Valuation Field

wu

2023 年 2 月 25 日

目录

1 环与理想

1.1 介绍

Definition 1.1. 称 A 为 **局部环**，如果 A 只有一个极大理想 I，称 $k = A/I$ 为 A 的 **剩余域**（residue field）

Proposition 1.2.
1. *设 A 为环，$I \subsetneq A$ 为理想，若每个 $x \in A \setminus I$ 均是单位元则 A 是局部环，I 是极大理想*
2. *若 A 为环，$I \subseteq A$ 为极大理想，若 $\forall a \in I$，有 $1 + a$ 均是单位元，则 A 是局部环*

1.2 分式化

Definition 1.3. 设 A 是一个整环，令 $A^\times = A \setminus \{0\}$，在 $A \times A^\times$ 上定义关系 $\sim$ 为

$$(a, s) \sim (b, t) \Leftrightarrow at - bs = 0$$

Definition 1.4. 称 $S \subseteq A$ 为 **乘法子集**，如果 $1 \in S$ 且 $a, b \in S \Rightarrow ab \in S$

Definition 1.5. 设 $S \subseteq A$ 是乘法子集，定义 $A \times S$ 上的等价关系 $\sim$ 为

$$(a, s) \sim (b, t) \Leftrightarrow \exists u \in S(u(at - bs) = 0)$$

将 (a, s) 的等价类记作 $\frac{a}{s}$，定义

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \quad \frac{a}{s}\frac{b}{t} = \frac{ab}{st}$$

则 $A \times S / \sim$ 是一个环，记作 $S^{-1}A$

Remark.
- $\forall x \in A$，$\frac{xa}{xs} = \frac{a}{s}$
- 若 S 有零因子，则 $S^{-1}A = 0$ 平凡
- $A \to S^{-1}A, a \mapsto \frac{a}{1}$ 是同态
- 若 A 是整环，$S = A^\times$，则 $S^{-1} = \mathrm{Frac}(A)$

Example 1.1. 若 $\mathfrak{p}$ 是素理想，$S = A \setminus \mathfrak{p}$ 是乘法子集

- 令 $A_{\mathfrak{p}} = S^{-1}A$
- 令 $\mathfrak{m} = \{\frac{a}{s} \mid a \in \mathfrak{p}, s \notin \mathfrak{p}\} = pA_{\mathfrak{p}} = \mathfrak{p}S^{-1}$，则 $A_{\mathfrak{p}}$ 是局部环，$\mathfrak{m}$ 是 $A_{\mathfrak{p}}$ 的极大理想

1.3 多项式环

设 A 是一个环，则多项式环 $A[X]$ 的元素都形如

$$\sum_{i=0}^{n} a_i x^i, \quad a_i \in A, i \in \mathbb{N}$$

Definition 1.6. 设 A 是环，$a \in A$ **不可约**如果 $a \neq 0$ 不是单位元且 $\forall b, c \in A(a = bc \Rightarrow) b$ 或 c 为单位元

一个整环 A 是 **唯一因子分解环**, 如果 $\forall a \in A$, 存在不可约元 $b_1, \dots, b_n \in A$ 使得 $a = b_1 \cdots_n$ 并且若存在不可约元 $c_1, \dots, c_m$ 使得 $a = c_1 \dots c_m$ 则 $m = n$, 则 $\forall i < n \exists j < n(b_i = u_{ij} c_j)$，其中 u_{ij} 是单位元

Proposition 1.7. *若 A 是唯一因子分解环，则 $A[X]$ 也是*

Corollary 1.8. *若 k 是域，则 $k[X_1, \dots, X_n]$ 是唯一因子分解环*

Corollary 1.9. *k 是域，$f \in k[X_1, \dots, X_n]$，则 (f) 是素理想 $\Leftrightarrow f$ 不可约*

证明. $\Rightarrow$：$k[X_1, \dots, X_n]/(f)$ 是整环，如果 f 可约，则 $f = gh$，其中 $g, h \in k[X_1, \dots, X_n]$ 且不是单位元, 于是 $g+(f), h+(f)$ 非零, 而 $(g+(f))(h+(f)) = 0 + (f)$，矛盾

$\Leftarrow$：对于任意 $g, h, p \in k[X_1, \dots, X_n]$, 若 $gh = fp$，因为 $k[X_1, \dots, X_n]$ 是唯一因子分解环，于是 f 整除 g 或者 f 整除 h □

2 局部环

一个环是局部环当且仅当所有非单位元构成一个理想。等价地，一个环是局部环当且仅当所有非单位元构成一个理想。

在环的语言 $\mathcal{L}_{ring} = \{+, \times, 0, 1\}$ 中局部环可以公理为

1. R 是环。

2. 所有的非单位元构成一个集合 $\mathfrak{m}$ 是理想，即 $\mathfrak{m}$ 关于 “+” 封闭，关于 “$\times$” 吸收。

但是非单位元关于 “$\times$” 总是吸收的，故而（2）可以改为

2. 所有非单位元关于“+”封闭，即 $\mathfrak{m}$ 是一个群。

Remark.

- $0 \in \mathbb{R}$ 出解析函数的函数芽的环 A 是局部环
- 一个函数 f 在 $0 \in \mathbb{R}$ 处解析 $\Leftrightarrow$ 存在开邻域 $U \ni 0$ 使得 f 在 U 上是个幂级数，即 $f\restriction_U = \sum_{n=0}^{\infty} a_n x^n$，其中 $a_n \in \mathbb{R}$。
- 显然，$\sum a_n x^n \sim \sum b_n x^n \Leftrightarrow \forall n(a_n = b_n)$，故而

$$A = \{f \mid f\text{是幂级数且收敛半径} > 0\}$$

- $\mathfrak{m} = xA = \{xf \mid f \in A\}$ 是唯一的极大理想，其中极大是因为 $A/\mathfrak{m} \cong \mathbb{R}$。

Example 2.1. 设 R 是一个环，称 $\sum_{n=0}^{\infty} r_n x^n$ $(r_n \in R)$ 的元素为 R 上的形式幂级数，令 $R[[x]]$ 为 R 上所有形式幂级数构成的集合，定义

1. $\sum r_n x^n + \sum s_n x^n = \sum (r_n + s_n) x^n$

2. $\sum r_n x^n \sum s_n x^n = \sum_n (\sum_{i+j=n} r_i s_j) x^n$

则 $(R[[x]], +, \times, 0_R, 1_R)$ 是一个环。

Definition 2.1. 设 R 是一个环，称 $R[[x]]$ 为 R 的 **形式幂级数环**，若 $g = \sum r_n x^n \in R[[x]]$，则 g 的 **度数**记作 $\deg(g)$，定义为

$$\deg(g) = \min(n \in \mathbb{N} \mid r_n \neq 0)$$

定义 $\deg(0) = \infty$。（因此 $\deg(g) \geq 0$）

Lemma 2.2. 假设 R

1. 若 $f \in R[[x]]$，且 $\deg(f) = n$，则

$$f = x^n(\sum r_k x^k)$$

其中 $r_0 \neq 0$，即 $f = x^n g$ 其中 $\deg(g) = 0$

2. 若 $f, g \in R[[x]]$，则 $\deg(fg) = \deg(f) + \deg(g)$

3. 若 $f = \sum r_n x^n, g = \sum s_n x^n$，则 $fg = 1 \Rightarrow r_0 s_0 = 1$

4. 若 $f = \sum r_n x^n$，则 f 是单位 $\Rightarrow r_0$ 是单位 $(r_0 \neq 0)$

证明. 1. 由定义，若 $f = \sum s_k x^k$ 且 $\deg(f) = n$，则 $s_0 = \cdots = s_{n-1} = 0$ 且 $s_n \neq 0$，因此 $f = x^n(\sum_{k=n}^{\infty} s_k x^k)$，对任意 $i \in \mathbb{N}$，令 $r_i = s_{i+n}$，则 $f = x^n(\sum r_k x^k)$，其中 $r_0 \neq 0$。

