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

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 $D(\beta_1, \cdots, \beta_n) = \det(\sigma_i(\beta_j))^2 \neq 0$

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*

Definition 1.10. Assume A, B are integrally closed in F, E, $\beta_1, \cdots, \beta_n \in B$ is an F-basis of E, $C = A\beta_1 + \cdots + A\beta_n \leq B$, $C^* = \{\beta \in E | \mathrm{Tr}_{E/F}(\beta\beta_i) \in A\}$, $\beta \in B \Rightarrow \beta\beta_i \in B \Rightarrow \mathrm{Tr}(\beta\beta_i) \in A \Rightarrow C \leq B \leq C^*$, $C^* = A\beta_1' + \cdots + A\beta_n'$, $\beta_1', \cdots, \beta_n'$ is a dual basis. For $\alpha \in E$, $\alpha = \sum \mathrm{Tr}_{E/F}(\alpha\beta_i)\beta_i'$

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

Example of dual basis

Example 1.11. $E = F(\beta)$, $f \in A[x]$ is the minimal polynomial of $\beta \in B$, $\deg f = n$, $C = A[\beta] \leq B$, Euler discovered

$$\mathrm{Tr}_{E/F}(\beta^i/f'(\beta)) = \begin{cases} 0 & 0 \leq i \leq n-1 \\ 1 & i = n-1 \end{cases}, \det \mathrm{Tr}_{E/F}(\frac{\beta^i\beta^j}{f'(\beta)}) = (-1)^n$$

$\dfrac{\beta^{n-1-i}}{f'(\beta)}$ is the dual basis of β^i

Proposition 1.12. *In Example 1.11, suppose $f(x) = \prod_{i=1}^n (x - \beta_i) \in \bar{E}[x]$, $f'(x) = \sum_{i=1}^n \prod_{j \neq i}(x - \beta_j)$. Then*

$$D(1, \beta, \cdots, \beta^{n-1}) = \prod_{1 \leq i < j \leq n} (\beta_i - \beta_j)^2 = (-1)^{\frac{n(n-1)}{2}} = N_{E/F}(f'(\beta))$$

Proof.

$$\begin{aligned} D(1, \beta, \cdots, \beta^{n-1}) &= \det(\sigma_i(\beta^j))^2 \\ &= \det(\beta_i^j)^2 \\ &= \prod_{1 \leq i < j \leq n} (\beta_i - \beta_j)^2 \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_i \prod_{j \neq i} (\beta_i - \beta_j) \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_i f'(\beta_i) \\ &= (-1)^{\frac{n(n-1)}{2}} N(f'(\beta)) \end{aligned}$$

□

Remark 1.13. $\Delta = \prod_{1 \leq i < j \leq n} (\beta_i - \beta_j)^2$ is the determinant $\mathrm{disc}(f) = \mathrm{disc}(E/F)$

Lemma 1.14. *$f(x) = x^n + ax + b$, $\mathrm{disc}(f) = (-1)^{\frac{n(n-1)}{2}}(n^n b^{n-1} + (-1)^n (n-1)^{n-1} a^n)$*

Example 1.15. $K = \mathbb{Q}(\beta)$, β is a root of $f(x) = x^5 - x - 1 \in \mathbb{Z}[x]$, $\mathrm{disc}(f) = 2869 = 19 \times 151$ is square free, hence $[\mathcal{O}_K : \mathbb{Z}[\beta]] = 1$, $\mathcal{O}_K = \mathbb{Z}[\beta]$

Definition 1.16. $K = \mathbb{Q}(\alpha)$, $f(x)$ is the minimal polynomial of α, thus $K \otimes_{\mathbb{Q}} \mathbb{R} \cong \dfrac{\mathbb{R}[x]}{(f)} \overset{\text{Chinese remainder theorem}}{\cong} \mathbb{R}^r \times \mathbb{C}^s$, $\alpha_1, \cdots, \alpha_r$ are the real roots of f, $\alpha_{r+1}, \bar{\alpha}_{r+1}, \cdots, \alpha_{r+s}, \bar{\alpha}_{r+s}$ are complex roots of f. $\mathcal{O}_K \hookrightarrow K_{\mathbb{R}} \cong \mathbb{R}^n$ is a lattice

Example 1.17. $\mathbb{Q}(\sqrt{5}) \hookrightarrow \mathbb{R} \times \mathbb{R}$ give the two real embeddings. $\mathbb{Q}(\sqrt{-5}) \hookrightarrow \mathbb{C}$ give the two complex embeddings

Proposition 1.18.

(1) $K = \mathbb{Q}(\alpha)$, $\operatorname{sgn}\mathrm{disc}(K/\mathbb{Q}) = (-1)^s$

(2) (Stickelberger) $\mathrm{disc}(\mathbb{O}_K/\mathbb{Z}) \equiv 0, 1 \bmod 4$

Proof.

