2^2:6	3:4	(3×2^2):6	3:8	7:4	3^3:2	3^4:2
	$\frac{1}{2}S_3^2$	$A_4 2$	$\frac{1}{2}4S_3$	A_4S_3	$\frac{1}{2}S_3 8$	$\frac{1}{2}D_7 4$	$\frac{1}{4}S_3^3$	$\frac{1}{8}S_3^4$
p	3299	163	229	547	257	577	3,321,607	1,876,623,871

A sample defining polynomial is

$$f_{(3\times 2^2):6,547}(x) = f_{A_4,547}(x)f_{S_3,547}(x) = (x^4-21x^2-3x+100)(x^3-x^2-3x-4).$$

On the table, the first description of G gives G':G^{ab} and the second emphasizes the compositum structure. The case of 3^r:2 $= \frac{1}{2^{r-1}}S_3^r$ has been studied intensively in the literature. With gp, it is easy to determine that $p = 3{,}321{,}607$ is minimal for 3^3:2. The smallest p for 3^4:2 comes from [Bel04].

3 General solvable groups: the case $G = S_4$

For a general solvable group G, one can in principle proceed inductively via the quotients of G using p-ray class groups. For F a number field, let $\mathrm{Cl}_p(F)$ be the p-ray class group of F. This group is infinite, as e.g. $\mathrm{Cl}_p(\mathbf{Q}) = \mathbf{Z}_p^\times$. However, for any positive integer m, the quotient $\mathrm{Cl}_p(F)/m$ is finite. Let $\tilde{F}$ be a maximal abelian extension ramified only at p with Galois group killed by m. Then by class field theory $\mathrm{Gal}(\tilde{F}/F) = \mathrm{Cl}_p(F)/m$.

To carry out the induction efficiently, one works with typically non-Galois number fields F of degree as low as possible. As an example that we will return to in Section 8, take G to be the length three solvable group S_4. To compute $\mathcal{K}_{S_4,p}$, we start from a list of cubic polynomials $f_i(x)$ with splitting fields running over $\mathcal{K}_{S_3,p}$. We compute $\mathrm{Cl}_2(\mathbf{Q}[x]/f_i(x))/2 \cong 2^r$. For each of the 2^r-1 order two quotients of this group, we find a corresponding sextic polynomial $g_{i,j}(x)$. For fixed i, there will be one polynomial with Galois group $6T_2 \cong S_3$. The remaining sextic polynomial are grouped in pairs, according to whether they have the same splitting field in $\mathcal{K}_{S_4,p}$. One member of each pair has Galois group $6T_7 \cong S_4$ and the other has Galois group $6T_8 \cong S_4$. The first primes in $\mathcal{P}_{S_4}$ are

$\lambda_p \backslash s$	0	1	2
4	$2713, 2777^{(2)}, 2857, 3137$	$59, 107, 139, 283^{(2)}, 307$	$229^{(2)}, 733, 1373, 1901$
211	$2777, 7537, 8069, 10273$	$283, 331, 491, 563, 643$	$229, 257, 761, 1129^{(2)}$

Here primes are sorted according to the quartic ramification partitions λ_p and $\lambda_\infty = 2^s1^{4-2s}$, as explained in the next section. For a given cubic resolvent, let m_4 and m_{211} be the number of corresponding S_4 fields with the indicated λ_p. From the underlying group theory, the possibilities for (m_4, m_{211}) are $(0, 2^j-1)$

and $(2^j, 2^j - 1)$ for any $j \geq 0$. There are thirteen primes ≤ 307 on the S_3 list, and the table illustrates the possibilities $(0,0)$, $(1,0)$, $(2,1)$, and $(0,1)$ by $\{23, 31, 83, 199, 211, 239\}$, $\{59, 107, 139, 307\}$, $\{229, 283\}$, and $\{257\}$ respectively.

4 Non-solvable groups

In [JR99,JR03] we describe how one can computationally determine all primitive extensions of $\mathbf{Q}$ of a given degree n which are unramified outside a given finite set of primes by means of a targeted Hunter search. Here we employ this method to find the first several G-p fields with $G = A_5$, S_5, A_6, S_6, $GL_2(3)$, and S_7. All together, the results presented in this section represent several months of CPU time. In each case, the first step is to quickly verify that there are are no wildly ramified fields.

For a tamely ramified prime p, the ramification possibilities are indexed by partitions of n, with $\lambda = 11 \cdots 11$ indicating unramified and $\lambda = n$ totally ramified. If the partition has $|\lambda|$ parts, then the degree n field $\mathbf{Q}[x]/f(x)$ has discriminant $\hat{p}^{n-|\lambda|}$. For fixed n and varying λ, the search for all such fields has run time roughly proportional to $p^{-|\lambda|(n-2)/4}$. As usual, we say that λ is even or odd according to the parity of its number of even parts, i.e. according to the parity of $n - |\lambda|$.