2. 假设 $\deg(f) = n$，$\deg(g) = m$，则由（1），$f = x^n(\sum r_k x^k)$，$g = x^m(\sum s_k x^k)$，其中 $r_0, s_0 \neq 0$，因此 $fg = x^{n+m} \sum_{n=0}^{\infty}(\sum_{i+j=n} r_i s_j)x^n$，因为 $r_0, s_0 \neq 0$，R 是整环，因此 $r_0 s_0 \neq 0$，因此 $\deg(fg) = n + m = \deg(f) + \deg(g)$。

3. 由定义，$fg = \sum_{n=0}^{\infty}(\sum_{i+j=n} r_i s_j)x^n = 1$，因此 $r_0 s_0 = 1$

4. 如果 f 是单位，则存在 $g \in R[[x]]$ 使得 $fg = 1$，由（3），r_0 是单位。

□

Proposition 2.3. *若 R 是局部环，则 $R[[x]]$ 也是局部环。*

证明. • 只需验证非单位元关于加法封闭。

- 设 $f \in R[[x]]$ 是单位元，则 $f = r_0 + g$，其中 r_0 是 R 的单位，$\deg(g) \geq 1$。
- 令一方面，若 $f = r_0 + g$ 且 $r_0 \in R$ 是单位，$\deg(g) \geq 1$，取 $s_0 \in R$ 使得 $s_0 r_0 = 1_R$，则 $s_0 f = 1 + s_0 g$，令 $h = -s_0 g$。

Claim: $h + h^2 + h^3 + \cdots \in R[[x]]$

证明. 设 $h = \sum s_k x^k$，其中 $s_0 = 0$，令 $g = \sum_{n=1}^{\infty} h^n = \sum r_k x^k$，于是 $r_0 \in R$，若 $r_0, \ldots, r_n \in R$，则 $r_{n+1} = s_{n+1} + \sum_{i=1}^{n-1} s_i r_{n-i} \in R$，因此对于任意 $k \in \mathbb{N}$，$r_k \in R$，因此 $g \in R[[x]]$。 □

- 考虑等式 $(1-h)(1+h+h^2+\dots)=1$，则 $s_0 f(1+h+h^2+\dots)=1$，故 f 是单位，因此
- $f\in R[[x]]$ 是单位 $\Leftrightarrow f=r_0+g$，其中 r_0 是单位且 $\deg(g)\geq 1$。
- $f\in R[[x]]$ 不是单位 $\Leftrightarrow \deg(f)\geq 1$ 或 $f=r+g$，其中 r 不是单位且 $\deg(g)\geq 1$。
- f 不是单位 $\Leftrightarrow f\in \mathfrak{m}_0+xR[[x]]=\{r+g \mid r\in\mathfrak{m}_0, g\in xR[x]\}$，其中 $\mathfrak{m}_0$ 是 R 的极大理想。
- 显然 $\mathfrak{m}_0+xR[[x]]$ 是"+"封闭的，故 $R[[x]]$ 是局部环。

□

Corollary 2.4. *若 R 是局部环，$\mathfrak{m}_0$ 为 R 的极大理想，则*

1. *$R[[x]]$ 是局部环，其极大理想为*

$$\mathfrak{m}_0+(x)$$

2. *若 k 是域，则 $k[[x]]$ 中的理想排成一个降链*

$$I_0=\mathfrak{m}_0+(x)\supseteq I_1=(x)\supseteq\cdots\supseteq I_n=(x^n)\supseteq\dots$$

证明. 1. 已证。

2. 设 J 是 $k[[x]]$ 的理想，令 $n=\min\{\deg(f)\mid f\in J\}$，若 $n=\infty$，则 $J=(0)$。

   若 $n<\infty$ 且 $f=x^n g\in J$ 其中 $\deg(g)=0$，由于 g 的首项是单位，因此 g 是单位，令 $h\in R[[x]]$ 使得 $hg=1$，则 $x^n=hf=hgx^n\in J$，因此 $(x^n)\subseteq J$，又由 n 的定义，$J\subseteq(x^n)$，所以 $J=(x^n)$。

□

Corollary 2.5. *若 k 是域，则 $k[[x]]$ 是局部环，其极大理想为 $(x)=xk[[x]]$，剩余域为 k。*

Corollary 2.6. 定义 $k[[X_1,\dots,X_{n+1}]] = k[[X_1,\dots,X_n]][[X_{n+1}]]$，则 $k[[X_1,\dots,X_{n+1}]]$ 为局部环，其极大理想 $\mathfrak{m}$ 为 $(X_1,\dots,X_{n+1})$，剩余域为 k。

Example 2.2. 令 $p \in \mathbb{Z}$ 是一个素数，

1. $\mathbb{Z}/p\mathbb{Z}$ 是一个域，这是因为若 $0 < r < p$，则 $(r,p) = 1$，故存在 m, n 使得

$$mr + np = 1 \Rightarrow mr \equiv_p 1$$

故 $\mathbb{Z}/p\mathbb{Z}$ 是一个局部环

2. 对每个 $n \in \mathbb{N}^+$，$\mathbb{Z}/p^n\mathbb{Z}$ 是局部环

   - $\mathbb{Z}$ 中包含 (p^n) 的理想与 $\mathbb{Z}/p^n\mathbb{Z}$ 中的理想一一对应
   - $\mathbb{Z}$ 中的理想均形如 (k)
   - $(p^n) \subseteq (k) \Leftrightarrow k \mid p^n \Rightarrow k = p^m$，其中 $m \le n$
   - 故 $\mathbb{Z}/p^n\mathbb{Z}$ 中的理想为

$$p^n\mathbb{Z}/p^n\mathbb{Z} = (0) \subseteq p^{n-1}\mathbb{Z}/p^n\mathbb{Z} \subseteq \cdots \subseteq p\mathbb{Z}/p^n\mathbb{Z}$$

   - 故 $p\mathbb{Z}/p^n\mathbb{Z}$ 为 $\mathbb{Z}/p^n\mathbb{Z}$ 的唯一极大理想，显然 $\mathbb{Z}/p^n\mathbb{Z}$ 中有 p^n 个元素。
   - $\mathbb{Z}/p^n\mathbb{Z}$ 的元素可唯一表示为

$$a_0 + a_1 p + \cdots + a_{n-1}p^{n-1}$$

其中 $a_i \in \{0,\dots,p-1\}$。

3. 若 $m > n$，则 $\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ 和 $\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ 诱导了

$$\begin{tikzcd}
\mathbb{Z} \arrow[r] \arrow[d] & \mathbb{Z}/p^m\mathbb{Z} \arrow[dl] \\
\mathbb{Z}/p^n\mathbb{Z} &
\end{tikzcd}$$

   - $\forall m > n$，令 π_{mn} 为 $\mathbb{Z}/(p^m)$ 到 $\mathbb{Z}/(p^n)$ 的自然同态，即

$$\pi_{mn}(a_0+a_1p+\dots+a_{m-1}p^{m-1})=a_0+\dots+a_{n-1}p^{n-1}$$

- 令 $\mathbb{Z}^*=\prod_{n=1}^{\infty}\mathbb{Z}/(p^n)=\{(x_1,x_2,\dots)\mid x_n\in\mathbb{Z}/(p^n)\}$,
- 将 x_n 看作 $a_0+\dots+a_{n-1}p^{n-1}$ 或序列 $(a_0,\dots,a_{n-1})$
- 定义 $\mathbb{Z}_p\subseteq\mathbb{Z}^*$ 为

$$\{(x_1,x_2,\dots,)\mid \pi_{mn}(x_m)=x_n, m>n\}$$

- 将 $(x_1,x_2,\dots)$ 中的每个 x_n 看作 $a_0+\dots+a_{n-1}p^{n-1}$,则 $(x_1,x_2,\dots)\in\mathbb{Z}_p\Leftrightarrow\forall m>n, x_m$ 是 x_n 的延长
- 故而 $(x_1,x_2,\dots)\in\mathbb{Z}_p$ 唯一对应一个幂级数 $a_0+a_1p+a_2p^2+\dots$
- 定义 $\mathbb{Z}^*$ 中的 + 为

