

# 代数学基础

杨金标. 地空楼 525

- 助教自我介绍. 风风群
- 考核成绩 = 平时成绩, 期中成绩, 期末成绩 加权平均
- 平时成绩 = 作业 (去掉一两个最低分) + 考勤 (课堂小测试, 或点名)
- 交作业与发作业时间: 周二上课前后. (晚交一天扣一个星期扣一半的分  
晚交一个星期以上不得分)
- 大二, 大三, 大四. 选修过近代代数
  - $\geq 80'$  交作业, 参加考证, 可以不用听课
  - $\geq 90'$  不交作业, 不用听课, 参加考证

} 需要书面申请

## §1. 群环域

- 主要内容:
- 1) (子)群, (子)环, (子)域, 同态等基本概念 (记住)
  - 2) 群, 环, 域的简单例子 (会验证)
  - 2) 群, 环, 域, 同态等基本性质 (会证明).

### §1.1\* 引言

二次方程:  $x^2 + bx + c = 0 \Rightarrow x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$

三次方程:  $x^3 + ax^2 + bx + c = 0 \xrightarrow{x=y-\frac{1}{3}a} y^3 + py + q = 0$

Cardano 方法. 
$$\begin{cases} (s+t)^3 - 3st(s+t) - (s^3 + t^3) = 0 \\ 3st + p = 0 \\ s^3 + t^3 + q = 0 \end{cases}$$

$$\Rightarrow y = s + t = \frac{1}{3}\sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{3s}} + \frac{1}{3}\sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{3s}} \quad (i=0,1,2)$$

例:  $x^3 - 15x - 4 = 0 \Rightarrow x = \sqrt[3]{2+11i} + \sqrt[3]{2-11i} \quad R=0,1,2.$

四次方程:  $x^4 + ax^3 + bx^2 + cx + d = 0 \xrightarrow{x=y-\frac{a}{4}} y^4 + \alpha y^2 + \beta y + \gamma = 0$

$$y^2 + z = \pm (\sqrt{2z - \alpha} y \pm \sqrt{z^2 - \gamma}) \Leftrightarrow (y^2 + z)^2 = (2z - \alpha)y^2 - \beta y + (z^2 - \gamma)$$

$\Downarrow$

$$y = \dots$$

完全平方?

$$\beta^2 = 4(2z - \alpha)(z^2 - \gamma)$$

$\Rightarrow$  四次方程也有类似公式 (比较复杂)

例:  $y^4 - y^2 + 6y - 2 = 0 \Rightarrow 36 = 4(2z+1)(z^2+1) (\Leftrightarrow z=1) \Rightarrow (y^2+1)^2 = 3(y-1)^2$

问题：大于4次的方程是否可解？即，根是否可由方程系数通过有限次  $+-\times\div\sqrt{\phantom{x}}$  得到？

Galois：不一定，存在五次方程不可解！

思路：设  $\phi \neq K \subseteq \mathbb{C}$ . 若  $K \neq \emptyset$  关于  $+-\times\div$  封闭，则称  $K$  为数域.

$$f(x) = x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n$$

记  $L_f \subseteq \mathbb{C}$  为包含  $\alpha_1, \alpha_2, \dots, \alpha_n$  的最小数域. 则 Galois 证明了

$$\text{**} \left( f=0 \text{ 可解} \Leftrightarrow \text{存在特殊域链 } \mathbb{Q} = K_1 \subset K_2 \subset \dots \subset K_m \subset K_{m+1} = L_f \right. \\ \left. \text{ie. } K_{i+1} = K_i[\sqrt[n_i]{\lambda_i}] \right)$$

如何判定这样的域链存在？Galois 引入群及子群.

$$\text{Gal}(L_f/\mathbb{Q}) := \left\{ \phi: L_f \rightarrow L_f \mid \phi \text{ 为保持 } +, \times \text{ 的双射} \right\}$$

并证明了：中间域  $\xleftrightarrow{1:1}$  子群

通过这一对应及引理，Galois 将方程可解性转化为纯群论问题：

问题：是否存在正规子群链

$$\{e\} = G_{m+1} \triangleleft G_m \triangleleft \dots \triangleleft G_2 \triangleleft G_1 = \text{Gal}(L_f/\mathbb{Q}).$$

使得  $G_i/G_{i+1}$  ( $1 \leq i \leq m$ ) 都为交换群.

方程可解性  $\xleftrightarrow{\text{域论}}$  域链存在性  $\xleftrightarrow{\text{群论}}$  子群链存在性.

Galois： $\exists$  5次多项式  $f$  s.t.  $\text{Gal}(L_f/\mathbb{Q}) \cong S_5$  不存在上述子群链.

## §1.2. 代数系统

定义： 1) 一个非空集合  $K$  上的 **(二元) 运算** 是指一个给定的映射

$$\varphi: K \times K \rightarrow K$$

有时为了方便将其写成  $+$   $*$   $\times$   $\cdot$   $-$   $\div$  等形式.

2) 都带有 (一个或几个) 运算的集合

$$(K, \varphi) \text{ 或 } (K, \varphi_1, \varphi_2, \dots, \varphi_m)$$

为一个 **代数系统**.

