Power-saving error terms for the number of D_4 quartic extensions over a number field ordered by discriminant

Alina Bucur (UCSD)

Joint work with Alexandra Florea, Allechar Serrano López, and Ila Varma

Dubrovnik 2023

Supported by NSF and the Simons Foundation

Setup and motivation

K a number field

d a degree

$G \hookrightarrow S_d$ a Galois group

We want to study the set

$$\mathcal{F}_{d,K}(G) = \left\{ L/K; [L:K] = d, \mathrm{Gal}(\tilde{L}/K) \simeq G \right\}$$

where $\tilde{L}$ denotes the normal closure of L over K.

$$N_{d,K}(G, X) = \{L \in \mathcal{F}_{d,K}(G), \mathrm{Norm}\left(\mathrm{Disc}(L/K)\right) < X\}$$

Question

How does $N_{d,K}(G, X)$ vary as $X \to \infty$?

General strategy

Study the generating series

$$Z_{d,K}(G,s) = \sum_{L \in \mathcal{F}_{d,K}(G)} \frac{1}{(\mathrm{Norm}\,\mathrm{Disc}(L/F))^s} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

where

$$a_n = \#\left\{L \in \mathcal{F}_{d,K}(G), \mathrm{Norm}\left(\mathrm{Disc}(L/K)\right) = n\right\}.$$

Then

$$N_{d,K}(G,X) = \sum_{n<X} a_n.$$

Analytic number theory magic

For any $\alpha > 1$

$$\frac{1}{2\pi i}\int_{\alpha-i\infty}^{\alpha+i\infty} x^s \frac{ds}{s} = \begin{cases} 1 & x > 1 \\ 1/2 & x = 1 \\ 0 & 0 < x < 1. \end{cases}$$

Thus if $\alpha > 1$ is in the region where $Z(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ is absolutely convergent, then

$$\frac{1}{2\pi i}\int_{\alpha-i\infty}^{\alpha+i\infty} Z(s) x^s \frac{ds}{s} = \sum_{n=1}^{\infty} a_n \frac{1}{2\pi i}\int_{\alpha-i\infty}^{\alpha+i\infty} (x/n)^s \frac{ds}{s}$$

$$= \sum_{n<x} a_n.$$

Analytic number theory magic

If $\alpha > 1$ is in the region where $Z(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ is absolutely convergent, then

$$\sum_{n<x} a_n = \frac{1}{2\pi i} \int_{\alpha - i\infty}^{\alpha + i\infty} Z(s) x^s \frac{ds}{s} = \sum_{n=1}^{\infty} a_n \frac{1}{2\pi i} \int_{\alpha - i\infty}^{\alpha + i\infty} (x/n)^s \frac{ds}{s}$$

If the right-most pole of $Z(s)$ is at $s = a$ and has order $b + 1$ then we get

$$\sum_{n<x} a_n \sim c X^a \log X^b.$$

Upshot: if we know the meromorphic/polar behavior of the generating series

$$Z_{d,K}(G,s) = \sum_{L \in \mathcal{F}_{d,K}(G)} \frac{1}{(\mathrm{Norm}\,\mathrm{Disc}(L/F))^s}$$

we will get a result of the form

$$N_{d,K}(G,X) \sim c_{d,K}(G) X^{a_{d,K}(G)} \log X^{b_{d,K}(G)}.$$

Problem

It is hard to pull this off.

Known results (a very incomplete list!)

