7

2021年8月16日 12:03

代数数论中的有限性

$$h_K = |Cl(K)| < +\infty$$

理想范

L/K $\quad N_{L/K}(\alpha) = \left(\prod_i \sigma_i(\alpha)\right) \in K$

? 用于: $N_{L/K} : I(L) \to I(K)$

$$\begin{array}{ccc} L^* & \longrightarrow & I(L) \\ N\downarrow & \circlearrowright & \downarrow N \\ K^* & \longrightarrow & I(K) \end{array}$$

$n = [L:K] = \sum e_i f_i$

$p \subset O_K$

$pO_L = \mathfrak{P}_1^{e_1} \mathfrak{P}_2^{e_2} \cdots \mathfrak{P}_r^{e_r}$

若 $p = \pi O_K = (\pi)$

应有 $N(pO_L) = N(\pi) O_K = \pi^n \cdot O_K = p^n$

$N(\prod \mathfrak{P}_i^{e_i}) = \prod N(\mathfrak{P}_i)^{e_i}$

应定义 $N(\mathfrak{P}_i) = p^{f_i}$

引定义(略) ↳ 的确使上图交换

$\forall\ \mathfrak{P} \subset O_L \quad p = \mathfrak{P} \cap O_K$

$f = f(\mathfrak{P}/p) = [O_L/\mathfrak{P} : O_K/p]$

$$N_{L/K}(\mathfrak{P}) := p^f$$

Prop $M/L/K$ $\quad I$ 是 M 的分式理想

$$N_{L/K}(N_{M/L}(I)) = N_{M/K}(I)$$

Prop L/K $[L:K] = n$ 那么

(1) $I \subset O_K$ 理想 则 $N_{L/K}(I \cdot O_L) = I^n$

(2) L/K Galois扩张, $\mathfrak{P} \subset O_L$ 素理想 $p = \mathfrak{P} \cap O_K$

(2) L/K Galois 扩张 $\mathfrak{B} \subset \mathcal{O}_L$ 素理想, $\mathfrak{p} = \mathfrak{B} \cap \mathcal{O}_K$

(Galois $\Rightarrow e_i = e$, $f_i = f$) $\mathfrak{p}\mathcal{O}_L = \mathfrak{B}_1^e \cdots \mathfrak{B}_g^e$

则有 $N_{L/K}(\mathfrak{B}) \cdot \mathcal{O}_L = (\mathfrak{B}_1 \cdots \mathfrak{B}_g)^{ef} = \sum_{\sigma \in Gal(L/K)} \sigma\mathfrak{B}$

数值范

当考虑理想范时. L/K, $K = \mathbb{Q}$ $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ PID

整理想只剩 $\{\pm 1\} = \mathbb{Z}^\times$

$K/\mathbb{Q}$ $0 \neq I \subset \mathcal{O}_K$ $\overset{Lem}{\Rightarrow} [\mathcal{O}_K : I] \overset{\in \mathbb{Z}}{< +\infty}$

记 $N(I) = [\mathcal{O}_K : I]$ 数值范.

Prop (1) $0 \neq I \subset \mathcal{O}_K$ $(N(I)) = N_{K/\mathbb{Q}}(I)$

(2) $I, J \in I(K)$ $N(IJ) = N(I)N(J)$

若还有 $J \subset I$ $[I : J] = N(I^{-1}J)$ $(I^{-1}J = J/I.)$

$= N(J)/N(I)$

Th K 数域 $[K:\mathbb{Q}] = n = r + 2s$ $d_K \overset{\in \mathbb{Z}}{\neq} 0$

则 $Cl(K)$ 中每一个理想类都至少有一个整理想代表元 I s.t.

$$N(I) \leq \underbrace{\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s |d_K|^{\frac{1}{2}}}_{\text{Minkowski 常数}}$$

Minkowski 常数

Cor $Cl(K)$ 是有限群. $h_K = |Cl(K)| < +\infty$

证 只需证明 $\forall M \in \mathbb{N}$ $N(I) \leq M$ 的整理想为有限个.