$$(x_1,x_2,\dots)+(y_1,y_2,\dots)=(x_1+y_1,x_2+y_2,\dots)$$

- 定义 $\mathbb{Z}^*$ 中的 “×” 为

$$(x_1,x_2,\dots)\cdot(y_1,y_2,\dots)=(x_1y_1,x_2y_2,\dots)$$

- 定义零为 $(0,0,\dots,)$，幺为 $(1,1,\dots)$，则 $\mathbb{Z}^*$ 为环。
- 由于每个 π_{mn} 是同态,故 $\mathbb{Z}_p$ 对“+”与“×”封闭:对任意 $(x_1,x_2,\dots),(y_1,y_2,\dots)\in\mathbb{Z}_p$，对任意 $m>n$，因为 π_{mn} 是同态，有 $\pi_{mn}(x_m+y_m)=\pi_{mn}(x_m)+\pi_{mn}(y_m)=x_n+y_n$，$\pi_{mn}(x_m\cdot y_m)=\pi_{mn}(x_m)\cdot\pi_{mn}(y_m)=x_n\cdot y_n$,故 $(x_1,x_2,\dots)+(y_1,y_2,\dots),(x_1,x_2,\dots)\cdot(y_1,y_2,\dots)\in\mathbb{Z}_p$。
- 故 $\mathbb{Z}_p$ 是一个环，称其为 ***p*-进整数环**。
- $\mathbb{Z}_p$ 也称为 $\mathbb{Z}/(p^n)$ 的逆极限，即 $\mathbb{Z}_p=\varprojlim\mathbb{Z}/(p^n)$

Remark. 设 $x=(x_1,x_2,\dots)\in\mathbb{Z}_p$，则 x 可以记作 $a_0+a_1p+a_2p^2+\dots$，其中每个 $a_i\in\{0,\dots,p-1\}$，因此 $x_1=a_0, x_2=a_0+a_1p$，…，$x_n=\sum_{k=0}^{n-1}a_kp^k$。

设 $y=(y_1,y_2,\dots)\in\mathbb{Z}_p$，设它可写作 $b_0+b_1p+\dots$，令 $z=x+y=(x_1+y_1,x_2+y_2,\dots)$，将 z 写作 $\sum_{k=0}^{\infty}c_kp^k$，则

$$z_n=x_n+y_n=(\sum_{k=0}^{n-1}a_kp^k+\sum_{k=0}^{n-1}b_kp^k)(\mod p^k)$$

即 z_n 是 x_n+y_n 的 p-进制展开的前 n 项。

同理若 $z=xy$，则 z_n 是 x_ny_n 的 p-进制展开的前 n 项。

故 $\mathbb{Z}_p$ 中的运算是“p-进制”运算。

Lemma 2.7. *label:6* 若 A,B 是局部环，则 $f:A\to B$ 是满同态，则 $a\in A$ 是单位 $\Leftrightarrow f(a)\in B$ 是单位

证明.
- 令 $\mathfrak{m}$ 是 B 的极大理想，
- 则 $\bar{f}:A/f^{-1}(\mathfrak{m})\to B/\mathfrak{m}$ 是同构，
- 而 $B/\mathfrak{m}$ 是域，故 $A/f^{-1}(\mathfrak{m})$ 是域，故 $f^{-1}(\mathfrak{m})$ 是极大理想，
- 故 $a\in A$ 是单位 $\Leftrightarrow a\notin f^{-1}(\mathfrak{m})\Leftrightarrow f(a)\notin\mathfrak{m}$ 是 B 的单位。

□

Proposition 2.8.
1. $\mathbb{Z}_p$ 是局部环
2. $\mathbb{Z}_p$ 的理想排成降链
$$p\mathbb{Z}_p\supseteq p^2\mathbb{Z}_p\supseteq\ldots$$
3. $\mathbb{Z}_p/p^n\mathbb{Z}_p\cong\mathbb{Z}/p^n\mathbb{Z}$

证明.
1. 设 $x=(x_1,x_2,\ldots)=a_0+a_1p+\cdots\in\mathbb{Z}_p$，即 $x_1=a_0$，$x_2=a_0+a_1p$，…。

   Claim: x 是单位 $\Leftrightarrow a_0\neq 0$

   证明. $\Leftarrow$:
   - 若 $a_0\neq 0$，则 $a_0\in\mathbb{Z}/p\mathbb{Z}$ 是单位，
   - 故存在 $b_0\in\mathbb{Z}/p\mathbb{Z}$ 使得 $a_0b_0\equiv 1\mod p$。
   - 由于 π_{21} 是同态，而 $a_0=\pi_{21}(a_0+a_1p)$ 是单位，由引理**??**，$a_0+a_1p\in\mathbb{Z}/p^2\mathbb{Z}$ 也是单位，
   - 同理，$\forall b_1\in\{0,\ldots,p-1\}$，$b_0+b_1p\in\mathbb{Z}/p^2\mathbb{Z}$ 是单位，

- 令 $c_0 + c_1 p \in \mathbb{Z}/p^2\mathbb{Z}$ 使得

$$(a_0 + a_1 p)(c_0 + c_1 p) = 1 \in \mathbb{Z}/p^2\mathbb{Z}$$

- 则 $\pi_{21}((a_0 + a_1 p)(c_0 + c_1 p)) = a_0 c_0 = 1 = a_0 b_0$。
- 故 $a_0 c_0 - a_0 b_0 \equiv 0 \mod p$，因此 $c_0 \equiv b_0 \mod p$，所以 $c_0 = b_0$。
- 一般地，设 $b_0 + b_1 x + \dots + b_{n-1} x^{n-1} \in \mathbb{Z}/(p^n)$ 使得 $(a_0 + \dots + a_{n-1} x^{n-1})(b_0 + \dots + b_{n-1} x^{n-1}) = 1 \in \mathbb{Z}/p^n\mathbb{Z}$，
- 则存在 $b_n \in \{0, \dots, p-1\}$ 使得在 $\mathbb{Z}/(p^{n+1})$ 中有 $(a_0 + \dots + a_n x^n)(b_0 + \dots + b_n x^n) = 1$。
- 令 $y = b_0 + b_1 + \dots = (y_1, y_2, \dots)$，则 $xy = 1$，故 x 是单位。

$\Rightarrow$：若 $a_0 = 0$，则 $x = (0, x_2, \dots)$ 显然不是单位。 $\square$

以上断言表明，所有非单位元形如 $x = (0, x_2, x_3, \dots)$ 是一个加法群，故而是极大理想，恰好是 $p\mathbb{Z}_p$

2. 设 $J \subseteq \mathbb{Z}_p$ 是一个非平凡理想
    - 令 $k = \min\{n \in \mathbb{N} \mid p^n \in J\}$，显然 $k > 0$，$p^k\mathbb{Z}_p \subseteq J$
    - 断言 $p^k\mathbb{Z}_p = J$。
    - 设 $x = a_0 + a_1 p + \dots \in J$，令 a_m 是第一个非零系数
    - 则 $x = p^m(a_m + a_{m+1} p + \dots)$，
    - 因为 $a_m \neq 0$，$a_m + a_{m+1} p + \dots$ 是单位，故存在 $y \in \mathbb{Z}_p$ 使得 $xy = p^m \in J$
    - 由定义，$k \leq m \Rightarrow p^m \in p^k\mathbb{Z}_p \Rightarrow x \in p^k\mathbb{Z}_p$，
    - 即 $\mathbb{Z}_p$ 的每个非平反理想都形如 $p^k\mathbb{Z}_p$。
3. 投射函数诱导了一个同态

$$\begin{tikzcd}
\mathbb{Z}^* \arrow[r, "\pi_n"] & \mathbb{Z}/(p^n) \\
\mathbb{Z}_p \arrow[u] \arrow[ur, "\pi_n"'] &
\end{tikzcd}$$

