PROGRESS TOWARDS COUNTING D_5 QUINTIC FIELDS

ERIC LARSON AND LARRY ROLEN

ABSTRACT. 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 $N(5, D_5, X) \sim C \cdot X^{\frac{1}{2}}$ for some constant C. The best known upper bound 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 $\ll X^{\frac{2}{3}}$. 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:

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

Here D_K denotes the discriminant of K, counting conjugate fields as one. Our goal is to study this function for $d = 5$ and $G = D_5$. In [6], Malle conjectured that

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

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 found a counterexample when $G = C_3 \wr C_2$ by showing that the conjecture predicts the wrong value for $b(G)$ in [5]. This conjecture has been modified to explain all known counter-examples in [8].

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

$$(2) \qquad N(5, D_5, X) \overset{?}{\sim} C \cdot X^{\frac{1}{2}}.$$

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

$r_D := \mathrm{rk}_\ell(\mathrm{Cl}_{\mathbb{Q}(\sqrt{D})})$. Then the heuristics of Cohen-Lenstra predicts that the average of $\ell^{r_D} - 1$ over all imaginary quadratic fields is 1, and the average of $\ell^{r_D} - 1$ 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 ([4]):

$$(3) \qquad\qquad \ell^{r_D} \le \# \mathrm{Cl}_{\mathbb{Q}(\sqrt{D})} = O(D^{\frac{1}{2}} \log D).$$

This gives $N(5, D_5, X) \ll X^{\frac{3}{4} + \varepsilon}$, and any improved bound would give non-trivial 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 corresponds a triple (A, B, C) with $A, B \in \mathcal{O}_{\mathbb{Q}[\sqrt{5}]}$ and $C \in \mathbb{Z}$, such that*

$$(4) \qquad\qquad \mathrm{Nm}_{\mathbb{Q}}^{\mathbb{Q}[\sqrt{5}]} \left(B^2 - 4 \cdot \overline{A} \cdot A^2 \right) = 5 \cdot C^2$$

and which satisfies the following under any archimedean valuation:

$$(5) \qquad\qquad |A| \ll D_K^{\frac{1}{4}}, \quad |B| \ll D_K^{\frac{3}{8}}, \quad \text{and} \quad |C| \ll D_K^{\frac{3}{4}}.$$

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 α; in particular the exponent appears to be much lower than $\frac{3}{4}$.

Before we prove Theorem 1.1, we show that earlier work of Wong [9] 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*

$$(4a_2^2 + 48a_4)^3 = \mathrm{Nm}_{\mathbb{Q}}^{\mathbb{Q}[\sqrt{-3}]} \left(32a_2^3 + 108a_3^2 - 6a_2(4a_2^2 + 48a_4) - 12\sqrt{-3}y \right),$$

and which satisfies the following under any archimedean valuation:

$$|a_2| \ll D_K^{\frac{1}{3}}, \ |a_3| \ll D_K^{\frac{1}{2}}, \ |a_4| \ll D_K^{\frac{2}{3}}, \ \text{and} \ |y| \ll D_K.$$

Conversely, given such a tuple, there corresponds at most one A_4-quartic field. In particular, we have that $N(4, A_4, X) \ll X^{\frac{5}{6} + \varepsilon}$.

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 α 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, α) 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 [9] that $N(4, A_4, X) \ll X^{\frac{5}{6}+\epsilon}$ 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 $|a_k| \ll X^{\frac{k}{6}}$ under any archimedean valuation and

$$256a_4^3 - 128a_2^2a_4^2 + (16a_2^4 + 144a_2a_3^2)a_4 - 4a_2^3a_3^2 - 27a_3^4 = \text{Disc}(x^4 + a_2x^2 + a_3x + a_4) = y^2$$

for some $y \in \mathbb{Z}$. (See equation 4.2 of [9].)

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

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

One now notes that there are $\ll X^{\frac{2}{3}}$ possibilities for $4a_2^2 + 48a_4$, and for each of these choices $(4a_2^2 + 48a_4)^3$ can be written in $\ll X^{\varepsilon}$ 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 [3]. 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

$$\operatorname{Spec} \mathbb{Q}[x_1, x_2, x_3, x_4, x_5]^{D_5}/(x_1 + x_2 + x_3 + x_4 + x_5)$$

inside a particular box. Write ζ for a primitive 5th 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. Note that 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. $\square$

Lemma 4.2. *We have $A, B \in \mathcal{O}_{\mathbb{Q}[\sqrt{5}]}$ 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 $\operatorname{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ 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 $\operatorname{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ 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 $C \in \mathbb{Z}$. $\square$

Now, we compute

$$B^2 - 4 \cdot \overline{A} \cdot A^2 = (V_1 \cdot V_2^2 + V_3^2 \cdot V_4)^2 - 4 \cdot V_1 \cdot V_4 \cdot (V_2 \cdot V_3)^2 = (V_1 \cdot V_2^2 - V_3^2 \cdot V_4)^2.$$

Therefore,

$$\operatorname{Nm}_{\mathbb{Q}}^{\mathbb{Q}[\sqrt{5}]} \left(B^2 - 4 \cdot \overline{A} \cdot A^2 \right) = (V_1 \cdot V_2^2 - V_3^2 \cdot V_4)^2 \cdot (V_2 \cdot V_4^2 - V_1^2 \cdot V_3)^2 = 5 \cdot C^2,$$

which verifies the identity claimed in Theorem 1.1.