For $G = A_n$ we can naturally restrict attention to even λ. For $G = S_n$ we can restrict attention to odd λ, since the Galois fields sought contain the ramified quadratic $\mathbf{Q}(\sqrt{\hat{p}})$. Similarly for the septic group $GL_3(2)$, we need only search $\lambda = 7$, 421, 331, and 22111. Finally, the fields $\mathbf{Q}[x]/f(x)$ sought have local root numbers ϵ_∞ and ϵ_p with $\epsilon_\infty \epsilon_p = 1$; see e.g. [JR06]. One has $\epsilon_\infty = (-i)^s$ with s the number of complex places. If all parts of λ_p are odd then $\epsilon_p = 1$. Thus whenever all parts of λ_p are odd, the fields we seek are totally real; this fact reduces search times by a substantial factor in each degree.

We now describe our results in degrees 5, 6, and 7 in turn. For the purposes of the next section, the last three columns of the tables give p-ray class group information in terms of elementary divisors. For a field F, we let $\mathrm{Cl}_p^t(F)$ be the tame part of its p-ray class group. Thus $\mathrm{Cl}_p^t(\mathbf{Q})$ is cyclic of order $p-1$; in general, $\mathrm{Cl}_p^t(F)$ is finite because of the tameness condition. To focus on the information which turns out to be interesting, we define $\mathrm{cl}_p(F)$ to be the product of the 2- and 3-primary parts of $\mathrm{Cl}_p^t(F)$ and abbreviate $\mathrm{cl}_p(\mathbf{Q}) = \mathrm{cl}_p$. Further degree-specific information is given below.

The four fields in our A_5 table with $\lambda = 221$ are all in Table 1 of [BK94], which lists all non-real A_5 fields with discriminant $\leq 2083^2$. The paper [DM06], for the purposes of constructing even Galois representations of prime conductor, focuses on totally real fields with $\lambda_p = 5$, 311, and 221 under the respective assumptions that $p \equiv 1$ modulo 5, 3, and 4 respectively. It finds the first primes in these three cases to be 1951, 10267, and 13613. Thus [DM06] skips over our fields with primes 1039 and 4253 because of its congruence conditions.

Theorem 4.1. *There are exactly five A_5-p fields with $p \leq 1553$ and five S_5-p fields with $p \leq 317$ as listed below. Moreover, the minimal prime for an A_5-p field with $\lambda = 311$ is $p = 4253$.*

p	λ	s	$f_{A_5,p}(x)$	$\mathrm{cl}_p(F_5)$	$\mathrm{cl}_p(F_6)$	cl_p
653	221	2	$x^5 + 3x^3 - 6x^2 + 2x - 1$	4·3	8·2	4
1039	5	0	$x^5 - 2x^4 - 414x^3 + 4945x^2 - 16574x + 5191$	2·2·3·3	8·2·3	2·3
1061	221	2	$x^5 - x^4 - 4x^3 + 15x^2 + 32x + 16$	4·3	8·2	4
1381	221	2	$x^5 - 2x^4 + 8x^3 - 18x^2 - x - 36$	4·3·3	8·2·3	4·3
1553	221	2	$x^5 - x^3 - 6x^2 + 16x - 1$	16·9	8·4	4
⋮						
4253	311	0	$x^5 - 2x^4 - 10x^3 + 23x^2 - 6x - 4$	2·2·4·3	8·4	4

p	λ	s	$f_{S_5,p}(x)$	$\mathrm{cl}_p(F_5)$	$\mathrm{cl}_p(F_6)$	cl_p
101	32	2	$x^5 - x^4 - 6x^3 + x^2 + 18x - 4$	4·2	4·4	4
151	32	1	$x^5 - 2x^4 - x^3 + 7x^2 - 13x + 7$	2·3	8·3	2·3
269	41	2	$x^5 - x^4 - 15x^3 - 11x^2 + 11x - 10$	4	4·4	4
281	32	2	$x^5 - 2x^4 + 17x^3 - 25x^2 + 38x - 13$	8	16·2	8
317	41	2	$x^5 - 2x^4 - 14x^3 + 28x^2 + 75x - 175$	4	4·4·2	4

A Galois A_5 or S_5 field can be presented by either an irreducible quintic or sextic polynomial, with corresponding fields $F_5 = \mathbf{Q}[x]/f_5(x)$ and $F_6 = \mathbf{Q}[x]/f_6(x)$. One can pass back and forth between F_5 and F_6 through sextic twinning, as explained with examples in e.g. [JR99]. In our cases, the maps $\mathrm{Cl}_p^t(F_n) \to \mathrm{Cl}_p^t(\mathbf{Q})$ are isomorphisms on ℓ primary parts for $\ell \neq 2, 3$.

Similarly, a Galois A_6 and S_6 field corresponds to a pair of non-isomorphic sextic fields interchanged by sextic twinning. Below we give a defining polynomial for one of these fields F_6 but not its twin F_6^t. Exactly as in the quintic case, the parts of $\mathrm{Cl}_p^t(F)$ and $\mathrm{Cl}_p^t(F^t)$ not coming from $\mathrm{Cl}_p(\mathbf{Q})$ are entirely 2- and 3-primary.

A sextic A_6 or S_6 field and its twin will have the same ramification partition λ_p with the exception of the interchanges $6 \leftrightarrow 321$, $33 \leftrightarrow 3111$, $222 \leftrightarrow 21111$. The interchanges help in conducting targeted Hunter searches since one needs only search the second partition which is easier in each case.

