WILD RAMIFICATION BOUNDS AND SIMPLE GROUP GALOIS EXTENSIONS RAMIFIED ONLY AT 2

JOHN W. JONES

ABSTRACT. We consider finite Galois extensions of $\mathbf{Q}_p$ and deduce bounds on the discriminant of such an extension based on the structure of its Galois group. We then apply these bounds to show that there are no Galois extensions of $\mathbf{Q}$, unramified outside of $\{2, \infty\}$, whose Galois group is one of various finite simple groups. The set of excluded finite simple groups includes several infinite families.

Understanding the Galois extensions of $\mathbf{Q}$ in terms of their Galois groups and sets of ramifying primes is one of the central goals of algebraic number theory. Here, we consider the problem from the perspective of severely limiting the set of ramifying primes and trying to understand what Galois extensions and Galois groups can then occur.

Let $\mathcal{K}_2$ be the set of finite Galois extensions of $\mathbf{Q}$ in $\mathbf{C}$ which are unramified outside of the set $\{2, \infty\}$, and let $\mathcal{G}_2 := \{\mathrm{Gal}(K/\mathbf{Q}) \mid K \in \mathcal{K}_2\}$. The sets $\mathcal{K}_2$ and $\mathcal{G}_2$ have been studied in several papers [Tat94, Har94, Bru01, Les, Mar63, Moo07, Jon]. One can restrict ramification even further and consider $\mathcal{K}_2^+$, the set of totally real fields in $\mathcal{K}_2$ and $\mathcal{G}_2^+ = \{\mathrm{Gal}(K/\mathbf{Q}) \mid K \in \mathcal{K}_2^+\}$. Relatively few examples are known of groups in $\mathcal{G}_2$, and fewer in $\mathcal{G}_2^+$. The case of 2-groups is fully understood by [Mar63]. The smallest non-2-group in $\mathcal{G}_2$ is $C_{17} : C_{16}$ [Har94], and recently, Dembélé [Dem09] has shown that $\mathcal{G}_2$ contains the non-solvable group, $SL_2(2^8)^2.C_8$.

We consider non-abelian finite simple groups and prove that in many cases, the group in question is either not in $\mathcal{G}_2$ or in $\mathcal{G}_2^+$. We focus on simple groups for two reasons. Much of the work in the area of studying extensions with restricted ramification makes use of class field theory, and non-abelian simple groups force us to develop and use other techniques. More importantly, any extension $K \in \mathcal{K}_2$ can be viewed as a tower of Galois extensions where each step has Galois group being a simple group. The first step then comes from a simple group in $\mathcal{G}_2$. In all known examples of $K \in \mathcal{K}_2$, this simple group is C_2, the cyclic group of order 2. So, it is natural to ask which, if any, non-abelian simple groups are in $\mathcal{G}_2$.

We will prove that various groups are not in $\mathcal{G}_2$ or $\mathcal{G}_2^+$ by discriminant bound arguments. We will make use of known bounds for root discriminants of number fields as developed by of Odlyzko, Serre, et.al.[Odl90, Ser86], and known techniques for computing similar bounds. Our principle objective then is to derive upper bounds on the contribution of a prime p to the discriminant of a Galois field based on the Galois group of the extension.

In Section 1, we review some background on higher ramification groups and the slope content of an extension. Section 2.1 defines the composita indices of a finite p-group, and shows how to use them to derive discriminant bounds. The work most

2010 *Mathematics Subject Classification.* Primary 11R21, 11S15.

similar to this in the literature are papers of Moon [Moo00] and Tate [Tat94], and Section 2.2 relates the methods and bounds here to those found in those papers.

While Sections 1 and 2 consider local number fields, Section 3 describes the process of deducing global discriminant bounds, and applies it to extensions $K/\mathbf{Q}$ where $2^4 \parallel [K:\mathbf{Q}]$. As an application, it considers the following. In [Har94], it is shown that the smallest extension in $\mathcal{K}_2$ whose degree is not a power or 2 has degree 272 and that there is a unique such extension of that degree. In Section 3, we show that the Generalized Riemann Hypothesis implies that this extension is even more special, being the unique extension in $K \in \mathcal{K}_2$ where $[K:\mathbf{Q}]$ is not a power of 2 and not a multiple of 32. Finally in Section 4, we deduce that various finite simple groups are not in $\mathcal{G}_2$ or not in $\mathcal{G}_2^+$. In particular, we show that GRH implies that there if $G \in \mathcal{G}_2$ is a non-abelian simple group, then $|G| > 1{,}000{,}000$.

1. Background on slope content and ramification groups

Here we provide some background on slope content. Throughout, we will use the numbering of [Ser79] for higher ramification groups and [JR06, JR99, JR03] for slopes.

1.1. **Slope content for Galois extensions.**

Let F be a finite Galois extension of $\mathbf{Q}_p$ with Galois group G. Let G^i denote the filtration on G of higher ramification groups in upper numbering $i \geq -1$ as in [Ser79]. For each index i, we let $G^{i+} := \cup_{\epsilon>0} G^{i+\epsilon}$. An index i is a jump in the filtration if $G^i \supsetneqq G^{i+}$. If we write the discriminant of $F/\mathbf{Q}_p$ as (p^{c_F}), then we have

$$c_F = \sum_{i\geq -1} ([G:G^{i+}] - [G:G^i])(i+1)\,. \tag{1}$$

The sum can be thought of as being over the finitely many jumps i, as these are the only non-zero terms. If i is a jump in the filtration of higher ramification groups of G, then we refer to $s = i+1$ as a slope for $F/\mathbf{Q}_p$. For a geometric interpretation of slopes, see [JR06].

For each slope, we consider the relative index $[G^{s-1} : G^{(s-1)+}]$. Unramified subextensions correspond to slope $s = 0$ (i.e., $i = -1$). We let $u := [G^{-1} : G^{(-1)+}] = [G : G^0]$, the degree of the maximum unramified subfield for $F/\mathbf{Q}_p$. Similarly, for slope $s = 1$ we let $t := [G^0 : G^{0+}] = [G^0 : G^1]$ as this is the degree of the maximal tamely totally ramified subextension within $F/\mathbf{Q}_p$. All other slopes are larger than 1 and correspond to the wild ramification subgroup, $W := G^1$, which is a p-group.