例：  $(\mathbb{N}, +)$ ,  $(\mathbb{N}, \cdot)$ ,  $\mathbb{N} = (\mathbb{N}, +, \cdot)$ ,  $(\mathbb{Q} \setminus \{0\}, \div)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{Q}, -)$   
 $(\mathbb{Z}, +, \cdot)$ ,  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{C}, +, \cdot)$

代数学任务之一：“同构”意义下分类代数系统

例：  $K = \{1, 2\}$ .  $\begin{array}{c|cc} \varphi & 1 & 2 \\ \hline 1 & x & y \\ 2 & z & t \end{array}$   $\varphi(1,1)=x$   $\varphi(1,2)=y$   
 $\varphi(2,1)=z$   $\varphi(2,2)=t$

$\varphi$  can be  
represented  
by  $\begin{array}{c|cc} x & y \\ \hline z & t \end{array}$

$(\mathbb{R}_2, \times, \cdot)$ $\begin{array}{c cc} 1 & 1 \\ \hline 1 & 1 \\ 2 & 2 \end{array}$	$(\mathbb{R}_2, \cdot)$ $\begin{array}{c cc} 1 & 1 \\ \hline 1 & 1 \\ 2 & 2 \end{array}$	$\begin{array}{c cc} 1 & 1 \\ \hline 2 & 1 \\ 2 & 1 \end{array}$ $2 \cdot 1 = 2$	$\begin{array}{c cc} 1 & 1 \\ \hline 2 & 2 \\ 2 & 2 \end{array}$ $a \cdot b = a$
$\begin{array}{c cc} 1 & 2 \\ \hline 1 & 1 \\ 2 & 1 \end{array}$ $2 \cdot 1 = 2$	$a \cdot b = b$ $\begin{array}{c cc} 1 & 2 \\ \hline 1 & 2 \\ 2 & 2 \end{array}$	$(\mathbb{R}_2, +)$ $\begin{array}{c cc} 1 & 2 \\ \hline 2 & 1 \\ 2 & 1 \end{array}$	$(\mathbb{R}_2, +)$ $\begin{array}{c cc} 1 & 2 \\ \hline 2 & 2 \\ 2 & 2 \end{array}$
$\begin{array}{c cc} 2 & 1 \\ \hline 1 & 1 \\ 1 & 1 \end{array}$ $1 \cdot 1 = 2$	$(\mathbb{R}_2, +)$ $\begin{array}{c cc} 2 & 1 \\ \hline 1 & 2 \\ 1 & 2 \end{array}$	$\begin{array}{c cc} 2 & 1 \\ \hline 2 & 1 \\ 1 & 1 \end{array}$ $1 \cdot 1 = 1$	$\begin{array}{c cc} 2 & 1 \\ \hline 2 & 2 \\ 1 & 2 \end{array}$ $1 \cdot 2 = 1$
$\begin{array}{c cc} 2 & 2 \\ \hline 1 & 1 \\ 1 & 1 \end{array}$ $1 \cdot 1 = 1$	$\begin{array}{c cc} 2 & 2 \\ \hline 1 & 2 \\ 1 & 2 \end{array}$ $1 \cdot 2 = 1$	$\begin{array}{c cc} 2 & 2 \\ \hline 2 & 1 \\ 1 & 2 \end{array}$ $1 \cdot 1 = 2$	$(\mathbb{R}_2, \times, \cdot)$ $\begin{array}{c cc} 2 & 2 \\ \hline 2 & 2 \\ 2 & 2 \end{array}$

### §1.3. 域的定义.

$$\mathbb{Q} = (\mathbb{Q}, +, \cdot), \quad \mathbb{R} = (\mathbb{R}, +, \cdot), \quad \mathbb{C} = (\mathbb{C}, +, \cdot)$$

$\uparrow$  有理数域

$\uparrow$  实数域

$\uparrow$  复数域

$+, \cdot$  满足四则运算规则, 其中有九条基本规则.

$$\textcircled{1} (a+b)+c = a+(b+c)$$

$$\textcircled{2} a+0 = a = 0+a$$

$$\textcircled{3} a+(-a) = 0 = (-a)+a$$

$$\textcircled{4} a+b = b+a$$

$$\textcircled{5} \begin{cases} a \cdot (b+c) = ab+ac \\ (a+b) \cdot c = ac+bc \end{cases}$$

$$\textcircled{6} (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

$$\textcircled{7} 1 \cdot a = a = a \cdot 1$$

$$\textcircled{8} a \cdot a^{-1} = 1 = a^{-1} \cdot a$$

$$\textcircled{9} ab = ba$$

定义: 设  $\varphi: K \times K \rightarrow K$  为集合  $K$  上的二元运算.

若  $\forall x, y, z \in K$  满足  $\varphi(\varphi(x, y), z) = \varphi(x, \varphi(y, z))$ , 则称  $\varphi$  满足结合律.

若  $\exists e \in K$  s.t.  $\forall x \in K$ , 都有  $\varphi(e, x) = x = \varphi(x, e)$ , 则称  $e$  为  $K$  在运算  $\varphi$  下的单位元.

若  $\forall x \in K, \exists y \in K$  s.t.  $\varphi(y, x) = e = \varphi(x, y)$ , 则称  $x$  在运算  $\varphi$  下可逆/存在逆元, 称  $y$  为在运算  $\varphi$  下  $x$  的逆元.

若  $\forall x, y \in K$ , 都有  $\varphi(x, y) = \varphi(y, x)$ , 则称  $\varphi$  满足交换律.

定义: 设集合  $K$  至少有两个元素.

$$+ : K \times K \rightarrow K, \quad \cdot : K \times K \rightarrow K$$

为  $K$  上两个运算. 若  $+, \cdot$  满足九条基本规则,

- $$+ \left\{ \begin{array}{l} 1) \text{ 加法结合律: } \forall a, b, c \in K, (a+b)+c = a+(b+c) \\ 2) \text{ 零元存在性: } \exists 0_K \in K \text{ s.t. } a+0_K = a = 0_K+a \\ 3) \text{ 负元存在性: } \forall a \in K, \exists b \in K \text{ s.t. } a+b = 0_K = b+a \\ 4) \text{ 加法交换律: } \forall a, b \in K, a+b = b+a \end{array} \right.$$



- + 相容
- 5) 分配律:  $\forall a, b, c \in K \quad a \cdot (b+c) = ab+ac \quad (a+b) \cdot c = ac+bc$
  - 6) 乘法结合律:  $\forall a, b, c \in K, (ab) \cdot c = a \cdot (b \cdot c)$
  - 7) 单位元存在性:  $\exists 1_K \in K \text{ s.t. } 1_K a = a = a \cdot 1_K$
  - 8) 可逆元存在性:  $\forall a \in K \setminus \{0\}, \exists b \in K \text{ s.t. } ab = 1_K = ba$
  - 9) 乘法交换律:  $\forall a, b \in K \quad ab = ba$

则称  $K = (K, +, \cdot)$  为一个域.

