离散数学

Discrete Mathematics

2020年新冠疫情网络教学版

蒋瀚

山东大学软件学院

Chapter
06

环与域

CONTENT

环 - 定义及基本性质

定义 1　设〈R，＋，·〉是一个代数系统，其中，＋，· 均为二元运算，如果

（1）〈R，＋〉是一个Abel群.

（2）〈R，·〉是一个半群.

（3）· 对 ＋ 满足分配律，即

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

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

称〈R，＋，·〉为一个环，其中的运算 ＋ 称作加法，· 称为乘法.　（乘法优先于加法，可省略· ）

环 - 定义及基本性质

□例 1　〈$\mathbf{Z}$，＋，·〉是一个环，称作整数环.

〈$2\mathbf{Z}$，＋，·〉，〈$\mathbf{Q}$，＋，·〉，〈$\mathbf{R}$，＋，·〉也为环.

□例 2　设i是虚数单位，即$i^2=-1$，令

$$\mathbf{Z}(i)=\{a+bi \mid a, b\in\mathbf{Z}\}$$

则 $\mathbf{Z}(i)$关于数的加法＋、乘法· 构成环，通常称作高斯环.

环 - 定义及基本性质

□例 3　n阶整数矩阵所成集合 $(\mathbf{Z})_n$,关于矩阵的加法与乘法作成一个环.

n阶有理数矩阵集合$(\mathbf{Q})_n$，n阶实数矩阵集合 $(\mathbf{R})_n$, 在矩阵加法与乘法运算下也均构成环.

□例 4　x的一切整（有理、实）系数多项式所成集合$\mathbf{Z}[x]$（$\mathbf{Q}[x]$, $\mathbf{R}[x]$）在多项式加法与乘法运算下构成环.

环 - 定义及基本性质

□例 5　〈$\mathbf{Z}_m$，$+_m$，$\times_m$〉构成环，称为模m剩余环.

□例 6　设〈A，$+$〉是一个Abel群，0为其零元，规定乘法$\cdot$如下：

$$a\cdot b=0,\quad \forall\, a,b\in A$$

则〈A，$+$，$\cdot$〉是一个环.

环的一些初步性质

- 设R是一个环，在Abel群〈R，＋〉中，单位元用 0 表示，称为零元，$a\in R$在〈R，＋〉中的逆元用$-a$表示，称为a的负元，且记

$$ma = a+a+\ldots+a\text{（共}m\text{个）}.$$

- 性质1 加法结合律 $(a+b)+c=a+(b+c)$
- 性质2 零元： $a+0=0+a=a$
- 性质3 负元： $a+(-a)=(-a)+a=0$
- 性质4 加法交换律 $a+b=b+a$
- 性质5 加法消去律 $a+b=a+c \Rightarrow b=c$

环的一些初步性质

- 性质6　指数律　$n(a+b)=na+nb$
- 性质7　指数律　$(m+n)a=ma+na$
- 性质8　指数律　$(mn)a=m(na)$　（加法）
- 性质9　$0a=a0=0$，　$\forall a\in R$　（哪个0？）
- 性质10　$a(-b)=(-a)b=-(ab)$
- 性质11　$(-a)(-b)=ab$，　$\forall a,b\in R$

环的一些初步性质

- 在环R中，$a+(-b)$可简记为$a-b$，并把符号“$-$”称作“减法”.
- 性质12　$a(b-c)=ab-ac.$
- 性质13　$a(b_1+b_2+\ldots+b_n)=ab_1+ab_2+\ldots+ab_n$

$$(b_1+b_2+\ldots+b_n)a=b_1a+b_2a+\ldots+b_na,\ \forall a,\ b_i\in R$$

- 性质14

$$(\sum_{i=1}^{n}a_i)(\sum_{j=1}^{m}b_j)=\sum_{i=1}^{n}\sum_{j=1}^{m}(a_ib_j)\quad \forall a_i,b_j\in R$$

- 性质15　$(na)b=a(nb)=n(ab),\quad \forall a,\ b\in R,\ n\in\mathbf{Z}.$

环 - 定义及基本性质

- 在环〈R，＋，·〉中，若〈R，·〉为幺半群，则称〈R，·〉的单位元为环R的单位元，通常用 1 表示，这时称R为有单位元的环或有 1 的环.
- 设R为有 1 的环，$a \in R$，如果a在〈R，·〉中有逆元，则称a为R中的可逆元．并把a在半群〈R，·〉中的逆元，称为a在环R中的逆元，用a^{-1}表示.
- 有 1 的环R中所有可逆元在乘法运算下构成一个群（？），该群记为R^*，并称为环R的乘法群.

