2021年8月13日 11:53

$\mathcal{O}_K$ 的唯一分解性质

motivation: $K=\mathbb{Q}$

$\mathcal{O}_K=\mathbb{Z}$ PID, UFD

$K=\mathbb{Q}(\sqrt{-5})$ $\mathcal{O}_K=\mathbb{Z}[\sqrt{-5}]$ 不是 UFD

$6=\overset{c}{2}\times\overset{d}{3}=\overset{e}{(1+\sqrt{-5})}\overset{f}{(1-\sqrt{-5})}$

2 不约: $2=ab$ $a=a_1+a_2\sqrt{-5}$, $b=b_1+b_2\sqrt{-5}\in\mathcal{O}_K$

$4=N(2)=N(a)N(b)$ $\in\mathbb{Z}$

$\Rightarrow N(a)=\pm 2 \Leftrightarrow N(a_1+a_2\sqrt{-5})=(a_1+a_2\sqrt{-5})(a_1-a_2\sqrt{-5})$ $\pm 2=$

$=a_1^2+5a_2^2$, $a_i\in\mathbb{Z}$

$N(a)=\pm 1 \Leftrightarrow a=\pm 1\in\mathcal{O}_K^\times$

对 $u\in\mathcal{O}_K^\times$ $c=eu$ ……

一般 $\mathcal{O}_K$ 不是 UFD

补救/理想: 找一个合适的框架, 唯一分解性:

理想和分解

Noether 环: R 交换幺环

Def 称 R 为 Noether 环, 如果它的每个理想是有限生成(作为 R-模)

例 PID ✓

K 或 $K[x]$ ✓

$K[x_1,x_2,\cdots,x_n]$ ✓

$\mathbb{Q}[x_1,x_2,\cdots,x_n,\cdots]$ ✗ $(x_1,x_2,\cdots)=\mathbb{Z}$

$\cap$

$\mathbb{Q}(x_1,x_2,\cdots,x_n,\cdots)$ ✓

Lem 以下等价

1) R Noether 环.

2) $I_1\subseteq I_2\subseteq\cdots\subseteq I_n\subseteq\cdots$ R 中理想升链必稳定

(1) R Noether 环.

(2) $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ R 中理想升链必稳定

$\exists N$ $\forall n > N$ $I_n = I_{n+1} = I_{n+2} = \cdots$

(3) $\Phi \neq \Sigma$ 是 R 中若干理想的集合. 则 Σ 存在极大元

证 (1) $\Rightarrow$ (2) $I = \bigcup_{i=1}^{\infty} I_{n_i} \subset R$ 理想, 有限生成 $I = (x_1, \cdots, x_m)$

$\forall j$ $\exists n_j$ $x_j \in I_{n_j}$ $n_0 = \max(n_j)$

$1 \le j \le m$

$\forall j$ $x_j \in I_{n_0}$, $\cup I_i \subset I \subset I_{n_0} \Rightarrow I_{n_0} = I_{n_0+1} = \cdots$

(2) $\Rightarrow$ (3) 反证法. 设 $\Phi \neq \Sigma$ 无极大元.

$\exists I_1 \in \Sigma$ $\exists I_2 \in \Sigma$ $I_1 \subsetneq I_2$

$\exists I_3 \cdots$ $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$ 不稳定序列.

(3) $\Rightarrow$ (1) 设 I 不是有限生成 $\Rightarrow I \neq 0$

$\exists x_1 \in I$ $I_1 = (x_1) \subsetneq I$

$\exists x_2 \in I \setminus I_1$ $I_2 = (x_1, x_2) \subsetneq I$

$\exists x_3 \cdots$ I_3

$\Phi \neq \Sigma = \{I_1, I_2, I_3 \cdots\}$ 无极大元 #

Dedekind 整环

Def 整环 R 称为 Dedekind 整环 若:

(1) R Noether 环.

(2) R 整闭 (无重根)

(3) R 中非 0 素理想均是极大理想 (1维性质)

Lem 一例 PID 是 Dedekind 整环.