A slope $s > 1$ is a wild slope and define its multiplicity m by $[G^{s-1} : G^{(s-1)+}] = p^m$. We then define the slope content, $\mathrm{SC}(F/\mathbf{Q}_p)$, to be $[s_1, s_2, \ldots, s_k]_t^u$ where t and u are as defined above, and the s_i are slopes greater than 1 listed so that $s_i \leq s_{i+1}$ and each slope s is repeated m times where m is the multiplicity described above. With these conventions, equation (1) becomes

$$c_F = u(t-1) + ut \sum_{j=1}^{k} (p^j - p^{j-1}) s_j\,. \tag{2}$$

With an eye toward root discriminants, we define the mean slope of $F/\mathbf{Q}_p$ by

$$\mathrm{MS}(F) := \frac{c_F}{[F\colon \mathbf{Q}_p]} = \frac{t-1}{p^k t} + \sum_{j=1}^{k} \left(\frac{1}{p^{k-j}} - \frac{1}{p^{k-j+1}} \right) s_j \,. \tag{3}$$

Since equation (3) does not involve the unramified degree u, so we will omit u from the notation for slope content $\alpha = [s_1, \dots, s_k]_t$.

1.2. **Slope content for subfields.** Let E be a finite extension of $\mathbf{Q}_p$. Then we can pick a finite Galois exension $F/\mathbf{Q}_p$ with $E \subseteq F$, and let $G = \mathrm{Gal}(F/\mathbf{Q}_p)$. Then for $H = \mathrm{Gal}(F/E) \le G$, we have $E = F^H$, the fixed field of H. Then we define the slope content of $E/\mathbf{Q}_p$ by considering the subgroups HG^i and HG^{i+} in place of G^i and G^{i+} respectively. In particular, we let $u = [G : HG^0]$, $t = [HG^0 : HG^1]$, and a slope $s > 1$ has multiplicity m if $p^m = [HG^{s-1} : HG^{(s-1)+}]$. Note, we still have that if the discriminant of $E/\mathbf{Q}_p$ is (p^{c_E}) and $\mathrm{SC}(E/\mathbf{Q}_p) = [s_1, s_2, \dots, s_k]_t^u$,

$$c_E = \sum_s ([G : HG^{(s-1)+}] - [G : HG^{s-1}])s = u(t-1) + ut \sum_{j=1}^{k} (p^j - p^{j-1}) s_j \,. \tag{4}$$

This definition of slope content for $E/\mathbf{Q}_p$ is consistent with the one above in the case where H is a normal subgroup of G. It does not depend on the choice of a Galois extension of $\mathbf{Q}_p$ containing E by Herbrand's theorem.

As above, we can extend the definition of mean slope to a possibly non-Galois extension E by

$$\mathrm{MS}(E) := \frac{c_E}{[E\colon \mathbf{Q}_p]} = \frac{t-1}{p^k t} + \sum_{j=1}^{k} \left(\frac{1}{p^{k-j}} - \frac{1}{p^{k-j+1}} \right) s_j \,. \tag{5}$$

As in the Galois case, the unramified degree u is not needed. Also, $\mathrm{MS}(E)$ is a function of only $SC(E/\mathbf{Q}_p)$. So, for a slope content $\alpha = [s_1, \dots, s_k]_t^u$, so we may write $\mathrm{MS}(\alpha)$.

Remark 1.1. If $\mathbf{Q}_p \subseteq E \subseteq E'$ are finite extensions and we embed E' in a finite Galois extension of $\mathbf{Q}_p$ with Galois group G, then E and E' correspond to subgroups of the Galois group, H and H' respectively. Then $H' \le H$ and so for all $i \ge -1$, $[HG^i : HG^{i+}] \le [H'G^i : H'G^{i+}]$. So, the multiplicity of a given slope $s > 1$ for E is less than or equal to its multiplicity for E'.

There is a simple partial ordering on the set of slope contents.

Definition 1.1. *For two slope contents $\alpha = [s_1, \dots, s_k]_t$ and $\alpha' = [s'_1, \dots, s'_n]_{t'}$, we say that α is* bounded by *α' and write $\alpha \le \alpha'$ if the following three conditions hold:*

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

It is easy to deduce the following from equation (3).

Proposition 1.2. *If α and α' are slope contents with $\alpha \le \alpha'$, then* $\mathrm{MS}(\alpha) \le \mathrm{MS}(\alpha')$.

1.3. **Composita.** Suppose $F_j \subseteq \overline{\mathbf{Q}}_p$ for $j = 1, \ldots, m$ are finite extensions of $\mathbf{Q}_p$. Proposition 1.3 below bounds the slope content of the compositum $F_1 \cdots F_m$ in terms of the slope contents of the F_j. First, a definition.

Definition 1.2. *Given two slope contents $\alpha = [s_1, \ldots, s_k]_t$ and $\alpha' = [s'_1, \ldots, s'_n]_{t'}$, their disjoint union $\alpha_1 \mathbin{\dot\cup} \alpha_2$ is the slope content with wild slopes being the list $s_1, \ldots, s_k, s'_1, \ldots, s'_n$ after being sorted, and tame degree equal to tt'.*

This extends in the obvious way to the disjoint union of a finite number of slope contents.

Proposition 1.3. *If $F_1, \ldots, F_m$ are finite extensions of $\mathbf{Q}_p$, then*

$$\mathrm{SC}(F_1 \cdots F_m) \leq \dot{\bigcup_i} \mathrm{SC}(F_i)$$

Proof. Let F be the Galois closure of the compositum $F_1 \cdots F_m$, and $G = \mathrm{Gal}(F/\mathbf{Q}_p)$. Then the fields F_j correspond to subgroups $H_j \leq G$, and $F_1 \cdots F_m$ is the fixed field of $\cap_{j=1}^m H_j$. Using that the higher ramification groups G^i are normal in G, it is easy to check that for all i,

$$\left[\left(\bigcap_{j=1}^m H_j\right) G^i : \bigcap_{j=1}^m H_j\right] \leq \prod_{j=1}^m [H_j G^i : H_j]. \tag{6}$$

For a slope content $\alpha = [s_1, \ldots, s_k]_t^u$ and a constant $C > 1$, let $m_C(\alpha)$ be the number of slopes $s_i \geq C$. For a field F_j, $p^{m_C(\mathrm{SC}(F_j))} = [H_j G^{C-1} : H_j]$. Thus, equation (6) gives for $C > 1$,

$$m_C(\mathrm{SC}(F_1 \cdots F_m)) \leq \sum_{j=1}^m m_C(\mathrm{SC}(F_j)).$$

Let $\mathrm{SC}(F_1 \cdots F_m) = [s_1, \ldots, s_k]_t$ and $\dot\cup_i \mathrm{SC}(F_i) = [s'_1, \ldots, s'_n]_{t'}$. Then for all $C > 1$ we have that the number of slopes in $[s_1, \ldots, s_k]_t$ which are $\geq C$ is less than or equal to the corresponding number of slopes for $[s'_1, \ldots, s'_n]_{t'}$. This gives conditions (1) and (2) of Definition 1.1. Then, applying equation (6) with $i = 0$ gives $p^k t \leq p^n t'$, which gives the last condition. $\square$

Example 1.4. An example where condition 3 of Definition 1.1 comes into play is given by $f = x^5 + 5x^3 + 5$ over $\mathbf{Q}_5$. This polynomial has Galois group $F_5 \cong C_5 : C_4$. If we pick two different roots of f, they each define fields with slope content $[7/4]_1$. However, their compositum is the splitting field which has slope content $[7/4]_4$, which is bounded by $[7/4]_1 \mathbin{\dot\cup} [7/4]_1 = [7/4, 7/4]_1$ in accordance with Prop. 1.3.

