Lecture 12 (4.12.)

Def 6.9

The *discriminant* of a lattice Λ is

$$d(\Lambda) := \sqrt{\det Gr_\Lambda(v_1, \dots, v_n)}$$

This is independent of the choice of basis since base change matrix has determinant ± 1.

If A is the matrix of Λ wrt some bases, then

$vol(\phi) = |\det A|$ (this is basically the definition of volume)

Moreover, $Gr_\Lambda = A \cdot A^t$

$$\Rightarrow \underline{d(\Lambda) = \sqrt{\det(A)^2} = |\det(A)| = vol(\phi).}$$

6.3. Quadratic supplement and Cholesky decomposition

Remember the following from school:

$$x^2 + bx + c = (x + \tfrac{1}{2}b)^2 + \left(c - \frac{b^2}{4}\right) \quad \text{"completing the square"}$$

There is a matrix version of this.

Lemma 6.10

Let $Q \in Mat_n(\mathbb{R})$ be symmetric and positive definite. Then there is an upper triangular $\tilde{Q} \in Mat_n(\mathbb{R})$ such that

$$xQx^t = \sum_{i=1}^{n} \tilde{Q}_{ii} \left(x_i + \sum_{j=i+1}^{n} \tilde{Q}_{ij} x_j \right)^2 \quad \forall x \in \mathbb{R}^n$$

$\tilde{Q}$ is called the *quadratic supplement* of Q.

Proof:

$$xQx^t = \sum_{i,j} x_i x_j Q_{ij}$$

Focussing on x_1:

$$xQx^t = x_1^2 Q_{11} + x_1 \sum_{j>1} x_j (\overbrace{Q_{1j} + Q_{j1}}^{=}) + \sum_{i,j>1} x_i x_j Q_{ij}$$

Now, complete the square

$$xQx^t = Q_{11}\Big(x_1^2 + 2x_1 \sum_{j>1} \frac{Q_{1j}}{Q_{11}} x_j\Big) + \sum_{i,j>1} x_i x_j Q_{ij}$$ ($Q_{11} \neq 0$ since Q pos. def.)

$$= Q_{11}\Big(x_1^2 + 2x_1 \sum_{j>1} \frac{Q_{1j}}{Q_{11}} x_j + \Big(\sum_{j>1} \frac{Q_{1j}}{Q_{11}} x_j\Big)^2\Big)$$

$$- Q_{11}\Big(\sum_{j>1} \frac{Q_{1j}}{Q_{11}} x_j\Big)^2 + \sum_{i,j>1} x_i x_j Q_{ij}$$

$$= Q_{11}\Big(x_1 + \sum_{j>1} \frac{Q_{1j}}{Q_{11}} x_j\Big)^2 + \dots$$ $x(Q')x^t$ for a smaller matrix Q'!

$\square$

<u>Remark 6.11</u>
The proof of Lemma yields an algorithm, see Exercise 6.2.

<u>Corollary 6.12</u>
For any symmetric positive definite matrix $Q \in Mat_n(\mathbb{R})$ there is a lower triangular matrix $A \in Mat_n(\mathbb{R})$ with $Q = AA^t$ (<u>Cholesky decomposition</u>).

<u>Proof:</u>
Let $\tilde{Q}$ be the quadratic supplement of Q.
Set $A_{ii} := \sqrt{\tilde{Q}_{ii}}$ and $A_{ij} := \sqrt{\tilde{Q}_{ii}}\,\tilde{Q}_{ji}$ $i \neq j$.
Now simply compute (Exercise 6.3.)

$\square$

6.4 Minkowski theory

Let L be a number field, $n = \dim_{\mathbb{Q}} L$. Recall from Lemma 2.21 that there are precisely n distinct $\mathbb{Q}$-morphisms

$$L \longrightarrow \mathbb{C} \quad \text{(all injective of course).}$$

Some of these land in $\mathbb{R} \subseteq \mathbb{C}$ (real embeddings). We will always stick to the following convention: $\sigma_1, \dots, \sigma_r$ denote the real embeddings; the remaining embeddings come in pairs $\sigma, \overline{\sigma}$ and are denoted

$$\sigma_{r+1}, \sigma_{r+2}, \dots, \sigma_{r+s}, \sigma_{r+s+1} = \overline{\sigma_{r+1}}, \dots, \sigma_{r+2s} = \overline{\sigma_{r+s}}$$

Let $L_{\mathbb{C}} := \mathbb{C}^{r+2s}$. We then have an embedding

$$j_{L,\mathbb{C}} : L \longrightarrow \mathbb{C}^{r+2s} \quad \text{(as } \mathbb{Q}\text{-vector spaces)}$$

mapping α to $(\sigma_i(\alpha))_{i=1}^{n}$.

We have

$$\langle j_{L,\mathbb{C}}(\alpha), j_{L,\mathbb{C}}(\alpha) \rangle = \sum_{i=1}^{n} \sigma_i(\alpha)\overline{\sigma_i(\alpha)} = \sum_{i=1}^{r} \sigma_i(\alpha)^2 + 2\sum_{i=r+1}^{r+s} \sigma_i(\alpha)\overline{\sigma_i(\alpha)}$$

$$= \sum_{i=1}^{r} \sigma_i(\alpha)^2 + 2\sum_{i=r+1}^{r+s} \left[(\mathrm{Re}\,\sigma_i(\alpha))^2 + (\mathrm{Im}\,\sigma_i(\alpha))^2 \right]$$

Let's get real! Let

$$L_{\mathbb{R}} := \mathbb{R}^{r+2s},$$ call this the Minkowski space associated to L.

