Math 430 Tom Tucker
NOTES FROM CLASS 11/08

Let

$$X_t = \{x_1, \dots, x_r, y_1, z_1, \dots, y_s, z_s \ \mid \ \sum_{i=1}^{r} |x_i| + \sum_{j=1}^{s} 2\sqrt{y_j^2 + z_j^2} \le t\}$$

from now on. It is easy to see that X_t is convex, bounded, and centrally symmetric, so we will be able to apply Minkowski's theorem to it.

Proposition 19.1. *Let $y \in L$. If $h(y) \in X_t$, then $\mathrm{N}_{L/\mathbb{Q}}(y) \le (t/n)^n$.*

Proof. Let $b_i = \sigma_i(y)$ for $1 \le i \le r$ and let

$$b_{r+1} = b_{r+2} = \sqrt{y_1^2 + z_1^2}, \dots, b_{n-1} = b_n = \sqrt{y_s^2 + z_s^2}.$$

Then

$$\mathrm{N}(y) = |\sigma_1(y)| \cdots |\sigma_n(y)||\sigma_{r+1}(y)|^2 |\sigma_{r+3}(y)|^2 \cdots |\sigma_{n-1}(y)|^2 = |b_1| \cdots |b_n|.$$

By the arithmetic/geometric mean inequality

$$t/n \ge \sum_{i=1}^{n} \frac{|b_i|}{n} \ge \sqrt[n]{|b_1| \cdots |b_n|}.$$

Taking n-th powers finishes the proof. □

Lemma 19.2. *(Arithmetic/geometric mean inequality) Let $b_1, \dots, b_n$ be positive numbers. Then*

$$\sum_{i=1}^{m} \frac{b_i}{n} \ge \sqrt[n]{b_1 \cdots b_n}. \tag{1}$$

(This also follows from Jensen's inequality, which you can read about on Wikipedia.)

Proof. Since the right and left-hand sides of (1) scale, we can assume that

$$\sum_{i=1}^{m} \frac{b_i}{n} = 1.$$

Thus, we need only show that

$$b_1 \cdots b_n \le 1.$$

We can write $b_i = (1 + a_i)$ with $a_1 + \cdots + a_n = 0$. To show that

$$(1 + a_1) \cdots (1 + a_n) \le 1$$

it will suffice to show that that the function

$$F(t) = (1 + a_1 t) \cdots (1 + a_n t)$$

is decreasing on the interval $[0,1]$. This can be checked by simply taking the derivative of F. We find that

$$F'(t) = \sum_{i=1}^{n} a_i \prod_{j\neq i}(1+a_i t).$$

If all of the a_i are 0, this is clearly 0. Otherwise, we can write

$$\begin{aligned} F'(t) &= \sum_{a_i>0} |a_i| \prod_{j\neq i}(1+a_i t) - \sum_{a_i<0} |a_i| \prod_{j\neq i}(1+a_i t) \\ &\leq (\sum_{a_i>0} |a_i|) \max_{a_k>0}\left(\prod_{j\neq k}(1+a_j t)\right) - (\sum_{a_i<0} |a_i|) \min_{a_k<0}\left(\prod_{j\neq k}(1+a_j t)\right). \end{aligned}$$

Since

$$\sum_{a_i>0} |a_i| = \sum_{a_i<0} |a_i|$$

and

$$\max_{a_k>0}\left(\prod_{j\neq k}(1+a_j t)\right) < \min_{a_k<0}\left(\prod_{j\neq k}(1+a_j t)\right)$$

we must have $F'(t) < 0$ on the desired interval, so F must be decreasing on this interval. □

Proposition 19.3.

$$\mathrm{Vol}(X_t) = \frac{2^{r-s}\pi^s t^n}{n!}.$$

Proof. The proof of this is in the book on p. 66. The last step in the calculation is integration by parts, which the book neglects to mention. □

Lemma 19.4. *Let U be any bounded region of V and let $\mathcal{L}$ be a full lattice in V. Then $\mathcal{L}\cap U$ is finite.*

Proof. Let $w_1,\ldots,w_n$ be a basis for $\mathcal{L}$ and let $x_1,\ldots,x_n$ be the basis for V that gives the volume form. If M is the matrix given by $Mx_i = w_i$, then for any integers m_i we have

$$\|\sum_{i=1}^{n} m_i w_i\| \geq \|M\|_{\mathrm{inf}} \sum_{i=1}^{n} m_i^2$$

where $\|M\|_{\mathrm{inf}}$ is the minimum value of $|M(y)|$ for y on the unit sphere centered at the origin (which is nonzero). For any constant C there are finitely many integers m_i such that

$$\sum_{i=1}^{n} m_i^2 \|M\|_{\mathrm{inf}}^2 \leq C^2$$

so there are finitely many elements of λ in the sphere of radius C centered at the origin. Any bounded region is contained in such a sphere, so we are done. □

Now, let I be a fractional ideal in $\mathcal{L}$. The ideal I is torsion-free as $\mathbb{Z}$-module. We can calculate the volume of $h(I)$ in terms of the degree of L, the discriminant $|\Delta(\mathfrak{o}_L/\mathbb{Z})|$, and $|\,\mathrm{N}_{L/K}(I)|$.