1.4. **Towers of fields.** When bounding slope content, it is often useful to proceed up a tower of fields. At a given step, we may know the slope content of a given extension, $\mathrm{SC}(F) = [s_1, \ldots, s_k]_t$, and want a bound on the slope content of a degree p-extension of F.

Proposition 1.5. *If F is a finite extension of $\mathbf{Q}_p$ with $\mathrm{SC}(F) = [s_1, \ldots, s_k]_t$, and F' is a degree p extension of F, then $\mathrm{SC}(F')$ is bounded by $[s_1, \ldots, s_k, s_{k+1}]_t$ where*

$$s_{k+1} = 1 + \frac{1}{p-1} + \frac{1}{p^k} + \frac{1}{p^k} \sum_{j=1}^k (p^j - p^{j-1}) s_j = \mathrm{MS}(F) + \frac{p}{p-1} + \frac{1}{p^k t}$$

Proof. Let u be the unramified degree of $F/\mathbf{Q}_p$. Note, if F'/F is unramified, the result trivially holds. So, assume F'/F is totally ramified, and is hence wildly ramified since it has degree p. By equation (4), we have

$$c_F = u(t-1) + ut\sum_{j=1}^{k}(p^j - p^{j-1})s_j$$

and then [Jon, Lemma 1.3] tells us that

$$c_{F'} \le pc_F + u(p-1+p^{k+1}t)\,.$$

Defining s_{k+1} to be the slope for F'/F using the upper bound, we have

$$\begin{aligned} s_{k+1} &= \frac{c_{F'} - c_F}{p^{k+1}ut - p^k ut} \\ &= \frac{pc_F + u(p-1+p^{k+1}t) - c_F}{p^k ut(p-1)} \\ &= \frac{(p-1)c_F + u(p-1) + up^{k+1}t}{p^k ut(p-1)} \\ &= \frac{c_F + u}{p^k ut} + \frac{p}{(p-1)} \\ &= \frac{u(t-1) + ut\left(\sum_{j=1}^{k}(p^j - p^{j-1})s_j\right) + u}{p^k ut} + 1 + \frac{1}{p-1} \\ &= 1 + \frac{1}{p-1} + \frac{t + t\sum_{j=1}^{k}(p^j - p^{j-1})s_j}{p^k t} \\ &= 1 + \frac{1}{p-1} + \frac{1}{p^k} + \frac{1}{p^k}\sum_{j=1}^{k}(p^j - p^{j-1})s_j \end{aligned}$$

This in turn easily simplifies to $\mathrm{MS}(F) + \frac{p}{p-1} + \frac{1}{p^k t}$.

Finally, we note that from Remark 1.1, the slope content for F' contains the slope content for F. Moreover, the additional factor of p for $[F' : \mathbf{Q}_p]$ corresponds to a slope s. The quantity $\frac{c_{F'} - c_F}{[F':\mathbf{Q}_p]-[F:\mathbf{Q}_p]}$ equals s iff $s \ge s_k$; otherwise, $\frac{c_{F'} - c_F}{[F':\mathbf{Q}_p]-[F:\mathbf{Q}_p]}$ is a weighted average of slopes all $\le s_k$. So, in all cases, the additional slope $s \le s_{k+1}$ computed above. ☐

2. Discriminant bounds from group structures

In this section we consider two filtrations on finite p-groups. Each can be applied to the Sylow p-subgroup of the Galois group of an extension $F/\mathbf{Q}_p$ to give upper bounds on the extension's mean slope.

Section 2.1 gives the first construct, and contains the main new ideas of this paper. Then Section 2.2 describes a construct due to Moon. We recast it in the framework used here for comparison with our approach and to make it easier to apply in subsequent sections.

2.1. **Composita indices.** Let G is a finite p-group, and define

$$L_k(G) := \bigcap_{[G:H]=p^k} H\,,$$

the intersection of all subgroups of index p^k. It is easy to see that each $L_k(G)$ is a normal subgroup of G, $L_0(G) = G$, and $L_1(G) = \Phi(G)$, the Frattini subgroup of G. Moreover, we have a series

$$\langle e\rangle = L_m(G) \leq L_{m-1}(G) \leq \cdots \leq L_1(G) \leq L_0(G) = G$$

for some $m \geq 0$. Note, for our purpose, the indexing of the series is important, not just which subgroups appear. One final basic property which will of use later is that

$$H \leq G \implies L_i(H) \leq L_i(G) \quad \text{for all } i. \tag{7}$$

Fix m to the the smallest index where $L_m(G) = \langle e\rangle$ and we let i_j be such that $p^{i_j} = [L_{j-1}(G) : L_j(G)]$. We refer the the vector $[i_1, i_2, \ldots, i_m]$ as the *compositum indices* of G. Clearly, $|G| = p^{\sum_j i_j}$.

Example 2.1. Consider the two non-abelian groups of order 8. For the dihedral group D_4, the series is $\langle e\rangle \leq \{e, R^2\} \leq D_4$, so the compositum indices are $[2, 1]$. On the other hand, for the quaternion group, Q_8, we have $\langle e\rangle \leq \{\pm 1\} \leq \{\pm 1\} \leq Q_8$, so the compositum indices are $[2, 0, 1]$.

We now come to the main theorem, which provides a link between composita indices and slope content, and in turn bounds the mean slope of an extension.

Theorem 2.2. *Suppose F is a finite Galois extension of $\mathbf{Q}_p$ with Galois group G. Let I and W be the inertia and wild ramification groups respectively, and $t = [I : W]$. If W has compositum indices $[i_1, \ldots, i_m]$, then the slope content for $F/\mathbf{Q}_p$ is bounded by a slope content consisting of tame index t and distinct slopes $1 + \frac{p}{p-1}$, $2 + \frac{p}{p-1}$, $\ldots$, $m + \frac{p}{p-1}$, where each slope $j + \frac{p}{p-1}$ is repeated with multiplicity i_j. Moreover, if we let $a_i = \sum_{j=0}^{i-1} i_{m-j}$, then*

$$\mathrm{MS}(F) \leq m + 1 + \frac{1}{p-1}\left(1 - \frac{1}{p^{a_m}}\right) - \sum_{i=1}^{m} \frac{1}{p^{a_i}} - \frac{1}{p^{a_m} t}$$

Proof. Denote the fixed field of W by F^W. A degree p^k extensions of F^W correspond to an index p^k subgroups of W by the Galois correspondence. Hence, their compositum corresponds to $L_k(W)$.

