离 散 数 学

Discrete Mathematics

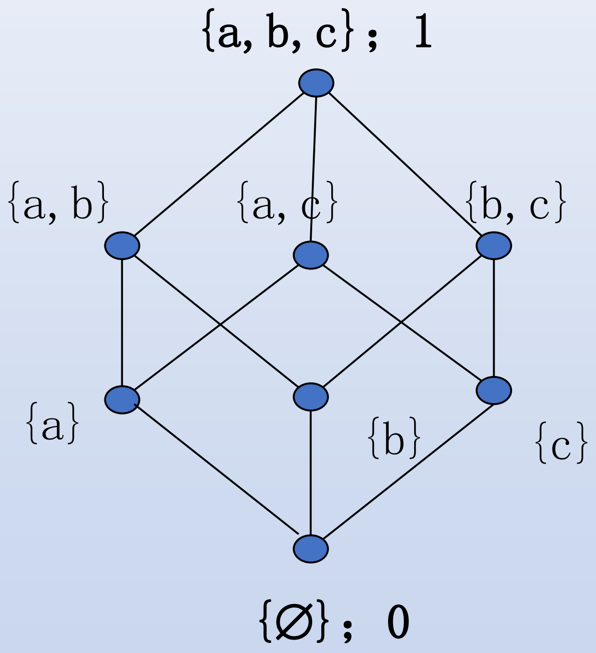
第4章 代数系统

$<2^U; ', \cup, \cap>$ 集合代数

$<N; +>$，$<N; \times>$

$<I;\ +, \times>$

$<Z_3;\ \oplus_3, \odot_3>$模3加、乘



第4章 代数系统

代数论由法国数学家**伽罗华**创立。

代数论的建立解决了古典数学难题：高次方程求根、倍立方、化圆为方、三等分角和作正n边形。

集合、**数理逻辑**和**布尔代数**从代数论的角度看是同一个代数系统，三者在代数论的基础上统一了起来。

4.1 运算

定义4-1 运算：设有非空集合A，**函数**f：$A^n \to A$称为A上的一个**n元运算**，n称为**运算的阶**。

函数 **f**：$A^2 \to A$是A上的二元运算，函数 **f**：$A \to A$是A上的一元运算。

例 ∪、∩：$(2^U)^2 \to 2^U$，是2^U上的二元运算。

例 A={0, 1, 2, …, p-1]} (p为正整数≥2)，则 x, y∈A，

模p加法：x+y(modp)，模p乘法：x×y(modp)都是A上的运算。

实数域上的加、减、乘、除运算。

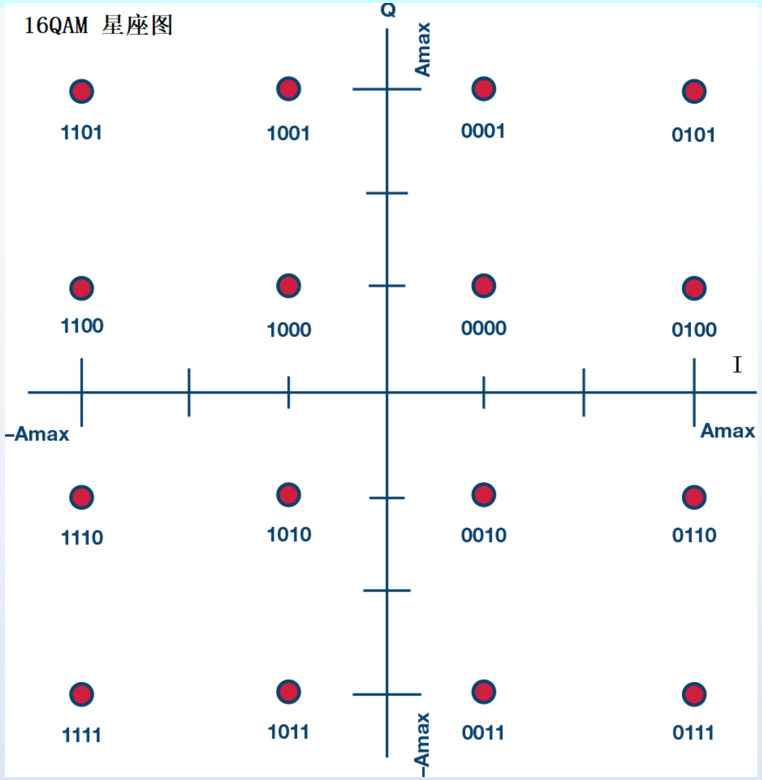
有时运算可以用表格来定义

+	a	b
a	a	a
b	b	a

●	a	b
a	a	a
b	a	b

*	奇	偶
奇	奇	奇
偶	奇	偶

数字通信中：



一元运算的例子：求集合的补集，关系的逆关系，

数的绝对值，矩阵的转置和逆矩阵

定义4-2 封闭性：设运算*是集合A上的一个n元运算，S⊆A，如果对于每一个$(a_1,a_2,\ldots,a_n)\in S^n$，都有$*(a_1,a_2,\ldots,a_n)\in S$，称**运算*在S上封闭**。