其中 $\pi_n : \mathbb{Z}_p \to \mathbb{Z}/(p^n)$，$x = (x_1, \dots, x_n, \dots) \mapsto x_n$，于是

$$\begin{aligned} x \in \ker(\pi_n) &\Leftrightarrow x_n = 0 \\ &\Leftrightarrow x = (0, \dots, 0, x_{n+1}, \dots) \\ &\Leftrightarrow x = a_n p^n + a_{n+1} p^{n+1} \dots \\ &\Leftrightarrow x \in p^n \mathbb{Z}_p \end{aligned}$$

$\square$

Remark. 证明 $\mathbb{Z}_p$ 是局部环的关键是验证

$$x = a_0 + a_1 p + \dots \text{是单位} \Leftrightarrow a_0 \neq 0$$

以下证明更简洁:

- 设 $x = (x_1, x_2, \dots) \in \mathbb{Z}_p \subseteq \prod \mathbb{Z}/(p^n)$，$x_1 = a_0, \dots, x_n = a_0 + a_1 p + \dots + a_{n-1} p^{n-1}, \dots$
- 由于每个 $\mathbb{Z}/(p^n)$ 都是局部环且 $p\mathbb{Z}/(p^n)$ 是其极大理想，
- 故每个 x_n 在 $\mathbb{Z}/(p^n)$ 中可逆，令 y_n 是 x_n 在 $\mathbb{Z}/(p^n)$ 的逆
- $\pi_{mn}(x_m y_m) = \pi_{mn}(x_m)\pi_{mn}(y_m) = x_n \pi_{mn}(y_m) = 1$，
- 故 $\forall n < m$，$\pi_{mn}(y_m)$ 都是 x_n 的逆
- 断言：$\pi_{mn}(y_m) = y_n$
- $x_n(y_n - \pi_{mn}(y_m)) = 0 \Rightarrow y_n x_n (y_n - \pi_{mn}(y_m)) = 0$，
- 故 $y = (y_1, y_2, \dots)$ 是 x 的逆

更加简洁的方法:

- 取 $b \in \{0, \dots, p-1\}$ 使得 $a_0 \cdot b \equiv 1 \mod p$，
- 则 $bx = 1 + p(b_0 + b_1 p + \dots) = 1 - py$，
- 令 $c = 1 + py + p^2 y^2 + \dots \in \mathbb{Z}_p$，

- 则 $bxc = (1-py)(1+py+(py)^2+\dots) = 1$

Remark.
- $\mathbb{Z} \mapsto \mathbb{Z}_p$, $x \mapsto x$ 的 p-进制展开是一个单同态。
- $\mathbb{Z}$ 中不能被 p 整除的元素都是 $\mathbb{Z}_p$ 的单位。
- 令 $S = \mathbb{Z} - (p)$，则 S 是乘法集，$\mathbb{Z}$ 关于 (p) 的局部化 $\mathbb{Z}_{(p)} = S^{-1}\mathbb{Z} \subseteq \mathbb{Q}$ 是局部环，且 $pS^{-1}\mathbb{Z}$ 是极大理想
- $\mathbb{Z}_{(p)} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \nmid b\} \subseteq \mathbb{Q}$
- $\mathbb{Z}$ 到 $\mathbb{Z}_p$ 的嵌入自然地扩张为 $\mathbb{Z}_{(p)}$ 到 $\mathbb{Z}_p$ 的嵌入

$$
\begin{gathered}
f : \mathbb{Z} \to \mathbb{Z}_p \\
\Big\downarrow \\
\tilde{f} : S^{-1}\mathbb{Z} \to \mathbb{Z}_p \\
\frac{a}{b} \mapsto (f(b))^{-1} a
\end{gathered}
$$

- $\mathbb{Z}_p \cap \mathbb{Q} = \mathbb{Z}_{(p)}$
- 在形式上，$\mathbb{Z}_p$ 与 $\mathbb{F}_p[[X]]$ 有相似之处，然而 $\mathrm{Char}(\mathbb{Z}_p) = 0$，而 $\mathrm{Char}(\mathbb{F}_p[[X]]) = p$

3 亨泽尔局部环

3.1 亨泽尔局部环（Henselian）

Definition 3.1. R 局部环，$\mathfrak{m}$ 极大理想，R 是 **亨泽尔环**如果对每个多项式 $f(x) \in R[x]$，$a \in R$，有

$$f(a) \in \mathfrak{m} \wedge f'(a) \notin \mathfrak{m}$$

则存在 $b \in R$ 使得 $f(b) = 0$ 且 $a \equiv b \mod \mathfrak{m}$

Remark.
1. 我们可以把 $\mathfrak{m}$ 中的元素看作 R 中的“无穷小量”，则 $f(a) \in \mathfrak{m}$ 且 $f'(a) \notin \mathfrak{m}$ 可理解为 $f(a)$ 在“0”点附近，而 $f(x)$ 在“a”处的斜率不为“0”，此时 $f(x) = 0$ 在 a 点附近可能有解

2. 设 $k=R/\mathfrak{m}$ 是 R 的剩余域，设 $f(x)=\sum_{k=1}^{n}c_kx^k\in R[x]$，定义，定义 $\bar{f}(x)\in k[x]$ 为 $\sum_{k=1}^{n}\bar{c}_kx^k$，其中

$$\bar{c}_k=c_k+\mathfrak{m}$$

则 $f(a)\in\mathfrak{m}$ 且 $f'(a)\notin\mathfrak{m}\Leftrightarrow\bar{f}(\bar{a})=0$ 且 $\bar{f}'(\bar{a})\neq 0\Leftrightarrow\bar{a}$ 是 $\bar{f}(x)$ 的非奇异零点（不是重根）

Lemma 3.2. *设 R 是一个局部环，$f(x)\in R[x], a\in R$, 若 $f(a)\in\mathfrak{m}$ 且 $f'(a)\notin\mathfrak{m}$，则至多有一个 $b\in R$ 使得 $f(b)=0$ 且 $a\equiv b\mod\mathfrak{m}$*

证明. 设 $b\in R$ 使得 $f(b)=0$ 且 $a\equiv b\mod\mathfrak{m}$, 则 $\bar{a}=\bar{b}$, 故 $\bar{f}'(\bar{a})=\bar{f}'(\bar{b})\neq 0$，故 $f'(b)\notin\mathfrak{m}$ 是一个单位，考虑 $f(x)$ 在 b 点的泰勒展开

$$f(x+b)=f(b)+f'(b)x+cx^2$$

若 $x_0\in\mathfrak{m}$，则

$$f(x_0+b)=f'(b)x_0+cx_0^2=x_0(f'(b)+cx_0)$$

因为 $f'(b)$ 是单位，因此 $f'(b)+cx_0$ 是单位，故 $f(x_0+b)=0\Leftrightarrow x_0=0$ □

3.2 剩余域的提升

Example 3.1. 设 k 是一个域，$R=k[[x]]$，则 R 是一个局部环，$\mathfrak{m}=(x)$ 是极大理想

$a\in k\mapsto\bar{a}=a+(x)$ 是 k 到 $R/\mathfrak{m}$ 的同构，即 R 中存在一个子域 k 使得自然投射 $x\mapsto\bar{x}$ 在 k 上是同构

称 k 是 R 的剩余域的提升

Example 3.2. 设 $R=\mathbb{Z}/p^2\mathbb{Z}$，其中 p 是素数，$\mathfrak{m}=p\mathbb{Z}/p^2\mathbb{Z}$，$R/\mathfrak{m}\cong\mathbb{F}_p$，而 R 中没有子域，故 $R/\mathfrak{m}$ 在 R 中没有提升

若有子域，一定有 1，但是 1 可以生成整个 R

Example 3.3. 考虑局部环 $\mathbb{Z}_p$，$\mathfrak{m}=p\mathbb{Z}_p$，$k=\mathbb{Z}_p/\mathfrak{m}\cong\mathbb{F}_p$，$\mathrm{Char}\,\mathbb{Z}_p=0\Rightarrow\mathbb{F}_p\not\subseteq\mathbb{Z}_p$，故 $\mathbb{Z}_p/\mathfrak{m}$ 在 $\mathbb{Z}_p$ 中没有提升

Definition 3.3. 设 R 是一个局部环，$\mathfrak{m}$ 和 k 分别为其极大理想和剩余域，若存在 R 的子域 E 使得 $\overline{E} = \{\bar{x} = x + \mathfrak{m} \mid x \in E\} = k$，则称 E 是 k 的提升

Remark.