约定: 零元:  $0 = 0_K$

单位元:  $1 = 1_K$

减法:  $a - b := a + (-b)$

除法:  $\frac{b}{a} := b \cdot a^{-1} = a^{-1}b$

	倍数	幂次
$n > 0$	$na := \underbrace{a + a + \dots + a}_n$	$a^n := \underbrace{a \cdot a \cdot \dots \cdot a}_n$
$n = 0$	$0a := 0$	$a^0 := 1$
$n < 0$	$na := (-n) \cdot (-a)$	$a^n := (a^{-1})^{-n}$

此时可以像数一样对集合  $K$  中的元素作四则运算.

eg:  $\frac{b}{a} - \frac{d}{c} = \frac{bc-ad}{ac}$

例: 下以集合与运算构成域

$K = \{x, \checkmark\}$   
False True  
 $(K, \oplus, \wedge)$

异或

$\oplus$	x	✓
x	x	✓
✓	✓	x

与

$\wedge$	x	✓
x	x	x
✓	x	✓

减法 = ?

$$\left. \begin{array}{l} \ominus x = x \\ \ominus \checkmark = \checkmark \end{array} \right\} \Rightarrow x \ominus y = x \oplus y$$

$$K = \{\text{偶}, \text{奇}\}$$

$$(K, +, \cdot)$$

+	偶	奇
偶	偶	奇
奇	奇	偶

$\cdot$	偶	奇
偶	偶	偶
奇	偶	奇

注: 若  $|K| = 6$ , 则不存在两个二元运算  $+, \cdot$  使得  $(K, +, \cdot)$  构成域

定义: 设  $K = (K, +, \cdot)$  为一个域  $F \subseteq K$  非空子集. 若  $F$  关于  $K$  的加法和乘法构成一个域, 则称  $F$  为  $K$  的子域.

例:  $\mathbb{Q} \subseteq \mathbb{R}$ ,  $\mathbb{Q} \subseteq \mathbb{C}$ ,  $\mathbb{R} \subseteq \mathbb{C}$ .

$$\mathbb{Q}[\sqrt{-1}] := \{a + b\sqrt{-1} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$$

$$\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{R}.$$

$$\mathbb{Q}[\sqrt[3]{2}] := \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\} \subseteq \mathbb{R}$$

$$\mathbb{Q}(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \text{ 为有理系数的多项式且 } g(x) \neq 0 \right\}$$

可以证明在通常方式多项式的加法和乘法下  $\mathbb{Q}(x)$  构成域.

性质: 设  $K = (K, +, \cdot)$  为一个域  $F \subseteq K$  非空子集.

$$F \text{ 为子域} \Leftrightarrow \begin{cases} 1 \in F \\ F \text{ 关于 } +, \cdot \text{ 封闭} \\ \text{若 } a \in F \text{ 则 } a^{-1} \in F \end{cases}$$

注: 代数系统  $(\mathbb{Z}, +, \cdot)$  不是域.

### §1.3 环的定义

为了得到更多的代数系统 (eg.  $\mathbb{Z}$ ) 我们需要放弃部分条件.

eg.  $(\mathbb{Z}, +, \cdot)$  满足 (1)-(7) & (9), 不满足 (8).

**定义**: 设  $R = (R, +, \cdot)$  为带两个运算的代数系统, 且  $R \neq \emptyset$ .

1) 若  $(R, +, \cdot)$  满足 (1)-(7) & (9), 则称  $R = (R, +, \cdot)$  为 **(含幺)交换环**

2) 若  $(R, +, \cdot)$  满足 (1)-(7), 则称  $R = (R, +, \cdot)$  为 **(含幺)环**

域  $\subseteq$  交换环  $\subseteq$  环

**注**: 1) 我们不要求  $\#R \geq 2$ . 若  $\#R = 1$ , 则  $0_R = 1_R$ , 此时称  $R$  为 **零环**.

2) 部分书籍中, 称满足 (1)-(6) 的  $(R, +, \cdot)$  为 **环**. 在这门课程中仅考虑含幺环. 即不做特别说明时, 所有环都指含幺环.

**例**  $\therefore$  **交换环**  $\mathbb{Z}$ ,  $\mathbb{Z}[i] := \{a+bi \mid a, b \in \mathbb{Z}\}$

**环(不含幺)**  $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$

**例 (非交换环)**:

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$   $2 \times 2$  **矩阵 (matrix)**

$$M_2(R) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in R \right\}$$

$$\text{加法: } \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} := \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}$$

$$\text{乘法: } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}$$

则  $(M_2(R), +, \cdot)$  构成含幺非交换环. **矩阵代数**.

习题: 验证  $(M_2(\mathbb{R}), +, \cdot)$  为环.

$$0_{M_2(\mathbb{R})} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad 1_{M_2(\mathbb{R})} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad -\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$$

非交换性:  $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$

环的基本性质.

性质: 设  $R$  为环, 则

- 1)  $0_R, 1_R$  负元存在且唯一.
- 2)  $x \cdot 0 = 0 = 0 \cdot x \quad (\forall x \in R)$
- 3)  $R$  为零环  $\Leftrightarrow 1 = 0$ .
- 4)  $\sum_{i=1}^m a_i \sum_{j=1}^n b_j = \sum_{i=1}^m \sum_{j=1}^n a_i b_j \quad (\forall a_i, b_j \in R)$

pf: 1).  $0_R = 0_R + 0'_R = 0'_R, \quad 1_R = 1_R \cdot 1'_R = 1'_R$

设  $b, c$  均为  $a$  的负元, 则  $b = b + (a + c) = (b + a) + c = c$ .

