第二章 代数基础

第二部分 环

- 2.4 环的概念
- 2.5 子环、理想与商环
- 2.6 环同态与多项式环

第二章 代数基础

第二部分 环

2.4 环的概念

2.5 子环、理想与商环

2.6 环同态与多项式环

引入

- 很多集合上可以定义两种代数运算，运算之间的关系?
  - ✓ 整数的加法和乘法
  - ✓ 有理数、实数加法和乘法
  - ✓ 矩阵加法和乘法
  - ✓ Z_n 加法和乘法

引入

- 很多集合上可以定义两种代数运算，运算之间的关系?

$$x \cdot (y + z) = x \cdot y + x \cdot z$$

学习目标

- 能阐述环定义
- 能解释环的性质
- 能阐述特殊环定义

2.4 环的定义

定义2.1 设 G 是一个非空集合， $\cdot$ 是 G 上的一个代数运算，如果该运算满足如下性质：

（1）结合律：$(a \cdot b) \cdot c = a \cdot (b \cdot c)$

则称 $(G, \cdot)$为一个**半群（Semigroup）**。

例1：$(Z_n, \otimes)$ 是半群。

例2：整数集合Z关于乘法运算构成半群。

2.4 环的定义

定义 2.2 设 R 是一个非空集合，如果在 R 中定义了两个代数运算 $+$ 和 $\cdot$ ，并且两个代数运算满足：

（1）$(R,+)$为一个交换群；

（2）$(R,\cdot)$ 为一个半群；

（3）对任意 $x,y,z\in R$，双边分配律成立

$$x\cdot(y+z)=x\cdot y+x\cdot z$$
$$(x+y)\cdot z=x\cdot z+y\cdot z$$

则称 $(R,+,\ \cdot)$ 为一个环（Ring）。

注：为了方便起见，通常记 $x\cdot y=xy$。

2.4 环的定义

- 环中加法单位元称为零元，通常记为0；环中元素a关于加法逆元记为$-a$，一般记$a-b=a+(-b)$。

- 环关于乘法可能没有单位元，如全体偶数构成环，如果环关于乘法有单位元，则就称为环的单位元，通常记为1。环中元素a关于乘法逆元如果存在，记为a^{-1}.

- 环加法子群如构成环则称为子环。

2.4 常见环的例子

问题1. 集合**(Z,+,×)**，**(Q,+,×)**，**(R,+,×)**是否构成环？

问题2. 实数域R上n阶方阵$(R^{n\times n},+,\times)$是不是环？

问题3. 模n的剩余类$(Z_n,\oplus,\otimes)$是不是环？

问题4. 集合**(Q, ×, +)** 是否构成环？

2.4 常见环的例子

例3 整数环(**Z**,+, ×)，有理数环(**Q**,+,×)， 实数环(**R**,+,×)， 复数环(**C**,+,×) .

例4 高斯整数环 $(Z[i]=\{a+bi \mid a,b\in Z\},+,\times)$

例5 实数域R 上n阶方阵环 $(R^{n\times n},+,\times)$

例6 模 $\boldsymbol{n}$ 的剩余类环 $(\mathbf{Z}_{\boldsymbol{n}},\oplus,\odot)$ 构成环.

例7 全体偶数P 关于加法和乘法构成环(**P**,+,×).

2.4 常见环的例子

例6 模 n 的剩余类环 $(Z_n,\oplus,\odot)$ 构成环

证： 运算 $\oplus,\odot$ 定义为 $x\oplus y = x+y \bmod n$， $x\odot y = xy \bmod n$。易知，$\oplus,\odot$ 满足封闭性。

1. $(Z_n,\oplus)$ 为交换群：结合律和交换律易证，零元为 0， x 的逆元为 $n-x$。

2. $(Z_n,\odot)$ 为半群：结合律易证。

3. 分配律：

$$x\odot(y\oplus z) = x(y+z \bmod n) \bmod n = xy + xz \bmod n$$

$$= (xy \bmod n) + (xz \bmod n) \bmod n$$

$$= (x\odot y)\oplus(x\odot z)$$

。右分配律同证。

2.4 环的基本性质

你觉得关于环R元素运算关系，如下哪几个正确？

1）$a0=0=0a$.

