近世代数.

2.26

Def $f: X \to Y$, $f': X' \to Y'$, f 与 f' 相等

若 $X = X'$, $Y = Y'$, $\forall x \in X$, $f(x) = f'(x)$

Let 范 a category

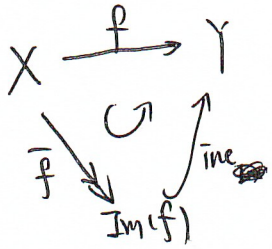
since the maps (morphisms) have associate law and identity

单射 sign $f: X \hookrightarrow Y$

满射 sign $f: X \twoheadrightarrow Y$

双射 sign $f: X \xrightarrow{\sim} Y$

Fact 有交换投图



可作 $f = inc \circ \bar{f}$ 称为典范分解

单 满

inc 的记号借助) 定义和性质

EX ① "$f: X \to Y$ 单" $\Leftrightarrow$ "$\forall\ Z \underset{g'}{\overset{g}{\rightrightarrows}} X$ 满足 $f \circ g = f \circ g' \Rightarrow g = g'$"

(f 对这个满足左消去律)

② "$f: X \to Y$ 满" $\Leftrightarrow$ "f 对这个满足右消去律

i.e. "$\forall\ Y \underset{h'}{\overset{h}{\rightrightarrows}} Z$. 满足 $hf = h'f \Rightarrow h = h'$"

③ "$f: X \to Y$ 双" $\Leftrightarrow$ ~~Set~~ language

Category

$\exists\ g: Y \to X$ s.t. $g \circ f = Id_X$

$f \circ g = Id_Y$

此时 g 是 f 的逆, 且唯一

($g = f^{-1}$)

构造集合 ① 无交并 $X \sqcup Y$ (X, Y 中元素不同).

② 笛卡尔积 $X \times Y = \{(x, y) \mid x \in X, y \in Y\}$ 相等 $\Leftrightarrow$ 含量相同.

③ $Map(X, Y) = \{f: X \to Y\}$

【EX】 令 $\mathcal{P}(X) := X$ 的幂集

证：有双射 $Map(X, \{0,1\}) \xrightarrow{\Phi}_{\sim} \mathcal{P}(X)$

hint: $\forall f \in LHS$, $\Phi(f) = \{x \in X \mid f(x) = 1\} \in RHS$

逆出逆即可.

【EX】① 有双射 $Map(X \sqcup Y, Z) \xrightarrow{\sim} Map(X,Z) \times Map(Y,Z)$

hint $f \mapsto (f|_X, f|_Y)$

Rmk: $f|_X = f \circ inc$

$X \hookrightarrow X \sqcup Y \to Z$

② $Map(X, Y \times Z) \xrightarrow{\sim} Map(X,Y) \times Map(X,Z)$

$g \mapsto (g_1(x), g_2(x))$

hint:

③ $Map(X \times Y, Z) \xrightarrow{\sim} Map(X, Map(Y,Z))$

hint $\Theta(f): X \to Map(Y,Z)$

$x \mapsto (y \mapsto f(x,y))$

Θ_X

等价关系

X 上的等价关系是 $R \subseteq X \times X$, 满足

① 自反 $(x,x) \in R \quad \forall x \in X$

② 对称 $(x,y) \in R \Rightarrow (y,x) \in R$

③ 传递 $(x,y) \in R, (y,z) \in R \Rightarrow (x,z) \in R$

~~记号~~ 记号 $\boxed{a \overset{R}{\sim} b}$

以下证作(用 $\overset{R}{\sim}$ 记号)

$x \overset{R}{\sim} x$

$x \overset{R}{\sim} y \Rightarrow y \overset{R}{\sim} x$

$x \overset{R}{\sim} y, y \overset{R}{\sim} z \Rightarrow x \overset{R}{\sim} z$.

设 $\overset{R}{\sim}$ 为 X 上的等价关系

$\forall a \in X$, $[a] := \{x \in X \mid x \overset{R}{\sim} a\}$

↑ a 的等价类

Fact: ① $\forall b \in [a]$ 则 $[b] = [a]$

$\forall x \in [b] \Rightarrow x \overset{R}{\sim} b, b \overset{R}{\sim} a$

$\Rightarrow x \overset{R}{\sim} a \Rightarrow x \in [a]$

~~$x \in [b]$~~ $\Rightarrow [b] \subseteq [a]$

$\forall y \in [a] \Rightarrow y \overset{R}{\sim} a, b \overset{R}{\sim} a \Rightarrow b \overset{R}{\sim} b$ (对称性)

$\Rightarrow y \overset{R}{\sim} b \Rightarrow y \in [b] \Rightarrow [a] \subseteq [b]$

Rmk. 这里不能写同比. 详细证明细节

Fact ② $[a] \cap [a'] \neq \phi \iff [a] = [a']$

left for exercise.

2.28

def 商集 $X/R = \{\text{所有等价类}\} \subseteq \mathcal{P}(X)$

商映射 $X \xrightarrow{\pi_R} X/R$

$x \mapsto [x]$

def 完全代表元集 (wrt R) $S \subseteq X$

s.t $\forall a \in X \ \exists! \ s \in S.$ sRa $([s]=[a])$

Fact. ① 设 S 为完全. 则 $S \xhookrightarrow{inc} X \longrightarrow X/R$ 是一个双射

$s \mapsto s \longmapsto [s]$

② $X = \bigsqcup_{s \in S} [s]$

def X 的一个分拆(割分) 指 $P \subseteq \{X_i \mid i \in I\} \subseteq \mathcal{P}(X)$

with 1. $X_i \neq \phi$

2. $X_i \cap X_j = \phi$

3. $\bigcup_{i \in I} X_i = X$ (即 $\bigcup_{X_i \in P} X$)

Fact $\{R\} \xleftrightarrow{1-1} \{\text{分拆}\}$

EX show $P = \{X_i \mid i \in I\} \longrightarrow \mathcal{P}$: $x \sim_P y$ 当 $\exists i \in I$ $x \in X_i$ & $y \in X_i$

Fact: $f: X \to Y$ 诱导了等价关系 $\sim_f$

$x \sim_f x'$ 当 $f(x) = f(x')$ 此时 $[x] = f^{-1}(f(x))$

NOTE. $f^{-1}(y) \neq \phi \iff y \in Im(f)$

映射的基本定理 $f: X \to Y$ 诱导双射 $\bar{f}$

$\bar{f}: X/\sim_f \to Im(f)$

$[x] \mapsto f(x)$

4. Q1. 证 $\bar{f}$ is well-defined. ?

i.e. 证 $[x]=[x']$. we have $f(x)=f(x')$

Q2. $\bar{f}$ is injective ? surjective ?