封闭性：运算f：$A^n\rightarrow B$，若B⊆A，则称运算在A上是封闭的。

定义4-3 交换性：设*是集合A上的一个二元运算，如果对于任意的a,b∈A，有

$$a*b=b*a$$

则称**运算*在A上是可交换的**。

定义4-4 结合性：设*是集合A上的一个二元运算，如果对于任意的a,b,c∈A，有

$$a*(b*c)=(a*b)*c$$

则称**运算*在A上是可结合的**。

定义4-5 分配性：设*和⋆是集合A上的二元运算，如果对于任意的a,b,c∈A，有

$$a*(b\star c)=(a*b)\star(a*c)$$

$$(b\star c)*a=(b*a)\star(c*a)$$

则称**运算*在A上对于⋆是可分配的**。

例 ***加法+和乘法**** *运算在自然数域N上*是封闭的、可交换的、可结合的，乘法*对加法+是可分配的。

但***减法-和除法/*** *运算在自然数域N上*是不封闭的，在实数R域上是封闭的，且除法对减法是可分配的。

例 任意集合A的幂集2^A上的**∩和∪运算**，是封闭的、可交换的、可结合的，∩对∪是可分配的，∪对∩也是可分配的。

当运算 * **可结合**时，可表示为

$$a * (b * c)=a * b * c$$

并定义（幂）　$a^1=a$

$a^{n+1}=a^n * a$

则　$a^m * a^n=a^{m+n}$　　$(a^m)^n=a^{mn}$

左单位元：* 是A上的二元运算，如果存在$e_l \in A$，使得对于所有的$a \in A$，有

$$e_l * a=a$$

称e_l为A上关于运算 * 的左单位元。

右单位元：* 是A上的二元运算，如果存在$e_r \in A$，使得对于所有的$a \in A$，有

$$a * e_r=a$$

称e_r为A上关于运算 * 的右单位元。

单位元：* 是A上的二元运算，如果存在$e \in A$，使得对于所有的$a \in A$，有

$$e * a=a * e=a$$

（既是左单位元又是右单位元）

称e为A上关于运算 * 的单位元。

●	a	b
a	a	b
b	a	b

+	a	b
a	a	a
b	b	b

<2^U; ’,∪> 中
$\varnothing \cup A=A \cup \varnothing=A$

<2^U; ’,∩> 中
$U \cap A=A \cap U=A$

浙江大学信息与电子工程学院 电子 宋牟平

定理4-2：如A上的运算∗同时存在左单位元e_l和右单位元e_r，则

$$e_l=e_r=e$$

且e是A上关于∗的唯一单位元。

证明：设存在左单位元和右单位元，即存在$e_l,e_r\in A$，则有

$$e_l=e_l * e_r=e_r=e$$

若e'也是单位元，e'∈A，则

$$e'=e' * e=e$$

单位元是唯一的。

定义4-7 **零元**：∗是A上的二元运算，

如果存在$z_l\in A$，使得对于所有的$a\in A$，有

$$z_l * a = z_l$$

称z_l为A上关于运算∗的左零元。

+	a	b
a	a	a
b	b	b

如果存在$z_r\in A$，使得对于所有的$a\in A$，有

$$a * z_r = z_r$$

称z_r为A上关于运算∗的右零元。

●	a	b
a	a	b
b	a	b

如果存在z∈A，使得对于所有的a∈A，有

$$\mathbf{z * a = a * z = z}$$

（既是左零元又是右零元）

称**z为A上关于运算 * 的**零元。

<2^U; ',∩> 中
∅∩A=A∩∅=∅

<2^U; ',∪> 中
U∪A=A∪ U = U

定理4-4：**如A上的运算 * 同时存在左零元z_l和右零元z_r，则**

$$\mathbf{z_l = z_r = z}$$

且z是A上关于 * 的唯一零元。

证明：设存在左零元和右零元，即存在z_l, z_r∈A，则有

$$z_l=z_l * z_r=z_r=z$$

若z'也是零元，z'∈A，则

$$z'=z' * z=z$$

零元是唯一的。

例 〈Z;+〉，0是单位元，不存在零元。

〈Z;×〉，1是单位元，0是零元。

∩的零元是∅，单位元是U。∪的零元是U，单位元是∅。

例

+	a	b
a	a	a
b	b	b

●	a	b
a	a	b
b	a	b

对运算+，a,b是左零元，也是右单位元。对运算●，a,b是左单位元，也是右零元。可以看到它们不唯一。

定义4-8 **幂等元**： * 是A上的二元运算，若有元素a∈A，满足

$$a * a=a$$

称**a为A上关于运算 * 的幂等元**。对幂等元，有

$$a^n=a$$

定义4-9 **逆元**： * 是A上具有单位元e的运算，

对于a∈A，如存在a_l^{-1}∈A，使

$$a_l^{-1} * a=e$$

则称称**a_l^{-1}为a的左逆元**。

如果存在$a_r^{-1}\in A$，使得

$$a * a_r^{-1}=e$$

称$\mathbf{a_r^{-1}}$**为a的**<u>右逆元</u>。

如果存在$a^{-1}\in A$，使得

$$a^{-1} * a=a * a^{-1}=e$$ （既是左逆元又是右逆元）

称$\mathbf{a^{-1}}$**为a的**<u>逆元</u>。

<u>定理4-4</u>：<u>设 * 是A上具有单位元e的运算</u>，且是<u>可结合的</u>。如果对元素$a\in A$，存在左逆元a_l^{-1}和右逆元a_r^{-1}，则

$$a_l^{-1}=a_r^{-1}=a^{-1}$$

且a^{-1}是a的唯一逆元。

<u>证明</u>：设元素a存在左逆元a_l^{-1}和右逆元a_r^{-1}，则有

$$a_l^{-1}=a_l^{-1} * e= a_l^{-1} * (a * a_r^{-1})=(a_l^{-1} * a) * a_r^{-1}=e * a_r^{-1}=a_r^{-1}$$

若b也是逆元，则

$$b=b * e=b * (a * a^{-1})=(b * a) * a^{-1}=e * a^{-1}=a^{-1}$$

浙江大学信息与电子工程学院 电子 宋牟平

逆元是唯一的。

零元是否可以和单位元相等?

<u>定理4-5</u>：设 * 是A上二元的运算，且#A>1，若运算 * 有单位元e和零元z，则$e \neq z$。

证明：设e=z，因#A>1，所以至少还存在一元素$x \in A$，$x \neq e$，但

$$x=e * x=z * x=z=e$$

与前设矛盾。

4.2 代数系统

代数系统

定义4-10 **代数系统**：**非空集合**和定义在该集合上的一个和多个**运算**所组成的系统称为**代数系统**，用记号$\langle S;O_1,O_2,\ldots,O_n \rangle$表示。

其中S是非空集合，称为该代数系统的**域**，

$O_1,O_2,\ldots,O_n$为S上的**运算**。

例 $\langle 2^U; ', \cup, \cap \rangle$ 集合代数

例 $\langle N;+\rangle$，$\langle N;\times\rangle$

代数系统的**基数**：非空集合的基数。

有限代数系统: 若代数系统的基数有限，称有限代数系统。

子代数系统：<S$_1$;**O**>,<S$_2$;**O**>为两个代数系统，若**$S_2 \subseteq S_1$**，则称<S$_2$;O>为<S$_1$;O>的**子代数系统**，简称**子代数**。若**$S_2 \subset S_1$**，则称<S$_2$;O>为<S$_1$;O>的**真子代数系统**。

