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 $i$, let $i \leq r+s-1$, there is $C_i \in \mathbb{R}^+$ such that given any non-zero $x \in \mathbb{G}$ there is a non-zero $\beta$ in $\mathbb{G}$ such that

1. $|N(\beta)| \leq C_i$
2. $|\sigma_j(\beta)| < \left| \sigma_j(x) \right|$ for $j \neq i$.

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

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

$$a_j < \left| \sigma_j(x) \right|$$

(note: $A \to 0 = \sigma_j(0) = 0$, so this is possible)

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

$$\frac{r+s}{|i|} C_{i,j} = \left( \frac{2}{\pi} \right)^{s} \sqrt{|d|} = C_i.$$

Consider the set $E_i := E_i(x) \subset \mathbb{R}^r \times \mathbb{R}^{2s}$ of all $(x_1, \ldots, x_{r+s})$ such that

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

and

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

Then

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

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

where $\Lambda := \mathcal{L}(\mathbb{G})$ is the Minkowski lattice.

Hence, by Minkowski's lattice point theorem (Thm 6.18), there is a non-zero point $\beta \in \mathbb{G}$ with $\beta \in E_i$. For such a point we have
\[ \tilde{u}(\beta) = (\sigma_1(\beta), \ldots, \sigma_r(\beta), \sqrt{2} \Re \kappa_1(\beta), \sqrt{2} \Im \kappa_1(\beta), \ldots, \sqrt{2} \Re \kappa_s(\beta), \sqrt{2} \Im \kappa_t(\beta)) \]

\[ 1 \leq i \leq r \]

\[ \Rightarrow |\sigma_i(\beta)| \leq C_{ij} \]

\[ \Rightarrow 2 |\sigma_i(\beta)|^2 \leq 2C_{ij}^2 \]

\[ \Rightarrow |\sigma_i(\beta)| \leq C_{ij} \]

Hence, we have

\[ |\sigma_i(\beta)| \leq C_{ij} \quad \forall j \]

Hence,

\[ |\sigma_j(\beta)| \leq \alpha_j < |\sigma_i(\alpha)| \quad \text{for} \quad j \neq i \]

and

\[ |N(\beta)| = \prod_{j=1}^{n} |\sigma_j(\beta)| = \prod_{j=1}^{r} |\sigma_j(\beta)|^\gamma_j \leq \prod_{j=1}^{r} C_{ij}^\gamma_j = C. \]

Lemma 7.10

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

Proof:

Since \( N(\alpha) \in \mathbb{Z} \) for \( \alpha \in G \), we can assume \( \mathbb{C} = \mathbb{C}_0 \).

Let \( I = \mathbb{C} : G \), non-zero ideal of \( G \). We first prove the following

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

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

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

Let \( X_\beta = \sum_{i=0}^{\infty} \alpha_i \cdot \beta_i \) be the characteristic polynomial of \( \beta \). Then \( \alpha_0 = \pm N(\beta) \).

Hence \( 0 = X_\beta(\beta) = \pm N(\beta) + \sum_{i=1}^{\infty} \alpha_i \cdot \beta_i = \pm N(\beta) + \beta \cdot \left( \sum_{i=1}^{\infty} \alpha_i \cdot \beta_i^{-1} \right) \cdot \beta = \pm N(\beta) + \beta \cdot \left( \sum_{i=1}^{\infty} \alpha_i \cdot \beta_i^{-1} \right) \cdot \beta \in \mathbb{C} \)

\[ \Rightarrow |N(\beta)| \leq |\beta| \in G \Rightarrow \frac{\alpha}{\beta} \in G \]

Similarly, \( \frac{\beta}{\alpha} \in G \Rightarrow \frac{\alpha}{\beta} \in G \) is a unit \( \Rightarrow \alpha \) and \( \beta \) are associated.
Now, let \( A = \{ x \mid x \in E, N(x) = c \} \subseteq G / I. \) By Lemma 5.23, \( \dim \mathbb{Z} = \dim \mathbb{Z}_6 \) \( \Rightarrow \) \( G / I \) is finite. Let \( \alpha_1, \ldots, \alpha_r \) be representatives of \( A. \) If \( x \in E \) with \( N(x) = c \), then \( x = \alpha_i \) and \( I \) for some \( i = \alpha_i \), associate. \( \square \)

Now, we can prove:

Prop 7.11

There are \( \varepsilon_1, \ldots, \varepsilon_{r+s-1} \in G^\ast \) satisfying the properties of Lemma 7.8.

Hence, \( G^\ast / \mathbb{Z}(G) \) is free of rank \( r+s-1 \) and \( \left\langle \varepsilon_1(G) \right\rangle \cap \mathbb{Z}(G) \) is a lattice.

Proof:

For each \( i, 1 \leq i \leq r+s-1, \) do the following:

Choose \( \varepsilon_i \) as in Lemma 7.9. Choose a non-zero \( \alpha_i, 1 \in G. \)

By Lemma 7.9, there is a non-zero \( \alpha_i, 1 \in G \) with \( N(\alpha_i, 1) \leq C_i \) and

\[
|\varepsilon_j(\alpha_i, 1)| = |\varepsilon_j(\alpha_i, 1)| \neq i.
\]

Repeating this process yields a sequence \( \varepsilon_i, 1 \in G \) with

\[
|N(\varepsilon_i)| \leq C_i, \quad |\varepsilon_j(\varepsilon_i)| = |\varepsilon_j(\varepsilon_i)|, \quad \forall j \neq i.
\]

By Lemma 7.10, there are only finitely many non-associate elements in \( G \) with norm bounded by \( C_i. \) Hence, there is \( \varepsilon_i, 1, 1 \in G \), \( h_i \geq k_i \), such that

\[
\varepsilon_i := \frac{\varepsilon_i, 1}{\varepsilon_i, 1} \in G^\ast
\]

We have

\[
|\varepsilon_j(\varepsilon_i)| = \frac{\varepsilon_j(\varepsilon_i, 1)}{\varepsilon_j(\varepsilon_i, 1)} < 1
\]

Since \( \varepsilon_i \in G^\ast \), we have \( N(\varepsilon_i) = 1 \) and since \( N(\varepsilon_i) = \prod_{i=1}^n \varepsilon_i(\varepsilon_i) \), we must have \( |\varepsilon_j(\varepsilon_i)| > 1 \).

