信息安全数学基础

第四章 环与域

聂旭云
信息与软件工程学院
电子科技大学

中国大学MOOC

信息安全数学基础

4.1 环的定义及基本概念

聂旭云
信息与软件工程学院
电子科技大学

中国大学MOOC

环的定义

定义4.1.1 设R是一个非空集合，R上定义有两个代数运算：加法（记为“＋”）和乘法（记为“ ”），假如

（1）R对于加法构成一个交换群。

（2）R的乘法满足结合律。即对于任意 $a,b,c \in R$，有

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

（3）乘法对加法满足左、右分配律，即对于任意$a,b,c \in R$，有

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(b + c) \cdot a = b \cdot a + c \cdot a$$

则称R为环。

环的定义（续）

如果，R还满足

（4）乘法交换，即对于任意$a, b \in R$，有$a \cdot b = b \cdot a$，

则称R为交换环。

如果R中存在元素$\mathbf{1}_R$，使得

（5）对于任意$a \in R$，有$a \cdot \mathbf{1}_R = \mathbf{1}_R \cdot a = a$，

则称R为有单位元环。元素$\mathbf{1}_R$（或简记为1）称为R中的单位元。

R的加法群中的单位元素记为0，称为环R的零元素。R中的元素a加法逆元称为负元，记为$-a$。

与第三章中的群的乘法一样，R中两个元素的乘法$a \cdot b$可简记为ab。

环的例子

例4.1.1 （1）全体整数关于数的普通加法和乘法构成一个环，称为整数环，记为Z。

（2）全体有理数（实数、复数）关于数的普通加法和乘法构成一个环，称为有理数域，记为Q（R、C）。

例4.1.2 整数n的所有倍数={nz|z∈Z}关于数的普通加法和乘法构成一个环，记为nZ。

R＝{所有模n的剩余类}，规定运算为

$$[\boldsymbol{a}]+[\boldsymbol{b}]=[\boldsymbol{a}+\boldsymbol{b}],\ [\boldsymbol{a}][\boldsymbol{b}]=[\boldsymbol{ab}]$$

可以证明R关于上述运算构成一个环，称为模n的剩余类环，记为Z/nZ或Z_n。

例4.1.1中的环都是有单位元的交换环，其单位元都为整数1。

例4.1.2中的Z_n也是有单位元的交换环，其单位元为[1]，而当n>1时，nZ没有单位元。

环的例子（续）

- 例4.1.3 数域F上的n阶方阵的全体关于矩阵的加法和乘法构成一个环，称为F上的n阶方阵环，记为$M_n(F)$。这个环的单位元为n阶单位矩阵。因为矩阵的乘法不满足交换律，所以$M_n(F)$不是交换环。
- 例4.1.4 令$R=\{0,a,b,c\}$，定义加法和乘法如下：

$+$	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

$\times$	0	a	b	c
0	0	0	0	0
a	0	0	0	0
b	0	a	b	c
c	0	a	b	c

容易验证

- 对于加法构成加法交换群
- 乘法满足结合律
- 乘法对加法满足分配律

中国大学MOOC

环中运算的性质

定理4.1.1 设R是一个环，$a, b \in R$，ma表示m个a相加，a^m表示m个a相乘，则

（1）$a \cdot 0 = 0 \cdot a = 0$；

（2）$a \cdot (-b) = (-a) \cdot b = -ab$；

（3）$n(a + b) = na + nb$；

（4）$m(ab) = (ma)b = a(mb)$；

（5）$a^m a^n = a^{m+n}$；

（6）$(a^m)^n = a^{mn}$。

证明：以（1），（3）为例，其余的留给读者思考

（1）根据乘法对加法分配律有

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$$

则

$$a \cdot 0 + \left(-(a \cdot 0)\right) = a \cdot 0 + a \cdot 0 + (-(a \cdot 0))$$

即$a \cdot 0 = 0$。同理可证$0 \cdot a = 0$。

（3）$n(a + b) = \overbrace{a + b + \cdots + a + b}^{n} = \overbrace{a + \cdots + a}^{n} + \overbrace{b + \cdots + b}^{n} = na + nb$