To finish the proof of Theorem 1.1, 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 $\overline{A} \cdot A^2 = V_1 \cdot V_2^2 \cdot V_3^2 \cdot V_4$, it follows that $\overline{A} \cdot A^2 = 0$, and hence

$$\mathrm{Nm}_{\mathbb{Q}}^{\mathbb{Q}[\sqrt{5}]}\left(B^2\right) = 5 \cdot C^2 \quad \Rightarrow \quad B = C = 0.$$

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 $\overline{B} = 0$, 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 α is $t^5 - c^5 = 0$, which is visibly not a D_5 extension. $\qquad\square$

Lemma 4.4. *For fixed* (A, B, C), *there are at most two possibilities for the ordered quadruple*

$$\left(V_1 V_2^2, V_3^2 V_4, V_2 V_4^2, V_1^2 V_3\right).$$

Proof. Since $V_1 V_2^2 + V_3^2 V_4 = B$ and $V_1 V_2^2 \cdot V_3^2 V_4 = \overline{A} \cdot A^2$ 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 $V_2 V_4^2 + V_1^2 V_3 = \overline{B}$, 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. $\qquad\square$

Lemma 4.5. *For fixed* (A, B, C), *there are at most ten possibilities for* (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

$$V_1^5 = \frac{V_1 V_2^2 \cdot (V_1^2 V_3)^2}{(V_2 V_3)^2} \qquad V_3 = \frac{V_1^2 V_3}{V_1^2} \qquad V_4 = \frac{V_3^2 V_4}{V_3^2} \qquad V_2 = \frac{V_2 V_4^2}{V_4^2}. \qquad\square$$

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*

$$(2\sqrt{5} - 10) \cdot (B^2 - 4 \cdot \overline{A} \cdot A^2).$$

Proof. Using the results of the previous section, we note that

$$\sqrt{(2\sqrt{5} - 10) \cdot (B^2 - 4 \cdot \overline{A} \cdot A^2)} = 2 \cdot (\zeta - \zeta^{-1}) \cdot (V_1 \cdot V_2^2 - V_3^2 \cdot V_4).$$

By inspection, the D_5-action on the above expression is by the sign representation, and the action of $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}[\sqrt{5}])$ 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. $\square$

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 α (in particular, much less than $O(X^{\frac{3}{4}})$). 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`.

X	$\#(A, B, C)$
10	17
31	103
100	266
316	717
1000	1553
3162	3473
10000	8985
31622	19735
100000	41445
316227	89395
1000000	189993
3162277	405263

The following log plot 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.
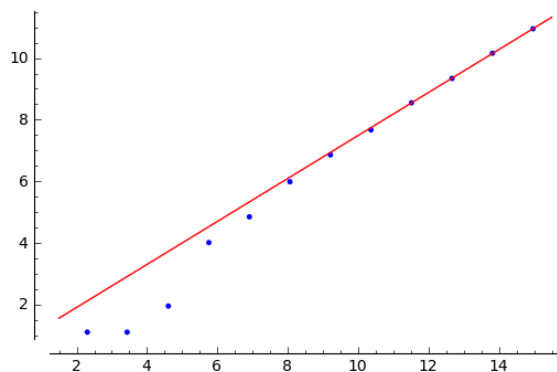
References

[1] H. Cohen. *A Survey of Discriminant Counting.* Algorithmic Number Theory (Sydney 2002), 80–94.

[2] H. Cohen and H.W. Lenstra Jr. *Heuristics on Class Groups of Number Fields.* In: Number Theory, Noordwijkerhout 1983, volume **1068** of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.

[3] D. R. Heath-Brown. *The Density of Rational Points on Curves and Surfaces.* Ann. Math. **155** (2002) 553-595.

[4] J. Klüners. *Asymptotics of Number Fields and the Cohen-Lenstra Heuristics.* J. Théor. Nombres Bordeaux 18 (2006), no. 3, 607–615.

[5] J. Klüners. *A Counterexample to Malle's Conjecture on the Asymptotics of Discriminants.* C. R. Math. Acad. Sci. Paris 340 (2005), no. 6. 411–414.

[6] G. Malle. *On the Distribution of Galois Groups II.* J. Number Theory 92 (2002), no. 2, 315–329.

[7] J. Neukirch. *Algebraic Number Theory.* Grundlehren der Mathematischen Wissenschaften, 322. Springer-Verlag, Berlin, 1999.

[8] S. Turkelli. *Connected Components of Hurwitz Schemes and Malle's Conjecture.* Submitted for publication.

[9] S. Wong. *Densities of Quartic Fields with Even Galois Groups.* Proceedings of the Amer. Math. Soc., 133 (2005), no. 10, 2873–2881.

DEPARTMENT OF MATHEMATICS. HARVARD UNIVERSITY, CAMBRIDGE, MA 02138.
  E-mail address: elarson3@gmail.com

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, EMORY UNIVERSITY, ATLANTA, GA 30322.
  E-mail address: larry.rolen@mathcs.emory.edu