例 <N;＋>是<R;＋>的子代数。

*定义4-11 **整环**：若代数系统**<J; +, ·>**满足

(1)交换律 对任意的i,j∈J，有

i+j=j+i，i·j=j·I

(2)结合律 对任意的i,j,k∈J，有

i+(j+k)=(i+j)+k，i·(j·k)=(i·j)·k

(3)分配律 对任意的i,j,k∈J，有

i·(j+k)=(i·j)+(i·k)

(4)单位元 存在元素0,1∈J，使对任意的i∈J

i+0=0+i=i，i·1=1·i=i

(5)+可逆　对任意的$i \in J$，存在元素$-i \in J$，

$$i+(-i)=(-i)+i=0$$

(6)削去律　若$i \neq 0$，则对于任意的$j,k \in J$,有

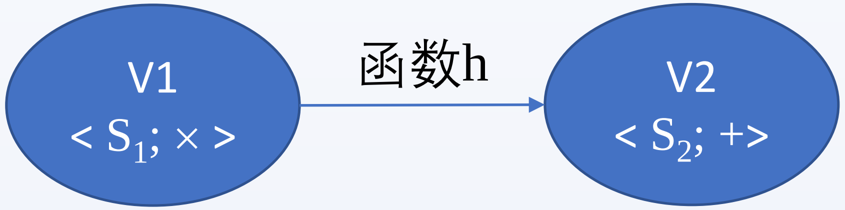
$$i \cdot j=i \cdot k \Rightarrow j=k$$

则称该代数系统为**整环**。

例 $<I;+,\times>$

例 $<Z_3;\oplus_3,\odot_3>$

4.3 同态和同构



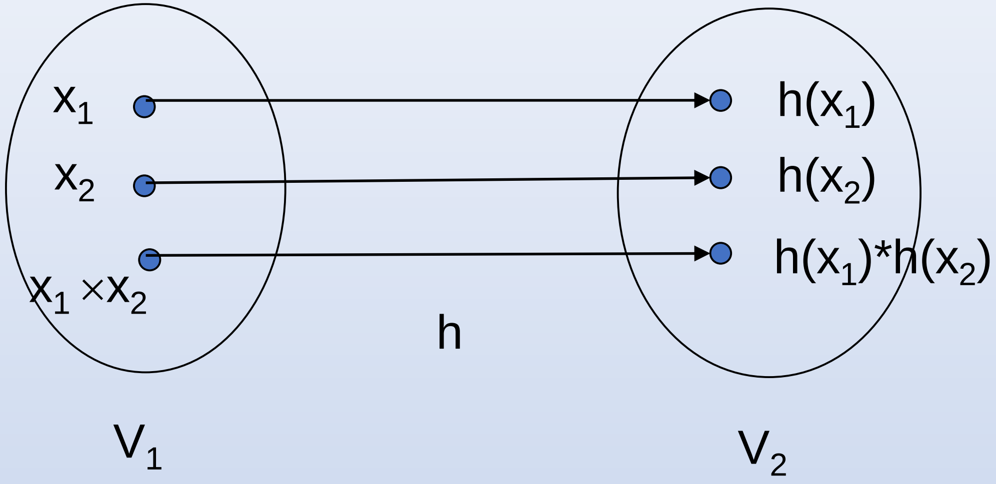
$\log_{10}(x_1 \times x_2)=\log_{10}(x_1)+\log_{10}(x_2)$

<u>同态与同构</u>

同态：$V_1=<S_1;\ \cdot>, V_2=<S_2;\ *>$为两个代数系统，若存在<u>$S_1$到$S_2$**函数h**</u>，对任意的$x_1,x_2 \in S_1$，满足方程

$$h(x_1 \cdot x_2)=h(x_1) * h(x_2)$$

则称h为**V_1到V_2的同态**，**V_2称为V_1的同态像**。



<u>例</u> 代数系统 $V_1=<R;\times>$，$V_2=<R;+>$

函数 $y:R \to R,\ y=\log_{10}x$。

对于任意的$x_1,x_2 \in R$，有

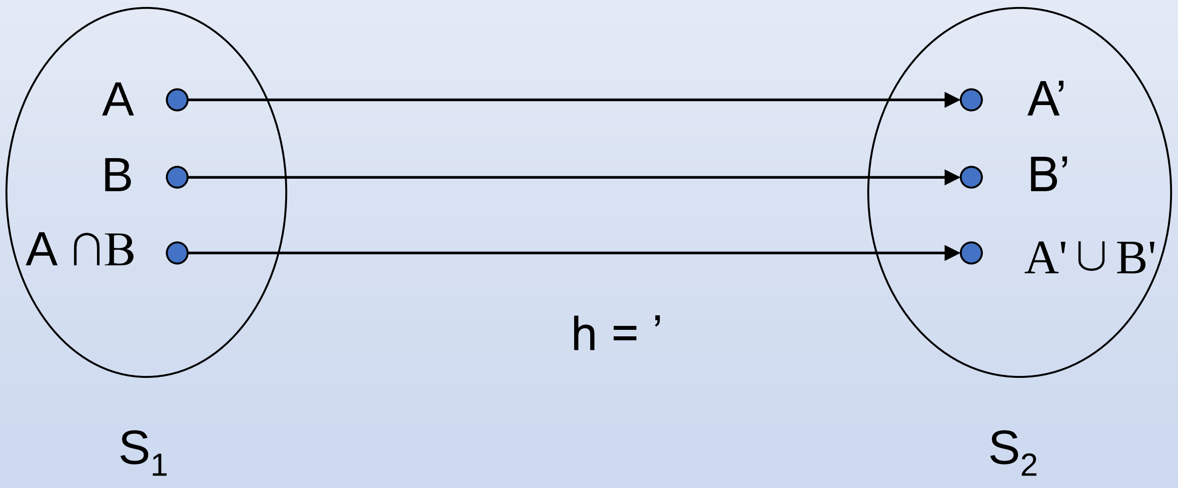
$$y(x_1 \times x_2)=\log_{10}(x_1 \times x_2)=\log_{10}(x_1)+\log_{10}(x_2)$$

