离散数学第四部分之三

环和域

环的定义与性质

- 环的定义
- 环的运算性质
- 环的子代数和环同态

环的定义

定义 设<**R**,+,·>是代数系统,+和·是二元运算。

如果满足以下条件:

(1) <**R**,+>构成交换群。

(2) <**R**,·>构成半群。

(3) ·运算关于+运算适合分配律。

则称<**R**,+,·>是一个环**(ring)**。

通常称+运算为环中的加法, · 运算为环中的乘法。

环的实例

(1)整数集、有理数集、实数集和复数集关于普通的加法和乘法构成环，分别称为整数环Z，有理数Q，实数环R和复数环C。

(2)$n(n\geq 2)$阶实矩阵的集合$M_n(R)$关于矩阵的加法和乘法构成环，称为n阶实矩阵环。

(3)集合的幂集P(B)关于集合的对称差运算和交运算构成环。

(4)设$Z_n=\{0,1,\ldots,n-1\}$, $\oplus$和$\otimes$分别表示模n的加法和乘法，则$<Z_n, \oplus, \otimes>$构成环,称为模n的整数环。

环的运算约定

- 加法的单位元记作0。
- 乘法的单位元记作1(对于某些环中的乘法不存在单位元)。
- 对任何环中的元素x，称x的加法逆元为负元，记作$-x$。
- 若x存在乘法逆元的话，则将它称为逆元，记作x^{-1}。
- 针对环中的加法，
  - $x-y$表示$x+(-y)$。
  - nx表示$x+x+\ldots+x$(n个x相加)，即x的n次加法幂。
  - $-xy$表示xy的负元。

环的运算性质

定理 设<R,+,·>是环，则

(1) $\forall a \in R$，$a0 = 0a = 0$

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

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

(4) $\forall a_1,a_2,\ldots,a_n,b_1,b_2,\ldots,b_m \in R(n,m \geq 2)$

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

(1) $\forall a \in R$，$a0=0a=0$

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

由环中加法的消去律得 $a0=0$。

同理可证 $0a=0$。

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

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

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

因此$(-a)b$是ab的负元。

由负元的唯一性可知 $(-a)b=-ab$。

同理可证 $a(-b)=-ab$。

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

$$a(b-c) = a(b+(-c)) = ab+a(-c) = ab-ac$$

(4) $\forall a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_m \in \mathrm{R}\,(n, m \geqslant 2)$

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

先证明 $\forall a_1, a_2, \ldots, a_n$ 有 $(\sum_{i=1}^{n} a_i) b_j = \sum_{i=1}^{n} a_i b_j$

对n进行归纳。

当n＝2时，由环中乘法对加法的分配律，等式显然成立。

假设 $(\sum_{i=1}^{n} a_i) b_j = \sum_{i=1}^{n} a_i b_j$ ，则有

$$(\sum_{i=1}^{n+1} a_i) b_j = (\sum_{i=1}^{n} a_i + a_{n+1}) b_j = (\sum_{i=1}^{n} a_i) b_j + a_{n+1} b_j$$

$$= \sum_{i=1}^{n} a_i b_j + a_{n+1} b_j = \sum_{i=1}^{n+1} a_i b_j$$

由归纳法命题得证。

同理可证，$\forall b_1, b_2, \ldots, b_m$ 有

$$a_i(\sum_{j=1}^{m} b_j) = \sum_{j=1}^{m} a_i b_j$$

于是

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

例

例 在环中计算$(a+b)^3$，$(a-b)^2$

解答 $(a+b)^3$

$= (a+b)(a+b)(a+b)$

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

$= a^3+ba^2+aba+b^2a+a^2b+bab+ab^2+b^3$

$(a-b)^2$

$= (a-b)(a-b)$

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

子环

定义（补充） 设R是环，S是R的非空子集。若S关于环R的加法和乘法也构成一个环，则称S为R的子环(subring) 。

若S是R的子环，且$S \subset R$，则称S是R的真子环。

举例：

整数环Z，有理数环Q都是实数环R的真子环。

{0}和R也是实数环R的子环，称为平凡子环。

子环判定定理

定理（补充） 设R是环，S是R的非空子集，若

(1) $\forall a,b \in S$，$a-b \in S$

(2) $\forall a,b \in S$，$ab \in S$

则S是R的子环。

证明：由(1)S关于环R中的加法构成群。

由(2)S关于环R中的乘法构成半群。

显然R中关于加法的交换律以及乘法对加法的分配律在S中也是成立的。

因此，S是R的子环。

例

(1)考虑整数环$<Z,+,\cdot>$，对于任意给定的自然数n，
$nZ=\{nz|z\in Z\}$是Z的非空子集，且$\forall nk_1,nk_2\in nZ$有