Rmk
$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle \pi_f}\downarrow & \circlearrowright & \uparrow{\scriptstyle i_{nc}} \\ X/_f & \xrightarrow[\sim]{\bar{f}} & Im(f) \end{array} \qquad f = i_{nc}\circ\bar{f}\circ\pi_f$$

$$\begin{array}{ccc} x & \longmapsto & f(x) \\ \downarrow & & \uparrow \\ [x] & \longmapsto & f(x) \end{array}$$

EX 若 $\exists\ h: X/_f \to Im(f)$, with $f = inc\circ h\circ\pi_f$ 则 $h=\bar{f}$

二元运算 *

结合律 $\psi(x,\psi(y,z)) = (\psi(x,y),z)$

$$\begin{array}{ccc} X\times X\times X & \xrightarrow{\psi\times Id_X} & X\times X \\ \downarrow{\scriptstyle Id_X\times\psi} & \circlearrowright & \downarrow{\scriptstyle\psi} \\ X\times X & \xrightarrow[\psi]{} & X \end{array}$$

1.2. 环 A1 ~ A4 加 结合律 交换律 唯一(易证唯一) 负元(易证唯一)
M1 ~ M2 乘 $a+0_R=a$ 记号 "$-a$"
D1 ~ D2 加乘相容 结合律 含么
$a\cdot 1_R = a = 1_R\cdot a$
分配律 左右分配 (易证么元唯一)

EX 0_R 的负元是 0_R

注① 这里默认为含么环.
② 环相等 $\Leftrightarrow$ 集合和运算都相等

例① 高斯整环 $\mathbb{Z}[\sqrt{-1}] = \{m+n\sqrt{-1} \mid m,n\in\mathbb{Z}\} \subseteq \mathbb{C}$; ② $\mathbb{Z}$
③ 一元多项式环 $\mathbb{Q}[x]$
④ 同余类环 $\mathbb{Z}_n$
⑤ $M_n(\mathbb{C})$ $\mathbb{C}$ 上的全体 $n\times n$ 矩阵

1-4 都交换 5. 含么非交换

EX $\mathbb{Z}_n$ 上的 $\bar{i}+\bar{j} = \overline{i+j}$ 良定.
$\bar{i}\cdot\bar{j} = \overline{ij}$

环的基本性质 R

① $-(-a)=a \quad \forall a\in R$

② 加法有消去律

③ 定义减法 $a-b:=a+(-b)$

④ 倍数 $na:=\underbrace{a+\cdots+a}_{n\text{个}a}$

$-na:=\underbrace{(-a)+\cdots+(-a)}_{n\text{个}}$

⑤ EX $\forall n,m\in\mathbb{Z},\ a\in R$

$(n+m)a=na+ma$

⑥ EX $\forall n\in\mathbb{Z},\ a\in R$

$na=(n\cdot 1_R)\cdot a$

$=a\cdot(n1_R)$

$n=0$ 有 $0_R=0_R\cdot a \quad \forall a\in R$

$0_R\cdot a=(0_R+0_R)\cdot a$

$=0_R\cdot a+0_R\cdot a$

$0_R=0_R\cdot a$

⑦ EX $\forall a,b\in R,\ n\in\mathbb{Z}$

$a\cdot(nb)=(na)\cdot b=n(a\cdot b)$

⑧ 广义分配律 $\sum_{i=1}^{n}a_i:=a_1+\cdots+a_n$

$\left(\sum_{i=1}^{n}a_i\right)\left(\sum_{j=1}^{m}b_j\right)=\sum_{i,j=1}^{n,m}a_ib_j=\sum_{i=1}^{n}\sum_{j=1}^{m}a_ib_j$

零环：R TFAE

(1) $0_R=1_R$

(2) $R=\{0_R\}$

(3) $\#R=1$

以下只研究非零环 ($R\neq\emptyset$ 是定义)

(2) $\Rightarrow$ (3) $\Rightarrow$ (1) $\Rightarrow$ (2)

$0_R\cdot a=1_R\cdot a$

$\|\quad\quad\|$

$0\quad\quad a$

二元环 $R=\{x_1,x_2\}$

$\|\quad\quad\|$

$0_R\neq 1_R$

+	0_R	1_R
0_R	0_R	1_R
1_R	1_R	0_R

·	0_R	1_R
0_R	0_R	0_R
1_R	0_R	1_R

$R\cong\mathbb{Z}_2$

6. 以下 R 为含幺交换环 非零环

$\forall n \geq 0$, $a \in R$

$a^0 = 1_R$ $a^n = \underbrace{a \cdots a}_{n个}$

有 $a^{n+m} = a^n \cdot a^m$ $\forall n, m \geq 0$

二项式定理 $a, b \in R$ $n \geq 1$

$$(a+b)^n = \sum_{i=1}^{n} \binom{n}{i} a^i b^{n-i}$$

EX ~~proof~~ prove it.

除法 $a \in R$ 称为单位，若 a 在 R 中乘法可逆

$\exists b \in R$, $a \cdot b = 1_R$

记 $b = a^{-1}$

Fact
- $(a^{-1})^{-1} = a$
- $(1_R)^{-1} = 1_R$
- 0_R 不可逆

R 的单位群

$U(R) = \{a \in R \mid a$ 可逆$\}$

- $a \in U(R) \Rightarrow a^{-1} \in U(R)$
- $a, b \in U(R) \Rightarrow ab \in U(R)$
- $1_R \in U(R)$

a 可逆 $\Rightarrow$ 可逆元可消去 $a \cdot x = a \cdot y$

$\Rightarrow x = y$

$x = a^{-1}ax = a^{-1}ay = y$

Fact (1) $-1_R \in U(R)$

$(1_R + -1_R)(1_R + -1_R) = 1_R \cdot 1_R - 1_R + (-1)_R(-1_R) = 0$

$\Rightarrow -1_R \cdot -1_R = 1_R$

(2) $U(\mathbb{Z}) = \{-1, 1\}$

$U(\mathbb{Q}) = \mathbb{Q}^*$

EX $U(\mathbb{Z}_n) = \{a \mid \gcd(a, n) = 1\}$

3.5

以下我们约定 R 为含幺交换环

Def 整环 R，若 "$a \cdot b = 0_R \Rightarrow a = 0_R$ 或 $b = 0_R$" $\Leftrightarrow$ "$a, b \neq 0_R \Rightarrow a \cdot b \neq 0_R$"（逆否）

例 $\mathbb{Z}$, $\mathbb{Z}_n$ 不 n 合.