满足同态方程，是V_1到V_2的同态。

浙江大学信息与电子工程学院 电子 宋牟平

从上例可以看出，**<u>同态可看成一种变换，将一个代数系统变为另一个代数系统</u>**，一个较复杂的问题转为较易解决的问题：对数尺，传输损耗，放大倍数等。

例 摩根定律 $(A \cap B)' = A' \cup B'$



浙江大学 信息与电子工程学院 电子 宋牟平

例 $V_1=<Z;+>$，$V_2=<Z_6;\oplus_6>$，$Z_6=\{0,1,2,3,4,5\}$，$\oplus_6$是模6加。

定义函数$\mathbf{h:Z\to Z_6}$, 对任意的$i\in Z$，有$\mathbf{h(i)=res_6(i)}$。

证明 h是V_1到V_2的同态。

证明：对任意的$i,j\in Z$,设

$$i=6q_1+r_1,\quad 0\le r_1<6$$

$$j=6q_2+r_2,\quad 0\le r_2<6$$

则 $$i+j=6(q_1+q_2)+(r_1+r_2)$$

$$h(i+j)=res_6(i+j)=res_6(r_1+r_2)$$

$$res_6(i)\oplus_6 res_6(j)=r_1\oplus_6 r_2=res_6(r_1+r_2)$$

故 $$res_6(i+j)=res_6(i)\oplus_6 res_6(j)$$

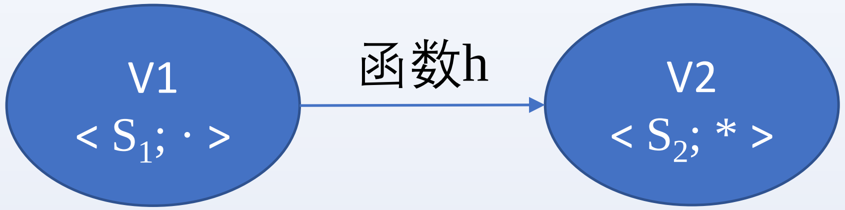
即 $$h(i+j)=h(i)\oplus_6 h(j)$$

<u>定义4-15</u> 设h是V_1到V_2的同态，$V_1=<S_1;\cdot>, V_2=<S_2;*>$，如果

（1）h是单射，则称h为**单同态**；

（2）h是满射，则称h为**满同态**；

（3）h是双射，则称h为**同构**。



<u>定理4-6</u> 若存在代数系统$V_1=<S_1;+_1,*_1>$到$V_2=<S_2;+_2,*_2>$的<u>满同态h</u>，则V_1具有的许多性质可在V_2中保持：

（1）**<u>交换</u>** 若$+_1(*_1)$可交换，则$+_2(*_2)$可交换；

（2）**<u>结合</u>** 若$+_1(*_1)$可结合，则$+_2(*_2)$可结合；

（3）**<u>分配</u>** 若$+_1$对$*_1$可分配，则$+_2$对$*_2$可分配；

（4）**<u>单位元</u>** 若$+_1(*_1)$存在单位元e，则$+_2(*_2)$也存在单位元**h(e)**；

（5）**<u>零元</u>** 若$+_1(*_1)$存在零元z，则$+_2(*_2)$也存在零元**h(z)**；

（6）**<u>逆元</u>** 若对运算$+_1(*_1)$，元素x存在逆元$\mathbf{x^{-1}}$，则对运算$+_2(*_2)$，元素h(x)也存在逆元$\mathbf{h(x^{-1})}$；

<u>推论</u>：若h是V_1到V_2的同构，则h的逆函数h^{-1}是V_2到V_1的同构，因此称V_1和V_2彼此同构。

证明：h是V_1到V_2的同构，则h是V_1到V_2的双射，其逆函数h^{-1}则是V_2到V_1的双射。又

设$V_1=\langle S_1;\ *\rangle, V_2=\langle S_2;\ \bullet\rangle$，则对任意的$y_1, y_2\in S_2$，必存在$x_1, x_2\in S_1$，使

$$y_1=h(x_1),\quad y_2=h(x_2)$$

故
$$\begin{aligned}h^{-1}(y_1\bullet y_2)&=h^{-1}(h(x_1)\bullet h(x_2))\\&=h^{-1}(h(x_1*x_2))\\&=h^{-1}h(x_1*x_2)\\&=x_1*x_2\\&=h^{-1}(y_1)*h^{-1}(y_2)\end{aligned}$$

逆函数h^{-1}也满足同态方程，是V_2到V_1的同构。

浙江大学信息与电子工程学院 电子 宋牟平

<u>**两代数系统在同构的情况下**</u>，它们的运算一一对应，满足的性质完全相同，元素一一对应，***从代数论的角度看，是同一个代数系统***，区别仅仅是运算符号和元素的名称不同，一个代数系统中的理论完全可用于同构的另一代数系统，一个代数系统的理论清楚了，所有和它同构的代数系统的问题也就清楚了。

<u>例如</u>**集合代数**、**布尔代数**、**逻辑代数**三者是同构的，在代数论的基础上统一了起来。

例 V_1=<{∅, A, A′, U} ; ∪>， V2=<{U, A′ , A, ∅} ; ∩>， h=′ 同构

∪	∅	A	A'	U
∅	∅	A	A'	U
A	A	A	U	U
A'	A'	U	A'	U
U	U	U	U	U

∩	U	A'	A	∅
U	U	A'	A	∅
A'	A'	A'	∅	∅
A	A	∅	A	∅
∅	∅	∅	∅	∅

作业

3(1)(4), 6, 7(1)(3)(5), 10, 12, 15, 16

内容提要

1. 集合 A 上的运算

- 集合 A 上的运算；
- 运算的封闭性；
- 二元运算的一些常见的性质；
- 集合中与二元运算相联系的一些特殊的元素：单位元、零元、幂等元、元素的逆元.

2. 代数系统

- 代数系统；
- ~~整环及其性质；~~
- 子代数.

3. 代数系统的同态与同构

- 同态；
- 满同态；
- 满同态的性质；
- 同构.

例题讲解

例 4-1 通常数的乘法运算是否可看做下列集合上的二元运算？请逐个回答，并说明理由.

