

A Concrete Introduction to Number Theory and Algebra—环与域

Libin Wang

School of Computer Science, South China Normal University

April 19, 2021

Table of contents

1 Ring (环)

2 Field (域)

Ring (环)

Definition

环 R 是一个非空集合，在 R 上有两种封闭的二元操作：加法（记为 $+: R \times R \mapsto R$ ）和乘法（记为 $*: R \times R \mapsto R$ ），并且满足以下条件：

- 1 在加法 (+) 上 R 是一个阿贝尔群，加法的单位元记为 0 ，加法上的逆元记为 $-a$ ；
- 2 R 在乘法 (*) 上满足结合律；
- 3 乘法在加法上满足分配律。

Ring (环) .

具体地表示为公式, 对任意 $a, b, c \in R$, 环 R 满足以下公理:

$$a + (b + c) = (a + b) + c \quad (+ \text{ 的结合律}) \quad (1)$$

$$a + b = b + a \quad (+ \text{ 的交换律}) \quad (2)$$

$$a + 0 = 0 + a \quad (+ \text{ 的单位元}) \quad (3)$$

$$a + (-a) = (-a) + a = 0 \quad (+ \text{ 的逆元}) \quad (4)$$

$$a * (b * c) = (a * b) * c \quad (* \text{ 的结合律}) \quad (5)$$

$$a * 1 = 1 * a = a \quad (* \text{ 的单位元}) \quad (6)$$

$$(a + b) * c = (a * c) + (b * c) \quad (\text{右分配律}) \quad (7)$$

$$a * (b + c) = (a * b) + (a * c) \quad (\text{左分配律}) \quad (8)$$

Ring (环) .

Definition

- 如果 R 在乘法上也满足交换律, 则称 R 为交换环, 否则称为非交换环。
- 如果 R 在乘法上具有单位元, 则称环 R 为带单位元的环。

Ring 实例.

Example

- ① $R = \{0\}$ 是只有一个元素的最小环，称为平凡环或零环。如果一个环中， $1 \neq 0$ ，则这个环是非平凡环。一个最小的非平凡环就是 $R = \{0, 1\}$ ，或者记为 \mathbb{Z}_2 。

Ring 实例.

Example

- ① $R = \{0\}$ 是只有一个元素的最小环，称为平凡环或零环。如果一个环中， $1 \neq 0$ ，则这个环是非平凡环。一个最小的非平凡环就是 $R = \{0, 1\}$ ，或者记为 \mathbb{Z}_2 。
- ② 在普通意义的加法和乘法上，容易验证 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 都是交换环。

Ring 实例.

Example

- ① $R = \{0\}$ 是只有一个元素的最小环，称为平凡环或零环。如果一个环中， $1 \neq 0$ ，则这个环是非平凡环。一个最小的非平凡环就是 $R = \{0, 1\}$ ，或者记为 \mathbb{Z}_2 。
- ② 在普通意义的加法和乘法上，容易验证 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 都是交换环。
- ③ 整数中所有的偶数在一般的加法与乘法上形成环，同样记为 $2\mathbb{Z}$ ，这是一个不带单位元的环。更一般地，对任意整数 $n \in \mathbb{Z}$ ， $n\mathbb{Z}$ 在一般的加法与乘法上形成环。

Ring 实例.

Example

- ① $R = \{0\}$ 是只有一个元素的最小环，称为平凡环或零环。如果一个环中， $1 \neq 0$ ，则这个环是非平凡环。一个最小的非平凡环就是 $R = \{0, 1\}$ ，或者记为 \mathbb{Z}_2 。
- ② 在普通意义的加法和乘法上，容易验证 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 都是交换环。
- ③ 整数中所有的偶数在一般的加法与乘法上形成环，同样记为 $2\mathbb{Z}$ ，这是一个不带单位元的环。更一般地，对任意整数 $n \in \mathbb{Z}$ ， $n\mathbb{Z}$ 在一般的加法与乘法上形成环。
- ④ 对任意正整数 $n \in \mathbb{N}$ ， \mathbb{Z}_n 是模 n 的加法群。如果给加法群 \mathbb{Z}_n 配置上乘法 $*$ ，乘法 $*$ 被定义为整数上的模 n 乘法，即 $\forall a, b \in \mathbb{Z}_n$ ， $a * b \triangleq ab \bmod n$ 。容易验证 \mathbb{Z}_n 是一个交换环。

Ring 实例.