$I = \prod \mathfrak{p}_i^{r_i}$ $N(I) = \prod \mathfrak{p}_i^{r_i f_i} < M$ 其中 $(p_i) = \mathfrak{p}_i \cap \mathbb{Z}$

$\Rightarrow \mathfrak{p}_i < M$ 为有限个

$\Rightarrow r_i$ 有界

$\Rightarrow$ I 为有限个可能. #

例 $K=\mathbb{Q}(i)$ $\mathcal{O}_K=\mathbb{Z}[i]$ PID/UFD

* 它是关于 $|\cdot|=|a+bi|=\sqrt{a^2+b^2}$ 的 Euclid 环.

* 用上述定理 $s=1, r=0, n=2, d_K=-4$

$N(I)\le \frac{2}{\pi}\left(\frac{\pi}{4}\right)^1 4^{\frac{1}{2}} < 1.27 \Rightarrow N(I)=1 \Rightarrow I=\mathcal{O}_K=(1)$ 得证.

例 $K=\mathbb{Q}(\sqrt{-5})$ $\mathcal{O}_K=\mathbb{Z}[\sqrt{-5}]$ $d_K=-20$ $n=2, s=1$ $r=0$.

不是PID. $Cl(K)\neq 1$

$\cong \mathbb{Z}/2\mathbb{Z}$

取 $c\in Cl(K)$ 非平凡理想类

I 是理想代表元

$1\le N(I)\le \frac{2}{\pi}\cdot\frac{4}{\pi}\sqrt{|-20|}<3 \Rightarrow N(I)=2$

$\Rightarrow I$ 素理想分解后因子为素理想 $\mathcal{O}_K$

$(2)=2\mathcal{O}_K=\mathfrak{p}^2$ 其中 $\mathfrak{p}=(2,1+\sqrt{-5}) \Rightarrow \mathfrak{p}\mid I$

$4=2^2=N(2)=N(\mathfrak{p}^2)=N(\mathfrak{p})^2 \Rightarrow N(\mathfrak{p})=2=N(I)$

$\|\mathcal{O}_K/\mathfrak{p}\| \quad \|\mathcal{O}_K/I\|$

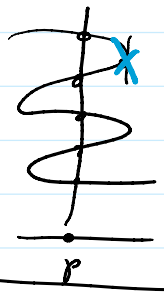
$\Rightarrow \mathfrak{p}=I$

$\Rightarrow |Cl(K)|=2 \Rightarrow Cl(K)\cong \mathbb{Z}/2\mathbb{Z}$

$\|$

$\langle c\rangle=\langle\mathfrak{p}\rangle$

Def L/K 称为非分歧扩张 (unramified) 若 $\forall \mathfrak{p}\subset\mathcal{O}_K$, $\mathfrak{p}\mathcal{O}_L=\prod \mathfrak{P}_i^{e_i}$ 分解中 $e_i=1$



Cor $K/\mathbb{Q}$ 非平凡有限扩张, 它必不是非分歧的.

Pf. p 分歧 $\Leftrightarrow p\mid d_K\in\mathbb{Z}$

$Cl(K) \ni I$

$1\le N(I)\le \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s\sqrt{|d_K|}$

$\frac{n!}{n^n}\left(\frac{\pi}{4}\right)^s \to n^{\frac{n}{2}}\left(\frac{\pi}{4}\right)^s \to n^{\frac{n}{2}}\left(\frac{\pi}{4}\right)^{\frac{n}{2}} \to \cdots$

$$1 \le |N(z)| = n^n \left(\frac{?}{?}\right) \sqrt{|d_K|}$$

$$\sqrt{|d_K|} \ge \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^s \underset{2s\le n}{\ge} \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{\frac{n}{2}} =: a_n$$

$a_2 > 1$ $\quad \frac{a_{n+1}}{a_n} = \sqrt{\frac{\pi}{4}}\underbrace{\left(1+\frac{1}{n}\right)^n}_{\le e} > 1$ $\quad a_n \uparrow \quad a_n > 1$

$\Rightarrow |d_K| > 1$

总 $\exists\, p \mid d_K$ $\quad p$ 在 O_K 上分歧 #

Rk 其他数域，存在非平凡非分歧扩张 L/K

类域论：$\forall K$ $\exists H/K$ Galois 扩张 非分歧，且

$Gal(H/K) \cong Cl(K)$ （当 $h_K \ne 1 \Rightarrow H/K$ 非平凡扩张）

H：称为 K 的 Hilbert 类域

例 $K = \mathbb{Q}(\sqrt{-5})$，$h_K \ne 1 \Rightarrow H = \mathbb{Q}(\sqrt{-5}, \sqrt{-1})$

"数的几何"

格 lattice

V：$\mathbb{R}$-向量空间 $\dim V = n$ $\quad \Lambda \subset V$ 加法子群

$\Lambda = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_r$

且 $(e_1, \cdots, e_r)$ 在 V 中 $\mathbb{R}$-线性无关

Def 此时 Λ 称为 V 中的格

若 $r = n$，称满格 full lattice.

