Introduction to Algebraic Number Theory
Lecture 20

Andrei Jorza

9 Counting Ideals

(9.1) We would like to count ideals I of the ring of integers $\mathcal{O}_K$ of a number field K such that $||I|| \leq t$. We will denote $n_K(t)$ this number. Over $\mathbb{Q}$, this is easy: all ideals are of the form $n\mathbb{Z}$ and so the number $n_{\mathbb{Q}}(t) = \lfloor t \rfloor = t -$ small error.

Theorem 1. *Let K be a number field and $C \in \mathrm{Cl}(K)$. Let $n_C(t)$ be the number of ideals of K in the class C of norm at most t. Then*

$$n_C(t) = \kappa t + O(t^{1-\frac{1}{n}})$$

where $n = [K : \mathbb{Q}]$ and

$$\kappa = \frac{2^r (2\pi)^s R_K}{w\sqrt{|\operatorname{disc}(K)|}}$$

Here r is the number of real embeddings, $2s$ is the number of torsion embeddings, w is the number of roots of unity in K and R_K, the **regulator***, is the volume of $\log \iota(\mathcal{O}_K^\times)$ in $\Delta = \ker(\mathbb{R}^{r+s} \xrightarrow{\sum} \mathbb{R})$.*

Summing over $C \in \mathrm{Cl}(K)$ we get the estimate

$$n_K(t) = h_K \kappa t + O(t^{1-1/n})$$

Remark 1. The regulator can be computed as follows: let $u_1, \dots, u_{r+s-1}$ be a basis of (the free part of) $\mathcal{O}_K^\times$ and let $\log \circ \iota(u_i) = (u_{i,1}, \dots, u_{i,r+s})$. Then R_K is the absolute value of the determinant of any full rank minor of the matrix $(u_{i,j})$.

Example 2. Take $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$ with four real embeddings $r = 4, s = 0$. The only roots of unity in K are ± 1 (they must be real!) so $w = 2$. The discriminant is $\operatorname{disc}(K) = 3600$ so $\sqrt{|\operatorname{disc}(K)|} = 60$. Finally, we've seen that a basis for $\mathcal{O}_K^\times$ is $(1 + \sqrt{5}))/2$, $(1 + \sqrt{5})/2 - \sqrt{3}$ and $(1 + \sqrt{5})/2 - \sqrt{3} - 1$. Thus

$$R_K = \begin{vmatrix} \log\left|\frac{1+\sqrt{5}}{2}\right| & \log\left|\frac{1+\sqrt{5}}{2}\right| & \log\left|\frac{1-\sqrt{5}}{2}\right| \\ \log\left|\frac{1+\sqrt{5}}{2} - \sqrt{3}\right| & \log\left|\frac{1+\sqrt{5}}{2} + \sqrt{3}\right| & \log\left|\frac{1-\sqrt{5}}{2} - \sqrt{3}\right| \\ \log\left|\frac{1+\sqrt{5}}{2} - \sqrt{3} - 1\right| & \log\left|\frac{1+\sqrt{5}}{2} + \sqrt{3} - 1\right| & \log\left|\frac{1-\sqrt{5}}{2} - \sqrt{3} - 1\right| \end{vmatrix}$$

where we take the first three real embeddings and leave out $\sqrt{3} \mapsto -\sqrt{3}, \sqrt{5} \mapsto -\sqrt{5}$.

(9.2)

Lemma 3. *Fix $J \in C^{-1}$. There is a bijection between the sets $\{I \in C | ||I|| \leq t\}$ and $\{(\alpha) \subset J | |N_{K/\mathbb{Q}}(\alpha) \leq t||J||\}$.*

Proof. The maps are $I \mapsto IJ$ which has to be principal (1 in $\mathrm{Cl}(K)$) and $(\alpha) \mapsto (\alpha)J^{-1}$ which lies in C. Indeed, $||IJ|| = ||I||||J|| \leq t||J||$ and $||(\alpha)J^{-1}|| = ||(\alpha)||||J||^{-1} = |N_{K/\mathbb{Q}}(\alpha)|||J||^{-1} \leq t$. ☐

Proof of Theorem. By the previous lemma we only need to count principal ideals $(\alpha) \subset J$ with $||(\alpha)|| \leq t||J||$ and the difficulty consists in the fact that (α) determines the element α up to a unit.

