6. Lattices and alg. integers

Recall from last week: $x \in \overline{\mathbb{Q}}$ is an alg. integer, if x is a root of some monic poly. $X^n + a_1 X^{n-1} + \dots + a_n$, where $a_i \in \mathbb{Z}$. $\Leftrightarrow$ the monic min. poly of x has coeff in $\mathbb{Z}$.

K = a number field $\Rightarrow$ $\mathcal{O}_K$ = ring of alg. int. in K.

E.g. $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$. As an abelian group this is $\cong \mathbb{Z}^2$, which is a lattice in $\mathbb{R}^2$

Def 1) A subgroup $\Lambda \subset \mathbb{R}^n$ is called discrete if $\exists \varepsilon > 0$, s.t.

$$\underbrace{\{v \in \mathbb{R}^n \mid \|v\| < \varepsilon\}}_{\varepsilon\text{-ball around } 0 \text{ for some norm } \|\cdot\|} \cap \Lambda = \{0\}$$

this notion does not depend on the choice of $\|\cdot\|$

2) A subgroup $\Lambda \subset \mathbb{R}^n$ is a lattice, if Λ is discrete and spans $\mathbb{R}^n$ (i.e. Λ contains a basis of $\mathbb{R}^n$)

Example 1) $e_1, \dots, e_n$ – basis of $\mathbb{R}^n$, then $\Lambda = \{\sum_{i=1}^n a_i e_i \mid a_i \in \mathbb{Z}\}$ is a lattice in $\mathbb{R}^n$

2) Let $\Lambda = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \subset \mathbb{R}$

Λ is not discrete $\Rightarrow$ not a lattice

Note $\mathbb{Z}^2 \xrightarrow{\sim} \Lambda$ surj. by def.

$(a,b) \longmapsto a + b\sqrt{2}$ inj.: $\underbrace{\sqrt{2} = -\frac{a}{b}}_{\text{irrational}}$

$\operatorname{rk} \Lambda \subset \dim \mathbb{R} = 1$

Why not discrete? Define $r = \inf\{z \in \Lambda \mid z > 0\}$

Claim: $r = 0$. Assume $r > 0$. Then $r \in \Lambda$

Otherwise $\exists$ sequence $z_i \in \Lambda$, s.t.

$z_i > r$, $z_i < z_j$ for $i > j$, $z_i \xrightarrow[i \to \infty]{} r$

$\exists\, z_{i_0} < z_{j_0}$: $z_{i_0} - r < r/2$, $z_{j_0} - r < r/2$

Then: $|z_{j_0} - z_{i_0}| = |z_{j_0} - r + r - z_{i_0}| \leq$

$$\leq |z_{j_0} - r| + |z_{i_0} - r| < \underbrace{\tfrac{r}{2} + \tfrac{r}{2}}_{= r}$$

so $0 < z_{j_0} - z_{i_0} < r$, $z_{j_0} - z_{i_0} \in \Lambda$ – contrad. the choice of r. $\Rightarrow r \in \Lambda$.

Then $\Lambda \simeq \mathbb{Z} \cdot r$. If not, then

$\exists\, z \in \Lambda : \quad n_0 \tau < z < (n_0+1)\tau$

$\Rightarrow \ 0 < \underbrace{z - n_0 \tau}_{\in \Lambda} < \tau$ – contradicts the choiche of τ.

<u>Lemma</u> Assume $\Lambda \subset \mathbb{R}^n$ is a lattice, and $M \subset \mathbb{R}^n$ a compact subset. Then

$\Lambda \cap M$ is finite.

<u>Proof</u> Assume not. Then $\exists$ a sequence $z_i \in \Lambda \cap M$, $z_i \neq z_j$ $i \neq j$. Since M is compact, we can choose a converging subsequence $z_i \xrightarrow[i\to\infty]{} x \in M$

Then $\forall \varepsilon > 0 \ \exists\, z_{i_0}, z_{j_0}$:

$|x - z_{j_0}| < \varepsilon/2, \quad |x - z_{i_0}| < \varepsilon/2$

Then $|z_{i_0} - z_{j_0}| < \varepsilon$, and $z_{i_0} - z_{j_0} \in \Lambda$

– contradicts discreteness of Λ $\square$

<u>Prop 6.1</u> Let $\Lambda \subset \mathbb{R}^n$ be a lattice. Then $\Lambda \simeq \mathbb{Z}^n$ (i.e. Λ is as in example 1 above)

Proof **Step 1** We show that Λ is finitely generated.

