Lecture 16 (18.12.)

Lemma 7.2

If L has at least one real embedding, then $TU(G^*) = \{\pm 1\}$.

Proof:

Let $\sigma : L \to \mathbb{R} \subset \mathbb{C}$. If $\alpha \in TU(G^*) \Rightarrow |\sigma(\alpha)| = 1$ by Prop 7.1, hence $\sigma(\alpha) = \pm 1 \Rightarrow \alpha = \pm 1$. $\square$

Lemma 7.3

$TU(G) = TU(G_L) \cap G$.

Proof:

$\subseteq$ is clear. Let $\alpha \in TU(G_L) \cap G$. Then $\alpha^k = 1$ for some $k > 0$. Hence $\alpha^{-1} = \alpha^{k-1} \in G$. $\square$

7.2 Units are finitely generated

Minkowski theory (§6.4) has a multiplicative version.

Denote by log the natural logarithm. To simplify notations, define

$$c_i := \begin{cases} 1 & \text{if } 1 \le i \le r \quad (\text{real embeddings}) \\ 2 & \text{if } r+1 \le i \le r+s \quad (\text{non-real embeddings}) \end{cases}$$

If $\alpha \in G^*$, then

$$1 = |N_{L|\mathbb{Q}}(\alpha)| = \prod_{i=1}^{n} |\sigma_i(\alpha)| = \prod_{i=1}^{r+s} |\sigma_i(\alpha)|^{c_i}$$

Hence,

$$0 = \underbrace{\log}_{\text{natural log}}(1) = \sum_{i=1}^{r+s} c_i \cdot \log|\sigma_i(\alpha)| \Rightarrow c_{r+s} \log|\sigma_{r+s}(\alpha)| = -\sum_{i=1}^{r+s-1} c_i \log|\sigma_i(\alpha)|$$

This leads to the following definition:

Def 7.4

The log-Minkowski map is the map

$$j^* : L^* \longrightarrow \mathbb{R}^{r+s-1}$$

mapping $\alpha \in L^*$ to

$$\left(c_i \log|\sigma_i(\alpha)|\right)_{i=1,\dots,r+s-1}$$

Lemma 7.5

a) j^* is a group morphism $(L^*, \cdot) \longrightarrow (\mathbb{R}^{r+s-1}, +)$

b) $\ker(j^*|_{G^*}) = TU(G)$.

Proof:

a) Let $\alpha, \beta \in L^*$. Then

$$\log|\sigma_i(\alpha\beta)| = \log|\sigma_i(\alpha)\sigma_i(\beta)| = \log|\sigma_i(\alpha)| + \log|\sigma_i(\beta)|$$

$$\Rightarrow j^*(\alpha\beta) = j^*(\alpha) + j^*(\beta)$$

b) $\alpha \in \ker(j^*|_{G^*}) \Leftrightarrow \log|\sigma_i(\alpha)| = 0 \ \forall i \Leftrightarrow |\sigma_i(\alpha)| = 1 \ \forall i \Leftrightarrow \alpha \in TU(G)$

by Prop 7.1

$\square$

Consider G^* as a $\mathbb{Z}$-module. Note that $\varepsilon_1, .., \varepsilon_k \in G^*$ linearly independent mesur that

$$\prod_{i=1}^{k} \varepsilon_i^{m_i} = 1 \implies m_i = 1 \ \forall i.$$

Prop 7.6

If $\varepsilon_1, .., \varepsilon_k \in G^*$ are linearly independent over $\mathbb{Z}$, then $j^*(\varepsilon_1), .., j^*(\varepsilon_k) \in \mathbb{R}^{r+s-1}$ are linearly independent over $\mathbb{R}$.

Proof: Suppose that $j^*(\varepsilon_1), .., j^*(\varepsilon_k)$ are linearly dependent over $\mathbb{R}$.

We need to show that $\varepsilon_1, .., \varepsilon_k$ are linearly dependent over $\mathbb{Z}$.

Wlog we assume that $j^*(\varepsilon_1)$ is an $\mathbb{R}$-linear combination of $j^*(\varepsilon_2), .., j^*(\varepsilon_k)$.

