Counting Number Field Extensions

Evan P. Dummit

University of Rochester

April 12, 2015

Some Notation

Let:

- n be a positive integer

Some Notation

Let:

- n be a positive integer,
- K be a number field of absolute discriminant D_K

Some Notation

Let:

- n be a positive integer,
- K be a number field of absolute discriminant D_K,
- G be a transitive subgroup of the symmetric group S_n

Some Notation

Let:

- n be a positive integer,
- K be a number field of absolute discriminant D_K,
- G be a transitive subgroup of the symmetric group S_n,
- $\mathcal{D}_{L/K}$ be the relative discriminant ideal of the extension L/K

Some Notation

Let:

- n be a positive integer,
- K be a number field of absolute discriminant D_K,
- G be a transitive subgroup of the symmetric group S_n,
- $\mathcal{D}_{L/K}$ be the relative discriminant ideal of the extension L/K,
- $\mathrm{Nm}_{K/\mathbb{Q}}$ be the absolute norm on ideals

Some Notation

Let:

- n be a positive integer,
- K be a number field of absolute discriminant D_K,
- G be a transitive subgroup of the symmetric group S_n,
- $\mathcal{D}_{L/K}$ be the relative discriminant ideal of the extension L/K,
- $\mathrm{Nm}_{K/\mathbb{Q}}$ be the absolute norm on ideals,
- The Galois closure of L/K be $\hat{L}/K$.

Counting Functions

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 $\mathrm{Nm}_{K/\mathbb{Q}}(D_{L/K})$ is less than X, and
- The Galois group $\mathrm{Gal}(\hat{L}/K)$ is permutation-isomorphic to G.

Counting Functions

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 $\mathrm{Nm}_{K/\mathbb{Q}}(D_{L/K})$ is less than X, and
- The Galois group $\mathrm{Gal}(\hat{L}/K)$ is permutation-isomorphic to G.

Also define $N_{K,n}(X)$ to be the number of extensions satisfying the first two conditions above (i.e., with no condition on the Galois group).

Counting Problems

Question 1

For a given K and n, how fast does $N_{K,n}(X)$ grow as X grows?

Counting Problems

Question 1

For a given K and n, how fast does $N_{K,n}(X)$ grow as X grows?

Conjecture 2 (Linnik?)

For all n and all base fields K,

$$N_{K,n}(X) \sim X.$$

Counting Problems

Question 1

For a given K and n, how fast does $N_{K,n}(X)$ grow as X grows?

Conjecture 2 (Linnik?)

For all n and all base fields K,

$$N_{K,n}(X) \sim X.$$

This result is known to hold for $n \leq 3$ for general base fields, and for $n \leq 5$ over $\mathbb{Q}$: these results are due to Davenport-Heilbronn, Datskovsky-Wright, Kable-Yukie, and Bhargava.

General Upper Bounds

We do have some upper bounds for larger n:

General Upper Bounds

We do have some upper bounds for larger n:

Theorem 3 (Schmidt (1995))

For all n and all base fields K,

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

General Upper Bounds

We do have some upper bounds for larger n:

Theorem 3 (Schmidt (1995))

For all n and all base fields K,

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

Theorem 4 (Ellenberg, Venkatesh (2006))

For all $n > 2$ and all base fields K,

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

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

More Conjectures

Question 5

For a given G, K, and n, how fast does $N_{K,n}(X; G)$ grow as X grows?

More Conjectures

Question 5

For a given G, K, and n, how fast does $N_{K,n}(X;G)$ grow as X grows?

Conjecture 6 (Malle, weak form (2002))

For any $\epsilon > 0$,

$$N_{K,n}(X;G) \ll X^{a(G)+\epsilon}$$

where $0 < a(G) \leq 1$ is a computable constant depending on G, contained in $\left\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots\right\}$.

More Conjectures

Question 5

For a given G, K, and n, how fast does $N_{K,n}(X;G)$ grow as X grows?

Conjecture 6 (Malle, weak form (2002))

For any $\epsilon > 0$,

$$N_{K,n}(X;G) \ll X^{a(G)+\epsilon}$$

where $0 < a(G) \leq 1$ is a computable constant depending on G, contained in $\left\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots\right\}$.

This conjecture (or a stronger version) is known in a number of cases: for example, if $n \leq 4$, or if G is a nilpotent group.

Counting by Discriminant

Theorem 7 (D. (2014))

Let $n \geq 2$, let K be any number field, and let G be a proper transitive subgroup of S_n. Also, let t be such that if G' is the intersection of a point stabilizer in S_n with G, then any subgroup of G properly containing G' has index at least t. Then for any $\epsilon > 0$,

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

where the f_i for $1 \leq i \leq n$ are a set of "primary invariants" for G, whose degrees (in particular) satisfy $\deg(f_i) \leq i$.

