Lecture 11 (2.12.)

5.9 Computing the p-multiplier

Let $\mathcal{O}$ be an order with basis $\alpha_1, \ldots, \alpha_n$ and let $I \subseteq \mathcal{O}$ be a non-zero ideal with basis $\gamma_1, \ldots, \gamma_n$

Step 1: Express each γ_i in the α_j's and write this as rows into the matrix $A \in \mathrm{Mat}_{n\times n}(\mathbb{Z})$, i.e.

$$\gamma_i = \sum_j A_{ij}\alpha_j \Rightarrow \alpha_i = \sum_j \underbrace{(A^{-1})_{ij}}_{\in \mathrm{Mat}_{n\times n}(\mathbb{Q})!}\gamma_j$$

Step 2: For each k express the products $\gamma_k\alpha_i$ in the α_j's and write this as rows into the matrix $A_{\gamma_k} \in \mathrm{Mat}_{n\times n}(\mathbb{Z})$, i.e.

$$\gamma_k\alpha_i = \sum_j (A_{\gamma_k})_{ij}\alpha_j$$

The rows of A_{γ_k} are linearly independent over $\mathbb{Z}$:

$$\sum_i c_i(\gamma_k\alpha_i) = 0 \Rightarrow \gamma_k\Big(\sum_i c_i\alpha_i\Big) = 0$$

$\Rightarrow \sum_i c_i\alpha_i = 0$ since $\gamma_k \neq 0$ and we are in an integral domain

$\Rightarrow c_i = 0 \ \forall i$ since α_i linearly independent

Lemma 5.32

Let $x = \sum x_i\alpha_i \in L$, $x_i \in \mathbb{Q}$ (any element of L can be written like this)

The $x \in [I/I]$ iff $(x_1, \ldots, x_n)\cdot(A_{\gamma_k}\cdot A^{-1}) \in \mathbb{Z}^n \ \forall k$.

Proof: By definition, $x \in [I/I]$ iff $xI \subseteq I$.

$\Leftrightarrow x\gamma_k \subseteq I \ \forall k$

Now, $\gamma_k \cdot x = \sum_i \gamma_k x_i\alpha_i = \sum_i x_i\Big(\sum_j (A_{\gamma_k})_{ij}\alpha_j\Big)$

$$= \sum_j \alpha_j\Big(\sum_i x_i(A_{\gamma_k})_{ij}\Big)$$

$$= \sum_j \left(\sum_l (A^{-1})_{jl} \gamma_l \right) \sum_i x_i (A\gamma_k)_{ij}$$

$$= \sum_l \gamma_l \sum_i x_i \sum_j (A\gamma_k)_{ij} (A^{-1})_{jl} = \sum_l \gamma_l \sum_i x_i (A_{\gamma_k} A^{-1})_{il}$$

This is a linear combination of the γ_l, and these form a $\mathbb{Z}$-basis of I,

so $\gamma_k x \in I$ iff $\sum_i x_i (A_{\gamma_k} A^{-1})_{il} \in \mathbb{Z} \ \forall l$

$$\Leftrightarrow (x_1, \ldots, x_n) \cdot (A_{\gamma_k} A^{-1}) \in \mathbb{Z}^n$$

So, $xI \subseteq I$ iff $(x_1, \ldots, x_n) \cdot (A_{\gamma_k} \cdot A^{-1}) \in \mathbb{Z}^n \ \forall k$. $\square$

<u>Note</u>: $[I/I] \supseteq G \Rightarrow e_i (A_{\gamma_k} \cdot A^{-1}) \in \mathbb{Z}^n \ \forall i \Rightarrow (A_{\gamma_k} \cdot A^{-1}) \in Mat_{n \times n}(\mathbb{Z})$.

