Algebraic Number Theory

Lecture 9, 3rd December 2021

Last lecture: $\mathcal{O}$: Dedekind domain, $K = \mathrm{Frac}(\mathcal{O})$

fractional ideal: fin. gen. $\mathcal{O}$-submodule $\mathfrak{a} \neq 0$ of K.

ideal group: J_K = set of all fract. ideals

$\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subseteq \mathcal{O}\}$.

(ideal) class group: $Cl_K = J_K / P_K$ ← subgroup of principal ideals $(a) = a\mathcal{O}$ $a \in K^\times$

$(V, \langle , \rangle)$ n-dim eucl. vector space.

lattice: $\Gamma \subset V$ discrete subgroup $\Gamma = \mathbb{Z}\alpha_1 + \dots + \mathbb{Z}\alpha_m$

Γ complete $:\Longleftrightarrow m = n$

lin. indep. $\in V$

fundamental mesh: $\Phi = \{x_1 v_1 + \dots + x_m v_m \mid 0 \leq x_i < 1,\ x_i \in \mathbb{R}\}$

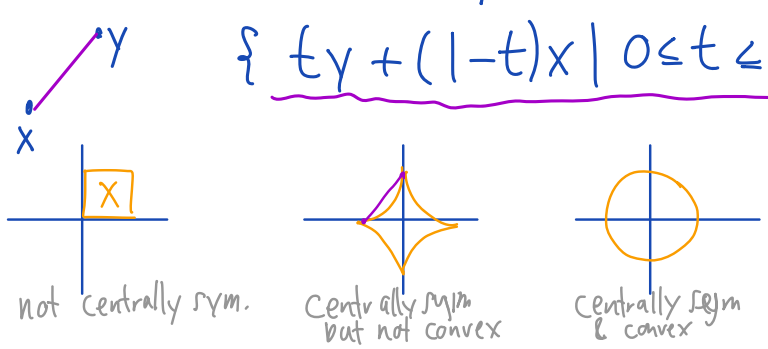
$\mathrm{vol}(\Gamma) = |\det(\langle v_i, v_j \rangle)|^{\frac{1}{2}}$

Definition 5.6 Let $X \subset V$. X is called

i) <u>centrally symmetric</u> if $x \in X \Rightarrow -x \in X$.

ii) <u>convex</u> if for all $x, y \in X$

$\{ty + (1-t)x \mid 0 \leq t \leq 1\} \subset X$.

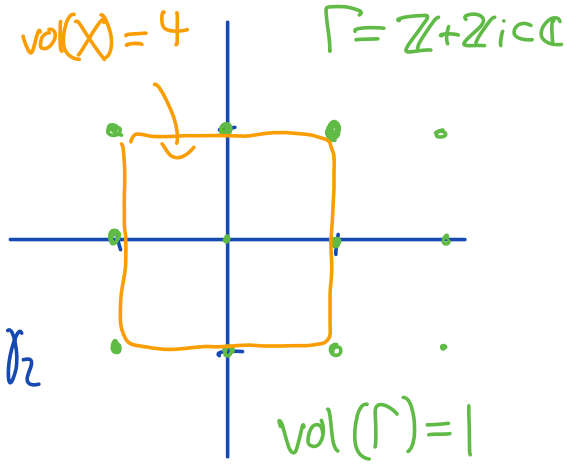


We now state Minkowski's lattice point theorem:

Theorem 5.7 Let Γ be a complete lattice in the euclidean vector space V and X a centrally symmetric, convex subset of V. Suppose that

$$\mathrm{vol}(X) > 2^n \mathrm{vol}(\Gamma). \qquad (*)$$

Then X contains at least one nonzero lattice point $\gamma \in \Gamma$.



Proof: We will show that for $\gamma_1, \gamma_2 \in \Gamma$ with $\gamma_1 \neq \gamma_2$ $(*)$ implies

$$\left(\tfrac{1}{2}X + \gamma_1\right) \cap \left(\tfrac{1}{2}X + \gamma_2\right) \neq \emptyset.$$

Then there exist $x_1, x_2 \in X$ with

$$\tfrac{1}{2}x_1 + \gamma_1 = \tfrac{1}{2}x_2 + \gamma_2,$$

i.e. $\gamma = \underset{\neq 0}{\gamma_1 - \gamma_2} = \underbrace{\tfrac{1}{2}x_2 - \tfrac{1}{2}x_1}_{\text{point on line between } x_2, -x_1 \in X} \in X.$

