

UPPER BOUNDS FOR THE NUMBER OF NUMBER FIELDS WITH ALTERNATING GALOIS GROUP

ERIC LARSON AND LARRY ROLEN

ABSTRACT. We study the number $N(n, A_n, X)$ of number fields of degree n whose Galois closure has Galois group A_n and whose discriminant is bounded by X . By a conjecture of Malle, we expect that $N(n, A_n, X) \sim C_n \cdot X^{\frac{1}{2}} \cdot (\log X)^{b_n}$ for constants b_n and C_n . For $6 \leq n \leq 84393$, the best known upper bound is $N(n, A_n, X) \ll X^{\frac{n+2}{4}}$; this bound follows from Schmidt's Theorem, which implies there are $\ll X^{\frac{n+2}{4}}$ number fields of degree n . (For $n > 84393$, there are better bounds due to Ellenberg and Venkatesh.) We show, using the important work of Pila on counting integral points on curves, that $N(n, A_n, X) \ll X^{\frac{n^2-2}{4(n-1)}+\epsilon}$, thereby improving the best previous exponent by approximately $\frac{1}{4}$ for $6 \leq n \leq 84393$.

1. INTRODUCTION AND STATEMENT OF RESULTS

For any positive integers n and X and for any fixed transitive permutation group G , we would like to count $N(n, G, X)$, defined to be the number of degree n number fields K whose Galois closure has Galois group G and for which $|D_K| \leq X$. Further let $N(n, X)$ denote the number of all degree n number fields with discriminant bounded in absolute value by X . It is an old conjecture, sometimes attributed to Linnik, that

$$N(n, X) \sim c_n X \quad (n \text{ fixed, } X \rightarrow \infty).$$

The conjecture is trivial when $n = 2$, and was proven for $n = 3$ by Davenport and Heilbronn [4] and for $n = 4, 5$ by Bhargava [1], [2]. For all but finitely many n , the current best upper bound, due to Ellenberg and Venkatesh [5] states:

$$N(n, X) \ll (X \cdot B_n)^{\exp(C \log \sqrt{n})}.$$

Here, B_n depends only on n and C is an absolute constant. For $6 \leq n \leq 84393$, the best bound, due to Schmidt [8], is

$$N(n, X) \ll X^{\frac{n+2}{4}}.$$

The authors are grateful for the support of the NSF in funding the Emory 2011 REU. The authors would like to thank our advisor Andy Yang, as well as Ken Ono for their guidance, useful conversations, improving the quality of exposition of this article, and hosting the REU.

In this note, we study the case when $G = A_n$. By a conjecture of Malle [6], we expect that

$$N(n, A_n, X) \stackrel{?}{\sim} c(n) \cdot X^{\frac{1}{2}} \cdot (\log X)^{b(n)-1},$$

for some constant $c(n)$ and an explicit constant $b(n)$. Here we improve Schmidt's general bound in our case. In particular, we can use Pila's results on counting integral points on geometrically irreducible curves [7] to show the following:

Theorem 1.1. *We have*

$$N(n, A_n, X) \ll X^{\frac{n^2-2}{4(n-1)}} \cdot \log(X)^{2n+1},$$

where the implied constant depends only on n .

Remark 1.2. Throughout this note, we write $f \ll g$ to mean that $f \leq c \cdot g$ for a constant c depending only on the degree of number field (or degree of the algebraic variety) in question.

Note that the exponent improves on the previous record by a power of X of about $\frac{1}{4}$ for these n . The method uses point counting on varieties in a similar manner as in [5]. The improvement follows from viewing these varieties as fibrations of curves, controlling the fibers which are not geometrically irreducible, and using a bound of Pila on counting integral points on geometrically irreducible curves.

2. UPPER BOUNDS VIA POINT COUNTING

If K is a number field of discriminant D_K and degree n , 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 .

When $\text{Gal}(K^{\text{gal}}/\mathbb{Q}) \simeq A_n$, then K must be a primitive extension of \mathbb{Q} , so $K = \mathbb{Q}(\alpha)$ and the characteristic polynomial of α will determine K . One can use this to give an upper bound on $N(n, A_n, X)$. To see this, note that every pair (K, α) as above gives a \mathbb{Z} -point of $\text{Spec } R$, for

$$R = \mathbb{Z}[x_1, x_2, \dots, x_n]^{A_n}/(s_1) \quad \text{where} \quad s_1 = x_1 + x_2 + \dots + x_n.$$

(Here $\mathbb{Z}[x_1, x_2, \dots, x_n]^{A_n}$ denotes the ring of A_n -invariants in $\mathbb{Z}[x_1, x_2, \dots, x_n]$.) Now, it is a classical theorem that the ring of A_n -invariant functions is generated by the symmetric functions and the square root of the discriminant, i.e. we have

$$\mathbb{Z}[x_1, x_2, \dots, x_n]^{A_n} \simeq \mathbb{Z}[s_1, s_2, \dots, s_n, D]/(D^2 = \text{Disc}(t^n - s_1 t^{n-1} + \dots \pm s_n)),$$

so therefore

$$R \simeq \mathbb{Z}[s_1, s_2, \dots, s_n, D]/(D^2 = \text{Disc}(t^n + s_2 t^{n-2} + \dots \pm s_n)).$$

