

群伦导引

回顾

2

□ 1: 等价关系与等价类

- 等价关系：自反、对称、传递；等价关系将元素分成等价类；所有等价类的集合为商集，商集即划分

□ 2: 偏序关系、偏序集及其特殊元素、偏序格

- 偏序关系：自反、反对称、传递；偏序集；哈斯图
- 偏序集中的特殊元素：最大元、最小元、极小元、极大元；上届、上确界、下届、下确界
- 偏序格：任意两个元素均有上下确界；对偶原理

本节提要

3

- 问题1：什么是代数系统？
- 问题2：代数系统相关性质？
- 问题3：什么是群？
- 问题4：群具有哪些性质？

引言

- 代数系统一般称为“抽象代数 (abstract algebra)”或“近世代数”，20世纪初被命名，但其研究的主要内容却于19世纪便已开展
- 代数系统研究的主要内容：代数结构、群、环、域、模、向量空间、格、布尔代数、李代数等等

运算的函数定义

- 函数 $f: A^n \rightarrow B$ 称为(从 A 到 B 的) n 元运算
 - 以下主要讨论二元运算
 - 实数集上的加、减、乘、除显然是二元运算
 - 但二元运算远不止加、减、乘、除
 - 例如：定义实数集上的一个新运算 “ $*$ ”：

$$x * y = x + y - xy$$

则： $2 * 3 = -1$ ； $0.5 * 0.7 = 0.85$

运算表

- 通常用于定义有限集合(一般元素很少)上的一元或二元运算 (如在集合 $\{a, b, c, d\}$ 上定义如下的运算*)

*	a	b	c	d
a	1	®	✱	M
b	&	6	K	M
c	7	6	Q	0
d	G	#	~	◻

运算的封闭性

- 对于运算 $f: A^n \rightarrow B$, 若 $B \subseteq A$, 则称该运算在集合 A 上封闭 (closeness)
- 例:
 - ▣ 加法在自然数集上封闭, 但减法在自然数集上不封闭
 - ▣ 减法在整数集上封闭, 但除法在整数集上不封闭
 - ▣ 对集合 $A = \{1, 2, 3, \dots, 10\}$, gcd运算封闭, lcm则否

例：证明运算封闭

□ 普通加法在正整数集之子集 $A = \{n \mid 9 \mid 21n\}$

上封闭

□ 证明：

▣ 设 x, y 是 A 中任意元素，存在 $p, q \in \mathbb{Z}^+$ ，满足：

$$21x = 9p, \quad 21y = 9q, \quad \text{则 } 21(x + y) = 9(p + q),$$

由于 $p + q \in \mathbb{Z}^+$ ，故 $9 \mid 21(x + y)$ ，即 $x + y \in A$. □

代数系统（简称代数）

- 定义（代数系统）：
 - ▣ 给定1个非空集合（其元素可以是任何对象）；
 - ▣ 给定1个或者若干个运算（以下主要讨论存在1个二元运算的情况）；
 - ▣ 运算对上述集合封闭.
- 记法： $\langle S, \circ \rangle$
- 例子：
 - ▣ 整数集与普通加法： $\langle \mathbb{Z}, + \rangle$ 构成代数系统

例：一个较复杂的代数系统

□ 设集合 $S = \mathbb{R} - \{0,1\}$ ，定义 S 上的6个函数如下：

$$\square f_1(x) = x, \quad f_2(x) = (1 - x)^{-1}$$

$$\square f_3(x) = x^{-1}(x - 1), \quad f_4(x) = x^{-1}$$

$$\square f_5(x) = x(x - 1)^{-1}, \quad f_6(x) = 1 - x$$

□ 则 $\langle \{f_1, f_2, f_3, f_4, f_5, f_6\}, \circ \rangle$ 是代数系统，其中 $\circ$ 是函数的复合运算

只需考虑运算的封闭性。例如： $f_2 \circ f_3 = f_1$, $f_4 \circ f_5 = f_2$, $f_3 \circ f_6 = f_4$ 等

本节提要

11

- 问题1：什么是代数系统？
 - ▣ 非空集合+封闭的(二元)运算
- 问题2：代数系统相关性质？
- 问题3：什么是群？
- 问题4：群具有哪些性质？

结合性 (associativity)

- 集合 A 上的运算 $\circ$ 具有结合性定义为：

$$\forall x, y, z \in A, (x \circ y) \circ z = x \circ (y \circ z)$$

- 如果 $\circ$ 满足结合性，表达式 $x_1 \circ x_2 \circ \cdots \circ x_n$ 可以在保持诸 x_i 先后次序不变的前提下按照任何顺序进行计算

交换性 (commutativity)

- 集合 A 上的运算 $\circ$ 具有交换性定义为：

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

- 如果 $\circ$ 同时满足交换律和结合律，表达式 $x_1 \circ$

$x_2 \circ \cdots \circ x_n$ 可以按照任何顺序进行计算，包括可

以随便重新排列诸 x_i 的先后次序

分配性 (distributivity)

- 分配性涉及两个不同的运算
- 集合 A 上的运算 $\circ$ 对 $*$ 满足分配性定义为：

$$\forall x, y, z \in A, x \circ (y * z) = (x \circ y) * (x \circ z)$$

单位元 (identity element)