2）$-ab=(-a)b$，

3）$a-a=0$.

4）如果$a+b=c$，则$b=c-a$.

5）$-(a+b)=-a-b$，

6）如果$ab=ac$，则$b=c$.

7）$a+b=b+a$

2.4 环的基本性质

定理 2.3 在环R中，如下几个性质成立

1） $a0=0=0a$.

2） $-ab=(-a)b$，

3） $a-a=0$.

4） 如果$a+b=c$，则$b=c-a$.

5） $-(a+b)=-a-b$，

6） $-(a-b)=-a+b$.

7） $\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right)=\sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$

2.4 常见环的例子

证2)：环 R 中，$-a\cdot b=(-a)\cdot b$

由分配律，$(-a)\cdot b+a\cdot b=\big((-a)+a\big)\cdot b=0\cdot b=0$

故 $(-a)\cdot b=-a\cdot b$。

证5)：$-(a+b)=(-a)+(-b)$

由交换律和结合律，

$$\begin{aligned}(-a)+(-b)+(a+b)&=(-a)+(a+b)+(-b)\\&=\big((-a)+a\big)+\big(b+(-b)\big)\\&=0+0=0\end{aligned}$$

2.4 常见环的例子

证7)：环 R 中，$(\sum_{i=1}^{n} a_i)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$

由分配律和交换律，

$$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right)$$

$$= \left(\sum_{i=1}^{n} a_i\right) b_1 + \cdots + \left(\sum_{i=1}^{n} a_i\right) b_m$$

$$= (a_1 b_1 + \cdots + a_n b_1) + \cdots + (a_1 b_m + \cdots + a_n b_m)$$

$$= \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$$

2.4 环的补充概念

定义 2.4 在环R中，令$R^* = R\backslash\{0\}$

1) R为交换环：R为环，并且$(R, \cdot)$满足交换律。

2) R为体：R为环，并且$(R^*, \cdot)$为群。

3) R为域：R为环，并且$(R^*, \cdot)$为交换群。

2.4 环的补充概念

例10　整数环是交换环，有理数环是域，实数环是域，复数环是域。

例11 高斯整数环$Z[i]=\{a+bi \mid a,b\in Z\}$是交换环。

例12 模 $\boldsymbol{n}$ 的剩余类环，当 $\boldsymbol{n}$ 是素数时是域。

2.4 环的补充概念

定义 2.5 设 R 为环，$0 \neq a, 0 \neq b \in R$，如果 $ab = 0$，则称 a, b 为 R 中**零因子**。

例13　环Z_{26}中13与2都是零因子。

定义 2.6 无零因子的交换环称为**整环**。

注： $(R, +, \cdot)$ 为整环，$0 \neq a \in R$，则 $xa = ya \Leftrightarrow x = y$

2.4 环的补充概念

注：$(R,+,\cdot)$ 为整环，$0 \neq a \in R$，则 $xa = ya \Leftrightarrow x = y$

证：$\Rightarrow$ $xa = ya$，则

$$xa - ya = xa + (-y)a = (x-y)a$$

由于 $(R,+,\ \cdot)$ 是整环，

$$(x-y)a = 0 \Leftrightarrow x-y = 0 \text{ 或 } a = 0$$

由于 $a \neq 0$，故 $x-y=0$，即 $x=y$。

$\Leftarrow$ 显然。

总结

- 环定义
- 环的性质
- 特殊环(交换环、域，体，整环)

第二章 代数基础

第二部分 环

2.4 环的概念

2.5 子环、理想与商环

2.6 环同态与多项式环

学习目标

- 能阐述理想定义
- 能判断集合是否为理想
- 能阐述主理想定义

本小节引入

问题：模9加群G={0,1,2,3,4,5,6,7,8}，正规子群H={0,3,6}是不是子环？是不是理想？

问题：模7乘群G={1,2,3,4,5,6}，正规子群H={1,6}是不是子环？是不是理想？

本小节引入

- 子环的定义

定义 如果 $\boldsymbol{R}$ 是一个环，$\boldsymbol{S}$ 为 $\boldsymbol{R}$ 的非空子集，若

1. 对任意的 $\boldsymbol{a}, \boldsymbol{b} \in \boldsymbol{S}$，$\boldsymbol{a} - \boldsymbol{b} \in \boldsymbol{S}$;
2. 对任意的 $\boldsymbol{a}, \boldsymbol{b} \in \boldsymbol{S}$，$\boldsymbol{ab} \in \boldsymbol{S}$,

