环论基本概念

讨论班

梁家浩

华南理工大学数学学院

2024.3.11

Contents

环 (Ring) 的概念和细分

环的定义

环

集合 R 上定义了两种二元运算 $+,\cdot$ 使得

- $(R,+)$ 是交换群.
- $(R,\cdot)$ 是半群.
- 满足左右分配律

$$\forall a,b,c\in R, a\left(b+c\right)=ab+ac, \left(b+c\right)a=ba+ca$$

则称 $(R,+,\cdot)$ 是一个环 (ring).

有大量环的例子

- $\mathbb{Z},\mathbb{Z}\left[\sqrt{d}\right],\mathbb{Z}_m,\mathbb{Q},\mathbb{R},\mathbb{R}^n,C^k\left[a,b\right],C^\infty\left[a,b\right],\mathbb{P}^{n\times n}\ldots$
- 环上的多项式也是环 $R\left[x\right]:\mathbb{Z}\left[x\right],\mathbb{Q}\left[x\right],\mathbb{P}\left[x\right],\mathbb{P}\left[x,y\right],\mathbb{Z}_m\left[x\right]\ldots$

基本性质

命题

容易验证环 R 满足以下性质 $\forall a, b \in R, 0 \in R, m, n \in \mathbb{Z}$

- $(m+n)a = ma + na, m(-a) = -ma$
- $m(na) = m(na), m(a+b) = ma + mb$
- $a^m a^n = a^{m+n}, (a^m)^n = a^{mn}$
- $a0 = 0a = 0, (-a)b = -ab$
- $$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$$
- $(na)(mb) = (mn)(ab)$.

注意：在一般的环中 $ab = 0$ 不一定有 $a = 0$ 或 $b = 0$. 若 $R = 0$, 则称 R 是零环。

幺元 (identity)、单位 (unit)、零因子

定义

对于环 R, 定义

- $R^* := R - \{0\}$
- 单位： R^* 中的可逆元
- 单位群： 单位全体构成一个群
  $U(R) := \left\{a \in R^* | \exists a^{-1} \in R^*, aa^{-1} = a^{-1}a = 1\right\}$
- 幺元 $1 \in R$: 指 $(R, \cdot)$ 中存在的幺元。
- 零因子： 若存在
  $$a, b \in R^*, ab = 0$$
  则称 a 为左零因子，b 称为右零因子，统称零因子。

- 环 $\mathbb{Z}_4$ 存在零因子 [2].
- Gauss 整环 $\mathbb{Z}[i]$ 的单位群 $\{1, i, -1, -i\}$
- 练习： 求环 $\mathbb{Z}[\sqrt{5}], \mathbb{Z}_9$ 的单位群。

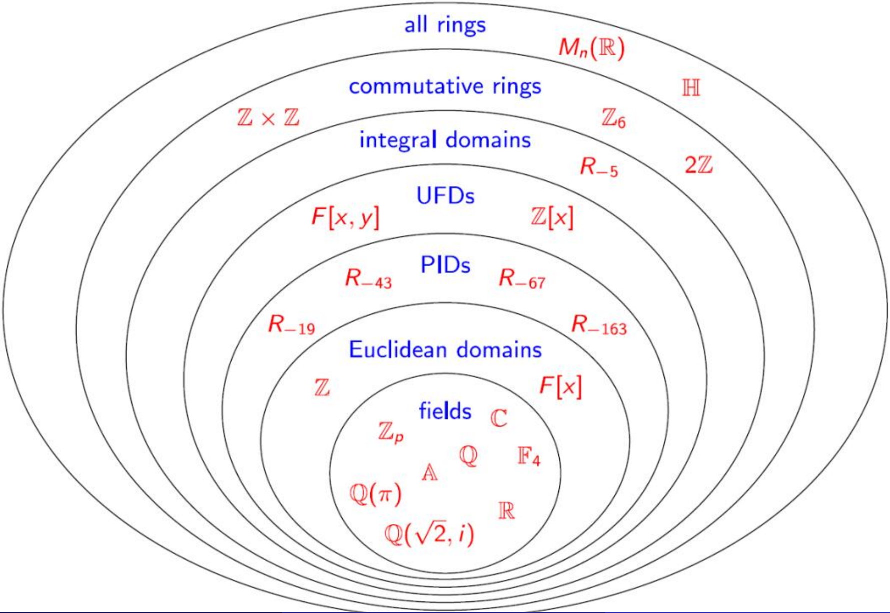
环的细分 (根据 R^* 乘法运算的性质

假设 R 是一个环，有以下定义

1. 若 R^* 关于乘法运算封闭 (即无零因子)，则 R 称为**无零因子环**。
2. 若 R^* 包含幺元，则称 R 是**幺环 unitary ring**。
3. 若 R^* 关于乘法可交换，则称 R 是**交换环 commutative ring**。
4. 若 $R^* = U(R)$，则称 R 是**除环 Division ring**。
5. 若同时满足 1.2.3 则称为**整环 domain=integral domain**(环论主要研讨的对象)。
6. 同时满足 1.2.3.4 则称为**域 field**。

