· 环. $(A,+,\cdot)$

(1) $(A,+)$ 加法 Abel 群

(2) $(A,\cdot)$ 半群 $x(yz)=(xy)z$

(3) $+$ 与 $\cdot$ 分配律

· 交换环 + 含幺 (0=1) . 子环. (含幺) . 零环

· 环同态 $f: A\to B$.

(1) $f(a+b)=f(a)+f(b)$

(2) $f(ab)=f(a)f(b)$

(3) $f(1_A)=1_B$.

· 环与理想

理想. $\mathfrak{a}\subseteq A$

1) $\mathfrak{a}$ 为加法子群

2) $\forall x\in A$. $y\in\mathfrak{a}$. $xy\in\mathfrak{a}$

第一同构定理. $A/\ker f\cong \mathrm{Im} f$

第二 ——, I. J 为 A 的理想

$\varphi: I\hookrightarrow I+J \twoheadrightarrow I+J/J$

$x \longmapsto x+J$ 满

$\Rightarrow I/I\cap J\cong (I+J)/J$

第三 ——, $I\subset J$ 为 A 理想

$\varphi: A/I\to A/J$

$\Rightarrow A/I\big/J/I\cong A/J$

第四 —— (对应定理) $\mathfrak{a}\subseteq A$

$\{\mathfrak{b}$ 是 A 理想 $|\ \mathfrak{a}\subseteq\mathfrak{b}\}\xrightarrow{\sim}$

$\{\mathfrak{b}/\mathfrak{a}$ 是 $A/\mathfrak{a}$ 理想 $\}$

且保持包含关系

· 零因子. $x\in A$. $\exists y\in A$ $xy=0$

↑ $\mathbb{Z}_6$ 整环: 只有 0 是 ~

· 幂零元: $x\in A$. $\exists n>0$.

$x^n=0$

幂零元集合 $\mathrm{nil}(A)$ 是 A 理想

· 可逆元. $x\in A$. $\exists y\in A$ $xy=1$

$(x)=(1)=A$

· 域: 环且 $\forall x\neq 0$ 可逆

Prop. (1) A 是域

(2) A 的理想只有 (0), 与 (1)

(3) 非零环同态 $f: A\to B$ 是单射

(1) ⇒ (2) $\forall\ \mathfrak{a}\neq(0)$ $\exists x\in\mathfrak{a}$

$(1)=(x)\subseteq\mathfrak{a}$ ⇒ $\mathfrak{a}=(1)$

(2) ⇒ (3) $\ker f$ 为 A 理想 $=(0)$ 或 (1)

$A/\ker f\cong f(A)\neq 0$

⇒ $\ker f=(0)$. ⇒ 单

(3) ⇒ (1) 若 $\exists x$ 不可逆

$f: A\to A/(x)$

$\ker f=(x)=(0)$ 或 (1) 矛盾

·素理想、极大理想

素：P · (1) $P\subseteq A$ 真理想

(2) $xy\in P \Rightarrow x\in P$ 或 $y\in P$

理想形式：$AB\subseteq P \Rightarrow A\subseteq P$ 或 $B\subseteq P$

商环 A/P 为整环

例. 对 $k[x]$，k为域（$k[x]$ ED）

素为 (0) 及 (f) f不可约

极大～：m. (1) $m\neq(1)$

(2) 不存在真理想 α，

$m\subsetneq\alpha\subsetneq(1)$

商环 A/m 为域

A为域 $\Leftrightarrow$ (0)为极大理想

对环同态 $f: A\to B$

$\mathfrak{q}$ 为素 $\subseteq B$ $\Rightarrow$ $f^{-1}(\mathfrak{q})\subseteq A$为素