则称 $\boldsymbol{S}$ 为 $\boldsymbol{R}$ 的子环。

2.5 理想的定义

定义 2.7 设 I 为环 R 的加法子群，并且对 $\forall a \in I$，$\forall r \in R$，均有 $ar, ra \in I$，则称 I 为 R的理想(Ideal)。

问题：全体整数是不是有理数环的理想?

答：否。记 $\langle \boldsymbol{Z}, +, \cdot \rangle$ 和 $\langle \boldsymbol{Q}, +, \cdot \rangle$，显然$\langle \boldsymbol{Z}, + \rangle \lhd \langle \boldsymbol{Q}, + \rangle$，但是，$\forall\, \boldsymbol{z} \in \boldsymbol{Z}, \boldsymbol{q} \in \boldsymbol{Q}$，不一定 $\boldsymbol{zq} \in \boldsymbol{Z}$，故不是理想。

问题：全体偶数是不是整数环的理想?

答：是。记 $\langle \boldsymbol{E}, +, \cdot \rangle$ 和 $\langle \boldsymbol{Z}, +, \cdot \rangle$，显然$\langle \boldsymbol{E}, + \rangle \lhd \langle \boldsymbol{Z}, + \rangle$，$\forall\, \boldsymbol{2k} \in \boldsymbol{E}, \boldsymbol{l} \in \boldsymbol{Z}$，有 $(\boldsymbol{2k})\boldsymbol{l} \in \boldsymbol{E}$，$\boldsymbol{l}(\boldsymbol{2k}) \in \boldsymbol{E}$，是理想。

2.5 理想的定义

例1 $\{0\}$与R都是R的理想。

例2 对每个正整数n，令 $I=(n)=\{kn \mid k\in Z\}$
则 $I=(n)$ 为 Z 的理想.

例3　环**R**的任意多个理想的交仍为理想.

2.5 理想的性质

- 设 I 为环 R 的理想，则

问题1：I 是否一定包含 R 的零元？ √

问题2：I 是否一定包含 R 的单位元？ 不一定！

问题3：I 关于环的运算是否构成子环？ √

问题4：子环一定是理想？ 不一定！

2.5 理想的性质

定理 2.8 设 R 是一个环，设 I 为 R 的理想，则

1）I 一定包含 R 的零元

2）I 为 R 的子环

3）如果 I 有单位元，则 $I=R$。

2.5 理想的性质

定理 2.8 设 R 是一个环，设 I 为 R 的理想，则

证：1）I 一定包含 R 的零元。

因为 $\langle I,+\rangle$ 是 $\langle R\ +\rangle$ 的加法子群，故 $\langle I,+\rangle$ 一定包含 R 的零元。

2）I 为 R 的子环。

由理想的定义知，对任意的 $a,b\in I$，$ab\in I$，故 I 为 R 的子环。

3）如果 I 有单位元，则 $I=R$。

若 $e\in I$，则对任意的 $a\in R$，$ea\in I$，故 $a\in I$，因此，$I=R$。

2.5 理想判定定理

定理 2.9 设 R是一个交换环，I 是 R 的一个非空子集，当以下条件成立时，I 是 R 的一个理想：

（1）对于任意 $a, b \in I$，$a-b \in I$.

（2）对于任意 $a \in I$ 和 $r \in R$，有 $ar \in I$.