Example

- ① 取 p 为任意素数, \mathbb{Z}_p 在模 p 的加法与模 p 的乘法下成环, 而且 \mathbb{Z}_p 的所有非零元素在乘法上都有逆元。以后我们将重点讨论这种特殊的环。

Ring 实例.

Example

- ① 取 p 为任意素数, \mathbb{Z}_p 在模 p 的加法与模 p 的乘法下成环, 而且 \mathbb{Z}_p 的所有非零元素在乘法上都有逆元。以后我们将重点讨论这种特殊的环。
- ② 对任意环 R , R 的直积 $R \times R$ 形成环, 环的加法与乘法定义为 $\forall (a, b), (c, d) \in R \times R$ 序对, $(a, b) + (c, d) \triangleq (a + c, b + d)$ 和 $(a, b)(c, d) \triangleq (ac, bd)$ 。

Ring 实例.

Example

- ① 取 p 为任意素数, \mathbb{Z}_p 在模 p 的加法与模 p 的乘法下成环, 而且 \mathbb{Z}_p 的所有非零元素在乘法上都有逆元。以后我们将重点讨论这种特殊的环。
- ② 对任意环 R , R 的直积 $R \times R$ 形成环, 环的加法与乘法定义为 $\forall (a, b), (c, d) \in R \times R$ 序对, $(a, b) + (c, d) \triangleq (a + c, b + d)$ 和 $(a, b)(c, d) \triangleq (ac, bd)$ 。
- ③ 实数上的 $n \times n$ 矩阵在普通的矩阵加法和矩阵乘法上形成环, 也称为矩阵环, 记为 $M_n(\mathbb{R})$ 。这是一种非交换环。

Ring 的属性.

Proposition

设 R 是一个环, 且 $a, b \in R$, 则有:

- ① $a0 = 0a = 0$
- ② $a(-b) = (-a)b = -ab$
- ③ $(-a)(-b) = ab$

Ring 的属性.

Proof.

根据分配律,

$$a0 = a(0 + 0) = a0 + a0$$

则 $a0 = 0$, 同理 $0a = 0$ 。同样根据分配律

$$ab + a(-b) = a(b + (-b)) = a0 = 0$$

所以, $-(ab) = a(-b)$, 同理 $-(ab) = (-a)b$ 。最后, 根据以上结论, $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$ 。 □

整环 (Integral Domain.)

Definition

给定一个环 R ，对任意元素 $a \in R$ ，如果存在元素 $b \in R$ 使得 $b \neq 0$ 且 $a * b = 0$ ，则称 a 为一个零因子 (zero divisor)。如果交换环 R 中没有除 0 以外的零因子，即 $\forall a, b \in R$ ，如果 $ab = 0$ 则有 $a = 0$ 或 $b = 0$ ，则称 R 为整环。

整环实例

Example

- ① 在普通意义的加法和乘法上, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 都是整环。比如, 考虑 $a, b \in \mathbb{Z}$, $ab = 0$ 当且仅当 $a = 0$ 或者 $b = 0$ 。其他实例, 验证类似。
- ② 可验证偶数环 $2\mathbb{Z}$ 是整环。更一般地, 对任意的 $n \in \mathbb{Z}$, $n\mathbb{Z}$ 都是整环。
- ③ 已知 \mathbb{Z}_n 是一个交换环。但是, \mathbb{Z}_n 并不是整环。比如, \mathbb{Z}_{15} 中, $(3 * 5) \bmod 15 = 0$, 3 和 5 都是 \mathbb{Z}_{15} 中的零因子。
- ④ 矩阵环 $M_n(\mathbb{R})$ 不是整环, 因为存在 $A, B \in M_n(\mathbb{R})$, 使得 $AB = 0$ 但是 A 和 B 都不为 0。

整环属性

Proposition

设 D 是一个交换环, D 是整环当且仅当对任意元素 $a, b, c \in D$, 且 $a \neq 0$, 若 $ab = ac$, 则 $b = c$ 。

整环属性

Proof.