Λ spans $\mathbb{R}^n \Rightarrow \exists\, e_1, \dots, e_n \in \Lambda$ – a basis of $\mathbb{R}^n$

Define $M = \{ \sum_{i=1}^n \lambda_i e_i \mid 0 \leq \lambda_i \leq 1 \}$

$\simeq [0,1]^n$

M is compact. By Lemma above

$M \cap \Lambda = \{0, e_1, \dots, e_n, e_{n+1}, \dots, e_N\}$ finite set

Let $z \in \Lambda$, then $z = \sum_{i=1}^n \alpha_i e_i$, $\alpha_i \in \mathbb{R}$

$z' = z - \sum_{i=1}^n \underbrace{\lfloor \alpha_i \rfloor}_{\text{round-down of } \alpha_i} e_i \in \Lambda \cap M$

$\Rightarrow \exists\, j = 1 \dots N$ $z' = e_j$ or $z' = 0$

$\Rightarrow z$ is a lin. comb. with integral coeff of $e_1, \dots, e_N$

$\Rightarrow e_1 \dots e_N$ generate Λ.

Step 2 From step 1 $\Rightarrow \Lambda \simeq \mathbb{Z}^m$ for some $m \geq n$.

Let $e_1, \dots, e_m$ be generators of Λ, and assume $e_1, \dots, e_n$ a basis of $\mathbb{R}^n$

Assume $m > n$; then

$$e_{n+1} = \sum_{i=1}^{n} \alpha_i e_i, \quad \alpha_i \in \mathbb{R}$$

If all $\alpha_i \in \mathbb{Q}$, then $\exists d \in \mathbb{Z}$:

$$d \cdot e_{n+1} = \sum_{i=1}^{n} \underbrace{\alpha_i d}_{\in \mathbb{Z}} e_i$$

– contradicts the fact that e_i are lin. indep in Λ.

We may assume $\alpha_1 \in \mathbb{R} \setminus \mathbb{Q}$

$$e_{n+1} = \underbrace{\alpha_1}_{\text{irrational}} e_1 + \sum_{i=2}^{n} \alpha_i e_i$$

Note: $\forall k_1 \neq k_2$ integers

$$k_1 e_{n+1} \not\equiv k_2 e_{n+1} \pmod{\mathbb{Z}e_1 \oplus \ldots \mathbb{Z}e_n}$$

(if $k_1 e_{n+1} - k_2 e_{n+1} = \sum_{i=1}^{n} \lambda_i e_i$, $\lambda_i \in \mathbb{Z}$

then $(k_1 - k_2)\alpha_1 = \lambda_1 \Rightarrow \alpha_1 \in \mathbb{Q}$ – contrad.)

Consider the vectors

$$k e_{n+1} - \sum \lfloor k \alpha_i \rfloor e_i \in \Lambda \cap M$$

M as above. By Lemma $\Lambda \cap M$ is finite $\Rightarrow \exists k_1 \neq k_2$

$$k_1 e_{n+1} \equiv k_2 e_{n+1} \pmod{\mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_n}$$

– contradiction $\square$

$\mathbb{Q} \subset K$ a number field.

$K \simeq \mathbb{Q}^n$ as a $\mathbb{Q}$-vector space for some n.

Consider $\mathbb{Q}^n \hookrightarrow \mathbb{R}^n \ (\simeq K \otimes_{\mathbb{Q}} \mathbb{R})$

Then $\mathcal{O}_K \subset K \hookrightarrow \mathbb{R}^n \Rightarrow \mathcal{O}_K$ is a subgroup of $\mathbb{R}^n$.

<u>Prop 6.2</u> 1) $\forall x \in K \ \exists d \in \mathbb{Z}, d \neq 0$, s.t. $dx \in \mathcal{O}_K$

2) $\forall x \in \mathcal{O}_K \quad Tr_{K/\mathbb{Q}}(x) \in \mathbb{Z}, \ N_{K/\mathbb{Q}}(x) \in \mathbb{Z}$ and $x \neq 0 \Rightarrow N_{K/\mathbb{Q}}(x) \neq 0$.

<u>Proof</u> 1) x is alg.