We'll want to define the discriminant of fractional ideal I first. We haven't yet defined the norm of a fractional ideal. Since a fractional ideal I of a Dedekind domain factors as

$$\mathfrak{q}_1^{e_1}\cdots\mathfrak{q}_m^{e_m}$$

we can simply define the norm of I to be

$$\mathrm{N}_{L/\mathbb{Q}}(I)=\mathrm{N}_{L/\mathbb{Q}}(\mathfrak{q}_1^{e_1})\cdots\mathrm{N}_{L/\mathbb{Q}}(\mathfrak{q}_m^{e_m}).$$

Definition 19.5. Let I be an fractional ideal of $\mathfrak{o}_L$. Let $\sigma_1,\ldots,\sigma_n$ be the n distinct embeddings of $L\longrightarrow\mathbb{C}$ and let $w_1,\ldots,w_n$ generate I over $\mathbb{Z}$. We define the discriminant of $\Delta(I/\mathbb{Z})$ to be

$$\Delta(I/\mathbb{Z}):=\det[\sigma_i(w_j)]^2.$$

This definition does not depend on our choice of the basis, since two different bases differ by a linear transformation with determinant ±1. (Note that this coincides with our earlier definition involving the trace form, by work done on the midterm.)

Definition 19.6. Let p be a prime in $\mathbb{Z}$. Let $S=\mathbb{Z}\setminus p\mathbb{Z}$. Let J be a fractional ideal of $S^{-1}\mathfrak{o}_L$. We define

$$\Delta(J/\mathbb{Z}_{(p)})=Z_{(p)}\det[\sigma_i(w_j)]^2,$$

where $w_1,\ldots,w_n$ is a basis for J over $\mathbb{Z}_{(p)}$

Lemma 19.7. *Let I be a fractional ideal of $\mathfrak{o}_L$. Then*

$$\mathbb{Z}_{(p)}\Delta(I/\mathbb{Z})=\Delta(S^{-1}I/\mathbb{Z}_{(p)}).$$

Proof. This follows immediately from the fact that any basis for I over $\mathbb{Z}$ is a basis for $S^{-1}I$ over $\mathbb{Z}_{(p)}$. □

Theorem 19.8. *We have $\mathbb{Z}\Delta(I/\mathbb{Z})=\mathrm{N}_{L/K}(I)^2\Delta(\mathfrak{o}_L/\mathbb{Z})$.*

Proof. Both the norm and the discriminant can be calculated locally, so it suffices to prove that for p a prime of $\mathbb{Z}$ and $S=\mathbb{Z}\setminus p\mathbb{Z}$ we have

$$\Delta(S^{-1}\mathfrak{o}_LI/\mathbb{Z}_{(p)})=\mathrm{N}_{L/K}(S^{-1}\mathfrak{o}_LI)\Delta(\mathfrak{o}_L/\mathbb{Z}_{(p)}).$$

Since $S^{-1}\mathfrak{o}_L$ is a principal ideal domain, we can write $S^{-1}I=S^{-1}\mathfrak{o}_Ly$ for some $y\in L$. Now, if $w_1,\ldots,w_n$ is a basis for $S^{-1}\mathfrak{o}_L$ over $\mathbb{Z}_{(p)}$, then $yw_1,\ldots,yw_n$ is basis for $S^{-1}I$ over $\mathbb{Z}_{(p)}$. The matrix $[\sigma_i(yw_j)]$ is equal to the matrix $[\sigma_i(y)|\sigma_i(w_j)]$ which is equal to $[\det \sigma_i(w_j)]$ times the matrix

$$\begin{pmatrix} \sigma_1(y) & 0 & \cdots & 0 \\ 0 & \sigma_2(y) & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \sigma_n(y) \end{pmatrix}$$

which has determinant equal to $\mathrm{N}_{L/\mathbb{Q}}(y)$. Thus,

$$\Delta(S^{-1}\mathfrak{o}_L I/\mathbb{Z}_{(p)}) = \left(\mathrm{N}_{L/K}(y)\det[\sigma_i(w_j)]\right)^2 = \mathrm{N}_{L/K}(y)^2\Delta(S^{-1}\mathfrak{o}_L/\mathbb{Z}_{(p)}).$$

□

Corollary 19.9. *Let $I \subset \mathfrak{o}_L$ be an fractional ideal. Then $h(I)$ is a lattice with volume*

$$(1/2)^s|\,\mathrm{N}_{L/\mathbb{Q}}(I)|\sqrt{|\Delta(\mathfrak{o}_L/\mathbb{Z})|}.$$

Proof. Since the volume of $h(I)$ is $|\det[h_i(w_j)]|$ this follows from taking square roots in Theorem 19.8 and noting the connection between the h_i and the σ_i. □

Now we are ready for our main Theorem.

Theorem 19.10. *Let I be a nonzero fractional ideal of $\mathcal{O}_L$. Then there exists $a \neq 0$ such that*

$$|\,\mathrm{N}_{L/\mathbb{Q}}(a)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{\Delta(\mathcal{O}_L/\mathbb{Z})}\,\mathrm{N}_{L/\mathbb{Q}}(I).$$