Assuming that $\frac{1}{2}X+\gamma$ are pairwise disjoint gives

$$\mathrm{vol}(\Gamma)=\mathrm{vol}(\Phi) \geq \sum_{\gamma\in\Gamma} \mathrm{vol}\left(\Phi \cap \left(\tfrac{1}{2}X+\gamma\right)\right) = (*)$$

(since $\Phi \cap \left(\frac{1}{2}X+\gamma\right)$ are also pairwise disjoint)

$$(*) = \sum_{\gamma\in\Gamma} \mathrm{vol}\Big(\underbrace{(\Phi-\gamma)}_{\substack{\text{translation}\\ \text{by } -\gamma}} \cap \tfrac{1}{2}X\Big).$$

Since $\Phi-\gamma$ cover V (Γ is complete) we get

$$\mathrm{vol}(\Phi) \geq \mathrm{vol}\left(\tfrac{1}{2}X\right) = \frac{1}{2^n}\,\mathrm{vol}(X)$$

which is a contradiction, i.e the $\frac{1}{2}X+\gamma$ are not pairwise disjoint. $\square$

§ 6 Minkowski Theory

From now on K is again a number field.

<u>Recall:</u> Let $[K:\mathbb{Q}] = n$ and θ a primitive element, i.e. $K = \mathbb{Q}[\theta]$ and the minimal polynomial of θ is

$$p_\theta(X) = \prod_{i=1}^{n} (X - \theta_i) \in \mathbb{Q}[X], \quad \theta_i \in \overline{K} \subset \mathbb{C}.$$

Any $a \in K$ can be written as

$$a = a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1}.$$

Each θ_i for $i = 1, \ldots, n$ gives an embedding

$$\begin{aligned} \tau_i : K &\longrightarrow \mathbb{C} \\ \sum_{j=0}^{n-1} a_j \theta^j &\longmapsto \sum_{j=0}^{n-1} a_j \theta_i^j . \end{aligned}$$

Some of the θ_i are real and $\tau_i(K) \subset \mathbb{R}$.
These embeddings τ_i are called <u>real embeddings</u>.

The other embeddings come in pairs of complex conjugates $\theta_i = \overline{\theta_{i'}} \in \mathbb{C} \setminus \mathbb{R}$ with $1 \le i < i' \le n$.

The corresponding embeddings $\tau_i, \tau_{i'}$ are called <u>complex embeddings</u>.

$$n = \underset{\substack{\uparrow \\ \#\text{ real embeddings}}}{r} + 2\underset{\#\text{ pairs of complex embeddings.}}{s}$$

Example: $K = \mathbb{Q}[\underset{\theta}{\underset{\shortparallel}{\sqrt[3]{2}}}]$, $p_\theta(X) = X^3 - 2$ $\quad \theta_2 = -\frac{1}{\sqrt[3]{4}} + \frac{\sqrt{3}}{\sqrt[3]{4}} i$, $\theta_3 = \overline{\theta_2} = -\frac{1}{\sqrt[3]{4}} + \frac{\sqrt{3}}{\sqrt[3]{4}} i$

$$= (X - \underset{\theta_1}{\sqrt[3]{2}})(X - \theta_2)(X - \theta_3)$$

We want to embedd K into some euclidean vector space in order to use the results on lattices.

- First consider all embeddings $\tau_i : K \to \mathbb{C}$ and define

$$j : K \longrightarrow K_{\mathbb{C}} := \prod_{\tau : K \to \mathbb{C}} \mathbb{C}$$
$$a \longmapsto j(a) = (\tau(a))_\tau =: (a_\tau)_\tau$$

$K_{\mathbb{C}}$ can be equipped with the hermitian scalar product

$$\langle x, y \rangle = \sum_{\tau} x_\tau \overline{y_\tau} \quad ,$$

sum over all embeddings

i.e. $\langle \cdot, y \rangle$ is linear, $\overline{\langle x, y \rangle} = \langle y, x \rangle$ and $\langle x, x \rangle > 0$ for $x \neq 0$.