- 若 E 是 k 的提升，则 $\pi : E \to \overline{E}$ 是同构，$x \in \ker \pi \Leftrightarrow x \in \mathfrak{m} \Leftrightarrow x$ 不可逆即 $x = 0$
- 故而若 k 有提升，则提升唯一

Theorem 3.4 (提升定理)**.** *设 $R, \mathfrak{m}, k$ 如上，若 R 是亨泽尔的，且 $\mathrm{Char}\, k = 0$，则 k 在 R 中有提升*

证明. □

3.3 域的扩张理论

Definition 3.5. 设 K, L 是两个域，若 K 是 L 的子域，则称 L 是 K 的一个扩张，记作 L/K

Definition 3.6. 设 L/K 是一个域扩张，$X \subseteq L$，则

1. $K[X]$ 表示由 $K \bigcup X$ 生成的 L 的子环，
$$K[X] = \langle K \cup X \rangle_L$$
2. $K(X)$ 表示 $K[X]$ 的分式域
3. 若 $X = \{a_1, \dots, a_n\}$ 有穷，则 $K[X]$ 记作 $K[a_1, \dots, a_n]$，$K(X)$ 记作 $K(a_1, \dots, a_n)$

Proposition 3.7. *若 L/K 是域扩张，$a_1, \dots, a_n \in L$，则*

$$K[a_1, \dots, a_n] = \{f(a_1, \dots, a_n) : f \in K[X_1, \dots, X_n]\}$$
$$K(a_1, \dots, a_n) = \{\frac{f(a_1, \dots, a_n)}{g(a_1, \dots, a_n)} \mid f, g \in K[X_1, \dots, X_n], g(a_1, \dots, a_n) \neq 0\}$$

Definition 3.8. 设 L/K 是一个域扩张，$a \in L$，称 a 在 K 上是代数的，如果存在一个非零多项式 $f(x) \in K[X]$ 使得 $f(a) = 0$，如果 a 不是代数的，则 a 在 K 上是超越的

Definition 3.9. 设 L/K 是域扩张，$a \in L$ 在 K 上代数，若 $p(x) \in K[x]$ 是使得 $p(a) = 0$ 的次数最小的首一多项式，则称 $p(x)$ 是 a 在 K 上的极小多项式，记作 $\min(K, a)$

Remark.
- 显然 $I = \{f(x) \in K[X] \mid f(a) = 0\}$ 是 $k[x]$ 的一个理想
- 由于 $K[x]$ 是主理想整环，即每个理想都形如 $(g(x))$，故 $I = (p(x))$，$p \in I$ 且 $\deg(p)$ 最小，若要求 $p(x)$ 首项为 1，则 $p(x)$ 唯一
- 显然 $p(x)$ 在 $K[X]$ 中不可约
- 设 $p = x^n + \sum_{k=0}^{n-1} c_k x^k$
- 将 $K[a] = \{f(a) \mid f \in K[x]\}$ 视作 K 上的向量空间
- 由于 p 是使得 $p(a) = 0$ 的次数最小的多项式
- 故 $1, a, a^2, \ldots, a^{n-1}$ 在 K 上线性无关
- a^n 是 $\{1, \ldots, a^{n-1}\}$ 的线性组合
- a^{n+1} 也类似
- 故 $\{1, a, \ldots, a^{n-1}\}$ 是 $k[a]$ 的一组基
- 现在 $K[a]$ 是一个环，同时是 K 上的 n 维向量空间，基为 $\{1, \ldots, a^{n-1}\}$
- $\forall f(x) \in K[x]$, $f(x)$ 与 $p(x)$ 互素
- 故存在 $s(x), t(x) \in K[x]$ 使得 $s(x)f(x) + t(x)p(x) = 1$，故每个 $f(a) \in K[a]$ 都可逆，$K[a]$ 是一个域

Definition 3.10. 设 L/K 是一个域扩张，则 L 是 K 上的向量空间，$[L : K]$ 表示 L 作为 K 空间的维数，称 L/K 是一个有穷扩张如果 $[L : K] < \infty$

Proposition 3.11. 设 L/K 是一个域扩张，且 $a \in L$，在 K 上代数

1. $\min(K, a)$ 是 K 上的不可约多项式

2. $\forall g(x) \in K[x]$，$g(a) = 0 \Leftrightarrow \min(K, a) \mid g(x)$

3. 若 $\min(K, a)$ 的次数为 n，则 $\{1, \dots, a^{n-1}\}$ 是 $K[a]$ 在 K 上的一组基

4. $K[a] = K(a)$ 是域，$[K(a) : K] = n$

5. $K[a] \cong K[x]/\min(K, a)$

Proposition 3.12. 设 $F \subseteq K \subseteq L$ 是域扩张，则

$$[L : F] = [L : K][K : F]$$

证明. 设 $\{a_i \mid i \in I\}$ 是 K/F 的一组基，$\{b_j \mid j \in J\}$ 是 L/K 的一组基

证明 $\{a_i b_j \mid i \in I, j \in J\}$ 是 L/F 的基 □

Definition 3.13. 设 L/K 是域扩张，若每个 $a \in L$ 都在 K 上代数，则称 L 是 K 的代数扩张

Lemma 3.14. 若 L/K 是有穷扩张，则 L 是 K 的代数扩张且存在 $a_1, \dots, a_n$ 使得

$$L = K(a_1, \dots, a_n)$$

证明. 对 $[L : K]$ 归纳

若 $L = K$，则证明结束

否则，取 $a \in L \setminus K$，则 $1 < [K(a) : K] \leq [L : K] < \infty$

故存在 n 使得 $\{1, a, \dots, a^{n-1}\}$ 线性无关，a 在 K 上是代数，故 L/K 是代数扩张， □

Remark. L 可以由“更少”的元素生成，取 $b_1, \dots, b_m \in L$ 使得 $b_1 \notin K$, $b_2 \notin K(b_1)$，..., $b_m \notin K(b_1, \dots, b_{m-1})$，则 $[K[b_1] : K] \geq 2$，故 $[K(b_1, \dots, b_m) : K] \geq 2^M$

Lemma 3.15. 若 L/K 是域扩张，$a_1, \dots, a_n \in L$，若每个 a_i 都在 K 上代数，则 $E = K[a_1, \dots, a_n]$ 是域且 $[K[a_1, \dots, a_n] : K] \leq \prod_{i=1}^{n} [K(a_i) : K]$

证明. a_2 在 K 上代数推出 a_2 在 $K[a_1]$ 代数

若 m 时满足，令 $E = K[a_1, \dots, a_m]$，则

$$[E[a_{m+1}] : K] = [E[a_{m+1}] : E][E : K] \leq \prod_{i1}^{m} [K[a_i] : K][E[a_{m+1}] : E]$$

令 $p(x)$ 为 $\min(E, a_{m+1})$,$q(x)$ 为 $\min(K, a_{m+1})$，当然 $\deg(p) \leq \deg(q)$

于是 $[E[a_{m+1}] : E] \leq [K[a_{m+1}] : K]$

从而 $[E[a_{m+1}] : K] \leq \prod_{i=1}^{m+1} [K[a_i] : K]$ □

Corollary 3.16.

