10. Counting number fields with a short generator

Let C_n' as in section 9.

Def An order in a number field L (of degree n) is a subring $\mathcal{O}$ of $\mathcal{O}_L$, $1 \in \mathcal{O}$, ~~which has rank n~~ such that $\mathbb{Q}\cdot\mathcal{O} = L$.

(equivalently: which has rank n as a $\mathbb{Z}$-module).

Def $\overline{\mathbb{Z}}_n' := \{\alpha \in \overline{\mathbb{Z}}_n \mid \mathrm{tr}(\alpha) = 0\}$. ~~And every $[\alpha] \in \overline{\mathbb{Z}}_n/\mathbb{Z}$ has exactly one representative in $\overline{\mathbb{Z}}_n'$~~

$\alpha - \mathrm{tr}(\alpha)/n$

$$
\begin{tikzcd}
\{\alpha \in \overline{\mathbb{Z}}_n'\} \arrow[r, "\text{(not surjective)}"] \arrow[dr] & \{\mathcal{O} \subseteq \overline{\mathbb{Z}} \text{ order in deg. } n \text{ number field}\} \arrow[d] \\
& \{L \text{ deg. } n \text{ number field}\}
\end{tikzcd}
$$

$\alpha \longmapsto \mathbb{Z}[\alpha]$

$\alpha \longmapsto \mathbb{Q}(\alpha)$

$\mathcal{O} \longmapsto \mathbb{Q}\cdot\mathcal{O}$

__Thm 10.1__ $\#\{\mathcal{O} \subseteq \overline{\mathbb{Z}} \text{ as above s.t. } \mathcal{O} = \mathbb{Z}[\alpha] \text{ for some } \alpha \in \overline{\mathbb{Z}}'_n \text{ with } |\alpha| \leq T\}$

$$\sim \frac{1}{2} C'_n \cdot T^{(n-1)(n+2)/2}.$$

__Pf__ "$\leq$" $\mathbb{Z}[\alpha] = \mathbb{Z}[-\alpha]$.

"$\geq$" We need to show that if we order the elements $\alpha \in \overline{\mathbb{Z}}'_n$ by $|\alpha|$, then

$$\mathbb{P}_\alpha\left(\exists \underset{\alpha, -\alpha}{\beta \underset{\neq}{}} \in \overline{\mathbb{Z}}'_n : \mathbb{Z}[\alpha] = \mathbb{Z}[\beta],\ |\beta|_2 \leq |\alpha|_2\right) = 0.$$

Euclidean norm on $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$

$$LHS \leq \mathbb{P}_\alpha\left(\exists\ \beta \in \mathbb{Z}[\alpha]^{\cap\{tr=0\}} \text{ lin. indep. from } \alpha : |\beta|_2 \leq |\alpha|_2\right)$$

Call α __bad__ if there is such a β.

$\mathbb{Z}[\alpha] \cap \{tr = 0\} \subseteq$ lattice $\Lambda = \Lambda(\alpha)$ spanned by $y_1, \ldots, y_{n-1}$,

where $y_i = y_i(\alpha) = \alpha^i - \frac{1}{n} tr(\alpha^i)$

Fix a signature (r_1, r_2).

Let $H = \{x \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid tr(x) = 0\}$.

For $i=1,\dots,n-1$, let $g_i(x)\geq 0$ be the (Euclidean) distance of $y_i(x)\in\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}\cong\mathbb{R}^n$ from the subspace spanned by $y_1(x),\dots,y_{i-1}(x)$. (as in Gram–Schmidt)

If $\rho_i(x)\neq\rho_j(x)$ $\forall i\neq j$ for the n maps $\rho_1,\dots,\rho_n:\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}\to\mathbb{C}$,

then $1,x,\dots,x^{n-1}$ are lin. indep. and hence $y_1,\dots,y_{n-1}$ are lin. indep.

Then, $g_i(x)>0$ $\forall i$. Let $h(x)=\min\limits_{2\leq i\leq n}\dfrac{g_i(x)}{g_{i-1}(x)}$.

