Algebraic Number Theory – Lecture 8

Michael Harvey

"It has long been an axiom of mine that the little things are infinitely the most important."

– Sherlock Holmes

1. Lattices

Recall that a lattice in $\mathbb{R}^n$ is a discrete additive subgroup of $\mathbb{R}^n$. If it is generated by the vectors $\{e_1, \ldots, e_n\}$ then its fundamental domain T is given by

$$T = \{\sum_{i=1}^{n} a_i e_i \,:\, 0 \leqslant a_i < 1\}.$$

We then define the volume of T to be

$$\mathrm{vol}(T) = |\det(e_1 \ldots e_n)|.$$

2. Geometric representation of algebraic numbers

Our aim is to embed a number field K into a real vector space of dimension $n = [K : \mathbb{Q}]$. From there we will establish a correspondence between ideals of $\mathcal{O}_k$ and lattices in this vector space.

We know there are n distinct embeddings $K \hookrightarrow \mathbb{C}$, say $\sigma_1, \ldots, \sigma_n$. Let s be the number of real embeddings and $2t$ be the number of complex embeddings, so $n = s + 2t$. After reordering we can let $\sigma_1, \ldots, \sigma_s$ be the real embeddings, and $\sigma_{s+1} = \overline{\sigma_{s+t+1}}, \ldots, \sigma_{s+t} = \overline{\sigma_{s+2t}}$ be the t pairs of complex embeddings.

Define $L^{st} = \mathbb{R}^s \times \mathbb{C}^t$, i.e. it is the the set of $s + t$-tuples

$$(\underbrace{x_1, \ldots, x_s}_{\in\mathbb{R}}, \underbrace{x_{s+1}, \ldots, x_{s+t}}_{\in\mathbb{C}}).$$

L^{st} as a vector space over $\mathbb{R}$ has dimension $s + 2t = n$. Define a map $\sigma : K \to L^{st}$ by

$$\sigma(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_s(\alpha), \sigma_{s+1}(\alpha), \ldots, \sigma_{s+t}(\alpha)).$$

Theorem 1. *If $\alpha_1, \ldots, \alpha_n$ form a basis for K over $\mathbb{Q}$ then $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$ are linearly independent over $\mathbb{R}$.*

Proof. Let

$$\sigma_k(\alpha_\ell) = x_k^{(\ell)} \text{ for } 1 \leqslant k \leqslant s,\ 1 \leqslant \ell \leqslant n,$$
$$\sigma_{s+j}(\alpha_\ell) = y_j^{(\ell)} + i z_j^{(\ell)} \text{ for } 1 \leqslant j \leqslant t,\ 1 \leqslant \ell \leqslant n.$$

So

$$\sigma(\alpha_\ell) = (x_1^{(\ell)}, \ldots, x_s^{(\ell)}, y_1^{(\ell)} + iz_1^{(\ell)}, \ldots, y_t^{(\ell)} + iz_t^{(\ell)}).$$

Now consider

$$\begin{vmatrix} x_1^{(1)} & \cdots & x_s^{(1)} & y_1^{(1)} & z_1^{(1)} & \cdots & y_t^{(1)} & z_t^{(1)} \\ \vdots & & & & & & & \vdots \\ x_1^{(n)} & \cdots & x_s^{(n)} & y_1^{(n)} & z_1^{(n)} & \cdots & y_t^{(n)} & z_t^{(n)} \end{vmatrix}$$

$$= \frac{1}{(2i)^t} \begin{vmatrix} x_1^{(1)} & \cdots & x_s^{(1)} & y_1^{(1)} + iz_1^{(1)} & y_1^{(1)} - iz_1^{(1)} & \cdots & y_t^{(1)} - iz_t^{(1)} \\ \vdots & & & & & & \vdots \\ x_1^{(n)} & \cdots & x_s^{(n)} & y_1^{(n)} + iz_1^{(n)} & y_1^{(n)} - iz_1^{(n)} & \cdots & y_t^{(n)} - iz_t^{(n)} \end{vmatrix}$$

$$= \frac{1}{(2i)^t} \begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_s(\alpha_1) & \sigma_{s+1}(\alpha_1) & \overline{\sigma_{s+1}(\alpha_1)} & \cdots & \overline{\sigma_{s+t}(\alpha_1)} \\ \vdots & & & & & & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_s(\alpha_n) & \sigma_{s+1}(\alpha_n) & \overline{\sigma_{s+1}(\alpha_n)} & \cdots & \overline{\sigma_{s+t}(\alpha_n)} \end{vmatrix}$$

$$= \frac{1}{(2i)^t} \sqrt{\Delta[\alpha_1, \ldots, \alpha_n]}$$

$$\neq 0.$$

□

Corollary 2. *If $\mathfrak{a} \subset \mathcal{O}_k$ is an ideal with a $\mathbb{Z}$-basis $\{\alpha_1, \ldots, \alpha_n\}$, then $\sigma(\mathfrak{a})$ is a lattice in L^{st} with generators $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$.*

