Lecture 11 (2.12)

5.9 Computing the \( p \)-multiplier

Let \( G \) be an order with basis \( \alpha_1, \ldots, \alpha_n \) and let \( I \subseteq G \) be a \( \mathbb{m} \)-zero ideal with basis \( \delta_1, \ldots, \delta_n \).

**Step 1.** Express each \( \gamma_i \) in the \( \alpha_j \)'s and write this as rows into the matrix \( A \in \text{Mat}_{mn}(\mathbb{Z}) \), i.e.

\[
\gamma_i = \sum_{j} A_{ij} \alpha_j \Rightarrow \alpha_i = \sum_{j} (A^{-1})_{ij} \gamma_j
\]

**Step 2.** For each \( k \), express the products \( \gamma_k \alpha_i \) in the \( \alpha_j \)'s and write this as rows into the matrix \( A_k \in \text{Mat}_{mn}(\mathbb{Z}) \), i.e.

\[
\gamma_k \alpha_i = \sum_{j} (A_k)_{ij} \alpha_j
\]

The rows of \( A_k \alpha_1 \) are linearly independent over \( \mathbb{Z} \):

\[
\sum_{i} c_i (\gamma_k \alpha_i) = 0 \Rightarrow \gamma_k (\sum_{i} c_i \alpha_i) = 0
\]

\[
\Rightarrow \sum_{i} c_i \alpha_i = 0 \text{ since } \gamma_k \neq 0 \text{ and we are in an integral domain,}
\]

\[
\Rightarrow c_i = 0 \text{ for } \alpha_i \text{ linearly independent}
\]

**Lemma 5.32**

Let \( \mathbf{x} = \sum \mathbf{x}_i \alpha_i \in \mathbf{L} \), \( \mathbf{x}_j \in \mathbf{L} \) (any element of \( \mathbf{L} \) can be written like this).

The \( \mathbf{x} \in [I:I] \) iff \((\mathbf{x}_i, \mathbf{x}) : (A_k \alpha_i, A^{-1}) \in \mathbb{Z}^n \forall k \).

**Proof:** By definition, \( \mathbf{x} \in [I:I] \) iff \( \mathbf{I} \subseteq \mathbf{I} \).

\[
(\Rightarrow) \quad x \gamma_k \alpha_i \subseteq \mathbf{I} \forall k
\]

Now, \[
\gamma_k \mathbf{x} = \sum \mathbf{x}_i \gamma_k \alpha_i = \sum \mathbf{x}_i \left( \sum (A_k)_{ij} \alpha_j \right)
\]

\[
= \sum_{j} \alpha_j \left( \sum_{i} \mathbf{x}_i (A_k)_{ij} \right)
\]
\[ \sum_{\ell} \left( \sum_{i} (A^{-1})_i \right) \sum_{i} x_i (A_{\ell}^{-1})_i \]

\[ = \sum_{\ell} \sum_{i} x_i \sum_{\ell} (A_{\ell}^{-1})_i = \sum_{\ell} \sum_{i} x_i (A_{\ell}^{-1})_i \]

This is a linear combination of the \( x_i \) and these form a \( \mathbb{Z} \)-basis of \( I \), so \( \forall \ell \sum_{i} x_i (A_{\ell}^{-1})_i \in \mathbb{Z} \)

\[ \iff (x_1, \ldots, x_n) \cdot (A_{\ell}^{-1}) \in \mathbb{Z}^n \]

\[ \forall \ell, x \in \mathbb{Z} \iff (x_1, \ldots, x_n) \cdot (A_{\ell}^{-1}) \in \mathbb{Z}^n \forall k. \]

**Note:** \([I/I] \equiv C \implies \sum (A_{\ell}^{-1})_i \in \mathbb{Z} \forall i \implies (A_{\ell}^{-1}) \in \text{Mat}_{n \times n}(\mathbb{Z}).

