近世代数

计算机科学与技术学院
苏敬勇

内容

- 第一章 基本概念
- 第二章 群
- 第三章 正规子群和群的同态与同构
- 第四章 环与域

第四章 环与域

- 环的定义
- 环的零因子和特征
- 除环和域

第四章 环与域

- 数、多项式、函数、矩阵和线性变换------有**两个代数运算**。
- 有两个代数运算的代数系统中，最基本最重要的就是**环与域**。
- 从加群而来。。。

1）可交换群，运算用“+”表示；

2）单位元称为零元，用“0”表示； $0+a=a+0=a$

3）元素a的逆元用“-a”表示，称为负元； $a+\left(-a\right)=-a+a=0$

4）若把 $a+\left(-b\right)$ 简记为 $a-b$，那么在加群中就有了一个减法，它是加法的逆运算。

易知，加群中以下运算律成立：

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

乘群中指数运算规则在加群中自然改为倍数规则：

$$0a = 0,$$

$$na = \overbrace{a + \cdots + a}^{n},$$

$$(-n)a = n(-a) = -(na)$$

对任意的整数 m,n 又有

$$ma + na = (m+n)a,$$

$$m(na) = (mn)a,$$

$$n(a+b) = na + nb$$

相应地，加群的非空子集H能作成子群的充要条件改写为：

$$a,b \in H \Rightarrow a+b \in H,$$

$$a \in H \Rightarrow -a \in H$$

或

$$a,b \in H \Rightarrow a-b \in H$$

第四章 环与域

- **定义1**：设非空集合R有两个代数运算，一个叫做加法（一般用+表示），另一个叫做乘法。如果：

1）R对加法作成一个加群；

2）R对乘法满足结合律：

$$(ab)c = a(bc)\ ;$$

3）乘法对加法满足左右分配律：

$$a(b+c) = ab + ac,\quad (b+c)a = ba + ca,$$

其中a,b,c为R中任意元素，则称R对这两个代数运算作成一个环。

例：数环都是环；另外，数域F上的全体**多项式的集合F[x]**，数域F上全体**n阶方阵的集合**以及数域F上一个向量空间的**全体线性变换的集合**。对各自的加法和乘法都作成环。分别称为：数域F上的**多项式环**、**n阶全阵环**和**线性变换环**。

- 若环R的乘法满足交换律，即对R中任意元素a,b都有$ab = ba$

则称R为交换环（可换环）；否则称R为非交换环（非可换环）。

- 若环R有有限个元素称为有限环，否则称为无限环；对应R的阶为有限环的元素个数，无限环阶无限，阶记为 $|R|$。
- **例1**：设R是一个加群，再对R中任意元素a，b规定

$$ab=0$$

则R显然作成一个环，称为**零环**。

- **例2**：设R为整数集。证明R对以下二元运算作成环：

$$a\oplus b=a+b-1,\quad a\circ b=a+b-ab$$

证明：首先，R关于⊕作成一个加群，1是零元，2-a是a的负元。

其次，乘法满足结合律 $(a\circ b)\circ c=a\circ(b\circ c)$

再次，乘法关于加法满足分配律

$$a\circ(b\oplus c)=(a\circ b)\oplus(a\circ c)$$

且乘法下可交换，故R在此两个代数运算下成交换环。

- **定义2**：如果环R中有元素e，它对环R中每个元素a都有

$$ea = a$$

则称e为环R的**一个左单位元**；如果环R中有元素e'，它对R中每个元素a都有

$$ae' = a$$

则称e'为环R的**一个右单位元**。

•**注**：

1）既是左单位元又是右单位元的元素，叫做R的**单位元**。环对乘法作成半群，环的左右单位元或单位元也是此半群的左右单位元或单位元。

2）若环R有单位元，则唯一，一般用1表示。

3）一个环可能既无左单位元又无右单位元，如偶数环；也可能只有左单位元，而无右单位元，或者只有右单位元而无左单位元。如下两例。

- 例：有左单位元但无右单位元：数域F上一切形如

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \quad (\forall a,b\in F)$$

的方阵作成环，$\begin{pmatrix} 1 & x \\ 0 & 0 \end{pmatrix} \quad (\forall x\in F)$都是左单位元，但无右单位元。反之，也可能

