Math 531 Tom Tucker
NOTES FROM CLASS 11/10

We'll need Minkowski's theorem, which guarantees the existence of certain elements of a lattice. We'll recall a a lemma from last time.

Lemma 29.1. *Let $\mathcal{L}$ be a lattice in V ($\mathbb{R}^n$ with a volume form) and let U be a measurable subset of V such that the translates $U + \lambda$, where $\lambda \in \mathcal{L}$ are disjoint. Then* $\operatorname{Vol}(U) \leq \operatorname{Vol}(\mathcal{L})$.

Proof. Let $\mathcal{T}$ be a fundamental parallelepiped for some basis of $\mathcal{L}$. For each $\lambda \in \mathcal{L}$, let

$$U_\lambda = \mathcal{T} \cap (U - \lambda).$$

We then have

$$U = \bigcup_{\lambda \in \mathcal{L}} (U_\lambda + \lambda).$$

Since the volume form is translate invariant, we see that

$$\sum_{\lambda \in \mathcal{L}} \operatorname{Vol}(U_\lambda) = \sum_{\lambda \in \mathcal{L}} \operatorname{Vol}(U_\lambda + \lambda) = \operatorname{Vol}(U).$$

Since all the U_λ are disjoint and contained in $\mathcal{T}$, we see that

$$\operatorname{Vol}(\mathcal{L}) = \operatorname{Vol}(\mathcal{T}) \geq \operatorname{Vol}(\bigcup_{\lambda \in \mathcal{L}} (U_\lambda)) = \sum_{\lambda \in \mathcal{L}} \operatorname{Vol}(U_\lambda) = \operatorname{Vol}(U).$$

$\square$

Theorem 29.2. *(Minkowsi) Let $\mathcal{L}$ be a full lattice in the volumed vector space V of dimension n and let U be a bounded, centrally symmetric, convex subset of V. If* $\operatorname{Vol}(U) > 2^n \operatorname{Vol}(\mathcal{L})$*, then U contains a nonzero element $\lambda \in \mathcal{L}$*

Proof. By the way, centrally symmetric means that for $x \in U$, we have $-x \in U$. Convex means that for $x, y \in U$ and $t \in [0, 1]$, we have $tx + (1 - t)y \in U$.

Now, let $W = \frac{1}{2}U$. Then $\operatorname{Vol}(W) = \frac{1}{2^n} \operatorname{Vol}(U)$, so $\operatorname{Vol}(W) > \operatorname{Vol}(\mathcal{L})$, so it follows from the Lemma, we just proved that not all of the translates $W+\lambda$ are disjoint. Taking $y \in (W+\lambda)\cap(W+\lambda')$, with $\lambda \neq \lambda'$, we can write $y = a + \lambda = b + \lambda'$, which gives us $a, b \in W$ with $(a - b) \in \mathcal{L}$ and $(a-b) \neq 0$. Since $a, b \in W = \frac{1}{2}U$, we can write $a = \frac{1}{2}x$ and $b = \frac{1}{2}y$ for $x, y \in U$. Since y is convex and centrally symmetric the element $a - b = \frac{1}{2}x - \frac{1}{2}y = \frac{1}{2}x + \frac{1}{2}(-y) \in U$ and we are done. $\square$

We will want to apply this to a lattice $h(I)$ for I a fractional ideal of $\mathcal{O}_L$. The region U that we use should consist of elements of bounded norm. Recall though, that the most natural sort of region is something like a sphere $\sqrt{x_1^2 + \cdots + x_n^2} \leq M$ and we are going to be interested in something like the product $x_1 \cdots x_n$, so we will need something relating these two. Also, we have messed around a bit at the complex places, to we'll have to tinker with that a bit. Let's label our coordinate system for V in the following way. We call the first r-coordinates corresponding to the real embeddings $x_1, \dots, x_r$. The remaining $2s$ coordinates we label as $y_1, z_1, \dots, y_s, z_s$.

Let

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

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

Proof. Let $b_i = \sigma_i(y)$ for $1 \leq i \leq r$ 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

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

Taking n-th powers finishes the proof. □

Lemma 29.4. *Let $b_1, \dots, b_n$ be positive numbers. Then*

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

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

$$b_1 \cdots b_n \leq 1.$$

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

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

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. $\square$