Progress towards counting $D_5$ quintic fields

Eric Larson and Larry Rolen
Progress towards counting $D_5$ quintic fields

Eric Larson and Larry Rolen

(Communicated by Ken Ono)

Let $N(5, D_5, X)$ be the number of quintic number fields whose Galois closure has Galois group $D_5$ and whose discriminant is bounded by $X$. By a conjecture of Malle, we expect that $N(5, D_5, X) \sim C \cdot X^{1 + \frac{1}{12}}$ for some constant $C$. The best upper bound currently known is $N(5, D_5, X) \ll X^{\frac{3}{4} + \varepsilon}$, and we show this could be improved by counting points on a certain variety defined by a norm equation; computer calculations give strong evidence that this number is $\ll X^{\frac{3}{2}}$. Finally, we show how such norm equations can be helpful by reinterpreting an earlier proof of Wong on upper bounds for $A_4$ quartic fields in terms of a similar norm equation.

1. Introduction and statement of results

Let $K$ be a number field and $G \leq S_n$ a transitive permutation group on $n$ letters. In order to study the distribution of fields with given degree and Galois group, we introduce the following counting function:

$$N(d, G, X) := \# \{ \text{degree } d \text{ number fields } K \text{ with } \text{Gal}(K^{gal}/\mathbb{Q}) \simeq G \text{ and } |D_K| \leq X \}.$$ 

Here $D_K$ denotes the discriminant of $K$, counting conjugate fields as one. Our goal is to study this function for $d = 5$ and $G = D_5$. Malle [2002] has conjectured that

$$N(d, G, X) \sim C(G) \cdot X^{a(G)} \cdot \log(X)^{b(G) - 1}$$ (1)

for some constant $C(G)$ and for explicit constants $a(G)$ and $b(G)$, and this has been proven for all abelian groups $G$. Although this conjecture seems to be close to the truth on the whole, Klüners [2005] found a counterexample when $G = C_3 \times C_2$.

\textbf{MSC2010:} primary 11R45; secondary 11R29, 14G05.

\textbf{Keywords:} quintic dihedral number fields, Cohen–Lenstra heuristics for $p = 5$.

The authors are grateful for the support of the NSF in funding the Emory 2011 REU. The authors would like to thank our advisor Andrew Yang, as well as Ken Ono for their guidance, useful conversations, improving the quality of exposition of this article, and hosting the REU.
by showing that the conjecture predicts the wrong value for \( b(G) \). This conjecture
has been modified to explain all known counterexamples in [Turkelli 2008].

We now turn to the study of \( N(5, D_5, X) \). By Malle’s conjecture, we expect that

\[
N(5, D_5, X) \approx C \cdot X^{\frac{1}{2}}.
\]  

(2)

This question is closely related to average 5-parts of class numbers of quadratic
fields. In general, let \( l \) be a prime, \( D \) range over fundamental discriminants, and
\( r_D := \text{rk}_l(\text{Cl}_{Q(\sqrt{D})}) \). Then the heuristics of Cohen–Lenstra predicts that the average
of \( l^{r_D} - 1 \) over all imaginary quadratic fields is 1, and the average of \( l^{r_D} - 1 \)
over all real quadratic fields is \( l^{-1} \).

In fact, one can show using class field theory that the Cohen–Lenstra heuristics imply that Malle’s conjecture is true for \( D_5 \) quintic fields. Conversely, the
best known upper bound for \( N(5, D_5, X) \) is proved using the “trivial” bound (see [Klüners 2006])

\[
l^{r_D} \leq \# \text{Cl}_{Q(\sqrt{D})} = O(D^{\frac{1}{2}} \log D).
\]

(3)

This gives \( N(5, D_5, X) \ll X^{\frac{3}{4} + \epsilon} \), and any improved bound would give nontrivial
information on average 5-parts of class groups in a similar manner.