- ① 充分性. D 是整环, 则 D 中无零因子。若 $a \neq 0$ 且 $ab = ac$, 则 $a(b - c) = 0$, 则 $b - c = 0$, 即 $b = c$ 。
- ② 必要性. 假设 D 中消去律成立, 即若 $ab = ac$, 则 $b = c$ 。设 $ab = 0$, 有 $ab = a0$ 。如果 $a \neq 0$, 根据消去律, 得到 $b = 0$ 。因此, a 不可能是零因子。



子环 (Subring)

Definition

给定环 R , R' 是 R 的子集, 如果 R' 在环 R 的加法和乘法上也形成环, 则称 R' 是 R 的子环, 记为 $R' \subset R$ 。

子环实例

Example

- ① 容易验证以下子环序列: $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ 。
- ② 偶数环是整数环的子环, 即 $2\mathbb{Z} \subset \mathbb{Z}$ 。由此可知, 子环并不自然继承母环的单位元。当然, 对任意的 $n \in \mathbb{Z}$, 有 $n\mathbb{Z} \subset \mathbb{Z}$ 。

子环属性

Proposition

给定环 R , R' 是 R 的子集。 R' 是 R 的子环, 当且仅当以下条件满足:

- ① $R' \neq \emptyset$;
- ② $\forall a, b \in R'$, 有 $ab \in R'$;
- ③ $\forall a, b \in R'$, 有 $a - b \in R'$ 。

Proof.

根据子群命题易得, 留作课后练习。



环同态与环同构

Definition

给定两个环 R 和 R' , 若映射 $\phi: R \mapsto R'$ 满足: $\forall a, b \in R$,

$$\phi(a + b) = \phi(a) + \phi(b)$$

$$\phi(ab) = \phi(a)\phi(b)$$

则称 ϕ 为一个环同态。如果 ϕ 是一个双射, 则 ϕ 是一个环同构。
环同态 ϕ 的 Kernel 定义为以下集合:

$$\text{Ker } \phi = \{r \in R : \phi(r) = 0\}.$$

环同态的性质

Proposition

设映射 $\phi: R \mapsto R'$ 是环同态, 则:

- ① 如果 R 是交换环, 则 $\phi(R)$ 也是交换环。
- ② 分别记 0 和 $0'$ 是 R 和 R' 的加法单位元, $\phi(0) = 0'$ 。
- ③ 分别记 1 和 $1'$ 是 R 和 R' 的乘法单位元, 如果 ϕ 是满射, 则 $\phi(1) = 1'$ 。

环同态实例-1

Example

请验证以下同态实例，体会环同态与群同态的异同点。

- ① 已知 \mathbb{Z} 是环，定义映射 $\phi: \mathbb{Z} \mapsto \mathbb{Z}$ 为 $\phi(k) = 2k, \forall k \in \mathbb{Z}$ ，即把所有整数映射到偶数 $2\mathbb{Z}$ 。已知 ϕ 是 \mathbb{Z} 到 \mathbb{Z} 的群同态，但是可以验证 ϕ 不是一种环同态。