- 设 L/K 是域扩张，$a \in L$，则 a 在 K 上代数当且仅当 $[K(a) : K] < \infty$
- L 在 K 上代数当且仅当对每个有穷的 $X \subseteq L$，都有 $[K(X) : X] < \infty$
- $X \subseteq L$ 使得每个 $a \in X$ 都在 K 上代数，则 $K(X)/K$ 是代数扩张

Remark. 设 $a \in L$ 在 K 上超越，则映射 $\mathrm{ev}_a : F[X] \to F[a]$ 是同构

Proposition 3.17. 设 $F \subseteq K \subseteq L$ 是域扩张，若 K/F 和 L/K 均是代数扩张，则 L/F 也是代数扩张

证明. 设 $a \in L$，令 $f(x) = k_0 + \dots + x^n$ 是 a 在 K 的极小多项式，显然 $f(x) \in F[k_0, \dots, k_n]$，故 a 在 $F[k_0, \dots, k_n]$ 上代数，从而 $[F[k_0, \dots, k_n][a] : F[k_0, \dots, k_n]] < \infty$，故 $[F[k_0, \dots, k_n, a] : F] < \infty$，故 $F[k_0, \dots, k_n, a]/F$ 是代数扩张，故 a 在 F 上代数。 □

Definition 3.18. 设 L/K 是一个域扩张，则称 $\{a \in L \mid a\text{在}K\text{上是代数的}\}$ 为 K 在 L 中的 **代数闭包**，若该闭包是 K 子自己，则称 K 在 L 中代数闭

Corollary 3.19. 设 L/K 是一个域扩张，令 E 为 K 在 L 中的代数闭包，则 E 是一个域，从而是 K 在 L 中最大的代数扩张

证明. 只需验证 E 中的元素关于加法乘法封闭

设 $a, b \in E$，则 $[K[a] : K], [K[b] : K] < \infty$，故 $[K[a, b] : K] < \infty$，$[K[a, b], K] \leq [K[a] : K][K[b] : K] < \infty$ □

Definition 3.20. 设 K 是一个域，K 是 **代数闭域**，如果 K 的任何真扩张都不是代数扩张

$E \supseteq K$ 是 K 的 **代数闭包**如果 E 是代数闭的，且 E 的包含 K 的真子域都不是代数闭的

Remark. 1. K 是代数闭域 $\Leftrightarrow$ 任何非常数 $f(x) \in K[x]$ 在 K 中有根 $\Leftrightarrow$ 只有 deg ≤ 1 的 $f(x) \in K[x]$ 不可约

2. 若 L 是代数闭的且 $K \subseteq L$，则 $E = \{a \in L \mid a\text{在 } K \text{ 上代数}\}$ 是 K 的代数闭包

下面给出代数闭包的构造

设 K 是一个域且 $\lambda = |K| + \omega$，令 $\{f_i(x) \mid i < \lambda\}$ 是 $K[x]$ 的一个枚举（选择公理），令 $K_0 = K$

若 $f_0(x)$ 在 K_0 上可约，则 $K_1 = K_0$

若不可约，则 $K_1 = K_0[x]/(f_0(x))$，于是 $f_0(x)$ 在 K_1 中有根（$x+(f_0(x))$）

一般地，若 $\{K_i \mid i < \alpha\}$ 已构造，若 $\alpha = \beta + 1$，则 $K_\alpha = K_\beta$ 或 $K_\alpha = K_\beta[x]/(f_\beta(x))$

若 α 是极限序数，则 $K_\alpha = \bigcup_{\beta<\alpha} K_\beta$

于是每个 K_{i+1}/K_i 是代数扩张，每个 $f_i(x) \in K[X]$ 在 K_{i+1} 中可约

令 $E = \bigcup_{\alpha<\lambda} K_\alpha$，断言 E/K 是代数的

设 $a \in E$，则 $\exists\alpha < \lambda$ 使得 $a \in K_\alpha$

令 $\beta_0 = \min\{\beta < \alpha \mid \alpha\text{在 } K_\beta \text{ 上代数}\}$，

则存在 $c_0, \dots, c_{n-1} \in K_{\beta_0}$ 使得 $\sum c_i a^i = 0$，

若 $\beta_0 \neq 0$，则 $\exists\alpha_0 < \beta_0$ 使得 $c_0, \dots, c_{n-1}$ 在 K_{α_0} 上代数，从而 a 在 $K_{\alpha_0}[c_0, \dots, c_{n-1}]$ 上代数，由传递性（index），a 在 K_{α_0} 上代数，与 β_0 的极小性矛盾，故 $\beta_0 = 0$

同理 E 是代数闭的，因为每个代数扩张对应一个极小多项式，但是在构造过程中多项式已经被用完了

E 是 K 的代数闭包

Proposition 3.21. 任何域 K 都有代数闭包，且其代数闭包相互同构，记作 K^{alg}

若 E' 是 K 的代数闭包，考虑 $E \to E'$ 的部分同构，back-and-forth 一步一步抓每个元素，极大同构就是真的同构

3.4 提升定理

设 R 是亨泽尔局部环，$\mathfrak{m} \subseteq R$ 是极大理想，$k = R/\mathfrak{m}$ 是剩余域，若 $\operatorname{Char} k = 0$，则 k 可以被提升，即存在子域 $E \subseteq R$ 使得

$$k = \overline{E} = \{a + \mathfrak{m} \mid a \in E\}$$

证明. 令 $n_R = \underbrace{1_R + \cdots + 1_R}_{n}$, 令 n_k 表示 $\underbrace{1_k + \cdots + 1_k}_{n}$, 则 $n_k = \bar{n}_R = n_R + \mathfrak{m}$, 由于 $\operatorname{Char} k = 0$，故 $n_k \neq 0$，从而 $n_R \notin \mathfrak{m}$，故 R 的特征为 0

不妨假设 $\mathbb{Z} \subseteq R$，$\forall n \in \mathbb{Z}$，$n \notin \mathfrak{m}$，由于 R 是局部环每个 $n \neq 0$ 均可逆，故 $\mathbb{Q} \subseteq R$

令 $\mathcal{F} = \{E \mid E是R的子域\}$

注意到每个 $E \in \mathcal{F}$ 中的非零元素都可逆，故而 E 到 k 都是单同态，$\ker(\pi) \subseteq \mathfrak{m}$，令 E^* 是 $\mathcal{F}$ 在 $\subseteq$ 下的极大元，证明 E^* 就是 k 的提升

断言 1:E^* 在 R 中代数闭

否则，$a \in R \setminus E^*$ 在 E^* 上代数，则 $E^*[a]$ 是 E^* 的真域扩张

下面证明 $\overline{E}^* = \{a + \mathfrak{m} \mid a \in E^*\}$ 是 $k = R/\mathfrak{m}$

否则，设 $\bar{b} = b + \mathfrak{m} \in k \setminus \overline{E}^*$，则 $\bar{b}$ 在 $\overline{E}^*$ 上代数或超越

若 $\bar{b}$ 在 $\overline{E}^*$ 上代数，则存在 $f(x)$ 使得 $\bar{f}(x)$ 是 $\bar{b}$ 在 $\overline{E}^*$ 上的极小多项式，即 $\bar{f}(\bar{b}) = 0$ 且 $\bar{f}'(\bar{b}) \neq 0$，即 $f(b) \in \mathfrak{m}$ 且 $f'(b) \notin \mathfrak{m}$，由亨泽尔性，存在 $\epsilon \in \mathfrak{m}$ 使得 $f(b + \epsilon) = 0$，即 $b + \epsilon$ 在 E^* 上代数，而 $\overline{b + \epsilon} = \bar{b} \notin \overline{E}^*$，于是 $\overline{E}^*$ 不是代数闭，矛盾

若 $\bar{b} \in k \setminus \overline{E}^*$ 是超越的，于是 $\forall f(x) \in E^*[X]$,$f(b) \notin \mathfrak{m}$，即 $E^*[b]$ 中每个非零元都不属于 $\mathfrak{m}$，从而可逆，故 $E^*(b)$ 是 R 的一个子域，是 E^* 的真扩张，矛盾

故 $\overline{E}^* = k = R/\mathfrak{m}$ □

4 超积与 Ax-Kochen 原理

4.1 环的一阶语言

考虑环的一阶语言 $\mathcal{L}_{ring} = \{+, \times, 0, 1\}$

4.2 Łoś 超积定理

4.3 局部 Ax-Kochen 原理

观察：$\mathbb{Z}_p = \{\sum_{n=0}^{\infty} a_n p^n \mid a_n \in \{0, \dots, p-1\}\}$ 与 $\mathbb{F}_p[[t]] = \{\sum_{n=0}^{\infty} a_n t^n \mid a_n \in \{0, \dots, p-1\}\}$ 的相似之处：