$$\underbrace{A \xrightarrow{f} B \xrightarrow{\phi}}_{g} B/\mathfrak{q}$$

$A/\ker g = A/f^{-1}(\mathfrak{q}) \cong f(A)/\mathfrak{q}$

n为极大 $\subseteq B$ $\not\Rightarrow$ $f^{-1}(n)$是A的极大

（例 $\mathbb{Z}\to\mathbb{Q}$ $(0)\leftarrow(0)$）

在 f 满时 "$\Rightarrow$" 成立

$A/\ker f\cong B$ $\Rightarrow$

n在B对应A中$f^{-1}(n)$ 对应 $A/\ker f$中 $m/\ker f$

n极大 $\Rightarrow$ m极大 $\subseteq A$

定理. 非零环 有极大理想

证：利用Zorn引理（对非空偏序集，若每个链有上界（在S上），则S有极大元）

取 $\Sigma=\{\alpha\mid\alpha$为$A$中真理想$\}$

$(0)\in\Sigma$ $\Rightarrow$ $\Sigma\neq\varnothing$

以包含关系"$\subseteq$"形成偏序结构

考虑链 $\alpha_1\subseteq\alpha_2\subseteq\cdots$

取 $\alpha=\bigcup_{i=1}\alpha_i$，下验 $\alpha\in\Sigma$

1. α为理想：$x\in\alpha_i$, $y\in\alpha_j$ $\Rightarrow$ $x+y\in\alpha_{\max(i,j)}$, $ax\in\alpha_i$

2. $1\notin\alpha$：（$\because$ $1\notin\alpha_i$ $\forall\alpha_i$）

$\Rightarrow$ 有上界 $\Rightarrow$ 有极大元 $\Rightarrow$ 即为极大理想

推论1 存在素理想

2. $\mathfrak{a}\subseteq A$为理想 $\exists$ m.极大 $\mathfrak{a}\subseteq m\subsetneq(1)$

3. x不可逆 $\exists$ m极大. $(x)\subseteq m\subsetneq(1)$

证2. $\phi: A\to A/\mathfrak{a}$ 有极大理想 n

而ϕ满 $\Rightarrow$ 其原像 $\phi^{-1}(n)$ 极大

局部环（local ring）

仅有唯一一个极大理想的环

例 $O_p=\{\frac{m}{n}\in\mathbb{Q}\mid (m,n)=1,\ p\nmid n\}$

易验证 pO_p 为素理想，且唯一

A/m 称为 剩余域（residue field）

命题：(1) $\forall x\in A\setminus m$ 都可逆 $\Rightarrow$ m为唯一极大

(2) m极大，$\forall x\in 1+m$ 可逆 $\Rightarrow$ 局部环

(1). $\forall$ 理想$\neq(1)$ $\mathfrak{a}$，由不可逆元生成

$\mathfrak{a}\subseteq m$

(2) 利用(1)，取 $x\in A$, $x\notin m$ 证 x可逆

$\because$ x与m生成A

$\Rightarrow$ $zx+y=1$ $\Rightarrow$ $zx=1-y$ 可逆

$\Rightarrow$ $x\in$单位 矛盾

例. $k[x_1,\cdots,x_n]$中 (f) 不可约为素

PID上，非零素 ideal $\Leftrightarrow$ 极大～

（素元生成） （不可约元生成）

取 $0\neq(x)$ 素

$(x)\subsetneq(y)$ 极大 $\Rightarrow$ $y\notin(x)$

$\Rightarrow$ $x\in(y)$

$\Rightarrow$ $x=yz$ $\Rightarrow$ $yz\in(x)$

$\Rightarrow$ $z\in(x)$ $\Rightarrow$ $z=xt$

$\Rightarrow$ $x=yxt$ $\Rightarrow$ $yt=1$ $\Rightarrow$ y可逆，矛盾

幂零根. Jacobson 根

$Nil(A)=\{x \mid \exists n\geq 0.\ x^n=0\}$ $0\in Nil(A)$

命题. 1. $Nil(A)$ 理想

2. $A/Nil(A)$ 无幂零根.