(1) $1, \alpha, \cdots, \alpha^n$ is a basis for K, since $disc(K/\mathbb{Q}) \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ $\operatorname{sgn} D(1, \alpha, \cdots, \alpha^n) = \operatorname{sgn}\det(\sigma_j(\alpha^i))^2 = \operatorname{sgn}\prod_{1\le i<j\le n}(\alpha_i - \alpha_j)^2 = \operatorname{sgn}\prod_{1\le j\le s}(\alpha_{r+j} - \bar{\alpha}_{r+j})^2 = (-1)^s$

(2) $\beta_1, \cdots, \beta_n$ is an $\mathbb{Z}$-basis of $\mathcal{O}_K$, $\mathrm{disc}(\mathcal{O}_K/\mathbb{Z}) = \det(\sigma_i(\beta^j))^2$, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $\mathrm{Hom}(K, \overline{\mathbb{Q}})$, $K \overset{\sigma}{\hookrightarrow} \overline{\mathbb{Q}} \xrightarrow{\tau} \overline{\mathbb{Q}}$. $\det A = \sum_{\tau\in S_n} \mathrm{sgn}(\tau) \prod_{i=1}^n a_{i\tau(i)} = P - N$, P for those $\tau \in A_n$, N for those aren't, so $\mathrm{disc}(\mathcal{O}_K/\mathbb{Z}) = (P - N)^2 = (P + N)^2 - 4PN$, $\eta \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ induce a permutation π_η on $\mathrm{Hom}(K, \overline{\mathbb{Q}})$, if π_η is even, $\pi_\eta(P) = P, \pi_\eta(N) = N$, if π_η is odd, then π_η swich P, N, and $P + N, PN$ are integral over $\mathbb{Z}$, thus $P + N, PN \in \mathbb{Z}$, hence $\mathrm{disc}(\mathcal{O}_K/\mathbb{Z}) \equiv 0, 1 \bmod 4$

$\square$

Definition 1.19. For any nonzero ideal $I \le \mathcal{O}_K$, since $I \cap \mathbb{Z} = m\mathbb{Z}$, $\mathcal{O}_K/m\mathcal{O}_K \cong (\mathbb{Z}/m\mathbb{Z})^m \to \mathcal{O}_K/I$ is surjective, hence the *norm* $N(I) = |\mathcal{O}_K/I| < \infty$. The *Dedekind zeta function* of an algebraic number field is $\zeta_K(s) = \sum_{I\neq 0} \dfrac{1}{N(I)^s} = \prod_{p} \dfrac{1}{1 - N(p)^{-s}}$

2 Minkowski's theorem

Definition 2.1. $L = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n \leq \mathbb{R}^n$ is a lattice, take $D = \{c_1v_1 + \cdots + c_nv_n | 0 \leq c_i \leq 1\}$ L, the *covolume* $\operatorname{covol}(L) = \operatorname{vol}(\mathbb{R}^n/L) = \operatorname{vol}(D)$, $\pi : D \to \mathbb{R}^n/L$ is the quotient map, $\operatorname{covol}(L)^2 = \det(\langle v_i, v_j \rangle)$

Theorem 2.2. If $B \subseteq \mathbb{R}^n$ is bounded, convex, symmetric (i.e. $B = -B$) subset such that either

1. $\operatorname{vol}(B) > 2^n \operatorname{covol}(L)$ or
2. $\operatorname{vol}(B) \geq 2^n \operatorname{covol}(L)$ and B is closed

Then $(B \cap L) \setminus \{0\} \neq \varnothing$

Proof.

1. $\mathbb{R}^2 \to \mathbb{R}^2/2L$ is not injective by volume, thus $\exists x \neq y \in B$ such that $x - y \in 2L \Rightarrow \frac{1}{2}(x - y) \in B \cap L$ since B is convex and symmetric
2. $C_k = L \cap (1 + \frac{1}{k})B \setminus \{0\} \neq \varnothing$, C_k is discrete and closed, $\cap_{k=1}^{\infty} C_k \neq \varnothing$, thus contains a limit point of B, but B is closed

□

Proposition 2.3. $D_K = \operatorname{disc}(\mathcal{O}_K/\mathbb{Z}) \in \mathbb{Z}$

1. The image of $\mathcal{O}_K$ in $K_{\mathbb{R}}$ is a lattice
2. $\operatorname{covol}(\mathcal{O}_K) = \sqrt{|D_K|}$
3. If I is an ideal of $\mathcal{O}_K$, $\operatorname{covol}(I) = [\mathcal{O}_K : I]\sqrt{|D_K|}$ (union of all members in the coset)

Proof.

