Lecture 17 (6.1.)

We call units as in Lemma 7.8 Dirichlet units.

We will now construct such units. This needs some preparation.

Lemma 7.9

For any i, $1 \le i \le r+s-1$, there is $C_i \in \mathbb{R}_{>0}$ such that given any non-zero $\alpha \in G$ there is a non-zero β in G such that

1. $|N(\beta)| \leq C_i$
2. $|\sigma_j(\beta)| < |\sigma_j(\alpha)| \quad \forall j \neq i.$

Proof: We will show that $C_i = \left(\frac{2}{\pi}\right)^s \sqrt{|d_G|}$ works (independent of i).

For $1 \le j \le r+s$ choose a $a_j > 0$ such that

$$a_j < |\sigma_j(\alpha)| \quad (\text{note: } \alpha \neq 0 \Rightarrow \sigma_j(\alpha) \neq 0\text{, so this is possible})$$

For $1 \le j \le r+s$ define $C_{i,j} := a_j$ if $j \neq i$ and let $C_{i,i}$ be such that

$$\prod_{j=1}^{r+s} C_{i,j}^{c_j} = \left(\frac{2}{\pi}\right)^s \sqrt{|d_G|} = C_i. \qquad c_j = \begin{cases} 1 & \text{if } 1 \le j \le r \\ 2 & \text{if } r+1 \le j \le r+s \end{cases}$$

Consider the set $E_i := E_i(\alpha) \subset \mathbb{R}^r \times \mathbb{R}^{2s}$ of all $(x_k)_{k=1}^{r+2s}$ such that

$$|x_j| \le C_{i,j} \quad \text{for } 1 \le j \le r$$

and

$$x_{2j-r-1}^2 + x_{2j-r}^2 \le 2C_{i,j}^2 \quad \text{for } r+1 \le j \le r+s$$

Then

$$\mathrm{vol}(E_i) = \prod_{j=1}^{r} 2C_{i,j} \cdot \prod_{j=r+1}^{r+s} \pi \cdot 2C_{i,j}^2 = 2^{r+s}\pi^s \prod_{j=1}^{r+s} C_{i,j}^{c_j}$$

$$= 2^{r+s}\pi^s \left(\frac{2}{\pi}\right)^s \sqrt{|d_G|} = 2^{r+2s}\sqrt{|d_G|} = 2^n d(\Lambda),$$

where $\Lambda = j(G)$ is the Minkowski lattice.

Hence, by Minkowski's lattice point theorem (Thm 6.18), there is a non-zero point $\beta \in G$ with $j(\beta) \in E_i$. For such a point we have

$$j(\beta) = (\sigma_1(\beta), \dots, \sigma_r(\beta), \sqrt{2}\,\mathrm{Re}\,\sigma_{r+1}(\beta), \sqrt{2}\,\mathrm{Im}\,\sigma_{r+1}(\beta), \dots, \sqrt{2}\,\mathrm{Re}\,\sigma_{r+s}(\beta), \sqrt{2}\,\mathrm{Im}\,\sigma_{r+s}(\beta))$$ 2

$|\cdot| \leq C_{ij}$

$\Rightarrow |\sigma_j(\beta)| \leq C_{ij}$

$$(\sqrt{2}\,\mathrm{Re}\,\sigma_j(\beta))^2 + (\sqrt{2}\,\mathrm{Im}\,\sigma_j(\beta))^2 \leq 2C_{ij}^2$$

$$\Rightarrow 2|\sigma_j(\beta)|^2 \leq 2C_{ij}^2$$

$$\Rightarrow |\sigma_j(\beta)| \leq C_{ij}$$

Hence, we have

$$|\sigma_j(\beta)| \leq C_{ij} \quad \forall j$$

Hence,

$$|\sigma_j(\beta)| \leq a_j < |\sigma_j(\alpha)| \text{ for } j \neq i$$

and

$$|N(\beta)| = \prod_{j=1}^{n} |\sigma_j(\beta)| = \prod_{j=1}^{r+s} |\sigma_j(\beta)|^{c_j} \leq \prod_{j=1}^{r+s} C_{ij}^{c_j} = C_i.$$

$\square$

Lemma 7.10

Given $C \in \mathbb{R}$, there are only finitely many non-associate elements $\alpha \in G$ with $|N(\alpha)| \leq C$.

Proof:

Since $N(\alpha) \in \mathbb{Z}$ for $\alpha \in G$, can assume $C \in \mathbb{N}_{>0}$.

Let $I := C \cdot G$, non-zero ideal of G. We first prove the following

Claim: If $\alpha, \beta \in G$ are such that $\alpha - \beta \in I$ and $|N(\alpha)| = C = |N(\beta)|$, then they are associated.

Proof: We have $\alpha - \beta = \gamma \cdot C$ for some $\gamma \in G$. Hence,

$$\frac{\alpha}{\beta} = 1 + \frac{C}{\beta} \cdot \gamma = 1 + \frac{|N(\beta)|}{\beta} \cdot \gamma$$

Let $\chi_\beta = \sum_{i=0}^{n} a_i X^i$ be the characteristic polynomial of β. Then $a_0 = \pm N(\beta)$.