(1) $A=\{1,2\}$；

(2) $B=\{x \mid x$ 是素数$\}$；

(3) $C=\{x \mid x$ 是偶数$\}$；

(4) $D=\{2^n \mid n\in\mathbf{N}\}$.

解 (1) 乘法运算不是集合 A 上的二元运算. 因为 $2\times 2=4\notin A$.

(2) 乘法运算不是集合 B 上的二元运算. 因为素数乘素数不再是素数. 例如 $3\times 5=15\notin B$.

(3) 乘法运算是集合 C 上的运算. 因为偶数乘偶数仍为偶数.

(4) 乘法运算是集合 D 上的二元运算. 因为对于任意 $2^n,2^m\in D$，$2^n\times 2^m=2^{n+m}\in D$.

例 4-2 设有集合 A，$A^A=\{f \mid f:A\to A\}$是由 A 到 A 的所有函数组成的集合. 因为对于任意 $f_1,f_2\in A^A$，f_1 与 f_2 的复合函数 $f_1\cdot f_2$ 仍是一由 A 到 A 的函数，因此函数的复合运算可看做是集合 A^A 上的一个二元运算.

例 4-3 通常数的加法运算可看做是正整数集 $\mathbf{N}$ 上的一个二元运算. 下列集合均是 $\mathbf{N}$ 的子集, 加法运算在这些子集上是封闭的吗? 说明理由.

(1) $S_1=\{n \mid n$ 是 15 的因子$\}$;

(2) $S_2=\{n \mid n$ 是 15 的倍数$\}$;

(3) $S_3=\{n \mid 6$ 整除 n, 而 24 整除 $n^2\}$.

解 (1) 加法运算在 S_1 上不封闭. 因为 $3\in S_1, 5\in S_1$, 但 $3+5=8\notin S_1$.

(2) 加法运算在 S_2 上是封闭的. 其证明如下.

对于任意 $n_1, n_2\in S_2$, 设 $n_1=15k_1, n_2=15k_2\,(k_1, k_2\in\mathbf{N})$, 则 $n_1+n_2=15k_1+15k_2=15(k_1+k_2), (k_1+k_2\in\mathbf{N})$. 因此 $n_1+n_2\in S_2$.

(3) 加法运算在 S_3 上是封闭的. 其证明如下.

首先, 对于任意 $n_1, n_2\in S_3$, 设 $n_1=6k_1, n_2=6k_2\,(k_1, k_2\in\mathbf{N})$, 则 $n_1+n_2=6k_1+6k_2=6(k_1+k_2)$, n_1+n_2 能被 6 整除.

又 $(n_1+n_2)^2=n_1^2+2n_1\cdot n_2+n_2^2$, 根据题意, n_1^2 能被 24 整除, n_2^2 能被 24 整除, 而

$$2n_1\cdot n_2=2\cdot 6k_1\cdot 6k_2=24\cdot(3k_1k_2)$$

也能被 24 整除, 因此 $(n_1+n_2)^2$ 能被 24 整除. 由此知 $n_1+n_2\in S_3$.

例 4-4 设 W 是集合 A 上所有关系的集合，H_1 是 A 上所有自反关系的集合，H_2 是 A 上所有可传递关系的集合. 显然关系的复合运算是 W 上的一个二元运算，试问关系的复合运算在 H_1 和 H_2 上是封闭的吗？为什么？

解 关系的复合运算∘在 H_1 上是封闭的，这是因为 A 上任意两个自反关系的复合关系仍是 A 上的自反关系；但∘在 H_2 上不封闭，这是因为 A 上任意两个可传递关系的复合关系不一定是可传递的. 举例如下.

设 $A=\{1,2,3\}$，定义集合 A 上的关系

$$\rho_1=\{(1,2),(2,3),(1,3)\},$$

$$\rho_2=\{(2,3),(3,1),(2,1)\},$$

显然，ρ_1 和 ρ_2 均是可传递的. 又

$$\rho_1 \cdot \rho_2=\{(1,3),(1,1),(2,1)\},$$

但 $\rho_1 \cdot \rho_2$ 不可传递.

例 4-7 实数集 **R** 上的二元运算 $*$ 定义为

$$r_1 * r_2 = r_1 + \frac{1}{2} r_2$$

集合 **R** 中关于运算 $*$ 存在有单位元、零元和幂等元吗？

解 （1）运算 $*$ 不可交换，因此我们分别考虑它是否有左单位元和右单位元.

若 r_1 是左单位元，则对于任意 $r \in \mathbf{R}$，应有

$$r_1 * r = r, \quad r_1 + \frac{r}{2} = r,$$

于是 $r_1 = \frac{r}{2}$.

由于 r 是任意的，因此不存在元素能成为运算 $*$ 的左单位元. 由此可知 $*$ 不存在单位元.

若 r_1 是右单位元，则对于任意 $r \in \mathbf{R}$，应有

$$r * r_1 = r, \quad r + \frac{r_1}{2} = r. \qquad (1)$$

要使式(1)成立，只有 $r_1 = 0$，因此 0 是运算 $*$ 的右单位元.

（2）若 r_1 是左零元，则对于任意的 $r\in\mathbf{R}$，应有

$$r_1 * r = r_1, \quad r_1 + \frac{r}{2} = r_1. \tag{2}$$

要使式(2)成立，必须 $r=0$，但 r 是任意的，因此运算 $*$ 没有左零元. 由此可知运算 $*$ 不存在零元.

若 r_1 是右零元，则对于任意的 $r\in\mathbf{R}$，应有

$$r * r_1 = r_1, \quad r + \frac{r_1}{2} = r_1,$$

于是

$$r = \frac{r_1}{2}, \quad r_1 = 2r.$$

由于 r 是任意的，因此运算 $*$ 也没有右零元.

（3）若 $r\in\mathbf{R}$ 是幂等元，则应有

$$r + \frac{r}{2} = r, \quad \frac{r}{2} = 0. \tag{3}$$

要使式(3)成立，必须 $r=0$，因此 0 是幂等元.