- 元素 e 是代数系统 $\langle S, \circ \rangle$ 的 **单位元** 当且仅当

$$\forall x \in S, e \circ x = x \circ e = x$$

- 单位元可记为 1_S ，或简记为 1 （读作幺）

- 例：

- 对于实数集 $\mathbb{R}$ 上的普通乘法 $(\cdot)$ ，实数 1 满足对任意实数 $x \in \mathbb{R}$ ，有 $1 \cdot x = x \cdot 1$

- 代数系统 **不一定有** 单位元

左单位元和右单位元

□ e_L 称为系统的左单位元(或左幺)当且仅当

$$\forall x \in S, e_L \circ x = x$$

□ 可以相应地定义系统的右单位元(右幺) e_R

*	a	b	c	d
a	a	d	c	a
b	b	d	c	b
c	c	d	c	c
d	d	d	b	d

*	a	b	c	d
a	a	b	c	d
b	a	b	c	d
c	a	b	c	d
d	a	b	c	d

关于单位元的进一步讨论

- 左、右单位元不一定存在
- 左、右单位元不一定唯一
- 假设一个代数系统同时有左、右单位元，则左、右单位元必相等且唯一；即系统的单位元（幺元）
 - ▣ $e_L = e_L \circ e_R = e_R$
- 系统若有单位元，必是唯一的
 - ▣ $e_1 = e_1 \circ e_2 = e_2$

逆元 (inverse element)

- 只对存在单位元的代数系统讨论逆元
- 给定系统 S 中的元素 x ，若存在 S 中的元素 x' ，满足 $x' \circ x = 1_S$ ，则称 x' 是 x 的左逆元；若存在 x'' ，满足 $x \circ x'' = 1_S$ ，则称 x'' 是 x 的右逆元
- 给定系统 S 中的元素 x ，如果存在 S 中的元素 x^* ，满足 $x \circ x^* = x^* \circ x = 1_S$ ，则称 x^* 是 x 的逆元，一般记为 x^{-1}
 - 逆元既是左逆元，又是右逆元
 - 如果 y 是 x 的逆元，则 x 也是 y 的逆元

例

*	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	a	c	a
d	d	b	c	d

注意：

- (1) b 的左、右逆不同。
- (2) c 有 2 个右逆，无左逆
- (3) d 有左逆，无右逆

关于逆元的进一步讨论

□ 如果代数系统 $\langle S, \circ \rangle$ 满足结合律：

▣ 若给定的元素既有左逆，又有右逆，二者必相等且唯一

■ 假设 x 的左逆是 x' ，右逆是 x'' ：

$$x' = x' \circ \mathbf{1}_S = x' \circ (x \circ x'') = (x' \circ x) \circ x'' = \mathbf{1}_S \circ x'' = x''$$

▣ 若每个元素均有左逆，则左逆即右逆，且逆元唯一

■ 任给 S 中元素 a ，设 a 的左逆是 b ， b 的左逆是 c ，则

$$\begin{aligned} a \circ b &= (\mathbf{1}_S \circ a) \circ b = ((c \circ b) \circ a) \circ b = (c \circ (b \circ a)) \circ b = \\ &= (c \circ \mathbf{1}_S) \circ b = c \circ b = \mathbf{1}_S \end{aligned}$$

零元

- 元素 t 是代数系统 $\langle S, \circ \rangle$ 的零元当且仅当

$$\forall x \in S, t \circ x = x \circ t = t$$

- 零元可记为 0_S ，或简记为 0

- 例：

- 对于实数集上的普通乘法 $(\cdot)$ ，实数 0 满足对任意实数 x ， $0 \cdot x = x \cdot 0 = 0$

- 一个代数系统不一定存在零元

例

- 利用普通加減法和乘法定义实数集上的二元运算“ $\circ$ ”如下：

$$\forall x, y \in \mathbb{R}, x \circ y = x + y - xy$$

- 交换律：显然
- 结合律： $(x \circ y) \circ z = x \circ (y \circ z) = x + y + z - xy - xz - yz + xyz$
- 单位元：0；零元：1
- $x (x \neq 1)$ 的逆元为： $\frac{x}{x-1}$ ，1无逆元

例：与编码有关的代数系统

- 设字母表 $A = \{0,1\}$, A^* 是 A 上的长度为 n 的字符串的集合
- 定义 A^* 上的运算 $\oplus$ 如下：
 $\forall x, y \in A^*$, $x \oplus y$ 是长度为 n 的二进数字串，第 i 位 ($i = 0, 1, \dots, n-1$) 为 1 当且仅当 x, y 的相应位互异
- $\langle A^*, \oplus \rangle$ 是代数系统
- 该系统满足：结合律、交换律、有单位元、每个元素均有逆元

“相似”的系统

- 比较 $\langle\{F, T\}, \vee\rangle$ （逻辑或）与 $\langle\{0, 1\}, +\rangle$ （布尔和）两代数系统：

$\vee$	F	T	$+$	0	1
F	F	T	0	0	1
T	T	T	1	1	1

- 若不考虑符号的形式及其含义，则两系统的“本质”没有差别

同构与同构映射

□ 代数系统 $\langle S_1, \circ \rangle$ 与 $\langle S_2, * \rangle$ 同构 (isomorphism)