1. $\mathbb{Z}_p/(p) = \mathbb{F}_p = \mathbb{F}_p[[t]]/(t)$
2. （局部）$\mathbb{Z}_p$ 是 $\{\mathbb{Z}/(p^n) \mid n \in \mathbb{N}^+\}$ 的逆向极限
3. （局部）$\mathbb{F}_p[[t]]$ 是 $\{\mathbb{F}_p[t]/(t^n) \mid n \in \mathbb{N}^+\}$ 的逆向极限
4. $\mathbb{Z}$ 在 $\mathbb{Z}_p$ 稠密，$\mathbb{F}_p[t]$ 在 $\mathbb{F}_p[[t]]$ 中稠密

差异：

1. $\mathrm{Char}\,\mathbb{Z}_p = 0$，$\mathrm{Char}(\mathbb{F}_p[[t]]) = p$
2. $\mathrm{Char}(\mathbb{Z}/p^n) = p^n$,$\mathrm{Char}(\mathbb{F}_p[t]/(t^n)) = p$

Theorem 4.1 (局部 Ax-Kochen 同构定理)**.** *令 $\mathcal{U}$ 是素数集上的一个非主超滤，则对每个 $n \in \mathbb{N}^+$，有*

$$\prod_{\mathcal{U}} (\mathbb{Z}/(p^n)) \cong \prod_{\mathcal{U}} (\mathbb{F}_p[t]/(t^n))$$

Lemma 4.2. *设 $\{A_i \mid i \in I\}$ 是一组亨泽尔局部环，A_i 的极大理想为 $\mathfrak{m}_i$，剩余域为 k_i，令 $\mathcal{U}$ 是 I 上的一个超滤，则*

1. *$\prod_{\mathcal{U}} A_i$ 是一个亨泽尔局部环*
2. *$\prod_{\mathcal{U}} \mathfrak{m}_i = \{[(a_i)_{i \in I}] \mid a_i \in \mathfrak{m}_i\}$ 是极大理想*

3. $\prod_{\mathcal{U}} k_i$ 同构于 $\prod_{\mathcal{U}} A_i / \prod_{\mathcal{U}} \mathfrak{m}_i$

证明. 1. 亨泽尔局部环是一阶句子

2. 设 $[a] \in \prod_{\mathcal{U}} A_i$，则

$$\begin{aligned} [a]\text{是单位} &\Leftrightarrow \exists [b], [a][b] = [1] \\ &\Leftrightarrow \{i \in I \mid a_i b_i = 1_i\} \in \mathcal{U} \\ &\Leftrightarrow \{i \in I \mid a_i\text{是单位}\} \in \mathcal{U} \\ &\Rightarrow [a] \notin \prod_{\mathcal{U}} \mathfrak{m}_i \end{aligned}$$

若 $[a] \notin \prod_{\mathcal{U}} \mathfrak{m}_i$, 则显然 $\{i \in I \mid a_i \notin \mathfrak{m}_i\} \in \mathcal{U}$, 故 $\pi(\prod_{i \in I} \mathfrak{m}_i) = \prod_{\mathcal{U}} \mathfrak{m}_i$ 是其极大理想

3. 设 $k_i = A_i/\mathfrak{m}_i$，令 $R_i : A_i \to k_i$ 为自然投射，令 $\prod_{\mathcal{U}} R_i : \prod_{\mathcal{U}} A_i \to \prod_{\mathcal{U}} (A_i/\mathfrak{m}_i)$，$[(a_i)_{i\in I}] \mapsto [(R_i(a_i))_{i \in I}]$，则 $\prod_{\mathcal{U}} R_i$ 是良定义的满同态，且 $\ker(\prod_{\mathcal{U}} R_i) = \prod_{\mathcal{U}} \mathfrak{m}_i$

□

Lemma 4.3. *若 $f(x) \in \mathbb{Z}[x]$, $n > 0$, $a \in \mathbb{Z}$ 使得 $f(a) \equiv 0 \mod p^n$, $f'(a) \not\equiv 0 \mod p$，则存在 $b \in \mathbb{Z}$ 使得 $a \equiv b \mod p^n$ 且 $f(b) \equiv 0 \mod p^{n+1}$*

证明. 对 n 归纳证明:

1. 若 $n = 1$，考虑同态 $\pi : \mathbb{Z} \to \mathbb{Z}/(p^2)$，$f'(a) \not\equiv 0 \mod p$，于是 $\pi(f'(a))$ 是 $\mathbb{Z}/(p^2)$ 的单位，令 $c \in \mathbb{Z}/(p^2)$ 是 $\pi(f'(a))$ 的逆

   任取 $\tilde{c} \in \mathbb{Z}$ 为 c 的提升，令 $\epsilon_1 = -\tilde{c} f(a)$，令 $b = a + \epsilon_1$，则

   $f(a) \equiv 0 \mod p \Rightarrow \epsilon_1 \equiv 0 \mod p \Rightarrow a \equiv b \mod p$

   $f(b) = f(a+\epsilon_1) = f(a) + f'(a)\epsilon_1 + \epsilon_1^2 r$, $\pi(f(b)) = \pi(f(a)) + \pi(f'(a)\epsilon_1) + \pi(\epsilon_1^2 r) = \pi(\epsilon_1^2 r)$

   $\epsilon_1 \equiv 0 \mod p$，因此 $\epsilon_1^2 \equiv 0 \mod p^2$

2. $f(a) \equiv 0 \mod p^n$，$f'(a) \not\equiv 0 \mod p$，令 $\pi_{n+1} : \mathbb{Z} \to \mathbb{Z}/(p^{n+1})$，令 $c \in \mathbb{Z}/(p^{n+1})$ 为 $\pi_{n+1}(f'(a))$ 的逆，令 $\tilde{c}$ 为 c 在 $\mathbb{Z}$ 的一个提升，令 $\epsilon_n = -\tilde{c} \cdot f(a)$，则 $\epsilon_n \equiv 0 \mod p^n$，令 $b = a + \epsilon_n$，则 $a \equiv b \mod p^n$，且 $f(a+\epsilon_n) = f(a) + f'(a)\epsilon_n + \epsilon_n^2 \cdot r$，

$$\begin{aligned}\pi_{n+1}(f(b)) &= \pi_{n+1}(f(a)) + \pi_{n+1}(f'(a))\pi_{n+1}(\epsilon_n) + 0 \\ &= 0\end{aligned}$$

□

Corollary 4.4. 设 $f(x) \in \mathbb{Z}[x]$, $a \in \mathbb{Z}$ 使得 $f(a) \equiv 0 \mod p$, $f'(a) \not\equiv 0 \mod p$，则对任意 $n > 0$，存在整数序列 $b_1 = a, b_2, \dots, b_n$ 使得 $b_k \equiv b_{k+1} \mod p^k$ 且 $f(b_k) \equiv 0 \mod p^k$

证明. □

若要求 $b_k < p^k$，则序列唯一

Corollary 4.5. 对每个 $n > 0$，$\mathbb{Z}/(p^n)$ 都是亨泽尔局部环

证明. 已知 $\mathbb{Z}/(p^n)$ 是局部环，下面证明 $\mathbb{Z}/(p^n)$ 的亨泽尔性。

同态 $\pi_n : \mathbb{Z} \to \mathbb{Z}/(p^n)$ 可以自然扩张为

$$\mathbb{Z}[x] \to \mathbb{Z}/(p^n)[x]$$

记作 π_n，用 $\tilde{f}$ 表示 $f(x) \in \mathbb{Z}/(p^n)[x]$ 在 $\mathbb{Z}[x]$ 中的提升，用 $\tilde{a}$ 表示 $a \in \mathbb{Z}/(p^n)$ 在 $\mathbb{Z}$ 的一个提升，显然对任意 $f(x) \in \mathbb{Z}/(p^n)[x]$ 以及 $a \in \mathbb{Z}/(p^n)$ 有