Prop R 整环 $\Rightarrow$ $a \neq 0$ "$a \cdot b = a \cdot c \Rightarrow b = c$" 即 消去律

Def R 域 $a \neq 0_R \Rightarrow a \in U(R)$ （非零元可逆）

Fact 域 $\Rightarrow$ 整环

Prop $n \geq 2$ 下TFAE

(1) $\mathbb{Z}_n$ 整

(2) $n=p$

(3) $\mathbb{Z}_n$ 域

(1)⇒(2) 显然. (2)⇒(3) Euler

(2)⇒(3) $au+pv=1$ Bezout

↑ 逆元

为强调, 记 $\mathbb{F}_p = \mathbb{Z}_p$

Ex 设 R 为有限环(含幺交换环) slogan "R 整 $\Leftrightarrow$ R 域"

Def 子环: $S \subseteq R$ 满足 $\begin{cases} 1 \in S \\ S \text{ 对 } +,-,\cdot \text{ 封闭} \end{cases}$

(i.e. $\forall a,b \in S$, $a+b, a-b, ab \in S$)

Def 设 K 域

子环 $S \leq K$ 满足 $\forall a \in S \Rightarrow a^{-1} \in S$

此时 S 是域

例 ① $\mathbb{Z} \subseteq \mathbb{Q}$ 子环 ② $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ 子域

例 $\mathbb{Z}$ 没有真子环 $1+\cdots$

$\mathbb{Q}$ 没有真子域 $1+\cdots \Rightarrow \mathbb{Z} \Rightarrow \mathbb{Q}$

$\mathbb{F}_p$ 没有真子域 (当然没有真子环)

Ex 分类 $\mathbb{Q}$ 的子环 Hint: $\left\{ \frac{m}{p^n} \;\middle|\; m \in \mathbb{Z},\ n \geq 0 \right\} \subseteq \mathbb{Q}$

$\mathbb{Z}\left[\frac{1}{p}\right]$

例 $\mathbb{Q}(\sqrt{-1}) = \{ a+b\sqrt{-1} \mid a,b \in \mathbb{Q} \} \subseteq$ 子域 $\mathbb{C}$

! 分类 $\mathbb{Q}(\sqrt{-1})$ 的子域

设 $S \subseteq$ 子域 $\mathbb{Q}(\sqrt{-1})$

证. $1 \in S \Rightarrow \mathbb{Z} \subseteq S \Rightarrow \mathbb{Q} \subseteq S$ $\mathbb{Q} = S$

若 $\mathbb{Q} \subsetneq S \Rightarrow \exists\ a+b\sqrt{-1} \in S$ $b \neq 0$, $a,b \in \mathbb{Q}$

$\Rightarrow b\sqrt{-1} \in S$. 又 $b^{-1} \in \mathbb{Q} \in S \Rightarrow \sqrt{-1} \in S$

$\Rightarrow a+b\sqrt{-1} \in S \Rightarrow S = \mathbb{Q}(\sqrt{-1})$.

8. 商环与理想

设 $(R,+,\cdot)$ 为两个含幺交换环（运算是不同的，但是不做区分）

$(S,+,\cdot)$

$\theta: R \to S$ 称为环同态（ring homomorphism）

满足 ① $\theta(a+_R b) = \theta(a) +_S \theta(b)$

② $\theta(a \cdot b) = \theta(a) \cdot \theta(b)$

③ $\theta(1_R) = 1_S$ ★

若 θ 为双射 $\Rightarrow$ θ 为环同构，记 $\theta: R \xrightarrow{\sim} S$

prop ① $\theta(0_R) = \theta(0_S)$

（$\theta(0_R+0_R)$ ···）

② **EX** θ 保减法 $\theta(a-b) = \theta(a) - \theta(b)$

③ $\theta(a^m) = (\theta(a))^m$

④ 环同态的存在是不平凡的

例 $\theta: \mathbb{Q} \to \mathbb{Z}_8$

否则 $\theta(1) = \bar{1}$

$\theta(8) = 0$ 但 $\theta(\frac{1}{8}) = ?$

$\theta(1) = \theta(8 \cdot \frac{1}{8}) = 0$ ↯

$\| $

$\bar{1}$

EX 同理可证 $\mathbb{Z}_8 \to \mathbb{Q}$

环同态的例子 $Id: R \to R$ （是同构）

lem $\theta: R \to S$ 同态 $a \in U(R) \Rightarrow \theta(a) \in U(S)$

且 $\theta(a^{-1}) = (\theta(a))^{-1}$

proof: $\theta(a) \cdot \theta(a^{-1}) = \theta(1) = 1 \Rightarrow \theta(a^{-1}) = (\theta(a))^{-1}$ □

故 $\theta|_{U(R)}: U(R) \to U(S)$ 是群同态

Fact. 若 θ 是环同构 $\Rightarrow \theta^{-1}$ 是环同构

proof. $\theta(1_R) = 1_S \quad \theta^{-1}(1_S) = 1_R$

(加法) $x, y \in S \quad \theta^{-1}(x) + \theta^{-1}(y) \overset{?}{=} \theta^{-1}(x+y)$

作用 θ 再拉回即可

(乘法) 类似 □

注 同态的定义是同态 $\Rightarrow$ CRing 范畴.

$Aut(R) = \{\theta: R \to R$ 是环自同构$\}$.

1°. $Id \in Aut(R) \Rightarrow Aut(R) \neq \emptyset$

2°. $Aut(R)$ 是 R 的自同构的群 (不一定 Abel)

例 $Aut(\mathbb{Z}) = \{Id_{\mathbb{Z}}\}$ (要求保环导致的"唯一")

类似 $Aut(\mathbb{Q}) = \{Id_{\mathbb{Q}}\}$ 先标 $\tau\circ\tau = Id$

例 $Aut(\mathbb{Z}[\sqrt{7}]) = \{Id, \tau\}$

proof: $\forall \theta \in Aut(\mathbb{Z}[\sqrt{7}])$

$1 \mapsto 1 \quad m \mapsto m \ (m \in \mathbb{Z})$ ✓

$\sqrt{7} \mapsto ?$ $(\theta(\sqrt{7}))^2 = \theta(7) = -1$

Question $(\theta\sqrt{7})^2 = -1$ 在 $\mathbb{Z}[\sqrt{7}]$ 上解

利用 $\mathbb{Z}[\sqrt{7}] \subseteq \mathbb{C}$

$\Rightarrow \theta(\sqrt{7}) = \begin{matrix} i & -i \\ \downarrow & \downarrow \\ Id & \tau \end{matrix}$

EX $Aut(\mathbb{Q}(\sqrt{7})) = \{Id, \tau\}$

EX 设 $\theta: R \to S$ 同构

则 ① $a \in U(R) \Leftrightarrow \theta(a) \in U(S)$

② $U(R) \to U(S)$

③ R 整 $\Leftrightarrow S$ 整

④ $Aut(R) \to Aut(S)$.