Now, the maximum slope for a degree p^k extension of F^W is $k + \frac{p}{p-1}$ by [Jon, Lemma 1.3]. By Proposition 1.3, their compositum then also has no slopes greater than $k + \frac{p}{p-1}$. So, if $[W : L_k(W)] = p^{a_k}$, then $F/\mathbf{Q}_p$ has at most a_k slopes strictly greater than $k + \frac{p}{p-1}$. If m is the smallest positive integer such that $L_m(W) = \langle e\rangle$, we have that all a_m wild slopes are bounded above by $m + \frac{p}{p-1}$. Of those, at least a_{m-1} are bounded above by $m - 1 + \frac{p}{p-1}$. Proceeding inductively, at each stage get at least i_k slopes less than or equal to $k + \frac{p}{p-1}$ since

$$i_k = \log_p([L_{k-1}(W) : L_k(W)]) = a_k - a_{k-1}\,.$$

For the bound on $\mathrm{MS}(F)$, we start with equation (3) and substitute our values for the slopes. Terms of the main sum with the same wild slope can be grouped together, giving the following.

$$\begin{aligned}
\mathrm{MS}(F) &\leq \sum_{j=1}^{m}\left(\frac{1}{p^{a_{j-1}}}-\frac{1}{p^{a_j}}\right)\left(m+1-j+\frac{p}{p-1}\right)+\frac{t-1}{p^{a_m}t}\\
&=\sum_{j=1}^{m}\left(\frac{1}{p^{a_{j-1}}}-\frac{1}{p^{a_j}}\right)(m+1-j)+\frac{p}{p-1}\sum_{j=1}^{m}\left(\frac{1}{p^{a_{j-1}}}-\frac{1}{p^{a_j}}\right)+\frac{t-1}{p^{a_m}t}\\
&=\sum_{j=1}^{m}\left(\frac{1}{p^{a_{j-1}}}-\frac{1}{p^{a_j}}\right)(m+1-j)+\frac{p}{p-1}\left(1-\frac{1}{p^{a_m}}\right)+\frac{t-1}{p^{a_m}t}
\end{aligned}$$

Here, the second sum telescopes. We use summation by parts on the remaining sum:

$$\mathrm{MS}(F) \leq \frac{p}{p-1}\left(1-\frac{1}{p^{a_m}}\right)+m-\sum_{j=1}^{m}\frac{1}{p^{a_j}}+\frac{t-1}{p^{a_m}t}$$

The result then follows since

$$\frac{p}{p-1}\left(1-\frac{1}{p^{a_m}}\right)+\frac{t-1}{p^{a_m}t}=1+\frac{p}{p-1}\left(1-\frac{1}{p^{a_m}}\right)-\frac{1}{p^{a_m}t}.$$

□

2.2. **Frattini indices.** For a finite p-group G, we can define another normal series using Frattini subgroups. let $\Phi_0(G) = G$ and $\Phi_i(G) = \Phi(\Phi_{i-1}(G))$ for $i > 0$. We refer to this series as the *Frattini filtration* of G. If N is the smallest index such that $\Phi_N(G) = \langle e\rangle$, then N is the p-length of G. For $1 \leq i < N$, let $p^{m_i} = [\Phi_i(G) : \Phi_{i+1}(G)]$; we define $[m_1, \ldots, m_N]$ to be the *Frattini indices* of G.

Let F be a finite Galois extension of $\mathbf{Q}_p$, and let H_p be the Sylow p-subgroup of $\mathrm{Gal}(F/\mathbf{Q}_p)$. In [Moo00], Moon derives a bound on the exponent of a prime p in the discriminant of a Galois extension based on the Frattini filtration of H_p. Proposition 2.3 below is a version of [Moo00, Lemma 2.3]. They are equivalent when $p - 1 \mid t$, the tame degree, which is always the case when $p = 2$. Otherwise, Moon's version is slightly sharper. Moon uses class field theory to prove [Moo00, Lemma 2.3], but we include a proof of Proposition 2.3 to see how it can be proved using the slope formalism discussed in Section 1.

Proposition 2.3 (Moon)**.** *Let F be a finite Galois extension of $\mathbf{Q}_p$ with ramification index e and whose wild ramification group has Frattini indices $[m_1, \ldots, m_N]$. Then*

$$\mathrm{MS}(F) \leq \frac{p}{p-1}\left(N-\sum_{i=1}^{N}\frac{1}{p^{m_i}}\right)+1-\frac{1}{e} \tag{8}$$

In comparing the statement with Theorem 2.2 we note that the final terms $\frac{1}{e}$ and $\frac{1}{p^{a_m}t}$ are equal, but expressed in different ways.

Proof. Let H_p be a Sylow p-subgroup of the wild ramification subgroup of $\mathrm{Gal}(F/\mathbf{Q}_p)$, and F_j be the fixed field of $\Phi_j(H_p)$. Let t and u be the tame and unramified degrees for $F/\mathbf{Q}_p$ as usual. Noting that $\mathrm{MS}(F_0) = \frac{t-1}{t} = 1 - 1/t$, we induct on j.

A p-extension of F_{j-1} has slope bounded by $s = \mathrm{MS}(F_{j-1}) + \frac{p}{p-1} + \frac{1}{e_{j-1}}$ by Proposition 1.5, where e_i will denote the ramification degree of $F_i/\mathbf{Q}_p$. By Proposition 1.3, the compositum of m_j different p-extensions contributes at most m_j

slopes all bounded by s. So, by equation (3),

$$\begin{aligned}
\mathrm{MS}(F_j) &\le \frac{1}{p^{m_j}}\mathrm{MS}(F_{j-1}) + s\left(1-\frac{1}{p^{m_j}}\right)\\
&= \frac{1}{p^{m_j}}\mathrm{MS}(F_{j-1}) + \left(\mathrm{MS}(F_{j-1}) + \frac{p}{p-1} + \frac{1}{e_{j-1}}\right)\left(1-\frac{1}{p^{m_j}}\right)\\
&= \mathrm{MS}(F_{j-1}) + \left(\frac{p}{p-1} + \frac{1}{e_{j-1}}\right)\left(1-\frac{1}{p^{m_j}}\right)\\
&\le \frac{p}{p-1}\left(j-1-\sum_{i=1}^{j-1}\frac{1}{p^{m_i}}\right) + 1 - \frac{1}{e_{j-1}} + \left(\frac{p}{p-1} + \frac{1}{e_{j-1}}\right)\left(1-\frac{1}{p^{m_j}}\right)\\
&= \frac{p}{p-1}\left(j-\sum_{i=1}^{j}\frac{1}{p^{m_i}}\right) + 1 - \frac{1}{e_j}
\end{aligned}$$

In the last line we use that $e_j = p^{m_j}e_{j-1}$ from the fact that F_j/F_{j-1} is totally ramified of degree p^{m_j}. □

In [Moo00], Moon also gives the following simpler, but weaker bound.