- The complex conjugation $F : z \mapsto \overline{z}$ generates the Galois group $G(\mathbb{C}/\mathbb{R})$, which acts on $\mathbb{C}$ and also on $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ by

$$\tau \longmapsto (\overline{\tau} : K \to \mathbb{C})$$
$$\overline{\tau}(x) := \overline{\tau(x)}$$

This gives an involution $F: K_{\mathbb{C}} \to K_{\mathbb{C}}$ with

$$(F(z))_\tau = \overline{z_{\bar{\tau}}}.$$

In the Example: $K_{\mathbb{C}} = \mathbb{C}^3 \ni z = \begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix}$ ← real emb. ↔ complex emb.

$$F\left(\begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix}\right) = \begin{pmatrix} \overline{z_1} \\ \overline{z_3} \\ \overline{z_2} \end{pmatrix}.$$

The scalar product satisfies

$$\langle F(x), F(y) \rangle = F\langle x, y \rangle.$$

- Define the linear map

$$\mathrm{Tr}: K_{\mathbb{C}} \to \mathbb{C}$$
$$(x_\tau)_\tau \mapsto \sum_\tau x_\tau.$$

We have $F \circ \mathrm{Tr} = \mathrm{Tr} \circ F$ and

$$\mathrm{Tr}_{K/\mathbb{Q}}: K \xrightarrow[j]{} K_{\mathbb{C}} \xrightarrow[\mathrm{Tr}]{} \mathbb{C}$$

gives the trace of L/K. (Proposition 3.6).

Definition 6.1 Let $K_{\mathbb{R}}$ denote the F-invariant subspace of $K_{\mathbb{C}}$, i.e

$$K_{\mathbb{R}} = \{ z \in K_{\mathbb{C}} \mid z_{\bar{\tau}} = \overline{z_\tau} \}.$$

(In the example: $K_{\mathbb{R}} = \left\{ \begin{pmatrix} z_1 \\ z_2 \\ \bar{z}_2 \end{pmatrix} \mid z_1 \in \mathbb{R},\ z_2 \in \mathbb{C} \right\}$)

The restriction of $\langle , \rangle$ on $K_{\mathbb{R}}$ gives a scalar product

$$\langle , \rangle : K_{\mathbb{R}} \times K_{\mathbb{R}} \to \mathbb{R}$$

on the $\mathbb{R}$-vector space $K_{\mathbb{R}}$, since

$$F\langle x, y \rangle = \langle F(x), F(y) \rangle = \underset{\langle y, x \rangle}{\overset{\parallel}{\langle x, y \rangle}} \in \mathbb{R}.$$

The euclidean vector space $(K_{\mathbb{R}}, \langle , \rangle)$ is called <u>Minkowski space</u>.

$\langle , \rangle$ is called the <u>canonical metric</u> and the associated measure (Definition 5.5) is called <u>canonical measure</u>. We denote for $X \subset K_{\mathbb{R}}$ its volume by $\mathrm{vol}(X)$.

Denote the real embeddings of K by $\rho_1, \dots, \rho_r : K \to \mathbb{R}$ and the complex ones by $\sigma_1, \overline{\sigma_1}, \dots, \sigma_s, \overline{\sigma_s} : K \to \mathbb{C}$. Then

$$K_{\mathbb{R}} = \{ (z_\tau) \in K_{\mathbb{C}} \mid z_{\rho_i} \in \mathbb{R},\ z_{\overline{\sigma_j}} = \overline{z_{\sigma_j}} \}$$

$i = 1, \dots, r_1 \quad j = 1, \dots, s$

$$\cong \prod_\tau \mathbb{R} = \mathbb{R}^{r+2s}$$

$$z_\rho \longmapsto z_\rho$$
$$z_\sigma \longmapsto \mathrm{Re}(z_\sigma)$$
$$z_{\overline{\sigma}} \longmapsto \mathrm{Im}(z_\sigma)$$

Notice: this isomorphism transforms the canonical metric into the scalar product

$$(x, y) = \sum_\tau a_\tau x_\tau y_\tau \qquad \text{on } \mathbb{R}^{r+2s}$$

$$a_\tau = \begin{cases} 1 & \tau \text{ real} \\ 2 & \tau \text{ complex} \end{cases}$$

Therefore the canonical measure and the Lebesgue measure differ by a factor of 2^s:

$$\mathrm{vol}(X) = 2^s \underbrace{\mathrm{vol}_{\mathrm{Leb}}}_{\text{volume defined via isom.}}(X).$$

Proposition 6.2 If $\mathfrak{a} \neq 0$ is an ideal of $\mathcal{O}_K$, then $\Gamma = j(\mathfrak{a})$ is a complete lattice in $K_{\mathbb{R}}$. Its fundamental mesh has volume

$$\mathrm{vol}(\Gamma) = \sqrt{|d_K|}\,(\mathcal{O}_K : \mathfrak{a})$$

Proof: Let $\alpha_1, \dots, \alpha_n$ be a $\mathbb{Z}$-basis of $\mathfrak{a}$, then

$$\Gamma = \mathbb{Z}\, j(\alpha_1) + \dots + \mathbb{Z}\, j(\alpha_n).$$

Now for embeddings $\tau_1, \dots, \tau_n : K \to \mathbb{C}$ set $A = (\tau_\ell(\alpha_i))$. Then we have

$$d(\mathfrak{a}) = d(\alpha_1, \dots, \alpha_n) = \det(A)^2 \underset{\text{Prop. 3.19}}{=} (\mathcal{O}_K : \mathfrak{a})^2 \underbrace{d(\mathcal{O}_K)}_{d_K}.$$

