26

回顾 域扩张

- 狭义 $k \overset{\text{inc}}{\subseteq} K$ 子域
- 广义一般 $k \xrightarrow[\text{同态}]{\theta} K$

那么 K 就能视为 k 上的线性空间

记 K/k $\quad \lambda \cdot v = \theta(\lambda) \cdot v$

当乘依赖 θ 的选取

例 K 域

$k = k \xrightarrow{\theta} K$ $\quad \theta$ 不满

$\dim_\theta K > 1$

但 $id \Rightarrow \dim_{id} k = 1$

以后默认 $\theta = id$ $\quad$ (就记 $\dim_k K = [K:k]$)

总是 $k \subseteq K$ $\quad k[x] \subseteq K[x]$

$\text{Root}_k(f) \subseteq \text{Root}_K(f)$

Fact (1) $f(x) \neq 0$

$\#\text{Root}_k(f) \leq \deg(f)$

证 EX

(2) f 的可约性会变. e.g. $\mathbb{R}[x] \subseteq \mathbb{C}[x]$

$x^2+1 \quad (x+i)(x-i)$

(3) $k \xrightarrow{\theta} K \longrightarrow k[x] \xrightarrow{\text{就}\tilde{\theta}} K[x]$

$f(x) \in k[x]$ $\quad f(x) = a_n x^n + \cdots \mapsto \tilde{\theta}(f(x)) = \theta(a_n)x^n + \cdots$

例 ① θ 不满 $\left(\text{root}_k(f) \subseteq \text{Root}_K^{\tilde{\theta}}(f)\right)$

② $f(x)$ 不可约 $\not\Rightarrow \tilde{\theta}(f)$ 不可约

【Ex】① $k \subseteq K$ $\quad f(x), g(x) \in k[x] \subseteq K[x]$.

对于 $\gcd_{k[x]}(f,g) = \gcd_{K[x]}(f,g)$. 【Bézout】

② $k \hookrightarrow K$ 唯一?

3.19

k 域

$f(x) \in k[x]$ 有一不可约 $f(x) = x^n + \cdots + a_0$.

$K = k[x]/f(x)$

① $k \hookrightarrow K$ $\quad \lambda \mapsto \bar{\lambda}$

$(k \xrightarrow{can} k[x] \xrightarrow[\text{商映射}]{can} K)$

以下 K 为 k 线性空间

$\lambda \cdot \overline{g(x)} = \overline{\lambda \cdot g(x)}$

【key Face】 $\dim_k K = n$. K 上有基 $\{\bar{1}, \cdots \bar{u}^{n-1}\}$

proof. $\forall \overline{g(x)} \in K$. $g(x) = q(x) f(x) + r(x)$ $\quad \deg r < \deg f / r = 0$.

$$\overline{g(x)} = \overline{r(x)} = \overline{c_{n-1}x^{n-1} + \cdots + c_0} = \bar{c}_{n-1}\bar{u}^{n-1} + \cdots + \bar{c}_0\bar{1}$$
$$= c_{n-1}\cdot u^{n-1} + \cdots + c_0 \cdot \bar{1}$$

$\Rightarrow \overline{g(x)} \in \operatorname{span}\{\bar{1}, \cdots \bar{u}^{n-1}\}$

$\{\bar{1}, \cdots \bar{u}^{n-1}\}$ 线性无关: $\lambda_0, \lambda_1, \cdots \lambda_{n-1} \in k$

s.t. $\lambda_{n-1}\cdot u^{n-1} + \cdots + \lambda_0 \cdot \bar{1} = \bar{0}$

$\Leftrightarrow \overline{\lambda_{n-1}x^{n-1} + \cdots + \lambda_0} = \bar{0}$

$\Leftrightarrow f(x) \mid \lambda_{n-1}x^{n-1} + \cdots + \lambda_0$ on $k[x]$ 矛

$\Leftrightarrow \lambda_0 = \cdots = \lambda_{n-1} = 0$.

【Rmk】 ① $n=1$ $f(x) = x + a$ 记 $k \simeq K$

② $n \geq 2$. $\operatorname{Root}_k(f(x)) = \emptyset$

8、 以下 $\theta: k \hookrightarrow K$ (不区分 $x, \bar{x}$)

$\hat{\theta}: k[x] \hookrightarrow K[x]$

↓

以 K 为系数的多项式

$u \in K$ 满足

$u^n + a_{n-1}u^{n-1} + \cdots + a_0 = 0$　　$f(u) = 0_K$

$\Rightarrow$ $u \in Root_K(f(x))$　添根

例. $\mathbb{R}[x]$ x^2+1 不可约

造 $K = \mathbb{R}[x]/(x^2+1)$

令 $u = \bar{x}$.　K 中元素 $\{au + b\bar{1}\}$ $a, b \in \mathbb{R}$

$(au+b)(cu+d) = ?$ in K

方法1.
~~$ac u^2 + (ad+bc)u + bd$~~

$= \overline{ax+b} \cdot \overline{cx+d}$

$= \overline{acx^2 + (ad+bc)x + bd}$

$= \overline{(ad+bc)x + (bd-ac)}$

$= (ad+bc)u + (bd-ac)$

$\therefore K \simeq \mathbb{C}$　EX

in $K[x]$

$u \in Root_K(x^2+1)$

$x^2+1 = (x+u)(x-u)$

方法2. 在 K 中唯一 ~~乘~~ 乘法表

EX　$K' = \mathbb{R}[x]/(x^2+2)$　　$u \mapsto \sqrt{2}i$

$K' \simeq \mathbb{C}$. 构造同构.