Corollary 2.4 (Moon)**.** *If G has p-length N, then*

$$\mathrm{MS}(K) < 1 + \frac{p}{p-1}N$$

This can be deduced readily from Proposition 2.3 (or, of course, the lemma stated in [Moo00]). However, there is a second interpretation of this bound in terms of slopes. In the proof of Proposition 2.3, we saw that the top slope of the extension is bounded by

$$1 + \frac{p}{p-1}\left(N - \sum_{i=1}^{N-1}\frac{1}{p^{m_i}}\right) < 1 + N + \frac{N}{p-1}$$

Since $\mathrm{MS}(F)$ is a weighted average of its slopes, it is bounded above by its top slope.

2.3. **Comparison.** Here we compare the discriminant bounds deduced from composita indices and Frattini indices, and relate both to a bound of Tate. Throughout, let H be a p-group, which will represent the wild ramification group for a finite Galois extension of $\mathbf{Q}_p$.

There are two simple cases where Frattini and composita indices always give the same bound, namely when H is cyclic, $H \cong C_{p^n}$, and when H is elementary abelian, $H \cong C_p^n$. In the cyclic case, both the composita and Frattini indices are $[1, 1, \dots, 1]$ and the bound on the mean slope is $n + 1 - \frac{1}{p^n t}$. This upper bound is met using a cyclotomic extension of a tame extension of $\mathbf{Q}_p$, so the bound here is sharp. Frattini indices and composita indices give lower discriminant bounds for other groups. So, a priori bounds which do not take into account the group structure of H will not be as sharp as those coming from Frattini and composita indices since they must allow for this case.

When $H \cong C_p^n$, both composita and Frattini indices are $[n]$ and the mean slope bound is $1 + \frac{p}{p-1}(1 - \frac{1}{p^n}) - \frac{1}{p^n t}$. It is not surprising that the two approaches agree here. Both Moon's approach and this paper were inspired by attempts to generalize Tate's work in [Tat94]. In that case, the Sylow 2-subgroup of $PSL_2(2^j)$

is elementary abelian, so the maximum slope is 3. Tate also shows that the tame degree must be 1, which in turn can be used to show that all slopes are either 2 or 3, and that at most one of them is 3. Feeding this information into equation (3) gives a bound on the mean slope of $\frac{5}{2} - \frac{1}{2^{n-1}}$ where the $H = C_2^n$.

To compare Frattini indices and composita indices for small p-groups, we consider the three groups of order 8, other than C_2^3 and C_8. They have the same Frattini indices, $[2, 1]$, whereas we saw above that the composita indices are $[2, 0, 1]$ for Q_8 and $[2, 1]$ for D_4 and $C_4 \times C_2$. The bounds on mean slope for $p = 2$ are as follows. Using Frattini indices, the three groups have a bound of $\frac{7}{2} - \frac{1}{8t}$ where t is the tame degree. Using compositum indices, the bound for D_4 and $C_4 \times C_2$ is $\frac{13}{4} - \frac{1}{8t}$ and the bound for Q_8 is $\frac{15}{4} - \frac{1}{8t}$. Frattini indices give a better bound for Q_8 whereas compositum indices give the better bound for D_4 and $C_2 \times C_4$.

Doing the analogous computation with the 12 groups of order 16 other than C_2^4 and C_{16}, the compositum indices give a better bound 9 times, Frattini indices give a better bound 3 times.

Proposition 3.1 below illustrates how one can improve on the bounds coming from either approach on its own.

3. Globalization and groups with $32 \nmid |G|$

3.1. **Global extensions.** The following notation will be used for the remainder of this paper.

Let $K/\mathbf{Q}$ be a Galois extension with Galois group G. Let p be rational prime, and $P_1, \ldots, P_g$ the primes of K above p. The g completions K_{P_i} are isomorphic as extensions of $\mathbf{Q}_p$, hence have the same discriminants. We define $\mathrm{MS}_p(K) = \mathrm{MS}(K_{P_1})$. Then $p^{\mathrm{MS}_p(K)}$ is the contribution from p to the root discriminant of $K/\mathbf{Q}$.

Let D_p be the decomposition group for P_1, W_p, the wild ramification group for P_1, and H_p a Sylow p-subgroup of G containing W_p. We identify D_p with $\mathrm{Gal}(K_{P_1}/\mathbf{Q}_2)$. We compute an upper bound on $\mathrm{MS}_p(K)$ primarily by means of composita indices from Proposition 2.2 applied to H_p. Given more information about W_p, then one could obtain sharper bounds by applying Proposition 2.2 to W_p. One can work with H_p instead by equation (7).

3.2. **Extensions where** $32 \nmid |G|$**.** In [Har94], Harbater shows that if $K \in \mathcal{K}_2$ and $16 \nmid [K : \mathbf{Q}]$, then $\mathrm{Gal}(K/\mathbf{Q})$ is a 2-group. Moreover, he shows that the smallest non-2-group in $\mathcal{G}_2$ has order 272, and there is a unique such extension, namely the Hilbert class field of $\mathbf{Q}(i(\zeta_{64} + \zeta_{64}^{-1}))$. We will denote this field by K_{272}. It has Galois group $C_{17} : C_{16}$.

Here we show that K_{272} is unique in another sense. Namely, assuming the Generalized Riemann Hypothesis (GRH) we show that this extension is the unique extension in $\mathcal{K}_2$ whose degree is not a power of 2 and not multiple of 32.

First, we establish a few preliminaries which do not rely on GRH. Then we illustrate the use of composita indices in a detailed case before treating $32 \nmid |G|$ more generally.

Proposition 3.1. *Suppose $G \in \mathcal{G}_2$ such that $|G|$ is not a multiple of 32 and $H_2 \not\cong C_{16}$, where H_2 is the Sylow 2-subgroup of G. Then G is a 2-group.*

Proof. Let $K \in \mathcal{K}_2$ be a Galois extension with $\mathrm{Gal}(K/\mathbf{Q}) \cong G$, and $W_2 \leq H_2$ the wild ramification subgroup for a prime of K above 2. Note that if $|W_2|$ is not a multiple of 16, Harbater [Har94, Thm. 2.23] has shown that G is a 2-group. So, we are reduced to case where $W_2 = H_2$ has order 16, but is not cyclic.

