Algebraic Number Theory

Lecture 8, 26th November 2021

Last lecture

Theorem 4.4 Every ideal $\mathfrak{a} \neq (0), (1)$ of a Dedekind domain $\mathcal{O}$ admits a factorization

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

into nonzero prime ideals $\mathfrak{p}_i$ of $\mathcal{O}$, which is unique up to the order of the factors.

Lemma 4.6 Let $\mathfrak{p} \subset \mathcal{O}$ be a prime ideal and set

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

Then we have $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathfrak{a}$ for any ideal $\mathfrak{a} \neq 0$.

$$\mathfrak{a}\mathfrak{p}^{-1} = \{\textstyle\sum a_i x_i \mid a_i \in \mathfrak{a}, x_i \in \mathfrak{p}^{-1}\}$$

In particular $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} \underset{\mathfrak{p}\text{ maximal.}}{\Longrightarrow} \mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$

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

Definition 4.7 i) A <u>fractional ideal</u> of K is a finitely generated $\mathcal{O}$-submodule $\mathfrak{a} \neq 0$ of K.

ii) The fractional ideals in $\mathcal{O}$ are called <u>integral ideals</u> of K

iii) For $a \in K^\times$ $(a) := a\mathcal{O}$ is a fractional ideal, called <u>fractional principal ideal</u>.

We define products & sums similar to ideals.

Proposition 4.8 A $\mathcal{O}$-submodule $\mathfrak{a} \neq 0$ of K is a fractional ideal if and only if there exists a $c \in \mathcal{O}$, $c \neq 0$ with $c\mathfrak{a} \subset \mathcal{O}$.

Proof: "$\Rightarrow$" Let $\mathfrak{a}$ be generated by $\alpha_1, \dots, \alpha_r$. Then we can choose c to be the product of the denominators of $\alpha_1, \dots, \alpha_r$.

"$\Leftarrow$" If $c\mathfrak{a} \subset \mathcal{O}$, then $c\mathfrak{a}$ is an ideal of $\mathcal{O}$, i.e it is fin. generated

since $\mathcal{O}$ is noetherian. If $\beta_1, \dots, \beta_r$ are the generators of $c\mathfrak{a}$ then $c^{-1}\beta_1, \dots, c^{-1}\beta_r$ generate $\mathfrak{a}$.

Proposition 4.9 The fractional ideals form an abelian group, the <u>ideal group</u> J_K of K. The identity is $(1) = \mathcal{O}$, and the inverse of a fractional ideal $\mathfrak{a}$ is

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

Proof: • Associativity, commutativity and $\mathfrak{a}(1) = \mathfrak{a}$ are clear.

• For prime ideals $\mathfrak{p} \subset \mathcal{O}$ we already saw that $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$.
For an integral ideal $\mathfrak{a} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$ the inverse is given by $\mathfrak{b} = \mathfrak{p}_1^{-1} \cdot \ldots \cdot \mathfrak{p}_r^{-1}$.
Since $\mathfrak{a}\mathfrak{b} = \mathcal{O}$ implies $\mathfrak{b} \subseteq \mathfrak{a}^{-1}$ and

if $x \in \mathfrak{a}^{-1}$ ($x\mathfrak{a} \subseteq \mathcal{O}$) we have

$x \underbrace{\mathfrak{a}\mathfrak{b}}_{\mathcal{O}} \subseteq \mathfrak{b}$, which gives $x \in \mathfrak{b}$.

$\Rightarrow \mathfrak{b} = \mathfrak{a}^{-1}$.

- If $\mathfrak{a}$ is fractional, i.e $c\mathfrak{a} \subseteq \mathcal{O}$ for some $c \in \mathcal{O}$, $c \neq 0$, then

$$(c\mathfrak{a})^{-1} = c^{-1}\mathfrak{a}^{-1}$$

$$\Rightarrow \mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}.$$

<u>Corollary 4.10</u> Every fractional ideal $\mathfrak{a}$ admits a unique representation as a product

$$\mathfrak{a} = \prod_{\substack{\mathfrak{p} \subseteq \mathcal{O} \\ \text{prime ideal}}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})},$$

with $v_{\mathfrak{p}}(\mathfrak{a}) \in \mathbb{Z}$ and $v_{\mathfrak{p}}(\mathfrak{a}) = 0$ for almost all $\mathfrak{p}$.

Proof: For some $c \in \mathcal{O}$, $c \neq 0$ $c\mathfrak{a}$ is an integral ideal, which has a prime decomposition (Thm. 4.4).