- $d = 2, K = \mathbb{Q}$: Gauss ? (the proof is not analytic!)

$$N_{2,\mathbb{Q}}(X) = \frac{6}{\pi^2} X + O\left(X^{1/2}\right)$$

- $d = 2$, K arbitrary: Datskovsky–Wright (1988)

$$a_{2,K} = 1 \qquad b_{2,K} = 0 \qquad c_{2,K} = 2^{-r_2(K)-1} \frac{1}{\zeta_K(2)} \operatorname{Res}_{s=1} \zeta_K(s)$$

- $d = 3$
  - $G = C_3, K = \mathbb{Q}$: Cohn (1954)

$$a_{3,\mathbb{Q}}(C_3) = 1/2 \qquad b_{3,\mathbb{Q}}(C_3) = 0 \qquad c_{3,\mathbb{Q}}(C_3) = \frac{11\sqrt{3}}{36\pi} \prod_{p \equiv 1 (\text{mod } 6)} \frac{(p+2)(p-1)}{p(p+1)}$$

  - $G = S_3, K = \mathbb{Q}$: Davenport–Heilbronn (1971)

$$a_{3,\mathbb{Q}}(S_3) = 1 \qquad b_{3,\mathbb{Q}}(S_3) = 0 \qquad c_{3,\mathbb{Q}}(S_3) = \frac{1}{3\zeta(3)}$$

  - $G = S_3$, K arbitrary: Datskovsy–Wright (1988)

$$a_{3,K}(S_3) = 1 \qquad b_{3,K}(S_3) = 0 \qquad c_{3,K}(S_3) = \left(\frac{2}{3}\right)^{r_1(K)-1} \left(\frac{1}{6}\right)^{r_2(K)} \frac{1}{3\zeta_K(3)} \operatorname{Res}_{s=1} \zeta_K(s)$$

Abelian groups: Wright (1989)

In 1980s, Wright proved an asymptotic for the general case of an abelian group G of order d.

$$a_{d,K}(G) = \frac{1}{d}\left(1 - \frac{1}{p}\right)^{-1}, \; b_{d,K}(G) = \frac{n_p}{[K(\zeta_p) : K]},$$

where p is the smallest prime dividing n, and n_p denotes the number of elements of G of order p.

Question

Can we predict $a_{n,K}(G), b_{n,K}(G), c_{n,K}(G)$?

Question

Are there general formulas for them?

Malle's conjecture

Inspired by Wright's result, as well as the Davenport–Heilbronn asymptotic (1971) for $K = \mathbb{Q}$, $n = 3$ and $G = S_3$ and Datskovsky–Wright (1988) for any number field K, $n = 3$ and $G = S_3$.

Conjecture (Malle 2000s)

The exponent $a_{d,K}(G)$ does not depend on the base field K and

$$a_d(G) = \frac{1}{\min_{g \in G \setminus 1} \operatorname{Ind}(g)},$$

where the index of an element g is defined as $\operatorname{Ind}(g) := d - \#$ orbits of $\{1, 2, \ldots d\}$ when acted upon by g via the embedding $G \hookrightarrow S_d$;

Note: If G contains a transposition, then $a_d(G) = 1$.

$b_{d,K}(G) + 1 = \#\{\mathrm{Gal}(\overline{K}/K)\text{-orbits of } G\text{-conjugacy classes of minimal index}\}$

In 2005 Klüners proved that for

$$G = C_3 \wr C_2 \text{ over the base field } K = \mathbb{Q}$$

there are 'too many' extensions of discriminant up to X, namely that the power of $\log X$ is higher than expected.

How about $c_{d,K}(G)$?

Bhargava predicts $c_{d,K}(G)$ for $G = S_d$ and $K = \mathbb{Q}$.

These predictions cannot be extended to $G = D_4$ as they would contradict a theorem of Cohen, Diaz y Diaz, Olivier (CDO).

Today: $d = 4, G = D_4$

$K = \mathbb{Q}$: Cohen, Diaz y Diaz, Olivier

K arbitrary: B, Florea, Serrano López, Varma

$G = D_4$: following Cohen, Diaz y Diaz, Olivier

Main idea: relate D_4 extensions to generating series we already understand from the work of Wright and get *uniformity* in the error terms for the infinitely many of the abelian extensions involved.

How exactly?

Any D_4 quartic extension L/K has a quadratic subextension:

$$\begin{array}{c} L \\ \big|\,2 \\ F \\ \big|\,2 \\ K \end{array}$$

Quadratic extensions of quadratic extensions

We can count quadratic extensions of quadratic extensions by studying the generating series

$$\tilde{\Phi}(s) = \sum_{[F:K]=2} \sum_{[L:F]=2} \frac{1}{\mathrm{Norm}(\mathrm{Disc}(L/K))^s}.$$

There are three possibilities for the extension L/K in this case.