3. Class group

Recall that $\mathcal{F}$ is the group of fractional ideals and $\mathcal{P}$ is the subgroup of principal fractional ideals. The class group is defined to be $\mathcal{H} = \mathcal{F}/\mathcal{P}$. We aim to show that it's a finite group.

We define an equivalence relation on $\mathcal{F}$ by setting, for $\mathfrak{a}, \mathfrak{b} \in \mathcal{F}$, $\mathfrak{a} \sim \mathfrak{b}$ if and only if $\mathfrak{a} = \mathfrak{c}\mathfrak{b}$ for some $\mathfrak{c} \in \mathcal{P}$. We write $[\mathfrak{a}]$ for the equivalence class containing $\mathfrak{a}$.

Proposition 3. *Every equivalence class contains an ideal.*

Proof. Since $\mathfrak{a} \in \mathcal{F}$, $\mathfrak{a} = \gamma^{-1}\mathfrak{b}$ for an ideal $\mathfrak{b}$ and some $\gamma \in \mathcal{O}_k$. So $\mathfrak{b} = \gamma\mathfrak{a} = (\gamma)\mathfrak{a}$. Since (γ) is a principal ideal we have $\mathfrak{b} \sim \mathfrak{a}$. □

Recall Minkowski's theorem: Given a lattice $M \subset \mathbb{R}^n$ with fundamental domain T, and a bounded, convex, symmetric set $X \subset \mathbb{R}^n$, then if

$$\operatorname{vol}(X) > 2^n \operatorname{vol}(T)$$

then X contains a nonzero lattice point of M.

Lemma 4. *Let M be a lattice of dimension $s+2t$ in L^{st}. Let T be the fundamental domain of M, and set $V = \operatorname{vol}(T)$. If $c_1, \ldots, c_{s+t} > 0$ satisfy*

$$c_1 \cdots c_{s+t} > \left(\frac{4}{\pi}\right)^t V$$

then there exists a nonzero element $x = (x_1, \ldots, x_s, x_{s+1}, x_{s+t})$ in M with

$$(*) \begin{cases} |x_i| < c_i \quad (1 \leqslant i \leqslant s) \\ |x_{s+j}|^2 < c_{s+j} \quad (1 \leqslant j \leqslant t). \end{cases}$$

Proof. Let X be the region in L^{st} described by $(*)$. X is convex, symmetric, and bounded. It has volume

$$\operatorname{vol}(X) = 2^s \pi^t c_1 \cdots c_{s+t}.$$

Minkowski's theorem says if $\operatorname{vol}(X) > 2^{s+2t} V$ then we're done. So we're done when

$$c_1 \cdots c_{s+t} > \left(\frac{4}{\pi}\right)^t V.$$

□

Now we want to find V when M is $\sigma(\mathfrak{a})$.

Theorem 5. *Let $\mathfrak{a} \neq 0$ be an ideal, then V for $\sigma(\mathfrak{a})$ is*

$$2^{-t} N(\mathfrak{a}) \sqrt{|\Delta|}.$$

Proof. V is the determinant

$$\begin{vmatrix} x_1^{(1)} & \cdots & x_s^{(1)} & y_1^{(1)} & z_1^{(1)} & \cdots & y_t^{(1)} & z_t^{(1)} \\ \vdots & & & & & & & \vdots \\ x_1^{(n)} & \cdots & x_s^{(n)} & y_1^{(n)} & z_1^{(n)} & \cdots & y_t^{(n)} & z_t^{(n)} \end{vmatrix}$$

from the proof of theorem 1, so

$$V = \left| \frac{1}{(2i)^t} \sqrt{\Delta[\alpha_1, \ldots, \alpha_n]} \right|.$$

From Lecture 6 we know that

$$N(\mathfrak{a}) = \left| \frac{\Delta[\alpha_1, \ldots, \alpha_n]}{|\Delta|} \right|^{1/2},$$

so

$$V = 2^{-t} N(\mathfrak{a}) \sqrt{|\Delta|}.$$

□

We'll use lemma 4 and theorem 5 to prove the following theorem.