In this paper, we consider a method of point counting on varieties to give upper
bounds on \( N(5, D_5, X) \). Our main result is the following:

**Theorem 1.1.** To any quintic number field \( K \) with Galois group \( D_5 \), there correspond a triple \((A, B, C)\) with \( A, B \in \mathbb{Q}[\sqrt{5}] \) and \( C \in \mathbb{Z} \), such that

\[
\text{Nm}_{\mathbb{Q}[\sqrt{5}]}(B^2 - 4 \cdot A \cdot A^2) = 5 \cdot C^2
\]

(4)

and satisfying the following bounds under any archimedean valuation:

\[
|A| \ll D_K^{\frac{1}{3}}, \quad |B| \ll D_K^{\frac{3}{8}}, \quad \text{and} \quad |C| \ll D_K^{\frac{3}{2}}.
\]

(5)

Conversely, the triple \((A, B, C)\) uniquely determines \( K \).

In Section 6, we further provide numerical evidence that \( N(5, D_5, X) \ll X^{\frac{2}{3} + \alpha} \)
for very small \( \alpha \); in particular the exponent appears to be much lower than \( \frac{3}{4} \).

Before we prove Theorem 1.1, we show that earlier results from [Wong 2005]
in the case of \( G = A_4 \) can be handled in a similar fashion. Namely, we give a
shorter proof of the following theorem:

**Theorem 1.2** (Wong). To any quartic number field \( K \) with Galois group \( A_4 \), there corresponds a tuple \((a_2, a_3, a_4, y)\) \( \in \mathbb{Z}^4 \) such that

\[
(4a_2^2 + 48a_4)^3 = \text{Nm}_{\mathbb{Q}[\sqrt{-3}]}(32a_2^3 + 108a_3^2 - 6a_2(4a_2^2 + 48a_4) - 12\sqrt{-3}y)
\]
and satisfying the following under any archimedean valuation:

$$|a_2| \ll D_K^{3/4}, \ |a_3| \ll D_K^{1/4}, \ |a_4| \ll D_K^{3/4}, \text{ and } |y| \ll D_K.$$  

Conversely, given such a tuple, there corresponds at most one $A_4$-quartic field. In particular, we have $N(4, A_4, X) \ll X^6 + \epsilon$.

2. Upper bounds via point counting

Let $G$ be a transitive permutation group. If $K$ is a number field of discriminant $D_K$ and degree $n$ for which $\text{Gal}(K^{\text{gal}}/\mathbb{Q}) \simeq G$, then Minkowski theory implies there is an element $\alpha \in \mathcal{O}_K$ of trace zero with

$$|\alpha| \ll D_K^{\frac{1}{2(n-1)}} \quad \text{(under any archimedean valuation),}$$

where the implied constant depends only on $n$. In particular, if $K$ is a primitive extension of $\mathbb{Q}$, then $K = \mathbb{Q}(\alpha)$, so the characteristic polynomial of $\alpha$ will determine $K$. One can use this to give an upper bound on $N(n, G, X)$ (at least in the case where $K$ is primitive), since every pair $(K, \alpha)$ as above gives a $\mathbb{Z}$-point of

$$\text{Spec } \mathbb{Q}[x_1, x_2, \ldots, x_n]^G/(s_1),$$

where $s_1 = x_1 + x_2 + \cdots + x_n$ (here $\mathbb{Q}[x_1, x_2, \ldots, x_n]^G$ denotes the ring of $G$-invariant polynomials in $\mathbb{Q}[x_1, x_2, \ldots, x_n]$).

3. Proof of Theorem 1.2

In this section, we sketch a simplified (although essentially equivalent) version of Wong’s proof [Wong 2005] that $N(4, A_4, X) \ll X^6 + \epsilon$ as motivation for our main theorem. In this section, we assume that the reader is familiar with the arguments in Wong’s paper. As noted in the last section, it suffices to count triples $(a_2, a_3, a_4)$ for which $|a_k| \ll X^6$ under any archimedean valuation and

$$256a_4^3 - 128a_2^2a_4^2 + (16a_4^4 + 144a_2a_4^2)a_4 - 4a_2^3a_3^2 - 27a_3^4 = \text{Disc}(x^4 + a_2x^2 + a_3x + a_4) = y^2$$

for some $y \in \mathbb{Z}$. (See Equation 4.2 of [Wong 2005].)