$$nk_1-nk_2=n(k_1-k_2)\in nZ$$

$$nk_1\cdot nk_2=n(k_1nk_2)\in nZ$$

根据判定定理,nZ是整数环的子环。

(2)考虑模6整数环$<Z_6,\oplus,\otimes>$，不难验证
$\{0\},\{0,3\},\{0,2,4\},Z_6$是它的子环。

其中$\{0\}$和Z_6是平凡的，其余的都是非平凡的真子环。

环的同态

定义（补充） 设R_1和R_2是环。φ：$R_1 \to R_2$，若对于任意的$x,y \in R_1$有

$$\varphi(x+y)=\varphi(x)+\varphi(y)，\varphi(xy)=\varphi(x)\varphi(y)$$

成立，则称φ是环R_1到R_2的同态映射，简称环同态。

说明 类似于群同态，可以定义环的单同态，满同态和同构等。

例

设R_1＝$<Z,+,\cdot>$是整数环，R_2＝$<Z_n,\oplus,\otimes>$是模n的整数环。

令　φ：$Z\to Z_n$，$\varphi(x)=(x)\bmod n$

则$\forall x,y\in Z$ 有

$$\varphi(x+y)=(x+y)\bmod n$$

$$=\varphi(x)\bmod n \oplus \varphi(y)\bmod n$$

$$=\varphi(x)\oplus\varphi(y)$$

$$\varphi(xy)=(xy)\bmod n$$

$$=(x)\bmod n \otimes (y)\bmod n$$

$$=\varphi(x)\otimes\varphi(y)$$

所以φ是R_1到R_2的同态,不难看出是满同态。

整环与域

定义 设<R,+,·>是环,

(1) 若环中乘法·适合交换律，则称R是交换环。

(2) 若环中乘法·存在单位元，则称R是含幺环。

(3) 若$\forall a,b \in R$，$ab=0 \Rightarrow a=0 \vee b=0$，
则称R是无零因子环。

(4) 若R既是交换环、含幺环，也是无零因子环，
则称R是整环。

实例

(1)整数环Z，有理数环Q，实数环R，复数环C都是交换环、含幺环、无零因子环和整环。

(2)令2Z＝{2z|z∈Z}，则2Z关于普通的加法和乘法构成交换环和无零因子环。但不是含幺环和整环，因为1∉2Z。

(3)设n是大于或等于2的正整数，则n阶实矩阵的集合$M_n(R)$关于矩阵加法和乘法构成环，它是含幺环，但不是交换环和无零因子环，也不是整环。

实例

(4)Z_6关于模6加法和乘法构成环，它是交换环、含幺环，但不是无零因子环和整环。

2⊗3＝0，但2和3都不是0。称2为Z_6中的左零因子，3为右零因子。类似地,又有3⊗2＝0,所以3也是左零因子，2也是右零因子，它们都是零因子。

一般说来，对于模n整数环Z_n，若n不是素数，则存在正整数s,t(s,t≥2)，使得s⊗t＝n。这样就得到st＝0，s,t是Z_n中的零因子，因此Z_n不是整环。