1. Need $\mathcal{O}_K \cap B_r$ is finite. $x \in \mathcal{O}_K \cap B_r \Rightarrow |\sigma(x)| \leq r$, for all complex embeddings $\sigma \Rightarrow f_{K/\mathbb{Q}.x}(t) = \prod_\sigma (t - \sigma(x))$, the characteristic monomial with $\mathbb{Z}$ coefficients of degree $[K : \mathbb{Q}]$, since coefficients are bounded, so only finitely many f, finitely many x since conjugates are roots
2. $\alpha_1, \cdots, \alpha_n$ is an $\mathbb{Z}$-basis of $\mathcal{O}_K$, $\operatorname{covol}(\mathcal{O}_K)^2 = \det(\langle \alpha_i, \alpha_j \rangle) = \det(M^T \bar{M})$, $M = (\sigma_i(\alpha_j))$, thus $\operatorname{covol}(\mathcal{O}_K) = \sqrt{|D_K|}$

□

Lemma 2.4. For $m \geq 1$, the number of ideals of $\mathcal{O}_K$ of index less than m is finite, if $[\mathcal{O}_K : I] \leq m$, then $\mathcal{O}_K/I$ is killed by $m!$, thus $m!\mathcal{O}_K \subseteq I \subseteq \mathcal{O}_K$, but $\mathcal{O}_K/m!\mathcal{O}_K \cong \mathbb{Z}^n/m!\mathbb{Z}^n \cong (\mathbb{Z}/m!)^n$ is finite

Theorem 2.5. For any $g \in \operatorname{Cl}(\mathcal{O}_K)$, $\exists I \subseteq \mathcal{O}_K$ such that $NI = [\mathcal{O}_K : I] \leq (\frac{2}{\pi})^s \sqrt{D_K} \Rightarrow \operatorname{Cl}(\mathcal{O}_K)$ is finite

Proof. J be an ideal representation for g^{-1}, if $0 \neq \alpha \in J$, then $0 \neq (\alpha) \subseteq J \Rightarrow \exists I$ ideal of $\mathcal{O}_K$ such that $(\alpha) = IJ$, so I represents g, $N\alpha = NI \cdot NJ$, for $c = (c_1, \cdots, c_r, c_{r+1}, \cdots, c_{r+s})$, $c_i > 0$

$$B(c) = \{(x_1, \cdots, x_r, x_{r+1}, \cdots, x_{r+s}) \in \mathbb{R}^r \times \mathbb{C}^s | |x_i| \leq c_i\}$$

$\operatorname{vol}(B(c)) = (2c_1)\cdots(2c_r)(2\pi c_{r+1}^2)\cdots(2\pi c_{r+s}^2) = 2^n(\frac{\pi}{2})^s c_1 \cdots c_r c_{r+1}^2 \cdots c_{r+s}^2 = 2^n(\frac{\pi}{2})^s \xi$. Pick c such that $\operatorname{vol}(B(c)) = 2^n \operatorname{covol}(J)$, by Minkowski's theorem, $B(c) \cap J \setminus \{0\} \neq \varnothing$, pick $\alpha \in B(c) \cap J \setminus \{0\}$, $|N(\alpha)| = |\sigma_1(\alpha)| \cdots |\sigma_n(\alpha)| \leq \xi$, thus $N\alpha = NI \cdot NJ \leq \xi = (\frac{2}{\pi})^s \operatorname{covol} J = (\frac{2}{\pi})^s [\mathcal{O}_K : J]\sqrt{|D_K|}$, hence $NI \leq (\frac{2}{\pi})^s \sqrt{|D_K|}$ □

3 Dirichlet's unit theorem

Example 3.1. $K = \mathbb{Q}(\zeta_p)$, $p \nmid rs$, then $\dfrac{\zeta^r - 1}{\zeta^s - 1} \in \mathbb{Z}[\zeta]^\times$

Proposition 3.2. For $\alpha \in \mathcal{O}_K$, $\alpha \in \mathcal{O}_K^\times \Leftrightarrow N_{K/\mathbb{Q}}(\alpha) = \pm 1$

Proof. Let $f = x^m + \cdots + a_0$ be the charateristic polynomial of α, $N\alpha = a_0$, if $N\alpha = \pm 1$, then $g(x) = x^m + a_0^{-1}a_1x^{m-1} + \cdots + a_0^{-1}a_{m-1}x + a_0^{-1} \in \mathbb{Z}[x]$ has α^{-1} as a root, thus $\alpha \in \mathcal{O}_K^\times$ $\square$

Lemma 3.3. $\mu(K)$ is the set of roots of unity in K which is also the torsion subgroup of $\mathcal{O}_K^\times$. $\mu(K)$ is finite, hence cyclic, $\zeta_m \in K \Rightarrow \varphi(m) | [K : \mathbb{Q}] \Rightarrow$ only finitely many such m