The \( \varepsilon_1, \ldots, \varepsilon_{r+s-1} \) constructed thus satisfy the assumptions of Lemma 7.8 \( \Rightarrow \) they are linearly independent \( \Rightarrow \) \( \dim \mathbb{Z} G^\ast / \mathbb{Z}(G) = r+s-1. \)

By Prop 7.6 \( \leq r+s-1 \), hence \( r+s-1. \) \( \square \)
Corollary 7.12 (Dirichlet's unit theorem)

\[ G^* \approx \left( \mathbb{Z}/m\mathbb{Z} \right) \times \mathbb{Z}^{r+s-1} \]

as abelian groups, where \( m = |TU(G)| \).

\[ \Box \]

Definition 7.13

A \( \mathbb{Z} \)-basis \( \epsilon_1, \ldots, \epsilon_{r+s-1} \) of the free part of \( G^* \) is called a system of fundamental units.

Definition 7.14

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

So,

\[ \text{reg} \ G = \left| \det \left( j^*(\epsilon_1), \ldots, j^*(\epsilon_{r+s-1}) \right) \right| \in \mathbb{R}_{>0} \]

for one (any) system of fundamental units.

We write \( \text{reg} \ L := \text{reg} \ G_L \).

Remark 7.15

Dirichlet units \( \epsilon_1, \ldots, \epsilon_{r+s-1} \) 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

\[ \left[ G^*, U \right] = \frac{\text{reg} \ U}{\text{reg} \ G} \] \[ \text{reg} \ U := \left| \det \left( j^*(\epsilon_1), \ldots, j^*(\epsilon_{r+s-1}) \right) \right| \]

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 \( \| j(\alpha) \|^2 = 1 \) (Prop 7.1).
2. Compute Dirichlet units \( \epsilon_1, \ldots, \epsilon_{r+s-1} \) (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 $\beta \in E_\gamma(\chi)$ whose existence is implied by Minkowski’s theorem. A brutal way to find this is as follows; $E_\gamma(\chi)$ was the set of $(x_k)_k \in \mathbb{N}$ with

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

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

Hence,

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

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

So

$$\|x_k\|^2 = \sum_{j=1}^{r} C_{i,j}^2 + 2 \sum_{j=r+1}^{r+s} C_{i,j}^2 = \sum_{j=1}^{r} C_{i,j}^2 + 4 \sum_{j=r+1}^{r+s} C_{i,j}^2 \:<: \: C_\gamma(\chi)^2$$

Thus determine all lattice points $x \in \Lambda$ with $\|x\| \leq C_\gamma(\chi)$ 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, $e_1, \ldots, e_{r+s}$ are linearly independent and $G^* / \mathbb{Z} \cdot \mathbb{Z}^{r+s-1}$ is finite by the proof of Prop 7.6 and 7.7.

3. Let $C' = \frac{1}{2} \sum_{i=1}^{r+s-1} \|x^*(e_i)\|$ and compute $U := \{ \mu \in G^* | \|j(\mu)\| \leq C \}$, $C = \text{fin} C'$. Then $G^* / \mathbb{Z} \cdot \{ e_1, \ldots, e_{r+s-1} \} \subseteq U$ by the proof of Prop 7.6 and 7.7.

Hence, $G^* = \mathbb{Z} \cdot \{ e_1, \ldots, e_{r+s-1} \} \subseteq U$.

4. The vectors $j^*(e_i)$ for $i \in U$ and $e \in E_{r+s-1}$ span the lattice $j^*(G^*)$.

Use $R$-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 $U = \mathbb{Z} \cdot \{e_1, \ldots, e_{r+s-1}\}$ 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 (§53):

$$G^*/U \simeq \mathbb{Z}/p_1^{n_1} \mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{n_k}\mathbb{Z},$$

where $[G^*/U] = p_1^{n_1} \cdots p_k^{n_k}$.

Hence, for any $p \mid [G^*/U]$ we have to determine the maximal $p$-subgroup $U_p$ of $G^*$, $U_p = \{ x \in G^* \mid x^{p^k} \in U \}$ for 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

$$[G^*/U] = \frac{\text{reg } G}{\text{reg } U},$$

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

$$[G^*/U] \leq \frac{\text{reg } U}{B},$$

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

We thus want good lower bounds for the regulator of $G$.

**Prop 7.16** (without proof, skipped)

Let $\mathcal{N}_2 : L \to \mathbb{R}^n$, $\alpha \mapsto (\log |\sigma_i(\alpha)|)_{i=1}^n$. Let $\Lambda = \mathcal{N}_2(G^*)$, a lattice in $\mathbb{R}^n$. $\Lambda \cong \mathbb{R}^{r+s-1}$. Then

$$(\text{reg } G)^2 \geq \frac{2^s \lambda_\infty(\Lambda) \cdots \lambda_{r+s-1}(\Lambda)}{n \gamma_{r+s-1}^{r+s-1}}$$

where $\gamma_{r+s-1}$ is the Hermite constant.