	封闭	单位元	逆元	交换
幺环		●		
交换环				●
无零因子环	●			
整环	●	●		●
除环/体	●	●	●	
域	●	●	●	●

代表性的例子



all rings
$M_n(\mathbb{R})$
commutative rings
$\mathbb{H}$
$\mathbb{Z} \times \mathbb{Z}$
$\mathbb{Z}_6$
integral domains
R_{-5}
$2\mathbb{Z}$
UFDs
$F[x, y]$
$\mathbb{Z}[x]$
PIDs
R_{-43}
R_{-67}
R_{-19}
R_{-163}
Euclidean domains
$\mathbb{Z}$
$F[x]$
fields
$\mathbb{Z}_p$
$\mathbb{C}$
$\mathbb{Q}$
$\mathbb{F}_4$
$\mathbb{A}$
$\mathbb{Q}(\pi)$
$\mathbb{R}$
$\mathbb{Q}(\sqrt{2}, i)$

练习

设 R 是一个环

1. 若 $|R| = p$ 是素数，求证 R 是交换环。
2. 若 $\forall a \in R, a^2 = a$ 则称 R 是布尔环，求证: 布尔环必为交换环。并且 $\forall a \in R, 2a = 0$.
3. 验证布尔环的例子并验证是不是幺环。

$$R = 2^X, A \backslash B := \{a \in A | a \notin B\}$$

$$A + B := (A \backslash B) \cup (B \backslash A)$$

$$AB := A \cap B$$

4. 设 R 是幺环，a 是幂零元 (i.e. $\exists m, a^m = 0$)，求证:
    - $e + a$ 是可逆元。
    - 若 $a + b = ab$ 则 $ab = ba$.
5. 设 R 是幺环, 则 $e - ab$ 可逆当且仅当 $e - ba$ 可逆.

Domain

命题

环 R 是无零因子环当且仅当满足左右消去律。

定理

若 R 是无零因子环，则 R^* 中的每个元素的加法阶相同。若这个阶是有限数，则必为素数。

特征 (charater)

若 R 是无零因子环，

- 若 R^* 中的元素的加法阶是 p, 则称 R 的特征为 p,
- 若 R^* 中加法的阶是无穷，则称 R 的特征为 0.
- 用记号 $\mathrm{Ch}R$ 表示环 R 的特征。

非零特征环的性质

定理

设 R 是无零因子交换环，且 $\mathrm{Ch}R = p$ 则

$$\forall a, b \in R,\ (a+b)^p = a^p + b^p\ ,\quad (a-b)^p = a^p - b^p$$

推论

设 R 是无零因子交换环，且 $\mathrm{Ch}R = p$ 则

$$\forall a, b \in R,\ (a+b)^{p^k} = a^{p^k} + b^{p^k}\ ,\quad (a-b)^{p^k} = a^{p^k} - b^{p^k}$$

四元数体 (不可交换的除环)

四元数体

设 $\mathbb{H}$ 是实数域上的四维线性空间，设一组基为

$$\{1, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}\}$$

规定乘法运算满足

$$\boldsymbol{i}^2 = \boldsymbol{j}^2 = \boldsymbol{k}^2 = \boldsymbol{ijk} = -1$$

并要求分配律成立，则 $\mathbb{H}$ 自然诱导一个乘法

$$(a_1 1 + b_1 \boldsymbol{i} + c_1 \boldsymbol{j} + d_1 \boldsymbol{k})(a_2 1 + b_2 \boldsymbol{i} + c_2 \boldsymbol{j} + d_2 \boldsymbol{k})$$

可以验证这个代数结构是一个非交换的除环，被称为四元数体 $\mathbb{H}$.

- $$x = a1 + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}\text{的共轭}\bar{x} = a1 - b\boldsymbol{i} - c\boldsymbol{j} - d\boldsymbol{k}$$
- $$x = a1 + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}\text{的范数}N(x) = x\bar{x}$$

四元数体矩阵表示

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \boldsymbol{i} = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix}, \boldsymbol{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \boldsymbol{k} = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}$$

$$\boldsymbol{i}^2 = \boldsymbol{j}^2 = \boldsymbol{k}^2 = \boldsymbol{ijk} = -1$$

$$x = a1 + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}$$

$$N(x) = \det \begin{pmatrix} a + b\sqrt{-1} & c + d\sqrt{-1} \\ -c + d\sqrt{-1} & a - b\sqrt{-1} \end{pmatrix}$$