例 4-8 设有集合 A,B，并设 $W=\{\rho \mid \rho$ 是由 A 到 B 的关系$\}$. 因为由 A 到 B 的任一关系均是 $A\times B$ 的一个子集，所以任意两个关系经过并运算和交运算后，其结果仍是 $A\times B$ 的一个子集，即仍是由 A 到 B 的一个关系. 若将 $A\times B$ 看做是全集合，则关系 ρ 的补 ρ' 也是 $A\times B$ 的一个子集，即也是由 A 到 B 的一个关系. 因此集合的并运算、交运算和补运算可分别看做是 W 上的二元运算和一元运算. 于是 $\langle W;\cup,\cap,'\rangle$ 是一代数系统.

例如 设 $A=\{0,1\}$, $B=\{a,b,c\}$,

则 $A\times B=\{(0,a),(0,b),(0,c),(1,a),(1,b),(1,c)\}$.

设 A 到 B 的关系

$$\rho_1=\{(0,a),(0,c),(1,a)\},$$

$$\rho_2=\{(0,b),(0,c),(1,c)\},$$

则 $$\rho_1\cup\rho_2=\{(0,a),(0,b),(0,c),(1,a),(1,c)\},$$

$$\rho_1\cap\rho_2=\{(0,c)\},$$

$$\rho_1'=\{(0,b),(1,b),(1,c)\}$$

也都是由 A 到 B 的关系.

例 4-9 设 $A=\left\{\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \middle| a,b\in \mathbf{Z}\right\}$，试证明集合 A 与矩阵的加法和乘法运算构成一个整环(这里 $\mathbf{Z}$ 表示整数集).

证 对于任意的 $\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}$，$\begin{bmatrix} c & d \\ 2d & c \end{bmatrix}\in A$，因为

$$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}+\begin{bmatrix} c & d \\ 2d & c \end{bmatrix}=\begin{bmatrix} a+c & b+d \\ 2(b+d) & a+c \end{bmatrix}\in A,$$

$$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}\cdot\begin{bmatrix} c & d \\ 2d & c \end{bmatrix}=\begin{bmatrix} ac+2bd & ad+bc \\ 2(bc+ad) & 2bd+ac \end{bmatrix}\in A,$$

所以$\langle A;+,\cdot\rangle$构成一个代数系统.

（1）根据矩阵加法运算的定义，+满足交换律. 对于运算 · ，因为

$$\begin{bmatrix} c & d \\ 2d & c \end{bmatrix} \cdot \begin{bmatrix} a & b \\ 2b & a \end{bmatrix} = \begin{bmatrix} ac+2bd & bc+ad \\ 2(ad+bc) & 2bd+ac \end{bmatrix},$$

与前面计算的 $\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \cdot \begin{bmatrix} c & d \\ 2d & c \end{bmatrix}$ 相等，所以 · 也满足交换律.

（2）矩阵的加法和乘法运算均满足结合律.

（3）矩阵的乘法运算对加法运算是可分配的.

（4）矩阵 $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ 是加法运算的单位元.

矩阵 $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ 是乘法运算的单位元.

（5）对任意$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \in A$，其加法逆元是矩阵$\begin{bmatrix} -a & -b \\ -2b & -a \end{bmatrix}$.

（6）所谓运算·满足消去律是指，对于任意的矩阵 $x,y,z\in A$，若 $x\neq 0$，则由 $x\cdot y=x\cdot z$，可得 $y=z$. 这里 $x\neq 0$ 指 x 不是加法运算的单位元.

设$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}$，$\begin{bmatrix} c & d \\ 2d & c \end{bmatrix}$，$\begin{bmatrix} e & f \\ 2f & e \end{bmatrix} \in A$，其中 a,b 至少有一个不为 0. 并设

$$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \cdot \begin{bmatrix} c & d \\ 2d & c \end{bmatrix} = \begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \cdot \begin{bmatrix} e & f \\ 2f & e \end{bmatrix},$$

于是

$$\begin{bmatrix} ac+2bd & ad+bc \\ 2(bc+ad) & 2bd+ac \end{bmatrix} = \begin{bmatrix} ae+2bf & af+be \\ 2(be+af) & 2bf+ac \end{bmatrix},$$

因此

$$ac+2bd=ae+2bf, \tag{1}$$

$$ad+bc=af+be. \tag{2}$$

浙江大学信息与电子工程学院 电子 宋牟平

将式(1)两边同乘以 a,将式(2)两边同乘以 $2b$,分别得

$$a^2c+2abd=a^2e+2abf, \tag{3}$$

$$2abd+2b^2c=2abf+2b^2e, \tag{4}$$

式(3)−式(4)得

$$(a^2-2b^2)c=(a^2-2b^2)e,$$

$$(a^2-2b^2)(c-e)=0,$$

因此 $$a^2-2b^2=0 \quad \text{或} \quad c-e=0.$$

因为 a,b 均为整数,且 a,b 中至少一个不为 0,所以 $a^2-2b^2\neq 0$,因此必有 $c=e$.

类似地,可以证明 $d=f$,故

$$\begin{bmatrix} c & d \\ 2d & c \end{bmatrix}=\begin{bmatrix} e & f \\ 2f & e \end{bmatrix}.$$

由上可知$\langle A;+,\cdot\rangle$是一整环.

例 4-11 设 $V=\langle \mathbf{Z};+,\cdot\rangle$，其中 $\mathbf{Z}$ 表示整数集，$+$ 和 $\cdot$ 分别表示通常数的加法和乘法运算. 对下面 $\mathbf{Z}$ 的每个子集，确定它是否能构成 V 的子代数？ 为什么？

(1) $H_1=\{2n+1 \mid n\in\mathbf{Z}\}$；

(2) $H_2=\{-1,0,1\}$；

(3) $H_3=\{2n \mid n\in\mathbf{Z}\}$.

解 (1) H_1 不能构成 V 的子代数.

因为对于任意的 $2n_1+1, 2n_2+1\in H_1$，有

$$(2n_1+1)+(2n_2+1)=2n_1+2n_2+2\notin H_1,$$

所以加法运算在 H_1 上不封闭.

(2) H_2 也不能构成 V 的子代数.

因为加法运算在 H_2 上也不封闭. 例如，$1+1=2\notin H_2$.

(3) H_3 能构成 V 的子代数.

因为对于任意的 $2n_1, 2n_2\in H_3$，有 $2n_1+2n_2=2(n_1+n_2)\in H_3$，且 $2n_1\cdot 2n_2=2(2n_1n_2)\in H_3$，所以加法运算和乘法运算在 H_3 上均是封闭的. 因此 $\langle H_3;+,\cdot\rangle$ 是 $\langle\mathbf{Z};+,\cdot\rangle$ 的子代数.