2).  $x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0 \Rightarrow x \cdot 0 = 0$  同理  $0 \cdot x = 0$ .

$$\left( \begin{array}{l} \text{加法消去律 } a + b = a + c \Rightarrow b = c : \\ b = (-a) + a + b = (-a) + (a + b) = (-a) + (a + c) = (-a) + a + c = c \end{array} \right)$$

3).  $\Rightarrow$ : 显然.

$\Leftarrow$ :  $\forall r \in R \Rightarrow r = r \cdot 1 = r \cdot 0 = 0 \Rightarrow R = \{0\} \Rightarrow V$ .

$$\begin{aligned} \text{LHS} &= a_1 \left( \sum_{j=1}^n b_j \right) + a_2 \left( \sum_{j=1}^n b_j \right) + \cdots + a_m \left( \sum_{j=1}^n b_j \right) \\ &= \sum_{j=1}^n a_1 b_j + \sum_{j=1}^n a_2 b_j + \cdots + \sum_{j=1}^n a_m b_j = \text{RHS} \end{aligned}$$

注: 乘法的消去律不一定成立. (例  $x^0 = 0 \nRightarrow x = 0$ .)

习以为常的定律不一定成立. 一切都要从公理定义出发推导!

从已知环构造新环.

课本上不作这一要求

**定义**: 设  $R=(R,+;)$  为一个环,  $T \subseteq R$  子集. 若  $1 \in T$  且  $T$  关于  $R$  的加法和乘法构成一个环, 则称  $T$  为  $R$  的**子环**.

子环判定

**性质**: 设  $R$  为环,  $T \subseteq R$  子集. 则

$$T \text{ 为子环} \Leftrightarrow \begin{cases} 1 \in T \\ T \text{ 关于 } - \text{ 和 } \cdot \text{ 封闭} \end{cases}$$

**性质**: 设  $K=(K,+;)$  为一个域  $F \subseteq K$  非空子集.

$$F \text{ 为子域} \Leftrightarrow \begin{cases} 1 \in F \\ F \text{ 关于 } - , \cdot \text{ 封闭} \\ \text{若 } a \in F \setminus \{0\}, \text{ 则 } a^{-1} \in F \end{cases}$$

**pf**:  $\Rightarrow) \checkmark$

$\Leftarrow) 1 \in T \checkmark$

加法封闭:  $\because 0=1-1 \in T$

$\cdot \forall a \in T, -a = 0-a \in T$

$\cdot \forall a, b \in T \Rightarrow a+b = a-(-b) \in T$

$\cdot$  乘法封闭:  $\checkmark$

$\cdot$  公理 (1) (4) (5) (6) (9)  $\checkmark$

$\cdot$  公理 (2) (7):  $\exists 0, \exists 1 \checkmark$

$\cdot$  公理 (3):  $\exists -a \checkmark$

$\cdot$  公理 (8):  $\exists a^{-1} \checkmark$

## §1.4 群的定义

考虑带有一个二元运算的代数系统

例:  $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\} = \{r \in \mathbb{Q} \mid r \neq 0\}$ . 则  $\cdot$  为  $\mathbb{Q}^*$  上的二元运算.

类似地,  $(\mathbb{R}^*, \cdot), (\mathbb{C}^*, \cdot), (\mathbb{S}^1, \cdot), (\mathbb{M}_n, \cdot), (\mathbb{S}^{\pm 1}, \cdot), \dots, (\mathbb{Q}, +), (\mathbb{R}, +)$

容易验证这些代数系统  $(G, \cdot)$  满足

- (1) 结合律:  $\forall a, b, c \in G \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- (2) 单位元存在性:  $\exists e \in G \text{ s.t. } \forall a \quad a \cdot e = a = e \cdot a$
- (3) 逆元存在性:  $\forall a \exists b \text{ s.t. } a \cdot b = e = b \cdot a$
- (4) 交换律:  $\forall a, b, \quad a \cdot b = b \cdot a$

定义 (群): 设  $(G, \cdot)$  为带有一个二元运算的代数系统,  $G \neq \emptyset$ .

- 1) 若  $(G, \cdot)$  满足 (1)-(4), 则称  $G = (G, \cdot)$  为 **交换群** (阿贝尔群) abelian gr.
- 2) 若  $(G, \cdot)$  满足 (1)-(3), 则称  $G = (G, \cdot)$  为 **群** gr.
- 3) 若  $(G, \cdot)$  满足 (1)-(2), 则称  $G = (G, \cdot)$  为 **含么半群** monoid
- 4) 若  $(G, \cdot)$  满足 (1), 则称  $G = (G, \cdot)$  为 **半群** semigr.

交换群  $\subseteq$  群  $\subseteq$  含么半群  $\subseteq$  半群

例:  $(\{1, 2, \dots, t\}, +)$  半群不含么  $(\{0, 1, 2, \dots, t\}, +)$  含么半群

例: 设  $S$  为一个非空集. 记  $\text{Aut}(S) := \{f: S \rightarrow S \mid f \text{ 为双射}\}$   
 则映射的合成  $\circ$  为  $\text{Aut}(S)$  上的二元运算且  $(\text{Aut}(S), \circ)$  构成群. ( $S$  的置换群/对称群)

$S_n := \text{Aut}(\{1, 2, \dots, n\})$ .  $S_2 = \{ \begin{smallmatrix} 1 \mapsto 1 \\ 2 \mapsto 2 \end{smallmatrix}, \begin{smallmatrix} 1 \mapsto 2 \\ 2 \mapsto 1 \end{smallmatrix} \}$ .  $S_3 = \dots$