环- 定义及基本性质

□环$R=\{0\}$称为零环.

□**定理 1**　设R为有单位元的环，且不只含一个元素，则 $1\neq 0$.

□**证明**　若 $1=0$，则　$\forall a\in R$,

$$a=a\cdot 1=a\cdot 0=0 .$$

故R只含一个元素 0，矛盾.

环与域 - 定义及基本性质

- 以后提到有单位元的环时，总指非零环．因此 $1 \neq 0$ 总成立．

- 当环R的乘法运算满足交换律，即〈R，·〉为（可）交换半群时，称R为（可）交换环．

作业

- 习题一 4，5，7

CONTENT

整环　除环　域

□在剩余环〈$\mathbf{Z}_6$，$+_6$，$\times_6$〉中，有

$[2]\neq[0]$，$[3]\neq[0]$，但

$[2]\times_6[3]=[0]$.

□定义1　设〈R，$+$，$\cdot$〉为一个环，$a\in R$且$a\neq 0$，若R中存在非零元素b，使$ab=0$（$ba=0$），则称a为R的左（右）零因子．R的左、右零因子统称为零因子.

整环　除环　域

□例 1　对于剩余环$\langle \mathbf{Z}_n, +_n, \times_n \rangle$，若$n$不是素数，则$\mathbf{Z}_n$中必存在零因子.

□$\mathbf{Z}_n$中的零元为$[0]$. 因为n不是素数，故存在整数n_1，n_2，使

$$n=n_1n_2 \quad , \quad 1<n_1\leq n_2<n$$

因此$[n_1]\neq[0]$，$[n_2]\neq[0]$，

但$[n_1]\times_n[n_2]=[0]$. 即$[n_1]$，$[n_2]$是$\mathbf{Z}_n$的一对零因子.

整环　除环　域

□例 2　用 $(\mathbf{R})_2$表示 2 阶实数矩阵集合，＋，·表示矩阵的加法与乘法，则

〈$(\mathbf{R})_2$，＋，·〉是一个环。

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

整环　除环　域

定理 1　若环R无零因子，则乘法消去律成立.

即

$$ab=ac\Rightarrow b=c$$

$$ba=ca\Rightarrow b=c \qquad \forall a,b,c\in R, a\neq 0$$

反之亦然.

证明　设R中无零因子，$\forall a\neq 0$，如果$ab=ac$，则$ab-ac=0$，$a(b-c)=0$. 由于$a\neq 0$，R中无零因子，故$b-c=0$，即$b=c$.

同理$ba=ac \Rightarrow b=c$;

反之，设环R中乘法消去律成立，若R中有零因子a，b，使得$ab=0=a0$，由消去律得$b=0$，矛盾. 故R中必无零因子.

整环　除环　域

- 定义 2　有单位元、无零因子的交换环称为整环.
- 例 3　整数环〈$\mathbf{Z}$，＋，·〉是一个整环，高斯环〈$\mathbf{Z}[i]$，＋，·〉是一个整环.
- 例 4　若p是一个素数，则〈$\mathbf{Z}_p$，$+_p$，$\times_p$〉是一个整环.

  （若 $[i]\times_p[j]=[0]$，则 $[ij]=[0]$，因而 $p\mid ij$. 故$p\mid i$或$p\mid j$，$[i]=[0]$ 或 $[j]=[0]$）
- 〈$\mathbf{Z}_n$，$+_n$，$\times_n$〉是整环 $\Leftrightarrow$ n为素数

整环　除环　域

定义 3　设R是一个有 1 的环，$\hat{R} = R - \{0\}$，如果〈 $\hat{R}$ ，·〉是一个群，则称R为除环，可交换的除环称为域.

（1）有单位元的环R是除环 $\Leftrightarrow$ R中非零元均可逆 $\Leftrightarrow$ R的乘法群$R^* = R - \{0\}$.

（2）有单位元的环R是域 $\Leftrightarrow$ R是交换环且R中非零元素均可逆.

整环　除环　域

例 5　〈**Q**，＋，·〉，〈**R**，＋，·〉均是域，分别称为有理数域和实数域.

例 6　令 $\mathbf{Q}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbf{Q}\}$，为通常数的加法和乘法，则

〈　　，＋，·〉是域.

整环　除环　域

定理 2　设R是一个无零因子的有限环，且$|R|\geq 2$，则R必为除环.

证明　需要证明$\langle R-\{0\},\cdot\rangle$为群.