Consider more generally the set $\mathcal{E}$ of all $\varepsilon \in G^*$ such that

$$j^*(\varepsilon) = \sum_{i=2}^{k} t_i j^*(\varepsilon_i) \text{ for some } t_i \in \mathbb{R}$$

Set $m_i := -\mathrm{round}(t_i) = -\lfloor t_i + 1/2 \rfloor \in \mathbb{Z}$ for $2 \le i \le k$, where $\lfloor t \rfloor$ denotes the largest integer $\leq t$. Then

$$j^A(\varepsilon) = \sum_{i=2}^{k} t_i j^A(\varepsilon_i) = \sum_{i=2}^{k} (t_i + m_i) j^A(\varepsilon_i) - \sum_{i=2}^{k} m_i j^A(\varepsilon_i)$$

Set $\eta := \eta(\varepsilon) := \varepsilon\, \varepsilon_2^{m_2} \cdot \ldots \cdot \varepsilon_k^{m_k}$. Then

$$j^A(\eta) = j^A(\varepsilon) + \sum_{i=2}^{k} m_i j^A(\varepsilon_i) = \sum_{i=2}^{k} (t_i + m_i) j^A(\varepsilon_i)$$

$$\Rightarrow \|j^A(\eta)\| \leq \sum_{i=2}^{k} \underbrace{|t_i + m_i|}_{\leq 1/2} \cdot \|j^A(\varepsilon_i)\| \leq \frac{1}{2} \sum_{i=2}^{k} \|j^A(\varepsilon_i)\| =: C'$$

$\Rightarrow \|j^A(\eta)\| \leq C' \;\; \forall \varepsilon \in E \Rightarrow c_i \log|\sigma_i(\eta)| \leq C' \;\forall i\; \forall \varepsilon$

depends on ε!

$\Rightarrow |\sigma_i(\eta)| \leq e^{C'} \;\; \forall i, \;\forall \varepsilon \in E$

$\Rightarrow E_\eta := \{\eta(\varepsilon) \mid \varepsilon \in E\} \subset \{\alpha \in G \mid \|j(\alpha)\| \leq \underbrace{\sqrt{n \cdot e^{C'}}}_{=:C}\}$

$\|j(\alpha)\|^2 = \langle j(\alpha), j(\alpha)\rangle = \langle j_{\mathbb{C}}(\alpha), j_{\mathbb{C}}(\alpha)\rangle = \sum_{i=1}^{n} |\sigma_i(\alpha)|^2$

This set is finite since $j(G)$ is a lattice.

$\Rightarrow$ Since $\varepsilon_1^m \in E \;\forall m \in \mathbb{Z}$, there must be $m_1, m_1' \in \mathbb{Z}$, $m_1 \neq m_1'$ with $\eta(\varepsilon_1^{m_1}) = \eta(\varepsilon_1^{m_2})$, i.e.

exponents depend on choice of ε

$$\varepsilon_1^{m_1} \varepsilon_2^{m_2} \cdots \varepsilon_k^{m_k} = \varepsilon_1^{m_1'} \varepsilon_2^{m_2'} \cdots \varepsilon_k^{m_k'}$$

$$\Rightarrow \prod_{i=1}^{k} \varepsilon_i^{m_i - m_i'} = 1$$

$\Rightarrow \varepsilon_1, \ldots, \varepsilon_k$ linearly dependent. $\square$

Prop 7.7

a) G^* is a finitely generated $\mathbb{Z}$-module

b) $G^*/TU(G)$ is a free $\mathbb{Z}$-module

c) $G^* \simeq TU(G) \oplus G^*/TU(G) \simeq TU(G) \oplus j^A(G^*)$

Proof: Let $\varepsilon_2, \ldots, \varepsilon_k \in G^*$ be a maximal linearly independent set. By

Prop 7.6 we know that $k \le r+s < \infty$. If $\varepsilon \notin \mathbb{Z}\cdot\{\varepsilon_2, .., \varepsilon_k\}$, then $\varepsilon, \varepsilon_2, .., \varepsilon_k$ are linearly dependent $\Rightarrow j^*(\varepsilon), j^*(\varepsilon_2), .., j^*(\varepsilon_k)$ are linearly dependent
$\Rightarrow \varepsilon$ is contained in the set E in the proof of Prop 7.6.
$\Rightarrow \eta(\varepsilon) = \varepsilon \cdot \varepsilon_2^{m_2} \cdots \varepsilon_k^{m_k}$ (for certain m_i) is contained in E_η.
As argued in the proof of Prop 7.6, $E_\eta = \{\eta_1, .., \eta_r\}$ is finite, hence $\varepsilon = \eta_i \varepsilon_2^{-m_2} \cdots \varepsilon_k^{-m_k}$ for some $k \Rightarrow G^* / \mathbb{Z}\{\varepsilon_2, .., \varepsilon_k\} \subseteq E_\eta$ (finitely many cosets)
$\Rightarrow G^*$ is a f.g. $\mathbb{Z}$-module. Now, b) and c) follow directly from the structure of f.g. $\mathbb{Z}$-modules (Thm 3.66, Lemma 3.67) $\square$

We still need to determine the dimension of the free part of G^*.