$\Rightarrow a_0 x^m + a_1 x^{m-1} + \ldots + a_m = 0, \quad a_0 \neq 0$

$$x^m + \frac{a_1}{a_0} x^{m-1} + \ldots + \frac{a_m}{a_0} = 0 \qquad (*)$$

$\exists d \in \mathbb{Z}: \quad d\frac{a_i}{a_0} \in \mathbb{Z} \quad \forall i$

Multiply $(*)$ by d^m

$$(dx)^m + d\frac{a_1}{a_0}(dx)^{m-1} + \ldots + d^m \frac{a_m}{a_0} = 0$$

all coefficients are in $\mathbb{Z} \Rightarrow dx \in \mathcal{O}_K$

2) Recall Prop 4.3 from Lecture 3:

$Tr(x) = \sum \sigma(x)$, $N(x) = \prod \sigma(x)$

over all $\sigma : K \hookrightarrow \overline{\mathbb{Q}}$

all $\sigma(x)$ are alg. integers

$\Rightarrow Tr(x), N(x)$ are allg. integers,

but they are also in $\mathbb{Q}$

$\Rightarrow Tr(x), N(x) \in \mathbb{Z}$

$x \neq 0 \Rightarrow \sigma(x) \neq 0 \Rightarrow N(x) \neq 0$ – clear

$\square$

<u>Thm 6.3</u> For a number field K $\mathcal{O}_K$ is a lattice in $\mathbb{R}^n = K \otimes_{\mathbb{Q}} \mathbb{R}$

<u>Proof</u> <u>Step 1</u>: $\mathcal{O}_K$ spans $\mathbb{R}^n$ as a vector space.

Let $e_1, \dots, e_n \in K$ form a basis of $K/\mathbb{Q}$ $\Rightarrow$ they form a basis of $\mathbb{R}^n = K \otimes_{\mathbb{Q}} \mathbb{R}$ / $\mathbb{R}$

By Prop 6.2. $\exists d \in \mathbb{Z}$: $d \cdot e_i \in \mathcal{O}_K$ $\forall i$

de_i also form a basis

<u>Step 2</u> $\mathcal{O}_K$ is a discrete subgroup

We may assume that K is normal. Otherwise embed $K \subset K'$, K' normal prove that $\mathcal{O}_{K'}$ is discrete in $K' \otimes_{\mathbb{Q}} \mathbb{R} \Rightarrow \mathcal{O}_K = K \cap \mathcal{O}_{K'}$ is also discrete (exercise).

Assume $\mathcal{O}_K$ not discrete. Then $\exists$ sequence $z_i \in \mathcal{O}_K$, $z_i \xrightarrow[i\to\infty]{} 0$, $z_i \neq 0$

Choose a basis $e_1 \dots e_n$ of $K/\mathbb{Q}$

$$z_i = \sum_{j=1}^{n} \lambda_{ij} e_j \qquad \lambda_{ij} \in \mathbb{Q}$$

Then $\forall j = 1 \dots n$ $\lambda_{ij} \xrightarrow[i\to\infty]{} 0$

Consider

$$N_{K/\mathbb{Q}}(z_i) = \prod_{\sigma: K \hookrightarrow \overline{\mathbb{Q}}} \sigma(z_i) =$$

$$= \prod_{\sigma: K \hookrightarrow \overline{\mathbb{Q}}} \left(\lambda_{i1} \sigma(e_1) + \dots + \lambda_{in} \sigma(e_n) \right)$$

$$= \sum_{k_1 + \dots + k_n = n} \lambda_{i1}^{k_1} \dots \lambda_{in}^{k_n} \underbrace{\prod_{j=1}^{n} \sigma(e_j)^{k_j}}_{\in K}$$

K fixed element (not depending on λ_{ij})

$N(z_i)$ is a polynomial function in λ_{ij}

$$\Rightarrow N(z_i) \xrightarrow[i\to\infty]{} 0$$

But $\underset{\#}{N}(z_i) \in \mathbb{Z}$ by Prop. 6.2

this is a contradiction

$\Rightarrow \mathcal{O}_K$ is discrete $\square$

<u>Corollary</u> as an abelian group

$$\mathcal{O}_K \simeq \mathbb{Z}^{[K:\mathbb{Q}]}$$

<u>Proof</u> follows from Prop 6.1 an. 6.3 $\square$

<u>Recall from the previous week</u>

$$(x, y) \longmapsto \mathrm{Tr}_{K/\mathbb{Q}}(xy) \in \mathbb{Q}$$

is a non-degenerate symmetric $\mathbb{Q}$-bilinear form on K. By Prop 6.2 $\forall x, y \in \mathcal{O}_K$

$\mathrm{Tr}_{K/\mathbb{Q}}(xy) \in \mathbb{Z}$

$\Rightarrow \mathcal{O}_K$ is a lattice $\mathbb{Z}^n$ with a scalar product defined by the trace form $\mathrm{Tr}: \mathcal{O}_K \times \mathcal{O}_K \longrightarrow \mathbb{Z}$

Let $e_1 \ldots e_n$ be a basis of $\mathcal{O}_K$.