10

例 $\forall R$，$\exists!$ 环同态

$\mathbb{Z} \xrightarrow{\theta} R$，$n \mapsto n 1_R$

特征同态

$f: X \to Y$ 映射

$X \xrightarrow{f} Y$

$\pi_f \downarrow$ ↷ $\uparrow$ inc

$X/\sim_f \xrightarrow{\tilde{f}} Im(f)$

explain

$\theta: R \to S$ 环同态

$R \xrightarrow{\theta} S$

$\pi_\theta \downarrow$ $\uparrow$ inc

R/θ $\quad Im(\theta) = \{\theta(r) \mid \forall r \in R\}$

S的子环

$a \underset{\theta}{\sim} b \Leftrightarrow \theta(a) = \theta(b)$

$\Leftrightarrow \theta(a-b) = 0 \Leftrightarrow a-b \in \ker\theta$

定义 $\ker\theta = \{r : \theta(r) = 0\} \subseteq R$

同态θ的核

不是子环！我们不要它

因为 $\theta(1) = 1_R$

那么 $[a] = \{b \mid a-b \in \ker\theta\}$

$= a + \ker\theta$

ker的等价

Fact. ① $\ker\theta$ 对加减乘封闭

↓

$\theta(rr') = \theta(r)\theta(r') = 0_{RS}$

② $1_R \notin \ker\theta$

③ $\forall a \in R$ $\quad r \in \ker\theta \Rightarrow a \cdot r \in \ker\theta$ 这一条很子 乘法左封闭

↓

对"任乘"封闭.

= 是这一根棍完全区别于子环

抽象这三条即为理想

3.7

定义(理想) $\emptyset \neq I \subseteq R$ 环 被称为环R的理想 ($I \lhd R$)

若 ① $\forall a, b \in I$. $a+b \in I$ （$\Rightarrow I$ 对 $+, -$ 都封闭，因 $-r = -1_R \cdot r$

② $\forall a \in R$ $r \in I \Rightarrow a \cdot r \in I$

例 $\{0_R\}$，R 都是R的理想

(2) I 是R的真理想 $\Leftrightarrow 1_R \notin I$

③ a的主理想

$(a) := \{ra \mid r \in R\}$ （因为我们总要求R交换，故记号随意）

$\| \quad aR$

a称为(a)的生成元

④ R域 $\Leftrightarrow$ R的理想都是主理想

$\Rightarrow$ $\{0_R\} \subsetneq I \lhd R$

取 $0 \neq a \in I$ $ra = 1 \Rightarrow r = (ra^{-1})a \in I$

$\Rightarrow I = R$

$\Leftarrow$ $0 \neq a \in R \Rightarrow (a) = R \quad \exists ra = 1$

$\Rightarrow$ R为域. □

例. 分类Z的理想

$\{0\}$, $\mathbb{Z}$, $n\mathbb{Z}\ (= -n\mathbb{Z})$ （$m \neq n \geq 1 \Rightarrow m\mathbb{Z} \neq n\mathbb{Z}$）

断言，这是所有的理想 $\forall I \lhd \mathbb{Z}$ $\exists! n \geq 0$, s.t. $I = n\mathbb{Z}$

~~考虑下的~~ 不妨 $\{0\} \subsetneq I$. $\exists!\ n_0$, s.t. $|n|_0$ 最小

不妨 $n_0 > 0 \Rightarrow n_0\mathbb{Z} \subseteq I$

若 $n_0 \nmid m$ $\boxed{m = qn_0 + r}$ $|r| < n_0$ 矛盾 $\Rightarrow r = 0$ ↯

ps: 我们ED是这样的

$\theta : R \to S$ 同态

$\ker\theta = \{r \in R \mid \theta(r) = 0_S\} \lhd R$

$a \sim b \Leftrightarrow a - b \in \ker\theta$

$[a] = a + \ker\theta$

由映射基本定理 $R/\ker\theta \xrightarrow{\bar{\theta}}_{\sim} \operatorname{Im}\theta$ 环

这也在说明环结构

Def（商环） $I \lhd R$，商环 R/I

STEP 1 等价关系 $a \equiv b \pmod I \Leftrightarrow a - b \in I$

$\bar{a} = \{b \in R \mid a - b \in I\} = a + I$ 平移

12.

STEP 2. $R/_{\equiv_I} := R/I = \{\bar{a} \mid a \in R\}$ Rmk $\bar{a} = \bar{a}' \Leftrightarrow a - a' \in I$

NOTE $R/I \subseteq \mathcal{P}(R)$

加法 $\bar{a} + \bar{b} := \overline{a+b}$ （新 / 老）

乘法 $\bar{a} \cdot \bar{b} := \overline{a \cdot b}$ （新 / 老） EX 验证良定性

STEP 3. $(R/I, +, \cdot)$ 是合乎定义的环

结合 交换 $\bar{0}$ 负

I 分配 结合

Fact $can : R \to R/I$ 典范同态

$a \mapsto \bar{a}$

显然 $\ker can = I$

无法表达一般的商集大小，但可在具体例子中，如多项式环等还能处理.

例、$n\mathbb{Z} \lhd \mathbb{Z}$ $\mathbb{Z}/n\mathbb{Z}$ 是模 n 同余类环

$= \{\bar{0}, \bar{1}, \cdots \overline{n-1}\}$

prop $I \lhd R$ $can : R \to R/I$

$\theta : R \to S$ s.t. $I \subseteq \ker\theta$

则 $\exists!$ $R/I \xrightarrow{\theta'} S$

$\theta = \theta' \circ can$

$$\begin{array}{ccc} R & \xrightarrow{\theta} & S \\ {\scriptstyle can}\downarrow & \nearrow_{\theta'} & \\ R/I & & \end{array}$$

典范映射的泛性质

唯一性 存在性 要定义，则只能唯一.

$\theta' : R/I \to S$

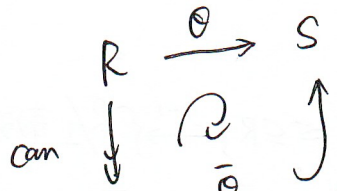
$[a] \to \theta(a)$ well-defined

$\bar{a} = \bar{a}' \Leftrightarrow a - a' \in I \subseteq \ker\theta \Rightarrow \theta(a) = \theta(a')$

Thm (环同态基本定理)

$\theta: R \to S$ 环同态

$\exists!$ 环同态 $\bar{\theta}$ 使下图交换



双射性映射基本定理保持

再强性 同态即可

应用 $\theta: R \to S$ 环同态

① θ 单 $\Leftrightarrow \ker\theta = \{0_R\}$ (can 同构)

此时 $R \xrightarrow{\sim} \mathrm{Im}(\theta)$ 也视 R 为 S 的子环

$a \mapsto \theta(a)$

② θ 满 $\Leftrightarrow \mathrm{Im}\,\theta = S$ 此时 $R/\ker\theta \xrightarrow{\sim} S$, S 为 R 的商环

③ 特征映射

φ 单: $\mathbb{Z} \to R$, $n \mapsto n1_R$

$\ker\varphi = n\mathbb{Z}$ $n = 0$ 或 $n \geq 2$ ($n=1$ 是环)

$n = \mathrm{char}\, R$ 环的特征

$n=0$ $\varphi: \mathbb{Z} \hookrightarrow R$ ($n1_R \neq 0$) R 是无限环

$n \geq 2$. φ 很单 $n1_R = 0_R$

Fact R 整 则 $n=0$ 或 $n=p$

例 $\mathbb{F}_p \hookrightarrow R$

$\mathbb{Z}/n\mathbb{Z} \hookrightarrow R$

$\bar{m} \mapsto m1_R$

应用 $I \subseteq J$ $I \lhd R$, $J \lhd R$

$R/I \twoheadrightarrow R/J$

$(a+I) \mapsto (a+J)$ well-defined?