证 (1) √ (2) 与"$\mathbb{Z}$ 在 $\mathbb{Q}$ 中整闭"证明一样, UFD

(3) $I \neq 0$ 素 $I = (a)$ $a \neq 0$ easy. a 必是不可约元

$I' \supset I$

$(a') \quad (a)$

$a \in I'$ $\exists b \in R$ $a = a'b \Rightarrow a'与b$ 之一为单位.

若 $a' \in R^\times$ $I' = (a') = R$

若 $b \in R^\times$ $I = (a) = (a) = I'$

从而 I 是极大理想 #

Th Dedekind 整环 R 中每个非 0 理想可以写成 R 有限个非 0 素理想的乘积. $I = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_n^{\alpha_n}$

Th Dedekind整环 R 中每个非0理想 $I \subsetneq R$ 总可以唯一写成非0素理想的乘积，$I = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_n^{\alpha_n}$

Lem R Noether整不，$0 \neq I \subsetneq R$，则存在有限个非0素理想 $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ 使 $I \supset \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_n$

Pf 令 Σ 为不具备上述性质的那些真理想的集合。要证 $\Sigma = \emptyset$
反证法，若 $\Sigma \neq \emptyset$，则有极大元 $M \in \Sigma$ $0 \subsetneq M \subsetneq R$.

M 不是素理想 $\exists\ r, s$ $rs \in M$ $r \notin M$, $s \notin M$

$M + (r) \supsetneq M$, $M + (s) \supsetneq M$. $(M + (r))(M + (s)) \subset M$

$M \neq R$ M 在 Σ 中极大 $\Rightarrow M + (r) \notin \Sigma$

$\exists \mathfrak{p}_1, \cdots, \mathfrak{p}_k$ 素. $M + (r) \supset \mathfrak{p}_1 \cdots \mathfrak{p}_k$
同理 $\exists \mathfrak{q}_1, \cdots, \mathfrak{q}_h$ $M + (s) \supset \mathfrak{q}_1 \cdots \mathfrak{q}_h$
$\Rightarrow \mathfrak{p}_1 \cdots \mathfrak{p}_k \mathfrak{q}_1 \cdots \mathfrak{q}_h \subset (M + (r))(M + (s)) \subset M$.
与 $M \in \Sigma$ 矛盾 #

Lem R Dedekind. $K = \mathrm{Frac} R$ $I \subsetneq R$ 理想
那么 $\exists\ \gamma \in K \setminus R$ 使 $\gamma I \subset R$.

Pf $I = 0$ ✓, $I \neq 0$ $0 \neq a \in I$, $0 \neq (a) \subsetneq R$

令 r 为 $(a) \supset \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r$ 式中的最小的 $r \in \mathbb{N}$

(Zorn引理) $\exists$ 极大理想 $M \supset I \supset (a) \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$

exer M 素 $M \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r \Longrightarrow \exists i$ $M \supseteq \mathfrak{p}_i$

不妨设 $M \supseteq \mathfrak{p}_1 \neq 0$ $\mathfrak{p}_1$ 为极大理想.
$\Rightarrow M = \mathfrak{p}_1$

r 最小性 $\Rightarrow \mathfrak{p}_2 \mathfrak{p}_3 \cdots \mathfrak{p}_r \notin (a)$
即 $\exists\ b \in \mathfrak{p}_2 \mathfrak{p}_3 \cdots \mathfrak{p}_r$ 但 $b \notin (a)$
令 $\gamma = \frac{b}{a} \in K \setminus R$
$bI \subset bM = b\mathfrak{p}_1 \subset \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r \subset (a) \Rightarrow \gamma I = \frac{b}{a} I \subset R$. #

Lem R Dedekind, $I \subset R$
则 $\exists\ J \subset R$ 使 IJ 为主理想
Pf $I = 0$ ✓ $0 \neq \alpha \in I \neq 0$ $\alpha \in R \subset \mathrm{Frac} R = K$

$J := \{\beta \in R \mid \beta I \subseteq (\alpha)\} \subset R$ 理想 $IJ \subseteq (\alpha)$

$J := \{\beta \in R \mid \beta I \subseteq (\alpha)\} \subset R$ 理想　　$IJ \subseteq (\alpha)$

记: $A = \frac{1}{\alpha} IJ \subseteq R$ 理想

存在性 $\forall A \subsetneq R$　上述 $\exists \gamma \in K \setminus R$　$\gamma A \subset R$