1. $x^n, y^m \Rightarrow (x+y)^{n+m-1}$

2. $(\bar{x})^n=\bar{0} \Rightarrow x^n\in Nil \Rightarrow x^{nk}=0$

对 $\bar{x}\neq\bar{0}$ 矛盾

命题. $Nil(A)=\bigcap_{p\text{为所有素理想}} p$

"$\Leftarrow$" 显然

"$\Rightarrow$" 反证. 取 $f\in nil(A)$ 证 $f\in\bigcap P$

$\forall n.\ f^n\neq 0$

取 $\Sigma=\{\alpha\text{为理想} \mid \forall n.\ f^n\notin\alpha\}$

引入 "$\subseteq$" 偏序 利用 Zorn引理

极大元 p. 下证 p为素理想

取 $p\subsetneq p+(x)$, $p+(y)$

则 $p+(x), p+(y)\notin\Sigma$

$\Rightarrow \exists n.\ f^n\in p+(x)$, $f^m\in p+(y)$

$\Rightarrow f^{m+n}\in(xy)+p$

$\Rightarrow p+(xy)\notin\Sigma$

$\Rightarrow xy\notin p \Rightarrow p$为素 □

Jacobson 根.

$Jac(A)=\bigcap_{m\text{为极大}\sim} m \supseteq \bigcap p = Nil(A)$

命题. $x\in Jac(A) \Leftrightarrow \forall y.\ 1+xy$ 可逆

"$\Rightarrow$" 反证. $\exists y$ $1+xy$ 不可逆

$\Rightarrow (1+xy)\subseteq m$. 极大 而 $x\in m$

$\Rightarrow 1\in m$ 矛盾

"$\Leftarrow$" 若 $\exists m$极大 $x\notin m$

$\Rightarrow x$与m生成 (1)

$\Rightarrow z+xy=1 \Rightarrow \underset{\in m}{z}=1-xy$ 可逆

矛盾 □

理想的运算

1. 和. $\mathfrak{a}, \mathfrak{b}$ 为A的理想

$\mathfrak{a}+\mathfrak{b}=\{x+y \mid x\in\mathfrak{a}, y\in\mathfrak{b}\}=\mathfrak{b}+\mathfrak{a}$

易证. 是理想. 且是包含 $\mathfrak{a}, \mathfrak{b}$ 的最小理想

对有限个. $\sum_{i=1}^n \mathfrak{a}_i=\{\sum_{i=1}^n x_i \mid x_i\in\mathfrak{a}_i\}$

无限个. $\sum_{\text{无穷}}\mathfrak{a}_i=\{\sum_{\text{有限}} x_i \mid x_i=0 \text{几乎处处成立}\}$

例. $\mathbb{Z}$中 $(15)+(21)=\underset{\gcd}{(3)}$

2. 交. $\mathfrak{a}\cap\mathfrak{b}=\{x: x\in\mathfrak{a}\text{且}x\in\mathfrak{b}\}$为A的理想

$\mathfrak{a}\cap\mathfrak{b}$ 是 $\mathfrak{a},\mathfrak{b}$ 的最大下界

$\bigcap_{\text{任意多}}\mathfrak{a}_i$ 是 A 的理想

包含关系下形成 "完备格"

3. 积 $\mathfrak{a}\cdot\mathfrak{b}=$ 由 $\{xy \mid x\in\mathfrak{a}, y\in\mathfrak{b}\}$ 生成的理想

$=\{\sum_{\text{有限}} x_iy_i \mid x_i\in\mathfrak{a}, y_i\in\mathfrak{b}\}$

例 $\mathbb{Z}$中. $\mathfrak{a}=(m)$. $\mathfrak{b}=(n)$

$\mathfrak{a}+\mathfrak{b}=(\gcd(m,n))$

$\mathfrak{a}\cap\mathfrak{b}=(\mathrm{lcm}(m,n))$

$\mathfrak{a}\cdot\mathfrak{b}=(mn)$

$\mathfrak{a}\cdot\mathfrak{b}\subseteq\mathfrak{a}\cap\mathfrak{b}$

$\mathbb{Z}$上 "=" $\Leftrightarrow (m,n)=1$ 互素

分配律.

