近世代数

李　涛

litao_l@hit.edu.cn

哈工大计算机系软件教研室

教材：离散数学引论

王义和，哈工大出版社

参考教材：

1）近世代数， 熊全淹，武大

2）近世代数基础习题指导，北师大

3）离散数学及其在计算机中的应用

4）代数结构与组合数学

引 言

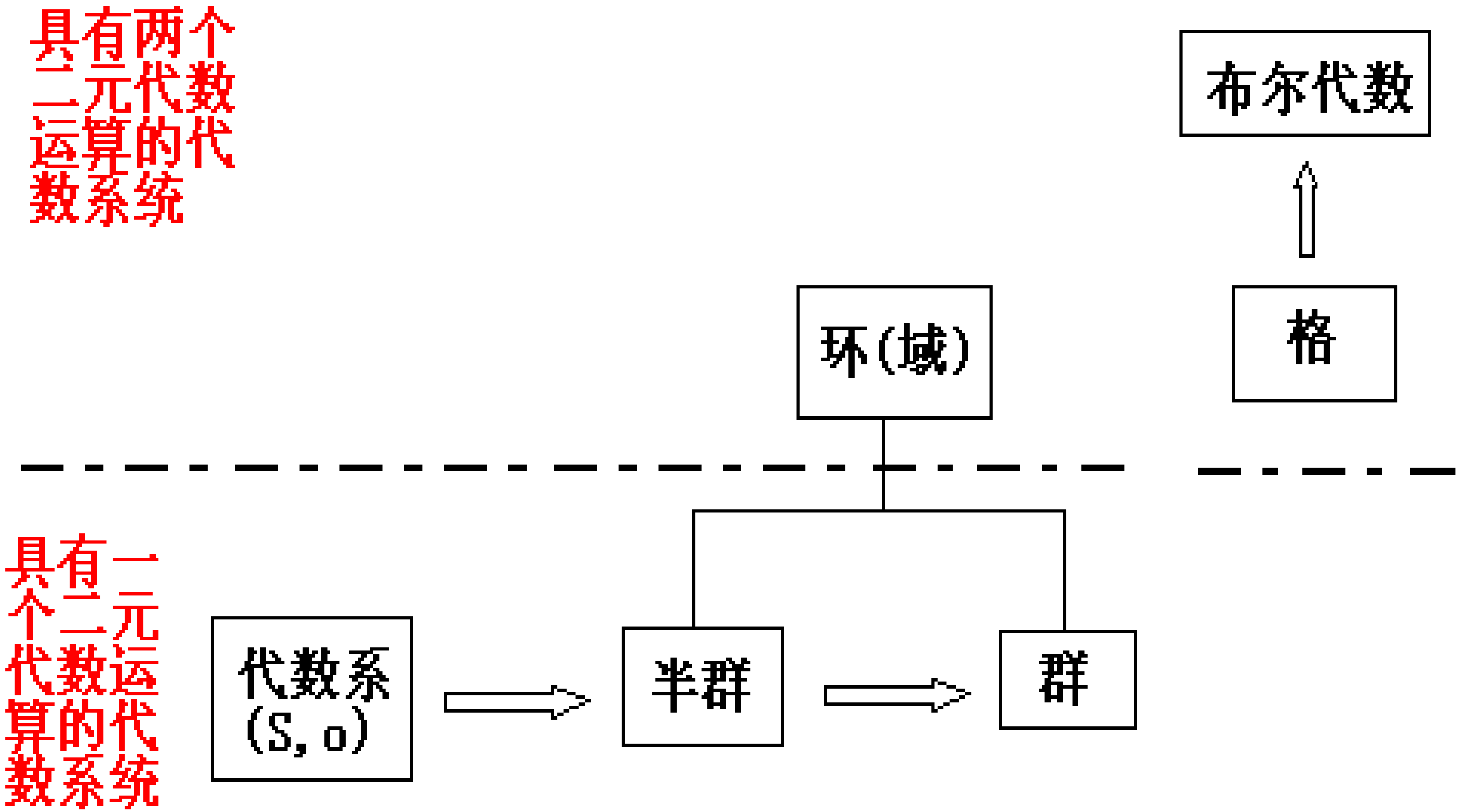
一、近世代数的研究对象

代数最初主要研究的是数，以及由数所衍生出来的对象，如代数方程的求根。数的基本特征是可以进行加法、乘法等运算，其共同点是对任两个数，通过相应法则可唯一求得第三个数。而对于很多抽象的对象也都具有类似数的这一特征，因此对于它们的结构和性质的研究就导致了近世代数的产生和发展。

近世代数拓展了代数的研究领域，它所研究的不再仅仅是数，而是具有某种（些）运算的代数系统。

即近世代数的主要研究对象是具有代数运算的集合（称为代数系）。比如最基本的有群、环和域。

二、本课程的内容体系



第1章 半群和幺半群

主要内容:

1）代数系的基本概念;

2）基本的代数系：半群、幺半群
子半群、子幺半群的定义及简
单性质定理;

