Math 531 Tom Tucker
NOTES FROM CLASS 11/22

Recall the definition of $Z_{(t)}$ from last time...

Let (t) be an $(r+s)$-tuple of positive numbers indexed as $(t)_i$. We define

$$\begin{aligned} Z_{(t)} :=& \{(x_1, \ldots, x_{s+r}) \in \mathbb{R}^r \times \mathbb{C}^s \;\mid\; |x_i| \le (t)_i, 1 \le i \le r \\ & \text{and } |x_i|^2 \le (t)_i \text{ for } r+1 \le i \le r+s\} \end{aligned}$$

The region $Z_{(t)}$ is just a cross product of regions in $\mathbb{R}$ and $\mathbb{C}$, specifically it is

$$\begin{aligned} &[-(t)_1, (t)_1] \times \cdots \times [-(t)_r, (t)_r] \\ &\times \{(x,y) \;\mid x^2 + y^2 \le (t)_{r+1}\} \times \cdots \times \{(x,y) \;\mid x^2 + y^2 \le (t)_{r+s}\}. \end{aligned}$$

Thus,

$$\mathrm{Vol}(Z_{(t)}) = 2^r \pi^s t_1 \cdots t_{r+s}$$

And $Z_{(t)}$ is convex and centrally symmetric. Now, let's fix a constant T, for which

$$2^r \pi^s T^{r+s} > 2^n \,\mathrm{Vol}(h^*(\mathcal{O}_L))$$

and let (γ) be any n-tuple of numbers for which

$$\gamma_1 \cdots \gamma_{r+s} = 1.$$

Then

$$\mathrm{Vol}(Z_{(T\gamma)}) = 2^r \pi^s T^n > 2^n \,\mathrm{Vol}(h^*(\mathcal{O}_L)),$$

so there exists a nonzero $b \in Z_{(T\gamma)} \cap h^*(\mathcal{O}_L)$, by Minkowski's lemma proven earlier. As said earlier, we want to control the signs of the logs of our units, so we will pick a particular (γ) where $(\gamma_i) < 1$ for all but one i. Specifically, we pick a number ϵ and define

$$(\epsilon_i) = \begin{cases} \epsilon & : \quad j \neq i \\ 1/\epsilon^{r+s-1} & : \quad j = i \end{cases}$$

As above, we know that there is a nonzero element of $h^*(\mathcal{O}_L)$ in $Z_{(T\epsilon_i)}$, call it b_i. The following Lemma is obvious. We state it to organize our exposition.

Proposition 34.1. *Let $b_i \in Z_{(T\epsilon_i)} \cap h^*(\mathcal{O}_L)$ with $b_i \neq 0$. Then*

$$|\,\mathrm{N}(b_i)| \le T^{s+r}.$$

Proof. Recall of course that $p_j(h^*(b)) = \sigma_j(b)$, so if $h^*(b) \in Z_{(T\epsilon_i)}$, then $|\sigma_j(b)| \leq (T\epsilon_i)_j$ for $1 \leq j \leq r$ and $|\sigma_j(b)|^2 \leq (T\epsilon_i)_j$ for $r+1 \leq j \leq (s+r)$. Thus, for $b_i \in Z_{(T\epsilon_i)}$, we have

$$|\operatorname{N}(b_i)| \leq \prod_{j=1}^{r} |\sigma_j(b)| \prod_{j=r+1}^{s+r} |\sigma_j(b)|^2 \leq \prod_{j=1}^{r+s} (T\epsilon_i)_j = T^{r+s}.$$

□

Unfortunately, the b_i are not units. However, we need only modify them slightly to obtain units. There are only finitely many nonzero principal ideals in $\mathcal{O}_L$ with norm less than T^{r+s} (since there are finitely many ideals in $\mathcal{O}_L$ of bounded norm). Let us number them as $I_1, \dots, I_N$, write $I_k = \mathcal{O}_L a_k$, for $a_k \in \mathcal{O}_L$ and pick $\epsilon > 0$ such that

$$0 < \epsilon T < \min\{|\sigma_i(a_k)|^{e_i}, i = 1, \dots, r+s, k = 1, \dots, N\},$$

where $e_i = 1$ if σ_i is a real place and $e_i = 2$ is σ_i is complex place. Note that this min cannot be zero because $a_k \neq 0$ and σ_i is injective. For each $i = 1, \dots, r+s$, let $Z_{(T\epsilon_i)}$ and b_i be as in the Proposition above. Since $\operatorname{N}(\mathcal{O}_L b_i) \leq T^{r+s}$, the ideal $\mathcal{O}_L b_i$ is equal to some $\mathcal{O}_L a_{k(i)}$. Let $u_i = a_{k(i)}/b_i$. Then, u_i must be a unit since b_i divides $a_{k(i)}$ and $a_{k(i)}$ divides b_i.