定理

$$\mathbb{H} = \left\{ \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} \middle| z, w \in \mathbb{C} \right\}$$

练习

- 求证: $x = a1 + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}$ 则 $N(x) = a^2 + b^2 + c^2 + d^2$
- 建立以下两个群的群同构 (运算是四元数乘法和矩阵乘法)

$$\mathrm{Sp}\,(1) = \{x \in \mathbb{H} |\, N\,(x) = 1\}$$

$$\mathrm{SU}\,(2) = \left\{A \in \mathrm{SL}\,(2, \mathbb{C}) |\, AA^H = I_2\right\}$$

- * 求证: 不能在实线性空间 $\mathbb{R}^3$ 上定义一个乘法 $\times$，使得 $\times$ 满足结合律并且每个非零向量都可逆 (可除代数)

子环 (subring)、理想 (ideal)、商环 (quotient ring)

子环与理想

子环 subring

环 R 的子集 S 在相同运算下也构成环，则称为子环。

命题

环 R 的非空子集 S 是子环当且仅当

$$\forall a, b \in S, a - b \in S, ab \in S$$

理想 ideal

子环 I 若满足

$$\forall r \in R, \forall i \in I, ir, ri \in I$$

则称 I 是 R 的一个理想。$\{0\}, R$ 被称为平凡理想。

命题

R 的非空子集 I 是 R 的理想当且仅当 $I - I, IR, RI \subset I$

生成理想、主理想

生成理想

设 $S\subset R$, 包含 S 的最小理想即由 S 生成的理想, 记为 $\langle S\rangle$。由一个元素 $a\in R$ 生成的理想称为主理想 (principal ideal)，记为 $\langle a\rangle$

- 一般的环 R 中

$$\langle a\rangle=\left\{\sum_{i=1}^{m}x_iay_i+ra+as+na\,\middle|\,x_i,y_i,r,s\in R;1\leqslant i\leqslant m;n\in\mathbb{Z}\right\}$$

- 若 R 是幺环

$$\langle a\rangle=\left\{\sum_{i=1}^{m}x_iay_i\,\middle|\,x_i,y_i\in R;1\leqslant i\leqslant m\right\}$$

- 若 R 是交换环

$$\langle a\rangle=\{ra+na|\,r\in R;n\in\mathbb{Z}\}$$

- 若 R 是交换幺环

$$\langle a\rangle=\{ra|\,r\in R\}$$

理想的例子

- $R = \mathbb{Z}$, $I = m\mathbb{Z}$
- $\mathbb{K}$ 是一个数域，$R = \mathbb{K}[x], I = \langle m(x) \rangle$
- $$R = C[a,b], Z_{x_0} = \{f \in R | f(x_0) = 0\}$$
- $$R = C^{\infty}(\mathbb{R}^n), \mathcal{O}_x = \{f \in R | \exists U_x, f(U) = \{0\}\}$$
- 矩阵环 $\mathbb{P}^{n\times n}$ 的理想只有平凡理想。
- 两个理想 I, J 的和也是理想。
$$I + J = \{a + b | a \in I, b \in J\}$$
- 任意多个理想的交也是理想。

理想的例子

定义环 R 的中心

$$C\left(R\right)=\left\{r\in R\left|\forall a\in R,ra=ar\right.\right\}$$

- $C(R)$ 是 R 子环，但不一定是理想

商环

定理 1

若 I 是环 R 的理想，则可以在加法群的商群上定义乘法

$$(a+I)(b+I)=ab+I$$

使得 R/I 是一个环，被称为商环。

- $R=\mathbb{Z}$, $I=m\mathbb{Z}, R/I=\mathbb{Z}_m$.
  并且 $m=p$ 是素数时，$\mathbb{Z}_m$ 是一个域。
- 微分几何中的局部化

$$\mathcal{F}_x\left(\mathbb{R}^n\right)=C^\infty\left(\mathbb{R}^n\right)/\mathcal{O}_x=\left\{[f]\,|\,f\in C^\infty\left(\mathbb{R}^n\right)\right\}$$

$$\mathcal{O}_x=\left\{f\in C^\infty\left(\mathbb{R}^n\right)|\exists U_x,f\left(U\right)=\{0\}\right\}$$

环同态

环同态 (homorphism as rings) 和环同构

Let $(R_1, +_1, *), (R_2, +_2, \circ)$ are rings, if there exists a mapping $f : R_1 \to R_2$, such that

$$\forall a, b \in R_1, f(a * b) = f(a) \circ f(b)$$

$$\forall a, b \in R_1, f(a +_1 b) = f(a) +_2 f(b)$$

Then we say f is a **homomorphism** as rings. Particularly isomorphism is a homomorphism as well as a bijection.