环同态实例-1

Example

请验证以下同态实例，体会环同态与群同态的异同点。

- ① 已知 \mathbb{Z} 是环，定义映射 $\phi: \mathbb{Z} \mapsto \mathbb{Z}$ 为 $\phi(k) = 2k, \forall k \in \mathbb{Z}$ ，即把所有整数映射到偶数 $2\mathbb{Z}$ 。已知 ϕ 是 \mathbb{Z} 到 \mathbb{Z} 的群同态，但是可以验证 ϕ 不是一种环同态。
- ② 对任意整数 $n \in \mathbb{Z}$ ，已知 \mathbb{Z}_n 为环，定义映射 $\phi: \mathbb{Z}_n \mapsto \mathbb{Z}_n$ 为 $\phi(a) = a^2 \bmod n, \forall a \in \mathbb{Z}_n$ ，即把所有 \mathbb{Z}_n 的元素映射到平方数。可以验证 ϕ 不是一种环同态，尽管这种映射在 \mathbb{Z}_n^* 中是一种群同态。

环同态实例-2

Example

请验证以下同态实例，体会环同态与群同态的异同点。

- ① 考虑一种特殊的环同态，定义 $\phi: 2\mathbb{Z} \mapsto \mathbb{Z}_2$ 为 $\forall k \in 2\mathbb{Z}$, $\phi(k) = k \bmod 2$ 。明显， ϕ 是同态，但不是满同态，它把所有偶数都映射到了 0。将这种把任意 R 映射到零环 $\{0\}$ 的环同态称为零同态。

环同态实例-2

Example

请验证以下同态实例，体会环同态与群同态的异同点。

- ① 考虑一种特殊的环同态，定义 $\phi: 2\mathbb{Z} \mapsto \mathbb{Z}_2$ 为 $\forall k \in 2\mathbb{Z}$, $\phi(k) = k \bmod 2$ 。明显， ϕ 是同态，但不是满同态，它把所有偶数都映射到了 0。将这种把任意 R 映射到零环 $\{0\}$ 的环同态称为零同态。
- ② 考虑一种更特殊的环同态，对任意的环 R ，定义映射 $\phi: R \mapsto \mathbb{Z}_2$ 为 $\forall a \in R$, $\phi(a) = 0$ 。可验证，这是一种零同态，显然不是满同态。特别提醒注意，如果环 R 有乘法单位元 1, $\phi(1) = 0$ 。并不是我们期望的映射到 \mathbb{Z}_2 的 1。

环同态实例-3

Example

- ① 对任意环 R , 已知 $R \times R$ 是环。定义映射 $\phi : R \times R \mapsto R \times R$ 为 $\forall (a, b) \in R \times R, \phi(a, b) = (a, 0)$ 。可验证, 这是一个环同态, 但并非满同态。注意, 在 $\phi(R \times R)$ 中的单位元是 $(1, 0)$, 但是 $R \times R$ 中的单位元是 $(1, 1)$ 。

环同态实例-4

Example

- ① 设 p 是任意一个奇素数，考虑 $2\mathbb{Z}$ 与 \mathbb{Z}_p 之间的映射 $\phi: 2\mathbb{Z} \mapsto \mathbb{Z}_p$ ，定义为 $\forall k \in 2\mathbb{Z}, \phi(k) = k \bmod p$ 。直观上看，该映射把所有的偶数做模 p 操作满射到环 \mathbb{Z}_p 。容易验证 ϕ 是满同态。值得注意的是，偶数环 $2\mathbb{Z}$ 没有乘法单位元，环 \mathbb{Z}_p 的乘法单位元是 1， $2\mathbb{Z}$ 中有无穷多的元素映射到 \mathbb{Z}_p 的乘法单位元 1 上。也就是说，即使乘法单位元必然映射为乘法单位元，也并非只有乘法单位元才映射为乘法单位元。

理想

环的理想在群论中的对应概念是正规子群。

Definition

给定环 R , I 是 R 的子环, 如果对任意的 $r \in R$ 有 $rl \subset I$ 和 $lr \subset I$, 则称 I 是 R 的理想。

理想

环的理想在群论中的对应概念是正规子群。

Definition

给定环 R , I 是 R 的子环, 如果对任意的 $r \in R$ 有 $rl \subset I$ 和 $lr \subset I$, 则称 I 是 R 的理想。