For groups of order 16, Table 1 gives composita indices for each group, the corresponding bound on $\mathrm{MS}_2(K)$, and an upper bound for the degree of such an extension. The groups are given in terms of their numbering as small groups of

TABLE 1. Composita Indices for groups of order 16 by gap number. For a given set of composita indices, we give an upper bound on the mean slope at 2. The degree column gives upper bounds for corresponding fields $K \in \mathcal{K}_2$.

Gap #	**Name**	**Compos. Ind.**	MS_2	**Deg**
1	C_{16}	[1,1,1,1]	5	-
2,3,4		[2,2]	29/8	38
5,6,7,8		[2,1,1]	33/8	140
9	Q_{16}	[2,1,0,1]	37/8	-
10,11		[3,1]	27/8	30
12,13		[3,0,1]	31/8	70
14	C_2^4	[4]	23/8	20

order 16 by `gap` [GAP06]. For example, the group $Q_8 \times C_2$ is `SmallGroup(16,12)` in `gap`, which we will denote by [16, 12]. Groups with the same composita indices are grouped in the same line. We give a familiar name for a group when it is the only group on its line.

For example, the groups numbered $[16,\ 2] \cong C_4 \times C_4$, $[16,\ 3] \cong (C_4 \times C_2) : C_2$, and $[16,\ 4] \cong C_4 : C_4$ have composita indices of $[2, 2]$. Thus by Proposition 2.2, the slope content is bounded by $[3, 3, 4, 4]_t$ for some $t \geq 1$ and

$$\mathrm{MS}_2([3,3,4,4]_t) = \frac{29}{8} - \frac{1}{16t} < \frac{29}{8}.$$

Then comparing $2^{29/8} < 12.338$ with Odlyzko's tables [Odl76] we find $[K : \mathbf{Q}] < 38$. Since Harbater [Har94] shows that $G \in \mathcal{G}_2$ and $|G| < 272$ implies G is a 2-group, Table 1 covers all possibilities with the exception of $[16,\ 1] \cong C_{16}$, which is excluded by our hypotheses, and $[16,\ 9] \cong Q_{16} \cong C_2.D_4$ which we treat now.

The composita indices for Q_{16} show that the first 3 slopes are bounded by $[3, 3, 4]$. Since $\mathrm{MS}([3, 3, 4]_t) = \frac{13}{4} - \frac{1}{8t}$, Proposition 1.5 shows that the final slope is at most

$$\frac{13}{4} - \frac{1}{8t} + 2 + \frac{1}{8t} = \frac{21}{4}\,.$$

So, the slope content for the whole extension is bounded $[3, 3, 4, 21/4]_t$ giving $\mathrm{MS}_2(K) \leq \frac{17}{4} - \frac{1}{16t}$, or a root discriminant of at most 19.0274. Using an implementation in `gp` of the program in [BD08] for computing root discriminant bounds, we obtain that $|G| = [K : \mathbf{Q}] \leq 270$. Again, we are done by [Har94]. □

Proposition 3.1 provides most of the proof of the following theorem.

Theorem 3.2. *If $G \in \mathcal{G}_2$ and $|G|$ is not a multiple of 32, then G is solvable.*

Proof. By Proposition 3.1, either G is a 2-group, hence solvable, or the Sylow 2-subgroup of G is isomorphic to C_{16}. But, by a classical theorem of Burnside, a finite group with cyclic Sylow 2-subgroup is is a semi-direct product of its Sylow 2-subgroup, which is solvable, and a group of odd order, which also must be solvable. Hence, G is solvable. □

Proposition 3.3. *Assuming GRH, if $K \in \mathcal{K}_2$ where $[K : \mathbf{Q}]$ is not a power of 2, then either $[K : \mathbf{Q}]$ is a multiple of 32 or $K = K_{272}$.*

Proof. The case where $16 \nmid [K : \mathbf{Q}]$ is covered by [Har94, Thm. 2.23]. Moreover, since he shows that this field of degree 272 is the lowest degree field in $\mathcal{K}_2$ whose Galois group is not a 2-group, Proposition 3.1 reduces us to the case where the Sylow 2-subgroup of $G = \mathrm{Gal}(K/\mathbf{Q})$ is cyclic.

Let H_2 denote the Sylow 2-subgroup of G. Since H_2 is cyclic, $G = N : H_2$ for a normal subgroup N of odd order by the result of Burnside. Since the maximal abelian subfield of K must be cyclotomic, it is contained in $\mathbf{Q}(\zeta_{2^n})$ for some n, so it is a 2-extension. On the other hand, K^N is Galois over $\mathbf{Q}$ with Galois group $G/N \cong H_2 \cong C_{16}$. Hence, K^N is a subfield of $\mathbf{Q}(\zeta_{2^n})$ with Galois group C_{16}. Moreover, since N is solvable, K^N admits a non-trivial abelian extension of odd degree. Since subfields of $\mathbf{Q}(\zeta_{2^n})$ are totally ramified at 2, odd degree abelian extensions unramified away from 2 are in fact unramified. Harbater checked that the only degree 16 field with odd class number is $K_{16} := \mathbf{Q}(i(\zeta_{64} + \zeta_{64}^{-1}))$, so this must be $K^N = K_{16}$. Since the class number of K_{16} is 17, the abelianization N/N' is isomorphic to C_{17} and $K^{N'} = K_{272}$.

It remains to show that K_{272} has no non-trivial abelian extensions of odd degree. Suppose it does; call the extension L and let $M = \mathrm{Gal}(L/K_{272})$. Now $\mathrm{Gal}(L/K_{16})$ has abelianization C_{17} since K_{272} is the maximal abelian extension of K_{16} which is unramified at 2. Moreover, C_{17} acts by conjugation on M, and the action is non-trivial or $\mathrm{Gal}(L/K_{16})$ would be abelian. Since the orbit of an element in the action has size 1 or 17, $|M| \geq 17$. Thus,

$$[L : \mathbf{Q}] = [L : K_{272}][K_{272} : \mathbf{Q}] = |M| \cdot 272 \geq 17 \cdot 272 = 4624\,.$$

From the composita indices for C_{16}, we have $\mathrm{rd}(K) \leq 2^5$. Now using an implementation in gp of the program in [BD08] for GRH root discriminant bounds, we compute that under GRH, $[L : \mathbf{Q}] < 2750$, a contradiction. □

4. Simple Galois groups

We now apply composita indices to show that certain simple groups are not elements of $\mathcal{G}_2$. Section 4.1 treats groups which we unconditionally prove are not elements of $\mathcal{G}_2$. Section 4.2 deals with some of the sporadic simple groups, showing they they are not in $\mathcal{G}_2^+$, and assuming GRH, are not in $\mathcal{G}_2$. It then treats families of simple groups in the same way.

