

代数学笔记 Chapter 5：环论基础 (Ring Theory)

整理自课堂笔记

2025 年 12 月 11 日

本章导读

本章内容涵盖了环论的核心基础结构。我们将从 ** 环的定义 ** 出发，区分 ** 子环 ** 与 ** 理想 ** 这两个关键概念。接着，通过引入 ** 商环 **，我们将建立起环同态与环结构之间的桥梁——** 第一同构定理 **。最后，作为同构定理的重要应用，我们将证明 ** 中国剩余定理 (CRT)** 的代数形式。

核心路径：理想 → 商环 → 同态基本定理 → 结构分解 (CRT)。

目录

1 环的基本概念 (Basic Definitions)	5
1.1 环的定义	5
1.2 子环与理想	5
2 商环与同态 (Quotient Rings & Homomorphisms)	6
2.1 商环的构造	6
2.2 环同态	7
3 环的第一同构定理 (First Isomorphism Theorem)	7
3.1 应用：构造扩域	9

4 中国剩余定理 (Chinese Remainder Theorem)	10
4.1 环的直积	10
4.2 中国剩余定理 (CRT)	11
4.3 与初等数论的联系 (Equivalence to Number Theory)	13
5 整环的定义	15
5.1 消去律 (Cancellation Law)	15
6 定义与判别法	16
6.1 素理想 (Prime Ideal)	16
6.1.1 定义与定理	16
6.1.2 详细证明	16
6.2 极大理想 (Maximal Ideal)	17
6.2.1 定义与定理	17
6.2.2 详细证明	17
6.3 素理想与极大理想的关系	19
7 Zorn 引理与极大理想的存在性	19
8 第三同构定理 (分数消去律)	20
8.1 定理陈述	20
8.2 详细证明	20
9 第二同构定理 (钻石同构定理)	21
9.1 定理陈述	21
9.2 详细证明	21
10 多项式环的万有性质 (Universal Property)	22

10.1 定理陈述	22
10.2 双射公式与符号详解	22
10.2.1 符号含义	23
10.3 直观解释：为什么是双射？	23
10.3.1 推广到多元多项式	24
11 $\mathbb{Z}[x]$ 的理想结构分类	24
11.1 分类讨论与详细证明	24
12 基本元素分类	26
13 三大整环的层级	27
13.1 贝祖定理	28
13.2 重要命题：元素性质的等价性	28
13.3 PID 推出 UFD	30
14 典型实例分析	33
14.1 1. 高斯整数环 $\mathbb{Z}[i]$	33
14.2 费马平方和定理	34
14.3 2. Eisenstein 整数 (Legendre 整数)	35
14.4 3. 非 UFD 的反例	35
15 唯一分解整环 (UFD) 上的多项式环	36
15.1 基本设定与 Gauss 引理	36
15.2 详细证明补充	36
16 不可约元与素元	38
16.1 不可约性的判定	38

16.2 不可约元与素元的等价性	40
17 模 n 整数环的单位群	40
17.1 基本定义与结构	40
17.2 素数幂模的群结构	41
17.3 $n = 2^r (r \geq 3)$ 无原根的证明	42

1 环的基本概念 (Basic Definitions)

Class #13: Rings and Definitions

1.1 环的定义

定义 1.1 (环 Ring). 一个环 $(R, 0, 1, +, \cdot)$ 是一个集合 R , 配备两个二元运算 (加法和乘法), 满足以下公理:

1. 加法群: $(R, +)$ 是阿贝尔群 (交换群)。
 - 结合律、交换律、零元 0 、加法逆元 $-a$ 。
2. 乘法半群: (R, \cdot) 满足结合律, 且有单位元 1 (幺环)。
3. 分配律: 乘法对加法满足左分配律和右分配律。

$$a(b+c) = ab + ac, \quad (a+b)c = ac + bc$$

例 1.2 (常见环). • 交换环: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 以及多项式环 $k[T]$ 。

- 非交换环: 矩阵环 $M_n(k)$ (矩阵乘法一般不交换)。
- 域 (Field): 如果交换环中的非零元素都可逆, 则称为域。

1.2 子环与理想

这是环论中最容易混淆但最重要的区分。

定义 1.3 (子环 Subring). 设 $S \subseteq R$ 。若 S 满足以下条件, 则称 S 为 R 的子环:

1. $1_R \in S$ (必须包含单位元);
2. 对加法、减法、乘法封闭: $a, b \in S \implies a \pm b \in S, ab \in S$ 。

定义 1.4 (理想 Ideal). 设 $I \subseteq R$ 。若 I 满足以下条件, 则称 I 为 R 的理想 (双边理想):

1. $(I, +)$ 是 $(R, +)$ 的子群 (对减法封闭);
2. 吸收律: 对任意 $r \in R, x \in I$, 有 $rx \in I$ 且 $xr \in I$ 。

直观理解：理想 vs 子环

- ** 子环 ** 是一个“小一号”的环，结构完整，包含 1。
- ** 理想 ** 类似于群论中的“正规子群”。它通常不包含单位元 1（除非 $I = R$ ）。
- 理想的 ** 吸收性 ** ($R \cdot I \subseteq I$) 是它能被用来定义商环的关键。想象理想像一个“黑洞”，任何外面的元素乘进去，都掉进理想里出不来了。

2 商环与同态 (Quotient Rings & Homomorphisms)

Quotient Structures

2.1 商环的构造

设 I 是 R 的双边理想。我们定义 ** 商环 ** R/I 为模 I 的陪集集合：

$$R/I = \{a + I \mid a \in R\}$$

命题 2.1 (商环的良定义性). 在 R/I 上定义运算：

- 加法: $(a + I) + (b + I) = (a + b) + I$
- 乘法: $(a + I) \cdot (b + I) = (ab) + I$

则 $(R/I, +, \cdot)$ 构成一个环。

证明步骤：证明乘法是良定义的 (Well-defined)

这是商环存在的基石。我们需要证明运算结果不依赖于代表元的选取。

设 $a \sim a'$ 且 $b \sim b'$, 即 $a' = a + x, b' = b + y$, 其中 $x, y \in I$ 。我们要证 $a'b' \sim ab$, 即 $a'b' - ab \in I$ 。

计算差值：

$$\begin{aligned}
 a'b' - ab &= (a+x)(b+y) - ab \\
 &= ab + ay + xb + xy - ab \\
 &= \underbrace{ay}_{\in I} + \underbrace{xb}_{\in I} + \underbrace{xy}_{\in I}
 \end{aligned}$$

- $ay \in I$: 因为 $y \in I$ 且 I 是理想 (右吸收律)。
- $xb \in I$: 因为 $x \in I$ 且 I 是理想 (左吸收律)。
- $xy \in I$: 理想内的乘积仍在理想内。

因此 $a'b' - ab \in I$, 即 $(a'b') + I = (ab) + I$ 。证毕。

2.2 环同态

定义 2.2. 映射 $\phi: R \rightarrow R'$ 是环同态, 若它保持加法、乘法和单位元:

$$\phi(a+b) = \phi(a) + \phi(b), \quad \phi(ab) = \phi(a)\phi(b), \quad \phi(1_R) = 1_{R'}$$

例 2.3 (自然同态). 映射 $\pi: R \rightarrow R/I$, 定义为 $\pi(a) = a + I$, 是一个满射环同态。

3 环的第一同构定理 (First Isomorphism Theorem)

The Core Theorem

定理 3.1 (环的第一同构定理 First Isomorphism Theorem). 设 R 和 S 是环, $\phi: R \rightarrow S$ 是一个环同态。令 $K = \ker(\phi) = \{r \in R \mid \phi(r) = 0_S\}$ 为同态 ϕ 的核。

则 K 是 R 的理想, 且商环 R/K 同构于 ϕ 的像 $\text{Im}(\phi)$ 。即:

$$R/\ker(\phi) \cong \text{Im}(\phi)$$

特别地, 如果 ϕ 是满同态 (*Surjective*), 即 $\text{Im}(\phi) = S$, 则:

$$R/\ker(\phi) \cong S$$

证明. 我们要寻找(构造)一个映射 $\bar{\phi} : R/K \rightarrow S$, 并证明它是双射且保持运算结构。证明过程分为以下四个步骤:

第一步: 构造映射与良定义性 (Construction & Well-definedness)

对于商环中的任意元素(陪集) $a + K$, 定义映射 $\bar{\phi}$ 为:

$$\bar{\phi}(a + K) = \phi(a)$$

由于陪集的代表元不唯一(即 $a + K$ 可能等于 $b + K$), 必须确保函数值不依赖于代表元 a 的选取。

假设 $a + K = b + K$ 。

$$\begin{aligned} a + K = b + K &\implies a - b \in K && (\text{陪集性质}) \\ &\implies a - b \in \ker \phi && (\text{核的定义}) \\ &\implies \phi(a - b) = 0 && (\text{核的性质}) \\ &\implies \phi(a) - \phi(b) = 0 && (\text{同态性质}) \\ &\implies \phi(a) = \phi(b) \end{aligned}$$

因此 $\bar{\phi}(a + K) = \bar{\phi}(b + K)$, 即映射 $\bar{\phi}$ 是良定义的。

第二步: 证明 $\bar{\phi}$ 是环同态 (Homomorphism)

我们需要验证 $\bar{\phi}$ 保持加法、乘法和单位元。设 $\bar{a} = a + K, \bar{b} = b + K$ 。

1. 保持加法:

$$\begin{aligned} \bar{\phi}(\bar{a} + \bar{b}) &= \bar{\phi}((a + b) + K) && (\text{商环加法定义}) \\ &= \phi(a + b) && (\text{映射定义}) \\ &= \phi(a) + \phi(b) && (\phi \text{ 是同态}) \\ &= \bar{\phi}(\bar{a}) + \bar{\phi}(\bar{b}) \end{aligned}$$

2. 保持乘法:

$$\begin{aligned} \bar{\phi}(\bar{a} \cdot \bar{b}) &= \bar{\phi}((ab) + K) && (\text{商环乘法定义}) \\ &= \phi(ab) && (\text{映射定义}) \\ &= \phi(a)\phi(b) && (\phi \text{ 是同态}) \\ &= \bar{\phi}(\bar{a}) \cdot \bar{\phi}(\bar{b}) \end{aligned}$$

3. 保持单位元:

$$\bar{\phi}(1_R + K) = \phi(1_R) = 1_{R'}$$

故 $\bar{\phi}$ 是一个环同态。

第三步：证明 $\bar{\phi}$ 是满射 (Surjective)

设 y 是像集 $S = \text{Im } \phi$ 中的任意元素。根据像的定义，存在 $x \in R$ 使得 $\phi(x) = y$ 。取商环元素 $x + K \in R/K$ ，则有：

$$\bar{\phi}(x + K) = \phi(x) = y$$

因此 $\bar{\phi}$ 是满射。

第四步：证明 $\bar{\phi}$ 是单射 (Injective)