从表面上看, 所谓环 R 的理想 I , 首先它是环 R 的子环, 其次它具有“吸收性”, 即对任意的环元素 $r \in R$, 无论它是否落在 I 中, 用 r 左乘或者右乘 I , 所得到的元素都会落回到 I 中。

理想的实例

Example

- ① 所有的环 R 都有两个平凡理想: $\{0\}$ 和 R 。
- ② 如果 R 的理想 I 中包括 1 , 则 $R = I$ 。
- ③ 对任意整数 $n \in \mathbb{Z}$, 集合 $n\mathbb{Z}$ 是环 \mathbb{Z} 的理想。直观上看, 集合 $n\mathbb{Z}$ 包含了所有 n 的倍数, $n\mathbb{Z}$ 在加法上成群, 而用任意整数乘 n 的倍数还是得到一个 n 的倍数, 虽然此时 $n\mathbb{Z}$ 中并不必然有单位元 1 , 也不必然有乘法逆元。

主理想 (Principal Ideal)

Proposition

设 R 是一个交换环且有单位元, 任取 $a \in R$, 则集合

$$\langle a \rangle = \{ar : r \in R\}$$

是环 R 的一个理想, 称之为主理想 (Principal Ideal)。

主理想 (Principal Ideal)

Proposition

设 R 是一个交换环且有单位元, 任取 $a \in R$, 则集合

$$\langle a \rangle = \{ar : r \in R\}$$

是环 R 的一个理想, 称之为主理想 (Principal Ideal)。

主理想 vs 循环群

环的主理想对应群论中的循环群。

主理想-证明

Proof.

首先, 验证 $\langle a \rangle$ 是非空集合, 至少包括 0 和 a 两个元素。其次, 验证 $\langle a \rangle$ 在加法上成群。最后, 验证 $\langle a \rangle$ 具有吸收性, 即任取 $s \in R$ 乘上 $\langle a \rangle$ 中任意元素 ar , 必然有

$$s(ar) = a(sr) \in \langle a \rangle$$

注意, 上式成立需要依赖交换律。所以, $\langle a \rangle$ 是 R 的理想。 \square

主理想-实例

Example

- ① 对任意环 R , 只包含一个元素 0 的主理想 $\langle 0 \rangle$ 称为零理想。
- ② 对任意带单位元的环 R , 称 $\langle 1 \rangle$ 为单位理想, 显然 $R = \langle 1 \rangle$ 。
- ③ 对任意整数 n , 集合 $n\mathbb{Z}$ 是整数环 \mathbb{Z} 的理想, 也是主理想, $n\mathbb{Z} = \langle n \rangle$ 。

理想与主理想

Proposition

整数环 \mathbb{Z} 的所有理想都是主理想。

Proof.

首先，零理想也是主理想，因为 $\langle 0 \rangle = \{0\}$ 。设 I 是整数环 \mathbb{Z} 的一个非零理想，则 I 中必然包括某些正整数，根据良序原则，则 I 中必然存在一个最小正整数 n 。对任意的元素 $a \in I$ ，根据除法算法，存在整数 q 和 r ， $0 \leq r < n$ ，使得：

$$a = qn + r$$

也就是， $r = a - qn$ ，利用理想的属性，可知 $r \in I$ 。又因为 n 是 I 中最小正整数，所以， $r = 0$ 。因此， $a = qn$ ，即 $I = \langle n \rangle$ 。 \square

环同态与 Kernel

Proposition

环同态 $\phi: R \mapsto R'$ 的 Kernel 是 R 的理想。

Proof.

