

代数结构

- 代数系统

- 运算、代数系统、同态与同构、直积

- 群

- 半群、群、子群、循环群、置换群、陪集

- 环与域

- 概念及性质、整环、除环、域的特征、素域

- 代数系统
 - 运算
 - 代数系统

运算

- 定义 1 设 A 是一个集合, $A \times A$ 到 A 的映射称为 A 上的二元运算. 一般地, A^n 到 A 的映射称为 A 上的 n 元运算.
- 设 f 是 A 上的 n 元运算, 对任意的 $x_1, x_2, \dots, x_n \in A$, $f(\langle x_1, x_2, \dots, x_n \rangle)$ 称作 $x_1, x_2, \dots, x_n$ 在 f 下的运算结果, 并简记为

$$f(x_1, x_2, \dots, x_n).$$

- 例 1 数的加法是实数集 $\mathbf{R}$ 上的二元运算.
- 因为 对任意 $\langle a, b \rangle \in \mathbf{R} \times \mathbf{R}$, 通过加法可唯一确定一个实数 $c = a + b$, 故加法是 $\mathbf{R} \times \mathbf{R}$ 到 $\mathbf{R}$ 的映射;
即是 $\mathbf{R}$ 上的二元运算.
- 同样, 数的乘法、减法都是实数集 $\mathbf{R}$ 上的二元运算.

- 例 2 数的除法不是实数集 $\mathbf{R}$ 上的二元运算.
- 因为0不能做除数，某些实数对 $\langle a, b \rangle$ 不能通过除法唯一确定一个与之相应的实数（比如， $2 / 0$ 无意义
- 但是，任何非0实数 a, b ，通过除法可唯一确定一个非0实数 a/b ，故除法是非0实数集 R^* 上的二元运算.

- 例 3 设 S 是一个集合，集合的并、交是 $P(S)$ 上的二元运算.
- 因为对任意 $\langle A, B \rangle \in P(S) \times P(S)$ ，通过集合的并（交）可唯一确定 $P(S)$ 的一个元素 $A \cup B$ （或 $A \cap B$ ），故集合的并(交)是 $P(S)$ 上的二元运算.

- 例 4 设 $\mathbf{R}$ 是实数集, 令

$$f: \langle a, b \rangle \mapsto a+b-ab \quad a, b \in \mathbf{R}$$

则 f 是 $\mathbf{R}$ 上的二元运算,

即 $f(a, b) = a+b-ab.$

- 例 5 设 $\mathbf{R}$ 是实数集，令

$$g: \langle a, b \rangle \mapsto \min \{a, b\}$$

$$h: \langle a, b \rangle \mapsto \max \{a, b\}, \forall a, b \in \mathbf{R}$$

则 g ， h 均为 $\mathbf{R}$ 上的二元运算.

- 今后主要讨论二元运算，简称“运算”
- 用一些称作运算符的特殊符号，表示二元运算， 比如： $\diamond$ ， $*$ ， $\cdot$ ， $\circ$ ， $+$ $\times$ 等
- 将 a ， b 在某运算 “ $*$ ” 下的运算结果 $*(a, b)$ 记为 $a*b$. 或简写成 ab .

- 实数加法: $a + b$
- 实数乘法: $a \cdot b$ 或 ab
- 集合并、交运算: $A \cup B, A \cap B$
- 定义 $*$ 运算:

$$a * b = a + b - ab$$

- 定义 $\circ$ 、 $\oplus$ 运算:

$$a \circ b = \min \{a, b\}$$

$$a \oplus b = \max \{a, b\}$$

- 例 6 设 n 为正整数， $\mathbf{Z}_n$ 为模 n 剩余类的集合：

$$\mathbf{Z}_n = \{ [0], [1], \dots, [n-1] \}$$

定义运算 $+_n$ 与 $\times_n$ 如下：

$\forall [i], [j] \in \mathbf{Z}_n$ ，规定

$$[i] +_n [j] = [i+j]$$

$$[i] \times_n [j] = [i \cdot j]$$

其中， $+$ 与 $\cdot$ 为通常整数的加法和乘法。

- $+_n, \times_n$ 是不是二元运算?
- $[i] +_n [j]$ 与 $[i] \times_n [j]$ 由剩余类 $[i], [j]$ 唯一确定, 而与代表元 i, j 的选取无关
- 设 $[i'] = [i], [j'] = [j]$
 则 $n \mid i' - i, \quad n \mid j' - j.$
 知 $n \mid (i' + j') - (i + j)$
 故 $[i' + j'] = [i + j].$

