MATH620 - Algebraic Number Theory

Taught by Niranjan Ramachandran
Notes taken by Haoran Li
2020 Spring

Department of Mathematics
University of Maryland

Contents

1 Disciminant

Definition 1.1. An *algebraic number field* K is a finite field extension of $\mathbb{Q}$, its ring of algebraic integers is denoted $\mathcal{O}_K$

$$\begin{tikzcd} \mathcal{O}_K \arrow[r, hook] & K \\ \mathbb{Z} \arrow[r, hook] \arrow[u, hook] & \mathbb{Q} \arrow[u, hook] \end{tikzcd}$$

More generally, if E/F is a finite separable field extension, B, A are their ring of integers

$$\begin{tikzcd} B \arrow[r, hook] & E \\ A \arrow[r, hook] \arrow[u, hook] & F \arrow[u, hook] \end{tikzcd}$$

Definition 1.2. $[E : F] = n$, then $B \cong A^n$ as an A module, assume $\beta_1, \cdots, \beta_n$ is a basis, define

$$D(\beta_1, \cdots, \beta_n) = \det(\mathrm{Tr}_{B/A}(\beta_i\beta_j)) \in A$$

The *discriminant* $\operatorname{disc}(B/A) = D(\beta_1, \cdots, \beta_n)$ is well-defined in $A/(A^\times)^2$. In particular, $\operatorname{disc}(\mathcal{O}_K/\mathbb{Z})$ is a well-defined integer

Lemma 1.3. $\gamma_1, \cdots, \gamma_n \in \mathcal{O}_K$ is an $\mathbb{Z}$-basis for $\mathcal{O}_K$ iff $D(\gamma_1, \cdots, \gamma_n) = \operatorname{disc}(\mathcal{O}_K/\mathbb{Z})$. More generally, if A is integral closed and Noetherian, $\gamma_1, \cdots, \gamma_n \in B$ is an A-basis of B iff $D(\gamma_1, \cdots, \gamma_n) = \operatorname{disc}(B/A)$

Proof. Write $\gamma_i = \sum c_{ji}\beta_j$, then $\det(\mathrm{Tr}(\gamma_i\gamma_j)) = (\det C)^2 \operatorname{disc}(\mathcal{O}_K/\mathbb{Z})$. Thus $D(\gamma_1, \cdots, \gamma_n) = \operatorname{disc}(\mathcal{O}_K/\mathbb{Z}) \Leftrightarrow \det C = \pm 1 \Leftrightarrow C \in \mathrm{GL}_n(\mathbb{Z}) \Leftrightarrow \gamma_1, \cdots, \gamma_n$ is an $\mathbb{Z}$-basis ☐

Example 1.4. $K = \mathbb{Q}(\sqrt{d})$, d is square free. $\mathcal{O}_K$ has $\{1, \sqrt{d}\}$ as an $\mathbb{Z}$-basis if $d \equiv 2, 3 \bmod 4$

$$\operatorname{disc}(\mathcal{O}_K/\mathbb{Z}) = \det \mathrm{Tr}_{\mathcal{O}_K/\mathbb{Z}} \begin{pmatrix} 1 & \sqrt{d} \\ \sqrt{d} & d \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d$$

$\mathcal{O}_K$ has $\{1, \frac{1+\sqrt{d}}{2}\}$ as an $\mathbb{Z}$-basis if $d \equiv 1 \bmod 4$

$$\operatorname{disc}(\mathcal{O}_K/\mathbb{Z}) = \det \mathrm{Tr}_{\mathcal{O}_K/\mathbb{Z}} \begin{pmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ \frac{1+\sqrt{d}}{2} & \frac{1+2\sqrt{d}+d}{4} \end{pmatrix} = \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{2+2d}{4} \end{pmatrix} = d$$

Therefore 7 can never be a discriminant

Proposition 1.5. $\gamma_1, \cdots, \gamma_n \in \mathcal{O}_K$, $N = \mathbb{Z}\gamma_1 + \cdots + \mathbb{Z}\gamma_n \le \mathcal{O}_K$ has finite index in $\mathcal{O}_K$ iff $D(\gamma_1, \cdots, \gamma_n) \ne 0$, $D(\gamma_1, \cdots, \gamma_n) = [\mathcal{O}_K : N]^2 \operatorname{disc}(\mathcal{O}_K/\mathbb{Z})$

Proof. Suppose $\beta_1, \cdots, \beta_n$ is an $\mathbb{Z}$-basis, $D(\beta - 1, \cdots, \beta_n) = \operatorname{disc}(\mathcal{O}_K/\mathbb{Z})$, $\gamma_i = \sum c_{ji}\beta_j$, $\det C = [\mathcal{O}_K : N]$ ☐

Proposition 1.6. If $D(\gamma_1, \cdots, \gamma_n)$ is square free, then $\gamma_1, \cdots, \gamma_n$ is an $\mathbb{Z}$-basis

Example 1.7. $K = \mathbb{Q}(\alpha)$, α is a root of irreducible polynomial $x^3 - x - 1$, $D(1, \alpha, \alpha^2) = -23$ which is square free, hence $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2 = \mathbb{Z}[\alpha]$

Proposition 1.8. $[E : F] = n$ is separable, Ω is the Galois closure of E, $\mathrm{Hom}_F(E, \Omega) = \{\sigma_1, \cdots, \sigma_n\}$ are distinct F-embeddings of E

$$\begin{tikzcd} B \arrow[r, hook] & E \\ A \arrow[r, hook] \arrow[u, hook] & F \arrow[u, hook] \end{tikzcd}$$

If $\beta_1, \cdots, \beta_n$ is an F-basis of E, then $D(\beta_1, \cdots, \beta_n) = \det(\sigma_i(\beta_j))^2 \ne 0$

Proof. Deonte $Q = \sigma_i(\beta_j)$, then

$$\begin{aligned}
D(\beta_1, \cdots, \beta_n) &= \det(\mathrm{Tr}_{E/F}(\beta_i\beta_j)) \\
&= \det(\sum \sigma_k(\beta_i\beta_j)) \\
&= \det(\sum \sigma_k(\beta_i)\sigma_k(\beta_j)) \\
&= \det(Q^T Q) \\
&= \det(\sigma_i(\beta_j))^2 \\
&\overset{\text{Theorem 1.9}}{\neq} 0
\end{aligned}$$

□

Dedekind's theorem

Theorem 1.9 (Dedekind's theorem)**.** G is group, Ω is a field, $\sigma_1, \cdots, \sigma_n$ are distinct homomorphisms $G \to \Omega^\times$, then σ_i's are linear independent over Ω

References

Index