(记 $S_1 \cong S_2$) 当且仅当存在双射函数 $f: S_1 \rightarrow S_2$,

满足: $\forall x, y \in S_1, f(x \circ y) = f(x) * f(y)$ 。其中

的双射函数 f 称同构映射

□ 同构关系是等价关系

同态与同态映射

- 只有两个代数系统的集合等大，它们才可能同构
- 代数系统 $\langle S_1, \circ \rangle$ 与 $\langle S_2, * \rangle$ 同态 (homomorphism, 记 $S_1 \sim S_2$)当且仅当存在函数 $f: S_1 \rightarrow S_2$, 满足:

$$\forall x, y \in S_1, f(x \circ y) = f(x) * f(y)$$

- 例: 整数加系统 $\langle \mathbb{Z}, + \rangle \sim \langle \mathbb{Z}_3, +_3 \rangle$ (模3剩余加系统)
 - 同态映射: $f: \mathbb{Z} \rightarrow \mathbb{Z}_3, f(3k + r) = r$
- 特别地, 若上述 f 是满射, 则称两系统满同态 (epimorphism)

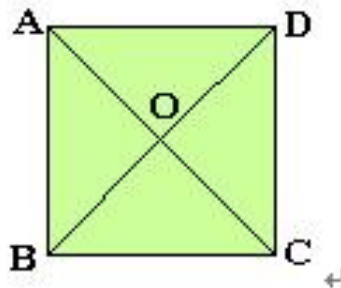
本节提要

28

- 问题1：什么是代数系统？
 - ▣ 非空集合+封闭的(二元)运算
- 问题2：代数系统相关性质？
 - ▣ 封闭性、结合性、交换性、分配性；单位元、零元、逆元；同态同构
- 问题3：什么是群？
- 问题4：群具有哪些性质？

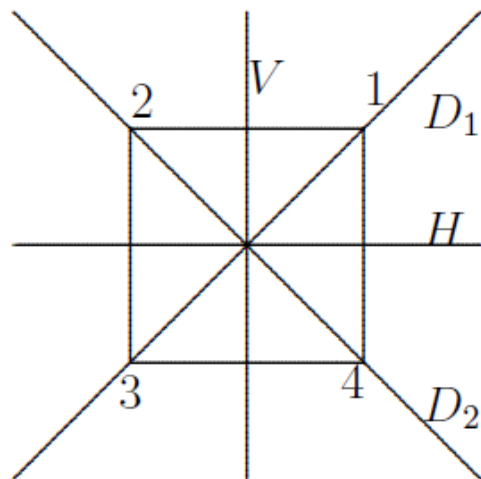
引例：对称变换

- 正方形的刚体运动是从四个顶点集到它本身的一一对应（变换），保持相邻点之间距离不变



引例：对称变换（续）

30



设正方形的4个顶点为1、2、3、4；重心为O，对角线为 D_1 和 D_2 ，水平中线为 H ，垂直中线为 V 。以下将从 $\{1, 2, 3, 4\}$ 到 $\{1, 2, 3, 4\}$ 的一一对应记成
$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ i_1 & i_2 & i_3 & i_4 \end{pmatrix}.$$

我们现在找出正方形所有的对称

引例：对称变换（续）

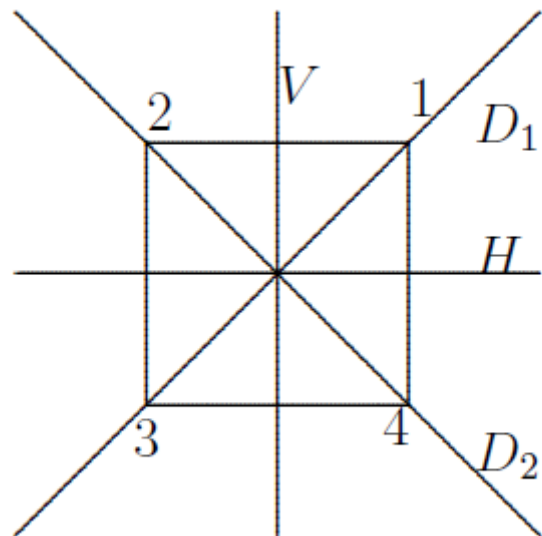
旋转对称：由以下刚体运动完成

$$R_1: \text{绕} O \text{顺时针转} 90^\circ, \text{易见} R_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$R_2: \text{绕} O \text{顺时针转} 180^\circ, \text{易见} R_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

$$R_3: \text{绕} O \text{顺时针转} 270^\circ, \text{易见} R_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$R_0: \text{绕} O \text{顺时针转} 360^\circ, \text{易见} R_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

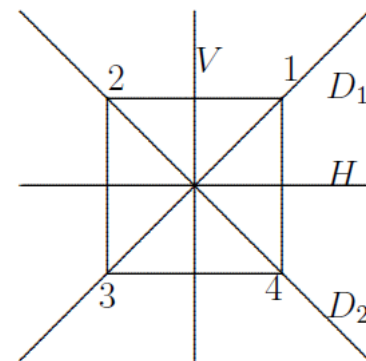


引例：对称变换（续）

反射对称：由以下刚体运动完成

H: 对于水平中线H的反射。 D_1 : 对于对角线 D_1 的反射。

V: 对于垂直中线V的反射。 D_2 : 对于对角线 D_2 的反射。

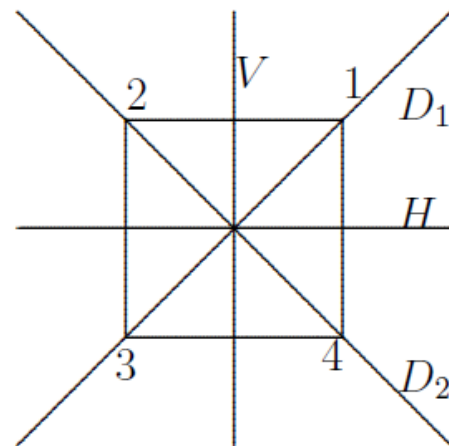


$$H = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \quad V = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \quad D_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \quad D_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