4.1. Unconditional results.

From the families of non-abelian simple groups, it was previously known that that the following groups are not in $\mathcal{G}_2$: $PSL_2(2^j)$ for $g \geq 2$, $R(3^{2m+1})$ for $n \geq 1$, A_n for $5 \leq n \leq 15$, and $PSL_3(2)$. This comes from the results of [Tat94, Har94, Bru01, Les, Jon]. The main result of this section is to extend these results.

Theorem 4.1. *The following simple groups are not in $\mathcal{G}_2$:*

- $PSL_2(q)$ *for* $q \not\equiv \pm 1 \pmod{32}$
- $PSL_3(q)$, $PSU_3(q)$, $PSp_4(q)$, ${}^3D_4(q^3)$, *and* $G_2(q)$ *for* $q \equiv 3, 5 \pmod 8$
- $PSL_3(4)$, $PSU_3(4)$, $PSL_4(2)$, $PSU_4(2)$, $PSp_4(4)$

Note, this means that when ordered by size, the first 17 non-abelian simple groups are not in $\mathcal{G}_2$. For the groups of the form $PSL_2(q)$, those with $q = 2^j$ for some j are covered by Tate's theorem. They are included in the statement above since to do otherwise would make the statement more awkward.

Proof. The groups $PSL_2(q)$ with $q \not\equiv \pm 1 \pmod{32}$, $PSL_3(q)$ with $q \equiv 3 \pmod 8$ and $PSU_3(q)$ with $q \equiv 5 \pmod 8$ all have Sylow 2-subgroups of order 16, so are ruled out by Theorem 3.2.

For most of the other groups, we refer to Table 2. It gives an overview showing

TABLE 2. For each group listed, we give the gap numbering for H_2, its Sylow 2-subgroup, the compositum indices for H_2, the mean slope bound, and an upper bound on the degree of a corresponding extension of from $\mathcal{K}_2$. Groups with isomorphic Sylow 2-subgroups are grouped together.

Group	H_2	**Comp. Ind.**	MS_2	**Deg**
$PSL_3(q) : q \equiv 5 \pmod 8$ $PSU_3(q) : q \equiv 3 \pmod 8$	$[32, 11]$	$[2, 2, 1]$	$69/16$	480
${}^3D_4(q^3) : q \equiv 3, 5 \pmod 8$ $G_2(q) : q \equiv 3, 5 \pmod 8$	$[64, 134]$	$[3, 2, 1]$	$139/32$	600
$PSp_4(q) : q \equiv 3, 5 \pmod 8$ $PSL_4(2), PSU_4(2)$	$[64, 138]$	$[3, 2, 1]$	$139/32$	600
$PSp_4(4)$	$[256, 8935]$	$[4, 4]$	$503/128$	72

the isomorphism type of the Sylow 2-subgroup, its composita indices, an upper bound for the mean slope of a corresponding Galois extension, and an upper bound on the degree of such an extension. In each case, the upper bound on the degree is smaller than the size of the smallest group for that row.

For the groups $PSL_3(4)$ and $PSU_3(4)$, the Sylow 2-subgroups have Frattini indices of $[4, 2]$. By Proposition 2.3, we get $\mathrm{MS}_2(K) < \frac{38}{8}$ for the corresponding Galois extension K. Comparing with Odlyzko bounds, the degree of such an extension is at most 960, which is smaller than either group. $\square$

4.2. **Groups not in $\mathcal{G}_2^+$ and results using GRH.** Let $K \in \mathcal{K}_2$ and $G = \mathrm{Gal}(K/\mathbf{Q})$. As above, we obtain upper bounds for $\mathrm{MS}_2(K)$, and then apply root discriminant bounds to obtain an upper bound on $[K : \mathbf{Q}] = |G|$. The unconditional root discriminant bounds for totally real fields are sharper than the GRH bounds for aribitrary fields of the same degree. So, in the latter two sections, we focus on showing a given group $G \notin \mathcal{G}_2$ under GRH, and get an unconditional proof of $G \notin \mathcal{G}_2^+$ as well.

In this section, we rule out several of the 26 sporadic simple groups from $\mathcal{G}_2$. In [Jon], the Mathieu groups M_{11} and M_{12} were excluded from $\mathcal{G}_2$ unconditionally.

Similarly, it follows from [Har94, Thm. 2.23] that the first Janko group $J_1 \notin \mathcal{G}_2$ since its order is not a multiple of 16.

Theorem 4.2. *The following groups are not elements of $\mathcal{G}_2^+$, and assuming GRH, they are not elements of $\mathcal{G}_2$.*

- *Mathieu groups M_{22}, M_{23}, and M_{24} of orders* 443,520, 10,200,960, *and* 244,823,040.
- *Janko groups J_2 and J_3 of orders* 604,800 *and* 50,232,960
- *Higman-Sims group HS of order* 44,352,000
- *McLaughlin group McL of order* 898,128,000
- *O'Nan group $O'N$ of order* 460,815,505,920
- *Conway group Co_3 of order* 495,766,656,000
- *Lyons group Ly of order* 51,765,179,004,000,000
- *Held group He of order* 4,030,387,200

Proof. For each group, the Sylow 2-subgroup H_2 is given by [Mal04]. We compute the composita indices for each H_2 using `gap`, and an upper bound for the mean slope as shown in Table 3. We do not list the individual Sylow 2-subgroups in

Table 3. Composita indices, mean slope bounds, and degree bounds for several sporadic simple groups.

Group	**Comp. Ind.**	MS_2	**Deg**
$J_2, J_3, M_{22}, M_{23}, McL$	$[3, 2, 1, 1]$	5.172	31,970
Ly	$[3, 2, 2, 1]$	5.336	2,391,978
$O'N$	$[3, 2, 3, 1]$	5.418	10^{10}
HS	$[3, 3, 2, 1]$	5.356	10^7
He, M_{24}, Co_3	$[4, 3, 2, 1]$	5.358	10^7

Table 3, but collect on the same line groups where the subgroup H_2 have the same composita indices. Then, in comparing with root discriminant bounds from [Odl76], we obtain an upper bound for the degree of corresponding extension in $\mathcal{K}_2$. In each case, the bound is less than the order of the groups in question. □

Turning our attention to groups of Lie type, we first note the following result for completeness. It is an easy consequence of the result of Moon.

Proposition 4.3 (Moon)**.** *The following simple groups are not elements of $\mathcal{G}_2^+$, and assuming GRH, they are not elements of $\mathcal{G}_2$: for $j \geq 2$, $PSL_3(2^j)$, $PSL_4(2^j)$, $PSU_3(2^j)$, $PSU_4(2^j)$, $PSp_4(2^j)$, $Sz(2^{2j-1})$.*

Groups from these families corresponding to $j = 1$ are either not simple, or have been treated in Section 4.1.