例. $\mathbb{F}_2 = \{\bar{0}, \bar{1}\}$.

$x^2 + x + \bar{1} \in \mathbb{F}_2[x]$

$\mathbb{F}_2 \hookrightarrow \mathbb{F}_2[x]/(x^2+x+\bar{1}) =: \mathbb{F}_4$.

$\mathbb{F}_4$ 有四个元素 $\{\bar{0}, \bar{1}, u, u+\bar{1}\}$ → 循环群

$\bar{u}+\bar{u} = \overline{x+x} = \overline{2x} = \bar{0}$

$u^2+u = 2u+1$

$u^2+u+\bar{1} = \bar{0} \Rightarrow u^2 = u+\bar{1}$

u^2+2u+1

计算乘法表

乘法	$\bar{0}$	$\bar{1}$	u	$u+\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	u	$u+\bar{1}$
u	$\bar{0}$	u	$u+\bar{1}$	$\bar{1}$
$u+\bar{1}$	$\bar{0}$	$u+\bar{1}$	$\bar{1}$	u

$u^3 = (u+\bar{1})^3 = \bar{1}$

EX $\mathbb{F}_4 \simeq \mathbb{Z}_4$

例 $\mathbb{F}_2 = \{0, \bar{1}, \bar{2}\}$, $\bar{2} = -\bar{1}$

x^2+1 in $\mathbb{F}_2[x]$ 不可约.

$\mathbb{F}_3 \longrightarrow \mathbb{F}_3[x]/(x^2+1) = \mathbb{F}_9$.

$\mathbb{F}_9 = \{\bar{0}, \bar{1}, \bar{2}, u, u+\bar{1}, u+\bar{2}, 2u, 2u+\bar{1}, 2u+\bar{2}\}$

$x^2+1 = (x-u)(x-2u)$

$(2u+\bar{1})^{-1} = ?$

~~$(2u+1)(u+1) = 2u^2+3u+1$~~

$= 2au^2 + (2b+a)u + b$

$(2u+1)(au+b) = (2b+a)u + (a+b)$

$\begin{cases} a = 2 \\ b = 2 \end{cases}$

证: Bezout $\gcd_{\mathbb{F}_3[x]}(1+2x, x^2+1) = \bar{1}$

$a(x)(1+2x) + b(x)(x^2+1) = 1 \quad a(x), b(x) \in \mathbb{F}_3[x]$

$\Rightarrow (\bar{1}+2u)^{-1} = a(x)$.

EX 算 $a(x)$

EX $\mathbb{F}_9$ 的乘法表

30、 题意、 $x^2+x+\bar{2} \in \mathbb{F}_3[x]$

$\mathbb{F}_q' = \mathbb{F}_3[x]/(x^2+x+\bar{2})$ $\cong$ $\mathbb{F}_q$

$v^2+v+2=0$

$k \xrightarrow{\theta} k[x]/(f(x))$ 为注嵌.

存在 $k \xrightarrow{\delta} F$ 域

$\alpha \in \mathrm{Root}_F(\delta(f))$ $\quad \delta(f) = x^n + \delta(a_{n-1})x^{n-1}+\cdots \in F[x]$

$k \xrightarrow{\delta} F$

$\theta \downarrow \quad \nearrow \delta'$

K

$\begin{cases} \delta' \circ \theta = F \\ \delta'(u) = \alpha \end{cases}$

注嵌的证明. $k \xrightarrow{\delta} F$

$\theta \downarrow \quad \downarrow \alpha$

K

$\exists!\, \tilde{\delta}: k[x] \to F$

$g(x) \to \delta(g)(\alpha)$ 多项式环的注嵌

$\Rightarrow (f(x)) \subseteq \ker \tilde{\delta}$

极大

$\tilde{\delta}$ 满射 $k[x]/(f(x)) \xrightarrow{\delta'} F$

Check later.

例、 $\mathbb{F}_3 \xrightarrow{\theta} \mathbb{F}_q = \mathbb{F}_3/(x^2+1)$ $\quad u=\bar{x}$

$\mathbb{F}_q' = \mathbb{F}_3[x]/(x^2+x+\bar{1})$

$v=\bar{x}$

$\mathbb{F}_3 \hookrightarrow \mathbb{F}_9'$

$\alpha \in \text{Root}_{\mathbb{F}_9'}(X^2+\bar{1})$ $\quad (V+2)^2 = V^2+2V+1 = \bar{0}$.

取 $\alpha = V+2$. or $2V+1$

if.