对于环同态，只需证明其核 (Kernel) 只有零元。计算 $\bar{\phi}$ 的核：

$$\begin{aligned}\ker \bar{\phi} &= \{a + K \in R/K \mid \bar{\phi}(a + K) = 0_{R'}\} \\ &= \{a + K \in R/K \mid \phi(a) = 0\} \\ &= \{a + K \in R/K \mid a \in \ker \phi\} \\ &= \{a + K \in R/K \mid a \in K\}\end{aligned}$$

若 $a \in K$ ，则 $a + K = K$ ，这正是商环 R/K 中的零元 $0_{R/K}$ 。即 $\ker \bar{\phi} = \{0_{R/K}\}$ ，故 $\bar{\phi}$ 是单射。

综上所述， $\bar{\phi}$ 既是单射又是满射，且保持环的运算结构，故 $\bar{\phi}$ 是一个环同构。□

直观理解：

直观理解：同态 ϕ 将 R “压缩”到了 R' 中，而 $\ker \phi$ 就是被压缩为 0 的信息。第一同构定理告诉我们，如果我们把这些“丢失的信息”先从 R 中剔除（构造商环），剩下的结构就和像完全一样了。

3.1 应用：构造扩域

这是同构定理在代数方程论中的精彩应用。

例 3.2 (构造扩域 $\mathbb{Q}(\alpha)$ 的详细解析). **背景设定：**设 $\alpha \in \mathbb{C}$ 是一个代数元（即 α 是某个非零有理系数多项式的根，例如 $\alpha = \sqrt{2}$ 或 $\alpha = i$ ）。

符号定义的详细说明：

- $\mathbb{Q}[T]$ (多项式环)：表示系数在有理数域 \mathbb{Q} 上的所有多项式的集合。 T 是形式变量。

$$\mathbb{Q}[T] = \{a_n T^n + \cdots + a_1 T + a_0 \mid a_i \in \mathbb{Q}, n \in \mathbb{N}\}$$

- $f(T)$ (极小多项式): α 在 \mathbb{Q} 上的极小多项式。它是满足以下三个条件的唯一多项式: 1. 首一性: 最高次项系数为 1。2. 不可约性: 在 \mathbb{Q} 上无法分解为两个低次多项式的乘积。3. 零点: $f(\alpha) = 0$ 。
- $(f(T))$ (主理想): 由 $f(T)$ 生成的理想, 即所有 $f(T)$ 的倍数构成的集合。这也是求值同态的核。

$$(f(T)) = \{f(T) \cdot g(T) \mid g(T) \in \mathbb{Q}[T]\}$$

- ev_α (求值同态): 一个从多项式环到复数域的映射, 定义为“将 T 替换为 α ”:

$$ev_\alpha : \mathbb{Q}[T] \rightarrow \mathbb{C}, \quad P(T) \mapsto P(\alpha)$$

- $\mathbb{Q}(\alpha)$ (扩域): 包含 \mathbb{Q} 和 α 的最小子域。对于代数元, 它等于 $\mathbb{Q}[\alpha]$ (包含 \mathbb{Q} 和 α 的最小子环)。

$$\mathbb{Q}(\alpha) = \{c_0 + c_1\alpha + \cdots + c_{d-1}\alpha^{d-1} \mid c_i \in \mathbb{Q}\}$$

其中 $d = \deg(f)$ 。

结论 (应用第一同构定理):

1. 同态基本定理: $R/\ker \phi \cong \text{Im } \phi$ 。

2. 代入本例:

$$\mathbb{Q}[T]/(f(T)) \cong \mathbb{Q}(\alpha)$$

物理意义: 这意味着要在数学上构造一个包含 $\sqrt{2}$ 的域, 不需要真的去计算无理数的小数, 只需要把多项式环 $\mathbb{Q}[T]$ 中的 $T^2 - 2$ 强制规定为 0 (即模掉它) 即可。

4 中国剩余定理 (Chinese Remainder Theorem)

Direct Products & CRT

4.1 环的直积

设 R_1, \dots, R_n 为环。它们的直积定义为:

$$R = R_1 \times \cdots \times R_n = \{(a_1, \dots, a_n) \mid a_i \in R_i\}$$

运算为 ** 逐分量 ** 加法和乘法。注意：直积通常会产生零因子（例如 $(1, 0) \cdot (0, 1) = (0, 0)$ ）。

4.2 中国剩余定理 (CRT)

定理 4.1 (CRT 代数形式). 设 I_1, \dots, I_n 是环 R 的理想。如果它们 ** 两两互素 ** (*Pairwise Coprime*)，即对于任意 $i \neq j$ ，满足 $I_i + I_j = R$ ，则有环同构：

$$R / \left(\bigcap_{i=1}^n I_i \right) \cong R/I_1 \times R/I_2 \times \cdots \times R/I_n$$

证明. 我们要证明自然同态 $\Phi : R \rightarrow \prod_{i=1}^n R/I_i$ 是满射。即：对于任意的目标向量 $(y_1, y_2, \dots, y_n) \in \prod R/I_i$ ，我们需要在 R 中构造一个元素 x ，使得 $\forall k, x \equiv y_k \pmod{I_k}$ 。

证明分为以下三个详细步骤：

第一步：利用理想互素性质分解单位元

题目已知 I_1, \dots, I_n 两两互素，即对于任意 $i \neq j$ ，有 $I_i + I_j = R$ 。这意味着单位元 $1 \in R$ 可以被分解。

固定一个下标 k （例如 $k = 1$ ），对于任意 $j \neq k$ ，因为 $I_k + I_j = R$ ，所以存在 $u_{kj} \in I_k$ 和 $v_{kj} \in I_j$ ，使得：

$$u_{kj} + v_{kj} = 1$$

这个等式给我们两个关键的同余信息：

$$\begin{cases} v_{kj} = 1 - u_{kj} \equiv 1 \pmod{I_k} & (\text{因为 } u_{kj} \in I_k) \\ v_{kj} \equiv 0 \pmod{I_j} & (\text{因为 } v_{kj} \in I_j) \end{cases} \quad (1)$$

第二步：构造“指示元素” e_k

我们的目标是构造一组元素 e_1, \dots, e_n ，使得 e_k 在模 I_k 时是 1，而在模其他 I_j 时是 0。

定义 e_k 为所有 v_{kj} ($j \neq k$) 的乘积：

$$e_k = \prod_{j \neq k} v_{kj}$$

让我们验证 e_k 的性质：

- **性质 A (针对 I_k):**

$$e_k \pmod{I_k} \equiv \prod_{j \neq k} (1) \pmod{I_k} \equiv 1$$

(因为对于所有 $j \neq k$ ，都有 $v_{kj} \equiv 1 \pmod{I_k}$)。

- **性质 B (针对 $I_m, m \neq k$):** 在乘积 $e_k = v_{k1}v_{k2}\dots v_{km}\dots v_{kn}$ 中, 必然包含因子 v_{km} 。由第一步可知 $v_{km} \in I_m$, 由理想的吸收律可知整个乘积必在 I_m 中。

$$e_k \equiv 0 \pmod{I_m}$$

综上所述, 我们构造出了满足如下性质的 e_k :

$$e_k \equiv \delta_{km} = \begin{cases} 1 & (\text{mod } I_m) \quad \text{若 } k = m \\ 0 & (\text{mod } I_m) \quad \text{若 } k \neq m \end{cases}$$

第三步: 构造最终解 x

令 x 为如下线性组合:

$$x = y_1e_1 + y_2e_2 + \dots + y_ne_n = \sum_{i=1}^n y_i e_i$$

我们需要验证对于任意 $k \in \{1, \dots, n\}$, 是否满足 $x \equiv y_k \pmod{I_k}$ 。在模 I_k 的意义下考察 x :

$$\begin{aligned} x \pmod{I_k} &\equiv \sum_{i=1}^n y_i e_i \pmod{I_k} \\ &\equiv y_1e_1 + \dots + y_k e_k + \dots + y_n e_n \pmod{I_k} \end{aligned}$$

根据第二步的结论:

- 当 $i \neq k$ 时, $e_i \equiv 0 \pmod{I_k}$ 。这些项全部消失。
- 当 $i = k$ 时, $e_k \equiv 1 \pmod{I_k}$ 。这一项保留。

因此:

$$x \equiv 0 + \dots + y_k \cdot 1 + \dots + 0 \equiv y_k \pmod{I_k}$$

这证明了 x 确实是原像。故 Φ 是满射。

□

注意 (NOTE): 互素条件的重要性

如果理想不是两两互素的, 映射 Φ 就不是满射, 同构就不成立。这对应于初等数论中, 如果模数 n_1, n_2 不互质, 同余方程组不一定有解。

4.3 与初等数论的联系 (Equivalence to Number Theory)

为了深入理解 CRT，我们将上述抽象的环论描述“翻译”回我们熟悉的整数环 \mathbb{Z} 中的语言。

定理 4.2 (数论形式的 CRT). 设 n_1, n_2, \dots, n_k 是两两互质的正整数 (即 $\gcd(n_i, n_j) = 1, \forall i \neq j$)。令 $N = n_1 n_2 \dots n_k$ 。

对于任意给定的整数 a_1, a_2, \dots, a_k , 同余方程组:

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

在模 N 意义下有唯一解。

证明等价性：从环论到数论

我们可以建立一个“词典”，将环论概念映射到数论概念，从而证明两者是等价的。

环论概念 (Ring Theory)	数论概念 (Number Theory)
环 R	整数环 \mathbb{Z}
理想 I_i	主理想 $n_i\mathbb{Z}$
理想互素 $I_i + I_j = R$	整数互质 $\gcd(n_i, n_j) = 1$ (由裴蜀定理: $un_i + vn_j = 1$)
理想的交 $\bigcap I_i$	最小公倍数 $\text{lcm}(n_1, \dots, n_k)\mathbb{Z} = N\mathbb{Z}$
商环 R/I_i	模 n 剩余类环 \mathbb{Z}_{n_i}
直积 $\prod R/I_i$	向量空间 (a_1, \dots, a_k) , 其中 $a_i \in \mathbb{Z}_{n_i}$

逻辑推导：

- 同构即双射: 环论形式的 CRT 告诉我们存在同构:

$$\Phi : \mathbb{Z}_N \xrightarrow{\sim} \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$$

$$x \pmod{N} \longmapsto (x \pmod{n_1}, \dots, x \pmod{n_k})$$

2. 满射对应“有解”：因为 Φ 是同构，所以它必然是满射。这意味着：对于右边任意一个向量 (a_1, \dots, a_k) （即任意设定的余数目标），在左边 \mathbb{Z}_N 中一定能找到一个原像 x 。 \Rightarrow 方程组一定存在解 x 。
3. 单射对应“唯一性”：因为 Φ 是同构，所以它必然是单射。这意味着：如果在 \mathbb{Z}_N 中有两个解 x, y 对应同一个目标向量，那么必须有 $x = y$ 。 \Rightarrow 解在模 N 意义下是唯一的。