$\mathfrak{a}\cdot(\mathfrak{b}+\mathfrak{c})=\mathfrak{a}\cdot\mathfrak{b}+\mathfrak{a}\cdot\mathfrak{c}$

$(\mathfrak{a}+\mathfrak{b})\cdot\mathfrak{c}=\mathfrak{a}\cdot\mathfrak{c}+\mathfrak{b}\cdot\mathfrak{c}$

模律. 若 $\mathfrak{b}\subseteq\mathfrak{a}$ 或 $\mathfrak{c}\subseteq\mathfrak{a}$

$\mathfrak{a}\cap(\mathfrak{b}+\mathfrak{c})=\mathfrak{a}\cap\mathfrak{b}+\mathfrak{a}\cap\mathfrak{c}$

$\supseteq$: $\mathfrak{b}\subseteq\mathfrak{b}+\mathfrak{c} \Rightarrow \mathfrak{a}\cap\mathfrak{b}\subseteq\mathfrak{a}\cap(\mathfrak{b}+\mathfrak{c})$

$\mathfrak{a}\cap\mathfrak{c}\subseteq\mathfrak{a}\cap(\mathfrak{b}+\mathfrak{c})$

$\Rightarrow \supseteq$ ✓

$\subseteq$: $\underset{\in\mathfrak{a}}{x}=\underset{\in\mathfrak{b}}{y}+\underset{\in\mathfrak{c}}{z}$.

若 $\mathfrak{b}\subseteq\mathfrak{a}$. $\Rightarrow y\in\mathfrak{b}\cap\mathfrak{a}$

$z=x-y\in\mathfrak{a}\cap\mathfrak{c}$ ✓ □

对$\mathbb{Z}$ 由 $\gcd\cdot\mathrm{lcm}=mn$

$\Rightarrow (\mathfrak{a}+\mathfrak{b})\cdot(\mathfrak{a}\cap\mathfrak{b})=\mathfrak{a}\cdot\mathfrak{b}$

对一般环. $(\mathfrak{a}+\mathfrak{b})\cdot(\mathfrak{a}\cap\mathfrak{b})=\mathfrak{a}\cdot(\mathfrak{a}\cap\mathfrak{b})+\mathfrak{b}\cdot(\mathfrak{a}\cap\mathfrak{b})$

$\subseteq\mathfrak{a}\cdot\mathfrak{b}\subseteq\mathfrak{a}\cap\mathfrak{b}$

当 $(\mathfrak{a}+\mathfrak{b})=(1)$ 时 上式 "$\subseteq$" 换成 "="

$\mathfrak{a}\cap\mathfrak{b}=\mathfrak{a}\cdot\mathfrak{b}$

直积：$A_1 \cdots A_n$ 为理想

$A_1\times\cdots\times A_n=\{(x_1,\cdots x_n)\mid x_i\in A_i\}=\prod_{i=1}^{n}A_i$

加法：$(x_1\cdots x_n)+(y_1\cdots y_n)=(x_1+y_1,\cdots x_n+y_n)$

乘法 $(\quad)\cdot(\quad)=(x_1\cdot y_1,\cdots x_n\cdot y_n)$

幺元 $(1_{A_1},\cdots 1_{A_n})$

投影 $p_i:\prod_{i=1}^{n}A_i\to A_i$

$(x_1,\cdots x_n)\longmapsto x_i$

环上的中国剩余定理：

若 $\alpha_i\ \alpha_j$ 互素

$A/\bigcap_{i=1}^{n}\alpha_i\cong\prod_{i=1}^{n}(A/\alpha_i)$

命题：$\phi:A\to\prod_{i=1}^{n}(A/\alpha_i)$

$x\mapsto(x+\alpha_1,\cdots,x+\alpha_n)$

(1) 若 $\forall i\neq j$，α_i 与 α_j 互素

$\Rightarrow\bigcap_{i=1}^{n}\alpha_i=\alpha_i\cdots\alpha_n$（记为 $\prod_{i=1}^{n}\alpha_i$）