3）代数系之间的同态、同构:
以（幺）半群为例

§1.1 若干基本概念

主要内容：

1）n元代数运算及其性质：结合律、交换律、分配律；

2）代数系：（左、右）单位元；

3）代数系半群、幺半群：定义、单位元、逆元及其相关性质。

定义1 映射：设X和Y是两个非空集合. 一个从X到Y的映射是一个满足以下两个条件的X×Y的子集f：

1)对X的**每一个**元素x，**存在**一个$y \in Y$使得$(x, y) \in f$

2)若(x, y)、$(x, y') \in f$，则 $y = y'$

定义2 二元代数运算:设X是一个集合,一个从X×X到X的映射 φ 称为X上的二元代数运算。

符号表示:“$\circ$”或“$\bullet$”,称为乘法,

记为 $x \circ y$ 称作x与y的积。

定义3 一元代数运算：一个从集合X到集合Y的映射称为X到Y的一个一元代数运算。当X＝Y时，则称此一元代数运算为X上的一元代数运算。

注：X上的一元和二元代数运算均满足运算的封闭性。

定义4 结合律：设“$\circ$”是X上的一个二元代数运算。如果$\forall a,b,c\in X$有：$(a\circ b)\circ c = a\circ(b\circ c)$

则称此二元代数运算适合结合律。

交换律：若对$\forall a,b \in X$有：

$$a \circ b = b \circ a$$

则称此二元代数运算适合交换律。

定义5 设“$\circ$”是非空集合S上的一个二元代数运算，则称二元组$(S,\circ)$为一个(有一个代数运算的)代数系。

定理1 设 $(S,\circ)$ 是一个代数系，如果二元代数运算“$\circ$”适合结合律，则 $\forall a_i \in S, i=1,2,\cdots n$, n个元素 $a_1, a_2, \cdots, a_n$ 的乘积仅与这n个元素及其次序有关而唯一确定。

定理2 设$(S,\circ)$是一个代数系，如果二元代数运算“$\circ$”适合结合律和交换律，则$\forall a_i \in S, i=1,2,\cdots n,$ n个元素$a_1, a_2, \cdots, a_n$的乘积仅与这n个元素有关而与它们的次序无关。

例 仅满足结合律而不满足交换律：

1）矩阵乘法　2）映射的复合运算

3）字符串的复合运算

同时满足结合律与交换律：

1）普通乘法　2）集合的并、交

3）逻辑与、逻辑或

两者均不满足：

1）普通除法　2）整除运算

仅满足交换律但不满足结合律：

定义乘法“$\circ$”：$N \times N \to N$

$$a \circ b = a * b + 1, a, b \in N,$$

其中*为普通乘法

定义6 设$(S,\circ,+)$是具有两个二元代数运算“$\circ$”和“$+$”的代数系。

如果$\forall a,b,c\in S$ 有：

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

则称“$\circ$”对“$+$”满足左分配律。

如果$\forall a,b,c\in S$ 有：

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

则称“$\circ$”对“＋”满足右分配律。

如果二元代数运算“$\circ$”满足交换律，

则左分配律与右分配律合为一，

此时称"$\circ$"对“＋”满足分配律。

定理3 设$(S,\circ,+)$是具有两个二元代数运算的代数系。如果加法“＋”满足结合律“∘”对“＋”满足左(右)分配律则对$\forall a_i \in S, i=1,2,\cdots n,$ 有：

$$a\circ(a_1+a_2+\cdots+a_n)=$$
$$(a\circ a_1)+(a\circ a_2)+\cdots+(a\circ a_n)$$
$$(a_1+a_2+\cdots+a_n)\circ a=$$
$$(a_1\circ a)+(a_2\circ a)+\cdots+(a_n\circ a)$$

定义7 设$(S,\circ)$是一个代数系，如果存在一个元素$a_l \in S$使得$\forall a \in S$有：

$$a_l \circ a = a$$

则称a_l为乘法“$\circ$”的左单位元素；

如果存在一个元素$a_r \in S$ 使得$\forall a \in S$有：$a \circ a_r = a$

则称a_r为乘法“$\circ$”的右单位元素；

如果存在一个元素$e \in S$使得$\forall a \in S$有：$e \circ a = a \circ e = a$

则称e为乘法“$\circ$”的单位元素；

例 （R, +, 0）

（R, *, 1）

$(2^S, \cup, \phi)$

定理4 设$(S,\circ)$是一个代数系，如果二元代数运算“$\circ$”既有左单位元a_l又有右单位元a_r 则 $a_l = a_r$ 从而有单位元。

注：若二元代数运算“$\circ$”满足交换律，则习惯上用“＋”代替“$\circ$”称为加法，若此时还有单位元，则单位元用“**0**”表示。

定义8 设$(S,\circ)$是一个代数系。若存在一个元素$z\in S$使得$\forall a\in S$ 有:

$$z\circ a=a\circ z=z$$

则称z是“$\circ$”的零元素.

定义9 设 $(S,\circ)$是一个代数系。$A, B \subseteq S$

定义：$A \circ B = \{a \circ b \mid a \in A 且 b \in B\}$

简记为AB。而把 $a \circ b$ 写成ab。

特别地，当A＝{a}时，AB＝{a}B,

简记为aB，即：

$$aB = \{a \circ b | b \in B\}, \; Ba = \{b \circ a | b \in B\}$$