Theorem 4.2. *There are exactly two Galois A_6-p fields with $p \leq 1677$ and seven Galois S_6-p fields with $p \leq 1423$ as listed below. Moreover, the minimal prime for an A_6-p field with $\lambda = 2211$ is $p = 3929$.*

p	λ	s	$f_{A_6,p}(x)$	$\mathrm{cl}_p(F_6)$	$\mathrm{cl}_p(F_6^t)$	cl_p
1579	42	2	$x^6 - x^5 + 41x^4 - 349x^3 + 12x^2 + 3099x + 2851$	2·3·3	2·2·3·3	2·3
1667	42	2	$x^6 - 2x^5 - 39x^4 + 60x^3 + 380x^2 + 1267x + 100$	2·3	2·2·3	2
⋮						
3929	2211	2	$x^6 - x^5 - 3x^4 + 9x^3 - 8x^2 + 2x - 1$	8·8·3	8·2·3	8

p	λ	s	$f_{S_6,p}(x)$	$\mathrm{cl}_p(F_6)$	$\mathrm{cl}_p(F_6^t)$	cl_p
197	6	2	$x^6 + 788x - 197$	4·2	4·2	4
593	321	2	$x^6 - 2x^3 - x^2 + 58x - 88$	16·2	16·2	16
929	321	2	$x^6 - 3x^5 - x^4 + 4x^3 + 56x - 32$	32·2	32·2	32
977	6	2	$x^6 - 977x^3 + 7816x^2 - 20517x + 17586$	16	16	16
1109	321	2	$x^6 - 10x^3 - 61x^2 - 41x - 218$	4·4	4	4
1301	411	2	$x^6 - 2x^5 + 5x^4 - 36x^3 - 24x^2 + 32x - 57$	4	4·2	4
1409	321	2	$x^6 - x^5 - 7x^4 - 30x^3 - 41x^2 - 177x + 191$	128	256·2·2	128

In our septic cases we give the entire tame class groups because for the second S_7 field the prime 5 also behaves non-trivially.

Theorem 4.3. *There is exactly one $GL_3(2)$-p field with $p \leq 227$ and exactly two S_7-p fields with $p \leq 191$.*

p	λ	s	$f_{GL_3(2),p}(x)$	$\mathrm{Cl}_p^t(F_7)$	$\mathrm{Cl}_p^t(F_7^t)$	$\mathrm{Cl}_p^t(\mathbf{Q})$
227	421	3	$x^7 + 2x^5 - 4x^4 - 5x^3 - 4x^2 - 3x + 10$	2·2·2·113	2·2·113	2·113

p	λ	s	$f_{S_7,p}(x)$	$\mathrm{Cl}_p^t(F_7)$		Cl_p^t
163	52	3	$x^7 - 2x^6 - 19x^4 + 65x^3 + 39x^2 + 3x + 1$	2·81		2·81
191	3211	3	$x^7 - 2x^6 + x^5 - x^4 + 3x^3 - 8x^2 + 7x - 2$	2·5·5·19		2·5·19

5 $PGL_2(7)$

The Klüners-Malle website [KM01] contains the polynomial

$$f_0(x) = x^8 - x^7 + 3x^6 - 3x^5 + 2x^4 - 2x^3 + 5x^2 + 5x + 1$$

defining a $PGL_2(7)$-53 field K_0 with octic ramification partition 611. In comparison with our previous results on first elements of $\mathcal{P}_G$ for nonsolvable G, the prime 53 is remarkably small. In fact,

Proposition 5.1 *Assuming the generalized Riemann hypothesis, K_0 is the only Galois $PGL_2(7)$-p field with $p \leq 53$.*

Proof. Let $f(x) \in \mathbf{Z}[x]$ be an octic polynomial defining a $PGL_2(7)$-p field with $p \leq 53$. We will use Odlyzko's GRH bounds [Odl76] to prove that $K = K_0$. To start, since K has degree 336, its root discriminant is at least 24.838.

We first consider the case where $p \notin \{2, 3, 7\}$ so that ramification is tame. Let λ_p be the octic ramification partition of K, and let e be the least common multiple of its parts. As λ_p must be odd and match a cycle type in $PGL_2(7)$, the possibilities are $\lambda_p = 22211$, 611, or 8. The root discriminant of K is then $p^{(e-1)/e}$ where $e = 2$, 6, or 8. Thus $p \geq 24.838^{e/(e-1)}$ which works out to $p > 616.926$,

$p > 47.221$, and $p > 39.302$ in the three cases. Thus either $e = 6$ and $p = 53$ or $e = 8$ and $p \in \{41, 43, 47, 53\}$.

Suppose for the next two paragraphs that $e = 8$. Then the p-adic field $\mathbf{Q}_p[x]/f(x)$ is a totally ramified octic extension of $\mathbf{Q}_p$ whose associated Galois group D_p is a subgroup of $PGL_2(7)$. But, a totally ramified octic extension of $\mathbf{Q}_p$ has $D_p = 8T_1$, $8T_8$, $8T_7$, or $8T_6$ depending on whether $p \equiv 1$, 3, 5, or 7 respectively modulo 8. Since $8T_8$ and $8T_7$ are not isomorphic to subgroups of $PGL_2(7)$, one must have $p \equiv \pm 1 \pmod 8$ when $e = 8$. Thus $p \in \{41, 47\}$.