(2) ϕ 满 $\Leftrightarrow$ α_i 与 α_j 互素

(3) ϕ 单 $\Leftrightarrow$ $\ker\phi=\bigcap_{i=1}^{n}\alpha_i=(0)$

证：(1) 数归：

$n=2$ 已证

若 $n-1$ 时成立

$b=\prod^{n-1}\alpha_i=\bigcap^{n-1}\alpha_i$

对 n. $(\prod^{n-1}\alpha_i)\,\alpha_n=b\cdot\alpha_n\ \underset{=}{\overset{若b与a_n互素}{=}}\ b\cap\alpha_n$

$=(\bigcap^{n-1}\alpha_i)\cap\alpha_i$

$=\bigcap^{n}\alpha_i$

$\because\ \alpha_i+\alpha_n=(1)$

$x_i+y_i=1$

$\Rightarrow\prod_{i=1}^{n-1}x_i=\prod_{i=1}^{n-1}(1-y_i)=1\pmod{\alpha_n}$

$\Rightarrow b+\alpha_n=(1)$

(2) 若 ϕ 满：$\exists x_i\in A$

$\phi(x_i)=(0,\cdots0,1,0,\cdots0)$

$\Rightarrow\begin{cases}x_i\equiv1 \pmod{\alpha_i}\\ x\in\alpha_j\quad j\neq i\end{cases}$

$\Rightarrow 1=\underbrace{1-x_i}_{\in\alpha_i}+\underbrace{x_i}_{\in\alpha_j}\Rightarrow\alpha_i+\alpha_j=(1)$

若互素，固定 i. $\alpha_i+\alpha_j=(1)$

$u_j+v_j=1$

$\Rightarrow\prod_{j\neq i}v_j\in\alpha_j\Rightarrow\prod v_j=\prod(1-u_j)\equiv1\ \mathrm{mod}\,\alpha_i$

$\Rightarrow x_i=\prod_{j\neq i}v_j\quad\phi(x_i)=(0,\cdots0,1,0,\cdots0)$ 满

(3) $\ker\phi=\{x\mid\phi(x)=(0,\cdots0)\}$

$\Rightarrow x\in\bigcap_{i=1}^{n}\alpha_i$ □

另外 $\mathfrak{a}\cup\mathfrak{b}$ 一般不是理想.

命题：(1) $p_1,\cdots p_n$ 素理想. $\alpha\subseteq\bigcup_{i=1}^{n}p_i$

则 $\exists i$ $\alpha\subseteq p_i$

(2) $\alpha_1,\cdots\alpha_n$

$p\supseteq\bigcap_{i=1}^{n}\alpha_i$ 则 $\exists i$ $p\supseteq\alpha_i$

若 $p=\bigcap_{i=1}^{n}\alpha_i$ 则 $\exists i$. $p=\alpha_i$

证明：(1) 反证

$\forall i$ $\alpha\nsubseteq p_i$. $\overset{证}{\Rightarrow}$ $\alpha\nsubseteq\bigcup_{i=1}^{n}p_i$