引例：对称变换（续）

- 两个对称变换的连续作用依然是对称变换

- 例如： $R_1 * H$ 指先右转 90° ，后做水平反射，结果得 D_1 ，故 $R_1 * H = D_1$ ；而 $H * R_1 = D_2$ ；由此可以看出 $R_1 * H \neq H * R_1$



引例：对称变换（续）

Cayley Table

.	R_0	R_{90}	R_{180}	R_{270}	V	H	D_1	D_2
R_0	R_0	R_{90}	R_{180}	R_{270}	V	H	D_1	D_2
R_{90}	R_{90}	R_{180}	R_{270}	R_0	D_2	D_1	V	H
R_{180}	R_{180}	R_{270}	R_0	R_{90}	H	V	D_2	D_1
R_{270}	R_{270}	R_0	R_{90}	R_{180}	D_1	D_2	H	V
V	V	D_1	H	D_2	R_0	R_{180}	R_{90}	R_{270}
H	H	D_2	V	D_1	R_{180}	R_0	R_{270}	R_{90}
D_1	D_1	H	D_2	V	R_{270}	R_{90}	R_0	R_{180}
D_2	D_2	V	D_1	H	R_{90}	R_{270}	R_{180}	R_0

引例：对称变换（续）

令 $S = \{R_0, R_1, R_2, R_3, V, H, D_1, D_2\}$

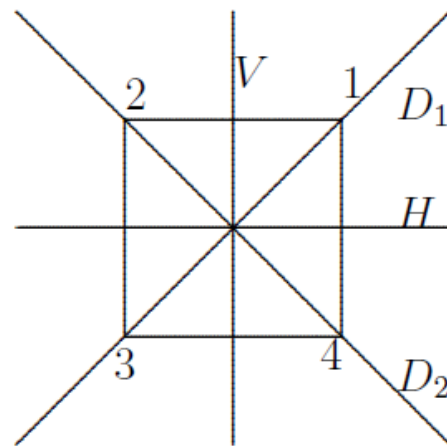
$*$ 为 S 上的两元运算

事实上可通过函数的复合来计算积。例如

$$R_1 * H = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = D_1$$

通过运算可知

- (1) $*$ 对于 S 是封闭的, 即 $(\forall x, y \in S)(x * y \in S)$
- (2) $(\forall x, y, z \in S)(x * (y * z) = (x * y) * z)$
- (3) $(\forall x \in S)(R_0 * x = x * R_0 = x)$
- (4) $(\forall x \in S)(\exists y \in S)(x * y = y * x = R_0)$



半群

定义 设 $(S, *)$ 为代数系统, $(S, *)$ 为半群 (Semigroup) 指

$$(1) (\forall x, y \in S)(x * y \in S)$$

$$(2) (\forall x, y, z \in S)((x * y) * z = x * (y * z))$$

若 $(\forall x, y \in S)(x * y = y * x)$ 则称 $(S, *)$ 为交换半群 (abelian半群)

■ “代数系统” + “结合性” = “半群”

■ 例: 代数系统 $\langle \{1,2\}, * \rangle$ 为半群, 其中 $*$ 定义为

$$\forall x, y \in \{1,2\}, x * y = y$$

么半群 (Monoid)

定义 设 $(S, *)$ 为代数系统, $(S, *)$ 为 Monoid (Semigroup with unit) 指

$$(1) (\forall x, y \in S)(x * y \in S)$$

$$(2) (\forall x, y, z \in S)((x * y) * z = x * (y * z))$$

$$(3) (\exists e \in S)(\forall x \in S)(e * x = x * e = x)$$

■ “半群” + “单位元” = “Monoid”

■ 注意: 代数系统中左右单位元若存在则必相等且唯一

么半群（续）

- 例1: $S = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$, $T = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{R} \right\}$

则集合 S 与 T 关于矩阵的乘法皆构成Monoid

- 例2: $\langle \mathbb{Z}^+, + \rangle$ 为半群，但非Monoid
- 例3: $\langle \mathbb{Z}_n, \oplus_n \rangle$ 为Monoid, $\oplus_n$ 是模 n 加法
- 例4: $\langle A^A, \circ \rangle$ 为Monoid, $\circ$ 是函数复合运算
- 例5: $\langle \mathcal{P}(B), \oplus \rangle$ 为Monoid, $\oplus$ 为对称差运算

群 (Group)

- $(G, *)$ 为群 **当且仅当** 有 $e \in G$ 和 G 上的一元运算⁻¹使

(0) $G \neq \emptyset$

(1) $(\forall x, y \in G)(x * y \in G)$ 代数系统

(2) $(\forall x, y, z \in G)(x * (y * z) = (x * y) * z)$...半群

(3) $(\forall x \in G)(x * e = e * x = x)$ 么半群

(4) $(\forall x \in G)(x * x^{-1} = x^{-1} * x = e)$ 群

(1) ~ (4) 有时被称为群论公理

群（续）

- 群的等价描述：

- 设 G 为非空集合， $*$ 为 G 上的二元运算， $\langle G, * \rangle$ 为群指 $\langle G, * \rangle$ 为Monoid，其单位元为 e ，且满足：

$$(\forall x \in G)(\exists y \in G)(x * y = y * x = e)$$

- 注意：可结合的代数系统中逆元若存在则唯一

群 (续)