$\tau \circ \sigma: S \xrightarrow{\sigma} S \xrightarrow{\tau} S \Rightarrow \tau \circ \sigma = \tau \circ \sigma \Rightarrow \tau \circ \sigma \in \text{Aut}(S)$

例: 设  $R$  为非零环. 则  $R^\times := \{r \in R \mid r \text{ 乘法可逆}\}$ . 则  $(R^\times, \cdot)$  构成群  
 称为  $R$  的 **单位群**, 也记作  $U(R)$ .

e.g.  $\mathbb{Z}^\times = \{\pm 1\}$ ,  $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ ,  $\dots$

例 :  $GL_2(\mathbb{R}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R}) \mid ad-bc \neq 0 \right\}$ , 则

1)  $GL_2(\mathbb{R})$  关于矩阵乘法, 封闭, 即  $\cdot$  为  $GL_2(\mathbb{R})$  上的二元运算.

2)  $(GL_2(\mathbb{R}), \cdot)$  构成群 (一般线性群), 实际上  $GL_2(\mathbb{R}) = M_2(\mathbb{R})^\times$ .

pf: 1°  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow (ad-bc)(a'd'-b'c') = 1 \Rightarrow ad-bc \neq 0$ .

2°  $ad-bc \neq 0 \Rightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

群的基本性质

性质 : 设  $G$  为群, 则 1) 单位元  $1_G$  唯一; 2) 逆元唯一; 3) 消去律成立.

pf: 1) 设  $e, e'$  均为单位元, 则  $e = ee' = e'$ .

2) 设  $b, c$  均为  $a \in G$  的逆, 则

$$b = b \cdot e = b(ac) = (ba) \cdot c = e \cdot c = c$$

3)  $ab = ac \Rightarrow b = e \cdot b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(ac) = (a^{-1}a) \cdot c = ec = c$

定义 : 设  $(G, \cdot)$  为群,  $H \subseteq G$  为子集. 若  $(H, \cdot)$  为群, 则称  $H$  为  $G$  的子群.

记为  $H \leq G$ . 此外, 若  $H \neq G$ , 则记为  $H < G$ , 称  $H$  为  $G$  的真子群.

性质 : 设  $(G, \cdot)$  为群,  $H \subseteq G$  为非空子集. 则

$$H \text{ 为 } G \text{ 的子群} \Leftrightarrow \begin{cases} a \cdot b \in H & (\forall a, b \in H) \\ a^{-1} \in H & (\forall a \in H) \end{cases} \Leftrightarrow ab^{-1} \in H \quad (\forall a, b \in H).$$

本课程的目的: 介绍一些群环域基本理论及一些基本例子.

并用这些理论来理解初等数论和多项式理论.

$$(R, +, \cdot) = \text{环} \Leftrightarrow \begin{cases} (R, +) = \text{交换群} & \dots (1) \text{-(4)} \\ (R, \cdot) = \text{含么半群} & \dots (5) \text{ \& (7)} \\ +, \cdot \text{ 满足分配律} & \dots (6) \end{cases}$$

$$(R, +, \cdot) = \text{域} \Leftrightarrow \begin{cases} (R, +, \cdot) = \text{交换环} \\ \text{逆元存在} \end{cases} \Leftrightarrow \begin{cases} (R, +) = \text{交换群} \\ (R \setminus \{0\}, \cdot) = \text{交换群} \\ +, \cdot \text{ 满足分配律} \end{cases}$$

## §1.5 同态与同构.

在不同的集合上可构造出不同的代数系统. 在一个代数系统上重要的不是元素本身, 而是它们之间的运算. 例如环中,  $0, 1$  由  $+, \times$  唯一确定.

**定义 (同态)** 设  $(G, \cdot)$  和  $(G', *)$  为两群. 设  $\varphi: G \rightarrow G'$  为映射.

1) 若对任意  $a, b \in G$  有

$$\varphi(ab) = \varphi(a) * \varphi(b) \quad \dots \text{保持乘法}$$

则称  $\varphi$  为 **(群)同态**

2) 若  $\varphi: G \rightarrow G'$  为群同态且  $\varphi$  为双射, 则称  $\varphi$  为 **(群)同构**.

..... 单射, ..... **群的单同态**

满射, ..... **群的满同态**.

**群同态基本性质:**

**性质**: 设  $f: G_1 \rightarrow G_2$  为群同态, 则

1)  $f(1) = 1, f(g^{-1}) = f(g)^{-1}$

2)  $\ker f := f^{-1}(1)$  为  $G_1$  的子群. 称为  $f$  的核 (kernel)

$\operatorname{im} f := \{f(g) \mid g \in G_1\}$  为  $G_2$  的子群. 称为  $f$  的像 (image)

3)  $f$  为同构, 则  $f^{-1}$  也为同构.

4).  $\varphi$  为群的单同态  $\Leftrightarrow \ker \varphi = \{1\}$

**Pf:** 1).  $f(1)f(1) = f(1 \cdot 1) = f(1) \xrightarrow{\text{消掉}} f(1) = 1. f(g^{-1})f(g) = f(g) \cdot f(g^{-1}) = f(1) = 1$

2).  $1 \in \ker f \Rightarrow \ker f \neq \emptyset. 1 = f(1) \in \operatorname{im} f \Rightarrow \operatorname{im} f \neq \emptyset.$

$\cdot \forall g_1, g_2 \in \ker f \Rightarrow f(g_1 g_2^{-1}) = f(g_1) f(g_2)^{-1} = 1 \cdot 1^{-1} = 1 \Rightarrow g_1 g_2^{-1} \in f^{-1}(1)$

$\cdot \forall g'_1 = f(g_1), g'_2 = f(g_2) \in \operatorname{im} f, g'_1 (g'_2)^{-1} = f(g_1) f(g_2)^{-1} = f(g_1 g_2^{-1}) \in \operatorname{im} f.$