The key observation of Wong’s paper (although he does not state it in this way) is that this equation can be rearranged as

$$(4a_2^2 + 48a_4)^3 = N_{\mathbb{Q}[\sqrt{-3}]}(32a_2^3 + 108a_3^2 - 6a_2(4a_2^2 + 48a_4) - 12\sqrt{-3}y). \quad (6)$$

One now notes that there are $\ll X^{3/2}$ possibilities for $4a_2^2 + 48a_4$, and for each of these choices $(4a_2^2 + 48a_4)^3$ can be written in $\ll X^{\epsilon}$ ways as a norm of an element
of \( \mathbb{Q}[\sqrt{-3}] \). Thus, it suffices to count the number of points \((a_2, a_3)\) for which
\[
32a_2^3 + 108a_3^2 - 6a_2(4a_2^2 + 48a_4) - 12\sqrt{-3}y \quad \text{and} \quad 4a_2^2 + 48a_4
\]
are fixed. But the above equation defines an elliptic curve, on which the number of integral points can be bounded by Theorem 3 in [Heath-Brown 2002]. This then gives Wong’s bound (as well as the conditional bound assuming standard conjectures as Wong shows).

4. Proof of Theorem 1.1

In this section, we give the proof of Theorem 1.1. As explained in Section 2, it suffices to understand the \( \mathbb{Z} \)-points of
\[
\text{Spec } \mathbb{Q}[x_1, x_2, x_3, x_4, x_5]_{D_5}/(x_1 + x_2 + x_3 + x_4 + x_5)
\]
inside a particular box. Write \( \zeta \) for a primitive fifth root of unity, and define
\[
V_j = \sum_{i=1}^{5} \zeta^{ij} x_i.
\]

In terms of the \( V_j \), we define
\[
A = V_2 \cdot V_3,
B = V_1 \cdot V_2^2 + V_3^2 \cdot V_4,
C = \frac{1}{\sqrt{5}} \cdot (V_1 \cdot V_2^2 - V_3^2 \cdot V_4) \cdot (V_2 \cdot V_4^2 - V_1^2 \cdot V_3).
\]

**Lemma 4.1.** The expressions \( A, B, \) and \( C \) are invariant under the action of \( D_5 \).

**Proof.** The generators of \( D_5 \) act by \( V_j \mapsto V_{5-j} \) and \( V_j \mapsto \zeta^j V_j \); the result follows immediately.

**Lemma 4.2.** We have \( A, B \in \mathbb{O}_{\mathbb{Q}[\sqrt{5}]} \) and \( C \in \mathbb{Z} \).

**Proof.** To see the first assertion, it suffices to show that \( A \) and \( B \) are invariant by the element of \( \text{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}) \) given by \( \zeta \mapsto \zeta^{-1} \). But this induces the map \( V_j \mapsto V_{5-j} \), so this is clear.

To see that \( C \) is in \( \mathbb{Z} \), we observe that the generator of \( \text{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}) \) given by \( \zeta \mapsto \zeta^2 \) acts by \( C \sqrt{5} \mapsto -C \sqrt{5} \). Since \( C \sqrt{5} \) is an algebraic integer, it follows that \( C \sqrt{5} \) must be a rational integer times \( \sqrt{5} \), so \( C \in \mathbb{Z} \).

Now, we compute
\[
B^2 - 4 \cdot \bar{A} \cdot A^2 = (V_1 \cdot V_2^2 + V_3^2 \cdot V_4)^2 - 4 \cdot V_1 \cdot V_4 \cdot (V_2 \cdot V_3)^2 = (V_1 \cdot V_2^2 - V_3^2 \cdot V_4)^2.
\]
Therefore,
\[
\text{Nm}_{\mathbb{Q}[\sqrt{5}]}(B^2 - 4 \cdot \tilde{A} \cdot A^2) = (V_1 \cdot V_2^2 - V_3^2 \cdot V_4)^2 \cdot (V_2 \cdot V_4^2 - V_1^2 \cdot V_3)^2 = 5 \cdot C^2,
\]
which verifies the identity claimed in Theorem 1.1.