由于$|R|\geq 2$，故$R-\{0\}$非空，又，R中不含零因子，故$R-\{0\}$对$\cdot$封闭，从而$\langle R-\{0\},\cdot\rangle$必构成半群，且由定理 1 知，在该半群中消去律成立，从而$\langle R-\{0\},\cdot\rangle$是一个满足消去律的有限半群，故必为群.

整环　除环　域

推论　有限整环必为域.

由于$\mathbf{Z}_p$是一个有限整环，知$\mathbf{Z}_p$为域（这个域称为素域）.

推论　若p为素数，则〈$\mathbf{Z}_p$，$+_p$，$\times_p$〉为域.

整环　除环　域

□设F是一个域，若$b\neq 0$，可将b^{-1}写成　　，$b^{-1}a$（或ab^{-1}）写成　，在这种记号下，有以下性质成立.

$\dfrac{a}{b}$

（1）　设$b\neq 0$，$d\neq 0$，则

$$ad = bc$$

（2）　设$b\neq 0$，$d\neq 0$，则 $\dfrac{a}{b}=\dfrac{c}{d}$.

$$\frac{a}{b}\pm\frac{c}{d}=\frac{ad\pm bc}{bd}$$

整环　除环　域

（3）　设$b\neq 0$，$d\neq 0$，则.

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}$$

（4）　设$b\neq 0$，$c\neq 0$，$d\neq 0$，则.

$$\frac{a}{b}/\frac{c}{d}=\frac{ad}{bc}$$

作业

习题二 1，4，5

CONTENT

CONTENT

域的特征 素域

- 定义 1　设F是一个域，$S \subseteq F$，若S在F的加法与乘法运算下也构成域，则称S为F的子域，F为S的扩域（或扩张）.
- 若S是F的子域，则〈S，＋〉是〈F，＋〉的子群，故 $0 \in S$，〈S^*，·〉是〈F^*，·〉的子群（其中，$S^* = S - \{0\}$，$F^* = F - \{0\}$），故 $1 \in S$.
- F的任意子域必含F的 0，1 .

域的特征 素域

定理 1 设〈F，＋，·〉是一个域，则：

（1） 在加法群〈F，＋〉中，每个非零元都具有同样的周期（阶）.

（2） 如果〈F，＋〉中非零元素的周期为有限数p，则p必为素数.

域的特征 素域

证明

（1）$a \in F$，设$a \neq 0$，用e表示F的单位元，则：

$$na = a+a+\ldots+a = ea+ea+\ldots+ea = (e+e+\ldots+e)a$$

$$= (ne)a$$

由于$a \neq 0$，且域中无零因子，故

$$na = 0 \Leftrightarrow (ne)a = 0 \Leftrightarrow ne = 0$$

故，a的加法周期与单位元e相同.

域的特征 素域

（2）设F中非零元素的周期为有限数p，则 $p>1$．如果

$$p=p_1p_2，\ 1<p_1\leq p_2<p，则$$

$$pe=(p_1p_2)e=p_1(p_2e)=(p_1e)(p_2e)$$

由$pe=0$知$(p_1e)(p_2e)=0$，由于域F中无零因子，因此$(p_1e)=0$或$(p_2e)=0$，与e的周期为p矛盾．

故p必为素数．

域的特征 素域

□定义 2　设〈F，＋，·〉是一个域，若〈F，＋〉中非零元的周期为有限数p，则称域F的特征为p．若〈F，＋〉中非零元的周期为∞，则称域F的特征为 0 ．

□域F的特征或者为素数或者为 0 ．

域的特征 素域

□ 例 1　设p是素数，则模p剩余类环$\mathbf{Z}_p$是一个域，$\mathbf{Z}_p$的特征为p.

□ 证明　容易看出$\mathbf{Z}_p$中单位元［1］的加法周期为p，故知$\mathbf{Z}_p$的特征为p.

□ 例 2　有理数域$\mathbf{Q}$的特征为 0 .

□ 证明　因为对任意正整数n，$n1 = n \neq 0$. 故 1 的加法周期为∞，故$\mathbf{Q}$的特征为 0 .

域的特征 素域

- 定理 2　S是F的子域，则S与F具有相同的特征.

- 证明：S与F的运算相同，具有相同的 0 ，1,….

- 定理 3　n元有限域的特征必为素数p，且$p \mid n$.

- 证明　若F是n元有限域，则〈F，＋〉是n阶群，故 1 ∈F在〈F，＋〉中的周期必为有限数p，且$p \mid n$. 由定义，F的特征为p. 且由定理1知p为素数.

域的特征 素域

定义3 设〈R，＋，·〉，〈S，⊕，⊗〉是两个环，$f: R \to S$，如果f保持运算，即满足：

$$f(a+b)=f(a)\oplus f(b)$$

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

则称f是环R到环S的同态.