$\ker = \{a+I \mid a \in J\} \overset{\text{def}}{=} J/I$ ← 不是商环 只是记号

$(a+I) \mapsto (a+J)$

$(b+I) \mapsto (b+J)$

$a+J = b+(a-b)+J = b+J$ ($a-b \in J$)

14.

$(R/I)/(J/I) \xrightarrow{\sim} R/J$ 用~~一致~~ 上一个满射 + 同态定理看商

$(a+I)+J/I \longmapsto (a+J)$

Thm(对应定理) 给定 $I \lhd R$，则∃双射 $\{J \lhd R \mid I \subseteq J \subseteq R\} \xleftrightarrow{1:1} \{R/I \text{ 的理想}\}$

(R的理想清楚，对商环也清楚) $J \mapsto J/I = \{\bar{a} \mid a \in J\}$

$\bar{a} = (a+I)$

$\{a \in R \mid \bar{a} \in U\} \longleftrightarrow U \lhd R/I$

证：**EX** $\begin{cases} \cdot \{a \in R \mid \bar{a} \in U\} \in \text{左} \\ \cdot \text{验} \end{cases}$

EX 分类 $\mathbb{Z}/n\mathbb{Z}$ 的理想 hint：用双射

EX R环，S子环，I ⊲ R

① $S+I = \{a+x \mid a \in S, x \in I\}$ (是子环)

② $(S \cap I) \lhd S$

③ 有环同构 $S/S\cap I \xrightarrow{\sim} S+I/I$

EX $I \lhd R$ $\{S \underset{\text{子环}}{\subseteq} R \mid I \subseteq S\} \xleftrightarrow{1:1} \{R/I \text{ 的子环}\}$

$S \longmapsto S/I$

1.4. ~~商域~~，分式域 商域

把 $\mathbb{Z}$ 扩域 → 整数

$\mathbb{Z} \hookrightarrow \mathbb{Q}$ (单射)，$\mathbb{Z} \twoheadrightarrow \mathbb{F}_p$ (满射)

Model

R 整 $R^* = R \setminus \{0_R\}$

$R \times R^* = \{(a,x) \mid a \in R, x \in R^*\}$

定义等价关系 $(a,x) \simeq (b,y)$ iff $ay = bx$ in R

$(a,x) \sim (b,y)$ $ay = bx$ ~~$a \cdot y = b$~~

$(b,y) \sim (c,z)$ $bz = cy$ ~~$b \cdot z = a \cdot cy$~~ $y \neq 0$

$az \cdot y = bxz = xcy$

$xz = cx$

~~2.26~~

→ 试 $\frac{a}{x} \longleftrightarrow \{(b,y)\in R\times R^* \mid (b,y)\simeq(a,x)\} \in \mathcal{P}(R\times R^*)$

$\frac{a}{x}=\frac{a'}{x'} \iff (a,x)\ \mathcal{R}\ (a',x') \iff ax'=a'x$ on R

$x, x'\neq 0$

$Frac(R) = R\times R^*/\simeq$

自然定义加法 $\frac{a}{x}+\frac{b}{y}=\frac{ay+bx}{xy}$ ($x,y\neq 0 \Rightarrow xy\neq 0$. 用到 R 整)

乘法 $\frac{a}{x}\cdot\frac{b}{y}=\frac{a\cdot b}{x\cdot y}$

If it is well-defined ?

乘法的验证. $\frac{a}{x}=\frac{a'}{x'}$ $\frac{b}{y}=\frac{b'}{y'}$ 要 $\frac{a\cdot b}{x\cdot y}=\frac{a'\cdot b'}{x'\cdot y'}$

$\Downarrow$ $ax'=a'x$ $by'=b'y$ $a\cdot b\,x'y' = (a\cdot x')(by') = a'x\cdot b'y$

$= a'b'\cdot xy$

[EX] 加法的验证

Fact (1) $(Frac(R), +, \cdot)$ 含幺交换环.

$0=\frac{0_R}{1_R}$ $-\frac{a}{x}=\frac{-a}{x}$ $1=\frac{1_R}{1_R}$

(2) $Frac(R)$ 是 R 的含 1 [域]

$\frac{a}{x}\neq\frac{0_R}{1_R} \iff a\neq 0_R$

$\frac{a}{x}\cdot\frac{x}{a}=\frac{ax}{ax}=\frac{1}{1}$ 即 $\left(\frac{a}{x}\right)^{-1}=\frac{x}{a}$

(3) $Can\ R \hookrightarrow$ 单 $Frac(R)$

$a \longmapsto \frac{a}{1_R}$

So $R \xrightarrow{\sim} Im(Can)$

(4) [Can 同构 $\iff$ R 为域]

[EX]

Fact K, L 为域 [$\theta: K\hookrightarrow L$ 同态 则 θ 单] 所以域同态不是很坏的事

$Can: R \to Frac(R)$

$\forall\ \phi: R\hookrightarrow K$ 单 则 $\exists!\ \tilde{\phi}: Frac(R)\to K$ s.t.

$$\begin{cases} 0\neq a\in \ker\theta \\ \theta(a\cdot a^{-1}) = 0 \\ \| \\ 1 \end{cases}$$ 矛

$R \xrightarrow{\phi} K$

$Can \downarrow \quad \nearrow \tilde{\phi}$

$Frac\ R$

(6. 至多唯一性：$\tilde{\phi}\left(\frac{a}{1}\right)=\phi(a)$ $a\in R$

$x\neq 0$ $\tilde{\phi}\left(\frac{1}{x}\right)=\left(\tilde{\phi}\left(\frac{x}{1}\right)\right)^{-1}=\left(\phi(x)\right)^{-1}$

In general. $\tilde{\phi}\left(\frac{a}{x}\right)=\tilde{\phi}\left(\frac{a}{1}\right)\tilde{\phi}\left(\frac{1}{x}\right)=\phi(a)\left(\phi(x)\right)^{-1}\in K$

存在性. $\tilde{\phi}\left(\frac{a}{x}\right)=\phi(a)\left(\phi(x)\right)^{-1}$ $\left(x\neq 0\Rightarrow \phi(x)\neq 0 \text{ 因 } \phi \text{ 单}\right)$

well-defined : $\frac{a'}{x'}=\frac{a}{x}$ $a'x=ax'$

$\Rightarrow \phi(a')\phi(x)=\phi(a)\phi(x')$

$\Rightarrow \phi(a')\left(\phi(x')\right)^{-1}=\phi(a)\left(\phi(x)\right)^{-1}$

唯一同态.