But $\mathfrak{a} = (c\mathfrak{a})(c)^{-1}$, i.e any fractional ideal is the quotient of two integral ideals. $\square$

Remark 4.11 Some properties of the exponents v_p:

i) $v_p(\mathfrak{a}\mathfrak{b}) = v_p(\mathfrak{a}) + v_p(\mathfrak{b})$

ii) $\mathfrak{a} \subseteq \mathcal{O} \iff v_p(\mathfrak{a}) \geq 0 \quad \forall p.$

iii) $\mathfrak{a} \subseteq \mathfrak{b} \iff v_p(\mathfrak{a}) \geq v_p(\mathfrak{b}) \quad \forall p$

iv) $v_p(\mathfrak{a} + \mathfrak{b}) = \min(v_p(\mathfrak{a}), v_p(\mathfrak{b}))$

Definition 4.12

i) By P_K we denote the subgroup of J_K generated by all fractional principal ideals $(a) = a\mathcal{O}$ with $a \in K^\times$.

ii) The quotient group

$$Cl_K = J_K / P_K$$

is called the <u>(ideal) class group</u> of K.

Remark 4.13

i) A Dedekind domain $\mathcal{O}$ is a PID if Cl_K is trivial.

ii) A Dedekind domain is a UFD iff it is a PID.

iii) We have the exact sequence

$$1 \to \mathcal{O}^\times \to K^\times \to J_K \to Cl_K \to 1.$$

$$a \longmapsto (a)$$

Numbers Ideals

measures the "contraction" going from numbers to ideals.

measures the "expansion" going from numbers to ideals

Goal: Understand $\mathcal{O}^\times$ & Cl_K in more detail for Number fields

§ 5 Lattices

In the proof of Prop 1.13 ($\mathbb{Z}[i] \subset \mathbb{C}$ is factorial) we already saw that lattices can help to understand algebraic objects.

Definition 5.1 Let V be an n-dimensional $\mathbb{R}$-vector space.

i) A <u>lattice</u> in V is a subgroup of the form

$$\Gamma = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_m$$

with linearly independent $v_1, \dots, v_m \in V$.

The $(v_1, \dots, v_m)$ is called a <u>basis of Γ</u> and the set

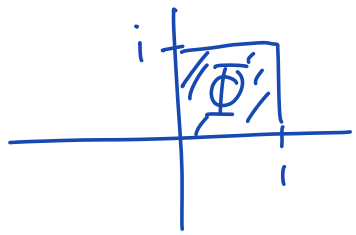
$$\Phi = \{ x_1 v_1 + \dots + x_m v_m \mid x_i \in \mathbb{R},\ 0 \leq x_i < 1 \}$$

a <u>fundamental mesh</u> of the lattice.

ii) Γ is called <u>complete</u> if $m = n$.

Example: i) $\mathbb{Z} \subset \mathbb{C}$ is a non complete lattice

ii) $\mathbb{Z} + \mathbb{Z}i$ is a complete lattice



V: n-dim $\mathbb{R}$-vectorspace

Definition 5.2 A subgroup $G \subseteq V$ is called <u>discrete subgroup</u> if all $\gamma \in G$ are isolated points in V. (with respect to the topology V obtains from isom. $V \cong \mathbb{R}^n$).

Every lattice $\Gamma = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_m \subset V$ is a discrete subgroup: Since if $(v_1, \dots, v_m, v_{m+1}, \dots, v_n)$ is a basis of V, then each point

$$\gamma = a_1 v_1 + \dots + a_m v_m \in \Gamma$$

has a neighbourhood

$$U_\gamma = \{ x_1 v_1 + \dots + x_n v_n \mid x_i \in \mathbb{R},\ |a_i - x_i| < 1 \text{ for } i = 1, \dots, m \}$$

with $U_\gamma \cap \Gamma = \{\gamma\}$.

Indeed the converse is also true:

Proposition 5.3 A subgroup $\Gamma \subset V$ is a lattice if and only if it is discrete.

Proof: Neukirch Prop. 4.2 $\square$

Lemma 5.4 A lattice $\Gamma \subset V$ is complete if and only if there exists a bounded subset $M \subset V$ whose translates cover V, i.e

$$V = \bigcup_{\gamma \in \Gamma} (M + \gamma) \qquad (*)$$

Proof: "$\Rightarrow$": clear by taking $M = \Phi$.

"$\Leftarrow$": Let V_0 be the subspace spanned by Γ. Want to show $V_0 = V$. For any $v \in V$ we can write for any $n \geq 1$

$$n \cdot v = a_n + \gamma_n$$

with $a_n \in M$ and $\gamma_n \in \Gamma$ (since $(*)$).