$\exists!\ \exists \varphi' : \mathbb{F}_9 \hookrightarrow \mathbb{F}_9'$

$\bar{0}, \bar{1}, \bar{2} \longmapsto \bar{0}, \bar{1}, \bar{2}$

$u \longmapsto V+2$

$\Rightarrow \mathbb{F}_9 \simeq \mathbb{F}_9'$

Ex $\mathbb{F}_9'' = \mathbb{F}_3[X]/(X^2+2X+2)$

$\mathbb{F}_9 \hookrightarrow \mathbb{F}_9''$

3.21

欧氏整环.

Def 整环 R 称为 ED, 若 $\exists$ size function $\varphi: R^\times = R\setminus\{0_R\} \to \{0,1,\cdots\}$

$a \longmapsto \varphi(a)$

s.t. $\forall a, b \in R^\times$ $\exists q, r \in R$. $a = q\cdot b + r$ (*)

其中 $r = 0_R$ 或 $\varphi(r) < \varphi(b)$

例. $\mathbb{Z}$. $\varphi = |\cdot|$

注. (1) (*) 不唯一. e.g. $33 = 4\cdot 9 + (-3)$

$= 3\cdot 9 + 6$

(2) $k[X]$, k 是域. $\varphi = \deg$ (当然 φ 也不唯一. $\tilde{\varphi} = 2\varphi$ 也行).

Thm ED $\Rightarrow$ PID

proof. R is ED. $0 \neq I \lhd R$. 取 $0 \neq b \in I$. $\varphi(b)$ 最小

Claim. $I = (b)$. ~~这是平凡的~~ 省先 $I \supseteq (b)$.

又显然 $I = (b)$

有 R is PID, but ED. However, it's not important here.

52. 例. 高斯整数 $\mathbb{Z}[i]$, 分式域为 $\mathbb{Q}(i)$

Claim, $\mathbb{Z}[i]$ is ED.

Recall norm map

$N = \mathbb{Q}(i)^\times \longrightarrow \mathbb{Q}^\times$ 是一个群同态

$a+bi \longrightarrow a^2+b^2$.

$N|_{\mathbb{Z}[i]^\times} \Rightarrow N : \mathbb{Z}[i]^\times \to$ [illegible].

证. $\frac{x}{y} = \frac{x\bar{y}}{y\bar{y}} \in \mathbb{Q}(i)$

$\searrow \alpha+\beta i$

找一个高斯整数逼近.

$|\alpha - m| \le \frac{1}{2}$, $|\beta - n| \le \frac{1}{2}$

$\Rightarrow \alpha+\beta i = \underbrace{m+ni}_{q} + \underbrace{(\alpha-m)+(\beta-n)i}_{r'}$

$\Rightarrow \frac{x}{y} = q + r'$

$\Rightarrow x = qy + r'y$

r

$N(r) \le (\frac{1}{4}+\frac{1}{4}) N(y) < N(y)$ □

注. $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$

例. $\gcd(4+7i, 3+4i)$

$\frac{4+7i}{3+4i} = \frac{(4+7i)(3-4i)}{25} = \frac{40+5i}{25} = \frac{8+i}{5}$

$\frac{4+7i}{3+4i} = 2 \text{ or } \frac{2}{5} + \frac{i}{5}$

$4+7i = 2(3+4i) + (\frac{2}{5}+\frac{i}{5})(3+4i)$

$= 2(3+4i) + (-2-i)$

$\frac{3+4i}{-2-i} = \frac{(3+4i)(-2+i)}{5} = \frac{-10-5i}{5} = -2-i$

$\gcd = 2+i$

~~(2+i)~~

例. $\mathbb{Z}[\sqrt{-2}] \subseteq \mathbb{Q}(\sqrt{-2})$.

Thm. $\mathbb{Z}[\sqrt{-2}]$ is ED $\Rightarrow$ PID.

$\varphi : \mathbb{Z}[\sqrt{-2}] \longrightarrow \mathbb{N}_{\geq 0}$

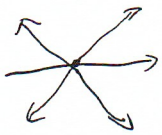
$a+b\sqrt{-2}i \mapsto a^2+2b^2$ 类似的处理就行

例

Fact $\mathbb{Z}[\sqrt{-3}]$ 不是PID $\Rightarrow$ 不是ED.

例 $(2, 1+\sqrt{-3}) = (2) + (1+\sqrt{-3})$ 是主理想但不是主理想

把环变大一些就是主理想了



$\omega^2+\omega+1=0$

$\mathbb{Z}[\omega] = \{m+n\omega\}$ Eisenstein 整数环

例 Frac $\mathbb{Z}[\omega] = \mathbb{Q}(\sqrt{-3})$.

Thm $\mathbb{Z}[\omega]$ 是ED $\Rightarrow$ 是PID.

注. $\mathbb{Q}(\sqrt{-3})$ 有两组基 $\{1, \omega\}$

$N(a+b\omega) = (a+b\omega)(a+b\bar{\omega}) = a^2+b^2-ab$.

