



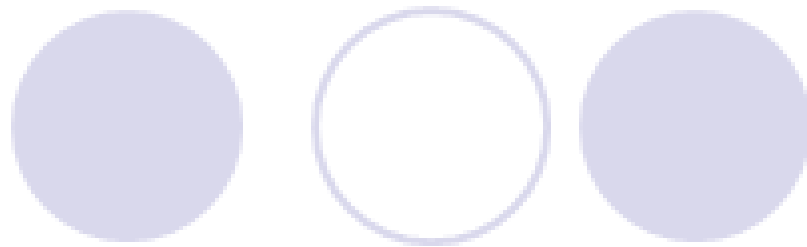
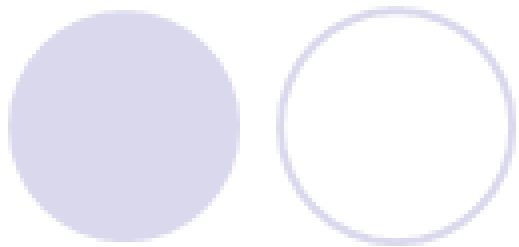
# 离散数学

大连理工大学软件学院

陈志奎 博士、教授、博士生导师

办公室：综合楼405，Tel: 62274392  
实验室：综合楼一楼，教学楼A502/C109，

Mobile: 13478461921  
Email: zkchen@dlut.edu.cn  
zkchen00@hotmail.com  
QQ: 1062258606



# 离散数学

## 第七章 群环域



# 回 顾



- 子群的陪集
- 陪集的性质
- 陪集与等价
- **Lagrange**定理
- 置换
- 置换群

循环群定义及性质

生成元、 $n$ 阶循环群、  
无限循环群

置换群定义及性质  
群的同态与同构

群同态映射：单一同  
态、满同态、群同构  
映射

## 7.6.1 环的概念与性质

• **定义7.24** 设 $\langle R, +, \cdot \rangle$ 是代数系统,  $+$  和  $\cdot$  是二元运算, 如果满足下列条件:

(1)  $\langle R, + \rangle$ 构成**交换群**。

(2)  $\langle R, \cdot \rangle$ 构成**半群**。

(3)  $\cdot$  运算关于  $+$  适合**分配律**。

则称 $\langle R, +, \cdot \rangle$ 是一个**环**。

➤ 为了区分环中的两个运算, 通常称 $+$ 为环中的加法,  $\cdot$ 为环中的乘法, 把 $\langle R, + \rangle$ 称为加法群,  $\langle R, \cdot \rangle$ 称为乘法半群。而且还规定, 运算的顺序是先计算乘法再计算加法。

## 7.6.1 环的概念与性质

- **定义7.25** 给定环 $\langle R, +, \cdot \rangle$ ,

若 $\langle R, \cdot \rangle$ 是可交换半群, 则称 $\langle R, +, \cdot \rangle$ 是**可交换环**;

若 $\langle R, \cdot \rangle$ 是独异点, 则称 $\langle R, +, \cdot \rangle$ 是**含幺环**;

若 $\forall a, b \in R, ab = 0 \Rightarrow a = 0 \vee b = 0$ , 则称 $R$ 是**无零因子环**;

若 $\langle R, \cdot \rangle$ 满足等幂律, 则称 $\langle R, +, \cdot \rangle$ 是**布尔环**;