If p were 41, then the compositum $K_{4,41}K$ would have degree $(336 \cdot 4)/2 = 672$ and root discriminant $41^{7/8} \approx 25.8$. But a degree 672 field has root discriminant ≥ 27.328, a contradiction proving $p \neq 41$. Similarly, if p were 47, then the compositum $K_{D_5,47}K$ would have degree $(336 \cdot 10)/2 = 1680$ and root discriminant $47^{7/8} \approx 29.05$. But a degree 1680 field has root discriminant ≥ 29.992 by [Odl76], a contradiction proving $p \neq 47$. Thus, in fact, $e \neq 8$.

Now suppose $p \in \{2, 3, 7\}$. For $p = 2$ and 3, there are a number of possibilities for the decomposition group D_p. However the maximum possible root discriminant for K would be $2^4 = 16$ and $3^{13/6} \approx 10.81$ respectively, each of which is less than 24.838. For $p = 7$, the field K is not totally real because it would contain $\mathbf{Q}(\sqrt{-7})$. So Khare's theorem [Kha06] applies, showing that there would exist a modular form of level 1 over $\overline{\mathbf{F}}_7$ associated to K. But by [Ser75], representations associated to such modular forms are reducible.

Finally, suppose K were a $PGL_2(7)$-53 extension different from K_0. Then the compositum K_0K would have degree $336^2/2 = 56448$ and so root discriminant at least 36.613 by Odlyzko's bounds. However also K_0K has root discriminant $53^{5/6} \approx 27.35$, a contradiction proving that in fact $K = K_0$. □

6 Groups of the form $2^r.G$ and $3.G$ for non-solvable G

In this section, we start from the groups G of Section 4. We use the fields there and the corresponding class group information to construct $\tilde{G}$-p fields with $\tilde{G}$ of the form $2^r.G$ and $3.G$.

Proposition 6.1 *The polynomials displayed in this section define $\tilde{G}$-p fields, with p as small as possible for the given $\tilde{G}$.*

In each case except for $\tilde{G} = 3.A_6$, there is only one Galois field corresponding to the minimal prime; for $3.A_6$ there are three, differing by cubic twists. The fields in Section 4 often give rise to the next few primes in these $\mathcal{P}_{\tilde{G}}$ as well.

For the case $\tilde{G} = 2^r.G$, we considered all the fields $F = \mathbf{Q}[x]/f(x)$ for each $f(x)$ appearing in Theorems 4.1, 4.2, and 4.3. For each such field F, we computed the quadratic extension corresponding to each order two character of $\mathrm{cl}_p(F)$. Among the defining polynomials found were

$$f^{34}_{2^4.A_5,1039}(x) = x^{10} - 149x^8 - 15640x^6 - 50311x^4 - 36993x^2 - 1369,$$
$$f^{37}_{2^4.S_5,101}(x) = x^{10} + 2px^6 - 32px^4 + p^2x^2 - p^2,$$

$$f^{285}_{2^5.S_6,197}(x) = x^{12} + 4px^8 - 4px^6 + 3p^2x^2 + 4p^2,$$
$$f^{33}_{2^3.GL_3(2),227}(x) = x^{14} + 33x^{12} + px^{10} + 3px^8 - 52px^6 - 62px^4 + p^2x^2 - p^2.$$

Here and below, subscripts indicate $\tilde{G}$ and p. Superscripts give the T-number of $\tilde{G}$ to remove ambiguities. Also we express coefficients by factoring out as many p's as possible. This makes the p-Newton polygon visible, and thus sometimes gives information about p-adic ramification. For example, $f^{37}_{2^4.S_5,101}(x)$ factors over $\mathbf{Q}_{101}$ as a totally ramified sextic times a totally ramified quartic; thus the discriminant of the given decic field is 101^8.

Necessarily, to ensure minimality in the sextic and septic cases, we also worked with the twin fields F^t, likewise using $\mathrm{cl}_p(F^t)$. Defining polynomials appearing here were

$$f^{277}_{2^5.A_6,1667}(x) = x^{12} + 341x^{10} - 303x^8 + 10158x^6 - 2998x^4 + 216x^2 + 1,$$
$$f^{286}_{2^6.A_6,1579}(x) = x^{12} - 109x^{10} + 1100x^8 + 2649x^6 - 567637x^4 + 661px^2 - 4356p,$$
$$f^{287}_{2^5.S_6,197}(x) = x^{12} + 9x^{10} - 75x^8 - 9x^6 + 3px^4 - 2px^2 + p.$$

The two degree 2^5 extensions of $K_{S_6,197}$ are disjoint. The group $14T_{33}$ is the non-split extension of $GL_3(2)$ by 2^3, to be distinguished from the semidirect product $14T_{34} \cong 8T_{48}$.