3).  $f^{-1}$  为双射. 仅需证其为群同态:

$\forall g', h' \in G_2 \Rightarrow \exists! g, h \in G_1 \text{ s.t. } f(g) = g', f(h) = h'.$

$f(gh) = f(g)f(h) \Rightarrow gh = f^{-1}(f(g)f(h)) \Rightarrow f^{-1}(g') \cdot f^{-1}(h') = f^{-1}(g'h') \quad \square$

4).  $\Rightarrow$ :  $\forall a \in \ker \varphi \Rightarrow \varphi(a) = 1 = \varphi(1) \xrightarrow{\varphi=\text{单}} a = 1 \Rightarrow \ker \varphi = \{1\}.$

$\Leftarrow$ :  $\forall a, b \in G_1$ , 若  $\varphi(a) = \varphi(b) \Rightarrow \varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = 1 \Rightarrow ab^{-1} \in \ker \varphi$   
 $\Rightarrow ab^{-1} = 1 \Rightarrow a = b \Rightarrow \varphi = \text{单}.$



例:  $\det: GL_2(\mathbb{R}) \rightarrow \mathbb{R}^\times$ .  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto ad-bc$  为群同态.

例 ( $GL_2(\mathbb{R})$  的子群): 1) 特殊线性群  $\ker(\det: GL_2(\mathbb{R}) \rightarrow \mathbb{R}^\times)$

$$SL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R}) \mid ad-bc=1 \right\} < GL_2(\mathbb{R})$$

2) 正交群 (全体保持原点的保距变换) = 圆的对称群

$$O_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix}^T = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \right\} < GL_2(\mathbb{R})$$

3) 特殊正交群 (全体保持原点的旋转变换)

$$SO_2(\mathbb{R}) = SL_2(\mathbb{R}) \cap O_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \mid \theta \in \mathbb{R} \right\} < GL_2(\mathbb{R})$$

定义 (同态) 设  $(R, +, \cdot)$  和  $(R', \oplus, *)$  为两环. 设  $\varphi: R \rightarrow R'$  为映射.

1) 若对任意  $a, b \in R$  有

$$\begin{cases} \varphi(a+b) = \varphi(a) \oplus \varphi(b) & \dots \text{保持加法} \\ \varphi(ab) = \varphi(a) * \varphi(b) & \dots \text{保持乘法} \\ \varphi(1_R) = 1_{R'} & \dots \text{保持单位元 (不能去掉!)} \end{cases}$$

则称  $\varphi$  为 (环) 同态

2) 若  $\varphi: R \rightarrow R'$  为环同态且  $\varphi$  为双射, 则称  $\varphi$  为 (环) 同构.

... - 单射, ... (环) 单同态  
... - 满射, ... (环) 满同态.

同构的对象 我们通常看成是一样的. 这是由于, 若

$$f: (K, \varphi_1, \dots, \varphi_m) \xrightarrow{\cong} (L, \psi_1, \dots, \psi_m)$$

则  $K$  上的性质可通过  $f$  搬到  $L$  上, 反之亦然.

性质: 设  $f: R_1 \rightarrow R_2$  为环同态, 则

- 1)  $f(0) = 0, f(1) = 1.$
  - 2)  $f(-a) = -f(a),$
  - 3) 若  $\varphi$  乘法可逆, 则  $f(\varphi^{-1}) = f(\varphi)^{-1}.$
- } 保持特殊元素

4)  $f: (R_1, +) \rightarrow (R_2, +)$  和  $f: (R_1^*, \cdot) \rightarrow (R_2^*, \cdot)$  为群同态

5)  $\text{im} f = \{f(r) \mid r \in R_1\}$  为  $R_2$  的子环.

6) 若  $R_2 \neq 0$ , 则  $\ker f$  不为  $R_1$  的子环. (这里子环必须含 1, 有些书子环不指定含 1, 则  $\ker$  也构成子环)  
但  $\ker f$  关于加, 减, 数乘和封闭. 即.

- $x, y \in \ker f \Rightarrow x \pm y \in \ker f$
  - $r \in R_1, x \in \ker f \Rightarrow r \cdot x, xr \in \ker f.$
- } 满足这一性质的非空子集称为环的理想

7)  $f$  为单同态  $\Leftrightarrow \ker f = \{0\}$

Pf: 1).  $f(0) = f(0+0) = f(0) + f(0) \Rightarrow \checkmark$

$f(1) = 1$  (定义)

2).  $f(g) + f(-g) = f(g-g) = f(0) = 0 \Rightarrow \checkmark$

3).  $f(g) \cdot f(g^{-1}) = f(gg^{-1}) = f(1) = 1 = f(g^{-1}g) = f(g^{-1}) \cdot f(g)$

4).  $f(g+h) = f(g) + f(h), f(gh) = f(g)f(h).$

5).  $1 = f(1) \in \text{im}(f)$

$f(r_1) - f(r_2) = f(r_1 - r_2) \in \text{im}(f)$

$f(r_1)f(r_2) = f(r_1r_2) \in \text{im}(f)$

6).  $R_2 \neq 0 \Rightarrow f(1) = 1 \neq 0 \Rightarrow 1 \notin \ker f \Rightarrow \ker f$  不为子环.

