第五部分　代数结构

第14章　代数系统

计算机（软件）学院

林　兰

linlan@scu.edu.cn

代数系统

代数系统又称为代数结构，群、环、域、格和布尔代数是典型的代数系统。代数系统理论对于可计算模型研究、抽象数据结构、形式语言理论、程序设计语言语义分析等许多方面产生的影响是深远的。

代数系统理论提供了对各种表面上不同的实际问题高度抽象的途径，使人们更能把握住事物的本质，进行形式化的研究，又反过来指导实践的深入。

主要内容

- 14.1 二元运算
- 14.2 代数系统

14.1 二元运算

f关于S是封闭的。

1. 定义

设S是一个非空集合，映射（或函数）f ：$S^n \to S$称为S上的n元代数运算，简称n元运算。当n＝1时，称为一元运算；当n＝2时，称为二元运算。

- 通常f(a, b)用中缀表示法：a+b，a×b
- 通常采用符号“•”，“。”，“*”表示一般的二元运算符。

14.1 二元运算

例如 设集合S={a, b, c, d}，在S上定义一种二元运算“•”，运算表如下。

•	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	b	d
d	a	d	c	b

14.1 二元运算

2. 二元运算的性质（基本运算定律）

设"•"是定义在集合S上的二元运算。如果

① ∀a，b∈S，a•b∈S，则称“ • ”在S上是封闭的；

② ∀a，b∈S，a•b= b•a，则称“ • ”在S上是可交换的，或称满足交换律；

③ ∀a, b, c∈S，（a•b）•c=a•（b•c），则称"•"在S上是可结合的，或称满足结合律；

④ ∀a∈S，a•a=a，则称“ • ”在S上是幂等的。

例如：（1）自然数集合N上的+，×，-运算。

（2）幂集2^A上的∪，∩运算。

14.1 二元运算

设“•”是定义在集合S上的二元运算。 对∀x, y∈S，

（1）若$\exists a \in S$，如果$a \bullet x = a \bullet y$，$(a \neq \theta)$，则$x = y$，则称$a$为S上关于运算“•”的左可消去元；

（2）若$\exists a \in S$，如果$x \bullet a = y \bullet a$，$(a \neq \theta)$，则$x = y$，则称$a$为S上关于运算“•”的右可消去元；

（3）若$\exists a \in S$，如果a既是上左可消去元，又是右可消去元，则称a为S上关于运算“•”的可消去元；

（4）若对$\forall a \in S(a \neq \theta)$，都是S上的可消去元，则称运算“ • ”在S上满足可消去律。

14.1 二元运算

设“•”和“∗”是同时定义在S上的两个二元运算。如果对∀a,b,c∈S，

① 若 a•(b∗c)=(a•b)∗(a•c)且(b∗c)•a=(b•a)∗(c•a)，则称“•”对“∗”在S上满足分配律。

② 设“•”、“∗”是可换运算，若a•(a∗b)=a及a∗(a•b)=a，则称运算“∗”与“•”满足吸收律。

例如：(1)数集上，×关于+是可分配的， 但+关于×是不可分配的。

(2)幂集2^A上的∪，∩运算相互可分配，且都满足吸收律。

主要内容

- 14.1 二元运算
- 14.2 代数系统

14.2 代数系统

1. 定义

一个非空集合S连同若干个定义在S上的运算$f_1, f_2, \ldots, f_m$所组成的系统称为一个**代数系统**，记为$\langle S, f_1, f_2, \ldots, f_m \rangle$。

✓ 两个要点：① 集合S非空；

② 这些运算$f_1, f_2, \ldots f_m$关于S是封闭的。

例如：常见的代数系统有$\langle Z, + \rangle$，$\langle Z, \times \rangle$，$\langle Q, +, \times \rangle$，$\langle 2^A, \cup, \cap \rangle$。

同一个集合与不同的运算构成不同的代数系统

$\langle Z, + \rangle$，$\langle Z, \times \rangle$，$\langle Z, \max \rangle$。

14.2 代数系统

2. 代数系统中的特异元

(1) 定义(幺元)

设“∗”是集合S上的二元运算，〈S, ∗〉是一个代数系统，如果$\exists e\in S$，使得对$\forall a\in S$，都有：$a*e=e*a=a$，则称e为(代数系统）的单位元或幺元;

例如：

< Z, + > ，0是幺元

< Z, × > ，1是幺元

< 2^A, ∪ >，∅是幺元

14.2 代数系统

(2) 定义（零元）：

设〈S, $*$〉是一个代数系统，如果$\exists\theta \in S$, 使得对$\forall a \in S$, 都有：　$a * \theta = \theta * a = \theta$，则称$\theta$为(代数系统）的零元。

例如：< Z, + > ，没有零元

< Z, × > ，0是零元

< 2^A, ∪ >，A是零元

14.2 代数系统

(3) 定义（幂等元）：

设〈S，•〉是一个代数系统，如果元素a∈S，满足a*a＝a，则称a是(代数系统）的一个幂等元。

例如：< Z， + > ，0是唯一的幂等元

< Z， × > ，0，1是幂等元

< 2^A， ∪ >，每个元都是幂等元(运算满足幂等律)

- 幂等元不一定唯一。

14.2 代数系统

(4) 定义（逆元）：

设在代数系统<S，•>中，e是幺元，**a**是S中的一个元素。如果∃b∈S，使得a•b=b•a=e，则称b是a的逆元，a也称为可逆的，记为$b=a^{-1}$。（同样，a也为b的逆元，b也称为可逆的，记为b^{-1}）