<u>Step 3</u>: Set

$$B := \begin{pmatrix} (A_{\gamma_1} A^{-1})^t \\ \vdots \\ (A_{\gamma_n} A^{-1})^t \end{pmatrix} \in Mat_{n^2 \times n}(\mathbb{Z})$$

For $x \in L$ expressed in the α_j's we thus have

$$x \in [I/I] \text{ iff } Bx^t \in \mathbb{Z}^{n^2}$$

Note that for any $U \in Gl_{n^2}(\mathbb{Z})$ we have

$$Bx^t \in \mathbb{Z}^{n^2} \text{ iff } UBx^t \in \mathbb{Z}^{n^2}$$

<u>Step 4</u>: Let $\tilde{B}$ be the HNF of B, $\tilde{B} = UB$. Since A_{γ_k} has full rank (see above), B has full rank as well. Hence the submatrix C of non-zero rows of $\tilde{B}$ is of size $n \times n$ and is invertible. Now,

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

Note that $Cx^t = y^t \in \mathbb{Z}^n$ iff $x^t = C^{-1} y^t$, hence all such x are integral linear combinations of the rows of $(C^{-1})^t \in Mat_{n \times n}(\mathbb{Q})$.

Step 5: Let

$$\beta_i := \sum_j (C^{-1})^t_{ij} \alpha_j$$

Then

$\beta_1, \dots, \beta_n$ is a basis of $[I/I]$.

5.10 Round-2 made constructive

Starting with a known order $\mathcal{O}$ (i.e. basis and multiplication known e.g. equation order), we now have a constructive algorithm for finding a basis of the maximal order $\mathcal{O}_L$.

Step 1: Compute $d_{\mathcal{O}} = d(\alpha_1, \dots, \alpha_n)$

Step 2: Determine the primes p with $p^2 \mid d_{\mathcal{O}}$.

Step 3: For each such p compute the p-maximal overorder $\mathcal{O}_p$ as follows

3.0 Initialize $\mathcal{O}' := \mathcal{O}$

3.1 Compute a basis of $\mathrm{rad}_p \mathcal{O}'$ in terms of the basis of $\mathcal{O}$ using § 5.6

3.2. Compute a basis of $\mathrm{mul}_p \mathcal{O}' = [\mathrm{rad}_p \mathcal{O}' / \mathrm{rad}_p \mathcal{O}']$ in terms of the basis of $\mathcal{O}$ using § 5.7

3.3. Using the HNF check whether $\mathrm{mul}_p \mathcal{O}' = \mathcal{O}'$.
If equal, then $\mathcal{O}_p = \mathrm{mul}_p \mathcal{O}'$. (Theorem 5.27)
otherwise, set $\mathcal{O}' := \mathrm{mul}_p \mathcal{O}'$ and repeat from 3.1.

Step 4: Let A be the matrix with rows the bases of the $\mathcal{O}_p$ for $p^2 \mid d_{\mathcal{O}}$.
Compute the HNF of A. The non-zero rows form a basis of $\mathcal{O}_L$.

Remark 5.34
Complete example in the exercises.

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

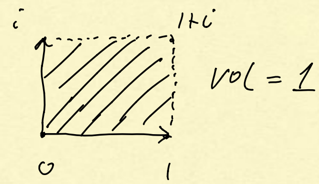
Remark 5.36
In Step 3 one can compute the HNF mod p. This avoids large numbers.

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 $\mathbb{Z}[i] = \mathbb{Z} + i\mathbb{Z} \subset \mathbb{C} \simeq \mathbb{R}^2$
The basis vectors 1 and i define a segment of $\mathbb{R}^2$ with positive volume: ↑ as $\mathbb{R}$-vector spaces



We can embed any number field L into $\mathbb{C}$, but if $\dim_{\mathbb{Q}} L > 2$, then $\mathcal{O}_L \subset \mathbb{C}$ is degenerate with zero volume.
Minkowski theory considers L in a larger space where $\mathcal{O}_L$ 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 $\operatorname{Spec} \mathcal{O}_L \to \operatorname{Spec} \mathbb{Z}$ 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 Λ 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 Λ
$\Rightarrow \Lambda$ is a free $\mathbb{Z}$-module, $\dim \Lambda = n = \dim V$.

Moreover, any $\mathbb{Z}$-basis of Λ is linearly independent over $\mathbb{R}$.