证：由（1）知，I 是 R 的加法子群。

又由 R 是一个交换环，条件（2）为对于任意 $a \in I$ 和 $r \in R$，有 $ar \in I$，故 $ra \in I$。因此，I 是 R 的理想。

2.5 主理想定义

定义 2.10 设 R 是一个交换环，I 是 R 的一个理想，若

$$I=\{ar \mid r\in R\}$$

则称 I 是 R 的一个**主理想**。由一个元素 a 生成的主理想可以表示为 $I=(a)$。

2.5 主理想定义

例 整数环 $\langle Z,+,\cdot\rangle$的任何理想都是主理想。

证：设 I 为 Z 中任意理想，

1. 如果 $I=\{0\}$ 为零理想，则 $I=(0)$。
2. 如果 $d>0$ 为 I 中最小正整数，则对每个 $a\in I$，存在 $b,r\in Z$，$0\le r<d$ 使得

$$a=bd+r$$

由于 I 为理想，且 $d\in I$，则 $bd\in I$，故

$$r=a-bd\in I$$

由于 d 为 I 中最小正整数，于是 $r=0$，从而 $d\mid a$，即 $I=(d)$，I 为主理想。

2.5 商环的定义

定理2.10 设$(R,+,\cdot)$为环，I 为R 的理想， 在商群

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

中定义如下乘法：$\forall(\boldsymbol{I + a}),(\boldsymbol{I + b}) \in \boldsymbol{R/I}$, 有

$$(\boldsymbol{I + a}) *_I (\boldsymbol{I + b}) = \boldsymbol{I} + (\boldsymbol{a} \cdot \boldsymbol{b})$$

则 $(R/I, \oplus_I, *_I)$ 为一个环，称之为商环.

例1：记 $R = Z$, $I = (n)$，则 $(R/I, \oplus_I, *_I)$ 为商环.

第二章 代数基础

第二部分 环

- 2.4 环的概念
- 2.5 子环、理想与商环
- 2.6 环同态与多项式环

引入

- 已知全班同学考试成绩的密文，如果加密是加法同态加密，此时可以直接求总成绩的密文
- 如何求成绩的方差?

学习目标

能描述商环的概念和商环的两个运算

解释环同态基本定理

2.6 环同态定义

定义2.11 设环$(R_1,+,\cdot)$和$(R_2,\oplus,\otimes)$,f 是从 R_1 到 R_2 的映射，如果满足：

(1) $\forall\, a,b\in R_1$, $\quad f(a+b)=f(a)\oplus f(b)$

(2) $\forall\, a,b\in R_1$, $\quad f(a\cdot b)=f(a)\otimes f(b)$

则称 f 为从 R_1到 R_2的环同态映射。特别的, 如果

f 为满射，则称 f 为满同态，记为 $R_1 \sim R_2$。

如果 f 为双射，则称 R_1 与 R_2 同构，记为 $R_1 \cong R_2$

例 证明 $\sigma: a+bi \to a-bi$ 是复数域 C 到自身的同构映射。

证： σ 是复数域 C 到自身的双射, 对任意的$a+bi, c+di \in C$

$$(a+bi)+(c+di)=(a+c)+(b+d)i$$

$$(a+bi)(c+di)=(ac-bd)+(ad+bc)i$$

根据 σ 的定义，有

$\sigma\big((a+bi)+(c+di)\big)=\sigma\big((a+c)+(b+d)i\big)=(a+c)-(b+d)i \ =(a-bi)+(c-di)=\sigma(a+bi)+\sigma(c+di)$

$\sigma\big((a+bi)(c+di)\big)=\sigma\big((ac-bd)+(ad+bc)i\big)=(ac-bd)-(ad+bc)i=(a-bi)(c-di)$
$=\sigma(a+bi)\sigma(c+di)$

2.6 环同态基本定理

定理2.12 (环同态基本定理)