Proposition 34.2. *Let u_i be as above. Then*

(1) $\sum_{j=1}^{r} \log|\sigma_j(u_i)| + \sum_{j=r+1}^{r+s} 2\log|\sigma_j(u_i)| = 0$
(2) $\log|\sigma_j(u_i)| < 0$ *for* $j \neq i$
(3) $\log|\sigma_i(u_i)| > 0$.

Proof. (1): This is easy since $|\operatorname{N}(u_i)| = 1$, so

$$0 = \log 1 = \log|\operatorname{N}(u_i)| = \sum_{j=1}^{r} \log|\sigma_j(u_i)| + \sum_{j=r+1}^{r+s} 2\log|\sigma_j(u_i)| = 0.$$

(2): Recall that $T\epsilon < |\sigma_j(a_{i(k)}^{e_j}|$, so

$$\log|\sigma_j(u_i)^{e_i}| = \log\frac{|\sigma_j(b_i)^{e_i}|}{|\sigma_j(a_{i(k)})^{e_i}|} < \log\frac{T\epsilon}{|\sigma_j(a_{i(k)})|^{e_i}} < \log 1 = 0.$$

Thus, $\log|\sigma_j(u_i)| = \frac{1}{2}\log|\sigma_j(u_i)^{e_i}| < 0$ as well.

(3): Follows immediately from (1) and (2)

□

Proposition 34.3. *The elements $\ell(u_i)$, $i = 1, \dots r+s-1$ (note we don't go up all the way to $r+s$) are linearly independent over $\mathbb{R}$.*

Proof. Let $m_{ij} = \log|\sigma_j(u_i)|$ for $1 \le i \le r$ and $m_{ij} = 2\log|\sigma_j(u_i)|$ for $r+1 \le i \le r+s-1$. Since

$$\sum_{j=1}^{r} \log|\sigma_j(u_i)| + \sum_{j=r+1}^{r+s} 2\log|\sigma_j(u_i)| = 0,$$

the $\log|\sigma_{r+s}(u_j)|$ is determined by the other $\log|\sigma_j(u_i)|$; that is why we only go up to $r+s-1$. To show that the $\ell(u_i)$ are linearly independent, it will suffice to show that the matrix $[m_{ij}]$ is nonsingular. It follows from Proposition 34.2 that for any i, we have

$$\sum_{j=1}^{r+s-1} m_{ij} > 0.$$

It also follows that $m_{ij} < 0$ for $i \neq j$ and $m_{jj} > 0$ for any j.

The embeddings of a fixed u_i gives us the i-th row of $[m_{ij}]$; it will be easier to show that the columns are linearly independent over $\mathbb{R}$. Suppose that we have a set $a_1, \dots, a_{r+s-1}$ of real numbers, not all of which are zero. We can show that there is some i such that

$$\sum_{j=1}^{r+s-1} a_j m_{ij} \neq 0.$$

Indeed, let us pick i so that $|a_i| \ge |a_j|$ for for all j; we may assume that $a_i > 0$ since multiplying everything though by -1 will not affect whether or not a sum is nonzero. Then we $a_i \ge a_j$ for every j and (since $m_{ij} < 0$ for $i \neq j$) we have

$$\sum_{j=1}^{r+s-1} a_j m_{ij} \ge a_i m_{ii} + \sum_{j \neq i} a_i m_{ij} \ge a_i \sum_{j=1}^{r+s-1} m_{ij} > 0$$

and we are done. □

Corollary 34.4. *$\ell(\mathcal{O}_L^*)$ is a full lattice in H.*

Proof. We have already seen that $\ell(\mathcal{O}_L^*)$ is a lattice in H. It is a full lattice since it generates a $\mathbb{R}$-vector space of dimension $r+s-1$, which must be equal to H (since $\dim_{\mathbb{R}} H = r+s-1$). □

Theorem 34.5 (Dirichlet Unit Theorem)**.** *Let μ_L be the roots of unity in L. There exist elements $v_1, \dots, v_{r+s-1} \in \mathcal{O}_L^*$ such that every unit $u \in \mathcal{O}_L^*$ can be written uniquely as*

$$u = v v_1^{m_1} \cdots v_{r+s-1}^{m_{r+s-1}}$$

for $v \in \mu_L$ and $m_i \in \mathbb{Z}$.

Proof. Let $v_1, \ldots, v_{r+s-1}$ have the property that $\ell(v_1), \ldots, \ell(v_{r+s-1})$ generate $\ell(\mathcal{O}_L^*)$ as a $\mathbb{Z}$-module. Since $\ker \ell = \mu_L$, we know that every unit $u \in \mathcal{O}_L^*$ can be written as vz, where z is in the subgroup generated by the $v_1, \ldots, v_{r+s-1}$. The element z is uniquely determine by $\ell(u)$ as

$$v_1^{m_1} \cdots v_{r+s-1}^{m_{r+s-1}}$$

for some integers m_i. Then $v = zu^{-1}$ and is therefore also uniquely determined. $\square$