归纳：$n=1$ 时 显然

对 n. $\because$ $n-1$ 时成立

$\forall\ 1\leq i\leq n\ \exists$ $x_i\in\alpha$

$x_i\notin\bigcup_{j\neq i}p_j$ $(\because\alpha\nsubseteq\bigcup_{j\neq i}p_j)$

对 n (1) 若 $\exists i$ $x_i\notin p_i$ 则已证

否则 $\begin{cases}x_i\notin\bigcup_{j\neq i}p_j\\ x_i\in p_i\end{cases}$

取 $y=\sum_{i=1}^{n}x_1\cdots x_{i-1}x_{i+1}\cdots x_n$

$\forall p_i$. 由于 对 x_i 出现的 $\underline{\quad}\in p_i$

对 $x_1\cdots x_{i-1}x_{i+1}\cdots x_n$

$x_j\notin p_i$ $\Rightarrow$ 上式 $\notin p_i$

$\Rightarrow y\notin\bigcup_{i=1}^{n}p_i$

(2) 反证

$\forall i$. $\alpha_i\nsubseteq p$ 证 $\bigcap_{i=1}^{n}\alpha_i\nsubseteq p$

$\because\exists\begin{cases}x_i\in\alpha_i\\ x_i\notin p\end{cases}$

$\Rightarrow\prod x_i\in\prod\alpha_i\subseteq\bigcap_{i=1}^{n}\alpha_i$

$\Rightarrow\prod_{i=1}^{n}x_i\notin p$

若 $p=\bigcap_{i=1}^{n}\alpha_i$

$\Rightarrow\exists i$ $p\supseteq\alpha_i$

又 $p=\bigcap_{i=1}^{n}\alpha_i\subseteq\alpha_i\Rightarrow p=\alpha_i$

商理想.

$(\mathfrak{a}:\mathfrak{b}) = \{x\in A : x\mathfrak{b} \subseteq \mathfrak{a}\}$

$(0:\mathfrak{b}) = \mathrm{Ann}(\mathfrak{b})$, 零化子

$\mathbb{Z}$上, $\mathfrak{a}=(21)$, $\mathfrak{b}=(15)$

$(\mathfrak{a}:\mathfrak{b}) = \{x\in\mathbb{Z} \mid 7\mid x\}$

对 $a = p_1^{u_1}\cdots p_n^{u_n} q_1^{r_1}\cdots q_m^{r_m}$

$b = p_1^{v_1}\cdots p_n^{v_n} r_1^{y_1}\cdots r_t^{y_t}$

则 对 $p_1\cdots p_n$ 中 $u_i>v_i$ 的

及 $q_1\cdots q_m$

$\Rightarrow (\mathfrak{a}:\mathfrak{b}) = (m)$. $m=\dfrac{a}{(a,b)}$

根理想.

$r(\alpha) = \sqrt{\alpha} = \{x\in A : \exists n.\ x^n\in\alpha\}$

$= \phi^{-1}(\mathrm{nil}(A/\alpha))$

利用对应定理

$\mathrm{nil}(A/\alpha) = \bigcap_{\bar{P}\text{为}A/\alpha\text{素}} \bar{P}$

$\Rightarrow r(\alpha) = \bigcap_{P\supseteq\alpha} P$

例. $r(p) = p$.

性质. (1) $r(\alpha)\supseteq\alpha$

(2) $r(r(\alpha)) = r(\alpha)$

(3) $r(\mathfrak{a}\mathfrak{b}) = r(\mathfrak{a}\cap\mathfrak{b}) = r(\mathfrak{a})\cap r(\mathfrak{b})$

(4) $r(\alpha) = (1) \Leftrightarrow \alpha = (1)$

(5) $r(\alpha+\mathfrak{b}) = r(r(\alpha)+r(\mathfrak{b}))$

(6) p素, $r(p^n) = p$. $\forall n>0$

(4) "$\Rightarrow$" $r(\alpha) = (1)$

$\Rightarrow 1^n\in\alpha \Rightarrow 1\in\alpha$

E是集合. $\sqrt{E} = \{x\in A \mid \exists n.\ x^n\in E\}$

$\sqrt{\bigcup_\alpha E_\alpha} = \bigcup_\alpha \sqrt{E_\alpha}$

命题. D为所有零因子构成的集合 ($D = \bigcup_{x\neq 0}\mathrm{Ann}(x)$) 则 $D=\sqrt{D}$

$\forall x\in\sqrt{D}$. $x^n\in D \Rightarrow x^n y = 0$

$\Rightarrow x(x^{n-1}y) = 0$

例. $\mathbb{Z}$上. $\mathfrak{a} = (m)$. $m = p_1^{e_1}\cdots p_r^{e_r}$

则 $r(\alpha) = r(p_1^{e_1}\cdots p_r^{e_r})$ 两两互素

$= \bigcap_{i=1}^r r(p_i^{e_i}) = \bigcap_{i=1}^r p_i = \prod_{i=1}^r p_i$

命题. $\mathfrak{a}.\mathfrak{b}$为理想,

$r(\mathfrak{a})+r(\mathfrak{b}) = (1)$ 则 $\mathfrak{a}+\mathfrak{b} = (1)$

pf. $r(\mathfrak{a}+\mathfrak{b}) = r(r(\mathfrak{a})+r(\mathfrak{b})) = r(1) = (1)$