只有右单位元，而无左单位元，例如数域F上一切形如

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \quad (\forall a,b\in F)$$

的方阵作成的环，$\begin{pmatrix} 1 & 0 \\ x & 0 \end{pmatrix} \quad (\forall x\in F)$都是右单位元，但无左单位元。

第四章 环与域

- 环中元素在乘法中的运算规则：

1） $0a = a0 = 0$ “零乘”，0是环R的零元

因为 $0a + 0a = (0+0)a = 0a \quad \Rightarrow 0a = 0$

$a0 + a0 = a(0+0) = a0 \quad \Rightarrow a0 = 0$

2） $(-a)b = a(-b) = -ab$ “负乘”

因为 $(-a)b + ab = (-a+a)b = 0b = 0$，故 $(-a)b = -ab$

同理 $a(-b) = -ab$，故 $(-a)b = a(-b) = -ab$ 。

3） $(-a)(-b) = ab$ “负负乘”

因为 $(-a)(-b) = a[-(-b)] = ab$

4） $c(a-b) = ca - cb,\quad (a-b)c = ac - bc$ “负分配”

因为 $c(a-b) = c[a+(-b)] = ca + c(-b) = ca - cb,$

$(a-b)c = [a+(-b)]c = ac + (-b)c = ac = bc$

5） $\left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right)=\sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j$ “多元分配”

证明方法---数学归纳

6） $(ma)(nb)=(na)(mb)=(mn)(ab)$ ，m，n为任意整数 “等元分配”

因为：m，n都为正整数是5）特例；

m，n中有零，成为1）的情况；

m，n中有负整数，利用环中加法的运算规则和2）或3）即得证。

- 此外，还可引入环中元素的正整数次幂的概念

$$a^n=\overbrace{aa\cdots a}^{n}$$

- 若有单位元则 $a^0=1$
- 若有逆元则

$$a^{-n}=\left(a^{-1}\right)^n$$

- **注**：1）通常的指数运算规则成立

2）由于环的乘法不一定可交换故如下运算不一定成立

$$(ab)^n = a^n b^n, \quad (a+b)^2 = a^2 + 2ab + b^2$$

- **定义3**：设S是环R的一个非空子集。如果S对R的加法与乘法也作成一个环，则称S是R的一个**子环**，记为 $S \le R$ 或 $R \ge S$ 。

- **定理1**：环R的非空子集S作成子环的充要条件是

$$a,b \in S \Rightarrow a-b \in S$$

$$a,b \in S \Rightarrow ab \in S$$

证明：充分性显然（条件推定义）；

必要性更显然（已经成环，条件自然成立）。

当S为R的一个非空有限子集时，上述的充分必要条件改为两个封闭即可。

- 设S是R的一个子环

当R有单位元时，S不一定有；当S有单位元时，R不一定有；即使二者都有单位元，此单位元也未必相同。

- **例3**：环R上的n阶全阵环 $R_{n\times n}$ ：设R为任意环，称

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \qquad \left(a_{ij}\in R\right)$$

为环R上的一个 $m\times n$ 矩阵。当 $m=n$ 时，称A为环R上的一个n阶方阵。

环上所有n阶方阵关于矩阵的加法和乘法构成环，表示为 $R_{n\times n}$ ，称为环R上的n阶全阵环。

- 一个环关于其加法作成一个加群，用 $(R,+)$ 表示，并称其为环R的加群。如果 $(R,+)$ 是一个循环群，则称环R是一个循环环。即

若 $(R,+)=\langle a\rangle$ ，则循环环R可表示为

$$R=\{\cdots,-2a,-a,0,a,2a,\cdots\},\quad a^2=ka,\quad k\in Z$$

若a在加群 $(R,+)$ 中的阶为n，则R可表示为

$$R=\{0,a,2a,\cdots,(n-1)a\},\quad a^2=ka,\quad 0\le k\le n-1,\quad k\in Z$$

- 注：

1）整数环是一个无限循环环。

2）循环环必是交换环。

3）循环环子环也为循环环。

4）循环环不一定有单位元。（例如：偶数环）

环的定义

- **定理2**：素数阶环，更一般地，阶为互异素数之积的有限环必为循环环。

证明：思路（第三章2节推论）--- 环中加群为循环群

- **注**：2，3，5，7，10，11，13，14，15，17，19，21，23，29，30…阶环均为循环环。
- 非结合环（乘法不满足结合律）
- 拟环（加法不要求可换）
- 半环（加法只要求作成半群）