Bounds on the Number of Extensions of a Number Field with Bounded Discriminant and Specified Galois Group

Evan P. Dummit

University of Wisconsin-Madison

January 15, 2014

A Motivating Question

Question 1. How many number fields are there whose Galois group is the simple group of order 168?

A Motivating Question

Question 1. How many number fields are there whose Galois group is the simple group of order 168?

This is not quite the right question. Let's try again:

An Improved Question

Question 1 (improved). How many number fields $L/\mathbb{Q}$ are there, such that $[L:\mathbb{Q}] = 7$, the Galois group of the Galois closure of $L/\mathbb{Q}$ is the simple group of order 168, and the (absolute) discriminant of $L/\mathbb{Q}$ is less than X?

An Improved Question

Question 1 (improved). How many number fields $L/\mathbb{Q}$ are there, such that $[L:\mathbb{Q}] = 7$, the Galois group of the Galois closure of $L/\mathbb{Q}$ is the simple group of order 168, and the (absolute) discriminant of $L/\mathbb{Q}$ is less than X?

The answer will be a function of X so a natural question is: how fast does it grow, in terms of X?

The General Question

Let K be a number field and G be a permutation group, and define $N_{K,n}(X;G)$ to be the number of number fields L (up to K-isomorphism) such that

- $[L:K]=n$,
- the discriminant norm $\mathrm{Nm}_{K/\mathbb{Q}}(D_{L/K})<X$ (where $D_{L/K}$ is the relative discriminant ideal of the extension L/K and $\mathrm{Nm}_{K/\mathbb{Q}}$ denotes the absolute norm on ideals), and
- the Galois group of the Galois closure of L/K is G.

The General Question

Let K be a number field and G be a permutation group, and define $N_{K,n}(X; G)$ to be the number of number fields L (up to K-isomorphism) such that

- $[L : K] = n$,
- the discriminant norm $\mathrm{Nm}_{K/\mathbb{Q}}(D_{L/K}) < X$ (where $D_{L/K}$ is the relative discriminant ideal of the extension L/K and $\mathrm{Nm}_{K/\mathbb{Q}}$ denotes the absolute norm on ideals), and
- the Galois group of the Galois closure of L/K is G.

Question 2. How fast does $N_{K,n}(X; G)$ grow as X grows?

History, I

Theorem 1 [Schmidt]. For all n and all base fields K,

$$N_{K,n}(X; S_n) \ll X^{(n+2)/4}.$$

History, I

Theorem 1 [Schmidt]. For all n and all base fields K,

$$N_{K,n}(X; S_n) \ll X^{(n+2)/4}.$$

Theorem 2 [Ellenberg, Venkatesh]. For all $n > 2$ and all base fields K,

$$N_{K,n}(X; S_n) \ll (X\, D_{K/\mathbb{Q}}^n\, A_n^{[K:\mathbb{Q}]})^{\exp(C\sqrt{\log\, n})},$$

where A_n is a constant depending only on n and C is an absolute constant.

History, II

Conjecture 3 [Malle, weak form]. For any $\epsilon > 0$, then $N_{K,n}(X; G) \ll X^{a(G)+\epsilon}$, where $0 < a(G) \leq 1$ is a computable constant depending on G and contained in $\left\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots\right\}$.

History, II

Conjecture 3 [Malle, weak form]. For any $\epsilon > 0$, then $N_{K,n}(X; G) \ll X^{a(G)+\epsilon}$, where $0 < a(G) \leq 1$ is a computable constant depending on G and contained in $\left\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots\right\}$.

This conjecture is known to hold over general number fields K when G is a nilpotent group, hence (in particular) when G is abelian.

Results, I

Theorem 4 [D.]. Let G be a proper transitive subgroup of S_n. Then

$$N_{K,n}(X; G) \ll X^{\frac{1}{2(n-1)}\left[\sum_{i=1}^{n-1} \deg(f_{i+1}) - 1\right] + \epsilon},$$

where the f_i for $1 \leq i \leq n$ are a set of "primary invariants" for G, whose degrees depend on the structure of G but which (at worst) satisfy $\deg(f_i) \leq i$.

Example

Corollary 5. If G is the simple group of order 168 embedded in S_7, then $N_{K,7}(X; G) \ll X^{11/6+\epsilon}$.

Example

Corollary 5. If G is the simple group of order 168 embedded in S_7, then $N_{K,7}(X; G) \ll X^{11/6+\epsilon}$.

Remark. For comparison, Schmidt's bound gives the weaker upper bound of $\ll X^{9/4}$, whereas Malle's conjecture posits that the actual count is $\ll X^{1/2+\epsilon}$.

Outline of Techniques

Here is a rough outline of the steps involved in the proof of Theorem 4:

Outline of Techniques

Here is a rough outline of the steps involved in the proof of Theorem 4:

- Use the geometry of numbers and Minkowski's lattice theorems to construct an element $x \in L$ whose archimedean norms are small.

Outline of Techniques

Here is a rough outline of the steps involved in the proof of Theorem 4:

- Use the geometry of numbers and Minkowski's lattice theorems to construct an element $x \in L$ whose archimedean norms are small.
- Use the invariant theory of G to construct a finite scheme map to affine space.

Outline of Techniques

Here is a rough outline of the steps involved in the proof of Theorem 4:

- Use the geometry of numbers and Minkowski's lattice theorems to construct an element $x \in L$ whose archimedean norms are small.
- Use the invariant theory of G to construct a finite scheme map to affine space.
- Count integral scheme points whose images lie in an appropriate box, to obtain an upper bound on the number of possible x and hence the number of possible extensions L/K.

Future Directions

Some ongoing and future work:

- Generalize results to more general representations of groups.
- Strengthen point-counting techniques.

Future Directions

Some ongoing and future work:

- Generalize results to more general representations of groups.
- Strengthen point-counting techniques.
- Adapt results to other types of extensions (e.g., of function fields).
- Investigate whether these methods give information about other kinds of arithmetic statistics (class groups, Cohen-Lenstra).

Acknowledgements

Thanks to

- My doctoral advisor, Jordan Ellenberg
- The organizers of this conference and this session
- You, for attending this talk!