**Step 2:** Set

\[ B := \begin{pmatrix} (A_{\ell}^{-1})_i \\ \vdots \\ (A_{\ell}^{-1})_n \end{pmatrix} \in \text{Mat}_{n \times n}(\mathbb{Z}) \]

For \( x \in \mathbb{Z} \) expressed in the \( x_i \)'s we thus have

\[ x \in [I/I] \iff Bx^t \in \mathbb{Z}^n \]

**Note:** That for any \( U \in GL_{n\times n}(\mathbb{Z}) \) we have

\[ Bx^t \in \mathbb{Z}^n \iff UBx^t \in \mathbb{Z}^n \]

**Step 3:** Let \( \widetilde{B} \) be the HNF of \( B \), \( \widetilde{B} = UB \). Since \( A_{\ell}^{-1} \) has full rank (as above), \( B \) has full rank as well. Hence the sub-matrix \( C \) of non-zero rows of \( \widetilde{B} \) is of size \( n \times n \) and is invertible. Now,

\[ x \in [I/I] \iff Cx^t \in \mathbb{Z}^n \]

**Note:** That \( Cx^t = y^t \in \mathbb{Z}^n \iff x = C^{-1}y \), hence all \( x \) are integral linear combinations of the rows of \( (C^{-1})^t \in \text{Mat}_{n \times n}(\mathbb{Z}). \)
Step 5: Let
\[ \beta_i := \sum_j (C_j)^i \xi_j \]
Then \( \beta_1, \ldots, \beta_n \) is a basis of \( [I/I'] \).

5.10 Round 2 made constructive

Starting with a known order \( G \) (i.e., basis and multiplication known e.g., equation order), we now have a constructive algorithm for finding a basis of the maximal order \( G_2 \).

Step 1: Compute \( d_6 = d(\xi_1, \ldots, \xi_n) \).

Step 2: Determine the primes \( p \) with \( p^2 \mid d_6 \).

Step 3: For each such \( p \) compute the \( p \)-maximal orders \( G_p \) as follows

1. Initialize \( G' := G \).
2. Compute a basis of \( \text{rad} G' \) in terms of the basis of \( G \) using § 5.6.
3. Compute a basis of \( \text{mul} G' = [\text{rad} G'/\text{rad} G'] \) in terms of the basis of \( G \) using § 5.7.
4. Using the HNF check whether \( \text{mul} G' = G' \).
   - If equal, then \( G_p = \text{mul} G' \). (Theorem 5.27)
   - Otherwise, set \( G' := \text{mul} G' \) and repeat from 3.1.

Step 4: Let \( A \) be the matrix with rows the bases of the \( G_p \) for \( p^2 \mid d_6 \). Compute the HNF of \( A \). The non-zero rows form a basis of \( G_2 \).

Remark 5.34
Complete example in the exercises.

Remark 5.35
The bottleneck in the algorithm is actually Step 2!

Remark 5.36
In Step 3 one can compute the HNF mod \( p \). This avoids large numbers.
Remark 5.37
There is a simpler criterion to decide whether an order is maximal without having to compute the $p$-multiplier: the Dedekind criterion (proof is elementary but takes a bit, thus skipped here).

6. Geometry of numbers (Minkowski theory)
Recall from the first lecture that we viewed $\mathbb{Z}[i] = \mathbb{Z} + ii \mathbb{C} \cong \mathbb{R}^2$
The basis vectors 1 and i define a segment of $\mathbb{R}^2$ with positive volume:

$$\text{Vol} = 1$$

We can embed any number field $L$ into $\mathbb{C}$, but if $\dim L > 2$, then $G_L \subset \mathbb{C}$ is degenerate with zero volume.
Minkowski's theory considers $L$ in a larger space where $G_L$ has positive volume.
This is also called "geometry of numbers." The volume is related to the discriminant.

Remark 6.1
The ramification of the morphism $\text{Spec } G_L \to \text{Spec } \mathbb{Z}$ is another "geometry of numbers."

6.1 Lattices
Let $V$ be an $n$-dimensional $\mathbb{R}$-vector space.

Def 6.2
A lattice in $V$ is a $\mathbb{Z}$-submodule $\Lambda$ of $V$ that has a generating set of $n$ $\mathbb{R}$-linearly independent vectors.

Remark 6.3
A generating set as in the definition is clearly a $\mathbb{Z}$-basis of $\Lambda$
$\Rightarrow \Lambda$ is a free $\mathbb{Z}$-module, $\dim \Lambda = n = \dim V$.
Moreover, any $\mathbb{Z}$-basis of $\Lambda$ is linearly independent over $\mathbb{R}$.
**Def 6.4**
Let \( \Lambda \) be a lattice with basis \( v_0, v_n \). Then
\[
\phi := \{ x_0 v_0 + \ldots + x_n v_n \mid 0 \leq x_i \leq 1 \ \text{for} \ \forall i \} \subset V
\]
is called the fundamental region of \( \Lambda \) (wrt the basis).

