Upper bound:

Thm 11.4 (Schmidt) Let $n \geq 2$.

$$\#\{L \subseteq \overline{\mathbb{Q}} \text{ ext. of } \mathbb{Q} \text{ of degree } n,\ |\mathrm{disc}(L)| \leq T\} \ll_n T^{(n+2)/4}.$$

(Recall: conjectured to be $\asymp T$.)

Pf that $\#\{L$ as above, $\nexists$ subset (primitive) $\mathbb{Q} \subsetneq F \subsetneq L\} \ll T^{(n+2)/4}$

Let $1 = \lambda_1 \leq \lambda_2 \leq \dots \leq \lambda_n$ be the succ. min. of $\mathcal{O}_L$.

$\lambda_2 \cdots \lambda_n \asymp \mathrm{covol}(\mathcal{O}_L) \asymp |\mathrm{disc}(L)|^{1/2} \leq T^{1/2}$

$\Rightarrow \lambda_2 \ll T^{1/2(n-1)}$.

There is a number $\alpha \in \mathcal{O}_L$ with $|\alpha| \asymp \lambda_2$, $\alpha \notin \mathbb{Z}$.

~~and $\mathrm{Tr}_{L|\mathbb{Q}}(\alpha) = 0$ (replace α by $n \cdot \alpha -$ $\mathrm{Tr}(\alpha)$ if necessary).~~

$\mathbb{Q} \subsetneq \mathbb{Q}(\alpha) \subseteq L$, so $\mathbb{Q}(\alpha) = L$.

By Thm 10.1 / Prop 10.2,

$$\#\{L \text{ gen. by some } \alpha \in \mathcal{O}_L \text{ with } |\alpha| \ll T^{1/2(n-1)}\} \ll T^{(n+2)/4}.$$

□

This shows the Thm when n is prime. For the general statement, Schmidt ~~uses induction over~~ proves the following more general statement by induction over n:

SKIPPED Thm 11.5 (Schmidt) For any number field $K \subset \overline{\mathbb{Q}}$ ~~of~~ degree m and any $n \geq 2$,

$$\#\{L \subseteq \overline{\mathbb{Q}} \text{ ext. of } K \text{ of degree } n,\ |\mathrm{disc}(L)| \leq T\} \ll_{n,m} |\mathrm{disc}(K)|^{-\frac{1}{2}} \cdot \left(\frac{T}{|\mathrm{disc}(K)|}\right)^{(n+}$$

For the general (nonprimitive) case :

$$\#\{L\} = \sum_{\substack{K \text{ ext. of } \mathbb{Q} \\ \text{of degree } m|n}} \underbrace{\#\{L \text{ ext. of } K \text{ of deg. } \tfrac{n}{m} \text{ s.t. } \nexists\, K \subsetneq F \subsetneq L\}}_{\text{count these using a similar strategy as before}}$$

↑ count these (by $|\mathrm{disc}(K)|$) using induction

For details, see Schmidt: Number fields of given degree and bounded discriminant

Rmk We expect

$$\lim_{\varepsilon \to 0} \mathbb{P}_K\left(\lambda_2(\mathcal{O}_K) < \varepsilon |\mathrm{disc}(K)|^{1/2(n-1)}\right) = 0.$$

The reason the upper and lower bounds are so far off is that $\mathbb{Z}[\alpha]$ usually has discriminant much larger than T (about $T^{n/2}$) for random $\alpha \in \overline{\mathbb{Z}}_n$ with $|\alpha| \asymp T^{1/2(n-1)}$.

Shankar–Tsimerman (2020) analyse how often $[\mathcal{O}_{\mathbb{Q}(\alpha)} ; \mathbb{Z}[\alpha]] = k$ and therefore how often $|\mathrm{disc}(K)| \asymp \frac{T^{n/2}}{k^2}$. Assuming a sufficiently (outrageously!) small error bound in the "sieve", they justify Conjecture 11.1.

Also see Bhargava–Shankar–Wang (2022)
and Anderson–Gafni–Hughes–Lemke Oliver–Lowry-Duda–
Thorne–Wang–Zhang (2022).

We can do better than Schmidt:

Idea (Ellenberg-Venkatesh, 2006)

Instead of writing down the min. pol. of one el. $\alpha \in \mathcal{O}_L$ (generating L), pick $1 \leq r \leq n$ generators $\omega_1, \dots, \omega_r \in \mathcal{O}_L$ and for some $d \geq 1$, write down the integers

$\mathrm{Tr}(\omega_1^{i_1} \cdots \omega_r^{i_r})$ for $i_1, \dots, i_r \geq 0$, $i_1 + \dots + i_r = d$.

[For large enough d these numbers should determine $\omega_1, \dots, \omega_r$ and therefore the field L.]

If $\rho_1, \dots, \rho_n$ are the embeddings $L \to \mathbb{C}$, each ω_i corr. to a vector $\underset{\rho(\omega_i)}{} = (\rho_j(\omega_i))_{j=1,\dots,n} \in \mathbb{C}^n$.