根据群论的结论, $K = \text{Ker } \phi$ 是 R 的加法子群 (并且是正规子群), 只需要证明 K 具有理想的“吸收性”, 即对任意的 $r \in R$ 和 $a \in K$ 有 $ar \in K$ 和 $ra \in K$ 。显然如此, 因为:

$$\phi(ar) = \phi(a)\phi(r) = 0\phi(r) = 0$$

且

$$\phi(ra) = \phi(r)\phi(a) = \phi(r)0 = 0$$



环同态与 Kernel

Example

对任意整数 $n \in \mathbb{Z}$, 定义映射 $\phi: \mathbb{Z} \mapsto \mathbb{Z}_n$ 为 $\forall a \in \mathbb{Z}$, $\phi(a) = a \bmod n$ 。容易验证这是一个环同态, 而 $\text{Ker } \phi$ 就是 $n\mathbb{Z}$ 。

商环

Lemma

设 R 是环, I 是 R 中的理想。商群 R/I 中元素的乘法定义为: 对任意的群元 $r, s \in R$,

$$(r + I)(s + I) = rs + I$$

该乘法是一种良定义操作, 且具有封闭性、结合律和对加法具有分配律。

商环

Proof.

首先证明乘法是一种良定义操作，即假设 $r' \in r + I$, $s' \in s + I$, 证明 $r's' \in (rs + I)$ 。因为 $r' \in r + I$, $s' \in s + I$, 即存在 $i_1, i_2 \in I$ 使得 $r' = r + i_1$ 和 $s' = s + i_2$, 因此,

$$r's' = (r + i_1)(s + i_2) = rs + ri_2 + i_1s + i_1i_2$$

根据理想的吸收性, $ri_2 + i_1s + i_1i_2 \in I$, 所以, $r's' \in rs + I$ 。商环乘法的封闭性、结合律和分配律留作课后练习。 \square \square

商环

Theorem

设 R 是环, I 是 R 中的理想。商群 R/I 在陪集加法与引理25中定义的乘法上形成环, 称为 R 模 I 的商环, 同样记为 R/I 。

商环

Example

任取 $n \in \mathbb{Z}$, $n\mathbb{Z} = \langle n \rangle$ 是整数环 \mathbb{Z} 的主理想, 则 $\mathbb{Z}/n\mathbb{Z}$ 是商环, 其中元素刚好构成模 n 的完全剩余系。

环的标准同态与第一同构定理

Definition

设 I 是环 R 的理想, 定义环同态映射 $\phi: R \mapsto R/I$ 为 $\phi(r) = r + I$, $\forall r \in R$. 并称该映射为环的**标准同态**或者**自然同态**, 且 $\text{Ker } \phi = I$.

Theorem (第一同构定理.)

设 $\psi: R \mapsto S$ 是环同态, 记 $K = \text{Ker } \psi$ 是 R 的理想. 如果 $\phi: R \mapsto R/K$ 是标准同态, 则存在唯一同构 $\eta: R/K \mapsto \psi(R)$ 使得 $\psi = \eta\phi$.

环的标准同态与第一同构定理

Example

任取 $n \in \mathbb{Z}$, 构造映射 $\phi: \mathbb{Z} \mapsto \mathbb{Z}_n$ 为, 任取 $a \in \mathbb{Z}$, $\phi(a) = a \bmod n$. 可验证, 这是一个环同态映射。 $\text{Ker } \phi = n\mathbb{Z}$, 因为所有 n 的倍数都映射为 0。根据第一同构定理, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ 。

域的定义

Definition

如果一个带单位元的交换环 R 中的非 0 元素都存在唯一的乘法逆元, 即 $\forall a \in R$ 且 $a \neq 0$, 则存在唯一的 $a^{-1} \in R$ 使得 $a * a^{-1} = a^{-1}a = 1$, 则称这种代数结构为域。

域-实例

Example

- ① 在普通的加法与乘法上, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ 都是域。 \mathbb{Z} 不是域, 因为乘法上 \mathbb{Z} 不是群。
- ② 任意给定素数 p , 在模 p 的加法与乘法上 \mathbb{Z}_p 是域。因为 \mathbb{Z}_p 在加法上是阿贝尔群, 而 \mathbb{Z}_p^* 在乘法上也是阿贝尔群。对任意合数 $n \in \mathbb{Z}$, \mathbb{Z}_n 则不是域, 因为 $\mathbb{Z}_n - \{0\}$ 乘法上不成群。

域的乘法逆元与零因子

Proposition (乘法逆元与零因子.)