$\Rightarrow \mathfrak{a}+\mathfrak{b} = (1)$ □

理想的扩张和局限

$f: A\to B$. 环同态,

$\mathfrak{a}$为A的~. $\mathfrak{b}$是B的~

·局限理想

$\mathfrak{b}^c := f^{-1}(\mathfrak{b})$ 是A的理想

且 $\mathfrak{b}$素 $\Rightarrow \mathfrak{b}^c$ 素 (in A)

·扩张:

$\mathfrak{a}^e = Bf(\mathfrak{a}) = \{\sum_{\text{有限}} y_i f(x_i)\}$, $y_i\in B$, $x_i\in A$

注.1 $f(\mathfrak{a})$ 不一定是理想.

$\mathbb{Z}\hookrightarrow\mathbb{Q}$

$(p)\to p\mathbb{Z}$ 不是理想

2. $\mathfrak{a}$素 $\not\Rightarrow$ $\mathfrak{a}^e$ 为素,

例: $\mathbb{Z}\hookrightarrow\mathbb{Z}[i]$

$p^e \to$
- $((1+i)^2)$ $p=2$
- $(a+bi)\cdot(a-bi)$ ($p\equiv 1 \bmod 4$)
- (p) $p\equiv 3 \pmod 4$

$p=2$: $2\to(1+i)^2\mathbb{Z}[i]$

$p\equiv 1 \bmod 4$ $\min(i,\mathbb{Q}) = x^2+1$

模p. $\exists a$. $x^2-a^2 = (x+a)(x-a)$

($\because \left(\frac{-1}{p}\right)=1$)

$P_1 = (p, i+a)$

$P_2 = (p, i-a)$

$p^e = P_1\cdot P_2$

($p=13$. $P_1 = (13, i-5) = (3+2i)$, $P_2 = (13, i+5) = (3-2i)$)

若 $\left(\frac{-1}{p}\right) = -1$, 即 $p\equiv 3 \pmod 4$

$p^e = p\mathbb{Z}[i]$. 素,

$w^2 = w+1$

例. $\mathbb{F}_4 = \mathbb{F}_2(w)$.

$\mathbb{F}_4[x,y]/(y^2+y-x^3)$　　令 $C = \{(\alpha,\beta)\in\mathbb{F}_4 : \alpha^3 = \beta^2+\beta\}$

由 $(x-1, y-w)$ 生成

$(x,y) = (0,0)$　　$(0,1)$　　　　$(1,w)$　　　　$(1,w+1)$

$\beta = 0$ 即 x.　　　　　　$\alpha = 1$ 即 $x-1$

此时 $y^2+y=0$　　　　　　此时 $y^2+y=1$

命题. $f: A \to B$ 环同态,

$\mathfrak{a}$. $\mathfrak{b}$ 理想

(1) $\mathfrak{a} \subseteq \mathfrak{a}^{ec}$. $\mathfrak{b} \supseteq \mathfrak{b}^{ce}$

(2) $\mathfrak{b}^c = \mathfrak{b}^{cec}$　　$\mathfrak{a}^e = \mathfrak{a}^{ece}$

(3) 记 C 为 B 上所有局限理想,

E 为 A 中所有理想在 B 的扩理想

$C = \{\alpha \subseteq A : \alpha^{ec} = \alpha\}$

$(\because \alpha = \mathfrak{b}^c = \mathfrak{b}^{cec} = \alpha^{ec})$

$E = \{\mathfrak{b} \subseteq B : \mathfrak{b}^{ce} = \mathfrak{b}\}$

由此 $C \xrightarrow{1:1} E$

$\alpha \longmapsto \alpha^e$　　$\mathfrak{b}^c \longleftarrow\!\shortmid\, \mathfrak{b}$