例 $2 \in \mathbb{Z}[\omega]$ 是素元

$\left(U(\mathbb{Z}[\omega]) = \{\pm 1, \pm\omega, \pm\omega^2\}\right.$ $\Rightarrow$ 2 与 $1+\sqrt{-3}$ 相伴.

注. $\mathbb{F} \subseteq \mathbb{C}$. 子域

$\dim_{\mathbb{Q}} \mathbb{F} < \infty$. $\alpha \in \mathbb{F}$ 称为代数整数. 若 $\alpha^m + b_{m-1}\alpha^{m-1} + \cdots = 0$ $b_i \in \mathbb{Z}$.

$\mathcal{O}_{\mathbb{F}} = \{\alpha \mid \alpha$ 是代数整数$\}$

Fact, $\mathcal{O}_{\mathbb{F}} \subseteq \mathbb{F}$ 是环. Amazing.

此时 $\cdot$ Frac $\mathcal{O}_{\mathbb{F}} = \mathbb{F}$

3/4

[EX] $\mathbb{F} = \mathbb{Q}(\sqrt{-3})$

算 ~~$\mathbb{Q}(\sqrt{-3})$~~ $\mathcal{O}_{\mathbb{F}} = ?$

Fact. $\mathcal{O}_{\mathbb{F}}$ 是 Dedekind 整环 ⇐ PID

而 $\mathbb{Z}[\sqrt{-3}]$ 模 Dedekind 整环.

例. $\mathbb{Z}[\sqrt{2}] = \{m+n\sqrt{2}\}$.

Frac $\mathbb{Z}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$.

[EX] σ $\mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ 是域自同构

$a+b\sqrt{2} \mapsto a-b\sqrt{2}$

[EX] $\mathbb{Z}[\sqrt{2}]$ is ED

hint $N(a+b\sqrt{2}) = |(a+b\sqrt{2})\sigma(a+b\sqrt{2})|$

$U(\mathbb{Z}[\sqrt{2}])$ 无限群

Fact $\mathbb{Z}[\sqrt{3}]$ is ED

$\mathbb{Z}[\sqrt{-5}]$ isn't ED

但 $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ is ED

Gauss 整数环

R 上相伴, if $(a) = (b)$

相伴 → 研究 $U(R)$.

Fact. R is PID

$\{R$ 素元$\}/$相伴 $\xleftrightarrow{1:1}$ Max(R)

$a \longmapsto (a)$

Spec $R = \{(0)\} \cup$ Max(R).

Aim, 分类 $\mathbb{Z}[\sqrt{-1}]$ 中的素元

素 $2 = (1+i)(1-i)$

$\sim (i+1)^2$

PID 素 ‖ 不可约 性质好, 不可验证 / 性质差, 好验证.

Fact $1+i$ 素

用 N $N(1+i) = N(x)N(y)$

‖
2

$N(x) = 1 \Rightarrow x \in U(R)$.

$\mathbb{Z}[\sqrt{-1}]/(1+i)$ = ? 这个域多大?

$m+ni \equiv \begin{cases} 0 \\ 1 \\ i \\ 1+i \end{cases} \Rightarrow \mathbb{Z}[\sqrt{-1}]/(1+i) = \{\bar{0}, \bar{1}\} \simeq \mathbb{F}_2$

$\bar{1} = \bar{i}$

EX $\mathbb{Z}[\sqrt{-1}] \xrightarrow{\phi} \mathbb{F}_2$

$m+ni \longmapsto \overline{m+n}$

(核)

那 $\mathbb{Z}[2i]/(2) \simeq \{0, 1, i, 1+i\}$

Lem $z \in \mathbb{Z}[i]$

$N(z) = p$ 素 $\Rightarrow z$ 是素元 in $\mathbb{Z}[i]$.

$z = x \cdot y$ 即可.

Lem. p素 $p=4k+3$. p是 Gauss 素.

$p^2 = N(x)N(y)$, $N(x)=p$, $N(y)=p$

$m^2+n^2=p$ 与 mod4 即可.

例 $5=(1+2i)(1-2i)$

这两不相伴.

$13=(2+3i)(2-3i)$

$17=(1+4i)(1-4i)$

Fermat. $p=4k+1$ 素 $\Leftrightarrow p=a^2+b^2$ (a, b, 唯一)

$0<a<b$ $0<c<d$

注(1) ($\Leftarrow$) ✓

($\Rightarrow$) 困难

(2) $p=(a+bi)(a-bi)$ — Gauss 素, 不相伴

(3) 唯一性证明

$p = a^2+b^2 = c^2+d^2$

$\Rightarrow c+di \mid p=(a+bi)(a-bi)$

$c+di$ 与一个相伴

36. (存在性) 证. $p=4k+1$ 是 Gauss 素

$p=xy$.

非单位

$\mathbb{Z}[i]/(p) \overset{\Phi}{\simeq} \mathbb{F}_p[x]/(x^2+1)$ ← 非整.