直观理解：直观总结

数论中的“解方程组”，本质上就是在问：映射 $x \mapsto (x \bmod n_1, \dots)$ 是否能覆盖所有的可能性？环论证明了这是一个同构（一一对应），所以不仅能覆盖（有解），而且是一对一的（解唯一）。

本章导读

本文档基于提供的课堂手写笔记整理，涵盖了以下核心主题：

- 整环 (Integral Domains) 的定义与性质。
- 素理想 (Prime Ideal) 与 极大理想 (Maximal Ideal) 的定义、判别法及存在性证明。
- 环同构定理：重点解析第二与第三同构定理。
- 多项式环： $\mathbb{Z}[x]$ 的理想结构分类及多项式环的泛性质。

整环 (Integral Domains)

5 整环的定义

整环是抽象代数中模拟整数集 \mathbb{Z} 性质的环结构。根据笔记，一个代数结构 $(R, 0, 1, +, \cdot)$ 被称为整环，需满足以下条件：

定义 5.1 (整环). 一个环 R 是整环，若满足：

1. R 是交换环 (Commutative Ring)。
2. R 是非平凡的，即 $0 \neq 1$ 。
3. R 没有零因子 (No Zero Divisors)。即：

$$\forall a, b \in R, \quad a \cdot b = 0 \implies a = 0 \text{ 或 } b = 0$$

5.1 消去律 (Cancellation Law)

“没有零因子”这一性质等价于消去律成立：

$$a \neq 0, \quad ab = ac \implies b = c$$

例 5.2 (常见的整环与非整环). • \mathbb{Z} 是整环。

- 所有的域 (Fields) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ 都是整环。

- 若 R 是整环，则多项式环 $R[x]$ 也是整环。
- \mathbb{Z}_6 不是整环（因为 $2 \cdot 3 = 0$ 但 $2 \neq 0, 3 \neq 0$ ）。

素理想与极大理想

6 定义与判别法

极大理想 (Maximal Ideal)

定义： I 是真理想，且不存在理想 J 使 $I \subsetneq J \subsetneq R$ 。
定义：若 $ab \in I \Rightarrow a \in I$ 或 $b \in I$ 。

判别法： I 是极大理想 $\Leftrightarrow R/I$ 是整域。
判别法： I 是素理想 $\Leftrightarrow R/I$ 是整环。

6.1 素理想 (Prime Ideal)

6.1.1 定义与定理

定义 6.1 (素理想). 设 I 是环 R 的一个真理想 ($I \neq R$)。若对于任意 $a, b \in R$, 满足：

$$ab \in I \Rightarrow a \in I \quad \text{或} \quad b \in I$$

则称 I 为 R 的素理想。

定理 6.2 (素理想判别法). 理想 I 是 R 的素理想，当且仅当商环 R/I 是整环 (Integral Domain)。

6.1.2 详细证明

证明. 我们将证明分为充分性与必要性两部分。

(\Rightarrow) **必要性：**假设 I 是素理想，求证 R/I 是整环。

1. **非平凡性：**因为 I 是真理想，所以商环 R/I 含有至少两个元素 ($\bar{0} \neq \bar{1}$)。

2. 无零因子检验：设 $\bar{a}, \bar{b} \in R/I$ 且满足 $\bar{a} \cdot \bar{b} = \bar{0}$ 。根据商环的运算定义，这意味着：

$$(a + I)(b + I) = ab + I = I \iff ab \in I$$

3. 利用素理想性质：因为 I 是素理想，由 $ab \in I$ 可推出 $a \in I$ 或 $b \in I$ 。

- 若 $a \in I$ ，则 $\bar{a} = \bar{0}$ 。
- 若 $b \in I$ ，则 $\bar{b} = \bar{0}$ 。

4. 结论： R/I 没有零因子，因此是整环。

(\Leftarrow) 充分性：假设 R/I 是整环，求证 I 是素理想。

1. 设 $a, b \in R$ 且 $ab \in I$ 。
2. 在商环中，这意味着 $\bar{ab} = \bar{0}$ ，即 $\bar{a} \cdot \bar{b} = \bar{0}$ 。
3. 因为 R/I 是整环（无零因子），所以必有 $\bar{a} = \bar{0}$ 或 $\bar{b} = \bar{0}$ 。
4. 还原回环 R 的语言，即 $a \in I$ 或 $b \in I$ 。
5. 这正是素理想的定义。

□

6.2 极大理想 (Maximal Ideal)

6.2.1 定义与定理

定义 6.3 (极大理想). 设 I 是环 R 的一个真理想。若不存在理想 J 使得：

$$I \subsetneq J \subsetneq R$$

则称 I 为 R 的极大理想。换言之， I 是包含关系下最大的真理想。

定理 6.4 (极大理想判别法). 理想 I 是 R 的极大理想，当且仅当商环 R/I 是域 (Field)。

6.2.2 详细证明

证明. (\Rightarrow) 必要性：假设 I 是极大理想，求证 R/I 是域。

目标：证明 R/I 中任意非零元素都有逆元。

1. 任取 $\bar{a} \in R/I$ 且 $\bar{a} \neq \bar{0}$ 。这意味着 $a \in R$ 但 $a \notin I$ 。
2. 构造由 I 和 a 生成的理想 $J = (I, a) = \{i + ra \mid i \in I, r \in R\}$ 。
3. 显然 $I \subseteq J$ 。因为 $a \in J$ 且 $a \notin I$, 所以 $I \subsetneq J$ 。
4. 根据 I 的极大性, 唯一的可能性是 $J = R$ 。
5. 既然 $J = R$, 单位元 $1 \in J$ 。因此存在 $i \in I$ 和 $r \in R$ 使得:

$$1 = i + ra$$

6. 在两边取模 I (注意 $i \equiv 0 \pmod{I}$):

$$\bar{1} = \bar{0} + \bar{r}\bar{a} \implies \bar{r}\bar{a} = \bar{1}$$

7. 结论: \bar{a} 存在逆元 \bar{r} , 故 R/I 是域。

(\Leftarrow) 充分性: 假设 R/I 是域, 求证 I 是极大理想。

目标：证明若理想 J 严格包含 I , 则 $J = R$ 。

1. 设 J 是 R 的理想, 且 $I \subsetneq J \subseteq R$ 。
2. 因为 $I \subsetneq J$, 存在 $a \in J$ 且 $a \notin I$ 。
3. 在商环 R/I 中, $\bar{a} \neq \bar{0}$ 。因为 R/I 是域, \bar{a} 必有逆元, 设为 \bar{b} 。即 $\bar{a}\bar{b} = \bar{1}$ 。
4. 这意味着 $ab - 1 \in I$ 。即存在 $i \in I$ 使得 $1 = ab - i$ 。
5. 检查元素归属:

- $a \in J \implies ab \in J$ (理想的吸收律)。
- $i \in I \subsetneq J \implies i \in J$ 。

所以 $1 = ab - i$ 是两个 J 中元素的差, 故 $1 \in J$ 。

6. 结论: 包含单位元的理想必然等于全环, 即 $J = R$ 。故 I 是极大理想。

□

6.3 素理想与极大理想的关系

推论 6.5. 在含幺交换环中，每一个极大理想必然是素理想。

证明. 逻辑推导如下：

$$I \text{ 是极大理想} \xrightarrow{\text{定理 2.2}} R/I \text{ 是域} \implies R/I \text{ 是整环} \xrightarrow{\text{定理 1.2}} I \text{ 是素理想}$$

注：域一定是整环，因为域中所有非零元素可逆，不可能存在两个非零元素乘积为零的情况。 \square

注意 (NOTE): 注意：逆命题不成立

素理想不一定是极大理想。

例 6.6. 在整数环 \mathbb{Z} 中，零理想 (0) 是素理想（因为 $\mathbb{Z} \cong \mathbb{Z}/(0)$ 是整环），但它不是极大理想（因为 \mathbb{Z} 不是域）。

7 Zorn 引理与极大理想的存在性

在包含幺元的环中，极大理想的存在性依赖于 Zorn 引理。

定理 7.1 (Krull 定理). 任何非零幺环 R 至少有一个极大理想。

证明. 令 Σ 为 R 中所有真理想构成的集合，按包含关系 \subseteq 排序。

1. Σ 非空（包含零理想）。
2. 取 Σ 中的任意一条链 $\mathcal{C} = \{I_\alpha\}$ 。令 $U = \bigcup I_\alpha$ 。
3. 易证 U 仍是理想。且因 $1 \notin I_\alpha (\forall \alpha)$ ，故 $1 \notin U$ ，即 U 是真理想。
4. U 是链 \mathcal{C} 的上界。

根据 Zorn 引理， Σ 存在极大元 M 。此 M 即为 R 的极大理想。 \square

环同构定理

8 第三同构定理 (分数消去律)

8.1 定理陈述

设 R 是环, I 和 J 均是 R 的理想, 且满足包含关系 $I \subseteq J$ 。则 J/I 是商环 R/I 的理想, 且有同构关系:

$$(R/I)/(J/I) \cong R/J$$

直观理解: 记忆技巧

类比繁分数的化简: $\frac{R/I}{J/I} \approx \frac{R}{J}$ 。分母中的 I 被“消去”了。

8.2 详细证明

证明. 我们将利用环的第一同构定理来证明。

1. 构造映射: 定义映射 $\varphi: R/I \rightarrow R/J$, 规则为:

$$\varphi(r+I) = r+J$$

即把 R/I 中的陪集映射到 R/J 中对应的陪集。

2. 验证良定性 (Well-defined): 设 $r+I = r'+I$, 则 $r-r' \in I$ 。由于已知 $I \subseteq J$, 所以 $r-r' \in J$ 。这意味着 $r+J = r'+J$ 。因此, 映射结果与陪集代表元的选取无关, 映射是良定的。
3. 验证同态与满射: 显然 φ 保持加法和乘法运算, 是一个环同态。对于任意 $y \in R/J$, 设 $y = r+J$, 则存在 $x = r+I \in R/I$ 使得 $\varphi(x) = y$ 。故 φ 是满射。
4. 计算核 (Kernel): 由核的定义计算:

$$\begin{aligned}\ker \varphi &= \{r+I \in R/I \mid \varphi(r+I) = 0_{R/J}\} \\ &= \{r+I \in R/I \mid r+J = J\} \\ &= \{r+I \in R/I \mid r \in J\}\end{aligned}$$