$\mathbb{R} \otimes_{\mathbb{Z}} \Lambda \longrightarrow V$ 是 $\mathbb{R}$-向量空间同构

$\sum r_i \otimes e_i \longmapsto \sum r_i e_i$

例 $V = \mathbb{C} \cong \mathbb{R}^2$ $\quad e_1 = 1, e_2 = i$ $\quad \Lambda = \mathbb{Z}\cdot 1 \oplus \mathbb{Z} i \subset \mathbb{C}$ 满格

⚠ $\mathbb{Z} + \mathbb{Z}\sqrt{2} \subset \mathbb{R}$ 是自由加法子群，但不是 $\mathbb{R}$ 中格. $1, \sqrt{2}$ $\mathbb{R}$-线性相关.

* V 取定基，$V \cong \mathbb{R}^n$ 拓扑（与基取法无关）

Prop $\Lambda \subset V$，以下等价

Prop $\Lambda \subset V$. 以下等价

(1) Λ 是离散子群

(2) 存在 V 的开集 U. $\Lambda \cap U = \{0\}$

(3) 任何子集 $C \subset V$, $C \cap \Lambda$ 有限

(4) 任何有界子集 $B \subset V$, $B \cap \Lambda$ 有限.

Prop 子群 $\Lambda \subset V$ 是格 $\Leftrightarrow$ Λ 是离散子群.

例 $\mathbb{Z}[i] = \mathbb{Z} \oplus \mathbb{Z}i$ 是 $\mathbb{C} = \mathbb{R}^2$ 的格

$\mathbb{Z} + \mathbb{Z}\sqrt{2} \subset \mathbb{R}$ 不离散 $\frac{a}{b} \approx \sqrt{2} \Rightarrow a - b\sqrt{2} \approx 0$

$\mathbb{Z} + \mathbb{Z}\alpha \subset \mathbb{R}$

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

$\alpha \notin \mathbb{Q} \Rightarrow$ 不离散

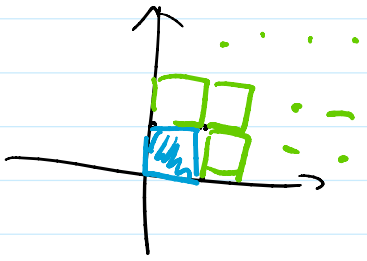
Def $\Lambda \subset V$ 满格. 称 $D = \{\lambda_0 + \sum a_i e_i \mid 0 \le a_i < 1\}$ 为一个

$\bigoplus_{i=1}^{n} \mathbb{Z}e_i$ 基本区域 / 基本平行六面体

fundamental domain.

它移动充全整地盖满 V.

$\mathbb{Z}[i] \subset \mathbb{C}$



定义 $\mu(\Lambda) = \mu(D) = |\det(e_1, \cdots e_n)| =$ D 的体积

若 Λ 换一组 $\mathbb{Z}$ 基 $(e_1, \cdots e_n) \rightsquigarrow (e_1', \cdots e_n')$

过渡阵 $P \in GL_n(\mathbb{Z})$ $\det P \in \mathbb{Z}^* = \pm 1$

$\Rightarrow \mu(\Lambda) = \mu(D)$ 不依赖于 $\mathbb{Z}$-基的选取.

对 V 的 $\Lambda \supset \Lambda'$ 两个满格 $[\Lambda : \Lambda'] = \frac{\mu(\Lambda')}{\mu(\Lambda)}$

Th Λ 满格. 取定一个 D_0 基本区域

则 $S \subset V$ 可测 且 $\mu(S) > \mu(D_0)$

$S \subset V \twoheadrightarrow V/\Lambda$

若 $S \subset V$ 可测 且 $\mu(S) > \mu(D_0)$

那么 $\exists\ \alpha \neq \beta \in S$ 使 $\alpha - \beta \in \Lambda$.