对任意的域 F , 任取 $a, b \in F$, 如果 $ab = 0$ 则 $a = 0$ 或者 $b = 0$ 。
即域中不存在零因子。

Proof.

不妨设 $a \neq 0$, 否则证完。因为 $a \neq 0$, 则存在 a 的乘法逆元 $a^{-1} \in F$ 且 $a^{-1} \neq 0$, 使得 $aa^{-1} = 1$ 。等式 $ab = 0$ 两边乘上 a^{-1} , 根据之前的命题, 则 $b = 0$ 。 □

域的乘法逆元与零因子

Proposition (整环与域.)

每一个有限整环都是域。

Proof.

证明的思路就是利用有限整环的性质，为每一个非 0 元素找到乘法逆元。设 D 是一个有限整环，记 D^* 为环中所有非 0 元素的集合。对任意的 $a \in D^*$ ，构造映射 $\lambda_a: D^* \mapsto D^*$ 为 $\lambda_a(d) = ad$ ， $\forall d \in D^*$ 。首先，证明这确实是合理的映射，因为如果 $a \neq 0$ ， $d \neq 0$ ，则 $ad \neq 0$ 。然后，因为 D^* 是有限集且 λ_a 是从 D^* 到 D^* 的单射，所以 λ_a 必然是满射。因此，必然存在某个 $d \in D^*$ 使得 $ad = 1$ ，又因为 D 是交换环，所以这个 d 就是 a 的乘法逆元。结论：可为 D^* 中每一个元素都找到乘法逆元，所以 D 是一个域。 □

特征 (Characteristic)

Definition (特征.)

环 R 的特征 (*characteristic*) 定义为最小的正整数 n 使得对任意的 $r \in R$, $\underbrace{r + r + \cdots + r}_{n\uparrow} = nr = 0$ 。如果不存在这样的 n , 则 R 的特征定义为 0。

Example

- 1 环 $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ 的特征都是 0。
- 2 对任意素数 p , 域 \mathbb{Z}_p 的特征是 p 。因为 \mathbb{Z}_p 加法群的阶为 p , 即对任意的 $a \in \mathbb{Z}_p$, $pa = 0$ 。

特征的属性

Lemma

设 R 为环, 若 1 在加法群的阶为 n , 则 R 的特征为 n 。

Proof.

若 1 在加法群的阶为 n , 则 n 是最小正整数使得 $n1 = 0$ 。那么, 任取 $r \in R$, 有:

$$nr = n(1r) = (n1)r = 0r = 0$$

即 n 是 R 的特征。



特征的属性

Proposition

整环的特征或者为素数，或者为 0。

Proof.

设整环 D 的特征为 n ，且 $n \neq 0$ 。如果 n 不是素数，则 $n = ab$ ，且 $1 < a, b < n$ 。根据以上引理，有

$$0 = n1 = (ab)1 = (a1)(b1)$$

因为 D 是整环， D 中无零因子，所以必然 $a1 = 0$ 或者 $b1 = 0$ 。但是这都意味着 D 的特征小于 n ，矛盾。 □

域的特征与阶的关系

Proposition (有限域的特征.)

阶为 n 的有限域 F 的特征是一个素数 p , 且 $p \mid n$ 。

Proof.