Primary Invariants?

Here is a quick recap of some invariant theory:

Primary Invariants?

Here is a quick recap of some invariant theory:

- If $\rho : G \to GL_n(\mathbb{C})$ is a (faithful) complex representation of G, let G act on $\mathbb{C}[x_1, \cdots, x_n]$ via ρ.

Primary Invariants?

Here is a quick recap of some invariant theory:

- If $\rho : G \to GL_n(\mathbb{C})$ is a (faithful) complex representation of G, let G act on $\mathbb{C}[x_1, \cdots, x_n]$ via ρ.
- Let $R = \mathbb{C}[x_1, \cdots, x_n]^G$ be the G-invariant polynomials.

Primary Invariants?

Here is a quick recap of some invariant theory:

- If $\rho : G \to GL_n(\mathbb{C})$ is a (faithful) complex representation of G, let G act on $\mathbb{C}[x_1, \cdots, x_n]$ via ρ.
- Let $R = \mathbb{C}[x_1, \cdots, x_n]^G$ be the G-invariant polynomials.
- There exist elements $f_1, \cdots, f_n \in R$ such that R is a finitely-generated module over $A := \mathbb{C}[f_1, \cdots, f_n]$. These polynomials are called “primary invariants” of ρ.

Primary Invariants?

Here is a quick recap of some invariant theory:

- If $\rho : G \to GL_n(\mathbb{C})$ is a (faithful) complex representation of G, let G act on $\mathbb{C}[x_1, \cdots, x_n]$ via ρ.
- Let $R = \mathbb{C}[x_1, \cdots, x_n]^G$ be the G-invariant polynomials.
- There exist elements $f_1, \cdots, f_n \in R$ such that R is a finitely-generated module over $A := \mathbb{C}[f_1, \cdots, f_n]$. These polynomials are called "primary invariants" of ρ.
- Moreover, there exist polynomials $g_1, g_2, \cdots, g_k \in R$ such that $R = A \cdot g_1 + \cdots + A \cdot g_k$; these polynomials are called "secondary invariants" of ρ.

Primary Invariants, II

Example

Let $G = S_n$ and ρ be the representation of G that acts on $\mathbb{C}[x_1, \cdots, x_n]$ by index permutation. Then the elementary symmetric polynomials are a set of primary invariants for G.

Primary Invariants, II

Example

Let $G = S_n$ and ρ be the representation of G that acts on $\mathbb{C}[x_1, \cdots, x_n]$ by index permutation. Then the elementary symmetric polynomials are a set of primary invariants for G.

In fact, the elementary symmetric polynomials are a set of primary invariants for any permutation representation...

Primary Invariants, II

Example

Let $G = S_n$ *and* ρ *be the representation of* G *that acts on* $\mathbb{C}[x_1, \cdots, x_n]$ *by index permutation. Then the elementary symmetric polynomials are a set of primary invariants for* G*.*

In fact, the elementary symmetric polynomials are a set of primary invariants for any permutation representation... but not necessarily of minimal degree!

Primary Invariants, III

Example

Let $G = \langle (1\,2\,3\,4\,5\,6\,7),\ (1\,2)(3\,6)\rangle \cong PSL_2(\mathbb{F}_7)$*, with* ρ *the natural permutation representation. The following polynomials are a set of primary invariants for* ρ*:*

$$
\begin{aligned}
f_1 &= x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 \\
f_2 &= x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2 \\
f_3 &= x_1^3 + x_2^3 + x_3^3 + x_4^3 + x_5^3 + x_6^3 + x_7^3 \\
f_4 &= x_1x_2x_3 + [\mathit{26\ more\ terms}] + x_5x_6x_7 \\
f_5 &= x_1^4 + x_2^4 + x_3^4 + x_4^4 + x_5^4 + x_6^4 + x_7^4 \\
f_6 &= x_1^2x_2x_3 + [\mathit{82\ more\ terms}] + x_5x_6x_7^2 \\
f_7 &= x_1^7 + x_2^7 + x_3^7 + x_4^7 + x_5^7 + x_6^7 + x_7^7
\end{aligned}
$$

Primary Invariants, IV: A New Hope

By the previous slide, we know that if G is the simple group of order 168 and ρ is its permutation embedding in S_7, then ρ has a set of primary invariants of degrees 1, 2, 3, 3, 4, 4, and 7. For this group, one can also check that the t-parameter is equal to 1. Therefore, Theorem 7 yields the following:

Primary Invariants, IV: A New Hope

By the previous slide, we know that if G is the simple group of order 168 and ρ is its permutation embedding in S_7, then ρ has a set of primary invariants of degrees 1, 2, 3, 3, 4, 4, and 7. For this group, one can also check that the t-parameter is equal to 1. Therefore, Theorem 7 yields the following:

Corollary 8

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

Primary Invariants, IV: A New Hope

By the previous slide, we know that if G is the simple group of order 168 and ρ is its permutation embedding in S_7, then ρ has a set of primary invariants of degrees 1, 2, 3, 3, 4, 4, and 7. For this group, one can also check that the t-parameter is equal to 1. Therefore, Theorem 7 yields the following:

Corollary 8

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

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 Proof

Here is a rough outline of the steps involved in the proof of Theorem 7:

Outline of Proof

Here is a rough outline of the steps involved in the proof of Theorem 7:

- Use the geometry of numbers and Minkowski's lattice theorems to construct an element $\alpha \in \mathcal{O}_L$ generating L/K whose archimedean norms are small.

Outline of Proof

Here is a rough outline of the steps involved in the proof of Theorem 7:

- Use the geometry of numbers and Minkowski's lattice theorems to construct an element $\alpha \in \mathcal{O}_L$ generating L/K whose archimedean norms are small.
- Use the invariant theory of G to construct a finite scheme map to affine space.

Outline of Proof

Here is a rough outline of the steps involved in the proof of Theorem 7:

- Use the geometry of numbers and Minkowski's lattice theorems to construct an element $\alpha \in \mathcal{O}_L$ generating L/K 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 α and hence the number of possible extensions L/K.

Transitive Subgroups of S_7

Here are the results of Theorem 7 for transitive subgroups of S_7:

#	Ord	Isom to	Invar. Degs.	Result	Malle	Schmidt
7T1	7	C_7	1,2,2,2,3,4,7	$X^{19/12}$	$X^{1/6}$	$X^{9/4}$
7T2	14	D_7	1,2,2,2,3,4,7	$X^{19/12}$	$X^{1/3}$	$X^{9/4}$
7T3	21	F_{21}	1,2,3,3,3,4,7	$X^{7/4}$	$X^{1/4}$	$X^{9/4}$
7T4	42	F_{42}	1,2,3,3,4,6,7	X^{2}	$X^{1/3}$	$X^{9/4}$
7T5	168	$PSL_2(\mathbb{F}_7)$	1,2,3,3,4,4,7	$X^{11/6}$	$X^{1/2}$	$X^{9/4}$
7T6	2520	A_7	1,2,3,4,5,6,7	$X^{13/6}$	$X^{1/2}$	$X^{9/4}$

Transitive Subgroups of S_7

Here are the results of Theorem 7 for transitive subgroups of S_7:

#	Ord	Isom to	Invar. Degs.	Result	Malle	Schmidt
7T1	7	C_7	1,2,2,2,3,4,7	$X^{19/12}$	$X^{1/6}$	$X^{9/4}$
7T2	14	D_7	1,2,2,2,3,4,7	$X^{19/12}$	$X^{1/3}$	$X^{9/4}$
7T3	21	F_{21}	1,2,3,3,3,4,7	$X^{7/4}$	$X^{1/4}$	$X^{9/4}$
7T4	42	F_{42}	1,2,3,3,4,6,7	X^{2}	$X^{1/3}$	$X^{9/4}$
7T5	168	$PSL_2(\mathbb{F}_7)$	1,2,3,3,4,4,7	$X^{11/6}$	$X^{1/2}$	$X^{9/4}$
7T6	2520	A_7	1,2,3,4,5,6,7	$X^{13/6}$	$X^{1/2}$	$X^{9/4}$

For horizontal brevity, the results appear without the $+\epsilon$ term in the exponent, and are also stated for the base field $K = \mathbb{Q}$. A superior bound is available for the cyclic and dihedral groups (the former is abelian, while dihedral extensions can be bounded using class field theory).

Future Directions

Some work I am still pursuing:

- Compute (or bound) the invariant degrees for more representations of groups.

Future Directions

Some work I am still pursuing:

- Compute (or bound) the invariant degrees for more representations of groups.
- Strengthen point-counting techniques.

Future Directions

Some work I am still pursuing:

- Compute (or bound) the invariant degrees for more representations of groups.
- Strengthen point-counting techniques.
- Generalize methods to other representations beyond permutation representations.

Future Directions

Some work I am still pursuing:

- Compute (or bound) the invariant degrees for more representations of groups.
- Strengthen point-counting techniques.
- Generalize methods to other representations beyond permutation representations.
- Adapt results to other types of extensions (e.g., of function fields).

End

Thank you for attending my talk!