The case $\tilde{G} = 3.G$ is attractive because one can quickly understand the 3-ranks of all the class groups printed in Theorems 4.1, 4.2, and 4.3. First, if $p \equiv 1\ (3)$, the extension $K_{3,p}$ contributes 1 to the 3-rank in all three columns. Second, in the A_5 cases, the abelian extension $F_{15} \cong K^V$ over $F_5 \cong K^{A_4}$ contributes an extra 1 to the the 3-rank of $\mathrm{cl}_p(F_5)$. This accounts for the full 3-rank except in the three A_6 cases. The extra 3's printed in the columns $\mathrm{cl}_p(F_6)$ and $\mathrm{cl}_p(F_6^t)$ are all accounted for by fields with Galois group the exceptional cover $3.A_6$. Specializing the lifting results of [Rob], an A_6-p field with defining polynomial $f(x)$ embeds in a $3.A_6$-p field if and only if $\mathbf{Q}_p[x]/f(x)$ is not the product of two non-isomorphic cubic fields. This is the case for all three of our A_6 fields, and a defining polynomial for the smallest prime is

$$f_{3.A_6,1579,a}(x) = x^{18} - 6x^{17} - 23x^{16} + 211x^{15} - 283x^{14} - 115x^{13} - 2146x^{12} + 6909x^{11} - 3119x^{10} + 9687x^9 - 35475x^8 - 3061x^7 + 47135x^6 + 14267x^5 - 13368x^4 - 19592x^3 - 10421x^2 - 4728x - 297.$$

When $p \equiv 1\ (3)$, each non-obstructed field in $\mathcal{K}_{A_6,p}$ gives three fields in $\mathcal{K}_{3.A_6,p}$, differing by cubic twists. When $p \equiv 2\ (3)$, each non-obstructed field in $\mathcal{K}_{A_6,p}$ gives rise to just one field in $\mathcal{K}_{3.A_6,p}$.

There is a similar but more complicated theory of lifting from S_6 fields to $3.S_6$ fields [Rob]. The first step in our setting is to look at the 3-ranks of $\mathrm{cl}_p(F_6 \otimes \mathbf{Q}(\sqrt{\tilde{p}}))$ and $\mathrm{cl}_p(F_6^t \otimes \mathbf{Q}(\sqrt{\tilde{p}}))$. A necessary condition for the existence of a $3.S_6$ field is that both of these 3-ranks are at least 1. This occurs first for $p = 593$. Indeed there is a unique lift, with defining polynomial

$$f_{3.S_6,593}(x) = x^{18} - 4x^{17} - 15x^{16} + 131x^{15} + 50x^{14} - 2686x^{13} + 1430x^{12} + 32366x^{11} - 37880x^{10} - 282470x^9 + 672468x^8 + 2272632x^7 - 6021114x^6 - 15149054x^5 + 18548349x^4 + 59752280x^3 + 15265273x^2 - 89821887x - 96674958.$$

7 Groups of the form 2.G

Let K be a G-p field. Let $\tilde{G}$ be a non-split double cover of G. The quadratic embedding problem in our context asks whether K embeds in a $\tilde{G}$-p field $\tilde{K}$. This section is similar in nature to the last; however, degrees here are forced to be larger, and relevant class groups often cannot be computed. We replace the class group considerations with a more theoretical treatment.

Let $c \in G$ be complex conjugation, and let $\{c_1, c_2\}$ be its preimage in $\tilde{G}$. An obviously necessary condition for the existence of $\tilde{K}$ is that c_1 and c_2 both have order ≤ 2; the other possibility is that they both have order 4. For general K, there can be local obstructions not only at ∞, but also at any prime ramifying in K with even ramification index. However, in general, by the known structure of the 2-torsion in the Brauer group of $\mathbf{Q}$, the set of obstructed places is even, and there are no further global obstructions. In our one-prime context, p is obstructed exactly when ∞ is obstructed. Thus the above necessary condition is also sufficient for the existence of $\tilde{K}$.

When the embedding problem is known to be solvable, we compute defining polynomials for the quadratic overfields as follows. As usual, for K, we have the flexibility of considering defining polynomials corresponding to any subgroup H of G such that the intersection of H with its conjugates is trivial. To be able to pass to the desired overfields, we need to choose H so that the induced double cover $\tilde{H} \to H$ is split. Following e.g. Section 5.4.4 of [Coh00], we carefully choose a degree $[G : H]$ defining polynomial $f(x)$ so that the splitting field for $f(x^2)$ solves the embedding problem. If $\sqrt{\hat{p}} \in K$, then $\mathcal{K}_{\tilde{G},p}$ consists of one field, the splitting field of $f(x^2)$. If $\sqrt{\hat{p}} \notin K$, then $\mathcal{K}_{\tilde{G},p}$ consists of two fields, the splitting fields of $f(x^2)$ and $f(\hat{p}x^2)$. If one field is real and the other is imaginary, we distinguish the two by the subscripts r and i respectively; if both have the same type, we use instead a and b. A particularly simple case is when the ramification index at p is odd, i.e. when all parts of the ramification partition for $f(x)$ are odd. Then K automatically embeds into two different $\tilde{K}$.

A general construction lets one "cancel obstructions" by working in a two element group as follows. Consider two different embedding problems of our type, $(K_1, G_1, \tilde{G}_1)$ and $(K_2, G_2, \tilde{G}_2)$, with z_i the order two element in the kernel of $\tilde{G}_i \to G_i$. Let $F = K_1 \cap K_2$ with $Q = \mathrm{Gal}(F/\mathbf{Q})$. Then the Galois group of the compositum is a fiber product: $\mathrm{Gal}(K_1K_2/\mathbf{Q}) = G_1 \times_Q G_2$. One has a product embedding problem of our type $(K_1K_2, G_1 \times_Q G_2, \tilde{G}_1 *_Q \tilde{G}_2)$, where $\tilde{G}_1 *_Q \tilde{G}_2$ is the central product $(\tilde{G}_1 \times_Q \tilde{G}_2)/\langle (z_1, z_2) \rangle$. The product embedding problem is obstructed if and only if exactly one of the factor embedding problems is obstructed. We will use this construction with $(K_1, G_1, \tilde{G}_1)$ an obstructed embedding problem with non-abelian G_1, and $(K_2, G_2, \tilde{G}_2)$ the obstructed embedding problem $(K_{2^r,p}, 2^r, 2^{r+1})$ with $r = \mathrm{ord}_2(p-1)$.

