ZAHLENTHEORIE SS 2019 - NOTE 5

§ DISCRIMINANT

Let $K/\mathbb{Q}$ be a number field of degree $[K:\mathbb{Q}]=n$
Then for any n-tuple (note: $n = [K:\mathbb{Q}]$)
$(\alpha_1,\dots,\alpha_n) \in K^n$ we can form the matrix

$$\left(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)\right)_{i,j} \in \mathbb{Q}^{n\times n}$$

The significance of this matrix is that for
$(a_1,\dots,a_n),(b_1,\dots,b_n) \in \mathbb{Q}^n$ we have

$$(a_1 \dots a_n)\left(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)\right)\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \sum_{i,j} a_i b_j \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)$$

$$= \mathrm{Tr}_{K/\mathbb{Q}}\left((a_1\alpha_1+\dots+a_n\alpha_n)\cdot(b_1\alpha_1+\dots+b_n\alpha_n)\right)$$

def: DISCRIMINANT of an n-TUPLE
$K/\mathbb{Q}$ = number field, $[K:\mathbb{Q}]=n$. The discriminant of an n-tuple is defined as

$$\mathrm{disc}(\alpha_1,\dots,\alpha_n) \overset{def}{:=} \det\left(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)\right).$$

Lemma: $K/\mathbb{Q}$ = number field, $[K:\mathbb{Q}]=n$
Let $\sigma_1,\dots,\sigma_n : K \hookrightarrow \overline{\mathbb{Q}}$ be the embeddings s.t.

$$(\quad (\quad))^2$$

$$\mathrm{disc}(\alpha_1,\dots,\alpha_n) = \left(\det(\sigma_i(\alpha_j))\right)^2.$$

proof: Let A be the matrix $A = (\sigma_i(\alpha_j))$. Then

$$(A^t A)_{ij} = \sum_{k=1}^{n} A^t_{ik} A_{kj} = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j)$$

$$= \sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j) = \mathrm{Tr}(\alpha_i\alpha_j). \text{ Hence}$$

$$(\mathrm{Tr}(\alpha_i\alpha_j)) = A^t A \text{ and}$$

$$\mathrm{disc}(\alpha_1,\dots,\alpha_n) = \det(\mathrm{Tr}(\alpha_i\alpha_j)) = (\det A)^2. \qquad \square$$

Prop: $\mathrm{disc}(\alpha_1,\dots,\alpha_n) = 0 \iff$ the α_i are linearly dependent over $\mathbb{Q}$

proof: $\mathrm{disc}(\alpha_1,\dots,\alpha_n) = 0 \iff \det(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)) = 0$

$\iff \exists\, (y_1,\dots,y_n) \in \mathbb{Q}^n \setminus \{\underline{0}\}$ s.t.

$$(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j))\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = 0.$$

$$\iff (x_1,\dots,x_n)(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j))\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = 0 \quad \forall x_i \in \mathbb{Q}$$

$$\iff \mathrm{Tr}_{K/\mathbb{Q}}((x_1\alpha_1 + \dots + x_n\alpha_n)(y_1\alpha_1 + \dots + y_n\alpha_n)) = 0 \quad \forall x_i \in \mathbb{Q}$$

($\Rightarrow$) Assume that disc $= 0$ and that the α_i are lin. indep. Then they are a basis of $K/\mathbb{Q}$, hence we get

$\mathrm{Tr}\ (x\cdot(y_1\alpha_1 + \dots + y_n\alpha_n)) = 0 \quad \forall x \in \mathbb{Q}$

Since the trace is nondegenerate, this means
$$y_1\alpha_1 + \dots + y_n\alpha_n = 0$$
hence $y_i = 0$ for all i, contradiction.