Thus, to give an upper bound on $N(n, A_n, X)$, it suffices to bound the number of \mathbb{Z} -points of $\text{Spec } R$ which satisfy the inequalities

$$(1) \quad |s_j| \ll X^{\frac{j}{2(n-1)}} \quad \text{and} \quad |D| \ll X^{\frac{n}{4}}.$$

3. PROOF OF THEOREM 1.1 WHEN n IS EVEN

When n is even, Theorem 1.1 is relatively straight-forward; therefore, we begin by examining this case.

Lemma 3.1. *Theorem 1.1 holds when n is even.*

Proof. By fixing s_2, s_3, \dots, s_{n-1} , we can view $\text{Spec } R$ as a fibration of plane curves over \mathbb{A}^{n-2} . Each of these curves is then the zero locus of a polynomial of the form

$$(2) \quad D^2 = \text{a polynomial of odd degree in } s_n.$$

In particular, these curves are geometrically irreducible. Therefore, we can apply Pila's bound [7], which states that the number of integral points on a geometrically irreducible plane curve of degree d whose coordinates are bounded in absolute value by B is at most

$$(3d)^{4d+8} \cdot B^{\frac{1}{d}} \cdot (\log B)^{2d+3} \ll B^{\frac{1}{d}} \cdot (\log B)^{2d+3}.$$

For the curves defined by (2), we seek to count integral points with

$$|s_n| \ll X^{\frac{n}{2(n-1)}} \quad \text{and} \quad |D| \ll X^{\frac{n}{4}}.$$

By Pila's result above, the number of such points is

$$\ll \left(X^{\frac{n}{4}}\right)^{\frac{1}{n-1}} \cdot (\log(X^{\frac{n}{4}}))^{2(n-1)+3} \ll X^{\frac{n}{4(n-1)}} \cdot (\log X)^{(2n+1)}.$$

Therefore, using the bounds (1) on the other s_j from the previous section, we have

$$N(n, A_n, X) \ll \left(\prod_{j=2}^{n-1} X^{\frac{j}{2(n-1)}}\right) \cdot X^{\frac{n}{4(n-1)}} \cdot (\log X)^{2n+1} = X^{\frac{n^2-2}{4(n-1)}} \cdot (\log X)^{2n+1}. \quad \square$$

4. PROOF OF THEOREM 1.1 WHEN n IS ODD

In the case when n is odd, the argument of Lemma 3.1 breaks down because the curves in the fibration do not have to be geometrically irreducible. In order to circumvent this difficulty, we will show in this section that “most” of the fibers of the map $\text{Spec } R \rightarrow \mathbb{A}^{n-2}$ are geometrically irreducible. We will then bound the number of integral points on the fibers that fail to be geometrically irreducible.

Definition 4.1. We say two polynomials $f, g \in \mathbb{C}[z]$ are *equivalent* if $f(z) = g(az+b)$ for some $a \in \mathbb{C}^\times$ and $b \in \mathbb{C}$.

Definition 4.2. We say that c is a *critical value* of a polynomial f if $c = f(d)$ for some d with $f'(d) = 0$.

Lemma 4.3. Fix a finite set of points $S \subset \mathbb{C}$ and an integer d . Then there are finitely many equivalence classes of polynomials of degree d whose set of critical values is contained in S .

Proof. Write $S = \{z_1, z_2, \dots, z_n\}$, and fix some $z_0 \notin S$. Then any polynomial of degree d whose set of critical values f is contained in S gives rise to a map

$$f^*: \pi_1(\mathbb{C} - S) \rightarrow \text{Aut}(f^{-1}(z_0)) \simeq S_d.$$

Since S is finite, $\pi_1(\mathbb{C} - S)$ is finitely generated; moreover, S_d is finite, so there are only finitely many possibilities for f^* .

Thus, it suffices to show that any two polynomials f and g for which $f^* = g^*$ are equivalent. But the classical theory of covering spaces implies that when $f^* = g^*$, then f and g must differ by a deck transformation, which must be analytic because f and g are analytic coverings. The desired conclusion then follows from the well-known fact that any automorphism of $\widehat{\mathbb{C}}$ fixing ∞ is of the form $z \mapsto a \cdot z + b$ with $a \in \mathbb{C}^\times$ and $b \in \mathbb{C}$. \square