这正是集合 J/I (即 J 在商环 R/I 中的像)。

5. 结论: 根据第一同构定理 $R/I/\ker \varphi \cong \text{Im } \varphi$, 即得:

$$(R/I)/(J/I) \cong R/J$$

□

应用实例：在 \mathbb{Z} 中，取 $I = 12\mathbb{Z}, J = 4\mathbb{Z}$ 。

$$(\mathbb{Z}/12\mathbb{Z})/(4\mathbb{Z}/12\mathbb{Z}) \cong \mathbb{Z}/4\mathbb{Z}$$

即 \mathbb{Z}_{12} 模掉其子群 $\{\bar{0}, \bar{4}, \bar{8}\}$ 同构于 \mathbb{Z}_4 。

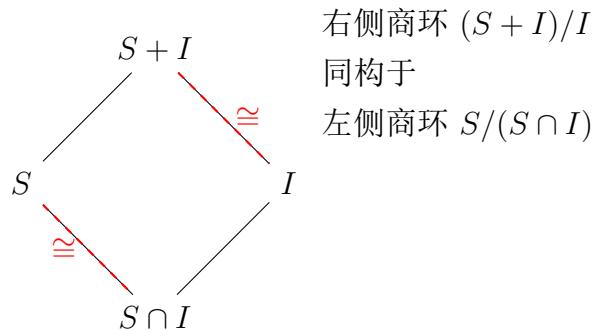
9 第二同构定理 (钻石同构定理)

9.1 定理陈述

设 S 是 R 的子环， I 是 R 的理想。则 $S + I$ 是 R 的子环， $S \cap I$ 是 S 的理想，且：

$$(S + I)/I \cong S/(S \cap I)$$

图解含义：



9.2 详细证明

证明。同样利用第一同构定理。我们的策略是构造一个从 S 出发的自然同态。

1. 构造映射：定义映射 $\phi: S \rightarrow (S + I)/I$ ，规则为：

$$\phi(s) = s + I$$

这本质上是自然同态 $\pi: R \rightarrow R/I$ 在子环 S 上的限制。显然 ϕ 是环同态。

2. 验证满射 (Surjective)：考查目标环 $(S + I)/I$ 中的任意元素。其形式为 $(s + i) + I$ ，其中 $s \in S, i \in I$ 。利用理想的吸收性质 ($i \in I \implies i + I = I$)：

$$(s + i) + I = s + (i + I) = s + I = \phi(s)$$

这意味着目标环中的任一元素都可以表示为某个 $s \in S$ 的像。故 ϕ 是满射。

3. 计算核 (Kernel): 由核的定义计算:

$$\begin{aligned}\ker \phi &= \{s \in S \mid \phi(s) = 0_{(S+I)/I}\} \\ &= \{s \in S \mid s + I = I\} \\ &= \{s \in S \mid s \in I\} \\ &= S \cap I\end{aligned}$$

4. 结论: 根据第一同构定理 $S/\ker \phi \cong \text{Im } \phi$, 即得:

$$S/(S \cap I) \cong (S + I)/I$$

□

多项式环的性质与结构

10 多项式环的万有性质 (Universal Property)

多项式环 $R[x]$ 是代数中的自由对象。这一性质刻画了多项式环最本质的特征: 它仅仅由系数和变量构成, 除此之外没有任何其它的代数约束。

10.1 定理陈述

定理 10.1 (多项式环的万有性质). 设 R, S 为交换环。给定一个环同态 $\phi_0 : R \rightarrow S$ (处理系数) 和一个元素 $\alpha \in S$ (指定变量的去向)。则存在唯一的环同态 $\Phi : R[x] \rightarrow S$ 满足以下两个条件:

1. 延拓性: $\Phi|_R = \phi_0$ (即对任意常数 $r \in R$, $\Phi(r) = \phi_0(r)$)。
2. 赋值性: $\Phi(x) = \alpha$ 。

10.2 双射公式与符号详解

上述定理可以用范畴论的语言总结为一个简洁的双射公式:

$$\text{Hom}_{\text{Ring}}(R[x], S) \cong \text{Hom}_{\text{Ring}}(R, S) \times S$$

10.2.1 符号含义

- $\text{Hom}_{\text{Ring}}(A, B)$: 表示从环 A 到环 B 的所有环同态构成的集合。
- \times : 集合的笛卡尔积。
- 左边 $\text{Hom}(R[x], S)$: 这是一个很大的集合, 包含所有从多项式环出发到 S 的复杂同态 Φ 。
- 右边 $\text{Hom}(R, S) \times S$: 这是一个由“简单数据”构成的对子 (ϕ_0, α) 。
- \cong (一一对应): 表示确定左边的一个复杂映射, 完全等价于确定右边的一组简单数据。

10.3 直观解释: 为什么是双射?

这个双射的本质是“代入求值原理”。

1. 从右往左 (\leftarrow): 构造映射如果你给了我一个系数的映射规则 ϕ_0 和一个 x 的替身 α 。对于任意多项式 $f(x) = \sum_{i=0}^n c_i x^i$, 我被迫只能这样定义 Φ :

$$\Phi(f(x)) = \sum_{i=0}^n \phi_0(c_i) \cdot \alpha^i$$

这实际上就是把 x 换成 α 进行计算。因为同态必须保持加法和乘法, 这个构造是唯一的。

2. 从左往右 (\rightarrow): 提取数据如果你给了我一个定义好的同态 $\Phi : R[x] \rightarrow S$ 。我可以立刻提取出两组信息:

- 它怎么处理常数? $\phi_0(r) = \Phi(r)$ 。
- 它把 x 变成了什么? $\alpha = \Phi(x)$ 。

直观理解: 自由对象的含义

之所以称多项式环是自由的, 是因为变量 x 没有任何约束。

- 对比 $\mathbb{Z}[i] \cong \mathbb{Z}[x]/(x^2 + 1)$: 在这里, i 必须满足 $i^2 = -1$ 。所以映射时, i 的像必须也是一个平方为 -1 的元素, 不能随意指定。
- 而在 $R[x]$ 中, x 可以被映射为 S 中的任意元素 α , 没有任何限制。

10.3.1 推广到多元多项式

对于 n 元多项式环 $R[x_1, \dots, x_n]$, 双射关系推广为:

$$\text{Hom}(R[x_1, \dots, x_n], S) \cong \text{Hom}(R, S) \times \underbrace{S \times \cdots \times S}_{n \text{ 个}}$$

即确定一个多元多项式同态, 只需要确定系数的映射 ϕ_0 以及 n 个变量分别对应的 n 个数值 $(\alpha_1, \dots, \alpha_n)$ 。

11 $\mathbb{Z}[x]$ 的理想结构分类

$\mathbb{Z}[x]$ 不是主理想整环 (PID), 其 Krull 维数为 2。我们可以根据理想 I 与 \mathbb{Z} 的交集情况对其素理想进行完全分类。

11.1 分类讨论与详细证明

设 I 是 $\mathbb{Z}[x]$ 的素理想。我们根据 I 与整数环 \mathbb{Z} 的交集 $I \cap \mathbb{Z}$ 进行分类讨论。

1. 情形一: $I \cap \mathbb{Z} = (0)$

此时 I 不包含任何非零整数 (常数)。

- 子情形 1.1: $I = (0)$ 显然 (0) 是素理想, 对应于 $\mathbb{Z}[x]$ 是整环的事实。
- 子情形 1.2: $I \neq (0)$

证明. 1. 选取生成元: 在 I 中选取一个次数最低且非零的多项式 $g(x)$ 。由于 $\mathbb{Z}[x]$ 是 UFD, 我们可以不妨设 $g(x)$ 是本原多项式 (即系数互素)。由于 I 是素理想且 $I \neq (0)$, 这样的 $g(x)$ 必然是 $\mathbb{Z}[x]$ 中的不可约多项式。

2. 断言 $I = (g(x))$: 假设存在 $h(x) \in I$ 使得 $g(x) \nmid h(x)$ 。
3. 利用 Gauss 引理转至 $\mathbb{Q}[x]$: 视 g, h 为有理多项式环 $\mathbb{Q}[x]$ 中的元素。由于 $g(x)$ 在 $\mathbb{Z}[x]$ 中本原不可约, 由 Gauss 引理知, 它在 $\mathbb{Q}[x]$ 中也是不可约的。因此, 在 $\mathbb{Q}[x]$ 中 $\gcd(g, h) = 1$ 。
4. Bézout 等式导出矛盾: 因为 $\mathbb{Q}[x]$ 是主理想整环 (PID), 存在 $u(x), v(x) \in \mathbb{Q}[x]$ 使得:

$$u(x)g(x) + v(x)h(x) = 1$$

等式两边同乘一个足够大的整数 d (u, v 分母的公倍数), 可清除分母得到:

$$A(x)g(x) + B(x)h(x) = d$$

其中 $A(x), B(x) \in \mathbb{Z}[x]$, 且 $d \in \mathbb{Z} \setminus \{0\}$ 。

观察等式左边: $A(x)g(x) \in I$ 且 $B(x)h(x) \in I$ (因为 $g, h \in I$)。故左边整体属于 I , 从而推导出 $d \in I$ 。即 $d \in I \cap \mathbb{Z}$ 。但根据前提 $I \cap \mathbb{Z} = (0)$, 这迫使 $d = 0$, 与 d 是非零整数矛盾!