$\mathbb{F}_p$

p $4k+1$ $\Rightarrow$ -1 是 $\square$ mod p 的二次剩余

$\Rightarrow$ x^2+1 在 $\mathbb{F}_p$ 上有根

以下. 证明 $\mathbb{Z}[i]/(p) \simeq \mathbb{F}_p[x]/(x^2+1)$ 即.

$\mathbb{Z}[i]/(2) \simeq \mathbb{F}_2[x]/(x^2+1)$

Φ 是

$\mathbb{F}_2[y]/(y^2)$

$p\geq 3$.

Step 1 $\mathbb{Z}[x]/(x^2+1) \xrightarrow{\Phi} \mathbb{Z}[i]$

有

$\overline{m+ni} \longmapsto \overline{m+nx}$

Step 2. $(p, x^2+1)/(x^2+1) \longmapsto (p)$

Step 3 中间等同构

$\mathbb{Z}[x]/(x^2+1) \xrightarrow{\sim} \mathbb{Z}[i]/(p)$

$\Big/ (p, x^2+1)/(x^2+1)$

$\Big\| \Psi$

$\mathbb{Z}[x]/(p, x^2+1) = \mathbb{Z}[x]/(p) \Big/ (p, x^2+1)/(p)$

$\mathbb{Z}[x]/(p) \overset{\Psi}{\simeq} \mathbb{F}_p[x]$ 诱导 $\mathbb{Z}[x]/(x^2+1) \Big/ (p, x^2+1)/(p) \xrightarrow{\widetilde{\Psi}} \mathbb{F}_p[x]/(x^2+1)$

$\Psi: (p, x^2+1)/(p) \longmapsto (x^2+1)$

[Thm] Gauss 素数分类定理

相伴下

① $1+i$

② $4k+3$ 型

③ $4k+1$ 型的 $p = a^2+b^2 = (a+bi)(a-bi)$ $a<b$.

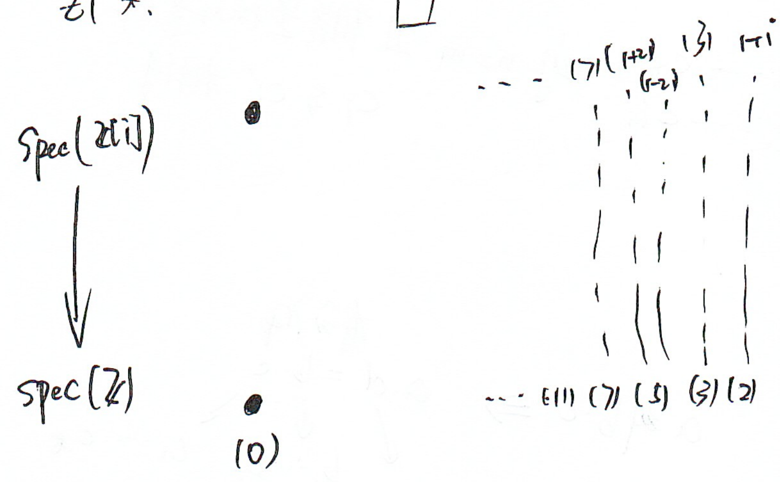
①②③ 都是 ✓

$z \in \mathbb{Z}[i]$, z 素

$N(z) = p_1^{e_1} \cdots p_\ell^{e_\ell}$ ①②③ 之积

$z \mid N(z) = [\cdots]$

$z \mid *$.   □



EX $\mathbb{Z} \hookrightarrow \mathbb{Z}[i]$

$\forall \mathfrak{p} \in \mathrm{spec}\,\mathbb{Z}[i]$ $\mathfrak{p} \cap \mathbb{Z} \in \mathrm{spec}(\mathbb{Z})$

3.26

在 $\mathbb{Z}[i]$ 中算数.

$29-2i$ 的分解 $N(29-2i) = 5 \times 13^2$

~~$1+2i = 5 \mid z\bar{z}$~~ $\frac{z}{1+2i} = \frac{z(1-2i)}{5} = \frac{(29-2i)(1-2i)}{5}$ ✓

$1+2i \mid z\bar{z}$ $\frac{z}{1-2i} = \frac{(29-2i)(1+2i)}{5}$ ✗

$\Rightarrow 1+2i \mid z$ $13 = (2+3i)(2-3i)$ 继续试

可能 $1+2i \mid z \Leftrightarrow 1-2i \mid \bar{z}$

注：$\mathbb{Z}[i]$ 有素分解.

二平方定理 $\Longleftrightarrow n = 2^{l} p_1^{\alpha_1} \cdots p_t^{\alpha_t}$

对 $p_i = 4k+3$ 型 α_i 偶

($\Leftarrow$) $(1+1)^{l}$ $\underbrace{(p_i^2+0^2)^{\alpha_i}}_{4k+3\text{型}}$ $\underbrace{(a^2+b^2)^{\alpha_i}}_{4k+1\text{型}}$

($\Rightarrow$) $n = a^2+b^2$
$= (a+bi)(a-bi)$
$= z\bar{z}$
$= \cdots$

EX 书 92. ex.2.