若 $R$ 既是**交换环**、**含幺环**, 又是**无零因子环**, 则称 $R$ 是**整环**。

## 7.6.1 环的概念与性质

- **例7.26**  $\langle \mathbf{Z}, +, * \rangle$ ,  $\langle \mathbf{R}, +, * \rangle$ ,  $\langle \mathbf{Q}, +, * \rangle$ ,  $\langle \mathbf{E}, +, * \rangle$ , 和  $\langle \mathbf{C}, +, * \rangle$  等都是环。而且除了  $\langle \mathbf{E}, +, * \rangle$  之外都是拥有加法零元（数0）和乘法幺元（数1）的可交换含幺环。这里  $\mathbf{Z}$ ,  $\mathbf{R}$ ,  $\mathbf{Q}$ ,  $\mathbf{E}$ ,  $\mathbf{C}$  分别为整数集合，实数集合，有理数集合，偶数集合和复数集合。而  $+$  和  $*$  分别为普通意义下的加法和乘法。
- **例7.27**  $\langle \mathbf{Z}_n, +_n, *_n \rangle$  是一个含幺可交换环，其中数字0是环的零元，数字1是环的幺元。

## 7.6.1 环的概念与性质

- **例7.27** 给定 $\langle P(S), +, * \rangle$ , 其中  $P(S)$  是结合  $S$  的幂集,  $+$ 和 $*$ 分别定义如下:

$$A + B = (A - B) \cup (B - A)$$

$$A * B = A \cap B$$

这里 $A, B \in P(S)$ ,  $\cap$ 和 $\cup$ 是集合的交与并运算。

不难验证,  $\langle P(S), +, * \rangle$ 是环, 并且拥有加法幺元 $\emptyset$ 和乘法幺元 $S$ 的可交换幺环。通常称该环为子集环。

## 7.6.1 环的概念与性质

- 证明：若  $A, B, C \in P(S)$ ，则

$$\begin{aligned} A * (B + C) &= A \cap ((B - C) \cup (C - B)) \\ &= (A \cap (B - C)) \cup (A \cap (C - B)) \\ &= ((A \cap B) - (A \cap C)) \cup ((A \cap C) - (A \cap B)) \\ &= (A \cap B) + (A \cap C) = A * B + A * C \end{aligned}$$

所以\*对于+是可分配的。这里仅给出\*对于+是可分配的证明。其他两条留给读者练习证明。



## 7.6.1 环的概念与性质

• **定理7.23** 设 $\langle R, +, \cdot \rangle$ 是环, 则

$$(1) \quad \forall a \in R, \quad a0 = 0a = 0;$$

$$(2) \quad \forall a, b \in R, \quad (-a)b = a(-b) = -ab;$$

$$(3) \quad \forall a, b, c \in R, \quad a(b - c) = ab - ac,$$

$$(b - c)a = ab - ca;$$

## 7.6.1 环的概念与性质

• **例7.29** 在环中计算 $(a + b)^3$ ,  $(a - b)^2$ 。

• **解:**

$$\begin{aligned}(a + b)^3 &= (a + b)(a + b)(a + b) \\&= (a^2 + ba + ab + b^2)(a + b) \\&= a^3 + ba^2 + aba + b^2a + a^2b + bab + ab^2 + b^3\end{aligned}$$

$$(a - b)^2 = (a - b)(a - b) = a^2 - ba - ab + b^2$$

## 7.6.2 域的概念

- **定义7.26** 设 $R$ 是整环，且 $R$ 中至少含有两个元素。若 $\forall a \in R^* = R - \{0\}$ ，都有 $a^{-1} \in R$ ，则称 $R$ 是**域**。
- **定理7.24** 给定可交换环 $\langle S, +, * \rangle$ ，若 $\langle S - \{0\}, * \rangle$ 为群，此时称 $\langle S, +, * \rangle$ 为**域**。
- **例7.30**  $\langle R, +, * \rangle$ 和 $\langle Q, +, * \rangle$ 都是域，而 $\langle Z, +, * \rangle$ 不是域，其中 $R$ ， $Q$ 和 $Z$ 分别为实数集合，有理数集合和整数集合， $+$ 和 $*$ 为一般意义下的加法运算和乘法运算。
- **例7.31** 整数环 $Z$ ，有理数环 $Q$ ，实数环 $R$ ，复数环 $C$ 都是**交换环、含么环、无零因子环和整环**，其中有理数环 $Q$ 、实数环 $R$ 、复数环 $C$ 是**域**。