Example 3.4. If $K \hookrightarrow \mathbb{R}$, then $\mu(K) = \{\pm 1\}$. If $K = \mathbb{Q}(\zeta_p)$, then $\mu(K) = \{\pm 1\} \times \langle \zeta_p \rangle$. If $K = \mathbb{Q}(\sqrt{d})$, $d < 0$, then $\zeta_m \in K \Rightarrow \varphi(m) \leq 2 \Rightarrow m = 2, 3, 4, 6$

Proposition 3.5. $\alpha \in \mathcal{O}_K$, $|\sigma(\alpha)| = 1$ for all $K \overset{\sigma}{\hookrightarrow} \mathbb{C}$, then $\alpha \in \mu(K)$

Proof. Fix $C, D > 0$

$$E_{C,D} = \{\beta \in \overline{\mathbb{Z}} | \deg(\beta) \leq C, |\sigma(\beta)| \leq D, \forall \mathbb{Q}(\beta) \overset{\sigma}{\hookrightarrow} \mathbb{C}\}$$

$f_\beta(x) \in \mathbb{Z}[x]$ is the monic irreducible polynomial of β. $\deg f_\beta \leq C \Rightarrow \deg f_\beta$ has finitely many choice and coefficients of f_β is bounded by function of $D \Rightarrow$ finitely many choices for $f_\beta \Rightarrow E_{C,D}$ is finite. $\alpha \in E_{n,1}$, $n = [K : \mathbb{Q}]$, $\alpha^2, \alpha^3, \cdots \in E_{n,1} \Rightarrow \alpha \in \mu(K)$ since $E_{n,1}$ is finite, α^n repeats $\square$

Definition 3.6. Define logarithm

$$\begin{aligned} \mathcal{L} : K_\mathbb{R}^\times = (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s &\to \mathbb{R}^{r+s} \\ (x_1, \cdots, x_{r+s}) &\mapsto (\log|x_1|, \cdots, \log|x_r|, 2\log|x_{r+1}|, \cdots, 2\log|x_{r+s}|) \end{aligned}$$

Note that $1 = |N_{K/\mathbb{Q}}(\alpha)| = |\sigma_1(\alpha)| \cdots |\sigma_r(\alpha)||\sigma_{r+1}(\alpha)||\overline{\sigma_{r+1}(\alpha)}| \cdots |\sigma_{r+s}(\alpha)||\overline{\sigma_{r+s}(\alpha)}|$, thus the image of α is contained in the hyperplane $H = \{a_1 + \cdots + a_{r+s} = 0\}$

Theorem 3.7. (i) $\ker \mathcal{L} = \mu(K) = \mathrm{Tor}(\mathcal{O}_K^\times)$

(ii) $\mathcal{L}(\mathcal{O}_K^\times)$ is a lattice in H

(iii) $\mathcal{O}_K^\times \cong \mathbb{Z}^{r+s-1} \times \mu(K)$, $\mathcal{O}_K^\times$ is finitely generated

Proof. $\mathbb{C} \xrightarrow{|\cdot|} \mathbb{R}_{>0}$ is a homomorphism, compact $\Leftrightarrow$ image compact, $\mathbb{C}^\times \cong U(1) \times \mathbb{R}^\times$, $\log : \mathbb{R}_{>0} \to \mathbb{R}$, compact $\Leftrightarrow$ image compact

$$\begin{tikzcd} \mathcal{O}_K^\times \arrow[r, hook] & K_\mathbb{R}^\times \cong (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s \arrow[r, hook, "\mathcal{L}"] \arrow[d, hook] & \mathbb{R}^r \times \mathbb{R}^s \\ \mathcal{O}_K \arrow[r, hook] & K_\mathbb{R} \cong \mathbb{R}^r \times \mathbb{C}^s & \end{tikzcd}$$

Show $\mathcal{L}(\mathcal{O}_K^\times)$ is discrete in $\mathbb{R}^r \times \mathbb{R}^s$, $\Rightarrow \mathrm{rank}_\mathbb{Z}\, \mathcal{O}_K^\times \leq r + s$. Let $B \subseteq \mathbb{R}^r \times \mathbb{R}^s$ be open bounded, $\mathcal{L}(\mathcal{O}_K^\times) \cap B$ is finite since $\mathcal{L}^{-1}(B)$ is open bounded in $K_\mathbb{R} \Rightarrow \mathcal{L}^{-1}(B) \cap \mathcal{O}_K$ is finite $\Rightarrow \mathcal{L}^{-1}(B) \cap \mathcal{O}_K^\times$ is finite $\Rightarrow \mathcal{L}(\mathcal{O}_K^\times) \cap B$ is finite. Two lattices, $\mathcal{O}_K$ is an additive group scheme, $\mathcal{O}_K^\times$ is a multiplicative group scheme $\square$

References

Index