- 定义 2 设 f 是 A 上的 n 元运算, $S \subseteq A$, 如果对 $x_1, x_2, \dots, x_n \in S$, 恒有 $f(x_1, x_2, \dots, x_n) \in S$, 则称 S 对运算 f 是封闭的. 运算 f 在 S 上是封闭的。
- 自然数集对实数集上的加法、乘法封闭
- 自然数集对实数集上的减法不是封闭的
- 设 $A \subseteq S$, 则 $P(A)$ 对 $P(S)$ 上的并、交封闭

运算表

- 当A是有限集时，A上的运算可用一个表来表示：

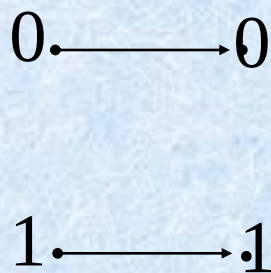
$\circ$	a_1	a_2	$\cdots$	a_j	$\cdots$	a_n
a_1	a_{11}	a_{12}	$\cdots$	a_{1j}	$\cdots$	a_{1n}
a_2	a_{21}	a_{22}	$\cdots$	a_{2j}	$\cdots$	a_{2n}
$\vdots$						
a_j	a_{j1}	a_{j2}	$\cdots$	a_{ij}	$\cdots$	a_{in}
$\vdots$						
a_n	a_{n1}	a_{n2}	$\cdots$	a_{nj}	$\cdots$	a_{nn}

- 例 7 $\mathbf{Z}_3 = \{[0], [1], [2]\}$, $+_3$ 、 $\times_3$ 的运算表分别为:

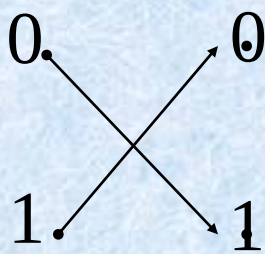
$+_3$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

$\times_3$	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

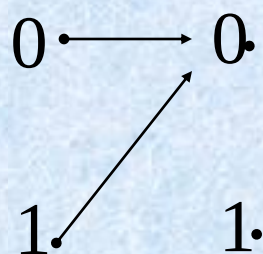
- 例 8 设 $A = \{0, 1\}$ ，则 A 到 A 的映射构成的集合 A^A 中有四个元素 f_0, f_1, f_2, f_3 ，如下：



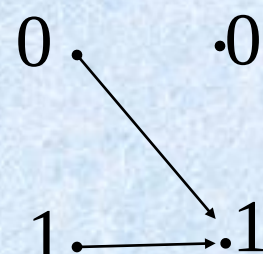
f_0



f_1



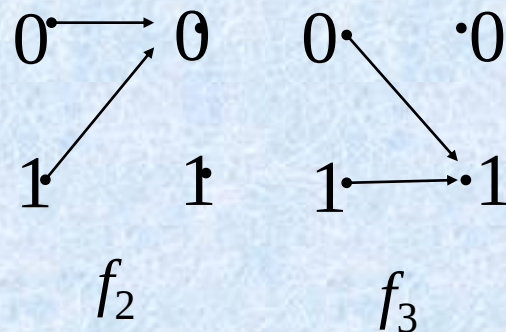
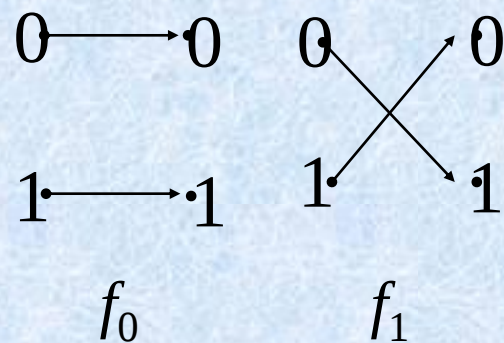
f_2



f_3

- A^A 中的函数复合的运算表

$\circ$	f_0	f_1	f_2	f_3
f_0	f_0	f_1	f_2	f_3
f_1	f_1	f_0	f_3	f_2
f_2	f_2	f_2	f_2	f_2
f_3	f_3	f_3	f_3	f_3