➤ 包含有限个元素的域被称为**有限域**。

## 7.6.2 域的概念

- **定理7.25**  $\langle S, +, * \rangle$  为域

$$\Rightarrow (\forall a)(\forall b)(a, b \in S \wedge a * b = 0 \rightarrow (a = 0 \vee b = 0)).$$

- **证明：**若  $a = 0$ ，定理显然成立。

若  $a \neq 0$ ，由  $\langle S, +, * \rangle$  为域可知， $a^{-1} \in S$ ，于是，

$$b = 1 * b = (a^{-1} * a) * b = a^{-1} * (a * b)$$

根据假设  $a * b = 0$ ，则  $b = a^{-1} * 0 = 0$

同理，若  $b \neq 0$ ，则  $a = 0$ 。因此，

$$a * b = 0 \Rightarrow a = 0 \vee b = 0$$

由于域是可交换含幺环，而且又知道域中没有零因子，所以域为整环。但反之不为真，即整环未必是域。

## 7.6.2 域的概念

- **定理7.26** 给定环 $\langle \mathbb{Z}_n, +_n, *_n \rangle$ , 则

$\langle \mathbb{Z}_n, +_n, *_n \rangle$ 是域  $\Leftrightarrow n$ 为素数。

- **证明:** 充分性: 假设 $n$ 为素数, 而 $\langle \mathbb{Z}_n, +_n, *_n \rangle$ 为环, 证 $\langle \mathbb{Z}_n, +_n, *_n \rangle$ 是域。因为 $\langle \mathbb{Z}_n, +_n, *_n \rangle$ 是含么环, 故只需证明 $\langle \mathbb{Z}_n, +_n, *_n \rangle$ 中非零元都具有乘法逆元即可。

设 $a \in \mathbb{Z}_n$ ,  $0 < a < n$ 。因为 $n$ 为素数, 则 $\gcd(a, n) = 1$ , 集合 $\mathbb{Z}_n$ 中于是存在 $r, s \in \mathbb{Z}$ , 使得

$$a * r + n * s = 1$$

由此

$$a *_n r = a * r +_n 0 = a * r +_n n * s = a * r + n * s = 1$$

2017/3/24 既得 $a^{-1} = r$ , 故 $\langle \mathbb{Z}_n, +_n, *_n \rangle$ 为域。

## 7.6.2 域的概念

必要性：用反证法证明。假设 $n$ 不是素数，则

$$n = a * b, 0 < a < n \text{ 且 } 0 < b < n$$

于是

$$a *_n b = a * b = n = 0,$$

但是 $a \neq 0$ ,  $b \neq 0$ , 因此 $a$ 与 $b$ 为环 $\langle \mathbb{Z}_n, +_n, *_n \rangle$ 的零因子。

通过定理7.12可知，域中无零因子，因此 $\langle \mathbb{Z}_n, +_n, *_n \rangle$ 不为域。与假设矛盾。

综上所述，定理得证。

## 7.7 应用：群与网络安全

- 群在网络安全中有重要的应用，其中，有限域在密码学中的地位越来越重要。许多密码算法都对有限域的性质有很大的依赖性。
- 有限域在许多密码学中扮演者重要的角色，在密码学中，有限域的阶（元素个数）必须是一个素数的幂 $p^n$ ， $n$ 为正整数。阶位 $p^n$ 的有限域记为 $GF(p^n)$ ，GF代表伽罗瓦域，以第一位研究有限域的数学家的名字命名。我们再次要关注两种特殊的情形： $n = 1$ 时的有限域 $GF(p)$ ，和 $p = 2$ 的域 $GF(2^n)$ 。