- 若 I 是 R 的理想，则有自然同态

$$\pi : R \longrightarrow R/I, \quad a \mapsto a + I$$

- 取定 $a \in \mathbb{R}^n$

$$\varphi_a : C\left(\mathbb{R}^n\right) \longrightarrow \mathbb{R}, \quad \varphi_a\left(f\right) = f\left(a\right)$$

例子

验证整环的分式域的构造。

- 设 R 是整环，验证 $R \times R^*$ 上定义等价关系 $(a, b) \sim (c, d) \Leftrightarrow ac = bd$
- 在商集 $F = R \times R^* / \sim$ 上定义运算
- 验证可以将 R 看成 F 的子环
- 验证 F 是包含 R 最小的环

矩阵与线性变换

- 设 V 有一组基 $\{v_1, ..., v_n\}$
- 取 $\mathscr{A} \in \mathrm{Hom}_{\mathbb{P}} V$ 存在唯一的 $A \in \mathbb{P}^{n \times n}$ 使得

$$\mathscr{A}\left(v_1, ..., v_n\right) = \left(v_1, ..., v_n\right) A$$

- 则有环同构

$$\mathrm{Hom}_{\mathbb{P}} V \longrightarrow \mathbb{P}^{n \times n}, \mathscr{A} \longmapsto A$$

多项式和矩阵

同态核、环同态基本定理

设有环同态 $f : R_1 \longrightarrow R_2$，定义同态核为 $\mathrm{Ker} f = f^{-1}(0)$.

引理

$\mathrm{Ker} f$ 是 R_1 的理想，$\mathrm{Im} f$ 是 R_2 的子环。

定理 1

设 $\pi : R_1 \longrightarrow R_1/\mathrm{Ker} f$ 是自然同态，则存在环同构

$$\bar{f} : R_1/\mathrm{Ker}\, f \longrightarrow \mathrm{Im}\, f$$

使得 $f = \bar{f} \circ \pi$.

对应定理

定理 (群同态对应定理)

设有群同态 $f : G_1 \longrightarrow G_2$ 是满同态，则由 f 诱导了两个双射

$$\{H \subseteq G_1 | H \leqslant G_1, \mathrm{Ker} f \subseteq H\} \xleftrightarrow{1:1} \{H \subseteq G_2 | H \leqslant G_2\}, \quad H \mapsto f(H)$$

$$\{H \subseteq G_1 | H \lhd G_1, \mathrm{Ker} f \subseteq H\} \xleftrightarrow{1:1} \{H \subseteq G_2 | H \lhd G_2\}, \quad H \mapsto f(H)$$

定理 2

设有环同态 $f : R_1 \longrightarrow R_2$ 是满同态，则由 f 诱导了两个双射

$$\{\text{子环} S \subseteq R_1 | \mathrm{Ker} f \subseteq S\} \xleftrightarrow{1:1} \{\text{子环} S \subseteq R_2\}, \quad S \mapsto f(S)$$

$$\{\text{理想} I \subseteq R_1 | \mathrm{Ker} f \subseteq I\} \xleftrightarrow{1:1} \{\text{理想} I \subseteq R_2\}, \quad I \mapsto f(I)$$

基本推论

推论 1

若 I 是 R_1 包含 $\mathrm{Ker} f$ 的理想，则有

$$R/I \simeq f\left(R\right)/f\left(I\right)$$

推论 2

对 R 的理想 I_1, I_2 有

$$I_2 \subseteq I_1 \subseteq R \Longrightarrow R/I_1 \simeq \left(R/I_2\right)/\left(I_1/I_2\right)$$

推论 3

对 R 的理想 I, J 有

$$\left(I+J\right)/I \simeq J/\left(I \cap J\right)$$

练习

1. 验证环同态，并求 $\mathrm{Ker}\varphi$, $\mathrm{Im}\varphi$
$$\varphi : \mathbb{Z}[x] \to \mathbb{R}, \quad \varphi(f) = f(1+\sqrt{2})$$
2. 求证：若 $(p,q)=1, p,q>1$ 则不存在环同构 $\mathbb{Z}[\sqrt{p}] \simeq \mathbb{Z}[\sqrt{q}]$
3. 求环 $\mathbb{Q}, \mathbb{Q}[\sqrt{2}]$ 的所有自同构
4. R 是除环，证明 $C(R)$ 是域
5. 求 $C(\mathbb{H})$.
6. 验证环同态 (Frobenius) 是不是环同构，其中 $\mathrm{Ch}R = p$ 且 R 是无零因子交换环
$$R \longrightarrow R, \quad a \mapsto a^p$$
7. 求证有环同构 $\mathbb{Z}[i] \simeq \mathbb{Z}[x]/\left\langle x^2+1 \right\rangle$
8. 求证有环同构 $\mathbb{C} \simeq \mathbb{R}[x]/\left\langle x^2+1 \right\rangle$

Thank you!