Introduction to Algebraic Number Theory
Lecture 16

Andrei Jorza

7 The Class group (continued)

(7.2) Optimizing the constant λ.

Recall that we seek elements α in ideals I with a bound on their norms. The insight of Minkowski's geometry of numbers is that I, being a finite $\mathbb{Z}$-module, is a lattice and so we seek points in a lattice with a certain property. The "idea" of the geometry of numbers is that if Λ is a lattice in $\mathbb{R}^N$ then a convex region of $\mathbb{R}^N$ should have roughly as many lattice points as the volume of the region, normalized so that the "unit cube" of the lattice has volume 1. This makes intuitive sense in the plane (one can approximate, poorly, π by computing the number of lattice points in circles of big radii) and we'll prove a lemma to formalize this statement.

Lemma 1. *Suppose $\Lambda \subset \mathbb{R}^n$ is a lattice with fundamental volume $\operatorname{vol}(\Lambda) := \operatorname{vol}(\mathbb{R}^n/\Lambda)$. Suppose E is a convex region of $\mathbb{R}^n$ which is symmetric around the origin. If $\operatorname{vol}(E) > 2^n \operatorname{vol}(\Lambda)$ then $\mathcal{E}$ contains a nonzero element of Λ.*

Proof. Let F be a fundamental parallelotope of Λ, i.e., the locus $\{\sum x_i v_i | x_i \in [0,1]\}$ for $v_1, \ldots, v_n$ a basis of Λ. Then $\operatorname{vol}(F) = \operatorname{vol}(\mathbb{R}^n/\Lambda)$. Since $\frac{1}{2}E = \bigsqcup_{v\in\Lambda} \frac{1}{2}E \cap (v+F)$ (as translates of F cover $\mathbb{R}^n$). Thus (the first inequality is the hypothesis)

$$\begin{aligned}\operatorname{vol}(F) &< 2^{-n}\operatorname{vol}(E)\\ &= \operatorname{vol}(\frac{1}{2}E)\\ &= \sum_{v\in\Lambda}\operatorname{vol}(\frac{1}{2}E \cap (v+F))\\ &= \sum_{v\in\Lambda}\operatorname{vol}(\frac{1}{2}E - v \cap F)\end{aligned}$$

This implies that at least two of the sets $\frac{1}{2}E - v \cap F$ for $v \in \Lambda$ must overlap. Thus we find $x - u = y - v$ in F with $x, y \in \frac{1}{2}E$ and $u, v \in \Lambda$. As E is symmetric around the origin and convex it follows that the difference $x - y \in E$ but $x - y = u - v$ and so $u - v \in E \cap (\Lambda - \{0\})$ as desired. □

A good vector space. First, we need a good vector space $\mathbb{R}^n$ containing the lattice attached to an ideal I. Again let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K into $\mathbb{C}$ fixing $\mathbb{Q}$. Suppose r of them are real embeddings, i.e., their image lands in $\mathbb{R}$ and after reordering we may assume they are $\sigma_1, \ldots, \sigma_r$. Suppose that the remaining $2s = n - r$ are complex embeddings, i.e., their image is not contained in $\mathbb{R}$. They come in conjugate pairs: $\sigma_{r+1}, \overline{\sigma}_{r+1}, \ldots, \sigma_{r+s}, \overline{\sigma}_{r+2s-1}$ and they define

$$K \to \mathbb{R}^n = \mathbb{R}^r \times (\mathbb{R}^2)^s$$

$$\iota : x \mapsto \bigoplus_{i=1}^{r} \sigma_i(x) \oplus \bigoplus_{j=1}^{s} (\operatorname{Re}\sigma_{r+j}(x) \oplus \operatorname{Im}\sigma_{r+j}(x))$$

If $N(x_1, \ldots, x_{r+2s}) = x_1 \cdots x_r(x_{r+1}^2 + x_{r+2}^2) \cdots (x_{r+2s-1}^2 + x_{r+2s}^2)$ then for $\alpha \in K$ we have $N(\iota(\alpha)) = N_{K/\mathbb{Q}}(\alpha)$.

A possible region? Suppose we defined the set $E \subset \mathbb{R}^n$ by $E = \{v \in \mathbb{R}^n | |N(v)| \leq \lambda ||I||\}$. If we could show that $\operatorname{vol}(E) > 2^n \operatorname{vol}(I)$ where $\operatorname{vol}(I)$ is the volume of the lattice $\iota(I) \subset \mathbb{R}^n$ then we would find $\alpha \in E \cap \iota(I)$ which would then satisfy the condition $|N_{K/\mathbb{Q}}(\alpha)| \leq \lambda ||I||$. The catch is that $\operatorname{vol}(E)$ is impossible to compute.

A good region. The issue with the choice of E above is that the volume of this region defined by $\prod |x_i| \prod (x_{r+2j-1}^2 + x_{r+2j}^2) \leq \lambda ||I||$ is difficult to compute. We'll use the AM-GM inequality to simplify the region, in effect making is larger than necessary with the effect that we don't get as good a value for λ as we could. The AM-GM inequality gives

$$\prod |x_i| \prod (x_{r+2j-1}^2 + x_{r+2j}^2) \leq \left(\frac{|x_1| + \cdots + |x_r| + 2\sqrt{x_{r+1}^2 + x_{r+2}^2} + \cdots + 2\sqrt{x_{r+2s-1}^2 + x_{r+2s}^2}}{n} \right)^n$$

and for $|N(v)| \leq \lambda ||I||$ it suffices that

$$|x_1| + \cdots + |x_r| + 2\sqrt{x_{r+1}^2 + x_{r+2}^2} + \cdots + 2\sqrt{x_{r+2s-1}^2 + x_{r+2s}^2} \leq n \sqrt[n]{\lambda ||I||}$$

Lemma 2. *The volume of the region* $\{v \in \mathbb{R}^n | |x_1| + \cdots + |x_r| + 2\sqrt{x_{r+1}^2 + x_{r+2}^2} + \cdots + 2\sqrt{x_{r+2s-1}^2 + x_{r+2s}^2} \leq t\}$ *is*

$$\frac{2^{r-s}\pi^s t^n}{n!}$$

Proof. Calc 3. □