证 $\tilde{\phi}\circ can=\phi$ 比较显然

注 $\tilde{\phi}:\mathrm{Frac}(R)\hookrightarrow K$ 是满的 $\Leftrightarrow$ $\omega\in K$. $\omega=\phi(a)\left(\phi(x)\right)^{-1}$ $a\in R$. $x\in R^{\times}$

Frac(R) 的大小一般讨论不了

例. (1) $\mathrm{Frac}(\mathbb{Z})=\mathbb{Q}$

(2) $\mathbb{Z}[F_1]$ $\mathbb{Z}[F_1]\hookrightarrow \mathbb{Q}(F_1)$

$\mathbb{Q}(F_1)$

EX $\mathrm{Frac}\left(\mathbb{Z}[F_1]\right)\tilde{=}\mathbb{Q}(F_1)$

(3) $\mathbb{F}$ 域 $\mathrm{char}(\mathbb{F})=0$

$$\begin{array}{ccc}\mathbb{Z} & \xrightarrow{\phi} & \mathbb{F} \\ {\scriptstyle can}\downarrow & \nearrow \exists! & \\ \mathbb{Q} & & \end{array}$$

$n\mapsto n1_{\mathbb{F}}$

$(m,n)\mapsto (m1_{\mathbb{F}})(n1_{\mathbb{F}})^{-1}$

此时 $\mathbb{F}$ 自然成为 $\mathbb{Q}$ 的线性空间

$\alpha\in\mathbb{Q}$ $v\in\mathbb{F}$ $\lambda v:=\tilde{\phi}(\lambda)v$

$\dim_{\mathbb{Q}}\mathbb{Q}(F_1)=2$

$\mathrm{char}=p$ 时

$\mathbb{Z}\xrightarrow{\phi}\mathbb{F}$ $\mathbb{F}_p\hookrightarrow\mathbb{F}$

$\ker\phi=p\mathbb{Z}$

$\mathbb{F}$ 是 $\mathbb{F}_p$ 线性空间

$\lambda v=\tilde{\phi}(\lambda)v$

若有限 $\Rightarrow |\mathbb{F}| = p^n$

还 $\operatorname{char}\mathbb{F} = p \Rightarrow \mathbb{F}_p \hookrightarrow \mathbb{F}$ $\mathbb{F}$为$\mathbb{F}_p$的线性空间 (有限维)

$\Rightarrow \mathbb{F} \simeq (\mathbb{F}_p)^d$ □

3.12

Review 整环 $R \hookrightarrow \operatorname{Frac}(R)$

$a \mapsto \frac{a}{1_R}$.

k域, "$\operatorname{char}(k)=0$" $\quad \mathbb{Q} \hookrightarrow k$ (无限域)

$\frac{m}{n} \mapsto (m1_k)\cdot(n1_k)^{-1}$

k视为$\mathbb{Q}$线性空间

(2) $\operatorname{char} k = p$ prime. $\quad \mathbb{F}_p \hookrightarrow k$ (可有限/无限)

$\bar{n} \mapsto n1_k$ $\quad \Downarrow$

$\#k = p^d$

从而 k为$\mathbb{F}_p$线性空间

数乘 $\bar{n}\cdot v := (n1_k)v$ (k中乘法)

Recall $I \lhd R$ $\quad R/I = \{\bar{a}(=a+I) : a \in R\}$

Def 真理想 $\mathfrak{p} \lhd R$ 称为素理想. 若 $a\cdot b \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ 或 $b \in \mathfrak{p}$

$\Downarrow$ "$a\cdot b \notin \mathfrak{p}$ & $b \in \mathfrak{p} \Rightarrow a\cdot b \in \mathfrak{p}$"

例 ① in $\mathbb{Z}$. $p \geq 0$

$p\mathbb{Z} \lhd \mathbb{Z}$ 是素理想 $\Leftrightarrow$ p is prime

($\Rightarrow$) 若否. $p = a\cdot b$ in $\mathbb{Z}$

($\Leftarrow$) $mn \in p\mathbb{Z} \Rightarrow p \mid mn \Rightarrow p \mid m$ or $p \mid n$ ... □

③ 素理想是素理想 $\Leftrightarrow$ R整环

($\Rightarrow$) $a\cdot b \in \{0_R\} \Rightarrow$ "$a\cdot b = 0 \Rightarrow a = 0_R$ or $b = 0_R$" ... def

($\Leftarrow$) 显然 □

18

prop $\mathfrak{p} \lhd R$ 则 $\mathfrak{p}$ 素 $\Leftrightarrow$ $R/\mathfrak{p}$ 整环.

proof ($\Rightarrow$) $\bar{a}\cdot\bar{b} \in R/\mathfrak{p}$ i.e. $a \notin \mathfrak{p}$, $b \notin \mathfrak{p}$

0^{*}

$\Rightarrow a\cdot b \notin \mathfrak{p} \Rightarrow \overline{ab} \neq 0$ ..

EX ($\Leftarrow$) $\bar{a}, \bar{b} \in R/\mathfrak{p} \Rightarrow \bar{a}\cdot\bar{b} \neq 0 \Rightarrow a\cdot b \notin \mathfrak{p}$

0^{*} $a, b \notin \mathfrak{p}$

元素真理想! i.e. $\mathfrak{p}$ 素

Let $\mathrm{Spec}(R)$ denote $\{R$ 的素理想$\}$

↓

R的素谱 Specerum

□

Spec 非空疑似用到 zorn lem?

Def 极大理想. 真理想 $m \lhd R$ 称为极大理想若

"$m \subseteq I \lhd R \Rightarrow I = m$ or $I = R$"

prop 真理想 m 是极大理想 $\Rightarrow$ R/m 是域

商域

proof. 1° (Senior) $\#\{I \mid m \subseteq I \lhd R\} = \#\{m, R\}$ ($1:1$ 对应关系)

$a \in \mathcal{O}m$

调换 $\bar{a} \in R/m$ 那 $\bar{a}^{-1} = ?$

R/m 的理想为 $\{0_R, R/m\}$

⇓

R/m 是域 □

2° (Junior) ($\Rightarrow$) $\bar{0} \neq \bar{a} \in R/m$ $\bar{a}^{-1} = ?$

$m \subsetneq m + (a) = \{x + ra \mid x \in m, r \in R\} \lhd R$

⇓

$m + (a) = R$ $\Rightarrow \exists\ x + ra = 1_R$ 类似 Bezout.

接到商环上. $\bar{r}\cdot\bar{a} = \bar{1}$ $\Rightarrow \bar{a}^{-1} = \bar{r}$

($\Leftarrow$) R/m is a field, $\bar{0} \neq \bar{a} \in R/m \Rightarrow \exists\ \bar{r} \in R/m$ s.t.