命题 设 $\langle G, *, e \rangle$ 为群, 任何元素之逆是唯一的。

证: 设 y, z 为 x 之逆, 从而

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

$$\because x * y = e \rightarrow z * (x * y) = z * e$$

$$\rightarrow (z * x) * y = z$$

$$\rightarrow e * y = z$$

$$\rightarrow y = z$$

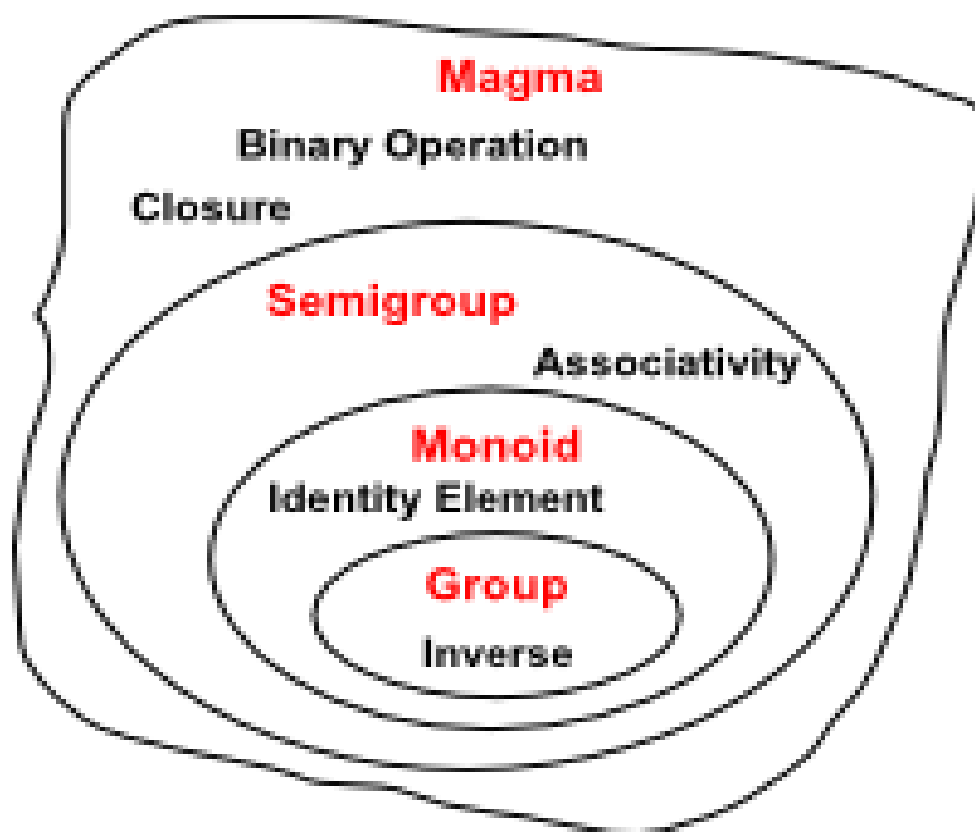
$$\therefore y = z \quad \square$$

群（续）

■ 示例

- $\langle \mathbb{R}, + \rangle, \langle \mathbb{Z}, + \rangle$ 为群，但 $\langle \mathbb{N}, + \rangle$ 不为群（1无逆）
- $\langle \mathbb{R} - \{0\}, * \rangle$ ，非零实数乘法群； a 的逆元素为 $1/a$
- $\langle \mathbb{Z}_n, \oplus_n \rangle$ 为群， i 之逆为 $n - i$
- 正方形的对称变换集与乘积构成群
- $T_A = \{f: A \rightarrow A \mid f \text{ 为双射} \}$ ，单位元 I_A ， f 的逆元 f^{-1}
- $A = \{f: \mathbb{R} \rightarrow \mathbb{R} \mid \text{呈形 } f(x) = ax + b\}$ ， $\langle A, \circ \rangle$ 是群？

群 (续)



本节提要

44

- 问题1：什么是代数系统？
 - ▣ 非空集合+封闭的(二元)运算
- 问题2：代数系统相关性质？
 - ▣ 封闭性、结合性、交换性、分配性；单位元、零元、逆元；同态同构
- 问题3：什么是群？
 - ▣ 封闭 + 结合律 + 单位元 + 逆元
- 问题4：群具有哪些性质？

群的性质

定理 设 $(G, *, e, ^{-1})$ 为群

$$(1) (a^{-1})^{-1} = a$$

$$(2) (ab)^{-1} = b^{-1}a^{-1}$$

$$(3) ab = ac \rightarrow b = c \text{ (左消去律)}$$

$$(4) ba = ca \rightarrow b = c \text{ (右消去律)}$$

$$(5) \text{ 方程 } ax = b \text{ 和 } ya = b \text{ 在 } G \text{ 中对 } x, y \text{ 有唯一解}$$