证 $\mu(S) = \sum_{\lambda \in \Lambda} \mu\left(S \cap (\lambda + D_0)\right)$

把 $S \cap (\lambda + D_0)$ 平移至 D_0 上

$\mu(S) > \mu(D_0) \Rightarrow$ 平移像 必有重叠.

即 $\exists\ \lambda \neq \lambda' \in \Lambda$ 及 $\alpha \in \lambda + D_0$, $\beta \in \lambda' + D_0$

$\alpha - \lambda = \beta - \lambda'$

$\Rightarrow \alpha - \beta \in \Lambda$. #

令 $T \subset V$ 满足:

$(**)$ $\alpha, \beta \in T \Rightarrow \frac{1}{2}(\alpha - \beta) \in T$

令 $S = \frac{1}{2}T$ 则 $\forall \alpha, \beta \in S \Rightarrow \alpha - \beta \in T$

Th $\Rightarrow$ 一定 $\mu(S) > \mu(D)$ 即 $T \cap \Lambda$ 至少包含一个非0元.

$\Uparrow$

$\frac{\mu(T)}{2^n} = \mu\left(\frac{1}{2}T\right) > \mu(D) \Leftrightarrow \mu(T) > 2^n \mu(D)$

Th (Minkowski) $T \subset V$ 是 凸, 中心对称 且 $\mu(T) \geq 2^n \mu(D)$

则 $T \cap \Lambda$ 包含一个非0元

证 说 中心对称 + 凸 $\Rightarrow T$ 满足 $(**)$

其次 $\forall \varepsilon > 0$ $(1+\varepsilon)T$ $\mu\left((1+\varepsilon)T\right) = (1+\varepsilon)^n \mu(T) \geq (1+\varepsilon)^n 2^n \mu(D) > 2^n \mu(D)$

于是 $\left((1+\varepsilon)T\right) \cap \Lambda$ 包含非0元

Λ 离散 $(1+1)T$ 是 $\Lambda \cap (1+1)T$ 有限集.

T 闭 $\Rightarrow T = \bigcap_{\varepsilon > 0} (1+\varepsilon)T$

若 $\Lambda \cap T = \{0\}$ 由于 $0 \in \Lambda \cap (1+\varepsilon)T$ 有限集

从可取出 $\varepsilon > 0$ $(1+\varepsilon)T$ 避开这有限个点

于是 $\Lambda \cap (1+\varepsilon)T = \{0\}$ 这与之前 矛盾

于是 $\Lambda \cap (1+\varepsilon)T = \{0\}$ 这与之前矛盾

于是 $T \cap \Lambda$ 的基一个非0元 #

回顾 V：$\mathbb{R}$-向量空间，$\|\cdot\| : V \to \mathbb{R}$ 称为范数，若

i) $\forall x \in V$ $\|x\| \geq 0$，"$=$" $\Leftrightarrow x = 0$.

ii) $\|rx\| = |r| \cdot \|x\|$

iii) $\|x+y\| \leq \|x\| + \|y\|$

$V = \mathbb{R}^r \times \mathbb{C}^s$ $\dim V = n = r+2s$

$\vec{x} = (x_1, \cdots, x_r, z_{r+1}, \cdots, z_{r+s})$

$\|x\| = \sum_{i=1}^{r} |x_i| + 2\sum_{i=r+1}^{r+s} |z_i|$ 是 V 上的范数.

Lem $\forall\, t \in \mathbb{R}^+$ $X(t) = \{ x \in V \mid \|x\| \leq t \}$

则体积 $\mu(X(t)) = 2^r \left(\frac{\pi}{2}\right)^s \frac{t^n}{n!}$

K，$[K:\mathbb{Q}] = n = r+2s$

$\sigma_1, \cdots, \sigma_r$ 实嵌入 $\sigma_{r+1}, \overline{\sigma_{r+1}}, \cdots, \sigma_{r+s}, \overline{\sigma_{r+s}}$ 对复嵌入.

$$\sigma : K \longrightarrow V = \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^n$$
$$\alpha \longmapsto (\sigma_1\alpha, \cdots, \sigma_{r+s}\alpha)$$

$\mathbb{C} \cong \mathbb{R} \oplus \mathbb{R}$:

Prop of $I \subset \mathcal{O}_K$ 则 $\sigma(I) \subset V$ 是一个满格，且

$$\mu(\sigma(I)) = 2^{-s} N(I) |d_K|^{\frac{1}{2}}$$

Pf $0 \neq \alpha \in I$ $(\alpha) = \alpha\mathcal{O}_K \subset I \subset \mathcal{O}_K$

作为加群同构 $\alpha\mathcal{O}_K \cong \mathcal{O}_K \cong \mathbb{Z}^n$

$\Rightarrow$ I 也必是秩 n 的自由加群

取一组 $\alpha_1, \cdots, \alpha_n$，$\sigma(I)$ 是 V 中满格 $\Leftrightarrow$

$\sigma(\alpha_1), \cdots, \sigma(\alpha_n)$ 是 $\mathbb{R}$-线性无关

$\Leftrightarrow$ 以下行列式 $\det \neq 0$

$\sigma(\alpha_1), \cdots, \sigma(\alpha_n)$ 是 $\mathbb{R}$-线性无关

$\Leftrightarrow$ 以下的 A, $\det A \neq 0$. $A \in M_n(\mathbb{R})$

A 的第 i 行 $\left(\sigma_1(\alpha_i), \cdots, \sigma_r(\alpha_i), \mathrm{Re}(\sigma_{r+1}\alpha_i), \mathrm{Im}(\sigma_{r+1}\alpha_i), \cdots, \mathrm{Re}(\sigma_{r+s}\alpha_i), \mathrm{Im}(\sigma_{r+s}\alpha_i)\right)$

先算 B, $\det B$ $\quad B \in M_n(\mathbb{C})$

B 第 i 行 $\left(\sigma_1(\alpha_i), \cdots, \sigma_r(\alpha_i), \sigma_{r+1}(\alpha_i), \overline{\sigma_{r+1}(\alpha_i)}, \cdots, \sigma_{r+s}(\alpha_i), \overline{\sigma_{r+s}(\alpha_i)}\right)$

$(\det B)^2 = \mathrm{disc}(\alpha_1, \cdots, \alpha_n) \neq 0$ $\quad (\alpha_1, \cdots, \alpha_n : \mathbb{Z}\text{-线性无关} \Rightarrow \mathbb{Q}\text{-}\cdots)$

A 与 B 关系:

① 把 B 的 $r+2$ 列加到 $r+1$ 列上.

② $r+2$ 列减去 $r+1$ 列的 $\frac{1}{2}$

③ $r+1$ 列 $/2$

④ $r+2$ 列 $/(-i)$

$\Rightarrow$ 得 A 的 $r+1$ 列, $r+2$ 列

$\det B = (-2i)^s \det A \Rightarrow \det A \neq 0.$

再计算 $\mu(\sigma(I)) = |\det A|$

$\mu(\sigma(I))^2 = (\det A)^2 = (-2i)^{-2s} \mathrm{disc}(\alpha_1, \cdots, \alpha_n)$ ①

对 $J = \mathcal{O}_K \subseteq \mathcal{O}_K$ 整基 $\gamma_1, \cdots, \gamma_n$ 有:

$\mu(\sigma(\mathcal{O}_K))^2 = (-2i)^{-2s} \mathrm{disc}(\gamma_1, \cdots, \gamma_n) = (-2i)^{-2s} d_K$ ②

$I \subset J = \mathcal{O}_K$ $\quad [\mathcal{O}_K : I] = [\sigma(\mathcal{O}_K) : \sigma(I)] = \dfrac{\mu(\sigma(I))}{\mu(\sigma(\mathcal{O}_K))}$ ③

① ② ③ $\Rightarrow |\mathrm{disc}(\alpha_1, \cdots, \alpha_n)| = [\mathcal{O}_K : I]^2 \cdot |d_K| = N(I)^2 |d_K|$

在①中取绝对值开平方, $\Rightarrow$ $\mu(\sigma(I)) = 2^{-s} |\mathrm{disc}(\alpha_1, \cdots, \alpha_n)|^{\frac{1}{2}}$

$= N(I) \cdot |d_K|^{\frac{1}{2}} \cdot 2^{-s}$ #

Prop 对于 $I \subset \mathcal{O}_K$, 那么 I 包含 $\alpha \in K^*$ 使得

$|N(\alpha)| \leq \left(\frac{4}{\pi}\right)^s N(I) |d_K|^{\frac{1}{2}}$

Prop 对于 $I \subset O_K$，那么 I 包含 $\alpha \in K^*$ 使

$$|N_{K/\mathbb{Q}}(\alpha)| \le \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} |d_K|^{\frac{1}{2}} N(I)$$

Pf. 令 D 为 $\sigma(I) \subset V$ 的一个基本区域.