The map $(\omega_1, \dots, \omega_r) \longmapsto (\mathrm{Tr}(\omega_1^{i_1} \cdots \omega_r^{i_r}))_{i_1+\dots+i_r=d}$

corr. to a map $\varphi_{nrd}: \mathbb{C}^{rn} \longrightarrow \mathbb{C}^{E_{r,d}}$ $\quad$ $\left(E_{r,d} = \#\{(i_1,\dots,i_r)\} = \binom{r+d-1}{d}\right)$

$$(x_{pq})_{\substack{p \leq r \\ q \leq n}} \longmapsto \left(\sum_q x_{1q}^{i_1} \cdots x_{rq}^{i_r}\right)_{i_1+\dots+i_r=d}$$

Lemma 11.6 If $d \geq 1$, $n \geq r \geq 6$ [and in many other cases], we have

$$\dim(\mathrm{im}(\varphi_{nrd})) = \min(rn, E_{r,d}).$$

Idea of pf It suffices to show that the Jacobian has full rank at some point.

$$\frac{\partial \varphi_{nrd}}{\partial x_{pq}} = \Bigg(\underbrace{\frac{\partial x_{1q}^{i_1} \cdots x_{rq}^{i_r}}{\partial x_{pq}}}_{\substack{\text{deriv. of hom.} \\ \text{deg. } d \text{ pol. evaluated at } (x_{1q},\dots,x_{rq}) =: P_q.}}\Bigg)_{i_1+\dots+i_r=d}$$

This is the Alexander–Hirschowitz theorem.
(Proven by induction, specialising some of the n points $P_1, \dots, P_n$ to lie on a hyperplane.)

"□"

<u>Cor 11.7</u> If $d \geq 1$, $n \geq r \geq 6$, $rn \leq E_{r,d}$, then there is a projection $\pi : \mathbb{C}^{E_{rd}} \longrightarrow \mathbb{C}^{rn}$ such that $\pi \circ \varphi_{nrd} : \mathbb{C}^{rn} \longrightarrow \mathbb{C}^{rn}$ is dominant and therefore we have $|(\pi \circ \varphi)^{-1}((\pi \circ \varphi)(P))| < \infty$ (and hence $\ll_{n,r,d} 1$) for <u>generic</u> points $P = (x_{pq})_{p,q} \in \mathbb{C}^{rn}$.

not satisfying a certain pol. equality

<u>Pf</u> AG ... "□"

<u>Thm 11.8</u> (Lemke Oliver – Thorne, 2020)

If $d \geq 1$, $n \geq r \geq 6$, $rn \leq E_{rd}$, then
$\#\{L \text{ number field of degree } n \,|\, |\mathrm{disc}(L)| \leq T\} \ll T^{rd}$.

<u>Pf</u> Let $\alpha_1, \dots, \alpha_n$ form a basis of $\mathcal{O}_L$ with $\alpha_i \asymp \lambda_i$. We have $\lambda_i \leq \lambda_n \ll T^{1/n}$ (HW).
Since $\rho(\alpha_1), \dots, \rho(\alpha_n)$ form a $\mathbb{C}$-basis of $\mathbb{C}^n$, there is a <u>generic</u> point $(\omega_1, \dots, \omega_r) \in \mathbb{C}^{rn}$ given by $\omega_p = \sum_j m_{pj} \alpha_j$ with $m_{pj} \in \mathbb{Z}$, $|m_{pj}| \ll_{n,r,d} 1$ such that ω_1 doesn't lie

in any subfield $F \subsetneq K$. Pick one!

Only $\ll_{n,r,d} 1$ fields L produce the same point

$\varphi_{n,r,d}(\omega_1, \dots, \omega_r) \in \mathbb{Z}^{rn}$, whose coordinates are

$\ll \max(|\omega_1|, \dots, |\omega_r|)^d \ll \lambda_n^d \ll T^{d/n}$.

The number of such points is $\ll (T^{d/n})^{rn} = T^{rd}$. $\square$

Minimising rd subject to the cond. $d \geq 1$, $n \geq r \geq 6$, $rn \leq \binom{r+d-1}{d}$,

shows: $\#\{L\} \ll T^{O((\log n)^2)}$.

(You can take $d, r \asymp \log n$.)

12. Étale algebras

Let K be a field.

<u>Def</u> An <u>étale K-algebra</u> is a product $L = L_1 \times \dots \times L_r$ of finitely many separable field extensions L_i of K.

The <u>degree</u> is

$$[L:K] = \dim_K(L) = \sum_i [L_i:K].$$

<u>Ex</u> The trivial degree n ext. $L = K^n = K \times \dots \times K$.

~~Ex If K is alg. closed, there is exactly one étale K ext of degree n, namely~~.

<u>Rmk</u> This is the only one if K is separably closed. (or algebraically)

<u>Rmk</u> If $f \in K[X]$ is separable of degree n, then $L = K[X]/(f(X))$ is an étale K-alg. of degree n.

<u>Rmk</u> The étale $\mathbb{R}$-algebras are $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ of degree $r_1 + 2r_2$.

<u>Rmk</u> A finite-dimensional K-algebra L is étale if and only if the trace form on L is nondegenerate.

<u>Rmk</u> Let $K'|K$ be any field extension.

L étale K-alg. of degree n

$$\Downarrow$$

$L \otimes_K K'$ étale K'-alg. of degree n

<u>Ex</u> For $K = \mathbb{Q}$ a) the factors of $L \otimes_{\mathbb{R}} \mathbb{C}$ corr. to the real/complex emb. of L.

b) the factors of $L \otimes_{\mathbb{Q}} \mathbb{Q}_p$ corr. to the primes of L above p.