反之，若Z_n不是整环，则Z_n一定不是无零因子环。

这就意味着存在a,b∈Z_n，使得a⊗b＝0，但a≠0且b≠0。根据模n乘法定义得n整除ab，从而推出n不是素数。

若不然必有n整除a或n整除b，与a≠0且b≠0矛盾。通过上面的分析可以得到下面的结论：Z_n是整环当且仅当n是素数。

环是无零因子环的充分必要条件

定理（补充） 设R是环，R是无零因子环当且仅当R中的乘法适合消去律，即$\forall a,b,c \in R$，$a \neq 0$，有

$$ab = ac \Rightarrow b = c \quad \text{和} \quad ba = ca \Rightarrow b = c$$

证明 充分性。任取$a, b \in R$，$ab = 0$且$a \neq 0$，

则由$ab = 0 = a0$和消去律得 $b = 0$。

这就证明了R是无零因子环。

必要性。任取$a, b, c \in R$，$a \neq 0$，由$ab = ac$得 $a(b-c) = 0$，

由于R是无零因子环，$a \neq 0$，必有$b-c = 0$，即 $b = c$。

这就证明了左消去律成立。

同理可证右消去律也成立。

环的直积

例 设R_1,R_2是环，$\forall$<a,b>,<c,d>$\in R_1\times R_2$,令

$$<a,b>+<c,d>=<a+c,b+d>$$

$$<a,b>\cdot<c,d>=<ac,bd>$$

不难验证$R_1\times R_2$关于+和·运算构成一个环，称为环R_1和R_2的直积，记作$R_1\times R_2$。

可以证明，

若R_1和R_2是交换环和含幺环，则$R_1\times R_2$也是交换环和含幺环。

若R_1和R_2是无零因子环，那么$R_1\times R_2$不一定是无零因子环。

例如Z_3和Z_2是无零因子环，因为消去律在Z_3和Z_2中都是成立的。但是$Z_3\times Z_2$就不是无零因子环。

若不然，由 $<2,0>\cdot<0,1>=<0,0>=<2,0>\cdot<0,0>$

和$<2,0>\neq<0,0>$，根据消去律就可得到$<0,1>=<0,0>$。错误。

因此我们可以说整环的直积不一定是整环。

域的定义与实例

定义 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。

例如：有理数集Q、实数集R、复数集C关于普通的加法和乘法都构成域，分别称为有理数域、实数域和复数域。

整数环只能构成整环Z，而不是域，因为并不是对于任意的非零整数$z \in Z$都有$1/z \in Z$。

对于模n的整数环Z_n，若n是素数，可以证明Z_n是域。

例

例 设p为素数，证明Z_p是域。

证明 p为素数，$p \geq 2$，所以$|Z_p| \geq 2$。

易见Z_p关于模p乘法可交换，单位元是1，且对于任意的$i,j \in Z_p$，$i \neq 0$ 有

$$i \otimes j = 0 \Rightarrow \text{p整除} ij \Rightarrow p | j \Rightarrow j = 0$$

所以Z_p中无零因子，Z_p为整环。

Z_p关于乘法$\otimes$构成有限半群，且Z_p关于$\otimes$适合消去律。

下面证明每个非零元素都有逆元。

任取$i \in Z_p, i \neq 0$,令 $i \otimes Z_p = \{i \otimes j | j \in Z_p\}$则$i \otimes Z_p = Z_p$，

否则必存在$j,k \in Z_p$，使得$i \otimes j = i \otimes k$，由消去律得$j = k$。这是矛盾的。

由于$1 \in Z_p$，这就推出，存在$i' \in Z_p$，使得$i \otimes i' = 1$。由于$\otimes$运算的交换性可知i'就是i的逆元。从而证明了Z_p是域。

例

判断下述集合关于给定的运算是否构成环、整环和域，如果不能构成，请说明理由。

(1) $A=\{a+b\sqrt{2} \mid a,b\in Z\}$，关于数的加法和乘法。

是环和整环，但不是域，例如 $\sqrt{2}\in A$，但$\sqrt{2}$没有逆元。

(2) $A=\{a+b\sqrt{3} \mid a,b\in Q\}$，关于数的加法和乘法。

是环，整环和域。

(3) $A=\{a+b\sqrt[3]{2} \mid a,b\in Z\}$，关于数的加法和乘法。

不是环，不是整环，也不是域。因为A关于数的乘法不封闭。

(4) $A=\{a+bi \mid a,b\in Z\wedge i^2=-1\}$，关于复数的加法和乘法。

是环和整环，但不是域，例如 $2i\in A$，但$2i$没有逆元。

例

(5)$A=\{\begin{pmatrix} a & b \\ b & a \end{pmatrix} \mid a,b\in Z\}$，关于矩阵的加法和乘法。

是环，但不是整环和域。

考虑矩阵$\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$和 $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ 。

它们都是A中的矩阵，且满足

$$\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

因此 $\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ 是左零因子，$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ 是右零因子。

A不是无零因子环。也不是整环和域。

- 本章内容

  - 环、整环、无零因子环的定义
  - 能够判断是否是环和域