In the rest of this section, we will combine the general theory just reviewed with earlier results of this paper, in particular proving the following proposition.

Proposition 7.1 *The polynomials displayed in the remaining portion of this section define $\tilde{G}$-p fields, with p as small as possible for the given $\tilde{G}$.*

In our discussion, we will also identify first primes for some other groups, without producing defining polynomials.

In general, for $n \geq 4$, the group A_n has a unique non-split double cover $\tilde{A}_n$. This double cover extends to two distinct double covers of S_n. These two double covers are distinguished by the cycle types $2^s 1^{n-s}$ of the splitting involutions: $s \equiv 0, 1\ (4)$ for $\tilde{S}_n$ and $s \equiv 0, 3\ (4)$ for $\hat{S}_n$. In the case of $n = 6$, the two double covers are interchanged by sextic twinning, reflecting the involution in conjugacy classes $222 \leftrightarrow 21111$.

In the A_4 case, the only possible ramification partition at p is 31, which yields the odd ramification index 3. Thus any A_4-p field is totally real and embeds into two $\tilde{A}_4$ fields. An S_4 field embeds in an $\tilde{S}_4$ field if and only if $s \leq 1$ and in a $\hat{S}_4$ field if and only if $s = 0$. So the first primes in these cases are 59 and 2713, by the table in Section 3. Since all elements of order 2 in S_4 lift to elements of order 4 in $\hat{S}_4$, the largest H we can take is 3. Defining polynomials are

$$f_{\tilde{A}_4,163,i}(x) = x^8 + 9x^6 + 23x^4 + 14x^2 + 1,$$

$$f_{\tilde{S}_4,59}(x) = x^8 + 7x^6 + 58x^4 - 52x^2 - 283,$$

$$\begin{aligned} f_{\hat{S}_4,2713}(x) = {} & x^{16} + 1773179px^{14} + 748029721760px^{12} + 158386491521428px^{10} \\ & + 464227394803676px^8 + 170883278708p^2x^6 + 23421860p^3x^4 + 739p^4x^2 + p^4. \end{aligned}$$

An alternative point of view on the first two fields just displayed comes from $\tilde{A}_4 \cong SL_2(3)$ and $\tilde{S}_4 \cong GL_2(3)$.

The first A_5 field in Theorem 4.1 yields the first two $\tilde{A}_5 * \tilde{4}$ fields, twists of one another at $p = 653$; the minimal degree is 48, beyond the reach of our computations. The second A_5 field and the first two S_5 fields in Theorem 4.1 yield

$$\begin{aligned} f_{\tilde{A}_5,1039,r}(x) = {} & x^{24} - 1378x^{22} + 530449x^{20} - 61379655x^{18} + 1188832770x^{16} \\ & - 9638857366x^{14} + 38717668417x^{12} - 76991153229x^{10} + 64169595698x^8 \\ & - 10073672645x^6 + 435756634x^4 - 150625x^2 + 1, \end{aligned}$$

$$\begin{aligned} f_{\tilde{S}_5 *_2 \tilde{4},101}(x) = {} & x^{24} + p(2x^{22} + 5183x^{20} + 5018386x^{18} + 1719346983x^{16} \\ & + 31145667541x^{14} + 191170958302x^{12} + 470365101611x^{10} \\ & + 19509244311x^8 - 98676327x^6 - 10345828x^4 - 139569x^2 + 121) \end{aligned}$$

$$\begin{aligned} f_{\tilde{S}_5,151}(x) = {} & x^{40} - 33x^{38} - 398x^{36} + 5788x^{34} + 180619x^{32} - 1960647x^{30} - 10306409x^{28} \\ & + 85964700x^{26} + 499284483x^{24} - 3672894736x^{22} + 3925357724x^{20} \\ & + 1667363482x^{18} + 5017492392x^{16} + 2279641280x^{14} + 1575477871x^{12} \\ & + 714220278x^{10} - 48630589x^8 - 48329892x^6 - 11843px^4 + 155px^2 - p. \end{aligned}$$

Here again, there is an alternative viewpoint: $\tilde{A}_5 \cong SL_2(5)$, and $\tilde{S}_5 *_2 \tilde{4} \cong GL_2(5)$.

From Theorem 4.2, the first p for $\tilde{A}_6 * \tilde{2}$, $\tilde{A}_6 * \tilde{4}$, and $\tilde{S}_6 \cong \hat{S}_6$ respectively are 1579, 3929, and 197. The minimal degree is 80 in each case, and corresponds to an action on $\mathbf{F}_9^2 - \{(0,0)\}$ via $\tilde{A}_6 = SL_2(9)$.