Proof. Each of these groups have 2-lengths of 2, so if there was a corresponding extension K has mean slope of at most 5 by Corollary 2.4. Then, $|G| = [K : \mathbf{Q}] \leq 4800$ by comparing to root discriminant tables, which in each case is a contradiction. □

Finally, we consider several more infinite families of simple groups.

Theorem 4.4. *The following simple groups are not elements of $\mathcal{G}_2^+$, and assuming GRH, they are not elements of $\mathcal{G}_2$:*

- $PSL_2(q)$ *for* $q \equiv 31, 33 \pmod{64}$
- $PSL_3(q)$ *and* $PSU_3(q)$ *for* $q \equiv 7, 9 \pmod{16}$
- $PSL_4(q)$ *and* $PSU_4(q)$ *for* $q \equiv 3, 5 \pmod{8}$
- $PSp_4(q)$*,* $G_2(q)$*, and* ${}^3D_4(q^3)$ *for* $q \equiv 7, 9 \pmod{16}$
- $PSp_6(q)$ *for* $q \equiv 3, 5 \pmod{8}$
- $PSL_5(2)$
- $O_7(q)$ *for* $q \equiv 3, 5 \pmod{8}$
- $O_8^-(q)$ *for* $q \equiv 3 \pmod{8}$

Proof. The structure of the proof is the same as in earlier sections. The basic data is summarized in Table 4. In each case, the orders of groups in a given row are larger than the upper bound given in the last column. All of the bounds come from [Odl76], with the exception of the one for $PSL_5(2)$. For that group, the tables in [Odl76] were not sufficiently refined for extensions of such large degree. So, we computed the given bound using the gp implementation of the program in [BD08]. □

Table 4. Data for groups in Theorem 4.4.

Group	**Comp. Ind.**	MS_2	**Deg**
$PSL_2(q) : q \equiv 31, 33 \pmod{64}$ $PSL_3(q) : q \equiv 7 \pmod{16}$ $PSU_3(q) : q \equiv 9 \pmod{16}$	$[2, 1, 1, 1]$	33.417	8,862
$PSL_3(q) : q \equiv 9 \pmod{16}$ $PSU_3(q) : q \equiv 7 \pmod{16}$	$[2, 2, 1]$	19.870	120
$PSL_4(q) : q \equiv 3 \pmod{8}$ $PSU_4(q) : q \equiv 5 \pmod{8}$	$[3, 2, 2]$	25.491	380
$PSL_4(q) : q \equiv 5 \pmod{8}$ $PSU_4(q) : q \equiv 3 \pmod{8}$	$[3, 2, 1, 1]$	36.049	31,970
$PSp_4(q) : q \equiv 7, 9 \pmod{16}$ $G_2(q) : q \equiv 7, 9 \pmod{16}$ ${}^3D_4(q^3) : q \equiv 7, 9 \pmod{16}$	$[3, 2, 2, 1]$	40.391	2,391,978
$PSp_6(q) : q \equiv 3, 5 \pmod{8}$	$[5, 2, 1, 1]$	36.343	31,970
$O_7(q) : q \equiv 3, 5 \pmod{8}$	$[4, 3, 2]$	26.261	480
$O_8^-(q) : q \equiv 3 \pmod{8}$	$[5, 3, 2]$	26.297	600
$PSL_5(2)$	$[4, 3, 2, 1]$	40.997	7,500,000

Comparing the results of the previous theorems with the list of finite non-abelian simple groups ordered by size, we see that all groups of order less than 1,000,000 are not elements of $\mathcal{G}_2^+$, and assuming GRH, not in $\mathcal{G}_2$.

References

[BD08] Sharon Brueggeman and Darrin Doud, *Local corrections of discriminant bounds and small degree extensions of quadratic base fields*, Int. J. Number Theory **4** (2008), no. 3, 349–361. MR MR2424327

[Bru01] Sharon Brueggeman, *Septic number fields which are ramified only at one small prime*, J. Symbolic Comput. **31** (2001), no. 5, 549–555. MR MR1828702 (2002e:11145)

[Dem09] Lassina Dembélé, *A non-solvable extension of $\mathbb{Q}$ ramified at 2 only*, arXiv:0811.4379, 2009.

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

[Har94] David Harbater, *Galois groups with prescribed ramification*, Arithmetic geometry (Tempe, AZ, 1993), Contemp. Math., vol. 174, Amer. Math. Soc., Providence, RI, 1994, pp. 35–60. MR MR1299733 (96a:12008)

[Jon] John W. Jones, *Number fields unramified away from* 2, to appear.

[JR99] John W. Jones and David P. Roberts, *Sextic number fields with discriminant* $(-1)^j 2^a 3^b$, Number theory (Ottawa, ON, 1996), CRM Proc. Lecture Notes, vol. 19, Amer. Math. Soc., Providence, RI, 1999, pp. 141–172. MR 2000b:11142

[JR03] ———, *Septic fields with discriminant* $\pm 2^a 3^b$, Math. Comp. **72** (2003), no. 244, 1975–1985 (electronic). MR MR1986816 (2004e:11119)

[JR06] ———, *A database of local fields*, J. Symbolic Comput. **41** (2006), no. 1, 80–97.

[Les] Sylla Lesseni, *The nonexistence of nonsolvable octic number fields ramified only at one small prime*, To appear in Math. Comp.

[Mal04] Sergey Malyushitsky, *On sylow* 2*-subgroups of finite simple groups of order up to* 2^{10}, Ph.D. thesis, The Ohio State University, 2004.

[Mar63] G. N. Markšaĭtis, *On p-extensions with one critical number*, Izv. Akad. Nauk SSSR Ser. Mat. **27** (1963), 463–466. MR MR0151452 (27 #1437)

[Moo00] Hyunsuk Moon, *Finiteness results on certain mod p Galois representations*, J. Number Theory **84** (2000), no. 1, 156–165.

[Moo07] ———, *On four-dimensional mod 2 Galois representations and a conjecture of Ash et al*, Bull. Korean Math. Soc. **44** (2007), no. 1, 173–176. MR MR2297707 (2007m:11157)

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

[Odl90] 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 MR1061762 (91i:11154)

[Ser79] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg. MR 82e:12016

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

[Tat94] John Tate, *The non-existence of certain Galois extensions of* $\mathbf{Q}$ *unramified outside* 2, Arithmetic geometry (Tempe, AZ, 1993), Contemp. Math., vol. 174, Amer. Math. Soc., Providence, RI, 1994, pp. 153–156. MR 95i:11132

School of Mathematical and Statistical Sciences, Arizona State University, PO Box 871804, Tempe, AZ 85287

E-mail address: `jj@asu.edu`