Hence $0 = \chi_\beta(\beta) = \pm N(\beta) + \sum_{i=1}^{n} a_i \beta^i = \pm N(\beta) + \beta \cdot \underbrace{\left(\sum_{i=1}^{n} a_i \beta^{i-1}\right)}_{\in G}$

$\Rightarrow \frac{|N(\beta)|}{\beta} \in G \Rightarrow \frac{\alpha}{\beta} \in G.$

Similarly, $\frac{\beta}{\alpha} \in G \Rightarrow \frac{\alpha}{\beta} \in G$ is a unit $\Rightarrow \alpha$ and β are associated.

Now, let $A := \{\bar{\alpha} \mid \alpha \in G, |N(\alpha)| = C\} \subseteq G/I$. By Lemma 5.23, $\dim_{\mathbb{Z}} I = \dim_{\mathbb{Z}} G$, 3
so G/I, and thus A, is finite. Let $\alpha_1, \dots, \alpha_r$ be representatives of A. If $\alpha \in G$ with $|N(\alpha)| = C$,
then $\alpha \equiv \alpha_i \mod I$ for some $i \Rightarrow \alpha, \alpha_i$ associate. $\square$

Now, we can prove:

Prop 7.11

There are $\varepsilon_1, \dots, \varepsilon_{r+s-1} \in G^*$ satisfying the properties of Lemma 7.8.

Hence, $G^*/TU(G)$ is free of rank $r+s-1$ and $j^*(G^*) \subset \mathbb{R}^{r+s-1}$ is a lattice.

Proof:

For each i, $1 \le i \le r+s-1$, do the following.

Choose C_i as in Lemma 7.9. Choose a non-zero $\alpha_{i,1} \in G$.

By Lemma 7.9, there is a non-zero $\alpha_{i,2} \in G$ with $|N(\alpha_{i,2})| \le C_i$ and

$|\sigma_j(\alpha_{i,2})| < |\sigma_j(\alpha_{i,1})| \quad \forall j \neq i$.

Repeating this process yields a sequence $\alpha_{i,k} \in G$ with

$$|N(\alpha_{i,k})| \le C_i, \quad |\sigma_j(\alpha_{i,k})| < |\sigma_j(\alpha_{i,k-1})| \quad \forall j \neq i$$

By Lemma 7.10 there are only finitely many non-associate elements in G
with norm bounded by C_i. Hence, there is $k, k' \in \mathbb{N}$, $k' > k$, such that

$$\varepsilon_i := \frac{\alpha_{i,k'}}{\alpha_{i,k}} \in G^*$$

We have

$$|\sigma_j(\varepsilon_i)| = \frac{\sigma_j(\alpha_{i,k'})}{\sigma_j(\alpha_{i,k})} < 1.$$

Since $\varepsilon_i \in G^*$, we have $N(\varepsilon_i) = 1$ and since $N(\varepsilon_i) = \prod_j \sigma_j(\varepsilon_i)$,

we must have $|\sigma_i(\varepsilon_i)| > 1$.

The $\varepsilon_1, \dots, \varepsilon_{r+s-1}$ constructed thus satisfy the assumptions of Lemma 7.8

$\Rightarrow$ they are linearly independent $\Rightarrow \dim_{\mathbb{Z}} G^*/T(G) \ge r+s-1$.

By Prop 7.6 $\le r+s-1$, hence $= r+s-1$. $\square$

Corollary 7.12 (Dirichlet's unit theorem)

$G^* \simeq (\mathbb{Z}/m\mathbb{Z}) \times \mathbb{Z}^{r+s-1}$ as abelian groups, where $m = |TU(G)|$. □

Def 7.13

A $\mathbb{Z}$-basis $\varepsilon_1, \dots, \varepsilon_{r+s-1}$ of the free part of G^* is called a system of fundamental units.

Def 7.14

The discriminant of the lattice $j^*(G^*) \subset \mathbb{R}^{r+s-1}$ is called the regulator of G, denoted $\operatorname{reg} G$.

So,

$$\operatorname{reg} G = |\det(j^*(\varepsilon_1), \dots, j^*(\varepsilon_{r+s-1}))| \in \mathbb{R}_{>0}$$

for one (any) system of fundamental units.

We write $\operatorname{reg} L := \operatorname{reg} G_L$.

Remark 7.15

Dirichlet units $\varepsilon_1, \dots, \varepsilon_{r+s-1}$ as constructed in Prop 7.11 generate an $r+s-1$ dimensional group, hence a subgroup U of G^* of finite index. But we do not need to have $G^* = U$. Similar situation as with equation order in the maximal order. We have

$$[G^* : U] = \frac{\operatorname{reg} U}{\operatorname{reg} G}, \quad \operatorname{reg} U := |\det(j^*(\varepsilon_1), \dots, j^*(\varepsilon_{r+s-1}))|$$

7.4 Remarks

The proof of Dirichlet's unit theorem (§7.1 – §7.3) yields an algorithm to compute G^*:

1. Compute $TU(G)$ by computing all $\alpha \in G$ with $\|j(\alpha)\|^2 = n$ (Prop 7.1).
2. Compute Dirichlet units $\varepsilon_1, \dots, \varepsilon_{r+s-1}$ (Lemma 7.8) by following the proof of Prop 7.11. To this end, one needs to make Lemma 7.9 constructive, more precisely

we need to find a $\beta \in E_i(\alpha)$ whose existence is implied by Minkowski's Theorem.
A brutal way to find this is as follows: $E_i(\alpha)$ was the set of $(x_k)_{k=1}^n$ with

$$|x_j| \leq C_{i,j} \quad \text{for } 1 \leq j \leq r$$

$$x_{2j-r-1}^2 + x_{2j-r}^2 \leq 2C_{i,j}^2 \quad \text{for } r+1 \leq j \leq r+s$$

Hence,

$$x_j^2 \leq C_{i,j}^2 \quad \text{for } 1 \leq j \leq r$$

$$x_{2j-r-1}^2, x_{2j-r}^2 \leq 2C_{i,j}^2$$

So

$$\|x_k\|^2 \leq \sum_{j=1}^{r} C_{i,j}^2 + 2\sum_{j=r+1}^{r+s} 2C_{i,j}^2 = \sum_{j=1}^{r} C_{i,j}^2 + 4\sum_{j=r+1}^{r+s} C_{ij}^2 =: C_i(\alpha)^2$$

Thus determine all lattice points $x \in \Lambda$ with $\|x\| \leq C_i(\alpha)$ and check if properties in Lemma 7.9 hold.
This is very inefficient, however. It can be done more efficiently using LLL.

By Lemma 7.8, $\varepsilon_1, \dots, \varepsilon_{r+s-1}$ are linearly independent and $G^*/\mathbb{Z}\cdot\{\varepsilon_1, \dots, \varepsilon_{r+s-1}\}$ is finite by the proof of Prop 7.6 and 7.7.

3. Let $C' := \frac{1}{2}\sum_{i=1}^{r+s-1} \|j^*(\varepsilon_i)\|$ and compute $U := \{\varepsilon \in G^* \mid \|j(\varepsilon)\| \leq C\}$, $C = \sqrt{n}e^{C'}$
Then $G^*/\mathbb{Z}\cdot\{\varepsilon_1, \dots, \varepsilon_{r+s-1}\} \subseteq U$ by the proof of Prop 7.6 and 7.7.

Hence, $G^* = \mathbb{Z}\cdot\{\varepsilon_1, \dots, \varepsilon_{r+s-1}, \varepsilon \in U\}$.

4. The vectors $j^*(\varepsilon)$ for $\varepsilon \in U$ and $\varepsilon = \varepsilon_1, \dots, \varepsilon_{r+s-1}$ span the lattice $j^*(G^*)$.
Use $\mathbb{R}$-linear algebra to find relations and extract a $\mathbb{Z}$-basis for this lattice.
The corresponding units yield a system of fundamental units.

Without improvements/modifications, this algorithm is very inefficient and cannot be used in practice.

Step 2 is about finding $r+s-1$ linearly independent units. There are also other ways to achieve this.

Step 3 is about the following. We have a subgroup $U := \mathbb{Z}\cdot\{\varepsilon_1, \dots, \varepsilon_{r+s-1}\}$ of finite index in G^*. We need to check whether $U = G^*$ already, and if not need to enlarge U. The situation is very similar to the computation of an integral basis (§5.3)

$$G^*/U \simeq \mathbb{Z}/p_1^{m_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_t^{m_t}\mathbb{Z}, \text{ where } [G^*:U] = p_1^{m_1}\cdot\ldots\cdot p_t^{m_t}.$$

Hence, for any $p \mid [G^*:U]$ we have to determine the <u>maximal p-subgroup</u> U_p of G^*, $U_p = \{x \in G^* \mid x^k \in U \text{ for } k \text{ some power of } p\}$ (or test whether $U = U_p$ already).

There is an algorithm to compute U_p (we skip this; note that for G we used that G is a ring; G^* is just a group).

What are the "critical" primes?

We have

$$[G^*:U] = \frac{\operatorname{reg} G}{\operatorname{reg} U}$$

Suppose we can bound $B \leq \operatorname{reg} G$ Then

$$[G^*:U] \leq \frac{\operatorname{reg} U}{B},$$

so if $p \mid [G^*:U]$, then $p \leq \frac{\operatorname{reg} U}{B}$.

We thus want good <u>lower bounds</u> for the regulator of G.

<u>Prop 7.16</u> (without proof, skipped)

Let $j_2^*: L \to \mathbb{R}^n$, $\alpha \mapsto (\log|\sigma_i(\alpha)|)_{i=1}^n$. Let $\Lambda := j_2^*(G^*)$, a lattice in $\mathbb{R}\cdot\Lambda \simeq \mathbb{R}^{r+s-1}$. Then

$$(\operatorname{reg} G)^2 \geq \frac{2^s \lambda_1(\Lambda)\cdots\lambda_{r+s-1}(\Lambda)}{n\,\underset{\substack{\uparrow\\ \text{Hermite constant.}}}{\gamma_{r+s-1}^{r+s-1}}}$$