From Theorem 4.3, the first two primes for $\hat{S}_7$ are 163 and 191. Here $H =$ 7:6. and so the minimal degree is 120. The other lift $\tilde{S}_7$ has $H =$ 7:3, and so requires

the even larger degree 240; it also requires larger primes as both 163 and 191 are obstructed. The first prime for $SL_2(7) * \tilde{2}$ is 227, with defining polynomial

$$f_{SL_2(7)*\tilde{2},227}(x) = x^{32} + 351px^{30} + 9952243px^{28} + 144266253px^{26} + 45335657253px^{24} - 1671679993p^2x^{22} + 2492032310p^2x^{20} + 873353354p^2x^{18} + 37974755524p^2x^{16} + 104438863p^3x^{14} + 243444277p^3x^{12} - 91558170p^3x^{10} + 19220043p^3x^8 + 15382p^4x^6 + 2530p^4x^4 + 64p^4x^2 + p^4.$$

This polynomial was calculated in two quadratic steps, starting from an octic polynomial.

For q a prime power congruent to 3 modulo 4, a non-split quadratic lift of $PGL_2(q)$ is the group $SL_2^{\pm}(q)$ of matrices of determinant plus or minus one. From Proposition 5.1, under GRH the group $SL_2^{\pm}(7) *_2 \tilde{4}$ first appears for $p = 53$. The minimal degree is 64. Finally, consider the $PGL_2(11)$-11 field corresponding to 11-torsion points on the first elliptic curve $X_0(11)$. This field is perhaps the most classical example in the subject of number fields ramified at one prime; a defining dodecic equation can be obtained by substituting $J = -64/297$ into Equation 325a of a 1888 paper of Kiepert [Kie88]. We find that a remarkably simple equation for the $SL_2^{\pm}(11)$ quadratic overfield is

$$f_{SL_2^{\pm}(11),11}(x) = x^{24} + 90p^2x^{12} - 640p^2x^8 + 2280p^2x^6 - 512p^2x^4 + 2432px^2 - p^3.$$

8 A density conjecture

If G^{ab} is non-cyclic, then $\mathcal{K}_{G,p}$ can only be non-empty for $p = 2$. We close with a conjecture which addresses the behavior of $|\mathcal{K}_{G,p}|$ in the non-trivial case that G^{ab} is cyclic. Our conjecture is inspired by a conjecture of Malle [Mal02] which deals with fields of general discriminant, not just prime power absolute discriminant.

Conjecture 1 *Let G be a finite group with $|G| > 1$ and G^{ab} cyclic. Then the ratio $\sum_{p \le x} |\mathcal{K}_{G,p}| / \sum_{p \le x} 1$ tends to a positive limit δ_G as $x \to \infty$.*

The conjecture is certainly true if G is the cyclic group m. In fact, $\mathcal{P}_m^{\mathrm{tame}}$ is the set of primes congruent to 1 modulo m ,and so $\delta_m = 1/\phi(m)$.

Bhargava [Bha07] has a heuristic which, when transposed from general fields to fields with prime power absolute discriminant, gives a formula for δ_{S_n}. Assume $n \ge 3$ and, for the moment, $n \ne 6$ so that S_n has no non-trivial outer automorphisms. Then any Galois extension K of $\mathbf{Q}$ with Galois group S_n has a well-defined involutory partition $\lambda_\infty = 2^s 1^{n-2s}$ corresponding to complex conjugation. Similarly, if K is not wildly ramified at p then it has a well-defined partition λ_p corresponding to the tame p-adic ramification. If K is ramified at p only, then λ_p must be an odd partition. The density that Bhargava's transposed heuristic gives for S_n-p fields with the indicated invariants is

$$\delta_{S_n,s,\lambda_p} = \frac{1}{(n-2s)!s!2^{s+1}}. \tag{8.1}$$

Here $1/((n-2s)!s!2^s)$ is the fraction of elements in S_n with cycle type 2^s1^{n-2s}. The extra factor of 2 in the denominator of (8.1) can be thought of as coming from the global root number condition $\epsilon_\infty\epsilon_p = 1$. Note that the right side of (8.1) is independent of λ_p.

Summing over the possible s and then multiplying by the number of possible λ_p gives the conjectured value for δ_{S_n}. For $n = 6$, all these considerations would go through without change if we were working with isomorphism classes of sextic fields. However, we have placed the focus on Galois fields, and there is one Galois field for each twin pair of sextic fields. Accordingly, we need to divide the right side of (8.1) by 2. The final conjectured values in degrees ≤ 7 are then

n	3	4	5	6	7
δ_{S_n}	$0.\overline{3}$	$0.41\overline{6}$	0.325	$0.1319\overline{4}$	$0.16\overline{1}$

Bhargava's heuristic can be recast more group-theoretically to give a conjectural formula for δ_G for arbitrary G. For length two solvable groups $G = \ell^r{:}G^{\mathrm{ab}}$, the δ_G one obtains is the same as that given by the Cohen-Lenstra heuristics applied to the ℓ part of class groups of fields of the form $K_{G^{\mathrm{ab}},p}$. Thus we expect e.g. $\delta_{A_4} = 1/8$ and hence, by automatic lifting and twisting as described in the previous section, $\delta_{\tilde{A}_4} = 1/4$.