有限群的运算表中每行（列）均为群中所有元素的一种排列，且不同行（列）不可能出现同样的排列。

群的性质：元素的阶

46

□ 定义

$$a^0 = e \quad (e \text{ 是单位元素})$$

$$a^{n+1} = a^n \circ a \quad (n \text{ 是非负整数})$$

$$a^{-k} = (a^{-1})^k \quad (k \text{ 为正整数})$$

□ 性质

$$a^n \circ a^m = a^{n+m}$$

$$(a^n)^m = a^{nm}$$

群的性质：元素的阶（续）

47

■ 设 G 是群， $a \in G$ ， a 的阶（周期）定义如下：

- $|a| = \min\{k \in \mathbb{Z}^+ \mid a^k = e\}$
- 如果这样的 k 不存在， a 为无限阶元

● 性质

- 有限群不存在无限阶元
- 群中元素及其逆元具有相同的阶
- 有限群中阶大于2的元素有偶数个
- 偶数群中阶为2的元素有奇数个 ($a = a^{-1}$)

群的性质：元素的阶（续）

□ 例

在Kleine 4群 $(V, *)$ 中, $|e| = 1$, 当 $a \neq e$ 时, $|a| = 2$ 。

在 $(\mathbb{Z}_7, +_7)$ 中, $|0| = 1$, $a \neq 0$, $|a| = 7$ 。

在 $(\mathbb{Z}_6, +_6)$ 中, $|0| = 1$

元素	0	1	2	3	4	5
阶	1	6	3	2	3	6

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

群的性质：元素的阶（续）

□ 定理（元素的阶的性质）

设 $(G, *)$, $a, b \in G$, $|a|, |b|$ 为有穷

$$(1) \text{ 对 } k \in \mathbb{Z}^+, a^k = e \Leftrightarrow |a| \mid k$$

$$(2) |a| = |a^{-1}|$$

$$(3) |ab| = |ba|$$

$$(4) |b^{-1}ab| = |a|$$

群的性质：元素的阶（续）

□

● (1) 对 $k \in \mathbb{Z}^+$, $a^k = e \Leftrightarrow |a| \mid k$

证明: (1) “ $\Rightarrow$ ” , 设 $|a| = m > 0$, $m = \min\{k \mid a^k = e \wedge k > 0\}$

故 $k \geq m$, 从而 $k = q \times m + r$, 这里 $0 \leq r < m$

$$\therefore a^k = a^{qm} * a^r = (a^m)^q * a^r = e^q * a^r = a^r$$

$$\therefore a^r = e$$

$$\therefore r < m$$

$$\therefore r = 0, \text{ 从而 } k = q \times m, \text{ 故 } m \mid k.$$

“ $\Leftarrow$ ” , 设 $|a| = r$

$$|a| \mid k \rightarrow r \mid k \rightarrow k = n \times r \rightarrow a^k = a^{n \times r} = (a^r)^n = e^n = e$$

群的性质：元素的阶（续）

(2) 令 $|a| = r$

$$\because (a^{-1})^r = (a^r)^{-1} = e^{-1} = e$$

$$\therefore |a^{-1}| \mid |a|, \text{ 同理 } |a| \mid |a^{-1}|, \text{ 故 } |a^{-1}| = |a|.$$

(3) $(ab)^{n+1} = abab \cdots ab = a(ba)^n b$

ab 的阶有穷，设为 r

$$\text{从而 } (ab)^{r+1} = a(ba)^r b$$

$$\text{从而 } ab = a(ba)^r b, \text{ 故 } (ba)^r = e$$

故 ba 的阶有穷，设为 r' ，由(1)知 $r' \mid r$

同理 $|ba| = r'$ 时有 $|ab|$ 有穷，若为 r ，则 $r \mid r'$

$$\text{因此 } |ab| = |ba|. \quad (4) \mid b^{-1}ab \mid = |abb^{-1}| = |ae| = |a|$$

群的性质：群的阶

- (1) 若 G 为有穷集，则称 $(G, *)$ 为有限群。当 $|G| = n$ 时称 $(G, *)$ 之阶为 n 且称 G 为 n 阶群
- (2) 若 G 为无穷集，则称 $(G, *)$ 为无限群
- (3) 若群 $(G, *)$ 满足 $(\forall x, y \in G)(xy = yx)$ ，则称 G 为交换群(abelian群)

下面我们给出1, 2, 3, 4阶全部不同构的群

- (1) 若 $(G, *)$ 为1阶群，从而设 $G = \{e\}$ 有 $ee = e$ 。故1阶群在同构意义下只有一个。
- (2) 若 $(G, *)$ 为2阶群，从而设 $G = \{e, a\}(a \neq e)$ ，易见 $ea = ae = a$ ， $ee = e$ 但 aa 呢？
若 $aa = a$ 则 $a = e$ 矛盾，故 $aa = e$ 。故2阶群在同构意义下只有一个。

乘法表见下：

$*$	e	a
e	e	a
a	a	e

群的性质：群的阶（续）

(3) 若 $\langle G, * \rangle$ 为3阶群，从而可设 $G = \{e, a, b\}$ ， e, a, b 互异。若 $a * a = e$ ，则 $a * b = b$ ，矛盾，故 $a * a = b$ 。运算表唯一。因此，3阶群在同构意义下只有一个。

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

群的性质：群的阶（续）

■ 证明：四阶群皆为Abel群

证：设 $G = \{e, a, b, c\}$ ， e 为幺。现证 $ab = ba$

情况1. $ab = e$ 从而 ba 只能为 e 或 c ，若 $ba = c$ 则 $aba = ac$ ，从而 $ea = ac$ ，从而 $c = e$ 矛盾，故 $ba = e$ 。