EX $p = a^2+b^2$ $\quad \mathbb{Z}[i]/(a+bi) \cong \mathbb{F}_p$

UFD

1. 存在不可约分解
2. 唯一性. $a = c_1 \cdots c_n = c_1' \cdots c_m'$ 则 $n=m$ 且相差置换而意义下 c_i 与 c_i' 相伴

有限

Fact. 设 R 为 UFD

则 (1). 不可约元 = 素元

proof: 设 $a \in R$ 不可约 $\quad a \mid b\cdot c \Rightarrow$ $a\cdot d = b\cdot c$ 有分解
$\downarrow$ $d_1 \cdots d_s$, $\downarrow$ $b_1 \cdots b_r$, $\downarrow$ $c_1 \cdots c_t$

由唯一分解 $\Rightarrow$ a 与 $b_1 \cdots b_r$. $c_1 \cdots c_t$ 之一相伴
$\Rightarrow a \mid b$ 或 $a \mid c$ $\qquad \square$

Rmk UFD 的不可约分解其实是素分解

R 中有标准分解

(2) R 为 UFD, $a = u p_1^{n_1} \cdots p_r^{n_r}$ $\quad p_i \not\sim p_j$ 时 $\quad n_i \geq 1$
p_i 素
u 单位

Cor 标准分解 $\Rightarrow$ a 的因子总形如 $v p_1^{\tilde{n}_1} \cdots p_r^{\tilde{n}_r}$ $\quad v \in U(R)$
$0 \le \tilde{n}_i \le n_i$

EX

(3) R UFD

gcd lcm exist

$a = u\, p_1^{n_1} \cdots p_r^{n_r}$

$b = v\, p_1^{m_1} \cdots p_r^{m_r}$ $\quad 0 \le m_i, n_i$

$\gcd(a, b) = \prod_i p_i^{\min \cdots} \cdots$

$\mathrm{lcm}(a, b) = \prod p_i^{\max \cdots}$

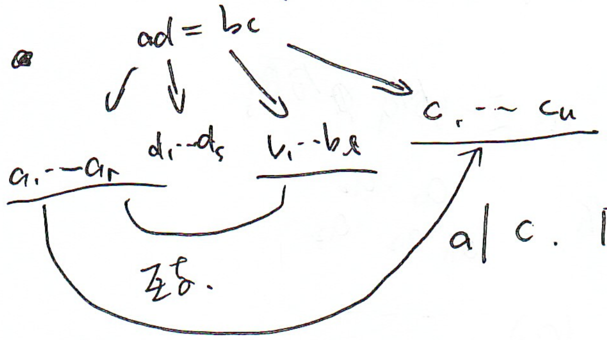
(4) R UFD

Frac R 有既约表达 $\frac{a}{b} = \frac{a'}{b'}$ $\gcd(a', b') = 1$ (约去gcd)

既约表达唯一 本质上. $\gcd(a,b) \sim 1 \sim \gcd(c,d)$. $\frac{a}{b} = \frac{c}{d}$.

则 $a \sim c$, $b \sim d$

proof



$a \mid c$. 同理 $c \mid a$. $\Rightarrow a \sim c$

还是唯一性.

$X \subseteq R$ 子集 $\quad (X) = RX = \left\{ \sum_{\text{finite}} r_i x_i \;\middle|\; \begin{matrix} r_i \in R \\ x_i \in X \end{matrix} \right\} \lhd R$

If $\# X = 1 \Rightarrow (X)$ is a principal ideal

so 有子集就有理想 (比主理想……的推广)

有限生成理想 $I = (X)$ $\# X < \infty$.

不有限生成的 $K[x_1, \cdots x_n] = R$

$M = (x_1, \cdots x_n)$ 才是一个

Def 环R 被称为Noether环. 若 $\forall I \lhd R$, I 是有限生成的 (f.g.)

例 PID、K.

4.0 [Thm] Hilbert 基定理 (基底)

设 R 为 Noether 环，则 $R[x_1, \cdots x_n]$ 的商环都是 Noether 环.

证明 只需证明 $n=1$ 即可

略

C_{n0} 基都是 Noether 环. (但 Noether 环的子环不一定)

[Thm] R Noether 整环 | 所有元有限个是素因子
则 R 中主不可约分解

证. 设 $a \in R$ 没有不可约分解 (a 一定可约)
非零非单位
$a = a_1 \cdot a_2$ a_1, a_2 之一必有分解
$\vdots$ 递归下去 $a_1 \cdot a_2$
$a_{11}\ a_{12}\ a_2$
$\cdots$

$\Rightarrow (a) \subsetneq (a_1) \subsetneq (a_{11})$
无限升链
ideal 向

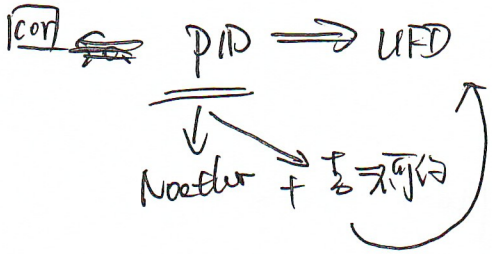
[EX] $\mathbb{Q}$ R Noether
$I_1 \subsetneq I_2 \subsetneq \cdots$
则升链稳定.