$x, y \in \ker f \Rightarrow f(x \pm y) = f(x) \pm f(y) = 0 \Rightarrow x \pm y \in \ker f.$

$r \in R_1, x \in \ker f \Rightarrow f(rx) = f(r)f(x) = 0 \Rightarrow rx \in \ker f.$

7).  $\varphi: (R_1, +) \rightarrow (R_2, +)$  为群同态. 因此

$\varphi$  为环的单同态  $\Leftrightarrow \varphi$  为群的单同态  $\Leftrightarrow \ker \varphi = \{0\}.$

例：复共轭为  $\mathbb{C}$  上环自同构。(域自同构)

pf:  $\forall r \in \mathbb{R}, \bar{r} = r$  (特别地,  $\bar{1} = 1$ )  $\cdot$  复共轭为双射.

$$\overline{(a+bi) + (c+di)} = \overline{a+bi} + \overline{c+di}$$

$$\overline{(a+bi) \cdot (c+di)} = \overline{a+bi} \cdot \overline{c+di}$$

例:  $\varphi: \mathbb{Z} \rightarrow \{\overset{1}{\text{对}}, \overset{0}{\text{错}}\}$  (环代数)  $2n \mapsto \text{错}, 2n+1 \mapsto \text{对}$

例: 设  $K$  为域, 设  $M_2(K)$  为  $K$  上的 2 阶矩阵代数. 则

$$K \rightarrow M_2(K) \quad a \mapsto \begin{pmatrix} a & \\ & a \end{pmatrix}$$

为环的单同态.

例: 设  $\varphi: \mathbb{C} \rightarrow M_2(\mathbb{R}) \quad a+bi \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ , 则

1)  $\varphi$  为环的单同态

2)  $\varphi: \mathbb{C}^* \rightarrow GL_2(\mathbb{R})$  为群的单同态, 且诱导群同构

$$S^1 \xrightarrow{\cong} SO_2(\mathbb{R})$$

例: 若  $T$  为环  $R$  的子环, 则  $\varphi: T \rightarrow R \quad t \mapsto t$  为环的单同态.

例(四元数体): 设  $\mathbb{H} := \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{C} \right\} \subseteq M_2(\mathbb{C})$ . 则

$(\mathbb{H}, +, \cdot)$  满足域的定义中的 (1)-(8), 但不满足 (9), 即  $(\mathbb{H}, +, \cdot)$  为非交换环, 且任意非零元可逆.

$$\text{记 } i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \quad \text{则 } \mathbb{H} = \mathbb{Q} \cdot 1 + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$$

$$\cdot i, j, k \in \mathbb{H}, \text{ 且 } i^2 = j^2 = k^2 = ijk = -1$$

$$\cdot ij = k = -ji, jk = i = -kj, ki = j = -ik$$

例(环的中心)  $R$  为环.  $C(R) := \{r \in R \mid \forall a \in R, ra = ar\}$ . 则

$$C(R) \text{ 为 } R \text{ 的交换子环. eg. } C(\mathbb{H}) = \left\{ \begin{pmatrix} r & \\ & r \end{pmatrix} \mid r \in \mathbb{R} \right\} \cong \mathbb{R}.$$

定义: 设  $(R, +, \cdot)$  为交换环. 若对任意  $a, b \in R \setminus \{0\}$  有  $ab \neq 0$ , 则称  $R$  为 **整环**.

性质: **整环 = 交换环 + 消去律**

$$\hookrightarrow \text{i.e.} \begin{cases} ab=ac & \xrightarrow{a \neq 0} b=c \\ ba=ca & \xrightarrow{a \neq 0} b=c \end{cases}$$

pf:  $\Rightarrow$ : 若  $ab=ac$  且  $a \neq 0 \Rightarrow a(b-c)=0 \xrightarrow[\text{整环}]{a \neq 0} b-c=0 \Rightarrow b=c \Rightarrow \checkmark$

$\Leftarrow$ :  $\forall a, b \in R \setminus \{0\}$ , 若  $ab=0$ , 则  $ab=a \cdot 0 \xrightarrow[\text{消去律}]{a \neq 0} b=0$  矛盾!

$$\{\text{域}\} \subsetneq \{\text{整环}\} \subsetneq \{\text{交换环}\} \subsetneq \{\text{环}\}$$

从已知环构造更大的环 (多项式环) 习题: 全体实系数多项式构成环. 更一般地:

设  $R$  为非零交换环. 任取  $a_0, a_1, \dots, a_n \in R$

$R$  上的多项式:

$$f = \underbrace{a_0}_{\text{常数项}} + a_1 x + \dots + \underbrace{a_n}_{\text{首项系数 (若 } a_n \neq 0)} x^n$$

记作  $\deg(f)$   
次数 (若  $a_n \neq 0$ )

- 首-多项式
- 零多项式 ( $\deg(0) = -\infty$ )
- 常多项式

-  $R[x] = \{\text{全体 } R \text{ 上的多项式}\}$

$$+ : \sum_i a_i x^i + \sum_j b_j x^j = \sum_i (a_i + b_i) x^i$$

$$\therefore \left( \sum_i a_i x^i \right) \cdot \left( \sum_j b_j x^j \right) = \sum_k \left( \sum_{i+j=k} a_i b_j \right) x^k$$

性质: 1)  $(R[x], +, \cdot)$  构成交换环.

2)  $R \subseteq R[x]$  为子环.  $0_{R[x]} = 0_R \quad 1_{R[x]} = 1_R$

3)  $-\left(\sum_i a_i x^i\right) = \sum_i (-a_i) x^i$

4)  $\forall a \in R$ , **赋值映射**  $R[x] \rightarrow R \quad f(x) \mapsto f(a)$  为环满同态.

性质: 设  $f, g \in R[x], \mathbb{R}$

$$1) \deg(f+g) \leq \max(\deg(f), \deg(g))$$

$$2) \deg(f \cdot g) \leq \deg(f) + \deg(g)$$

3) 若  $R$  为整环, 则  $R[x]$  也为整环. 且

$$\deg(f \cdot g) = \deg(f) + \deg(g)$$

递归地, 可定义:  $R[x_1, x_2, \dots, x_n] := R[x_1, \dots, x_{n-1}][x_n]$ .

$$f = \sum_{i_1, i_2, \dots, i_n} a_{i_1, i_2, \dots, i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \quad (\text{有限和})$$

$$\deg(f) = \begin{cases} \max\{\bar{i}_1 + \bar{i}_2 + \dots + \bar{i}_n \mid a_{\bar{i}_1, \dots, \bar{i}_n} \neq 0\} & f \neq 0 \\ -\infty & f = 0 \end{cases}$$

$$\deg_{x_i}(f) = \begin{cases} \max\{\bar{i}_k \mid a_{\bar{i}_1, \dots, \bar{i}_n} \neq 0\} & f \neq 0 \\ -\infty & f = 0 \end{cases}$$

单项式:  $a x_1^{\bar{i}_1} \dots x_n^{\bar{i}_n}$

若  $f$  的非零单项式均为  $d$  次, 则称  $f$  为  $d$  次齐次多项式.