$X(t) = \{x \in V \mid \|x\| \le t\}$ 中心对称. 凸. 紧

一旦 t 使得 $\mu(X(t)) \ge 2^n \mu(D)$ $\left(\text{即 } 2^r \left(\frac{\pi}{2}\right)^s \frac{t^n}{n!} \ge 2^n \mu(D), \text{ 即 } t^n \ge n! \frac{2^{n-r}}{\pi^s} |d_K|^{\frac{1}{2}} \cdot N(I)\right)$

$2^{-s} \cdot 2^n |d_K|^{\frac{1}{2}} N(I)$

则有 $X(t)$ 包含 $\sigma(I)$ 的一个非 0 元. $\sigma(\alpha)$ $(\alpha \in I, \alpha \neq 0)$

对于 $\alpha \in I$ $\sigma(\alpha) \in X(t)$ $\|\sigma(\alpha)\| \le t$

$$|N_{K/\mathbb{Q}}(\alpha)| = |\sigma_1(\alpha) \cdots \sigma_r(\alpha) \sigma_{r+1}(\alpha) \overline{\sigma_{r+1}(\alpha)} \cdots \sigma_{r+s}(\alpha) \overline{\sigma_{r+s}(\alpha)}|$$

$$= |\sigma_1(\alpha)| \cdots |\sigma_r(\alpha)| \cdot |\sigma_{r+1}(\alpha)|^2 \cdots |\sigma_{r+s}(\alpha)|^2$$

几何均值 $\le$ 算术均值

$$\le \left(\frac{\sum_{i=1}^{r} |\sigma_i(\alpha)| + \sum_{i=r+1}^{r+s} 2|\sigma_{r+i}(\alpha)|}{n}\right)^n \le \left(\frac{t}{n}\right)^n$$

取右边 t^n 正好是 $n! \frac{2^{n-r}}{\pi^s} |d_K|^{\frac{1}{2}} N(I)$ 代入得:

$$|N_{K/\mathbb{Q}}(\alpha)| \le \frac{n!}{n^n} \frac{2^{n-r}}{\pi^s} N(I) |d_K|^{\frac{1}{2}}$$

$$\ge \left(\frac{4}{\pi}\right)^s$$

#

Th $Cl(K)$ 中每一个类都有一个整理想代表 I 使得

$$N(I) \le \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s |d_K|^{\frac{1}{2}}$$

Pf $c \in I(K)$ $c^{-1} \in I(K)$

$\exists d \in K^*$ $J = d \cdot c^{-1}$ 整理想.

由 Prop. $\exists 0 \neq \beta \in J$ 使

由 Prop. $\exists\ 0\neq\beta\in J$ 使

$$|N_{K/\mathbb{Q}}(\beta)| \le \underbrace{\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s |d_K|^{\frac{1}{2}}}_{B_K} \cdot N(J)$$

$(\beta) = \beta\mathcal{O}_K \subset J$ $\quad J \mid (\beta)$ $\exists\ I \subset \mathcal{O}_K$ s.t. $IJ = (\beta)$

$I \sim J^{-1} \sim \mathcal{C}$

则 $N(I)N(J) = N(\beta) = |N_{K/\mathbb{Q}}(\beta)| \le B_K N(J)$ #

其他有限性定理

Th (Hermite) 固定 $d\in\mathbb{Z}$. 则只有有限个数域 K 使 $d_K = d$.

Th (Dirichlet 单位定理) K 数域 $r = [K:\mathbb{Q}] = r+2s$

那么 $\mathcal{O}_K^\times$ 是有限生成 Abel 群 $\mathcal{O}_K^\times = T \oplus \mathbb{Z}^m$

其中 T : torsion $= \mu(K)$ 有限群

秩 $m = r+s-1$

即 $\mathcal{O}_K^\times \hookrightarrow \mathbb{R}^{r+s}$ 说明它嵌入一个矩阵之中成为一个离散.