代数学笔记 Chapter 5：环论基础 (Ring Theory)

整理自课堂笔记

2025 年 12 月 8 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 $\to$ 商环 $\to$ 同态基本定理 $\to$ 结构分解 (CRT)。

目录

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 $\phi : R \to R'$ 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 $\pi : R \to R/I$，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

证明. 我们要寻找（构造）一个映射 $\bar{\phi} : R/K \to S$，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 $S=\operatorname{Im}\phi$ 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 3.1 (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。
$$\mathbb{Q}[T] = \{a_nT^n + \cdots + a_1T + a_0 \mid a_i \in \mathbb{Q}, n \in \mathbb{N}\}$$
- $f(T)$ ***(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”：

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

- $\mathbb{Q}(\alpha)$ *(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：** $R/\ker\phi \cong Im\ \phi$。
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 $R_1, \ldots, R_n$ 为环。它们的直积定义为：

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

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 $I_1, \ldots, I_n$ 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 $\Phi : R \to \prod_{i=1}^{n} R/I_i$ 是满射。即：对于任意的目标向量 $(y_1, y_2, \ldots, y_n) \in \prod R/I_i$，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 $I_1, \ldots, I_n$ 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：

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

第二步：构造“指示元素” e_k

我们的目标是构造一组元素 $e_1, \ldots, e_n$，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：

$$e_k \equiv \delta_{km} = \begin{cases} 1 \pmod{I_m} & 若 k = m \\ 0 \pmod{I_m} & 若 k \neq m \end{cases}$$

第三步：构造最终解 x

令 x 为如下线性组合：

$$x = y_1e_1 + y_2e_2 + \cdots + y_ne_n = \sum_{i=1}^{n} y_ie_i$$

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：

$$\begin{aligned} x \pmod{I_k} &\equiv \sum_{i=1}^{n} y_ie_i \pmod{I_k} \\ &\equiv y_1e_1 + \cdots + y_ke_k + \cdots + y_ne_n \pmod{I_k} \end{aligned}$$

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：

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

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 $n_1, n_2, \ldots, n_k$ 是两两互质的正整数（即 $\gcd(n_i, n_j) = 1, \forall i \neq j$）。令 $N = n_1 n_2 \ldots n_k$。

对于任意给定的整数 $a_1, a_2, \ldots, a_k$，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 $\operatorname{lcm}(n_1, \ldots, n_k)\mathbb{Z} = N\mathbb{Z}$
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 $(a_1, \ldots, a_k)$，其中 $a_i \in \mathbb{Z}_{n_i}$

逻辑推导：

1. **同构即双射：**环论形式的 CRT 告诉我们存在同构：

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

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

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 $(a_1, \ldots, a_k)$（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。 $\Longrightarrow$ **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 $x = y$。 $\Longrightarrow$ **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 $x \mapsto (x \bmod n_1, \ldots)$ 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)	素理想 (Prime Ideal)
定义： I 是真理想，且不存在理想 J 使得 $I \subsetneq J \subsetneq R$。	**定义：** 若 $ab \in I \implies a \in I$ 或 $b \in I$。
判别法： I 是极大理想 $\iff$ R/I 是**域**。	**判别法：** I 是素理想 $\iff$ 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：

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

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。

(⇒) **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 $\overline{ab} = \bar{0}$，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：

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

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。 □

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。 □

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 $\varphi : R/I \to R/J$，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 $R/I/\ker\varphi \cong \operatorname{Im}\varphi$，即得：

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

□

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

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

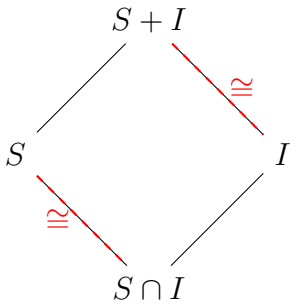
即 $\mathbb{Z}_{12}$ 模掉其子群 $\{\bar{0}, \bar{4}, \bar{8}\}$ 同构于 $\mathbb{Z}_4$。

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：
右侧商环 $(S + I)/I$
同构于
左侧商环 $S/(S \cap I)$

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 $\phi : S \to (S + I)/I$，规则为：

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

   这本质上是自然同态 $\pi : R \to R/I$ 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 $S/\ker\phi \cong \operatorname{Im}\phi$，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 $\phi_0 : R \to S$（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 $\Phi : R[x] \to S$ 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：

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

10.2.1 符号含义

- $\mathrm{Hom}_{\mathrm{Ring}}(A, B)$：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** $\mathrm{Hom}(R[x], S)$：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** $\mathrm{Hom}(R, S) \times S$：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 $\Phi : R[x] \to S$。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 $R[x_1, \ldots, x_n]$，双射关系推广为：

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

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 $(\alpha_1, \ldots, \alpha_n)$。

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 $I = (g(x))$。 □

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）：

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

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。 □