($\Leftarrow$) If the α_i are linearly dependent, there is $(y_1, \dots, y_n) \in \mathbb{Q}^n \setminus \{0\}$ s.t. $y_1\alpha_1 + \dots + y_n\alpha_n = 0$

hence $Tr_{K/\mathbb{Q}}((x_1\alpha_1 + \dots + x_n\alpha_n)(y_1\alpha_1 + \dots + y_n\alpha_n)) = 0$ $\forall x_i \in \mathbb{Q}$. $\square$

<u>Lemma</u>: $K/\mathbb{Q}$ = number field, $[K:\mathbb{Q}] = n$
$\alpha_1, \dots, \alpha_n$ integral basis of $\mathcal{O}_K$
$\beta_1, \dots, \beta_n$ integral basis of $\mathcal{O}_K$. Then

$$\mathrm{disc}(\alpha_1, \dots, \alpha_n) = \mathrm{disc}(\beta_1, \dots, \beta_n).$$

<u>proof</u>: Let M be the matrix that represents the change of basis from $\alpha_1, \dots, \alpha_n$ to $\beta_1, \dots, \beta_n$.
Then M, M^{-1} have integer coefficients, hence $\det(M) \in \mathbb{Z}^*$, so that $\det M = \pm 1$. Now since the matrices $(Tr(\alpha_i\alpha_j)), (Tr(\beta_i\beta_j))$ represent the bilinear form $Tr: K \times K \to \mathbb{Q}$ w.r.t. the bases $(\alpha_1, \dots, \alpha_n)$ and $(\beta_1, \dots, \beta_n)$, we have

$$(Tr(\alpha_i\alpha_j)) = M^t\,(Tr(\beta_i\beta_j))\,M, \text{ hence}$$

[illegible]

$= 1$

<u>def</u>: DISCRIMINANT of a NUMBER FIELD

$K/\mathbb{Q}$ = number field. We define the DISCRIMINANT of K as the discriminant of any integral basis of $\mathcal{O}_K$.

Sometimes we write
$$\mathrm{disc}(K) = \Delta_K.$$

We want to give some examples, but first a method to compute the discriminant:

<u>Notation</u>: If $K = \mathbb{Q}(\alpha)$ and $[K:\mathbb{Q}] = n$ then $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ is a basis of $K/\mathbb{Q}$. We denote

$$\mathrm{disc}(\alpha) = \mathrm{disc}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}).$$

<u>Prop</u>: $K = \mathbb{Q}(\alpha)$ and $[K:\mathbb{Q}] = n$. Then let $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \overline{\mathbb{Q}}$ embeddings of $K/\mathbb{Q}$

$m_\alpha(x)$ = min poly of α over $\mathbb{Q}$.

Then
$$\mathrm{disc}(\alpha) = \prod_{i<j} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(m_\alpha'(\alpha)).$$

proof: Exercise.

Example: QUADRATIC EXTENSIONS

Let d be a sqfr integer. We know

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}], & d \equiv 2,3 \ (4) \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & d \equiv 1 \ (4) \end{cases}$$

- $d \equiv 2,3 \ (4)$

An integral basis of $\mathbb{Z}[\sqrt{d}]$ is given by $1, \sqrt{d}$. Then

$$\Delta_{\mathbb{Q}(\sqrt{d})} = \mathrm{disc}(\sqrt{d}) = (\sqrt{d} - (-\sqrt{d}))^2$$
$$= (2\sqrt{d})^2 = 4d$$

Also, we see that

$$m_{\sqrt{d}}(x) = x^2 - d$$
$$m'_{\sqrt{d}}(x) = 2x$$
$$m'_{\sqrt{d}}(x) = 2\sqrt{d}$$

$$N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(2\sqrt{d}) = 2^2(\sqrt{d})(-\sqrt{d}) = -4d$$

We can also compute it from the definition: the matrix with the traces is

$$\begin{pmatrix} \mathrm{Tr}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(1) & \mathrm{Tr}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(\sqrt{d}) \\ \mathrm{Tr}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(\sqrt{d}) & \mathrm{Tr}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(d) \end{pmatrix}$$

$= \Big(2 \quad 0 \Big)$ has determinant $4d$

$0 \qquad 2d$

- $d \equiv 1 \ (4)$

An integral basis is $1, \alpha$ with $\alpha = \frac{1+\sqrt{d}}{2}$.
Then

$$\Delta_{\mathbb{Q}(\sqrt{d})} = \mathrm{disc}(\alpha) = \left(\frac{1+\sqrt{d}}{2} - \frac{1-\sqrt{d}}{2} \right)^2$$

$$= (\sqrt{d})^2 = d. \qquad \square$$

We present an application of the discriminant:

Prop: $K/\mathbb{Q}$ = number field, with $[K:\mathbb{Q}] = n$, $\alpha_1, \dots, \alpha_n$ basis of $K/\mathbb{Q}$, with $\alpha_i \in \mathcal{O}_K$, $d = \mathrm{disc}(\alpha_1, \dots, \alpha_n)$.
Then every $\alpha \in \mathcal{O}_K$ can be written as

$$\alpha = m_1 \frac{\alpha_1}{d} + m_2 \frac{\alpha_2}{d} + \dots + m_n \frac{\alpha_n}{d} \qquad m_i \in \mathbb{Z}, \quad d \mid m_i^2.$$

proof: consider the isomorphism

$$\widetilde{Tr}_{K/\mathbb{Q}} : K \longrightarrow \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{Q})$$

and let $\varphi_1, \dots, \varphi_n$ be the dual basis of $\alpha_1 \dots \alpha_n$ in $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{Q})$ i.e. $\varphi_i(\alpha_j) = \delta_{ij}$.
If we let $\beta_i = \widetilde{Tr}_{K/\mathbb{Q}}^{-1}(\varphi_i)$, we know already that $\mathcal{O}_K \subseteq \mathbb{Z}\beta_1 + \dots + \mathbb{Z}\beta_n$, hence we can write every $\alpha \in \mathcal{O}_K$ as

$$\alpha = \ell_1 \beta_1 + \dots + \ell_n \beta_n. \qquad \ell_i \in \mathbb{Z}.$$

Now we want to write the β_i w.r.t. the basis

Now we want to write that α w.r.t. the basis $\alpha_1, .., \alpha_n$. Observe that the matrix representing the map $\widetilde{Tr_{K/\mathbb{Q}}}$ w.r.t. the bases $(\alpha_1 .. \alpha_n)$ $(e_1 .. e_n)$ is precisely $(Tr_{K/\mathbb{Q}}(\alpha_i \alpha_j))$.

Hence the coordinates of $\beta_1, .., \beta_n$ w.r.t. $(\alpha_1 .. \alpha_n)$ are given precisely by the columns of the inverse $(Tr_{K/\mathbb{Q}}(\alpha_i \alpha_j))^{-1} =$

$$= \frac{1}{d} \operatorname{adj}\left((Tr_{K/\mathbb{Q}}(\alpha_i \alpha_j)) \right)$$

Since the adjoint has integer coefficients, we see that

$$\beta_i = \frac{1}{d} m_{i1}\alpha_1 + .. + \frac{1}{d} m_{in}\alpha_n, \text{ hence}$$

$$\alpha = \sum e_i \beta_i = \sum_{i,j} e_i m_{ij} \frac{\alpha_j}{d} \quad \text{with } e_i, m_{ij} \in \mathbb{Z}.$$

$$= \sum m_j \frac{\alpha_j}{d}$$

with some more work one can show $d \mid m_i$? $\square$

As a corollary, we get:

<u>Cor</u>: $K/\mathbb{Q}$ = number field, $[K:\mathbb{Q}] = n$
$\alpha_1, .., \alpha_n$ basis of $K/\mathbb{Q}$ with $\alpha_i \in \mathcal{O}_K$.
Suppose $d = \operatorname{disc}(\alpha_1, .., \alpha_n)$ is sqfr, then $\alpha_1, .., \alpha_n$ are an integral basis of $\mathcal{O}_K$.

<u>proof</u>: the α_i are linearly independent, hence we

need to show that they generate $\mathcal{O}_K$.
By the previous proposition we have $\forall \alpha \in \mathcal{O}_K$

$$\alpha = \frac{m_1}{d}\alpha_1 + \dots + \frac{m_n}{d}\alpha_n, \quad m_i \in \mathbb{Z}, \ d \mid m_i^2.$$

Since d is sqfr and $d \mid m_i^2$, we have that $d \mid m_i$.
Hence the coefficients $\frac{m_i}{d}$ are in $\mathbb{Z}$ and we are done $\square$

As an application of the discriminant (to be proved in the exercises) we have:

Example: RINGS of INTEGERS of CYCLOTOMIC FIELDS
Let $\zeta_n = e^{2\pi i/n}$ a primitive n-th root of unity, and let $\mathbb{Q}(\zeta_n)$ be the corresponding cyclotomic field. Then

$$\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$$

In particular an integral basis is
$1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{\varphi(n)-1}$.

Ultima modifica: 11:42