Consider the map

$$j_L := j_{L,\mathbb{R}} : L \longrightarrow L_{\mathbb{R}}$$

mapping $\alpha \in L$ to

$$(\sigma_1(\alpha), \dots, \sigma_r(\alpha), \sqrt{2}\,\mathrm{Re}\,\sigma_{r+1}(\alpha), \sqrt{2}\,\mathrm{Im}\,\sigma_{r+1}(\alpha), \dots, \sqrt{2}\,\mathrm{Re}\,\sigma_{r+s}(\alpha), \sqrt{2}\,\mathrm{Im}\,\sigma_{r+s}(\alpha)) \in L_{\mathbb{R}}$$

This is an injective $\mathbb{Q}$-vector space map, let's call it Minkowski map.

With respect to the standard scalar product we have

$$\langle j_{L,\mathbb{R}}(\alpha), j_{L,\mathbb{R}}(\alpha)\rangle_{\mathbb{R}^n} = \langle j_{L,\mathbb{C}}(\alpha), j_{L,\mathbb{C}}(\alpha)\rangle_{\mathbb{C}^n}$$

This explains the $\sqrt{2}$ in the definition of j_L.

<u>Def 6.13</u>

For $\alpha \in L$ call $T_2(\alpha) := \langle j_L(\alpha), j_L(\alpha)\rangle$ the <u>T_2-norm</u> of α.
(It's stupid terminology since this is not a norm; would need to take $\sqrt{\cdot}$)

<u>Thm 6.14</u>

Let $\mathcal{O} \subset L$ be an order and let $I \subseteq \mathcal{O}$ be a non-zero ideal.
Then $j_L(I) \subset \mathbb{R}^n$ is a lattice and

$$d(j_L(I)) = [\mathcal{O} : I] \cdot \sqrt{|d_{\mathcal{O}}|}$$

We call $j_L(I)$ the <u>Minkowski lattice</u> associated to I.

<u>Proof:</u>

Recall from Lemma 5.23 that $I, \mathcal{O}$ are free $\mathbb{Z}$-modules of dimension n.
Let $\alpha_1, \dots, \alpha_n$ be a basis of I. Since j_L is a linear map, $j_L(I)$ is generated as a $\mathbb{Z}$-module by $j_L(\alpha_1), \dots, j_L(\alpha_n)$. Let $A := (\sigma_i(\alpha_j))_{ij}$. Then
By Lemma 2.41, Lemma 2.42, §2.7 we have

$$\det(A)^2 = d_L(\alpha_1, \dots, \alpha_n) = [\mathcal{O} : I]^2 \cdot d_{\mathcal{O}} \neq 0$$

Moreover,

$$\langle j_L(\alpha_i), j_L(\alpha_j)\rangle = \langle j_{L,\mathbb{C}}(\alpha_i), j_{L,\mathbb{C}}(\alpha_j)\rangle = \sum_k \sigma_k(\alpha_i)\overline{\sigma_k(\alpha_j)} = (A^t \cdot \overline{A})_{ij}$$

$$\Rightarrow \det\big((\langle j_L(\alpha_i), j_L(\alpha_j)\rangle)\big) = \det(A)^2 \neq 0$$

$\Rightarrow j_L(I)$ is a lattice.

Also,

$$d(j_L(I)) = \sqrt{(\langle j_L(\alpha_i), j_L(\alpha_j)\rangle)} = \sqrt{\det(A)^2}$$

$$= [G:I]\cdot\sqrt{|d_G|}. \qquad \square$$

<u>Corollary 6.15</u>

$j_L(G_L) \subset \mathbb{R}^n$ is a lattice with $d(j_L(G_L)) = \sqrt{|d_L|}$. $\square$

<u>Lemma 6.16</u>

For $\alpha \in G$ we have

$$|N_{L|\mathbb{Q}}(\alpha)|^{2/n} \leq \frac{1}{n}\langle j(\alpha), j(\alpha)\rangle$$

and

$$n \leq \langle j(\alpha), j(\alpha)\rangle \quad (\alpha \neq 0)$$

<u>Proof</u>:

We have

$$|N_{L|\mathbb{Q}}(\alpha)|^2 = \prod_{i=1}^{n} |\sigma_i(\alpha)|^2$$

$|N_{L|\mathbb{Q}}(\alpha)|^{2/n}$ is the geometric mean of the factors.

This is $\leq$ the arithmetic mean of the factors, which is

$$\frac{1}{n}\left(\sum_{i=1}^{n} |\sigma_i(\alpha)|^2\right) = \frac{1}{n}\left(\sum_{i=1}^{r} \sigma_i(\alpha)^2 + \sum_{i=r+1}^{n}(\operatorname{Re}\sigma_i(\alpha)^2 + \operatorname{Im}\sigma_i(\alpha)^2)\right)$$

$$= \frac{1}{n}\left(\sum_{i=1}^{r}\sigma_i(\alpha)^2 + \sum_{i=r+1}^{r+s} 2(\operatorname{Re}\sigma_i(\alpha)^2 + \operatorname{Im}\sigma_i(\alpha)^2)\right)$$

$$= \frac{1}{n}\langle j(\alpha), j(\alpha)\rangle. \qquad \square$$