To finish the proof, it remains to show that to each triple \((A, B, C)\), there corresponds at most one \(D_5\)-quintic field. To do this, we begin with the following lemma.

**Lemma 4.3.** None of the \(V_j\) are zero.

**Proof.** Suppose that some \(V_j\) is zero. Since \(\tilde{A} \cdot A^2 = V_1 \cdot V_2^2 \cdot V_3^2 \cdot V_4\), it follows that \(\tilde{A} \cdot A^2 = 0\), and hence
\[
\text{Nm}_{\mathbb{Q}[\sqrt{5}]}(B^2) = 5 \cdot C^2,
\]
which implies \(B = C = 0\). Using \(B = 0\), we have \(V_1 V_2^2 \cdot V_3^2 V_4 = V_1 V_2^2 + V_3^2 V_4 = 0\), so \(V_1 V_2^2 = V_3^2 V_4 = 0\). Similarly, using \(\tilde{B} = 0\), we have \(V_2 V_4^2 = V_1^2 V_3 = 0\). Thus, all pairwise products \(V_i V_j\) with \(i \neq j\) are zero, so at most one \(V_k\) is nonzero. Solving for the \(x_i\), we find \(x_i = \zeta^{-ik} c\) for some constant \(c\). (It is easy to verify that this is a solution, since \(\sum \zeta^i = 0\); it is unique up to rescaling because the transformation \((x_i) \mapsto (V_i)\) is given by a Vandermonde matrix of rank 4). Hence, the minimal polynomial of \(\alpha\) is \(t^5 - c^5 = 0\), which is visibly not a \(D_5\) extension. \(\Box\)

**Lemma 4.4.** For fixed \((A, B, C)\), there are at most two possibilities for the ordered quadruple
\[
(V_1 V_2^2, V_3^2 V_4, V_2 V_4^2, V_1^2 V_3).
\]

**Proof.** Since \(V_1 V_2^2 + V_3^2 V_4 = B\) and \(V_1 V_2^2 \cdot V_3^2 V_4 = \tilde{A} \cdot A^2\) are determined, there are at most two possibilities for the ordered pair \((V_1 V_2^2, V_3^2 V_4)\). Similarly, there at most two possibilities for the ordered pair \((V_2 V_4^2, V_1^2 V_3)\); thus if \(V_1 V_2^2 = V_3^2 V_4\), then we are done. Otherwise,
\[
V_2 \cdot V_4^2 - V_1^2 \cdot V_3 = \frac{C \sqrt{5}}{V_1 \cdot V_2^2 - V_3^2 \cdot V_4}.
\]
Since \(V_2 V_4^2 + V_1^2 V_3 = \tilde{B}\), this shows that the ordered pair \((V_1 V_2^2, V_3^2 V_4)\) determines \((V_2 V_4^2, V_1^2 V_3)\). Hence there are at most two possibilities our ordered quadruple. \(\Box\)

**Lemma 4.5.** For fixed \((A, B, C)\), there are at most ten possibilities for the ordered quadruple \((V_1, V_2, V_3, V_4)\).

**Proof.** In light of Lemmas 4.4 and 4.3, it suffices to show there at most five possibilities for \((V_1, V_2, V_3, V_4)\) when we have fixed nonzero values for
\[
(V_1 V_4, V_2 V_3, V_1 V_2^2, V_3^2 V_4, V_2 V_4^2, V_1^2 V_3).
\]
But this follows from the identities
\[
V_1^5 = \frac{V_1 V_2^2 (V_1 V_3)^2}{(V_2 V_3)^2}, \quad V_3 = \frac{V_2 V_3}{V_1^2}, \quad V_4 = \frac{V_2 V_4}{V_3^2}, \quad V_2 = \frac{V_2 V_4^2}{V_3^3}.
\]

This completes the proof of Theorem 1.1, because \(|D_5| = 10\), so each \(D_5\)-quintic field corresponds to ten ordered quadruples \((V_1, V_2, V_3, V_4)\), each of which can be seen to correspond to the same triple \((A, B, C)\). Thus, the triple \((A, B, C)\) uniquely determines the \(D_5\)-quintic field, since otherwise we would have at least 20 quadruples \((V_1, V_2, V_3, V_4)\) corresponding to \((A, B, C)\), contradicting Lemma 4.5.