Since

$$\left(\langle j(\alpha_i), j(\alpha_k) \rangle \right) = \left(\sum_{\ell=1}^{n} \tau_\ell(\alpha_i) \overline{\tau_\ell}(\alpha_k) \right)$$

$$= A \overline{A}^T$$

we get

$$\mathrm{vol}(\Gamma) := \left| \det(\langle j(\alpha_i), j(\alpha_k) \rangle) \right|^{\frac{1}{2}}$$

$$= |\det(A)| = \sqrt{d_K}\,(\mathcal{O}_K : \mathfrak{a}) \qquad \square$$

Now we can use Minkowski's lattice point theorem to obtain the following:

<u>Theorem 6.3</u> Let $\mathfrak{a} \neq 0$ be an ideal of $\mathcal{O}_K$, and let $c_\tau > 0$ be real numbers for each $\tau \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ such that $c_\tau = c_{\bar{\tau}}$ and

$$(*) \quad \prod_{\tau} c_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\,(\mathcal{O}_K : \mathfrak{a}).$$

Then there exists $a \in \mathfrak{a}$, $a \neq 0$ with

$$|\tau(a)| < c_\tau$$

for all $\tau \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$.

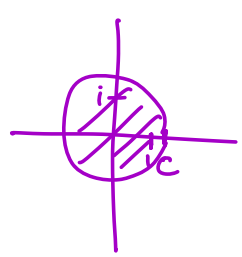
<u>Ex:</u> $K = \mathbb{Q}(i)$ $\quad \tau_1 : a+bi \mapsto a+bi$ $\quad c = c_{\tau_1} = c_{\tau_2} > 0.$

$\tau_2 : a+bi \mapsto a-bi$ $\quad s = 1$

$\mathfrak{a} = \mathcal{O}_K$

$$d_K = \det\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}^2 = (-2i)^2 = -4$$

$$c^2 > \frac{2}{\pi} \cdot 2 \underset{c>0}{\iff} c > \sqrt{\frac{4}{\pi}} \approx 1.12\ldots$$



<u>Proof</u>: The set $X = \{ (z_\tau) \in K_{\mathbb{R}} \mid |z_\tau| < c_\tau \}$ is centrally symmetric and convex.

Consider the isomorphism

$$f : K_{\mathbb{R}} \longrightarrow \prod_\tau \mathbb{R}$$
$$z_\tau \longmapsto x_\tau$$

with $x_\rho = z_\rho$ and $x_\sigma = \mathrm{Re}(z_\sigma)$, $x_{\bar\sigma} = \mathrm{Im}(z_\sigma)$.

Then

$$f(X) = \{ (x_\tau) \in \prod_\tau \mathbb{R} \mid |x_\rho| < c_\rho,\ x_\sigma^2 + x_{\bar\sigma}^2 < c_\sigma^2 \}$$

which gives

$$\underset{\text{canonical vol}}{\mathrm{vol}(X)} = 2^s \, \mathrm{vol}_{\text{Lebesgue}}(f(X))$$

$$= 2^s \underbrace{\prod_\rho (2c_\rho)}_{r} \underbrace{\prod_\sigma (\pi c_\sigma^2)}_{\text{one for each pair } (s)} = 2^{r+s} \pi^s \prod_\tau c_\tau .$$

By $(*)$ and <u>Prop. 6.2</u> we get

$$\mathrm{vol}(X) \overset{(*)}{>} 2^{r+s} \pi^s \left(\frac{2}{\pi}\right)^s \underbrace{\sqrt{|d_K|}\,(\mathcal{O}_K : \mathfrak{a})}_{\mathrm{vol}(\Gamma)}$$

$$= 2^{\overbrace{r+2s}^{n}} \operatorname{vol}(\Gamma).$$

Theorem 5.7 (Minkowski's lattice point thm.) then implies that there exist a nonzero $j(a) \in X$, i.e. $a \neq 0$, $a \in \mathfrak{a}$ with $|\tau(a)| < c_\tau$ for all $\tau \in \operatorname{Hom}_{\mathbb{Q}}(k, \mathbb{C})$.