5. 结论: 假设不成立, 故 I 中所有元素都能被 $g(x)$ 整除, 即 $I = (g(x))$ 。 \square

2. 情形二: $I \cap \mathbb{Z} \neq (0)$

此时 I 包含非零整数。

证明. 1. 确定素数 p : 考察 $I \cap \mathbb{Z}$ 。这是 \mathbb{Z} 的一个非零理想。由于 I 是环 $\mathbb{Z}[x]$ 的素理想, 容易验证 $I \cap \mathbb{Z}$ 必须是 \mathbb{Z} 的素理想。 \mathbb{Z} 中的非零素理想形如 (p) , 其中 p 是素数。故存在素数 p 使得 $I \cap \mathbb{Z} = (p)$, 且 $p \in I$ 。

2. 模 p 约化: 考虑自然同态 (模 p 映射):

$$\pi : \mathbb{Z}[x] \rightarrow (\mathbb{Z}/p\mathbb{Z})[x] \cong \mathbb{F}_p[x]$$

该映射将多项式的系数模 p 。根据对应定理, $\mathbb{Z}[x]$ 中包含 (p) 的理想 I 与商环 $\mathbb{F}_p[x]$ 中的理想 $\bar{I} = \pi(I)$ 一一对应。

3. 利用 PID 性质: 由于 I 是素理想, 其像 \bar{I} 在 $\mathbb{F}_p[x]$ 中也是素理想。 $\mathbb{F}_p[x]$ 是域上的多项式环, 因而是主理想整环 (PID)。故 \bar{I} 必由某个多项式 $\bar{f}(x) \in \mathbb{F}_p[x]$ 生成, 即 $\bar{I} = (\bar{f}(x))$ 。

4. 分类讨论 \bar{I} :

- 若 $\bar{I} = (\bar{0})$: 这意味着 I 中的多项式模 p 后都是 0, 即 $I \subseteq (p)$ 。结合 $p \in I$, 得 $I = (p)$ 。
- 若 $\bar{I} \neq (\bar{0})$: 此时生成元 $\bar{f}(x)$ 必须是 $\mathbb{F}_p[x]$ 中的不可约多项式 (因为 \bar{I} 是非零素理想)。取 $\bar{f}(x)$ 在 $\mathbb{Z}[x]$ 中的原像 $f(x)$ (选取首一多项式)。则 I 由 p 和 $f(x)$ 生成。即 $I = (p, f(x))$, 其中 $f(x)$ 在模 p 下不可约。

5. 结论: 此情形下, 素理想为 (p) 或 $(p, f(x))$ 。后者是极大理想, 因为商环 $\mathbb{Z}[x]/(p, f(x)) \cong \mathbb{F}_p[x]/(\bar{f}(x))$ 是一个有限域。 \square

本章导读

本章基于 P6-P18 笔记整理，旨在梳理抽象代数中关于整环（Integral Domain）的核心层级结构。我们从具体的算术系统（如整数 \mathbb{Z} 和高斯整数 $\mathbb{Z}[i]$ ）出发，抽象出三类重要的环：

1. 欧几里得环 (ED): 拥有带余除法。
2. 主理想整环 (PID): 所有理想都是主理想。
3. 唯一分解整环 (UFD): 拥有类似“算术基本定理”的唯一分解性质。

核心目标是理解它们之间的蕴含关系，以及素元与不可约元在不同环境下的等价性。

一、环的层级结构与核心定义

12 基本元素分类

设 R 是一个整环（无零因子的交换幺环）。对于 $a \in R, a \neq 0$ ，我们定义以下三类元素：

定义 12.1 (单位, 不可约元, 素元). • **单位 (Unit):** 如果 $a \in R^\times$ ，即存在逆元，则称 a 为单位。

- **不可约元 (Irreducible Element):** 非零非单位元素 a 。若 $a = bc$ ，则 b 是单位或 c 是单位（即 a 没有非平凡因子）。
- **素元 (Prime Element):** 非零非单位元素 a 。若 $a | bc$ ，则 $a | b$ 或 $a | c$ （即 (a) 是素理想）。

命题 12.2 (素元与不可约元的关系). 在任意整环中：

$$\text{素元} \implies \text{不可约元}$$

但是在一般整环中，反之不成立（例如在 $\mathbb{Z}[\sqrt{-5}]$ 中）。只有在 UFD 或 PID 中，两者才等价。

1. 回顾定义：设 $p \in R$ 是一个素元。根据定义， $p \neq 0$ 且 p 不是单位。

2. 假设分解: 假设 p 有一个因子分解:

$$p = ab \quad (\text{其中 } a, b \in R)$$

要证明 p 是不可约元, 我们需要证明 a 和 b 中至少有一个是单位。

3. 应用素元性质: 由等式 $p = ab$ 可知, $p \mid ab$ 。因为 p 是素元, 根据定义, 必有 $p \mid a$ 或 $p \mid b$ 。

4. 分情况讨论:

- 情形 1: 若 $p \mid a$ 。这意味着存在 $k \in R$, 使得 $a = pk$ 。将此代回原分解式:

$$p = (pk)b = p(kb)$$

因为 R 是整环且 $p \neq 0$, 由消去律可得:

$$1 = kb$$

根据单位的定义, 这说明 b 是单位 (可逆元)。

- 情形 2: 若 $p \mid b$ 。同理可得, 存在 k 使得 $b = pk$, 进而推导出 $1 = ka$, 说明 a 是单位。

5. 结论: 在 p 的任意分解 $p = ab$ 中, 因子 a, b 必有一个是单位。这正是不可约元的定义。

13 三大整环的层级

环论中最重要的包含链如下:

$$(\mathbf{ED}) \implies (\mathbf{PID}) \implies (\mathbf{UFD})$$

- ED (欧几里得环): 存在范数 $N(r)$, 使得对任意 α, β , 存在 q, r 满足 $\alpha = \beta q + r$, 且 $r = 0$ 或 $N(r) < N(\beta)$ 。
- PID (主理想整环): 环中每一个理想 I 都是由单个元素生成的主理想, 即 $I = (a)$ 。
- UFD (唯一分解整环): 任意非零非单位元素能唯一 (相伴、不计次序意义下) 分解为不可约元的乘积。

二、主理想整环 (PID) 的核心性质

PID 是性质非常好的环, 它不仅保证了 UFD 性质, 还融合了数论中的贝祖定理。

13.1 贝祖定理

定理 13.1 (贝祖定理 Bézout's Identity). 设 R 是主理想整环 (PID)。对于任意 $a, b \in R$ (不全为 0)，令 d 是它们的一个最大公约数 (GCD)。则存在 $x, y \in R$ 使得：

$$ax + by = d$$

核心思路：构造由 a 和 b 生成的理想，利用 PID 性质将其“塌缩”为由单个元素 d 生成的主理想。

1. **构造线性组合构成的集合：**考察集合 $I = \{ra + sb \mid r, s \in R\}$ 。容易验证 I 是 R 的一个理想（即对加法封闭，且吸收环中的乘法）。这个理想通常记作 (a, b) 。
2. **利用 PID 性质：**因为 R 是 PID，所以 R 中所有的理想都是主理想。这意味着理想 I 必须由某个单独的元素 d' 生成。即存在 $d' \in R$ 使得：

$$I = (a, b) = (d')$$

3. **证明 d' 就是 a, b 的最大公约数：**

- **公因数性质：**显然 $a = 1 \cdot a + 0 \cdot b \in I$ 。因为 $I = (d')$ ，所以 $a \in (d')$ ，即 $d' \mid a$ 。同理 $b = 0 \cdot a + 1 \cdot b \in I$ ，即 $d' \mid b$ 。所以 d' 是 a 和 b 的公因数。
- **“最大”性质：**设 c 是 a 和 b 的任意公因数（即 $c \mid a$ 且 $c \mid b$ ）。对于 I 中的任意元素 $z = ra + sb$ ，由于 c 能整除 a 和 b ，它必然也能整除 a, b 的线性组合。即 $c \mid (ra + sb)$ 。因为 $d' \in I$ ，所以 d' 也可以写成 $ra + sb$ 的形式，故 $c \mid d'$ 。

综上， d' 满足最大公约数的定义。我们可以令 $d = d'$ （相伴意义下）。

4. **得出贝祖等式：**既然 d 是理想 I 的生成元，那么显然 $d \in I$ 。根据 I 的定义，集合 I 中的任何元素都可以写成 a 和 b 的线性组合。因此，必然存在 $x, y \in R$ ，使得：

$$d = xa + yb$$

13.2 重要命题：元素性质的等价性

定理 13.2 (PID 中的四重等价). 设 R 是 PID，对于 $a \neq 0$ 且非单位，以下四条等价：

(a) a 是不可约元

(b) a 是素元

(c) (a) 是素理想

(d) (a) 是极大理想

命题 13.3. 设 R 是主理想整环 (PID), $a \in R$ 是不可约元。则主理想 (a) 是 R 中的极大理想。

证明. 我们需要证明: 对于任意理想 I 满足 $(a) \subseteq I \subseteq R$, 必有 $I = (a)$ 或 $I = R$ 。

1. 引入中间理想: 设 I 是 R 的一个理想, 且满足 $(a) \subseteq I \subseteq R$ 。
2. 利用 PID 性质: 因为 R 是主理想整环 (PID), 所以 R 中的每一个理想都是主理想。因此, 存在某个元素 $b \in R$, 使得 $I = (b)$ 。此时包含关系变为: $(a) \subseteq (b) \subseteq R$ 。
3. 将理想包含转化为元素整除: 由 $(a) \subseteq (b)$ 可知, $a \in (b)$ 。根据主理想的定义, 这意味着存在 $c \in R$, 使得:

$$a = b \cdot c$$

即 b 是 a 的因子 ($b | a$)。

4. 利用不可约元的定义: 已知 a 是不可约元。根据定义, 不可约元的因子 b 只有两种可能的情况:

- 情形 1: b 是单位 (Unit)。
- 情形 2: b 与 a 相伴 (Associates) (即 c 是单位)。

5. 分情况讨论理想的等规性:

- 若 b 是单位: 根据理想的性质, 包含单位的理想必然是全环。即:

$$(b) = R \implies I = R$$

- 若 b 与 a 相伴: 这意味着存在单位 u 使得 $b = ua$ 。
 - 一方面, 已知 $(a) \subseteq (b)$ 。
 - 另一方面, 由 $a = u^{-1}b$ 可知 $a \in (b)$ (这一点已知), 但更重要的是, 因为 a 和 b 互为单位倍数, 它们生成相同的理想:

$$(a) = (b) \implies I = (a)$$

6. 结论: 综上所述, 包含 (a) 的理想 I 只能是 (a) 本身或者全环 R 。根据极大理想的定义, (a) 是极大理想。

□

13.3 PID 推出 UFD

命题 13.4. 若 R 是 PID，则 R 是 UFD。

- **存在性:** 利用 PID 的诺特性质（理想升链条件 ACC），证明分解步骤必然终止，不会无限分解。
- **唯一性:** 利用“PID 中不可约元即素元”。若有两个分解 $p_1 \dots p_m = q_1 \dots q_n$ ，则 $p_1 \mid$ 右边，必与某个 q_j 相伴，消去后归纳证明。

证明： $PID \implies UFD$. 我们需要验证 UFD 的两个定义条件：(1) 分解的存在性，(2) 分解的唯一性。

第一步：证明分解的存在性 (Existence)

思路：利用 PID 的诺特性质（Noetherian Property），即理想升链条件 (ACC)。

1. **反证法:** 假设 R 中存在一个非零非单位元素 a ，它不能写成有限个不可约元的乘积。
2. 既然 a 不能分解成有限个不可约元，那么 a 本身一定不是不可约元。于是 a 可以分解为 $a = a_1 b_1$ ，其中 a_1, b_1 都是非单位。
3. 由于 a 没有有限分解，那么 a_1 和 b_1 中至少有一个也没有有限分解。不妨设是 a_1 。此时我们有真包含关系： $(a) \subsetneq (a_1)$ 。
4. 对 a_1 重复上述过程，我们可以构造出一个无限的、严格递增的主理想升链：