Recall the map $K \to \mathbb{R}^n$ given by $\iota : x \mapsto (\sigma_i(x), \operatorname{Re}\tau_i(x), \operatorname{Im}\tau_i(x))$ where σ_i are the real embeddings and $\tau_i, \overline{\tau}_i$ are the complex embeddings. Then $\iota(J) \subset \mathbb{R}^n$ is a lattice. Further recall the maps $\log : \mathbb{R}^n - 0 \to \mathbb{R}^{r+s}$ given by $(x_i) \mapsto (\log(|x_1|), \ldots, \log(|x_r|), \log(x_{r+1}^2 + x_{r+2}^2), \ldots)$ and $\sum : \mathbb{R}^{r+s} \to \mathbb{R}$ given by adding the coordinates. Then for every $x \in K^\times$ one has $\sum \log \iota(x) = \log |N_{K/\mathbb{Q}}(x)|$. Remark that $\ker \log = \{\pm 1\}^r (S^1)^s$ and that the kernel of ι is the group of roots of unity in K.

Consider $\mathcal{F}$ a fundamental parallelotope of $\log \iota(\mathcal{O}_K^\times) \subset \Delta \subset \mathbb{R}^{r+s}$, i.e., the span of a basis of $\log \iota(\mathcal{O}_K^\times)$ with coefficients in $[0,1)$. Also let $\mathcal{D} \subset \mathbb{R}^{r+s}$ the region spanned by $\mathcal{F}$ and the vector $(1, \ldots, 1, 2, \ldots, 2)$ (where 1 appears r times and 2 appears s times).

Note that $n_C(t)$ is the number of $\{(\alpha) \subset J | |N_{K/\mathbb{Q}}(\alpha)| \leq t||J||\} \cong \{\alpha \in J | |N_{K/\mathbb{Q}}(\alpha) \leq t||J||\}/\mathcal{O}_K^\times$ and via ι this becomes

$$n_C(t) = w^{-1} |\{\iota(\alpha) \in \iota(J) | N(\iota(\alpha)) \leq t||J||\}/\iota(\mathcal{O}_K^\times)|$$

because $|\ker \iota| = w$.

Further composing with $\log : \mathbb{R}^n \to \mathbb{R}^{r+s}$ we see that $\mathbb{R}^{r+s}/\log \iota(\mathcal{O}_K^\times) \cong \mathcal{D}$ and, since $\ker \log \iota$ consists of roots of unity it follows that

$$\{\iota(\alpha) \in \iota(J) | N(\iota(\alpha)) \leq t||J||\}/\iota(\mathcal{O}_K^\times) \cong \{\iota(\alpha) \in \iota(J) | N(\iota(\alpha)) \leq t||J||, \log \iota(\alpha) \in \mathcal{D}\}$$

Let $\mathcal{D}_\lambda \subset \mathcal{D}$ consist of tuples $(x_1, \ldots, x_{r+s}) \in \mathcal{D}$ with $\sum(x_i) \leq \lambda$. Then $N(\iota(\alpha)) \leq t||J||$ is equivalent to $\sum \log \iota(\alpha) \leq \log(t||J||)$ and so, putting everything together,

$$n_C(t) = w^{-1} |\{\iota(\alpha) \in \iota(J) | N(\iota(\alpha)) \leq t||J||, \log \iota(\alpha) \in \mathcal{D}\}| = w^{-1} |\{\iota(\alpha) \in \iota(J) | \log \iota(\alpha) \in \mathcal{D}_{\log(t||J||)}\}$$

For simplicity let $\lambda := \log(t||J||)$ and let $\mathcal{D}'_\lambda = \log^{-1}(\mathcal{D}_\lambda)$. Then

$$n_C(t) = w^{-1} |\{\iota(\alpha) \in \iota(J) \cap \mathcal{D}'_{\log(t||J||)}\}| = w^{-1} |\iota(J) \cap \mathcal{D}'_{\log(t||J||)}|$$

(To be continued) □