Def 6.4

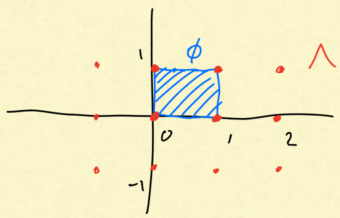
Let Λ be a lattice with basis $v_1, \dots, v_n$. Then

$$\phi := \{ x_1 v_1 + \dots + x_n v_n \mid 0 \le x_i \le 1 \ \forall i \} \subset V$$

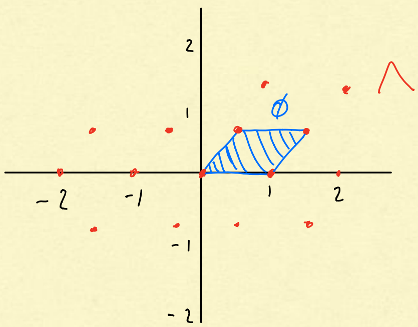
is called <u>fundamental region</u> of Λ (wrt the basis).

Ex 6.5

a) $V = \mathbb{R}^2$, $v_1 = (1 \ \ 0)$, $v_2 = (0 \ \ 1)$ $\rightsquigarrow$ 2-dim'l lattice Λ



b) $V = \mathbb{R}^2$, $v_1 = (1 \ \ 0)$, $v_2 = (-1/2 \ \ \sqrt{3}/2)$ $\rightsquigarrow$ 2-dim'l lattice Λ



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

Generates a free $\mathbb{Z}$-submodule of $\mathbb{R}^2$ of dim 2 but this is is <u>not</u> 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 Λ and Λ' in V are called isomorphic if there is an orthogonal linear transformation of V mapping Λ to Λ'.

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 Λ be a lattice.

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

Then

$$v_i = \sum_j A_{ij} e_j \ , \quad A \in GL_n(\mathbb{R}).$$

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

$$(*) \quad \text{Lattices}/_{\cong} \longrightarrow GL_n(\mathbb{R})/_{\sim}$$

where $A' \sim A$ iff $A' = PAT$, $P \in GL_n(\mathbb{Z})$, $T \in O_n(\mathbb{R})$

Conversely, let $A \in GL_n(\mathbb{R})$.

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

$$v_i := \sum_j A_{ij} e_j.$$

Then $\Lambda := \mathbb{Z}\cdot\{v_1,\dots,v_n\}$ is a lattices.

This gives inverse to $(*)$.

II Let Λ be a lattice again.

Let $v_1,\dots,v_n$ be a basis of Λ. The Gram matrix wrt the basis is

$$Gr_\Lambda(v_1,\dots,v_m) := (\langle v_i, v_j\rangle)_{ij} \in Mat_n(\mathbb{R})$$

Since $\langle\cdot,\cdot\rangle$ is a scalar product, $Gr_\Lambda(v_1,..,v_n)$ is symmetric and positive definite.

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

$$(**) \quad \text{Lattices}/\sim \longrightarrow \{\text{symm. pos. def } Q \in Mat_n(\mathbb{R})\}/\sim$$

where $Q \sim Q'$ iff $Q' = PQP'$ for some $P \in GL_n(\mathbb{Z})$

Conversely, let $Q \in Mat_n(\mathbb{R})$ be symmetric and positive definite.
We will show in §6.3 that there is a (lower triangular) matrix $A \in Mat_n(\mathbb{R})$ such that $Q = AA^t$ (<u>Cholesky decomposition</u>).

Let $e_1,\dots,e_n$ be an orthonormal basis of V.

Let $v_i = \sum_j A_{ij} e_j$. Then

$$\langle v_i, v_j\rangle = \left\langle \sum_k A_{ik} e_k, \sum_\ell A_{j\ell} e_\ell \right\rangle = \sum_{k,\ell} A_{ik} A_{j\ell} \langle e_k, e_\ell\rangle$$

$$= \sum_k A_{ik} A_{jk} = (AA^t)_{ij} = Q_{ij}.$$

$\Rightarrow$ Setting $\Lambda := \mathbb{Z}\cdot\{v_1,..,v_n\} \subset \mathbb{R}^n$, we have $Gr_\Lambda(v_1,..,v_n) = Q$.

$\rightsquigarrow$ This gives an inverse to $(**)$.