考虑前

Fact. R 整环，若 $a \in R$ 有分解 $a = p_1 \cdots p_r$
则 a 的不可约分解唯一

proof. $p_1 \mid c_1 \cdots c_r = c_1' \cdots c_s'$ □

[Cor] 整环 R UFD $\Leftrightarrow$ R 有分解.
(2) 环有不可约分解 UFD $\Leftrightarrow$ "不可约 $\Rightarrow$ 素"
分解唯一



3.28.

Thm (Gauss) R is UFD ⇒ R[x] is UFD

例 Z[x] 与 not a PID

$R[x,y] = (R[x])[y]$

Key difficulty: $f(x) \in R[x]$ 不可唯一化.

Pf (Content) $f = a_n x^n + \cdots + a_0 \in R[x]$ $a_n \neq 0$

$c(f) = \gcd(a_n, \cdots a_0)$

$f(x)$ 称为本原的 若 $c(f) = 1$ (相伴)

Idea $R \hookrightarrow K$ 分式域

$R[x] \hookrightarrow \frac{K[x]}{\text{UFD}}$

Lem (Gauss lemma) $f(x), g(x) \in R[x]$. $f(x), g(x)$ 是本原的 ⇒ $f(x)\cdot g(x)$ 是本原的

proof of Gauss thm. $f = c(f)\cdot f_0(x) = c_1 \cdots c_n f_0(x)$

~~$g(x) = c(f) \cdot f_0(x)$~~

Step 1 c_i 在 R 中 ⇒ c_i 在 R[x] 中

Ex hint $R[x]/(c_i)$ 是整环. ($\cong R/(c_i)[x]$)

Step 2. $f_0(x)$ 在 K[x] 中分解 $f_1(x) \cdots f_n(x)$ 真分 (在 K[x] 上不可约)

$f_1(x) = \frac{1}{a}\tilde{f}_1(x) = \frac{c(\tilde{f}_1)}{a}\cdot \bar{f}_1(x)$ ($\frac{c(\tilde{f}_1)}{a} \in K$; $\bar{f}_1(x)$ 在 R[x] 中本原)

$\Rightarrow a f_0(x) = \frac{b}{\text{本原}} \bar{f}_1(x) \cdots \bar{f}_n(x)$

- $\bar{f}_i \in R[x]$ 本原
- $\bar{f}_i$ 在 K[x] 中不可约

由 Gauss lem $\bar{f}_1(x) \cdots \bar{f}_n(x)$ 本原

⇒ 求 Content $a \sim b$

⇒ $f_0(x) = \bar{f}_1(x) \cdots \bar{f}_n(x)$ in R[x] ∎

4.

Step 3. $\bar{f}_i(x)$ 在 $R[x]$ 中是

$\bar{f}_i(x) \mid u(x)\cdot v(x) \Rightarrow \bar{f}_i(x) \mid u(x)$ or ...

$R[x]$

$\bar{f}_i(x) \mid u(x)v(x) \Rightarrow \bar{f}_i(x) \mid u(x)$ or ...

$K[x]$ $K[x]$

$\Rightarrow u(x) = \bar{f}_i(x)\, h(x)$ 通分

$u(x) \in R[x]$, $\bar{f}_i(x) \in R[x]$, $h(x) \in K[x]$

$h(x) = \frac{b}{a}\bar{h}(x)$ $\in R[x]$ 本原 $\quad u(x) = \bar{f}_i(x)\cdot\frac{b}{a}\bar{h}(x)$

本原

$\Rightarrow a c(u) \sim b$ in R

$\Rightarrow$

$\Rightarrow u(x) = c(u)\, \bar{f}_i(x)\, \bar{h}(x)$

推论 一个引理. $f(x)$ $R[x]$ 本原, $K[x]$ 是 $\Rightarrow f(x)$ 在 $R[x]$ 是

证. $R[x] \hookrightarrow K[x] \to K[x]/(f(x)) := L$

域

$R[x] \cap (f(x)K[x]) \overset{\text{Step 3}}{=\!=} f(x)R[x]$

整环 $R[x]/(f(x)R[x]) \hookrightarrow L$ 环同态 是域

$\square$

proof of Gauss lem

(proof 1) $f(x)\cdot g(x) = \sum_{l=0}^{m+n} c_l x^l$

$c_l = \sum_{i+j=l} a_i b_j$

Claim $c_1 \sim c_{m+n}$ 至少 $\exists$ 一个 p 使 $p \mid c_1 \cdots p \mid c_{m+n}$

$\exists!\ i_0 \quad 0 \le i_0 \le n$

$p \mid a_0 \cdots p \nmid a_{i_0}$

$\exists!\ j_0$ for $b \cdots$

$c_{i_0+j_0} = (a_0 b_{i_0+j_0} + \cdots) + a_{i_0} b_{j_0} + (a_{i_0+1} b_{j_0-1} + \cdots)$

$p \mid$ $\qquad$ $p \mid$

$\Rightarrow p \nmid c_{i_0+j_0}$. □

(proof 2) 要 $p \in R$. $p \mid c_l \ \forall l$

$\pi : R \longrightarrow R/(p)$

$r \longmapsto \bar{r}$

$\bar{\pi} : R[x] \longrightarrow R/(p)[x]$

$\bar{\pi}(f(x)g(x)) = \bar{0}$

$\bar{\pi}(f(x)) \cdot \bar{\pi}(g(x)) = \bar{0}$ 在 $R/(p)$ 整.