Consider the matrix $A = (a_{ij})$

$$a_{ij} = \mathrm{Tr}(e_i e_j) \in \mathbb{Z}$$

Def The discriminant of K is
$$d_K = \det(A).$$
Lemma d_K does not depend on the choiche of a basis in $\mathcal{O}_K$

Proof Let $f_1 \dots f_n$ be another basis

$f_i = \sum m_{ij} e_j, \quad m_{ij} \in \mathbb{Z} \quad M = (m_{ij})$

$e_k = \sum m'_{k\ell} f_\ell, \quad m'_{k\ell} \in \mathbb{Z} \quad M' = (m'_{k\ell})$

Then $MM' = M'M = \mathrm{Id}. \Rightarrow \det M \cdot \det M' = 1$

$\det M = \pm 1$ because $\det M \in \mathbb{Z}$

Let $b_{ij} = Tr(f_i f_j) =$
$$= \sum_{\alpha,\beta=1}^{n} m_{i\alpha} m_{j\beta} \underbrace{Tr(e_\alpha e_\beta)}_{a_{\alpha\beta}}$$
$$\Rightarrow B = (b_{ij}) = MAM^t$$
$$\Rightarrow \det B = \underbrace{(\det M)^2}_{1} \det A = \det A$$
$\square$

Example 1) $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]; \quad 1, i$ – basis
$$A = \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix} \Rightarrow d_{\mathbb{Q}(i)} = -4$$

2) $\mathcal{O}_{\mathbb{Q}(\sqrt{2})} = \mathbb{Z}[\sqrt{2}]$ $\quad 1, \sqrt{2}$ – basis

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix} \Rightarrow d_{\mathbb{Q}(\sqrt{2})} = 8$$

<u>Prop 6.4</u> For a number field K either $d_K \equiv 0 \pmod 4$ or $d_K \equiv 1 \pmod 4$

<u>Proof</u> A = matrix of the trace form in a basis $e_1 \dots e_n \in \mathcal{O}_K$

Consider $B = (b_{ij})$

$$b_{ij} = \sigma_j(e_i), \quad \sigma_j : K \hookrightarrow \overline{\mathbb{Q}} \text{ embedding}$$

In lecture 3 we have seen:

$$A = B \cdot B^t \Rightarrow d_K = (\det B)^2$$

$$\det B = \sum_{\substack{\pi\text{-even} \\ \text{permut. of } 1\dots n}} \prod_{i=1}^{n} b_{i\pi(i)} - \sum_{\substack{\pi\text{- odd} \\ \text{permut. of } 1\dots n}} \prod_{i=1}^{n} b_{i\pi(i)}$$

Define $\displaystyle \alpha = \sum_{\pi\text{- all permut.}} \prod_{i=1}^{n} b_{i\pi(i)}$

$$\beta = \sum_{\pi\text{-odd permut}} \prod_{i=1}^{n} b_{i\pi(i)}$$

Then $\quad \det B = \alpha - 2\beta$

α, β are alg. integers

Note: α is Galois-invariant

$\Rightarrow \alpha \in \mathbb{Q} \Rightarrow \alpha \in \mathbb{Z}$

$$d_K = (\det B)^2 = \alpha^2 - 4\alpha\beta + 4\beta^2$$

$$= \alpha^2 + 4(\beta^2 - \alpha\beta) \in \mathbb{Z}$$

$$\Rightarrow \beta^2 - \alpha\beta = \frac{d_K - \alpha^2}{4} \in \mathbb{Q}$$

$\beta^2 - \alpha\beta$ is an alg. integer

$\Rightarrow \beta^2 - \alpha\beta \in \mathbb{Z}$

$$\Rightarrow d_K = \alpha^2 + 4\underbrace{(\beta^2 - \alpha\beta)}_{\in \mathbb{Z}} \equiv \alpha^2 \pmod 4$$

$\alpha^2 \equiv 0$ or $1 \pmod 4$ $\square$