$\forall \alpha \in I \Rightarrow A = \frac{1}{\alpha} IJ \supseteq J$　　$\gamma J \in \gamma A \subseteq R$

$\forall \beta \in J$　$\gamma\beta \in R$ 且 $\gamma\beta I \subseteq \gamma J I = \gamma \alpha A \subseteq (\alpha)$

($A = \frac{1}{\alpha} IJ$, $\gamma A \subset R$)

$\gamma\beta I \subset (\alpha) \xRightarrow{J\text{定义}} \gamma\beta \in J$ 于是 $\gamma J \subset J$

R Noether $\Rightarrow J$ 有限生成　$J = (\alpha_1, \cdots, \alpha_m)$　$\alpha \neq 0$

$\gamma \alpha_i \in J$

$\exists M \in Mat_{m\times m}(R)$　$\gamma \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} = M \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix}$　　$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} \neq 0$

$\Rightarrow \det(\gamma I_m - M) = 0$

即 γ 是 $\det(xI_m - M) \in R[x]$ 的根

$\Rightarrow \gamma$ 在 R 上整，R 整闭 $\Rightarrow \gamma \in R$ 与 $\gamma \in K \setminus R$ 矛盾 #

lem (消去律) R Dedekind, I_1, I_2, J 理想, $I_1 J = I_2 J \Rightarrow I_1 = I_2$

证 取 J' 使 $JJ' = (\alpha)$ 主理想

$I_1 J J' = I_2 J J' \Rightarrow I_1 \cdot \alpha = I_2 \cdot \alpha$

$\xRightarrow[R\text{整环}]{} I_1 = I_2$　#

(⇒ 给理想得到极小生成)

lem R Dedekind. $I \supset J \Leftrightarrow \exists I'$　$II' = J$

(后证时称 $I|J$ 序关系)

证 $\Leftarrow$ √

$\Rightarrow$: 取 I_0 使 $II_0 = (\alpha)$

$(\alpha) = II_0 \supset JI_0$

$\Rightarrow$: 取 I_0 使 $II_0=(\alpha)$

$(\alpha)=II_0\supset JI_0$

$R\supseteq \frac{1}{\alpha}I_0J=I'$ 理想, $II'=\frac{1}{\alpha}II_0J=J$ #

主理想证明

存在性 $\Sigma=\{I\neq 0, I\subsetneq R, I$ 不可写成两个真理想之积$\}$

希望说明 $\Sigma=\phi$

否则, $\Sigma\neq\phi$ $\xrightarrow{\text{Noether}}$ Σ 有极大元 $M\in\Sigma, 0\neq M\subsetneq R$

(Zorn引理) $\Rightarrow$ $M\subset P$, $M\in\Sigma$ $M\neq P$

$M\subsetneq P$

Lem $\Rightarrow \exists I$ $M=PI\subsetneq I$ ("$\subsetneq$"由假设得)

$M\in\Sigma$ 极大 $\Rightarrow I\notin\Sigma$ $\left.\begin{matrix}M\subsetneq P\\ M=PI\end{matrix}\right\}\Rightarrow I\neq R$

$I=P_1\cdots P_s$, $M=PI=PP_1\cdots P_s$ 这与 $M\in\Sigma$ 矛盾

唯一性: $I=P_1\cdots P_r=Q_1\cdots Q_s$

$P_1\supseteq P_1\cdots P_r=I=Q_1\cdots Q_s \Rightarrow P_1\supseteq Q_j$

不妨设 $P_1\supseteq Q_1$

$\overset{\text{极大理想}}{\Rightarrow}$ $P_1=Q_1$, 消去律 + 归纳法 #

Rk (easy). 与之类似

$I=\mathfrak{p}_1^{r_1}\cdots\mathfrak{p}_s^{r_s}$ $m_i=\min(r_i,t_i)$

$J=\mathfrak{p}_1^{t_1}\cdots\mathfrak{p}_s^{t_s}$ $M_i=\max(r_i,t_i)$

$I\cap J=\mathfrak{p}_1^{m_1}\cdots\mathfrak{p}_s^{m_s}$ $I+J=\{\alpha+\beta\mid\alpha\in I,\beta\in J\}$

$=\mathfrak{p}_1^{M_1}\cdots\mathfrak{p}_s^{M_s}$

Prop R: Dedekind整环, R 是PID $\Leftrightarrow$ R 是UFD

证略.