运算律

- 定义 3 设 X 为集合, $*$, $\circ$ 为 X 上的运算.
- 如果对任意 $x, y, z \in X$, 有 $(x * y) * z = x * (y * z)$
则称 $*$ 满足结合律 (可结合的);
- 如果对任意 $x, y \in X$, 有 $x * y = y * x$
则称 $*$ 满足交换律 (可交换的);
- 如果对任意 $x, y, z \in X$, 有 $x * (y \circ z) = (x * y) \circ (x * z)$
则称 $*$ 对 $\circ$ 满足左分配律 (左可分配);
- 如果对任意 $x, y, z \in X$, 有 $(y \circ z) * x = (y * x) \circ (z * x)$
则称 $*$ 对 $\circ$ 满足右分配律 (右可分配);
- 若 $*$ 对 $\circ$ 既满足左分配律, 又满足右分配律, 称 $*$ 对 $\circ$ 满足分配律 (可分配).

- 如果对任意 $x, y, z \in X$,
当 $x * y = x * z$ 时, 必有 $y = z$,
则称 $*$ 满足左消去律;
- 如果对任意 $x, y, z \in X$,
当 $y * x = z * x$ 时, 必有 $y = z$,
则称 $*$ 满足右消去律;
- 若 $*$ 既满足左消去律, 又满足右消去律,
称其满足消去律.

- 整数集上的加法、乘法 满足哪些运算律
- 设 A 是一集合, $P(A)$ 上的并、交运算均满足结合律、交换律、分配律, 不满足消去律.
- 运算表怎么表现运算律?
- 作业: 习题一 1, 3

代数系统

- 定义 1 设 A 是一个非空集合, $f_1, f_2, \dots, f_n$ 是 A 上的运算 (其元数可以不同), 我们说 A 在运算 $f_1, f_2, \dots, f_n$ 下构成一个代数系统, 记为 $\langle A, f_1, f_2, \dots, f_n \rangle$. 在不引起混乱的情况下, 也可将其简记为 A .
- $\langle \mathbf{N}, + \rangle, \langle \mathbf{N}, \cdot \rangle, \langle \mathbf{N}, +, \cdot \rangle$.
- $\langle \mathbf{Z}, + \rangle, \langle \mathbf{Z}, \cdot \rangle, \langle \mathbf{Z}, +, \cdot \rangle$,
- $\langle \mathbf{Q}, + \rangle, \langle \mathbf{Q}, \cdot \rangle, \langle \mathbf{Q}, +, \cdot \rangle, \langle \mathbf{R}, + \rangle, \langle \mathbf{R}, \cdot \rangle, \langle \mathbf{R}, +, \cdot \rangle$.

- 设 A 是一个集合， $P(A)$ 与集合的并和交运算构成代数系统

$$\langle P(A), \cup \rangle, \langle P(A), \cap \rangle, \langle P(A), \cup, \cap \rangle$$

- 模 n 剩余类集 $\mathbf{Z}_n$ 在运算 $+_n$ 和 $\times_n$ 下可构成代数系统

$$\langle \mathbf{Z}_n, +_n \rangle, \langle \mathbf{Z}_n, \times_n \rangle, \langle \mathbf{Z}_n, +_n, \times_n \rangle$$

- 设 A 是一个集合，在 A 上规定运算 $*$ 如下：

$$\forall x, y \in A, x * y = x$$

则得到一个代数系统 $\langle A, * \rangle$

- 定义 2 设 $\langle A, * \rangle$ 是代数系统, $S \subseteq A$, 如果 S 对 $*$ 封闭, 则称 $\langle S, * \rangle$ 为 $\langle A, * \rangle$ 的子代数.
- 任一代数系统均为自身的子代数
- $\langle \mathbf{N}, + \rangle$, $\langle \mathbf{Z}, + \rangle$, $\langle \mathbf{Q}, + \rangle$, $\langle \mathbf{R}, + \rangle$, $\langle \mathbf{Z}, \cdot \rangle$

- **定义 3** 设 $\langle A, \circ \rangle$ 是一个代数系统, $e_l \in A$, 如果 $\forall x \in A$, 有 $e_l x = x$, 则称 e_l 为 A 的**左单位元** (左恒等元); 设 $e_r \in A$, 如果 $\forall x \in A$, 有 $x e_r = x$, 称 e_r 为 A 的**右单位元** (右恒等元); A 中的一个元素如果既是左单位元, 又是右单位元, 则称之为**单位元** (恒等元) .
- $\langle \mathbf{N}, + \rangle$, $\langle \mathbf{N}, \cdot \rangle$ $\langle \mathbf{Z}, + \rangle$, $\langle \mathbf{Q}, + \rangle$,
- $\langle \mathbf{R}, + \rangle$, $\langle \mathbf{Z}, \cdot \rangle$, $\langle \mathbf{Q}, \cdot \rangle$, $\langle \mathbf{R}, \cdot \rangle$,
- $\langle P(A), \cup \rangle$, $\langle P(A), \cap \rangle$, $\langle \mathbf{Z}_n, +_n \rangle$, $\langle \mathbf{Z}_n, \times_n \rangle$
- $\forall x, y \in A, x * y = x$, 任何元素均为右单位元