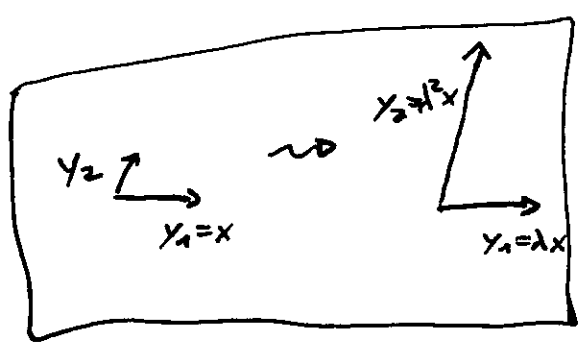
Claim: If x is bad, then $h(x)\leq 1$.

Pf: If $h(x)>1$, then any vector in $\Lambda(x)$ lin. indep. from $y_1^{(x)}=x$ has distance $>g_1(x)=|x|_2$ from some subspace, and in particular has length $>|x|_2$. $\square$ (claim)

Note: $y_i(\lambda x)=\lambda^i y_i(x)$ $\quad\forall\lambda\geq 0$

$\Rightarrow g_i(\lambda x)=\lambda^i g_i(x)$

$\Rightarrow h(\lambda x)=\lambda h(x)$



Let $B_\varepsilon = \{ x \in H \mid |x| \leq 1,\ h(x) \leq \varepsilon \}$.

For all $T \geq \frac{1}{\varepsilon}$, $T \cdot B_\varepsilon$ contains all bad $x \in H$ with $|x| \leq T$.

$\Rightarrow$ The fraction of bad x goes to 0 as $T \to \infty$ because B_ε goes monotonically to $\emptyset$ as $\varepsilon \to 0$.

$\square$

Bror

10.2

$\#\{K \subseteq \overline{\mathbb{Q}} \text{ as above s.t. } K = \mathbb{Q}(\alpha) \text{ for some } \alpha \in \mathbb{Z}_n' \text{ with } |\alpha| \leq T\}$

$\asymp T^{(n-1)(n+2)/2}$

To prove "$\gg$", one can use a (difficult!) sieve to show that $\mathcal{O}_{\mathbb{Q}(\alpha)} = \mathbb{Z}[\alpha]$ for a positive proportion of α.

In fact, $\mathbb{Z}[\alpha]$ has squarefree discriminant for a positive proportion of α.

(See Bhargava, Shankar, Wang: Squarefree values of polynomial discriminants.)

11. Counting number fields of small discriminant

Conjecture 11.1 (Folklore, Malle) Let $n \geq 2$. Let K be any n.f.

There are constants $C_{n,K}, C'_{n,K} > 0$ s.t.

a) $\# \{ L \subseteq \overline{\mathbb{Q}}$ ext. of K of degree $n \mid |\operatorname{disc}(L)| \leq T \} \sim C_{n,K} T$

b) $\# \{$ ... ... and Galois group $S_n \} \sim C'_{n,K} T$.

Conj. 11.2 (Malle) We have $C_{n,K} = C'_{n,K}$ if and only if n is prime.

Known cases:

$n=2$: Exer 1 (for $K = \mathbb{Q}$), Datskovsky–Wright (any K)

$n=3$: Davenport–Heilbronn (using a parametrisation, for $K=\mathbb{Q}$), Bhargava–Shankar–Wang (any K)

$n=4,5$: Bhargava (— " — , for $K=\mathbb{Q}$), — " —

Lower bound:

Thm 11.3 (B–S–W)

$\# \{ L \subseteq \overline{\mathbb{Q}}$ ext. of $\mathbb{Q}$ of degree n, $|\operatorname{disc}(L)| \leq T$, $\operatorname{Gal} = S_n \} \gg T^{\frac{1}{2} + \frac{1}{n}}$.

Pf If $\alpha \in \overline{\mathbb{Z}}$ generates L, then

$$\operatorname{disc}(L) \leq \operatorname{disc}(\mathbb{Z}[\alpha]) = \det\left((\rho_i(\alpha^j))_{\substack{i=1,\dots,n \\ 0 \leq j \leq n-1}} \right)^2$$

$$\ll |\alpha|^{2(0+1+\dots+(n-1))} = |\alpha|^{n(n-1)}.$$

$$\Rightarrow \text{LHS} \gg \# \{ L \text{ gen. by } \alpha \text{ with } |\alpha| \ll T^{1/n(n-1)} \text{ with } \operatorname{Gal} = S_n \} \gg T^{(n+2)/2n}$$

Prop 10.2

∎