**Ex 6.5**
\( V = \mathbb{R}^2 \)
\( v_1 = (1, 0), v_2 = (0, 1) \) \( \sim \) 2-dim lattice \( \Lambda \)

\( b) \ V = \mathbb{R}^2 \) \( v_1 = (1, 1), v_2 = (-\frac{1}{2}, \frac{\sqrt{3}}{2}) \) \( \sim \) 2-dim lattice \( \Lambda \)

\( c) \ V = \mathbb{R}^2 \) \( v_1 = (1, 0), v_2 = (\pi, 0) \)

Generate a free \( \mathbb{Z} \)-submodule of \( \mathbb{R}^2 \) of dim 2 but this is not a lattice in \( \mathbb{R}^2 \) since \( v_1, v_2 \) are linearly dependent over \( \mathbb{R} \).

**Remark 6.6**
The translates \( x + \phi, x \in \Lambda \) cover all of \( V \).
6.2 Lattices in Euclidean space

Fix a scalar product $\langle \cdot, \cdot \rangle$ on $V$.

**Def 6.7**

Two lattices $\Lambda$ and $\Lambda'$ in $V$ are called isomorphic if there is an orthogonal linear transformation of $V$ mapping $\Lambda$ to $\Lambda'$.

**Remark 6.8**

A lattice isomorphism is clearly an isomorphism of $\mathbb{Z}$-modules.

We can encode lattices as matrices in two ways (see Exercise 6.1).

I. Let $\Lambda$ be a lattice.

Let $v_1, \ldots, v_n$ be a basis of $\Lambda$ and $e_1, \ldots, e_n$ be an orthonormal basis of $V$.

Then

$$V_i = \sum_j A_{ij} e_j, \quad A \in \text{GL}_n(\mathbb{R}).$$

Can show (Exercise 6.1) that this gives a well-defined map

$$\Lambda \mapsto V_{\Lambda} \in \text{GL}_n(\mathbb{R})$$

Conversely, let $A \in \text{GL}_n(\mathbb{R})$.

Let $e_1, \ldots, e_n$ be an orthonormal basis of $V$ and set

$$V_i = \sum_j A_{ij} e_j.$$

Then $\Lambda = \mathbb{Z} \cdot \langle v_1, \ldots, v_n \rangle$ is a lattice.

This gives inverse to (I).

II. Let $\Lambda$ be a lattice again.

Let $v_1, \ldots, v_n$ be a basis of $\Lambda$. The Gram matrix with the basis is

$$G_{\Lambda} (v_1, \ldots, v_n) := (\langle v_i, v_j \rangle)_{ij} \in \text{Mat}_n(\mathbb{R}).$$
Since \(<\cdot,\cdot>\) is a scalar product, \(G_{\wedge}(v_1, v_n)\) is symmetric and positive definite.

Can show (Exercise 6.1) that this gives a well-defined map

\[(\star) \quad \text{Lattice} / \sim \rightarrow \{\text{symm. pos. def } Q \in \text{Mat}_n(\mathbb{R})\} / \sim\]

where \(Q = Q^\top\) iff \(Q = PQP^\top\) for some \(P \in \text{GL}_n(\mathbb{R})\).

Conversely, let \(Q \in \text{Mat}_n(\mathbb{R})\) be symmetric and positive definite. We will show in §6.3 that there is a (lower triangular) matrix \(A \in \text{Mat}_n(\mathbb{R})\) such that \(Q = AA^\top\) (Cholesky decomposition).

Let \(e_1, \ldots, e_n\) be an orthonormal basis of \(V\).

Let \(v_i = \sum A_{ij}e_j\). Then

\[
\langle v_i, v_j \rangle = \langle \sum A_{ik}e_k, \sum A_{jl}e_l \rangle = \sum A_{ik}A_{jl} \langle e_k, e_l \rangle = \sum A_{ik}A_{jl} (A^AT)_{ij} = Q_{ij}.
\]

\(\therefore\) setting \(\Lambda := \sum \langle v_i, v_j \rangle e_i e_j \in \mathbb{R}^n\), we have \(G_{\wedge}(v_1, v_n) = \Lambda\).

\(\sim\) This gives an inverse to \((\star)\).