- 定理 1 设代数系统 $\langle A, \circ \rangle$ 中既有左单位元 e_l ，又有右单位元 e_r ，则 $e_l = e_r$.
- 证明 因 e_l 为左单位元，故 $e_l e_r = e_r$ ，又因 e_r 为右单位元，故 $e_l e_r = e_l$ ，所以 $e_l = e_r$.
- 推论 代数系统 $\langle A, \circ \rangle$ 中的单位元如果存在，则必定唯一.

- 定义 4 代数系统 $\langle A, * \rangle$, e 是单位元.
对于 $a \in A$,
如果存在 $b \in A$, 使得 $ba = e$, 则称 a 为左可逆的, 且称 b 为 a 的左逆元;
如果存在 $c \in A$, 使得 $ac = e$, 则称 a 是右可逆的, 且称 c 为 a 的右逆元;
如果存在 $a' \in A$, 使得 $a'a = aa' = e$, 则称 a 是可逆的, 且称 a' 为 a 的逆元.

- $\langle \mathbf{N}, + \rangle$, $\langle \mathbf{Z}, + \rangle$, $\langle \mathbf{Q}, + \rangle$, $\langle \mathbf{R}, + \rangle$
- $\langle \mathbf{N}, \cdot \rangle$, $\langle \mathbf{Z}, \cdot \rangle$,
- $\langle \mathbf{Q}, \cdot \rangle$, $\langle \mathbf{R}, \cdot \rangle$
- $\langle P(A), \cup \rangle$, $\langle P(A), \cap \rangle$
- $\langle \mathbf{Z}_n, +_n \rangle$, $\langle \mathbf{Z}_n, \times_n \rangle$

$\times_3$	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

- 定理 2 设 e 是代数系统 $\langle A, * \rangle$ 单位元, $*$ 满足结合律, 如果 $a \in A$ 的左逆元 b 及右逆元 c 均存在, 则 $b = c$.
- 证明 $b = b e = b (ac) = (ba) c = ec = c$.
- 推论 设 $\langle A, * \rangle$ 是有单位元的代数系统, $*$ 满足结合律. 如果 $a \in A$ 的逆元存在, 则必定唯一.

- 定义 5 设 $\langle A, * \rangle$ 是一个代数系统，如果 $a \in A$ 满足 $a * a = a$ ，称 a 为 A 的幂等元.
- 代数系统的单位元如果存在则必为幂等元.
- $\langle P(A), \cup \rangle$, $\langle P(A), \cap \rangle$

$\langle \mathbf{Z}_n, +_n, \times_n \rangle$ 的性质

- 关于 $+_n$ 的性质:
- 结合律 $([i] +_n [j]) +_n [k] = [i] +_n ([j] +_n [k])$
- 交换律 $[i] +_n [j] = [j] +_n [i]$
- 单位元 $[i] +_n [0] = [0] +_n [i] = [i]$
- 逆元 $[i] +_n [n-i] = [n-i] +_n [i] = [0]$

$\langle \mathbf{Z}_n, +_n, \times_n \rangle$ 的性质

- 关于 $\times_n$ 的性质.
- 结合律

$$([i] \times_n [j]) \times_n [k] = [i] \times_n ([j] \times_n [k])$$

- 交换律 $[i] \times_n [j] = [j] \times_n [i]$
- 单位元 $[i] \times_n [1] = [1] \times_n [i] = [i]$

$\langle \mathbf{Z}_n, +_n, \times_n \rangle$ 的性质

- $\times_n$ 对 $+_n$ 的分配律

- $$[i] \times_n ([j] +_n [k]) = ([i] \times_n [j]) +_n ([i] \times_n [k])$$

- $$([j] +_n [k]) \times_n [i] = ([j] \times_n [i]) +_n ([k] \times_n [i])$$

作业：习题二 1, 3, 4