Then $v = \frac{1}{n} a_n + \frac{1}{n} \gamma_n$ i.e

$$v = \underbrace{\lim_{n\to\infty} \frac{1}{n} a_n}_{=0} + \lim_{n\to\infty} \frac{1}{n} \gamma_n = \lim_{n\to\infty} \frac{1}{n} \gamma_n \in V_0 .$$

M bounded

Since V_0 is closed $\square$

Definition 5.5 i) A <u>euclidean vector space</u> is a finite dimensional $\mathbb{R}$-vector space V equipped with a symmetric, positive definite bilinear form

$$\langle , \rangle : V \times V \longrightarrow \mathbb{R}.$$

ii) On V we have a notion of volume. Let $e_1, \dots, e_n$ be a orthonormal basis of V. For lin. indep. $v_1, \dots, v_n$ with

$$v_i = \sum_{j=1}^{n} a_{ij} e_j$$

we define the volume of the parallelepiped

$$\Phi = \Phi(v_1, \dots, v_n) = \{ x_1 v_1 + \dots + x_n v_n \mid x_i \in \mathbb{R}, 0 \le x_i < 1 \}$$

by

$$\mathrm{vol}(\Phi) = |\det(a_{ij})| = |\det(A)| .$$

Since $\langle v_i, v_j \rangle = \sum a_{ik} a_{jl} \langle e_k, e_l \rangle$

$$= (AA^T)_{ij}$$

we get $\mathrm{vol}(\Phi) = \left| \det((\langle v_i, v_j \rangle)_{ij}) \right|^{\frac{1}{2}}$.

ii) For a lattice Γ we define

$$\mathrm{vol}(\Gamma) = \mathrm{vol}(\underset{\substack{\uparrow \\ \text{fundamental} \\ \text{mesh of } \Gamma}}{\Phi})$$

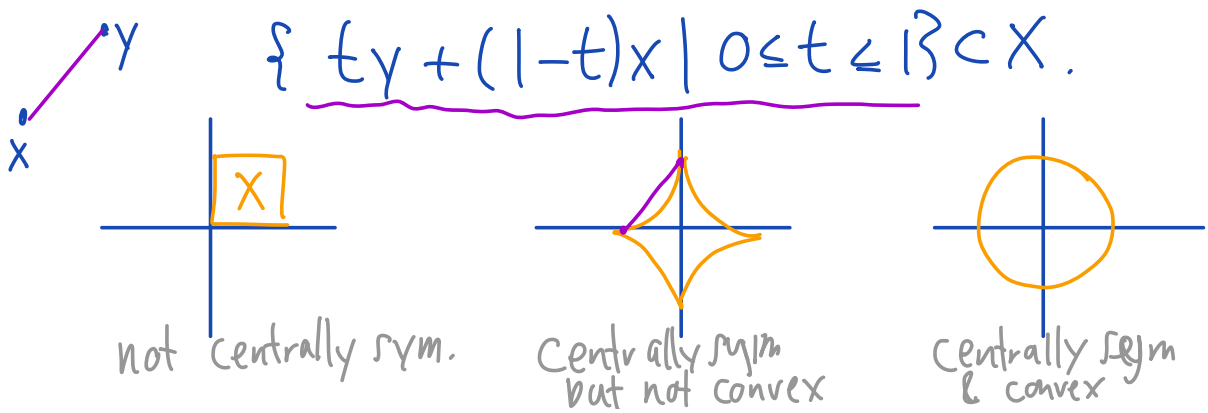
This is independent of the choice of a basis of Γ, since the change of basis matrices have determinant ± 1.

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 $x, y \in X$

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

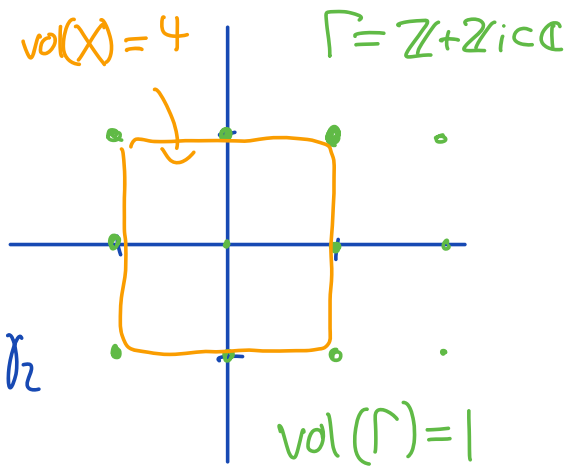


We now state Minkowski's lattice point theorem:

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. $\square$