$\Rightarrow$ WLOG $\bar{\pi}(f(x)) = \bar{0}$ 勿 □

用 $R[x]$ 元不可约性判断 $K[x]$ 元不可约性.

If R is a UFD, $K = \mathrm{Frac}\, R$.

If $f(x) \in R[x]$ 本原. TFAE

$f(x)$ 在 $R[x]$ 中不可约 $\Leftrightarrow$ $f(x)$ 在 $K[x]$ 中不可约

Ex

难一些 our Aim.

例.

$f(x) = x^3 + 3x - 2$.

在 $\mathbb{Q}$ 上是否不可约?

mod p 方法.

Ges--- 判别 RUFD

$f(x) \in R[x]$ 本原, 不可约 $\Leftarrow$ 设 p 在 R 中素 $p \nmid c_n$. $p \mid c_i$ $p \nmid c_0$

$c_n x^n + \cdots + c_0$ 则 $f(x)$ 在 $R[x]$ 中不可约

证 (证一) $f(x)=g(x)h(x)$ in $R[x]$
m次 $n-m$次 g, h 都是本原

$\Rightarrow c_0 = a_0 \cdot b_0$
$p \mid c_0$, $p^2 \nmid c_0$ $\Rightarrow$ WLOG $p \mid a_0$ $p \nmid b_0$
$\exists 1$ $i_0 \geq 1$ $p \mid a_0 \cdots p \mid a_{i_0-1}$ $p \nmid a_{i_0}$ $(i_0 \leq m < n)$

$c_{i_0} = \underline{a_{i_0} b_0} + \underbrace{\cdots + a_0 b_{i_0}}_{p \mid}$

$p \nmid c_{i_0}$

(证二) $R[x] \xrightarrow{\pi} R/(p)[x]$
$f(x) = g(x)h(x)$
$\downarrow$ $\downarrow$ $\downarrow$
$c_n x^n$ 单项式 但 $p^2 \nmid c_0$ 矛盾

例 $x^2-2 \in \mathbb{Q}[x]$ $p=2$
例 $1+\cdots+x^{p-1}$ $\mathbb{Q}[x]$
引理(平移) R UFD, $b \in R$, $g(x) \in R[x]$. $g(x+b) = a_n(x+b)^n + \cdots + a_0$ 展开
1. $g(x)$ 不可约 $\Leftrightarrow$ $g(x+b)$ 不可约
2. $g(x)$ 本原 $\Leftrightarrow$ $g(x+b)$ 本原

EX

例 $y^3-x^2 \in k[x,y] = (k[x])[y]$ 在 $k[x]$ 上 不可约 本原
then $k(x)[y]/(y^3-x^2)$ 是域 $\simeq$ Frac$\left(k[x,y]/(y^3-x^2)\right)$

Ex $R = k[t]$.

$S = \{ f(t) \in R \mid f(t) = a_0 + a_2 t^2 + \cdots \}$

子环 $\subseteq R$.

(1) $S \simeq k[x,y]/(y^2 - x^3)$

(2) $\mathrm{Frac}(S) \simeq k(t)$ $\quad \frac{t^3}{t^2} \mapsto t$

一元有理"函数"域

$k(t) = \mathrm{Frac}(k[t])$

$= \left\{ \frac{f(t)}{g(t)} \mid g(t) \neq 0 \right\}$

环的直积

R, S 环 $\quad R \times S = \{ (r,s) \mid r \in R, s \in S \}$

$+, \cdot$ 分量.

$R \times S$ 非整 $\quad (1,0) \cdot (0,1)$

Fact $U(R \times S) = U(R) \times U(S)$

中国剩余定理.

$I_1, \cdots I_n \lhd R$.

$I_i + I_j = R$ (两两互素)

则 $\phi: R \longrightarrow \prod_{i=1}^{n} R/I_i$ 是环同态 ($\forall i \neq j$)

$r \longmapsto (r + I_1, \cdots r + I_n)$

满射同构 $R/(I_1 \cap \cdots \cap I_n) \xrightarrow{\sim} \prod_{i=1}^{n} (R/I_i)$

$\ker \phi = (I_1 \cap \cdots \cap I_n)$. 只要 ϕ 是满射

$\begin{cases} b \equiv a_1 \bmod I_1 \\ \vdots \\ b \equiv a_n \bmod I_n. \end{cases}$

只要证 $x \mapsto (1, 0 \cdots 0)$

$\#\ I_1 + I_2 \cdots I_n = R$ 即可

~~check~~

fill 坑 了.