例 4-12 设 $V=\langle \mathbf{R};*\rangle$，其中 $\mathbf{R}$ 是实数集，运算 $*$ 定义为

$$x*y=[x,y].$$

符号$[x,y]$表示不小于 x 和 y 的最小整数，又设

$$H_1=\{x\mid 0\leqslant x\leqslant 10, x\in\mathbf{R}\},$$

$$H_2=\{x\mid 0\leqslant x<10, x\in\mathbf{R}\},$$

试问 H_1 与 H_2 能否构成 V 的子代数？

解 正确理解符号$[x,y]$的含义. 例如

$$[1.5,\sqrt{2}]=2,\quad [-3,-2.1]=-2.$$

因为运算 $*$ 在 H_1 上是封闭的，所以$\langle H_1;*\rangle$是$\langle \mathbf{R};*\rangle$的子代数. 但 H_2 与运算 $*$ 不能构成 V 的子代数，因为 $*$ 在 H_2 上不封闭. 例如$\lceil 9.8,2\rceil=10$，但 $10\notin H_2$.

浙江大学 信息与电子工程学院 电子 宋牟平

例 4-13 设有代数系统 $V_1=\langle \mathbf{R};+,\sim\rangle$ 和 $V_2=\langle \mathbf{R}_+;\cdot,'\rangle$，其中 $\mathbf{R}$ 和 $\mathbf{R}_+$ 分别表示实数集和正实数集，$+$ 和 $\cdot$ 是通常数的加法和乘法，$\sim$ 表示求相反数的运算，$'$ 表示求倒数的运算.

设有函数 $h:\mathbf{R}\to\mathbf{R}_+$，对于任意 $x\in\mathbf{R}$，$h(x)=\mathrm{e}^x$. 于是对于任意 $x,y\in\mathbf{R}$，

$$h(x+y)=\mathrm{e}^{x+y}=\mathrm{e}^x\cdot\mathrm{e}^y=h(x)\cdot h(y).$$

对于任意 $x\in\mathbf{R}$，

$$h(\sim(x))=h(-x)=\mathrm{e}^{-x}=\frac{1}{\mathrm{e}^x}=(h(x))'.$$

因此 h 是由 V_1 到 V_2 的一个同态.

例 4-14 设 $V=\langle \mathbf{R}^*;\cdot\rangle$,其中 $\mathbf{R}^*$ 表示非零实数集,$\cdot$ 表示通常数的乘法运算.试问下列两个函数是否由 V 到 V 的满同态?

(1) $h(x)=x^2$;

(2) $g(x)=\dfrac{1}{x}$.

解 (1) 对任意 $x\in\mathbf{R}^*$,有 $x^2\in\mathbf{R}^*$,所以 h 是由 $\mathbf{R}^*$ 到 $\mathbf{R}^*$ 的函数.又对于任意 $x,y\in\mathbf{R}^*$,有

$$h(x\cdot y)=(x\cdot y)^2=x^2\cdot y^2=h(x)\cdot h(y),$$

所以 h 是从 V 到 V 的同态.

但 h 不是从 V 到 V 的满同态.因为 h 不是由 $\mathbf{R}^*$ 到 $\mathbf{R}^*$ 的满射,例如 $-5\in\mathbf{R}^*$,但不存在 $x\in\mathbf{R}^*$,使 $x^2=-5$.

(2) 对任意 $x \in \mathbf{R}^*$，因为 $x \neq 0$，所以有 $\frac{1}{x} \in \mathbf{R}^*$，因此 g 是由 $\mathbf{R}^*$ 到 $\mathbf{R}^*$ 的函数. 又对于任意 $x, y \in \mathbf{R}^*$，

有
$$g(x \cdot y) = \frac{1}{x \cdot y} = \frac{1}{x} \cdot \frac{1}{y} = g(x) \cdot g(y),$$

所以 g 是从 V 到 V 的同态.

对于任意 $x \in \mathbf{R}^*$，有 $\frac{1}{x} \in \mathbf{R}^*$，且 $\frac{1}{\frac{1}{x}} = x$，因此 $g\left(\frac{1}{x}\right) = x$. 即 $\mathbf{R}^*$ 中任一元素在 $\mathbf{R}^*$ 中均有像源. 所以 g 是由 $\mathbf{R}^*$ 到 $\mathbf{R}^*$ 的满射，因此 g 是从 V 到 V 的满同态.

浙江大学 信息与电子工程学院 电子 宋牟平

例 4-15 设 $A=\{a,b,c\}$，试问代数系统 $\langle\{\varnothing,A\};\cup,\cap\rangle$ 和 $\langle\{\{a,b\},A\};\cup,\cap\rangle$ 是否同构?

解 令 $S=\{\varnothing,A\}$，$H=\{\{a,b\},A\}$. 定义函数 $f:S\to H$，使得 $f(\varnothing)=\{a,b\}$，$f(A)=A$. 显然 f 是一双射.

对于任意 $x,y\in S$，若 $x=y$，则

$$f(x\cup y)=f(x),$$

$$f(x)\cup f(y)=f(x)\cup f(x)=f(x),$$

所以

$$f(x\cup y)=f(x)\cup f(y).$$

若 $x\neq y$，则

$$f(x\cup y)=f(A)=A,$$

$$f(x)\cup f(y)=\{a,b\}\cup A=A,$$

所以

$$f(x\cup y)=f(x)\cup f(y).$$

因此对于任意 $x,y\in S$，都有 $f(x\cup y)=f(x)\cup f(y)$.

类似地，对于任意 $x,y\in S$，若 $x=y$，则

$$f(x\cap y)=f(x),$$

$$f(x)\cap f(y)=f(x)\cap f(x)=f(x),$$

所以

$$f(x\cap y)=f(x)\cap f(y).$$

若 $x\neq y$，则

$$f(x\cap y)=f(\varnothing)=\{a,b\},$$

$$f(x)\cap f(y)=\{a,b\}\cap A=\{a,b\},$$

所以

$$f(x\cap y)=f(x)\cap f(y).$$

因此对于任意的 $x,y\in S$，都有 $f(x\cap y)=f(x)\cap f(y)$.