5. The quadratic subfield

**Proposition 5.1.** Suppose that \(K\) is a \(D_5\)-quintic field corresponding to a triple \((A, B, C)\) with \(C \neq 0\). Then the composite of \(\mathbb{Q}[\sqrt{5}]\) with the unique quadratic subfield \(F \subset K^{gal}\) is generated by adjoining to \(\mathbb{Q}[\sqrt{5}]\) the square root of
\[
(2\sqrt{5} - 10) \cdot (B^2 - 4 \cdot A \cdot A^2).
\]

**Proof.** Using the results of the previous section, we note that
\[
\sqrt{(2\sqrt{5} - 10) \cdot (B^2 - 4 \cdot A \cdot A^2)} = 2 \cdot (\zeta - \zeta^{-1}) \cdot (V_1 \cdot V_2^2 - V_3^2 \cdot V_4).
\]
By inspection, the \(D_5\)-action on the above expression is by the sign representation, and the action of \(\text{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}[\sqrt{5}])\) is trivial. Hence, adjoining the above quantity to \(\mathbb{Q}[\sqrt{5}]\) generates the composite of \(\mathbb{Q}[\sqrt{5}]\) with the quadratic subfield \(F\).

6. Discussion of computational results

Numerical evidence indicates that the number of triples \((A, B, C)\) satisfying the conditions of Theorem 1.1 is \(O(X^{\frac{2}{3}} + \alpha)\) for a small number \(\alpha\) (in particular, much less than \(O(X^{\frac{2}{3}})\)). More precisely, we have the following table of results. The computation took approximately four hours on a 3.3 GHz CPU, using the program available at http://web.mit.edu/~elarson3/www/d5-count.py.

<table>
<thead>
<tr>
<th>(X)</th>
<th>#((A, B, C))</th>
<th>(X)</th>
<th>#((A, B, C))</th>
<th>(X)</th>
<th>#((A, B, C))</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>3</td>
<td>1000</td>
<td>127</td>
<td>100000</td>
<td>5145</td>
</tr>
<tr>
<td>31</td>
<td>3</td>
<td>3162</td>
<td>397</td>
<td>316227</td>
<td>11385</td>
</tr>
<tr>
<td>100</td>
<td>7</td>
<td>10000</td>
<td>951</td>
<td>100000</td>
<td>25807</td>
</tr>
<tr>
<td>316</td>
<td>55</td>
<td>31622</td>
<td>2143</td>
<td>3162277</td>
<td>57079</td>
</tr>
</tbody>
</table>

The log plot on the next page shows that after the first few data points, the least squares best fit to the last four data points given by \(y = 0.698x + 0.506\) with slope
a little more than \( \frac{2}{3} \) is quite close.

References


Elliptic curves, eta-quotients and hypergeometric functions
David Pathakjee, Zef RosnBrick and Eugene Yoong

Trapping light rays aperiodically with mirrors
Zachary Mitchell, Gregory Simon and Xueying Zhao

A generalization of modular forms
Adam Haque

Induced subgraphs of Johnson graphs
Ramin Naimi and Jeffrey Shaw

Multiscale adaptively weighted least squares finite element methods for convection-dominated PDEs
Bridget Kraynik, Yifei Sun and Chad R. Westphal

Diameter, girth and cut vertices of the graph of equivalence classes of zero-divisors
Blake Allen, Erin Martin, Eric New and Dane Skabelund

Total positivity of a shuffle matrix
Audra McMillan

Betti numbers of order-preserving graph homomorphisms
Lauren Guerra and Steven Klee

Permutation notations for the exceptional Weyl group $F_4$
Patricia Cahn, Ruth Haas, Aloysius G. Helminck, Juan Li and Jeremy Schwartz

Progress towards counting $D_5$ quintic fields
Eric Larson and Larry Rolen

On supersingular elliptic curves and hypergeometric functions
Keenan Monks