实际中的Dedekind整环

数论中的 Dedekind 整环

Th K 数域，则 $\mathcal{O}_K$ 是 Dedekind 整环.

证 (1) $\mathcal{O}_K \cong \mathbb{Z}^n$ 作为 Abel 群

对于 $I \subset \mathcal{O}_K$ 也是有限 Abel 群 $I = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_s$

$\forall \alpha \in I \quad \alpha = \sum a_i \alpha_i \quad a_i \in \mathbb{Z} \subset \mathcal{O}_K$

即 $I = (\alpha_1, \cdots, \alpha_s)$ 即 $\mathcal{O}_K$ Noether ✓.

(2) 整闭：设 $\alpha \in K$ 在 $\mathcal{O}_K$ 上整

$\exists\ f = x^n + c_1 x^{n-1} + \cdots + c_n \in \mathcal{O}_K[x] \quad f(\alpha) = 0$

$R = \mathbb{Z}[c_1, \cdots, c_n] \subset \mathcal{O}_K$ 作为 Abel 群有限生成.

$R = \mathbb{Z}r_1 + \cdots + \mathbb{Z}r_s$

$f(\alpha) = 0$ + 归纳法 $\Rightarrow \forall r \geq 1$ α^r 是 $1, \alpha, \cdots, \alpha^{n-1}$ 的 R-线性组合.

$\mathbb{Z}[c_1, \cdots, c_n, \alpha] = R[\alpha] = R\cdot 1 + R\cdot\alpha + \cdots + R\cdot\alpha^{n-1}$

$= (\mathbb{Z}r_1 + \cdots + \mathbb{Z}r_s) + (\mathbb{Z}r_1\alpha + \cdots \mathbb{Z}r_s\alpha) + \cdots +$

从而 α 包含于一个有限生成的 $\mathbb{Z}$-模中，它在 $\mathbb{Z}$ 上整 $\Rightarrow \alpha \in \mathcal{O}_K$

(3) $0 \subsetneq P \subsetneq \mathcal{O}_K \quad 0 \neq \alpha \in P \quad 0 \neq m = N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$

$m/\alpha =$ α 的其他所有共轭之积，在 $\mathbb{Z}$ 上整

$m/\alpha \in K \Rightarrow m/\alpha \in \mathcal{O}_K$，于是 $m = \alpha \cdot (m/\alpha) \in P$

$(m) \subset P$

$\mathcal{O}_K$ 取基 $w_1, \cdots w_n$

$\mathcal{O}_K = \mathbb{Z}w_1 \oplus \cdots \oplus \mathbb{Z}w_n$

$\mathcal{O}_K/m\mathcal{O}_K = (\mathbb{Z}w_1 \oplus \cdots \oplus \mathbb{Z}w_n) / (\mathbb{Z}mw_1 \oplus \cdots \oplus \mathbb{Z}mw_n) \cong (\mathbb{Z}/m\mathbb{Z})^n$ 有限.

$(m) \subset P \Rightarrow \mathcal{O}_K/P$ 也是有限

(exer) 有限整环必是域

从而 P 是极大理想 #

Exer）证明商环为域

从而 P 是极大理想。 #

例 $K=\mathbb{Q}(\sqrt{-5})$ $\quad O_K=\mathbb{Z}[\sqrt{-5}]$ 不是 UFD（$\Leftrightarrow$ 不是 PID）

$$6=2\times 3=(1+\sqrt{-5})(1-\sqrt{-5}) \quad \text{不唯一}$$

$$(6)=(2)(3)=(1+\sqrt{-5})(1-\sqrt{-5})$$

均不是素理想，还可以再细分解

$$(2,1+\sqrt{-5})^2=(2^2,\ 2(1+\sqrt{-5}),\ (1+\sqrt{-5})^2)$$

$$=(4,\ 2+2\sqrt{-5},\ -4+2\sqrt{-5})=(2)$$

["$\subset$"：$2\mid 4,\ 2\mid 2+2\sqrt{-5},\ 2\mid -4+2\sqrt{-5}$

"$\supset$"：$2=(2+2\sqrt{-5})-4-(-4+2\sqrt{-5})$]