The computations in [tRW03] for S_3-p fields for several billion primes are strongly supportive of Cohen-Lenstra heuristics in this setting, and hence our expectation $\delta_{S_3} = 1/3$. We have carried out similar computations for S_4-p fields for the first 10^6 primes ≥ 5:

	S_3		S_4					
(s,λ)	$(0,21)$	$(1,21)$	$(0,211)$	$(1,211)$	$(2,211)$	$(0,4)$	$(1,4)$	$(2,4)$
10^2	.02	.21	0	.03	.02	0	.12	.02
10^3	.050	.193	.002	.056	.031	.013	.077	.034
10^4	.0634	.2080	.0080	.0698	.0399	.0161	.0965	.0462
10^5	.06911	.22714	.01047	.08589	.04567	.01676	.10525	.04837
10^6	.073965	.234667	.013471	.097131	.050874	.018186	.111884	.052834
∞	$.08\overline{3}$	.25	$.0208\overline{3}$	.125	.0625	$.0208\overline{3}$	.125	.0625

Our S_4 data roughly tracks the slowly convergent S_3 data. There are more fields with $\lambda_p = 4$ than with $\lambda_p = 211$, corresponding to the asymmetry noted in Section 3; we expect this discrepancy to go away in the limit. For each λ_p, the dependence on s already agrees well with the expected limiting ratios $1 : 6 : 3$.

For $n = 5$ through 7, our very small initial segments of $\mathcal{P}_G$ all have smaller density than our conjectured value of δ_{S_n}. This is to be expected, given the behavior for $n = 3$ and 4. However, our determination of first primes 59, 101, 197, 163 at least reflects our expectation $\delta_{S_4} > \delta_{S_5} > \delta_{S_6} < \delta_{S_7}$, including the perhaps surprising inequality $\delta_{S_6} < \delta_{S_7}$.

References

[Bel04] Karim Belabas. On quadratic fields with large 3-rank. *Math. Comp.*, 73(248):2061–2074 (electronic), 2004.

[Bha07] Manjul Bhargava. Mass Formulae for Extensions of Local Fields, and Conjectures on the Density of Number Field Discriminants. *Int Math Res Notices*, 2007(rnm052):rnm052–20, 2007.

[BK94] Jacques Basmaji and Ian Kiming. A table of A_5-fields. In *On Artin's conjecture for odd 2-dimensional representations*, volume 1585 of *Lecture Notes in Math.*, pages 37–46, 122–141. Springer, Berlin, 1994.

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

[DM06] Darrin Doud and Michael W. Moore. Even icosahedral Galois representations of prime conductor. *J. Number Theory*, 118(1):62–70, 2006.

[Har94] David Harbater. Galois groups with prescribed ramification. In *Arithmetic geometry (Tempe, AZ, 1993)*, volume 174 of *Contemp. Math.*, pages 35–60. Amer. Math. Soc., Providence, RI, 1994.

[Hoe07] Jing Long Hoelscher. *Galois extensions ramified at one prime*. PhD thesis, University of Pennsylvania, 2007.

[JR99] John W. Jones and David P. Roberts. Sextic number fields with discriminant $(-1)^j 2^a 3^b$. In *Number theory (Ottawa, ON, 1996)*, volume 19 of *CRM Proc. Lecture Notes*, pages 141–172. Amer. Math. Soc., Providence, RI, 1999.

[JR03] John W. Jones and David P. Roberts. Septic fields with discriminant $\pm 2^a 3^b$. *Math. Comp.*, 72(244):1975–1985 (electronic), 2003.

[JR06] John W. Jones and David P. Roberts. A database of local fields. *J. Symbolic Comput.*, 41(1):80–97, 2006.

[Kha06] Chandrashekhar Khare. Serre's modularity conjecture: the level one case. *Duke Math. J.*, 134(3):557–589, 2006.

[Kie88] L. Kiepert. Ueber die Transformation der elliptischen Functionen bei zusammengesetztem Transformationsgrade. *Math. Ann.*, 32(1):1–135, 1888.

[KM01] Jürgen Klüners and Gunter Malle. A database for field extensions of the rationals. *LMS J. Comput. Math.*, 4:182–196 (electronic), 2001.

[Mal02] Gunter Malle. On the distribution of Galois groups. *J. Number Theory*, 92(2):315–329, 2002.

[Odl76] Andrew Odlyzko. Table 2: Unconditional bounds for discriminants. `http://www.dtc.umn.edu/~odlyzko/unpublished/discr.bound.table2`, 1976.

[PAR06] The PARI Group, Bordeaux. *PARI/GP, Version 2.3.2*, 2006.

[Rob] David P. Roberts. 3.G number fields for sextic and septic groups G. In preparation.

[SD73] H. P. F. Swinnerton-Dyer. On l-adic representations and congruences for coefficients of modular forms. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972)*, pages 1–55. Lecture Notes in Math., Vol. 350. Springer, Berlin, 1973.

[Ser75] Jean-Pierre Serre. Valeurs propres des opérateurs de Hecke modulo l. In *Journées Arithmétiques de Bordeaux (Conf., Univ. Bordeaux, 1974)*, pages 109–117. Astérisque, Nos. 24–25. Soc. Math. France, Paris, 1975.

[tRW03] Herman te Riele and Hugh Williams. New computations concerning the Cohen-Lenstra heuristics. *Experiment. Math.*, 12(1):99–113, 2003.