7.3 Free rank of the unit group

Lemma 7.8

Suppose that $\varepsilon_1, .., \varepsilon_k \in G^*$, $k \le r+s-1$, satisfy

$$|\sigma_i(\varepsilon_i)| > 1 \quad \text{and} \quad |\sigma_j(\varepsilon_i)| < 1 \quad \forall i \ne j.$$

Then $\varepsilon_1, .., \varepsilon_k \in G^*$ are linearly independent.

Proof:

Consider the matrix

$$A = \left(c_j \log |\sigma_j(\varepsilon_i)| \right)_{\substack{i=1,..,k \\ j=1,..,r+s-1}} \in \mathrm{Mat}_{k \times (r+s-1)}(\mathbb{R})$$

We will show that A has full rank, i.e. $\operatorname{rk} A = k$.
By assumption:

$$A_{ii} = c_i \log|\sigma_i(\varepsilon_i)| > c_i \log 1 = 0 \quad \forall i \Rightarrow |A_{ii}| = A_{ii} \ \forall i$$

$$A_{ij} = c_j \log|\sigma_j(\varepsilon_i)| < c_i \log 1 = 0 \quad \forall i \ne j \Rightarrow |A_{ij}| = -A_{ij} \ \forall i \ne j.$$

For each i we have

$N(\varepsilon_i) = 1$ since ε_i is a unit

$$\sum_{j=1}^{r+s} c_j \log|\sigma_j(\varepsilon_i)| = \log \prod_{j=1}^{r+s} |\sigma_j(\varepsilon_i)|^{c_j} = \log |N_{L|\mathbb{Q}}(\varepsilon_i)| = \log 1 = 0$$

Hence

$$|A_{ii}| = A_{ii} = c_i \log|\sigma_i(\varepsilon_i)|$$

$$> c_i \log|\sigma_i(\varepsilon_i)| + \underbrace{c_{r+s} \log|\sigma_{r+s}(\varepsilon_i)|}_{<0 \text{ by ass.}}$$

$$= -\sum_{\substack{j=1 \\ j \neq i}}^{r+s-1} c_j \log|\sigma_j(\varepsilon_i)| = -\sum_{\substack{j=1 \\ j \neq i}}^{r+s-1} A_{ij} = \sum_{\substack{j=1 \\ j \neq i}}^{r+s-1} |A_{ij}|$$

A is "strictly diagonally dominant"

Denote by A_j the j-th column of A and suppose

$$\sum_{j=1}^{k} t_j A_j = 0 \quad , \; t_j \in \mathbb{R}, \text{ not all zero}$$

Let ℓ be such that $|t_\ell|$ is maximal among $|t_1|, \ldots, |t_k|$. Then

$$0 = \sum_{j=1}^{k} t_j A_{\ell j} = t_\ell \Big(A_{\ell\ell} + \sum_{\substack{j=1 \\ j \neq \ell}}^{k} \frac{t_j}{t_\ell} A_{\ell j} \Big)$$

$$\Rightarrow A_{\ell\ell} = -\sum_{\substack{j=1 \\ j \neq \ell}}^{k} \frac{t_j}{t_\ell} A_{\ell j} \Rightarrow |A_{\ell\ell}| = \Big| \sum_{\substack{j=1 \\ j \neq \ell}}^{k} \frac{t_j}{t_\ell} A_{\ell j} \Big| \leq \sum_{\substack{j=1 \\ j \neq \ell}}^{k} \underbrace{\frac{|t_j|}{|t_\ell|}}_{\leq 1} |A_{\ell j}|$$

$$\leq \sum_{\substack{j=1 \\ j \neq \ell}}^{k} |A_{\ell j}| \leq \sum_{\substack{j=1 \\ j \neq \ell}}^{r+s-1} |A_{\ell j}|$$

↯ To property of A proven above

$\square$