## 7.7 应用：群与网络安全

- 给定一个素数  $p$ ，元素个数为  $p$  的有限域  $GF(p)$  被定义为整数  $\{0, 1, \dots, p-1\}$  的集合  $Z_p$ ，其运算为模  $p$  的算术运算。
- 在整数  $\{1, 2, \dots, n-1\}$  的集合  $Z_n$ ，在模  $n$  的算术运算下，构成一个交换环。
- $Z_n$  中的任一整数有乘法逆元当且仅当该整数与  $n$  互素。当  $n$  为素数， $Z_n$  中所有非零整数都与  $n$  互素，此时  $Z_n$  所有非零整数都有乘法逆元。



## 7.7 应用：群与网络安全

- 例：在 $GF(p)$ 中求乘法逆元。

如果 $\gcd(m, b) = 1$  ( $\gcd$ : greatest common divisor 最大公约数), 那么 $b$ 有模  $m$  的乘法逆元。对于正整数 $b < m$ , 存在 $b^{-1} < m$ 使得 $bb^{-1} = 1 \bmod m$ 。求出 $\gcd(m, b)$ 之后, 当 $\gcd(m, b)$ 为1时, 算法返回 $b$ 的乘法逆元。

## 7.7 应用：群与网络安全

扩展的EUCLID ( $m, b$ )

$$1. \quad (A_1, A_2, A_3) \leftarrow (1, 0, m);$$

$$(B_1, B_2, B_3) \leftarrow (0, 1, b);$$

$$2. \quad \text{if } B_3 = 0$$

$\text{return } A_3 = \gcd(m, b);$  无逆元

$$3. \quad \text{if } B_3 = 1$$

$\text{return } B_2 = b^{-1} \bmod m$

$$4. \quad Q = \left\lfloor \frac{A_3}{B_3} \right\rfloor$$

$$5. \quad (T_1, T_2, T_3) \leftarrow (A_1 - Q B_1, A_2 - Q B_2, A_3 - Q B_3)$$

$$6. \quad (A_1, A_2, A_3) \leftarrow (B_1, B_2, B_3)$$

## 7.7 应用：群与网络安全

7.  $(B_1, B_2, B_3) \leftarrow (T_1, T_2, T_3)$

8. *goto* 2

注意到，如果  $\gcd(m, b) = 1$ ，在最后一步我们将得到  $B_3 = 0$  和  $A_3 = 1$ 。因此，在上一步， $B_3 = 1$ 。

$$mB_1 + bB_2 = B_3$$

$$mB_1 + bB_2 = 1$$

$$bB_2 = 1 - mB_1$$

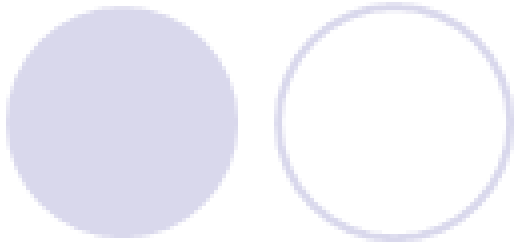
$$bB_2 = 1 \pmod{m}$$

此时  $B_2$  为  $b$  的模  $m$  乘法逆元。

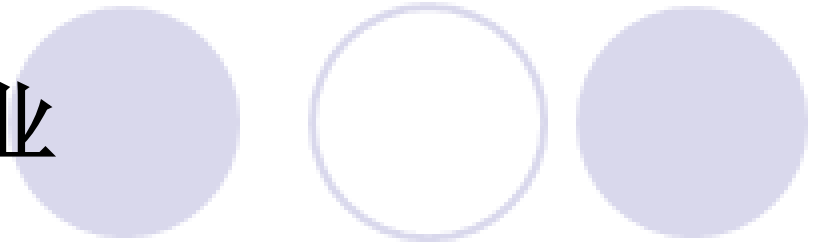


# 总 结

- 环的概念与性质
- 域的概念
- 应用：群与网络安全
  - 有限域的应用



# 作 业



- **P174:** 17,18