情况2. $ab = c$ ，同理 $ba = c$

同理 $bc = cb$ ， $ac = ca$ 。 $\square$

■ 证明：四阶群中元素的阶为1、2或者4（不为3）。

假设有个元素 a 的阶为3， $\{e, a, a^2, b\}$ ， $ab=?$ （矛盾）

群的性质：群的阶（续）

(4) 只有两种四阶群

- 有个元素的阶为4:

$$\{e, a, a^2, a^3\}$$

与 $\langle \mathbb{Z}_4, \oplus_4 \rangle$ 同构

- 元素的阶均不为4:

Klein四元群

*	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

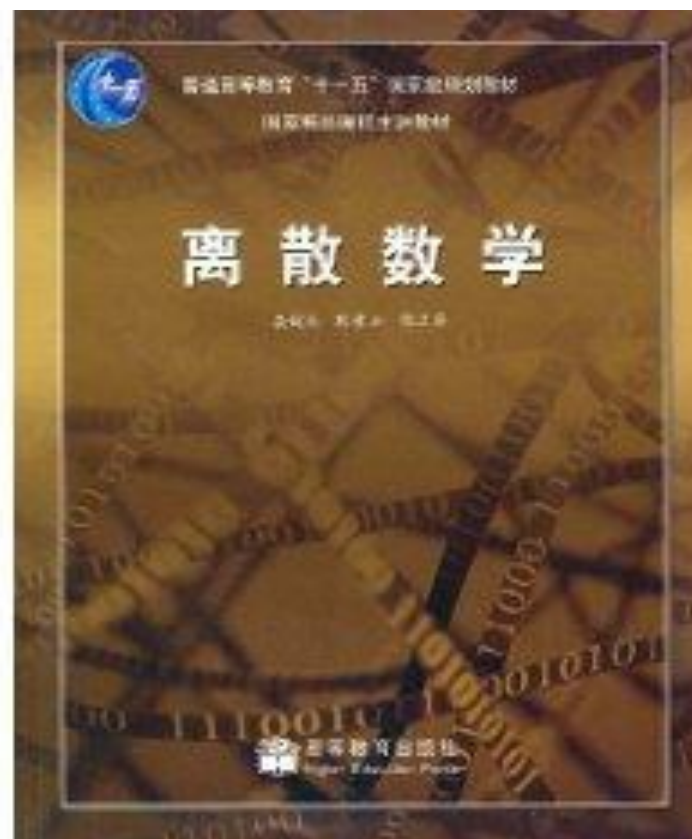
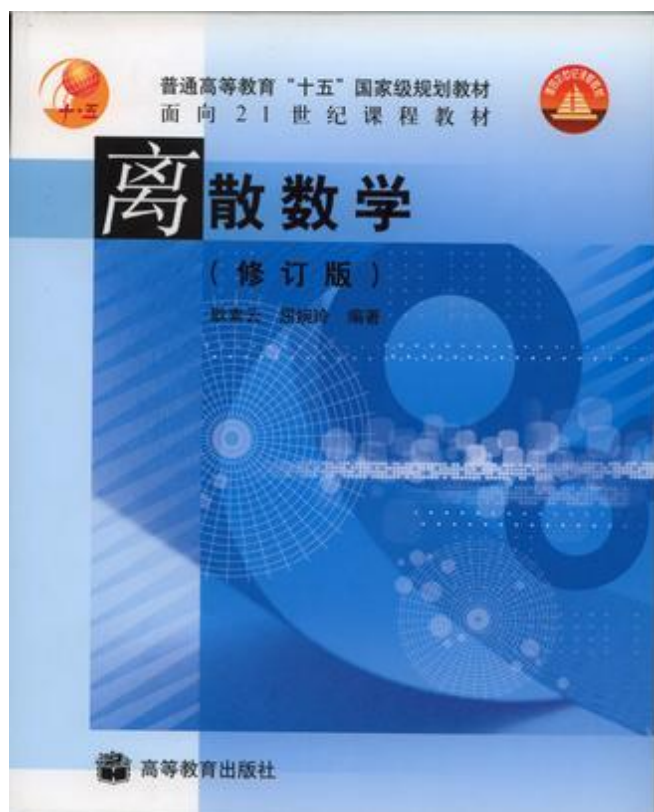
本节小结

56

- 问题1：什么是代数系统？
 - ▣ 非空集合+封闭的(二元)运算
- 问题2：代数系统相关性质？
 - ▣ 封闭性、结合性、交换性、分配性；单位元、零元、逆元；同态同构
- 问题3：什么是群？
 - ▣ 封闭 + 结合律 + 单位元 + 逆元
- 问题4：群具有哪些性质？
 - ▣ 元素的阶、群的阶