设 f 是从环 R_1 到 R_2 的满同态，则加法群同态的核

$$ker f = \{ r \in R_1 \mid f(r) = 0 \}$$

满足

（1）$ker f$ 为 R_1 的理想

（2）$R_1 / ker f \cong R_2$

小节

- 商环的概念和商环的两个运算
- 环同态基本定理

引入

问题1　Z上的多项式全体Z[*x*]关于加法和乘法运算构成环吗？

问题2　Q上的多项式全体Q[*x*]关于加法和乘法运算构成环吗？

学习目标

- 能描述多项式环的概念
- 能计算两个多项式乘法、加法、次数

2.6 多项式的定义

定义2.13　设$(R,\oplus,\otimes)$是有单位元的交换环，称

$$f(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}+a_nx^n$$

是R上关于x的**多项式**，其中x是不定元，$a_i\in R$。

全体多项式记为$R[x]$。

2.6 多项式的定义

- a_0x^0 等价为 a_0
- 系数为单位元的系数可以省略不写, $1x^i$为可简记为 x^i
- 系数为零元的多项式可以省略不写，则R上关于x的多项式可以简单记为

$$f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n$$

$$= \sum_{i=0}^{n} a_ix^i, \quad a_i \in R$$

2.6 多项式的定义

- 如果 $a_n \neq 0, a_i = 0\ (i > n)$，则称
  - $a_n x^n$ 为 $f(x)$ 的首项，
  - a_n称为首项系数，
  - n 是多项式 $f(x)$ 的次数，记为

$$\deg(f(x)) = n$$

- 如果 $a_n = 1$，则称 $f(x)$为首一多项式。
- 当 a_i 全为 0 时，记为 $f(x) = 0$，称为零多项式。

2.6 多项式的定义

例1 环 Z上的多项式 $f(x) = 13x^{0}+x+5x^{2}+4x^{4}+x^{6}$是首一多项式，且次数为6。

2.6 多项式环

定理2.14 对于$R[x]$中的任意两个多项式

$$f(x) = a_0 x^0 + a_1 x + \ldots + a_{n-1} x^{n-1} + a_n x^n, \quad a_i \in R,$$

$$g(x) = b_0 x^0 + b_1 x + \ldots + b_{m-1} x^{m-1} + b_m x^m, \quad b_j \in R,$$

则$R[x]$关于如下加法和乘法构成环，称为R上的**多项式环**

$$f(x) + g(x) = \sum_{i=0}^{\max\{m,n\}} (a_i \oplus b_i) x^i$$

$$f(x) \cdot g(x) = \sum_{k=0}^{m+n} \Big(\sum_{i+j=k} a_i \otimes b_j \Big) x^k$$

2.6 多项式环

- $R[x]$有单位元吗，是交换环吗？
- $R[x]$零元是什么？
- 如果R有可逆元，则$R[x]$中也有可逆元？

2.6 多项式环

定理2.15 对于多项式环$R[x]$

- R单位元为$R[x]$单位元
- R的零元为$R[x]$零元
- $R[x]$中的可逆元是R的可逆元

2.6 多项式环

例 2 求环 Z_2 上的两个多项式相加和相乘的结果

$$f(x) = 1+x+x^2+x^4+x^6，\quad g(x) = 1+x+x^7$$

$$f(x) + g(x) = x^2+x^4+x^6+x^7$$

$$f(x)g(x) = 1+x^3+x^4+x^5+x^6+x^8+x^9+x^{11}+x^{13}$$

2.6 多项式运算次数关系

例3 求环 Z_2上的两个多项式相加和相乘后的多项式代数次数

$$f(x) = 1+x+x^2,\quad g(x) = 1+x+x^2$$

$$\deg(f+g)=0,\ \deg(fg)=4$$

例4 求环 Z_6上的两个多项式相加和相乘后的多项式代数次数

$$f(x) = 1+x+2x^2,\quad g(x) = 1+x+3x^3$$

$$\deg(f+g)=3,\ \deg(fg)=4$$

2.6 多项式运算次数关系

定理2.16 对于$R[x]$中的任意两个多项式

$$f(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + a_nx^n\text{，}\quad a_i \in R,$$

$$g(x) = b_0 + b_1x + \ldots + b_{m-1}x^{m-1} + b_mx^m\text{，}\quad b_j \in R,$$

则:

$$\deg(f(x)+g(x)) \le \max\{\deg(f(x)), \deg(g(x))\}$$

$$\deg(f(x)g(x)) \le \deg(f(x)) + \deg(g(x))$$

且当R是整环时:

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

小结

- 多项式环的概念
- 两个多项式乘法、加法、次数