零因子

- ab = 0 => a = 0 或 b = 0?
- 当n是合数时，Z_n中不成立：Z_{12}中[3][4]=[12]=[0]，而$[3] \neq [0], [4] \neq [0]$。
- 定义4.1.2 设R是一个环，如果存在$\boldsymbol{a, b \in R}$，满足$\boldsymbol{ab = 0}$，但$\boldsymbol{a \neq 0, b \neq 0}$，则称环R为有零因子环，称$\boldsymbol{a}$为R的左零因子，称$\boldsymbol{b}$为R的右零因子，否则称R为无零因子环。对于交换环，左零因子、右零因子、零因子不加以区分。
- 例4.1.5 Z、Q、R、C均是无零因子环，而对于在一个合数n，Z_n为有零因子环。
- 例4.1.6对于环$\boldsymbol{M_n(F)}$，当$\boldsymbol{n \geq 2}$时，这个环是有零因子环。
- 如$R = \left\{ \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \middle| a, b \in \mathrm{R} \right\}$，$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$既是左零因子又是右零因子，因为
- $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$，$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

无零因子环的例子

例4.1.7 设p是一个素数，则Z_p是无零因子环。

证明：根据推论2.2.1，Z_p中任何一个非零元均存在逆元。

设$[a],[b] \in Z_p$。若

$$[a][b] = [0]，即 ab \equiv 0(mod\, p)$$

则有当$a \not\equiv 0(mod\, p)$，

$$ab \equiv 0(mod\, p) \Rightarrow b \equiv a^{-1} \cdot 0(mod\, p) \Rightarrow b \equiv 0(mod\, p)$$

当$b \not\equiv 0(mod\, p)$，有$a \equiv 0(mod\, p)$。

也就是说，由$[a][b] = [0]$，可得出$[a] = [0]$或$[b] = [0]$。

因此，Z_p是无零因子环。

可逆元

- 定义4.1.3 设R是一个有单位元环，$a \in R$，若存在$b \in R$，满足$ab = ba = 1$，则称a是一个可逆元
- 在整数环Z中，仅有±1是可逆元。
- 可逆元一定不是零元，也不是零因子。
- 例4.1.8 设R是一个有单位元环，则R中所有可逆元构成的集合对于R中的乘法构成群，记为R^*。
- 证明：根据群和环的定义，R^*上乘法显然满足结合律，有单位元，有逆元，所以仅需证明R^*对环中的乘法封闭。
- 若$a, b \in R^*$，则有$ab \cdot b^{-1}a^{-1} = b^{-1}a^{-1} \cdot ab = 1$，所以$ab \in R^*$，即对乘法封闭。

中国大学MOOC

无零因子环的特征

定理4.1.3 设**R**是一个无零因子环，则**R**中非零元的加法阶相等，这个加法阶或者是∞，或者是个素数p。

证明：当环**R**中每个非零元的加法阶都是无穷大时，定理成立。

设$a, b \in R$是非零元，a的加法阶为**n**，b的加法阶是**m**。则由

$$(na)b = a(nb) = 0$$

可得$nb = 0$，所以$n \geq m$。同理可证$m \geq n$。因此，$m = n$。即所有非零元的加法阶相等。

设R中所有非零元的加法阶为**n**。若**n**不是素数，不妨设$n = n_1 n_2$，$n_1 < n, n_2 < n$。对于$a \in R, a \neq 0$，有

$$(n_1 a)(n_2 a) = n_1 n_2 a^2 = 0$$

又**R**是无零因子环，所以有

$$n_1 a = 0 \text{或} n_2 a = 0$$

这与**n**是a的加法阶矛盾。因此，**n**是素数。

无零因子环的特征（续）

- 定义4.1.4 设R是一个无零因子环，称R中非零元的加法阶为环R的特征，记为Char$R$。当R中非零元的加法阶为无穷大时，称R的特征为零，记Char$R=0$；当R中非零元的加法阶为某个素数p时，称R的特征为p，记Char$R=p$。

无零因子环的特征（续）

- 例4.1.9 设R是特征为p的交换环，$a, b \in R$，有$(a \pm b)^p = a^p \pm b^p$。
- 证明：$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \cdots + \binom{p}{p-1} a b^{p-1} + b^p$。
- 因为，对于$1 \leq k \leq p-1$，$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p \cdot (p-1)!}{k!(p-k)!}$。
- 由上式可知$k!\,(p-k)!\,|p \cdot (p-1)!$，而$k!\,(p-k)!$与素数$p$互素，所以$k!\,(p-k)!\,|(p-1)!$，因此$\binom{p}{k}$是$p$的倍数，进而有$\binom{p}{k} a^{p-k} b^k = 0$，由此可得
- $(a+b)^p = a^p + b^p$
- $(a-b)^p = a^p - b^p$的证明留给读者。

感 谢 聆 听！

xynie@uestc.edu.cn

中国大学MOOC