1. $f(a) \in \mathfrak{m} \Leftrightarrow \tilde{f}(\tilde{a}) \equiv \mod p$
2. $f'(a) \notin \mathfrak{m} \Leftrightarrow \tilde{f}'(\tilde{a}) \not\equiv 0 \mod p$

设 f, a 满足条件 1，2，则由引理 4.3 存在 $* \in \mathbb{Z}$ 使得 □

Theorem 4.6. 若 R 是一个局部环，如果存在 $t \in R$ 使得 $\mathfrak{m} = tR$ 是极大理想，则存在 $n > 0$ 使得 $t^n = 0$，则 R 是一个亨泽尔环

Remark. 设 R 是局部环，$\mathfrak{m}$ 是极大理想，$t \in R$ 使得 $\mathfrak{m} = (t)$，$t^{n-1} \neq 0$，$t^n = 0$，则

$$R = (t^0) \supsetneq (t) \supsetneq \cdots \supsetneq (t^n) \supsetneq (t^{n+1} = \emptyset)$$

是一个严格降链

对每个 $r \in R$，存在 $m \leq n$ 使得

$$r \in (t^m) \setminus (t^{m+1})$$

定义 r 的 **范数** $|r|$ 为

$$r \neq 0 \Rightarrow |r| = 2^{-m}$$
$$r = 0 \Rightarrow |r| = 0$$

则 $(R, ||)$ 是一个完备的（超度量）空间

1. $r = 0 \Leftrightarrow |r| = 0$，$|1| = 1$
2. $|r_1 + r_2| \leq \max\{|r_1|, |r_2|\}$
3. $|r_1 r_2| \leq |r_1||r_2|$

这种范数称为 **超范数**，对应的度量称为 **超度量**。

$\mathbb{Z}/(p^n)$ 和 $k[t]/t^n$ 都是完备的超度量空间

Remark. 若 R 是一个局部整环，$t \in R$ 使得 $\mathfrak{m} = (t)$ 且 $(t^n) \neq 0$

$$\bigcap_{n=0}^{\infty} (t^n) = \{0\}$$

则 $(t^0) \supsetneq \cdots \supsetneq (t^n) \supsetneq \ldots$ 是一个严格降链，设 $r \in R$，定义

$$|r| = \begin{cases} 2^{-m} & r \in (t^m) \setminus (t^{m-1}) \\ 0^r = 0 & \end{cases}$$

则 $(R, ||)$ 是一个超度量空间

1.

2.

3. $|r_1 r_2| = |r_1||r_2|$

但 R 不一定完备

Lemma 4.7. 设 R 是一个亨泽尔局部环，$\mathfrak{m}$ 是极大理想，k 是剩余域，若 $t \in R$ 使得 $\mathfrak{m} = (t)$ 且

$$\text{Char}(k) = 0, t^{n-1} \neq 0, t^n = 0$$

则 $R \cong k[X]/(x^n)$

证明. 由提升定理，k 在 R 中有提升 E，则 R 是 E 上的向量空间。

断言 1：$\{1, t, \dots, t^{n-1}\}$ 是 R 在 E 上的一组基。

1. 线性无关：设 $e_0 + \dots + e_{n-1}t^{n-1} = 0$，若 $e_0, \dots, e_{n-1} \in E$ 不全为 0，令 $i = \min\{k \mid e_k \neq 0\}$，则 $e^i t^i = -(e_{i+1}t^{i+1} + \dots + e_{n-1}t^{n-1})$，两边乘 t^{n-i-1}，则 $e_i t^{n-1} = 0 \Rightarrow t^{n-1} = 0$，矛盾

2. 设 $r \in R$，我们找出

   断言 2：若 $s \in (t^k)$，则存在 $e \in E$ 使得

   $$s - et^k \in (t^{k+1})$$

   若 $s \in (t^{k+1})$，则 $e = 0$；若 $s \notin (t^{k+1})$，则 $s = at^k$，$a \notin (t)$，由于 $E/\mathfrak{m} = R/\mathfrak{m}$，故存在 $e \in E$ 使得 $e/\mathfrak{m} = a/\mathfrak{m}$，故 $et^k - s = et^k - at^k = (e-a)t^k \in (t^{k+1})$

   由以上断言，可递归构造 $e_0, e_1, \dots, e_{n-1}$ 如下

   - 取 $e_0 \in E$ 使得 $r - e_0 \in (t)$
   - 取 $e_1 \in E$ 使得 $r - e_0 - e_1 t \in (t^2)$
   - 取 $e_{n-1} \in E$ 使得 $r - e_0 - \dots - e_{n-1}t \in (t^n) = \{0\}$

   即 $r = e_0 + e_1 + \dots + e_{n-1}t^{n-1}$

定义 $\pi : E[X] \to R$，$f(x) \mapsto f(t)$。

则断言 1 保证 π 是满同态且 $\ker(\pi) = (x^n)$，即

$$R \cong E[X]/(x^n) \cong k[X]/(x^n)$$

□

若 $k \subseteq R$, $a_1, \dots, a_n \in R$, $R = k[a_1, \dots, a_n]$，则

Theorem 4.8 (局部 Ax-Kochen 同构定理)**.** 令 $\mathcal{U}$ 是素数集上的一个非主超滤，则对每个 $n \in \mathbb{N}^+$，有

$$\prod_{\mathcal{U}}(\mathbb{Z}/(p^n)) \cong \prod_{\mathcal{U}}(\mathbb{F}_p[t]/(t^n))$$

证明. 令 $\mathcal{U}$ 是素数集 $\mathcal{P}$ 上的一个非主超滤，则 $\prod_{\mathcal{U}} \mathbb{F}_p$ 是 $\prod_{\mathcal{U}} \mathbb{Z}/(p^n)$ 与 $\prod_{\mathcal{U}} \mathbb{F}_p[t_p]/(t_p^n)$ 的剩余域

对每个 $n > 0$，$p > n$ 能推出 $\mathbb{F}_p \vDash n \neq 0$，故 $\{p \in \mathcal{P} \mid \mathbb{F}_p \vDash n \neq 0\}$ 是 $\mathcal{P}$ 的余有穷集，故 $\forall n > 0$，有 $\prod_{\mathcal{U}} \mathbb{F}_p \vDash n \neq 0$，故

1. Char $\prod_{\mathcal{U}} \mathbb{F}_p = 0$
2. 同理 $a = [(p)_{p\in\mathcal{P}}]$ 满足 a 是 $\prod_{\mathcal{U}} \mathbb{Z}/(p^n)$ 的极大理想，且 $a^{n-1} \neq 0$，$a^n = 0$
3.

□

Theorem 4.9 (局部 Ax-Kochen 转移原理)**.** 给定 $n > 0$ 以及一个 $\mathcal{L}_{ring}$-句子 σ 存在有限的素数集 E_σ 使得对每个 $p \notin E_\sigma$ 有

$$\mathbb{Z}/p^n \vDash \sigma \Leftrightarrow (\mathbb{F}_p[t]/t^n) \vDash \sigma$$

证明. 否则，

$$X_\sigma = \{p \in \mathcal{P} \mid \mathbb{Z}/p^n \vDash \sigma \Leftrightarrow (\mathbb{F}_p[t]/t^n) \vDash \sigma\}$$

的补集 $Y_\sigma = \mathcal{P} \setminus X_\sigma$ 是无穷集。

则存在非主超滤 $\mathcal{U}$ 使得 $Y_\sigma \in \mathcal{U}$

令 $Z_\sigma = \{p \in \mathcal{P} \mid \mathbb{Z}/p^n \models \sigma\}$,$F_\sigma = \{p \in \mathcal{P} \mid \mathbb{F}_p[t]/t^n \models \sigma\}$，则 $Z_\sigma \cap F_\sigma \cap Y_\sigma = \emptyset$，故 $Z_\sigma \in \mathcal{U} \Rightarrow F_\sigma \notin \mathcal{U}$，

若 $\prod_{\mathcal{U}} \mathbb{Z}/$ $\square$