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \dots \subsetneq (a_n) \subsetneq \dots$$

5. 令 $I = \bigcup_{n=1}^{\infty} (a_n)$ 。易证 I 也是 R 的一个理想。
6. **利用 PID 性质:** 因为 R 是 PID，所以 I 必须是主理想，设 $I = (d)$ 。
7. 因为 $d \in I$ ，根据并集的定义， d 必须属于链条中的某一个理想，即存在 k 使得 $d \in (a_k)$ 。
8. 这意味着 $(d) \subseteq (a_k)$ 。但同时我们有 $(a_k) \subseteq I = (d)$ 。
9. 于是 $(a_k) = (d) = I$ 。这意味着对于所有的 $n \geq k$ ，都有 $(a_n) = (a_k)$ 。
10. **矛盾:** 这与我们构造的“严格递增”链条矛盾。因此，假设不成立，任何元素都能分解为有限个不可约元的乘积。

第二步：证明分解的唯一性 (Uniqueness)

思路：利用 PID 中“不可约元 \iff 素元”的关键性质。

1. 设元素 a 有两种不可约分解：

$$a = p_1 p_2 \dots p_m = q_1 q_2 \dots q_n$$

其中 p_i, q_j 均为不可约元。

2. 考虑 p_1 。显然 $p_1 \mid a$, 即 $p_1 \mid q_1 q_2 \dots q_n$ 。
3. 利用素性：在 PID 中，不可约元 p_1 也是素元。根据素元定义， p_1 必须整除乘积中的某一个因子。不妨设 $p_1 \mid q_1$ (必要时重排顺序)。
4. 因为 q_1 也是不可约元，它的因子只能是单位或相伴元。由于 p_1 不是单位，故 p_1 与 q_1 相伴。即 $q_1 = u_1 p_1$, 其中 u_1 是单位。
5. 在等式两边利用消去律消去 p_1 , 得到：

$$p_2 \dots p_m = u_1 q_2 \dots q_n$$

6. 重复上述过程。每次消去一个 p_i , 必然对应右边的一个 q_j 。
7. 如果 $m < n$, 左边消完变成 1, 右边还剩不可约元, 矛盾 (不可约元非单位)。同理 $m > n$ 也不可能。
8. 结论：必须有 $m = n$, 且经过重排后, 每个 p_i 都与 q_i 相伴。证毕。

□

补充证明：其余逻辑链条 $(d) \Rightarrow (c) \Rightarrow (b) \Rightarrow (a)$

上述证明已经确立了 $(a) \Rightarrow (d)$ 。为了完成等价性证明，我们只需证明反向链条成立。以下推导在任意整环中均有效：

1. 证明 $(d) \Rightarrow (c)$: 极大理想 \implies 素理想

证明。

- 设 (a) 是 R 的极大理想。根据环论基本定理，商环 $R/(a)$ 是一个域 (Field)。
- 域必然是无零因子的，因此 $R/(a)$ 也是整环 (Integral Domain)。

- 理想 I 是素理想的充要条件是商环 R/I 为整环。
- 因此, (a) 必然是素理想。

□

2. 证明 $(c) \Rightarrow (b)$: 素理想 \implies 素元

证明. 这直接源于定义的翻译:

- 设 (a) 是素理想。假设 $x, y \in R$ 满足 $a | xy$ 。
- 整除关系 $a | xy$ 等价于元素关系 $xy \in (a)$ 。
- 根据素理想定义: 若 $xy \in (a)$, 则 $x \in (a)$ 或 $y \in (a)$ 。
- 翻译回整除语言: $a | x$ 或 $a | y$ 。
- 这正是素元的定义。

□

3. 证明 $(b) \Rightarrow (a)$: 素元 \implies 不可约元

证明. • 设 a 是素元。假设 a 有分解 $a = xy$ 。

- 显然 $a | xy$ 。因为 a 是素元, 所以 $a | x$ 或 $a | y$ 。
- **情形 1:** 若 $a | x$ 。这意味着存在 $k \in R$ 使得 $x = ak$ 。代回原分解式: $a = (ak)y = a(ky)$ 。因为 R 是整环且 $a \neq 0$, 利用消去律可得 $1 = ky$ 。这意味着 y 是单位。
- **情形 2:** 若 $a | y$ 。同理可推导出 x 是单位。
- **结论:** a 的任意分解中必有一个因子是单位, 故 a 是不可约元。

□

注意 (NOTE): 总结

完整的逻辑闭环如下:

$$\text{不可约元}(a) \xrightarrow{\text{PID}} \text{极大理想}(d) \rightarrow \text{素理想}(c) \rightarrow \text{素元}(b) \rightarrow \text{不可约元}(a)$$

这说明在 PID 中, 这四个概念是完全等价的。

14 典型实例分析

三、典型实例分析

14.1 1. 高斯整数环 $\mathbb{Z}[i]$

定义 $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, 它是复数域 \mathbb{C} 的子环。

定理 14.1. $\mathbb{Z}[i]$ 是欧几里得环 (ED), 因此也是 PID 和 UFD。

目标: 对于任意 $z \in \mathbb{Q}(i)$ (商域中的元素), 寻找一个高斯整数 $q \in \mathbb{Z}[i]$, 使得范数 $N(z - q) \leq \frac{1}{2}$ 。

1. **写成分量形式:** 设 $z = x + yi$, 其中 $x, y \in \mathbb{Q}$ (事实上对任意实数都成立)。
2. **实部与虚部的逼近:** 对于任意实数 x , 我们总能在数轴上找到一个距离最近的整数 $m \in \mathbb{Z}$, 使得:

$$|x - m| \leq \frac{1}{2}$$

(直观理解: 这就是“四舍五入”。如果 x 恰好在两个整数正中间, 任选一个即可)。

同理, 对于虚部 y , 存在整数 $n \in \mathbb{Z}$, 使得:

$$|y - n| \leq \frac{1}{2}$$

3. **构造高斯整数 q :** 令 $q = m + ni$ 。显然 $q \in \mathbb{Z}[i]$ 。

4. **计算距离 (范数):** 考察 z 与 q 的差:

$$z - q = (x + yi) - (m + ni) = (x - m) + (y - n)i$$

计算其范数 (即复数模长的平方):

$$N(z - q) = (x - m)^2 + (y - n)^2$$

5. **不等式放缩:** 代入步骤 2 中的不等式:

$$N(z - q) \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$

6. **结论:** 对于任意除法 $\alpha \div \beta$, 令 $z = \alpha/\beta$, 我们找到了 q 使得 $N(\frac{\alpha}{\beta} - q) < 1$ 。令余数 $r = \alpha - \beta q$, 则 $N(r) = N(\beta)N(\frac{\alpha}{\beta} - q) \leq \frac{1}{2}N(\beta) < N(\beta)$ 。这正是欧几里得除法所需的条件。

直观理解：几何直观

复平面上的高斯整数构成格点。对于任意复数 $z \in \mathbb{Q}(i)$, 总能找到最近的格点 q , 使得距离平方 $N(z - q) \leq \frac{1}{2} < 1$ 。这是欧氏除法成立的关键。

高斯素数的分类 (Classification of Gaussian Primes)

整数环 \mathbb{Z} 中的素数 p 扩充到 $\mathbb{Z}[i]$ 后, 会发生什么? 根据费马平方和定理, 分为三类:

类型	条件 ($p \in \mathbb{Z}$)	在 $\mathbb{Z}[i]$ 中的分解	几何意义
分歧 (Ramified)	$p = 2$	$2 = -i(1+i)^2$	模长平方为 2
惰性 (Inert)	$p \equiv 3 \pmod{4}$	保持不可约 (如 3, 7, 11)	在轴上
分裂 (Split)	$p \equiv 1 \pmod{4}$	$p = \pi\bar{\pi}$ (如 $5 = (1+2i)(1-2i)$)	非轴上格点

14.2 费马平方和定理

定理 14.2. 设 p 是奇素数。 $p = x^2 + y^2 \iff p \equiv 1 \pmod{4}$ 。

必要性证明 (\Rightarrow). 若 $p = x^2 + y^2$, 考察模 4 的余数。整数的平方模 4 只能余 0 或 1。因此 $x^2 + y^2 \pmod{4}$ 只能是 0, 1, 2。因为 p 是奇数, 排除 0 和 2。且 p 不能余 3, 故只能 $p \equiv 1 \pmod{4}$ 。 \square

充分性证明 (\Leftarrow). 若 $p \equiv 1 \pmod{4}$, 我们需要构造 x, y 。

1. 因为 $p \equiv 1 \pmod{4}$, 由数论性质知 -1 是模 p 的二次剩余。即存在 $n \in \mathbb{Z}$ 使得 $p \mid (n^2 + 1)$ 。
2. 在 $\mathbb{Z}[i]$ 中分解: $p \mid (n+i)(n-i)$ 。
3. 假设 p 在 $\mathbb{Z}[i]$ 中是不可约元 (即素元)。则 $p \mid (n+i)$ 或 $p \mid (n-i)$ 。
4. 但 $\frac{n+i}{p} = \frac{n}{p} \pm \frac{1}{p}i \notin \mathbb{Z}[i]$, 因为虚部 $1/p$ 不是整数。
5. 产生矛盾, 说明 p 在 $\mathbb{Z}[i]$ 中可约。设 $p = \alpha\beta$ (α, β 非单位)。
6. 取范数: $N(p) = p^2 = N(\alpha)N(\beta)$ 。
7. 唯一的非平凡解是 $N(\alpha) = p$ 。设 $\alpha = x + yi$, 则 $x^2 + y^2 = p$ 。

□

注意 (NOTE): 费马平方和定理的应用

素数 p 可以写成两个整数的平方和 $p = x^2 + y^2$, 当且仅当 p 在 $\mathbb{Z}[i]$ 中可约 (分裂), 即 $p \equiv 1 \pmod{4}$ (或 $p = 2$)。

14.3 2. Eisenstein 整数 (Legendre 整数)

笔记 P16 提到了 $\mathbb{Z}[\omega]$, 其中 $\omega = \frac{-1+\sqrt{-3}}{2}$ 。

- 这是 $d = -3$ 的二次整数环。
- 它也是 ED (欧氏环), 因此是 UFD。
- 几何上对应复平面上的正三角形 (六边形) 格点。

14.4 3. 非 UFD 的反例

考察 $R = \mathbb{Z}[\sqrt{-5}]$ 。

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

这里 $2, 3, 1 \pm \sqrt{-5}$ 都是不可约元, 但它们互不相伴。这破坏了分解的唯一性, 因此 $\mathbb{Z}[\sqrt{-5}]$ 不是 UFD, 当然也不是 PID 或 ED。

四、UFD 的判别准则

根据笔记 P12, 我们有一个判断 UFD 的实用命题:

命题 14.3. 设 R 是整环, 则 R 是 UFD 当且仅当满足以下两个条件:

1. **可分解性:** 任何非零非单位元素可写成不可约元的乘积。
2. **素性条件:** 不可约元是素元。

这个命题再次强调了“不可约元 \iff 素元”对于唯一分解性质的重要性。

15 唯一分解整环 (UFD) 上的多项式环

15.1 基本设定与 Gauss 引理

设定：设 R 是唯一分解整环 (UFD)， K 是 R 的商域 (Field of Fractions)。

定义 15.1 (内容与本原多项式). 对于非零多项式 $f(x) \in R[x]$, 定义 f 的内容 (*Content*) $C(f)$ 为 f 所有系数的最大公约数 (在相伴意义下唯一)。若 $C(f) \sim 1$ (即单位元), 则称 $f(x)$ 为本原多项式 (*Primitive Polynomial*)。

引理 15.2 (Gauss 引理). 设 $f, g \in R[x]$ 。则：

$$C(fg) \sim C(f)C(g)$$

特别地，两个本原多项式的乘积依然是本原多项式。

证明. 只需证明：若 f, g 是本原多项式，则 fg 也是本原多项式。使用反证法与模理想的方法：

1. 假设 fg 不是本原的，则存在 R 中的素元 p 使得 $p \mid C(fg)$ ，即 p 整除 fg 的所有系数。
2. 考虑商环 $k = R/(p)$ 。因为 p 是素元且 R 是 UFD，故 (p) 是素理想，从而 k 是整环。
3. 考虑自然同态 $\phi : R[x] \rightarrow k[x]$ ，记 $\phi(h) = \bar{h}$ 。
4. 因为 f, g 是本原的， p 不能整除它们的所有系数，故 $\bar{f} \neq 0$ 且 $\bar{g} \neq 0$ 。
5. 因为 k 是整环，故多项式环 $k[x]$ 也是整环。因此 $\overline{fg} = \bar{f}\bar{g} \neq 0$ 。
6. 这意味着 p 不能整除 fg 的所有系数，即 fg 是本原的。矛盾。

□

15.2 详细证明补充

命题 15.3 (整除关系的下降). 设 R 是 UFD， K 是其商域。设 $f, g \in R[x]$ ，且 g 是本原多项式。若 $g \mid f$ 在 $K[x]$ 中成立，则 $g \mid f$ 在 $R[x]$ 中也成立。

证明. 假设在 $K[x]$ 中有 $f(x) = g(x)h(x)$, 其中 $h(x) \in K[x]$ 。由于 $h(x) \in K[x]$, 我们可以将其系数的分母提取出来, 写成 $h(x) = \frac{1}{d}h_0(x)$, 其中 $d \in R$, $h_0(x) \in R[x]$ 且 h_0 是本原多项式 (提取出分子所有公因子后的结果)。于是方程变为:

$$d \cdot f(x) = g(x) \cdot h_0(x)$$

两边取内容 (Content)。根据 Gauss 引理, 本原多项式的乘积仍为本原多项式, 即 $C(g \cdot h_0) \sim C(g)C(h_0) \sim 1 \cdot 1 \sim 1$ 。因此, 上式两边的内容满足:

$$C(d \cdot f) \sim d \cdot C(f) \sim C(g \cdot h_0) \sim 1$$

这意味着 d 必须整除 $C(f)$ (在相伴意义下)。既然 $d \mid C(f)$, 而 $C(f)$ 是 f 系数的公因子, 这意味着 d 整除 $f(x)$ 的每一个系数。因此, $\frac{f(x)}{d}$ 仍然是一个整系数多项式, 即 $\frac{f(x)}{d} \in R[x]$ 。回到方程 $f(x) = g(x) \cdot \frac{h_0(x)}{d}$ 。故 $f(x) = g(x)h(x)$ 且 $h(x) \in R[x]$, 即 $g \mid f$ 在 $R[x]$ 中成立。 \square

定理 15.4. 若 R 是 UFD, 则 $R[x]$ 也是 UFD。

证明. 我们需要证明 $R[x]$ 中的元素既存在分解, 且分解在相伴意义下唯一。

1. 存在性 (Existence): 设 $f \in R[x]$ 为非零非单位元。对 $\deg(f)$ 归纳:

- 若 $\deg(f) = 0$, 则 $f \in R$ 。因 R 是 UFD, 故 f 可分解为 R 中不可约元的乘积。 R 中不可约元在 $R[x]$ 中仍不可约, 故得证。
- 若 $\deg(f) > 0$, 将 f 视为 $K[x]$ 中元素。因 $K[x]$ 是 PID (欧几里得整环), 故 $f = F_1 \cdots F_k$, 其中 $F_i \in K[x]$ 不可约。写成 $F_i = \frac{a_i}{b_i}g_i$, 其中 $g_i \in R[x]$ 本原。于是 $f = (\prod \frac{a_i}{b_i})g_1 \cdots g_k = \lambda g_1 \cdots g_k$ ($\lambda \in K$)。写成 $\lambda = \frac{u}{v}$ ($u, v \in R$), 则 $vf = ug_1 \cdots g_k$ 。取内容: $vC(f) = uC(g_1 \cdots g_k) = u$ (因 g_i 本原, 由 Gauss 引理积也本原)。故 $\lambda = \frac{u}{v} = C(f) \in R$ 。 $C(f)$ 在 R 中可分解为不可约元 (即 $R[x]$ 的常数不可约元), g_i 是本原且在 $K[x]$ 中不可约 (相伴于 F_i), 故 g_i 在 $R[x]$ 中也不可约。因此 f 获得了分解。

2. 唯一性 (Uniqueness): 设 f 有两种分解:

$$f = p_1 \cdots p_m q_1 \cdots q_r = p'_1 \cdots p'_n q'_1 \cdots q'_s$$

其中 p_i, p'_j 是 R 中的不可约元 (常数), q_i, q'_j 是 $R[x]$ 中的正次本原不可约多项式。

步骤一: 比较内容两边取内容。由于 q_i, q'_j 均为本原多项式, 其乘积的内容为 1 (单位元)。故 $C(f) \sim p_1 \cdots p_m \sim p'_1 \cdots p'_n$ 。因 R 是 UFD, 常数部分的分解是唯一的。故 $m = n$, 且适当重排后 $p_i \sim p'_i$ 。

步骤二：比较本原部分消去常数因子后，剩下 $q_1 \cdots q_r \sim q'_1 \cdots q'_s$ 。将这些多项式视为 $K[x]$ 中的元素。它们在 $R[x]$ 中本原且不可约 \Rightarrow 在 $K[x]$ 中不可约。因 $K[x]$ 是 ED（可进行带余除法），故 $r = s$ ，且适当重排后 q_i 与 q'_i 在 $K[x]$ 中相伴。即 $q_i = \frac{a}{b}q'_i$ ($a, b \in R$)。整理得 $bq_i = aq'_i$ 。取内容得 $bC(q_i) = aC(q'_i)$ 。因 q_i, q'_i 本原， $C(q_i), C(q'_i)$ 为单位元，故 $a \sim b$ ，即 $\frac{a}{b}$ 是 R 中的单位元。所以 q_i 与 q'_i 在 $R[x]$ 中也是相伴的。

综上，分解是唯一的。 \square

推论 15.5. 若 R 是 UFD，则 $\mathbb{Z}[x_1, \dots, x_n]$ 是 UFD。

证明. 由归纳法证明。

- $n = 1$ 时， \mathbb{Z} 是欧几里得整环 \Rightarrow PID \Rightarrow UFD。由上述定理， $\mathbb{Z}[x_1]$ 是 UFD。
- 假设 $n = k$ 时 $\mathbb{Z}[x_1, \dots, x_k]$ 是 UFD。
- 当 $n = k + 1$ 时，视为单变元多项式环：

$$\mathbb{Z}[x_1, \dots, x_{k+1}] \cong (\mathbb{Z}[x_1, \dots, x_k])[x_{k+1}]$$

令 $R' = \mathbb{Z}[x_1, \dots, x_k]$ 。由归纳假设 R' 是 UFD。再次应用上述定理， $R'[x_{k+1}]$ 也是 UFD。

故对任意 n ， $\mathbb{Z}[x_1, \dots, x_n]$ 均为唯一分解整环。 \square

16 不可约元与素元

16.1 不可约性的判定

在 $R[x]$ 中判断一个多项式是否不可约，可以转化为 $K[x]$ 上的判定。

证明. 设 K 是 R 的商域。我们分两种情况讨论 $f \in R[x]$ 的次数。

情形 1: $\deg(f) = 0$ (即 $f \in R$)

在这种情况下， f 作为 $R[x]$ 的元素和作为 R 的元素是完全一样的。

- (\Rightarrow) 若 f 在 $R[x]$ 中不可约，则 f 不能写成两个非单位多项式的乘积。特别地，它不能写成 R 中两个非单位元的乘积。故 f 在 R 中不可约。

- (\Leftarrow) 若 f 在 R 中不可约。假设 $f = g(x)h(x)$ 在 $R[x]$ 中分解。因为 $\deg(f) = 0$, 且 R 是整环, 所以 $\deg(g) + \deg(h) = 0$, 这意味着 $g, h \in R$ 。因为 f 在 R 中不可约, 所以 g 或 h 必有一个是 R 中的单位元, 也就是 $R[x]$ 中的单位元。故 f 在 $R[x]$ 中不可约。

情形 2: $\deg(f) > 0$

方向一 (\Leftarrow): 假设 f 是本原多项式, 且在 $K[x]$ 中不可约。我们证明 f 在 $R[x]$ 中不可约。使用反证法: 假设 f 在 $R[x]$ 中可约, 即 $f = g \cdot h$, 其中 $g, h \in R[x]$ 且都不是单位元。

1. 若 $\deg(g) = 0$ (即 $g \in R$)。因为 $g | f$ 且 f 是本原多项式, 常数因子 g 必须整除 f 的所有系数的最大公约数 (即 1)。这意味着 g 是 R 中的可逆元 (单位元)。这与假设矛盾。
2. 若 $\deg(g) \geq 1$ 且 $\deg(h) \geq 1$ 。那么 $f = g \cdot h$ 也是在 $K[x]$ 中的分解。因为 g, h 的次数都大于 0, 它们在 $K[x]$ 中都不是单位元。这与 “ f 在 $K[x]$ 中不可约” 矛盾。