因为有限域 F 的阶为 n , 且 F 是加法群, 所以对任意的 $a \in F$, 有 $na = 0$ 。所以, F 的特征必然是素数 p , 且 $p \mid n$ 。□

有限域的阶

以下不加证明给出另一个重要结论。

Proposition (有限域的阶)

如果有限域 F 的特征是素数 p ，则 F 的阶是 p^n ， n 是某个正整数。进一步，对任意的素数 p 和正整数 n ，存在阶为 p^n 的有限域，并且所有的 p^n 阶有限域都同构。

Example

p^n 阶的有限域也记为 $\text{GF}(p^n)$ ，GF 是 Galois Field 的缩写。

域的理想

Proposition (域的理想)

任何一个域 F 的理想只有 0 和自己本身 F 。

Proof.

首先, 已知 0 和 F 都是 F 的理想。设 I 是域 F 的非 0 理想, 则存在非零元素 $a \in I$ 。因为 F 是域, 则存在 a 的乘法逆元 $a^{-1} \in F$ 。根据理想的吸收性, $a^{-1}a = 1 \in I$ 。包含 1 的理想 I 等于 F , 即 $I = F$ 。 □

域同态是单射

Proposition (域同态是单射.)

任何一个域同态或者是单射或者是零同态。

Proof.

域 F_1 到域 F_2 的域同态 ϕ 是单射，当且仅当 $\text{Ker } \phi = \{0\} \subset F_1$ 。因为 F_1 的理想只有 0 和 F_1 本身，所以当 $\text{Ker } \phi = \{0\}$ 时 ϕ 是单射，而当 $\text{Ker } \phi = F_1$ 时， ϕ 是零同态。 \square

极大理想与素理想

Definition (极大理想与素理想.)

设 R 是环, M 是 R 的真子集且是 R 的理想, 则称 M 是 R 的真理想。设 M 是 R 的真理想, 如果 M 不是 R 的任意真理想的真子集, 则称 M 是极大理想 (*maximal ideal*)。即如果 M 是 R 的极大理想, 则对 R 的任意理想 I , 若 $M \subset I$, 则 $I = R$ 。设 P 是交换环 R 的真理想, 如果对任意 $ab \in P$, 则或者 $a \in P$, 或者 $b \in P$, 就称 P 为素理想 (*Prime Ideal*)。

极大理想与素理想

Example

素理想的“素”确实有“素数”的意味。设 p 为素数，如果 $p \mid ab$ ，则 $p \mid a$ 或 $p \mid b$ 。请体会素理想定义中要求与之类似之处：对任意 $ab \in P$ ，则 $a \in P$ 或 $b \in P$ 。令 $P = p\mathbb{Z}$ ， p 是任意素数， $a \in P$ 当且仅当 $p \mid a$ 。所以，从整数的角度上看，素理想确实是素数的倍数形成的理想。当然，理想不能仅停留于此，还需要进一步的抽象，但是这个例子告诉我们，抽象代数的“抽象”并非凭空而出，往往源自于具体的实例。

极大理想与素理想

Example

设 $P = \{0, 2, 4, 6\}$ 为环 \mathbb{Z}_8 的理想, 可验证 P 是极大理想, 也是素理想。任取素数 p , 则 $p\mathbb{Z}$ 是 \mathbb{Z} 的素理想。

极大理想与域

Theorem (极大理想与域.)

设 R 是交换环, M 是 R 的理想, 则 M 是 R 的极大理想, 当且仅当 R/M 是域。

极大理想与域

Example

任取素数 p ，已知 $p\mathbb{Z}$ 是 \mathbb{Z} 的素理想。因为 $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$ ， \mathbb{Z}_p 是域，所以 $p\mathbb{Z}$ 是 \mathbb{Z} 的极大理想，

素理想与整环

Theorem (素理想与整环.)

设 R 是交换环, P 是 R 的理想, 则 P 是 R 的素理想, 当且仅当 R/P 是整环。

素理想与整环

Example

设 p 是素数, 则 $p\mathbb{Z}$ 是 \mathbb{Z} 的理想。可知, $p\mathbb{Z}$ 是 \mathbb{Z} 的极大理想, 因为 $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$ 是域。

极大理想与素理想

Proposition (极大理想与素理想.)

交换环的每一个极大理想都是素理想。