0^{*}

$\bar{r}\bar{a} = 1_R \Rightarrow \exists\ x \in m$ s.t. $x + ra = 1$

$\Rightarrow m \subsetneq m + (a) = R$

since the choice of a is arbitrary $\Rightarrow$ we shall see

m is the maximal ideal.

$\underset{\text{极大理}}{\operatorname{Max}(R)} = \{m \mid m \text{是极大理想}\} \subseteq \operatorname{Spec}(R)$ check 本

Facts. 含幺交换环 $\Rightarrow \operatorname{Max} R \neq \emptyset$ (Zorn Lem) $\because R/m$ 是域

例 $\operatorname{Max}(\mathbb{Z}) = \{(2), (3), (5), \cdots\}$

$\downarrow$

$\mathbb{F}_2$ ---

$\operatorname{Spec}(\mathbb{Z}) = \{\{0_R\}\} \cup \operatorname{Max}(R)$.

约定. R 整. $a \neq 0$ $a \mid b \Leftrightarrow b \in (a)$ ie. $\exists r$ s.t. $b = ar$.

Def $0_R \neq a \in R$ 为素元 若 $(a) \in \operatorname{Spec}(R)$

Rmk (1) a 不是可逆元. 否则 $(a) = R$.

(2) a 非0非单位. a 素 $\Leftrightarrow$ "$x \cdot y \in (a) \Rightarrow x \in (a)$ or $y \in (a)$"

不可约元. 非0非单位的 $a \in R$. 称为不可约元. 若 $a = b \cdot c$ 则 b or c 可逆

$\left(a = a(u^{-1}a)\right)$ $u \in U(R)$

Facts. 素元一定不可约.

proof. 设 a 素 $a \neq 0$ 非单位

若 $a = b \cdot c \Rightarrow$ ~~$c \in (a)$~~ $a \mid b \cdot c \Rightarrow a \mid b$ or $a \mid c$

$\Downarrow$

$b = ax$

$a = a \underset{\text{逆(除消)}}{xc}$ c 是单位

例. $\mathbb{Z}$ 中不可约元 = 素元

例 $\mathbb{Z}[\sqrt{3}]$ EX 2 不可约 但 2 不是素元

$4 = 2 \cdot 2$

$\Vert$

$2 \mid (1+\sqrt{3})(1-\sqrt{3})$

UFD 的时

1.5 一元多项式环

R 环　　R 上关于 x 的(形式)多项式

$$f(x) = a_n x^n + \cdots + a_0 \qquad a_i \in R \qquad (a_0 x^0 := a_0)$$

$f(x) = g(x) \iff$ 对应系数相等.

约定 $\begin{cases} 1_R x^i := x^i \\ -1_R x^i = -x^i \\ 0_R x^i \text{ 略去} \end{cases}$

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

$a_n x^n$ 首项　　a_n 首项系数.　　a_0 常数项

$a_n \neq 0$

$\deg f = n$.

零多项式：$f = 0$ (不定义次数)

常值多项式 $f = a_0$　　$\deg f = 0$ if $a_0 \neq 0$.

首一多项式 若 $a_n = 1_R$

$R[x]$ 是环

(1) $+$

(2) $\cdot$　　$f(x) = a_n x^n + \cdots + a_0$

$g(x) = b_m x^m + \cdots + b_0$

$$f(x)g(x) = \sum_{k=0}^{m+n} c_k x^k \qquad c_k = \sum_{i=0}^{n} a_i b_{k-i}$$

(3) $0_{R[x]} = 0_R$　　$1_{R[x]} = 1_R$.

Rmk　$R \hookrightarrow R[x]$

Prop　R 整 $\iff R[x]$ 整

$\Longrightarrow$　$f(x) \neq 0$, $g(x) \neq 0$. $\Rightarrow f(x)g(x) = \underset{\neq 0}{a_n b_m} x^{m+n} + \cdots \neq 0$

Prop (泛性质)　设 R 为环, $\psi : R \to S$ 为环同态　$s \in S$

则 $\exists!$ 环同态 $\tilde{\psi} : R[x] \to S$ s.t. $\tilde{\psi}|_R = \psi$　　$\tilde{\psi}(x) = s$.

proof. (1) 至多唯一. $\tilde{\psi}(x^i) = s^i \Rightarrow \tilde{\psi}(a_i x^i) = \psi(a_i) \cdot s^i$

In general $\tilde{\psi}\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} \psi(a_i) \cdot s^i \in S$ ✓

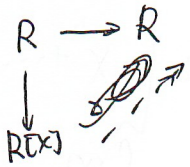
(2) 存在 (EX)

$$\begin{array}{ccc} R & \xrightarrow{\psi} & S \\ \downarrow & \nearrow \tilde{\psi} & \\ R[x] & & \end{array}$$

例 $\mathrm{Id}_R : R \to R$ then $\exists!$ 同态 ev_a s.t. $b \mapsto b$, $x \mapsto a$

a处的赋值同态

$$ev_a(f(x)) := f(a) \in R$$



3.14.

Fact $\forall f(x) \in R[x]$, $a \in R$

则 $\exists f(x) = q(x)(x-a) + f(a)$

proof. $f(x) - f(a) = \sum_{i=1}^{n} a_i (x^i - a^i) = \sum_{i=1}^{n} a_i (x-a)(\cdots)$ □

Question. $\ker(ev_a)$ 默认 $x-a \in \ker(ev_a)$

EX $\ker(ev_a) = (x-a)$ 由 $x-a$ 生成的主理想

那么 $R[x]/(x-a) \xrightarrow{\sim} R$. 同态基本定理

EX X是集合, R 环. $\mathrm{Map}(X, R) = \{f \mid f: X \to R\}$

加法

乘法: $\theta: X \to R$, $\beta: X \to R$ $\quad \theta\cdot\beta(x) := \theta(x)\beta(x)$

验证 函数环 $\mathrm{Map}(X, R)$ 是含幺交换环.

hint. 零和幺是零函数和常值函数

Fact. $\forall g(x) \in R[x]$ ⇝ 多项式函数 g

$g: R \to R$

$a \mapsto ev_a(g(x))$ $\quad g \in \mathrm{Map}(R, R)$

EX $R[x] \xrightarrow{ev} \mathrm{Map}(R, R)$

$g(x) \longmapsto$ 多项式函数

ev 是环同态

为什么要强调多项式和函数不同?

ev 满 ⇒ ev 不单

EX $\mathbb{F}_2[x] \xrightarrow{ev} \mathrm{Map}(\mathbb{F}_2, \mathbb{F}_2)$

不单 $\quad x^2 + x \longmapsto 0$.

ev 不单 可以

check 1. ev 满

2. $\ker(ev) = (x^2+x)$

3. $\mathrm{Map}(\mathbb{F}_2, \mathbb{F}_2)$ 不整.