同理 $(3)=(3,1+\sqrt{-5})(3,1-\sqrt{-5})$

$$(6)=(2)(3)=(2,1+\sqrt{-5})(2,1+\sqrt{-5})(3,1+\sqrt{-5})(3,1-\sqrt{-5})$$

$$=(1-\sqrt{-5})(1+\sqrt{-5})$$

Exer 验证 $\mathbb{Z}[\sqrt{-5}]/(2,1+\sqrt{-5})\cong\mathbb{F}_2$

$\mathbb{Z}[\sqrt{-5}]/(3,1\pm\sqrt{-5})\cong\mathbb{F}_3$

Rk $L/K \quad O_L/O_K \quad \mathfrak{p}\subset O_K$

$$I=\mathfrak{p}O_L\subset O_L$$
$$=\mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_r^{e_r}$$

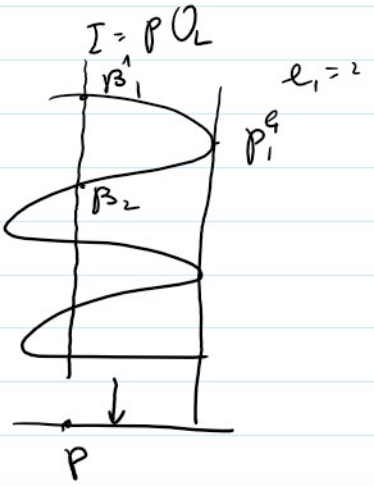
$$O_K\hookrightarrow O_L \leadsto O_K/\mathfrak{p}\longrightarrow O_L/\mathfrak{P}_i$$

$$f_i=[O_L/\mathfrak{P}_i : O_K/\mathfrak{p}]$$

则 $n=[L:K]=\sum e_i f_i$ ……

$\mathfrak{p}_i = \mathfrak{P}_i \cap \mathcal{O}_K = \mathfrak{P}_i^{e_i} \cap \mathcal{O}_K$

Th $n = [L:K] = \sum_{i=1}^{r} e_i f_i$



几何意义 $\operatorname{Spec} \mathcal{O}_L$ 由性之间

$\varphi \downarrow \deg(\varphi) = n$

$\operatorname{Spec} \mathcal{O}_K$

$e=1$ 非分歧

$e>1$ 分歧.

Th K $d_K \in \mathbb{Z}$ discriminant

p 在 K 中分歧 $\Leftrightarrow$ $p \mid d_K$

Rk 当 $K = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f)$ 且 $\mathcal{O}_K = \mathbb{Z}[\alpha]$

$$d_K = d_{K/\mathbb{Q}}(1, \alpha, \alpha^2, \cdots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(f'(\alpha)) \in \mathbb{Z}$$

$p \mid d_K \approx f'(\alpha) \equiv 0 \pmod{p}$

即 $\alpha \bmod p$ 是重根

分式理想

$\mathbb{N} = \{0, 1, 2, \cdots\}$ $(\mathbb{N}, +)$ 幺半群

类比 $a - b$ $(a, b \in \mathbb{N})$ 加入负得出一个群 $(\mathbb{Z}, +)$

R Dedekind 整环.

$0 \neq I = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r}$ $\alpha_i \in \mathbb{N}$

$\{R$ 的非0理想$\}$ 幺半群 幺元 R. $I \cdot R = I$

允许 $\alpha_i \in \mathbb{Z} \rightsquigarrow$ $\{$分式理想$\}$ 群.