由上证得 $\langle\{\varnothing,A\};\cup,\cap\rangle$ 与 $\langle\{\{a,b\},A\},\cup,\cap\rangle$ 同构.

例 4-16 代数系统 $V_1=\langle \mathbf{Z};+\rangle$ 与 $V_2=\langle \mathbf{N};\cdot\rangle$ 是否同构? 这里 **Z** 和 **N** 分别表示整数集和正整数集,+和·分别表示通常数的加法和乘法.

解 **Z** 和 **N** 都是可数集,因此 **Z** 和 **N** 之间存在有双射. 例如可以定义函数 $f:\mathbf{Z}\to\mathbf{N}$,使得

$$f(i)=\begin{cases}1, & i=0,\\ 2i, & i>0,\\ 2|i|+1, & i<0.\end{cases}$$

因为 **Z** 和 **N** 均是无限集,因此由 **Z** 到 **N** 可以定义许多甚至无穷多个双射函数. 这些双射函数中是否有满足同态条件的呢? 这里不可能对所有的双射函数去一一考察,为了回答这一问题,可以先来考察这两个代数系统所具有的性质.

$\langle \mathbf{Z};+\rangle$ 中运算+具有单位元 0;$\langle \mathbf{N};\cdot\rangle$ 中运算·也具有单位元 1.

$\langle \mathbf{Z};+\rangle$ 中每一整数 i 对于运算+均有逆元 $-i$,即 $i+(-i)=(-i)+i=0$;但 $\langle \mathbf{N};\cdot\rangle$ 中除单位元 1 对于运算·具有逆元 1 外,其他正整数对于运算·均不存在逆元. 这就是说,任何一个由 **Z** 到 **N** 的双射函数都不能使 V_2 中运算·具有 V_1 中运算+每一元素均有逆元的这一条性质. 而"保持运算的性质"是 f 为同构的必要条件,由此可知 V_1 与 V_2 不同构.

例 4-23 设有代数系统⟨S; $*$, $\circ$⟩，其中 $*$ 和 $\circ$ 均是二元运算，并分别具有单位元 e_1 和 e_2. 已知运算 $*$ 和 $\circ$ 相互之间均是可分配的. 试证明对于 S 中任意的元素 x，有 $x * x = x \circ x = x$.

证 因为 e_1 是 $*$ 的单位元，e_2 是 $\circ$ 的单位元，所以

$$e_1 = e_2 \circ e_1 = (e_2 * e_1) \circ e_1 = (e_2 \circ e_1) * (e_1 \circ e_1) = e_1 * (e_1 \circ e_1) = e_1 \circ e_1,$$

$$e_2 = e_1 * e_2 = (e_1 \circ e_2) * e_2 = (e_1 * e_2) \circ (e_2 * e_2) = e_2 \circ (e_2 * e_2) = e_2 * e_2.$$

于是，对于任意的 $x \in S$，有

$$x * x = (x \circ e_2) * (x \circ e_2) = x \circ (e_2 * e_2) = x \circ e_2 = x,$$

$$x \circ x = (x * e_1) \circ (x * e_1) = x * (e_1 \circ e_1) = x * e_1 = x.$$

故对于任意 $x \in S$，有

$$x * x = x \circ x = x.$$

例 4-24 设 f_1 和 f_2 都是从代数系统 $\langle S_1;*\rangle$ 到 $\langle S_2;\circ\rangle$ 的同态，这里 $*$ 和 $\circ$ 都是二元运算，且 $\circ$ 是可交换和可结合的. 定义函数 $h: S_1 \to S_2$，使得对于任意 $x \in S_1$，$h(x) = f_1(x) \circ f_2(x)$. 试证明 h 也是从 $\langle S_1;*\rangle$ 到 $\langle S_2;\circ\rangle$ 的同态.

证 对于任意 $x, y \in S_1$，因为 f_1 和 f_2 都是从 $\langle S_1;*\rangle$ 到 $\langle S_2;\circ\rangle$ 的同态，所以有

$$
\begin{aligned}
h(x*y) &= f_1(x*y) \circ f_2(x*y) \\
&= (f_1(x) \circ f_1(y)) \circ (f_2(x) \circ f_2(y)).
\end{aligned}
$$

又因为 $\circ$ 是可交换和可结合的，所以

$$h(x*y) = (f_1(x) \circ f_2(x)) \circ (f_1(y) \circ f_2(y)) = h(x) \circ h(y).$$

由 x, y 的任意性，可知 h 也是从 $\langle S_1;*\rangle$ 到 $\langle S_2;\circ\rangle$ 的同态.

例 4-28 代数系统 $V_1=\langle \mathbf{R}-\{0\};\cdot\rangle$ 与 $V_2=\langle \mathbf{R};+\rangle$ 同构吗？其中 **R** 表示实数集，$\cdot$ 和 $+$ 分别表示通常数的乘法和加法运算.

分析 如果 V_1 与 V_2 同构，则这两个代数系统应具有完全相同的性质. 例如 V_1 中有单位元 1，V_2 中有单位元 0. 但是我们发现在 V_1 中元素 -1 满足等式 $(-1)\cdot(-1)=1$，而在 V_2 中却找不出除单位元 0 以外的元素 x，满足 $x+x=0$. 因此 V_1 与 V_2 不可能同构. 下面给出这一结论的证明.

证 用反证法证明之. 设存在函数 $h:\mathbf{R}-\{0\}\to\mathbf{R}$ 是从 V_1 到 V_2 的同构，则由单位元映射为单位元，有 $h(1)=0$.

又设 $h(-1)=b$，则

$$h(1)=h((-1)\cdot(-1))=h(-1)+h(-1)=b+b.$$

因此 $b+b=0$，即 $b=0$，由此导致 $h(1)=h(-1)$，这与 h 是双射相矛盾. 故 $\langle \mathbf{R}-\{0\};\cdot\rangle$ 与 $\langle \mathbf{R};+\rangle$ 不同构.

若代数系统 V_1 和 V_2 是同一个代数系统 V，则从 V_1 到 V_2 的同态称为 V 的自同态. 从 V_1 到 V_2 的同构称为 V 的自同构.

End of Chapter 4.