22. 以下 k 是域，$k[x]$ 为 k 上的一元多项式环.

(都可以整环看)

$$f(x) = a_n x^n + \cdots + a_0 = a_n \left(x^n + \cdots \right)$$

$$= a_n \quad \tilde{f}(x)$$

因为 $(f(x)) = (\tilde{f}(x))$ 没有缺失信息

key Fact $k[x]$ 上有带余除法

$$f(x) \in k[x] \quad 0 \neq h(x) \in k[x]$$

$$\exists!\ f(x) = q(x)h(x) + r(x) \quad s.t.\ \deg r < \deg h \quad \text{or} \quad r(x) = 0$$

$\mathbb{F}_2[x]$

$$f(x) = x^4 + x^3 + x^2 + x + 1$$

$$h(x) = x^2 + x + 1$$

$$\left(x^4 + \cdots + 1\right) = \left(x^2+1\right)\left(x^2+x\right) + 1$$

$$\begin{array}{r|l} x^4+x^3+x^2+x+1 & x^2+x \\ \cline{2-2} x^4+x^3+x^2 & \\ \cline{1-1} x^3+x+1 & \\ x^3+x & \\ \cline{1-1} 1 & \end{array}$$

唯一性

$$f(x) = q(x)h(x) + r(x)$$

$$= q'(x)h(x) + r'(x)$$

$$\Rightarrow \left(q(x) - q'(x)\right)h(x) + \left(r(x) - r'(x)\right) = 0$$

$\neq 0$; $\deg r < \deg h$

得到唯一性

例. $f(x) = g(x)(x-a) + f(a)$

$(x-a) \mid f(x) \iff f(a) = 0_k$

so

$Root_K(f) = \{a \in K \mid f(a) = 0_K\} \subseteq K$

等号

方程 $\Longleftrightarrow$ 在 $K[x]$ 中找 $f(x)$ 一次因子.

↑

研究 $Root_K(f)$

PID 主理想整环

定理. $\mathbb{Z}$ 和 $K[x]$ 都是 PID.

proof $\forall I \lhd K[x]$ 取 $h(x) \in K[x]$, $\deg h$ 最小.

$(h(x)) \ni I$

$\forall f(x) \in I$. $f(x) = q(x)h(x) + r(x)$ 若 $r \neq 0$. $\deg r < \deg h$ 矛

PID 的性质

(1) PID 是整环

最大公因数. $\gcd(a,b) = d$ $\begin{cases} d \mid a,\ d \mid a \\ \forall d' \mid a,\ d' \mid b \Rightarrow d' \mid d \end{cases}$

注 $\begin{cases} \gcd \text{不一定存在} \\ \text{若存在, 则在相伴意义下唯一.} \end{cases}$

$a, b \in R$. a, b 相伴 $\Leftrightarrow \exists u \in U(R)$, $a = ub$

$\Leftrightarrow (a) = (b)$.

$\Leftrightarrow a \mid b \wedge b \mid a$

Fact R 是 PID. 则 $\gcd(a,b)$ 存在且有 Bezout 等式.

证. $(a) + (b) = (d)$ claim $d = \gcd$.

$a \in (a) \subseteq (d)$ $d \mid a$ $d \mid b$

$(d) = (a) + (b) \subseteq (d')$ $d' \mid d$ □

EX $\mathbb{Z}[\sqrt{-3}] = R$ $a = 4$, $b = (1-\sqrt{-3})^2$ $\gcd(a,b)$ ∃ ?

Rmk 整除 $\Leftrightarrow$ 主理想包含

证 Fact 1) PID中 素元=不可约元

只要证 不可约元是素的

若 $a \mid bc$ $a \nmid b$

$\Rightarrow 1 = \gcd(a,b)$ 因为 a 不可约

Bezout $\Rightarrow 1 = au + bv$

$c = acu + bcv \Rightarrow a \mid c$. □

(3) 若 R是非域的PID

则R的素理想都是极大理想

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

Krull 维数 ≤ 1

要证 $\subseteq$.

$0 \neq p \in \operatorname{Spec} R \Rightarrow p = (a)$ a是素

若 $p \subsetneq I \lhd R \Rightarrow b \mid a \Rightarrow b \overset{(b)}{=} R$ 或 $a \overset{eu(R)}{=} 0$.

$\Rightarrow I = R \Rightarrow p$ 是极大理想

具体到 $k[x]$

要求首一.

$f(x), g(x)$ 最大公因式 $\gcd(f,g) = h$

$\begin{cases} h \mid f \quad h \mid g \\ a \mid f, a \mid g \Rightarrow a \mid h \end{cases}$

辗转除法算 $\gcd(f,g)$ 欧氏算法

$\operatorname{Spec}(k[x]) = \{0\} \cup \operatorname{Max}(k[x])$

约定 $k[x]$ 上的不可约多项式 = $k[x]$ 中的不可约元 又素元

(deg ≥1)

$\{k$ 上的首一不可约多项式$\} \overset{1:1}{\longleftrightarrow} \operatorname{Max}(k[x])$

$f(x) \mapsto (f(x))$

$\forall \lambda \in k[x]$.

$x-\lambda$ 有根 $\rightsquigarrow (x-\lambda) \in \mathrm{Max}(k[x])$

$k \hookrightarrow \mathrm{Max}(k[x])$

单射.

Fact $k[x]/(x-\lambda) \xrightarrow{\sim} k$ (这点 in ex).

添根构造. $\deg f \geq 2$. $\boxed{k} = k[x]/(f(x))$ 域!

Fact (1) $\mathbb{C}[x]$ 中 不可约多项式都是 $x-\lambda$. ($\mathbb{C}$ 已经够大)

(2) $\mathbb{R}[x]$ 是 x^2+1

(3) $\mathbb{F}_2[x]$. x^2+x+1 不可约 $x^2+1 = (x+1)^2$ 可约.

K, $g(x) \in k[x]$.

$\overline{g(x)} \in K$

$\Vert g(x) + (f(x))$

. $\lambda \in k$ $\overline{\lambda} \in K$.

$\Vert$

$\lambda + (f(x))$

| $k \xrightarrow{\theta} K$ (嵌入) So $k \xrightarrow{\sim} \mathrm{Im}\theta \subseteq K$ 子域

| $\lambda \longmapsto \overline{\lambda}$

| θ 很自然. $\theta(\lambda) = \overline{\lambda}$ 也能记为自入

. $u = x + (f(x)) \in K$. u 不是未定元, 是 K 中具体的元素

. $\overline{g(x)} \in k$. $g(x) = q(x) f(x) + r(x)$

$\Rightarrow \overline{g(x)} = \overline{r(x)}$ with $d = \deg f$.

$$\overline{a_{d-1}x^{d-1}+\cdots} = \overline{a_{d-1}}\,u^{d-1}+\cdots$$

$$= \theta(a_{d-1})\,u^{d-1}+\cdots$$