例如：< Z，+ >，每个元a都有逆元−a

< Z，× >，−1, 1有逆元自身，其它元没有逆元。

- 在一个代数系统中，并不是每个元都有逆元！

14.2 代数系统

- 特异元的性质

定理　设〈S, ∗〉是一个代数系统：

1）若〈S, ∗〉存在幺元，则该幺元唯一；

2）若〈S, ∗〉存在零元，则该零元唯一；

3）若“∗”满足结合律且e是〈S, ∗〉的幺元(即幺元存在)，则对∀a∈S，若a存在逆元, 则该逆元唯一。

证明：1）（反证法）设〈S, ∗〉含有幺元e_1，e_2，根据定义

$e_1=e_1*e_2=e_2$，因此，幺元是唯一的。

3）设e是〈S, ∗〉的幺元，元素a有两个逆元a_1，a_2，

则　$a_1=a_1*e= a_1*(a*a_2) = (a_1*a)*a_2=e*a_2=a_2$

因此，逆元也是唯一的。

14.1 二元运算

例1 设$S=\{a,b\}$，则在S上可以定义多少个二元运算？

有多少个运算表即有多少个二元运算。设S是n元集合，运算表有n^2个元素，所以，共可以定义n^{n^2}个不同的二元运算。

此处，可定义2^4个二元运算。

其中的四个运算f_1，f_2，f_3，f_4如下面运算表：

f_1	a	b
a	a	a
b	a	a

f_2	a	b
a	a	b
b	b	a

f_3	a	b
a	b	a
b	a	a

f_4	a	b
a	a	b
b	a	b

满足交换律的有 f_1,f_2,f_3；满足幂等律的有 f_4；有幺元的是 f_2；有零元的是 f_1。

14.2 代数系统

3. 二元运算的代数系统分层

一般地，我们把只含一个二元运算的代数系统<S, ∗>称为二元代数。

定义 设<S, •>是一个代数系统，则

- 当"•"是封闭的，称<S, •>为广群。
- 如果<S, •>是广群，且"•"是可结合运算，则称<S, •>是半群。
- 如果<S, •>是半群，且存在幺元，则称<S, •>为含幺半群。
- 如果<S, •>是含幺半群，且每个元素都有逆元，则称<S, •>为群。

- 群⊂含幺半群⊂半群⊂广群

14.2 代数系统

例2 设$\underline{n}$＝｛0, 1, 2, …, n-1｝，定义$\underline{n}$上的运算$+_n$如下：$\forall x, y \in \underline{n}$，$x+_n y = x+y \pmod{n}$（即为x＋y除以n的余数）。证明$\langle \underline{n}, +_n \rangle$是含幺半群。

证明：①封闭性：$\forall x, y \in \underline{n}$，令$k = x+y \pmod{n}$，则$0 \leqslant k \leqslant n-1$，即$k \in \underline{n}$，所以封闭性成立；

②结合律：$\forall x, y, z \in \underline{n}$，有

$$(x+_n y)+_n z = x+y+z \pmod{n} = x+_n (y+_n z)$$

所以结合律成立。

③单位元：$\forall x \in \underline{n}$，显然有$0+_n x = x+_n 0 = x$

所以0是单位元。

故$\langle \underline{n}, +_n \rangle$是含幺半群。

14.2 代数系统

例3 设$k\in Z$，令集合$S_k=\{x \mid (x\in Z)\wedge(x\geq k)\}$，“+”是一个普通的加法运算，试判断$\langle S_k, +\rangle$是否是一个半群？

解：(1) 显然二元运算“+”是可结合的；

(2) ① 若 $k<0$， 由于 $k\in S_k$， 而 $(k+k)=2k<k$， 即 $(k+k)\notin S_k$，故运算“+”在S_k上不是封闭的；

② 若$k\geq 0$，则对$\forall x$，$y\in S_k$，有$(x+y)\in S_k$，所以运算“+”在S_k上是封闭的。

由1)、2)知：当$k<0$时，$\langle S_k, +\rangle$不是半群；当$k\geq 0$时，$\langle S_k, +\rangle$是一个半群。

14.2 代数系统

例4

1. $\langle Z, +\rangle$, $\langle N, +\rangle$, $\langle R, +\rangle$是一个可换的含幺半群；

   0是单位元，也是唯一的幂等元，但没有零元。

2. $\langle Z, \times\rangle$, $\langle N, \times\rangle$, $\langle R, \times\rangle$是一个可换的含幺半群；

   1是单位元，0是零元，1和0都是幂等元。

3. $\langle Q^+, +\rangle$是半群，但不是含幺半群；

   无幂等元和零元。

14.2 代数系统

4. 设$M_n(R)$为全体$n \times n(n \geq 2)$实数矩阵集合，+和·分别是矩阵的加法和乘法运算，则

① $\langle M_n(R), +\rangle$可交换的含幺半群，

其幺元为零矩阵；也是唯一的幂等元；无零元；

② $\langle M_n(R), \cdot\rangle$是含幺半群，

其幺元为单位矩阵，零矩阵是零元，单位矩阵和零矩阵都是幂等元。

14.2 代数系统

5. 设A＝{a, b, c, ⋯, z}，A中的元素称为字符，由A中有限个字符组成的序列称为A中的字符串，不包含任何字符的字符串称为空串，用ε表示，令

$$A^*=\{x \mid x\text{是A中的字符串}\}$$

α·β为两个字符串的连接：即对任意两个字符串α、β，α·β为将字符串α写在字符串β的左边而得到的字符串。

显然，α·β既是A*上的二元运算（封闭的），并且满足结合律，但不满足交换律；又对任意α∈A*，有α·ε＝ε·α＝α，所以ε 是A*中关于运算的幺元；也是唯一的幂等元；无零元。

因此，<A*, ·>是含幺半群。

作业

✓习题十四

4、5、6