$\frac{I}{J}$

Def $I \subset K$ 子集 称为 K 的分式理想 若 $\exists\, 0 \neq \mu \in \mathcal{O}_K$

Def $I \subset K$ 是称为 K 的分式理想 若 $\exists\, 0\neq\mu\in\mathcal{O}_K$

使得 $\mu I \subset \mathcal{O}_K$ 为 $\mathcal{O}_K$ 的理想。

$I(K)=\{K\text{的分式理想}\} \supset I^{\circ}(K)=\{\underbrace{\mathcal{O}_K\text{的非}0\text{理想}}_{\text{整理想}}\}$

记 $A=\mu I$ 为理想 $\quad I=\frac{1}{\mu}A=\{\frac{a}{\mu}\mid a\in A\}$

$A\cdot B=\{\sum_{i=1}^{n} a_i b_i \mid a_i\in A,\ b_i\in B\}$

$\alpha,\beta\in\mathcal{O}_K$ A',B' 理想 $A=\frac{1}{\alpha}A'$, $B=\frac{1}{\beta}B'$

$A\cdot B=\frac{1}{\alpha\beta}\cdot A'\cdot B'$ 仍是分式理想

$\rightsquigarrow (I(K),\cdot)$ 交换幺半群, 幺元 $\mathcal{O}_K$

Th (1) $I(K)$ 关于 $\cdot$ 成Abel群, $I^{\circ}(K)$ 非群

(2) $\forall I\in I(K)$ 可分式两个整理想之商 $I=\frac{A}{B}$, $A,B\in I^{\circ}(K)$, $A+B=\mathcal{O}_K$

即 $\forall I\in I(K)$ $I=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}$ 其中 $e_i\in\mathbb{Z}$, $\mathfrak{p}_i$ 非0素理想

Pf (1) I 有逆元. $I=\frac{1}{\mu}A$, $A\in I^{\circ}$ 非 $0\neq\mu\in\mathcal{O}_K$

Lem: $\exists B\in I^{\circ}(K)$ $AB=(\alpha)$

$IB=(\frac{1}{\mu}A)\cdot B=\frac{1}{\mu}(AB)=\frac{1}{\mu}\alpha\mathcal{O}_K$

从而 $I\cdot\underbrace{(\frac{\mu}{\alpha}B)}_{\text{记}B'\text{为}I\text{的逆元}}=\mathcal{O}_K$, 存 $\mu\in\mathcal{O}_K$ 使 $\mu B\in I^{\circ}(K)$

(2) $\forall I\in I(K)$ $\exists\mu\in\mathcal{O}_K$ $I=\frac{1}{\mu}A$

$(\mu)\cdot I=A$ (μ), A 整理想 存唯一分解

设有 $MI=N$ M,N 互素整理想

$I=N/M$ #

Def $I(K)$ 称作 K 的分式理想群.

Def $I(K)$ 称为 K 的分式理想群.

引理 $\forall \alpha \in K^*$ $\exists n \in \mathbb{Z}$ $n\alpha \in O_K$

$\alpha O_K = \frac{1}{n}(n\alpha O_K) \in I(K)$ 称为分式理想

事实上 $\frac{1}{n} O_K$ 也是分式理想

$K^* \xrightarrow{\varphi} I(K)$ 其中 $\mathrm{Im}(\varphi) = P(K) \lhd I(K)$

$\alpha \longmapsto \alpha O_K$

Def $Cl(K) = I(K)/P(K)$ K 的理想类群/类群 (class group)

$= \mathrm{Coker}\left(K^* \to I(K)\right)$

明天证:

Th $Cl(K)$ 是有限群 $h_K = |Cl(K)|$ 称为类数 (class number)

Rk $h_K = 1 \Leftrightarrow$ PID $\Leftrightarrow$ UFD

为什么关心 h_K?

① h_K 衡量 O_K 离 UFD/PID 有多远.

② Fermat $x^p + y^p = z^p$ $(x, y, z \in \mathbb{Z})$ (*)

$x^p = z^p - y^p = (z-y)(z-\zeta_p y)(z-\zeta_p^2 y) \cdots (z-\zeta_p^{p-1} y)$

$K = \mathbb{Q}(\zeta_p)$ $O_K = \mathbb{Z}[\zeta_p]$ 若 $h_K = 1 \Rightarrow$ (*) 无非平凡解

$p \nmid h_K \Rightarrow \cdots$

③ $\mathbb{Z} \rightsquigarrow \mathbb{Z}_{(p)} \subset \mathbb{Q}$ local ring PID

$O_K \rightsquigarrow O_{K,p} \subset K_p$ PID

h_K $h_{K_p} = 1$ 可以为 h_K 衡量整体与局部之间的差距.