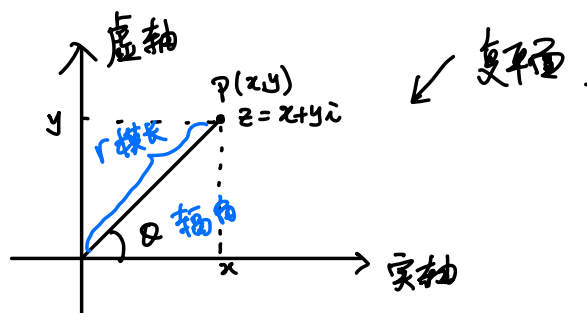
例:  $R[x, y] := R[x][y]$

$$\begin{cases} \cdot \deg(x^2 + x^2y + y) = 3 \\ \cdot \deg_x(x^2 + x^2y + y) = 2 \\ \cdot \deg_y(x^2 + x^2y + y) = 1 \end{cases} \quad x^3 + 3x^2y + 4xy^2 + 7y^3 \text{ 为 3 次齐次多项式.}$$

## 复数的三角表示与乘法的几何解释:

$$z = x + iy$$

$\uparrow$        $\uparrow$   
 实部    虚部  
 $\operatorname{Re} z$      $\operatorname{Im} z$



三角表示:  $z = r(\cos \theta + i \sin \theta)$

性质:  $z_1 = r_1(\cos \theta_1 + i \sin \theta_1)$ ,  $z_2 = r_2(\cos \theta_2 + i \sin \theta_2)$  则

$$z_1 z_2 = r_1 r_2 (\cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2))$$

Pf:  $\cos(\theta_1 + \theta_2) = \cos \theta_1 \cos \theta_2 - \sin \theta_1 \sin \theta_2$

$\sin(\theta_1 + \theta_2) = \sin \theta_1 \cos \theta_2 + \cos \theta_1 \sin \theta_2$  □

Euler 公式  $e^{i\theta} = \cos \theta + i \sin \theta$ .

$\uparrow$  暂时看成 - 个记号

性质: 1)  $r_1 e^{i\theta_1} \cdot r_2 e^{i\theta_2} = (r_1 r_2) e^{i(\theta_1 + \theta_2)}$

2) (de Moivre)  $(r e^{i\theta})^n = r^n \cdot e^{in\theta}$ ,  $\forall n \in \mathbb{Z}$

复数乘法的几何解释:  $w = r(\cos \theta + i \sin \theta)$   $z \xrightarrow{\text{伸缩}} rz \xrightarrow{\text{旋转}} wz$

例 (子群)  $\mu_n \subset \mu_\infty = \bigcup_{n \geq 1} \mu_n \subset S^1 \subset \mathbb{C}^*$

$$\mu_n = \left\{ e^{\frac{2k\pi i}{n}} \mid 0 \leq k \leq n-1 \right\}$$

$\uparrow$   $n$  次单位根

任取  $\zeta \in \mu_n$ , 若对任意  $1 \leq m < n$ ,  $\zeta^m \neq 1$ , 则称  $\zeta$  为  $n$  次本原单位根

### 半群 $(G, \cdot)$

- 1) 乘法结合律

### 含么半群 $(G, \cdot)$

- 1) 乘法结合律
- 2) 单位元存在性

### 群 $(G, \cdot)$

- 1) 乘法结合律
- 2) 单位元存在性
- 3) 逆元存在性

### 交换半群 $(G, \cdot)$

- 1) 乘法结合律
- 4) 乘法交换律

### 含么交换半群 $(G, \cdot)$

- 1) 乘法结合律
- 2) 单位元存在性
- 4) 乘法交换律

### 交换群 $(G, \cdot)$

- 1) 乘法结合律
- 2) 单位元存在性
- 3) 逆元存在性
- 4) 乘法交换律

### 交换群 $(G, +)$

- 1) 加法结合律
- 2) 零元存在性
- 3) 负元存在性
- 4) 加法交换律

### (不含么)环 $(R, +, \cdot)$

- 1) - 4):  $(R, +)$  为交换群
- 5) 分配律
- 6) 乘法结合律

### (含么)环 $(R, +, \cdot)$

- 1) - 4):  $(R, +)$  为交换群
- 5) 分配律
- 6) 乘法结合律
- 7) 单位元存在性

### 除环 $(D, +, \cdot)$

- 1) - 4):  $(R, +)$  为交换群
- 5) 分配律
- 6) 乘法结合律
- 7) 单位元存在性
- 8) 逆元存在性

### (不含么)交换环 $(R, +, \cdot)$

- 1) - 4):  $(R, +)$  为交换群
- 5) 分配律
- 6) 乘法结合律
- 9) 乘法交换律

### (含么)交换环 $(R, +, \cdot)$

- 1) - 4):  $(R, +)$  为交换群
- 5) 分配律
- 6) 乘法结合律
- 7) 单位元存在性
- 9) 乘法交换律

### 域 $(R, +, \cdot)$

- 1) - 4):  $(R, +)$  为交换群
- 5) 分配律
- 6) 乘法结合律
- 7) 单位元存在性
- 8) 逆元存在性
- 9) 乘法交换律