“代数系统”参考教材

57



作业

58

□ 见课程主页

群方程*

定理 若代数系统 $(G, *)$ 为半群且在 G 中方程 $ax = b$ 与 $ya = b$ 有唯一解, 则 $(G, *)$ 为群

证: 第一步 证明有左幺 $e_l \in G$ 使 $(\forall a \in G)(e_l a = a)$

取定 $b \in G$, $xb = b$ 有唯一解, 设为 e_l 。对任何 $a \in G$ 下证 $e_l a = a$ 。

$\because bx = a$ 有解 c , $\therefore e_l a = e_l(bc) = (e_l b)c = bc = a$

第二步 证明 $(\forall a \in G)(\exists a^{-1} \in G)(a^{-1}a = e_l)$ 即左逆存在

令 a^{-1} 为 $ya = e_l$ 的唯一解即可

第三步 证明 $aa^{-1} = e_l$ 即左逆=右逆

$\because a^{-1} \in G \therefore ya^{-1} = e_l$ 有唯一解 a' , 从而 $a'a^{-1} = e_l$ 从而

$$aa^{-1} = e_l(aa^{-1}) = (a'a^{-1})(aa^{-1}) = a'(a^{-1}a)a^{-1} = a'e_la^{-1} = a'a^{-1} = e_l$$

第四步 $(\forall a \in G)(ae_l = a)$ 即左幺=右幺

$$\because ae_l = a(a^{-1}a) = (aa^{-1})a = e_la = a \therefore ae_l = a$$

因此 $(G, *, e, ^{-1})$ 为群 $\square$

群的方程定义*

- 群有以下二种等价的定义：
- (1) 若 $\langle G, * \rangle$ 为半群且方程 $ax = b$ 与 $ya = b$ 有唯一解，则称 $\langle G, * \rangle$ 为群
- (2) 若 $\langle G, * \rangle$ 为半群，存在左单位元，且每个元素都具有左逆元，则 $\langle G, * \rangle$ 称为群

群的方程定义*

对于半群 $\langle G, * \rangle$, 设 e_l 为其左幺元 (题设), 对任意 $a \in G$, a_l 为其左逆元 (题设), 故 $a_l * a = e_l$, 因为 $a_l \in G$, 故对于 a_l , $\exists a^{-1} \in G$, 使得 $a^{-1} * a_l = e_l$, 则立即有: $a * a_l = e_l * (a * a_l) = (a^{-1} * a_l) * (a * a_l) = a^{-1} * (a_l * a) * a_l = a^{-1} e_l a_l = a^{-1} a_l = e_l$. 故左逆元 = 右逆元;

下证 e_l 即为右幺: $\forall a \in G$, $a * e_l = a * (a_l * a) = (a * a_l) * a = e_l * a = a$, 故 e_l 即为系统的幺元, $\forall a \in G$, a_l 为 a 之逆. 综上, $\langle G, * \rangle$ 即为群.

群的方程定义*

推论 设 $(G, *)$ 为半群且 $|G|$ 有穷, 若 $(G, *)$ 满足消去律, 则 $(G, *)$ 为群

证: 设 $G = \{a_1, \dots, a_n\}$, $\forall a, b \in G$ 下证明方程 $ax = b$ 有唯一解, 令 $aG = \{aa_i | i = 1, 2, \dots, n\}$

$\because$ 左消去律 $\therefore |aG| = n$ 从而 $aG = G$ 而 $b \in G$ 故有 $a_i \in G$ 使 $aa_i = b$ 从而 $ax = b$ 有解,
又 $\because$ 左消去律 $\therefore$ 解唯一。同理可证 $ya = b$ 有唯一解。因此 $(G, *)$ 为群。 $\square$

有穷代数系统若满足结合律和消去律, 则必为**群**。

$\langle \mathbb{Z}^+, * \rangle$ (普通乘法) 满足结合律和消去律, 但**不是**群

Évariste Galois (1811-1832)



在伽罗瓦还只有十几岁的时候，他就发现了 n 次多项式可以用根式解的充要条件，解决了长期困扰数学界的问题。他是第一个使用群这一个数学术语来表示一组置换的人。**与尼尔斯·阿贝尔并称为现代群论的创始人。**

1830年法国七月革命发生，保皇势力出亡，高等师范学校校长将学生锁在高墙内，引起伽罗瓦强烈不满，12月伽罗瓦在校报上抨击校长的作法，由于强烈支持共和主义，从1831年5月后，伽罗瓦两度因政治原因下狱，也曾企图自杀。

据说1832年3月他在狱中结识一个医生的女儿并陷入狂恋，因为这段感情，他陷入一场决斗，自知必死的伽罗瓦在决斗前夜将他的所有数学成果狂笔疾书纪录下来，并时不时在一旁写下“我没有时间”，第二天他果然在决斗中身亡，时间是1832年5月31日。这个传说富浪漫主义色彩，为后世史家所质疑。

Niels Abel (1802-1829)



阿贝尔的第一个抱负不凡的冒险，是试图解决一般的五次方程。…失败给了他一个非常有益的打击；它把他推上了正确的途径，使他怀疑一个代数解是否是可能的。他**证明了不可解**。那时他大约十九岁。

阿贝尔的《关于非常广泛的一类超越函数的一般性质的论文》呈交给巴黎科学院。这就是勒让德后来用贺拉斯的话描述为“永恒的纪念碑”的工作，埃尔米特说：“**他给数学家们留下了够他们忙上五百年的东西。**”它是现代数学的一项登峰造极的成就。（摘自贝尔：《数学精英》）

这篇论文的一个评阅人勒让德74岁，发现这篇论文很难辨认，而另一位评阅人，39岁的柯西正处于自我中心的顶峰，把论文带回家，不知放在何处，完全忘了。4年后，当柯西终于将它翻出来时，阿贝尔已经不在人世。作为补偿，科学院让阿贝尔和雅可比一起获得1830年的数学大奖。