Lemma 4.4. Let n be an integer. For any monic polynomial $p(z) \in \mathbb{C}[z]$ of degree $n - 1$, there are only finitely many values of $(a_2, a_3, \dots, a_{n-1}) \in \mathbb{C}^{n-2}$ such that $p(z)$ is the discriminant of the polynomial

$$q(t) = t^n + a_2 t^{n-2} + \dots + a_{n-1} t - z.$$

Proof. In order for $p(z)$ to be the discriminant of $q(t)$, every root r of $p(z)$ must be (with multiplicity) a critical value of the polynomial $q_0(t) = t^n + a_1 t^{n-1} + \dots + a_{n-1} t$. Since q_0 is a polynomial of degree n , it has $n - 1$ critical values (counted with multiplicity); since $p(z)$ is a polynomial of degree of $n - 1$, it has $n - 1$ zeros (counted with multiplicity). Therefore, every critical value of q_0 is a root of $p(z)$. This completes the proof by Lemma 4.3. \square

Lemma 4.5. The locus of $(s_2, s_3, \dots, s_{n-1}) \in \mathbb{A}^{n-2}$ such that the plane curve

$$x^2 = \text{Disc}(t^n + s_2 t^{n-2} + \dots \pm s_{n-1} t - y)$$

fails to be geometrically irreducible is an affine variety of dimension at most $\frac{n-1}{2}$.

Proof. The corresponding plane curve fails to be geometrically irreducible if and only if the polynomial

$$p(y) = \text{Disc}(t^n + s_2 t^{n-2} + \dots \pm s_{n-1} t - y)$$

is a perfect square. But the coefficients of $p(y)$ are regular functions in s_2, s_3, \dots, s_{n-1} . Moreover, the map $\mathbb{A}^{n-2} \rightarrow \mathbb{A}^{n-1}$ induced by these regular functions is a finite map by Lemma 4.4.

Since the locus of $(b_1, b_2, \dots, b_{n-1}) \in \mathbb{A}^{n-1}$ such that $t^{n-1} + b_1 t^{n-2} + \dots + b_{n-1}$ is a perfect square is a Zariski-closed set of dimension $\frac{n-1}{2}$, this completes the proof. \square

Using the above lemma together with the ideas from Section 3, we can complete the proof of Theorem 1.1.

Proof of Theorem 1.1 for n odd. When $n = 3$, this follows from a result of Wright [9], and when $n = 5$, this follows from a result of Bhargava [2]. Thus, we can assume $n \geq 7$.

Again, we consider the fibration $\text{Spec } R \rightarrow \mathbb{A}^{n-2}$ given by fixing s_2, s_3, \dots, s_{n-1} . The argument given in Lemma 3.1 implies the number of integral points lying on the geometrically irreducible fibers satisfies the required bound; it remains to see that the number of integral points lying on the geometrically reducible fibers also satisfies the required bound.

To prove this, we first note that by Lemma 4.5, all such points are contained in a subvariety of $\text{Spec } R$ of dimension at most $\frac{n-1}{2} + 1 = \frac{n+1}{2}$. Moreover, the projection map $\text{Spec } R \rightarrow \mathbb{A}^{n-1}$ given by fixing s_2, s_3, \dots, s_n is finite, so it suffices to bound the number of integral points in the box

$$|s_j| \leq X^{\frac{j}{2(n-1)}}$$

lying in a particular affine variety of dimension $\frac{n+1}{2}$. But the number of such points can be bounded by the product of the $\frac{n+1}{2}$ largest sides of the box, and therefore is

$$\ll \prod_{j=\frac{n+1}{2}}^n X^{\frac{j}{2(n-1)}} = X^{\frac{(3n+1)(n+1)}{16(n-1)}},$$

and therefore satisfies the required bound, as long as $n \geq 7$. \square

REFERENCES

- [1] M. Bhargava. *The Density of Discriminants of Quartic Rings and Fields*. Ann. of Math. (2) 162 (2005), no. 2, 1031–1063.
- [2] ———. *The Density of Discriminants of Quintic Rings and Fields*. Ann. of Math. (2) 172 (2010), no. 3, 1559–1591.
- [3] H. Cohen. *A Survey of Discriminant Counting*. Algorithmic Number Theory (Sydney 2002), 80–94.
- [4] H. Davenport and H. Heilbronn. *On the Density of Discriminants of Cubic Fields II*. Proc. Roy. Soc. London Ser. A **322** (1971), no. 1551, 405–420.
- [5] J. Ellenberg and A. Venkatesh. *The Number of Extensions of a Number Field with Fixed Degree and Bounded Discriminant*. Ann. of Math. (2) 163 (2006), no. 2, 723–741.
- [6] G. Malle. *On the Distribution of Galois Groups II*. J. Number Theory 92 (2002), no. 2, 315–329.
- [7] J. Pila. *Density of Integer Points on Plane Algebraic Curves*. Internat. Math. Res. Notices **1996**, no. 18, 903–912.

- [8] W. M. Schmidt. *Number Fields of Given Degree and Bounded Discriminant*. Columbia University Number Theory Seminar (New York 1992), Astérisque **228** (1995), 189-195.
- [9] D. Wright. *Distribution of Discriminants of Abelian Extensions*. Proc. London Math. Soc. (3) 58 (1989), no. 1, 17-50.

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`