- L/K is a degree 4 non-Galois extension whose normal closure has Galois group D_4 over K. These are the extensions we want to count.
- L/K is a Galois extensions with Galois group C_4, the cyclic group of order 4.
- L/K is a Galois extension with Galois group $V_4 \simeq C_2 \times C_2$, the Klein four-group.

Quadratic extensions of quadratic extensions

- For a fixed quadratic extension F/K, conjugate D_4-extensions of K will be counted separately and every D_4-extension contains a single quadratic subextension (shared with its unique K-conjugate).
- The C_4-extensions are counted up to K-isomorphism just once since these extensions are Galois and contain a single quadratic subextension.
- Each V_4-extension L/K contains three quadratic subfields, so each V_4-extension is counted, up to K-isomorphism, three times.

Therefore

$$Z_{4,K}(D_4, s) = \frac{1}{2}\left(\tilde{\Phi}(s) - Z_{4,K}(C_4, s) - 3Z_{4,K}(V_4, s)\right).$$

A better generating series

Note that

$$\tilde{\Phi}(s) = \sum_{[F:K]=2} \sum_{[L:F]=2} \frac{1}{\mathrm{Norm}(\mathrm{Disc}(L/K))^s}$$

$$= \sum_{[F:K]=2} \frac{1}{\mathrm{Norm}(\mathrm{Disc}(F/K))^{2s}} Z_{2,F}(C_2, s).$$

It is more convenient to work with

$$\Phi(s) = \sum_{[F:K]=2} \frac{1}{\mathrm{Norm}(\mathrm{Disc}(F/K))^{2s}} (1 + Z_{2,F}(C_2, s))$$

which can be expressed as

$$\Phi(s) = 2Z_{4,K}(D_4, s) + Z_{2,K}(C_2, 2s) + Z_{4,K}(C_4, s) + 3Z_{4,K}(V_4, s).$$

Fit the pieces together

$$\Phi(s) = 2Z_{4,K}(D_4, s) + Z_{2,K}(C_2, 2s) + Z_{4,K}(C_4, s) + 3Z_{4,K}(V_4, s)$$

The functions $Z_{2,K}(C_2, s)$, $Z_{4,K}(C_4, s)$ and $Z_{4,K}(V_4, s)$ have been studied by Wright.

$$\Phi(s) = \sum_{[F:K]=2} \frac{1}{\mathrm{Norm}(\mathrm{Disc}(F/K))^{2s}} \left(1 + Z_{2,F}(C_2, s)\right)$$

Key point: We need uniform estimates for $Z_{2,F}(C_2, s)$ for all quadratic extensions F/K in order to get a good enough handle on the analytic behavior of $\Phi(s)$.
In particular, we need uniform estimates for $\zeta_F(s)$ inside the critical strip.

Main result

Let K be a number field with $[K:\mathbb{Q}] = d$. Asymptotically, as X grows, the number of (K-isomorphism classes of) quartic D_4-extensions of K whose absolute norm of the relative K-discriminant is bounded by X is

$$N_{4,K}(D_4, X) = c_{4,K}(D_4) \cdot X + O\left(X^{\frac{3}{4}+\epsilon}\right),$$

where

$$c_{4,K}(D_4) = \sum_{[F:K]=2} \frac{1}{2^{r_2(F)+1}} \cdot \frac{1}{\mathrm{Norm}(\mathrm{Disc}(F/K))^2} \cdot \frac{\mathrm{Res}_{s=1}\,\zeta_F(s)}{\zeta_F(2)}$$

and $r_2(F)$ denotes the number of pairs of conjugate complex embeddings of F.

If we assume the Lindelöf hypothesis, then the error term above can be improved to $O\left(X^{\frac{1}{2}+\epsilon}\right)$.

Thank you!