Theorem 6. *If $\mathfrak{a} \neq 0$ is an ideal then there exists $\alpha \in \mathfrak{a}$ such that*

$$N(\alpha) \leqslant \left(\frac{2}{t}\right)^t N(\mathfrak{a}) \sqrt{|\Delta|}.$$

Proof. Fix $\varepsilon > 0$ and choose $c_1, \ldots, c_{s+t} > 0$ such that

$$c_1 \cdots c_{s+t} = \left(\frac{2}{\pi}\right)^t N(\mathfrak{a})\sqrt{|\Delta|} + \varepsilon.$$

Since

$$c_1 \cdots c_{s+t} > \left(\frac{4}{\pi}\right)^t \underbrace{2^{-t} N(\mathfrak{a})\sqrt{|\Delta|}}_{V},$$

by lemma 4 there exists $\alpha \in \mathfrak{a}$ such that

$$|\sigma_i(\alpha)| < c_i \quad (1 \leqslant i \leqslant s)$$
$$|\sigma_{s+j}(\alpha)|^2 < c_{s+j} \quad (1 \leqslant j \leqslant t).$$

Multiplying these together we get

$$\begin{aligned} |N(\alpha)| &< c_1 \cdots c_{s+t} \\ &= \left(\frac{2}{\pi}\right)^t N(\mathfrak{a})\sqrt{|\Delta|} + \varepsilon. \end{aligned}$$

The above inequality holds for some set of α for every $\varepsilon > 0$. Taking the intersection of these sets of α over all $\varepsilon > 0$ gives at least one $\alpha \in \mathfrak{a}$ such that

$$N(\alpha) \leqslant \left(\frac{2}{\pi}\right)^t N(\mathfrak{a})\sqrt{|\Delta|}.$$

□

Corollary 7. *Every nonzero ideal* $\mathfrak{a} \subset \mathcal{O}_k$ *is equivalent to an ideal with norm at most* $(2/\pi)^t\sqrt{|\Delta|}$.

Proof. Consider the equivalence class $[\mathfrak{a}^{-1}] \in \mathcal{H}$. By proposition 3, $\mathfrak{a}^{-1} \sim \mathfrak{b} \subset \mathcal{O}_k$, and by theorem 6 there exists some $\beta \in \mathfrak{b}$ such that

$$N(\beta) \leqslant \left(\frac{2}{\pi}\right)^t N(\mathfrak{b})\sqrt{|\Delta|}.$$

Recall that $\beta \in \mathfrak{b}$ means $\mathfrak{b} \mid (\beta)$, so $(\beta) = \mathfrak{b}\mathfrak{c}$ for some ideal $\mathfrak{c} \subset \mathcal{O}_k$. We have

$$|N(\beta)| = N((\beta)) = N(\mathfrak{b})N(\mathfrak{c}),$$

so

$$N(\mathfrak{c}) \leqslant \left(\frac{2}{\pi}\right)^t \sqrt{|\Delta|}.$$

Moreover, $\mathfrak{a}^{-1} \sim \mathfrak{b}$, so $\mathfrak{a} \sim \mathfrak{b}^{-1}$, and $\mathfrak{b}^{-1}(\beta) = \mathfrak{c}$ so $\mathfrak{b}^{-1} \sim \mathfrak{c}$. Hence $\mathfrak{a} \sim \mathfrak{c}$. □

Theorem 8. *The class number* $h = |\mathcal{H}| < \infty$.

Proof. Let $[\mathfrak{b}] \in \mathcal{H}$. So $[\mathfrak{b}]$ contains an ideal $\mathfrak{a}$ by proposition 3, and by corollary 7, $\mathfrak{a} \sim \mathfrak{c}$ for an ideal $\mathfrak{c}$ with

$$N(\mathfrak{c}) \leqslant \left(\frac{2}{\pi}\right)^t \sqrt{|\Delta|}.$$

We learnt in Lecture 6 that only finitely many ideals have a given norm, so there are only finitely many such $\mathfrak{c}$, hence only finitely many classes $[\mathfrak{b}]$. □