综上, f 在 $R[x]$ 中必须不可约。

方向二 (\Rightarrow): 假设 f 在 $R[x]$ 中不可约。

1. **先证本原性:** 假设 f 不是本原的, 则 f 的系数有非单位公因子 $c \in R$ 。即 $f = c \cdot f_0$, 其中 $f_0 \in R[x]$ 。因为 $\deg(f) > 0$, 所以 f_0 不是单位元; 因 c 不是单位元, 这是一个 $R[x]$ 中的非平凡分解, 与 f 不可约矛盾。故 f 必为本原多项式。
2. **再证在 $K[x]$ 中不可约:** 使用反证法: 假设 f 在 $K[x]$ 中可约。即 $f = G \cdot H$, 其中 $G, H \in K[x]$ 且 $\deg(G), \deg(H) \geq 1$ 。我们可以通过提取分母和内容, 将 G, H 转化为 $R[x]$ 上的本原多项式:

$$G = \frac{a}{b}g_0, \quad H = \frac{c}{d}h_0$$

其中 $a, b, c, d \in R$, 且 $g_0, h_0 \in R[x]$ 是本原多项式。代回原式:

$$f = \frac{ac}{bd}g_0h_0 \implies bd \cdot f = ac \cdot g_0h_0$$

两边取内容 (Content)。由 Gauss 引理, 本原多项式的积仍为本原, 即 $C(g_0h_0) \sim 1$ 。又因为 f 是本原的, $C(f) \sim 1$ 。

$$bd \cdot C(f) \sim ac \cdot C(g_0h_0) \implies bd \sim ac$$

这意味着 $\frac{ac}{bd}$ 是 R 中的单位元 u 。于是 $f = u \cdot g_0 \cdot h_0$ 。因为 $\deg(g_0) = \deg(G) \geq 1$ 且 $\deg(h_0) = \deg(H) \geq 1$, 且 u 是单位元, 这表明 f 在 $R[x]$ 中分解成了两个非单位多项式的乘积。这与 “ f 在 $R[x]$ 中不可约” 矛盾。

故 f 在 $K[x]$ 中不可约。 \square

16.2 不可约元与素元的等价性

在一般的整环中, 素元 \Rightarrow 不可约元, 反之不一定成立。但在 UFD 中两者等价。以下是在 $R[x]$ 中的具体证明路径。

命题 16.1. 在 $R[x]$ (UFD) 中, 不可约元一定是素元。

证明. 设 $g \in R[x]$ 不可约, 且 $g \mid f_1 f_2$ 。

1. 下沉到 $K[x]$: 由前述定理, g 在 $K[x]$ 中不可约, 且 $C(g) = 1$ 。
2. 利用 PID 性质: $K[x]$ 是 PID, 其中不可约元即素元。因 $g \mid f_1 f_2$ 在 $K[x]$ 成立, 故 $g \mid f_1$ 或 $g \mid f_2$ 在 $K[x]$ 中成立。不妨设 $g \mid f_1$ 。
3. 回升到 $R[x]$: 因为 g 是本原的, 且 $g \mid f_1$ 在 $K[x]$ 中, 由 Gauss 引理推论, 可知 $g \mid f_1$ 在 $R[x]$ 中成立。
4. 结论: g 是素元。

\square

注 (更广泛的代数视角). 上述证明利用了多项式环的特殊结构 (Gauss 引理)。事实上, 我们可以给出一个纯粹基于 UFD 定义的通用证明, 适用于任何唯一分解整环, 而不仅仅是 $R[x]$ 。

定理 16.2 (UFD 中不可约元即素元). 设 D 是一个唯一分解整环 (UFD)。若 $p \in D$ 是不可约元, 则 p 是素元。

证明. 设 p 是 D 中的不可约元, 且 $p \mid ab$ ($a, b \in D$)。我们需要证明 $p \mid a$ 或 $p \mid b$ 。

由整除定义, 存在 $k \in D$ 使得 $ab = pk$ 。

由于 D 是 UFD, 我们将 a, b, k 分解为不可约元素的乘积:

$$a = u \cdot \pi_1 \cdots \pi_m, \quad b = v \cdot \rho_1 \cdots \rho_n, \quad k = w \cdot \sigma_1 \cdots \sigma_t$$

其中 u, v, w 是单位元, π_i, ρ_j, σ_l 均为不可约元。

代入方程 $ab = pk$, 我们得到两个分解式:

$$(uv) \cdot \pi_1 \cdots \pi_m \cdot \rho_1 \cdots \rho_n = w \cdot p \cdot \sigma_1 \cdots \sigma_t$$

方程左边是 ab 的不可约分解，右边也是 ab 的不可约分解。根据 UFD 的 **唯一性** 定义（分解在相伴意义下唯一）：右边的不可约因子 p 必须与左边的某一个不可约因子相伴 (Associate)。

- **情形 1：**若 p 与某个 π_i 相伴。即 $p \sim \pi_i$ ，这意味着 $p \mid \pi_i$ 。因为 π_i 是 a 的因子 ($\pi_i \mid a$)，所以 $p \mid a$ 。
- **情形 2：**若 p 与某个 ρ_j 相伴。即 $p \sim \rho_j$ ，这意味着 $p \mid \rho_j$ 。因为 ρ_j 是 b 的因子 ($\rho_j \mid b$)，所以 $p \mid b$ 。

综上所述，必有 $p \mid a$ 或 $p \mid b$ 。因此 p 是素元。 \square

17 模 n 整数环的单位群

17.1 基本定义与结构

定义 17.1 (单位群). 环 R 的单位群定义为 $U(R) = R^\times = \{a \in R \mid \exists b \in R, ab = 1\}$ 。对于 $R = \mathbb{Z}/n\mathbb{Z}$, 有:

$$U(\mathbb{Z}/n\mathbb{Z}) = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a, n) = 1\}$$

群的阶为欧拉函数 $\phi(n)$ 。

定理 17.2 (基于 CRT 的分解). 设 n 的素因子分解为 $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ 。由中国剩余定理 (CRT)，有环同构 $\mathbb{Z}/n\mathbb{Z} \cong \prod \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ 。限制在单位群上，有群同构：

$$U(\mathbb{Z}/n\mathbb{Z}) \cong U(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times \cdots \times U(\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})$$

证明. 证明分为两步：首先回顾 CRT 建立的环同构，然后证明该同构限制在单位群上后，结构依然保持。

第一步：建立环同构 设 $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ 。由于 $p_i^{\alpha_i}$ 两两互素，根据中国剩余定理 (CRT)，存在如下的环同构映射：

$$\psi : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}$$

该映射定义为 $\psi(x \bmod n) = (x \bmod p_1^{\alpha_1}, \dots, x \bmod p_r^{\alpha_r})$ 。因为 ψ 是环同构，它是一个双射，且保持加法和乘法运算，即 $\psi(xy) = \psi(x)\psi(y)$ 和 $\psi(1) = (1, \dots, 1)$ 。

第二步：限制在单位群上 我们需要证明：一个元素 x 在 $\mathbb{Z}/n\mathbb{Z}$ 中可逆，当且仅当其像 $\psi(x)$ 在右侧的直积环中可逆。

1. 直积环的可逆元结构: 考察直积环 $R = R_1 \times \cdots \times R_r$ 。其中的乘法是分量逐点运算。设 $a = (a_1, \dots, a_r) \in R$ 。 a 是可逆元当且仅当存在 $b = (b_1, \dots, b_r)$ 使得 $ab = 1_R = (1, \dots, 1)$ 。

$$(a_1 b_1, \dots, a_r b_r) = (1, \dots, 1) \iff a_i b_i = 1 \text{ 在 } R_i \text{ 中对于所有 } i \text{ 成立}$$

这意味着, a 是 R 的单位元当且仅当每一个分量 a_i 都是 R_i 的单位元。因此, 直积环的单位群同构于各分量环单位群的直积:

$$U(R_1 \times \cdots \times R_r) \cong U(R_1) \times \cdots \times U(R_r)$$

2. 映射的限制: 对于任意 $x \in \mathbb{Z}/n\mathbb{Z}$:

$$\begin{aligned} x \in U(\mathbb{Z}/n\mathbb{Z}) &\iff \gcd(x, n) = 1 \quad (\text{单位群定义}) \\ &\iff \gcd(x, \prod p_i^{\alpha_i}) = 1 \\ &\iff \forall i, \gcd(x, p_i^{\alpha_i}) = 1 \quad (\text{与积互素等价于与每个因子互素}) \\ &\iff \forall i, (x \bmod p_i^{\alpha_i}) \in U(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}) \end{aligned}$$

这说明环同构 ψ 将左边的单位元集合精确地映射到了右边直积环的单位元集合。

结论: 由于 ψ 是环同构, 它限制在乘法单位群上必然诱导出一个群同构:

$$U(\mathbb{Z}/n\mathbb{Z}) \xrightarrow{\cong} U(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}) \cong \prod_{i=1}^r U(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})$$

□

17.2 素数幂模的群结构

根据 p 的奇偶性, 结构有所不同。

- 情形 1: p 为奇素数

$$U(\mathbb{Z}/p^r\mathbb{Z}) \cong C_{p^{r-1}(p-1)}$$

这是一个循环群, 存在原根。

- 情形 2: $p = 2$

- $r = 1 \implies U(\mathbb{Z}/2\mathbb{Z}) \cong \{1\}$ (平凡群)。
- $r = 2 \implies U(\mathbb{Z}/4\mathbb{Z}) \cong C_2$ 。
- $r \geq 3 \implies U(\mathbb{Z}/2^r\mathbb{Z}) \cong C_2 \times C_{2^{r-2}}$ 。

17.3 $n = 2^r (r \geq 3)$ 无原根的证明

当 $r \geq 3$ 时, 单位群并非循环群。

结构证明. 群的阶为 $\phi(2^r) = 2^{r-1}$ 。

1. 考察元素 5 的阶: 利用归纳法可证 $5^{2^{r-3}} \equiv 1 + 2^{r-1} \not\equiv 1 \pmod{2^r}$, 且 $5^{2^{r-2}} \equiv 1 \pmod{2^r}$ 。故 5 生成一个阶为 2^{r-2} 的子群 $\langle 5 \rangle$ 。
2. 考察元素 -1: 显然 $-1 \notin \langle 5 \rangle$ (因为 $5^k \equiv 1 \pmod{4}$ 而 $-1 \equiv 3 \pmod{4}$)。
3. 结论: $U(\mathbb{Z}/2^r\mathbb{Z})$ 由 $\langle -1 \rangle \cong C_2$ 和 $\langle 5 \rangle \cong C_{2^{r-2}}$ 直积而成。所有元素的最高阶为 $\text{lcm}(2, 2^{r-2}) = 2^{r-2} < \phi(2^r)$, 故无生成元。

□

推论 17.3 (原根存在性定理). 模 n 存在原根 (即 $U(\mathbb{Z}/n\mathbb{Z})$ 是循环群) 当且仅当 n 为以下形式之一:

$$2, 4, p^r, 2p^r \quad (p \text{ 为奇素数})$$