域的特征 素域

定理 4 若域F的特征为素数p，则F中必存在与$\mathbf{Z}p$同构的子域 $\mathbf{Z}'p$.

证明 设e是F的单位元，令$\mathbf{Z}'p = \{ie \mid i \in \mathbf{Z}\}$

因为e的加法周期为p，故

$$\mathbf{Z}'p = \{0, e, 2e, \ldots, (p-1)e\}$$

作$\mathbf{Z}p$到$\mathbf{Z}'p$的映射 φ: $[i] \mapsto ie$, $[i] \in \mathbf{Z}p$

显然 φ 是$\mathbf{Z}p$到$\mathbf{Z}'p$的双射.下证 φ 保持运算.

$$\varphi([i] +_p [j]) = \varphi([i+j]) = (i+j)e$$

$$= (ie) + (je) = \varphi([i]) + \varphi([j])$$

$$\varphi([i] \times_p [j]) = \varphi([ij]) = (ij)e$$

$$= (ie) \cdot (je) = \varphi([i]) \cdot \varphi([j])$$

由此便知 φ 是$\mathbf{Z}p$到$\mathbf{Z}'p$的同构，即 φ: $\mathbf{Z}p \cong \mathbf{Z}'p$.

由于$\mathbf{Z}p$是域，与之同构的$\mathbf{Z}'p$必为域，从而是F的子域.

域的特征 素域

- 设F是一个特征为素数p的域，

  F的任何子域S，必包含单位元e，

  从而包含e的所有整数倍ie，故$\mathbf{Z}'_p \subseteq S$.

  因此$\mathbf{Z}'_p$是F的最小子域.

  从同构观点来看，特征为素数p的域F含有$\mathbf{Z}_p$为其最小子域.

- 若域F的特征为 0，则$\mathbf{Z}'0 = \{ie \mid i \in \mathbf{Z}\}$与整数环$\mathbf{Z}$同构，不能构成$F$的子域

域的特征 素域

定理 5 若域F的特征为 0，则F中含有与有理数域$\mathbf{Q}$同构的子域.

证明 用e表示F的单位元，令

$$\mathbf{Q}' = \left\{ \frac{me}{ne} \mid m, n \in \mathbf{Z}, n \neq 0 \right\},$$

作有理数域$\mathbf{Q}$到$\mathbf{Q}'$的映射

$$\varphi: \quad \frac{m}{n} \longmapsto \frac{me}{ne}, \quad m, \frac{me}{ne} \in \mathbf{Z}, \quad n \neq 0 .$$

域的特征 素域

- 以上定义是合理的，即有理数q的象由q唯一确定, 而与其表示方法无关：

设 $\frac{m}{n}=\frac{m'}{n'}$，则$mn'=nm'$， 故

$(mn')e=(nm')e$. 由于

$(mn')e=m(n'e)=(me)\ (n'e)$，

$(nm')e=n(m'e)=(ne)\ (m'e)$，

故$(me)\ (n'e)=(ne)\ (m'e)$ $\frac{me}{ne}=\frac{m'e}{n'e}$

同乘 $(n'e)^{-1}$ $(ne)^{-1}$ 有 $\varphi(\frac{m}{n})=\varphi(\frac{m'}{n'})$ 或说

域的特征 素域

□不难看出 φ 是满射，且容易验证 φ 是单射、保持运算，因而 φ: $\mathbf{Q} \cong \mathbf{Q}'$.

由于$\mathbf{Q}$是域，知$\mathbf{Q}'$是域，从而是F的子域，这样就证明了F中存在与$\mathbf{Q}$同构的子域

域的特征 素域

- 设F是一特征为 0 的域，则对F的任何子域S，S必包含F的单位元e，从而包含e的所有整数倍me，由域的定义，

  $(me)^{-1}$ 及形如$(me)(ne)^{-1}$的元素均应包含在S中，故 $\mathbf{Q}' \subseteq S$. 因此$\mathbf{Q}'$是F的最小子域.

- 从同构观点来看，特征为 0 的域F包含有理数域$\mathbf{Q}$为其最小子域.

域的特征 素域

- 如果将F中的单位元记为 1，则F中的元素me，可记作m，可记作 $\frac{me}{ne}$ $\frac{m}{n}$
- 特别地，对于素域$\mathbf{Z}p$，其中的元素$[i]=i\,[1]$常记为i，在这种记号下，$\mathbf{Z}_p=\{0,\ 1,\ \ldots,\ p-1\}$.

作业

习题四 1、2