

Chapter 4

代数系统

Discrete Mathematics

October 8, 2012

黄正华, 数学与统计学院, 武汉大学

4.1

教学内容

代数系统的引入, 运算及其性质, 半群, 群与子群, 阿贝尔群和循环群, 陪集与拉格朗日定理, 同态与同构, 环与域.

4.2

教学目的

- (1) 掌握运算及其性质;
- (2) 理解半群、群、阿贝尔群、循环群的概念、性质;
- (3) 知道陪集的概念, 掌握拉格朗日定理;
- (4) 知道同态、同构的概念;
- (5) 理解环、域的概念.

4.3

Contents

1	代数系统的引入	72
2	运算及其性质	72
3	半群	78
4	群与子群	80
5	阿贝尔群和循环群	85
7	陪集和拉格朗日定理	90
8	同态与同构	93
9	环与域	100

4.4

1 代数系统的引入

运算 & 封闭

Definition 1. 对集合 A , 一个从 A^n 到 B 的映射, 称为集合 A 上的一个 n 元运算 (n -nary operation). 如果 $B \subseteq A$, 则称该运算是封闭的.


Example 2. • 例如 $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}, f(\langle x, y \rangle) = x + y$ (这里 $+$ 表示普通的加法运算) 就是自然数集合 \mathbb{N} 上封闭的二元运算.

- 而普通的减法不是自然数集合 \mathbb{N} 上封闭的二元运算. 因为两个自然数相减可能得负数, 而负数不是自然数. 这时称集合 \mathbb{N} 对减法运算不封闭.

4.5

代数系统

Definition 3. 一个非空集合 A 及定义在 A 上的 k 个运算 f_1, f_2, \dots, f_k 所组成的系统, 称为一个代数系统 (algebraic system), 记作 $\langle A, f_1, f_2, \dots, f_k \rangle$.

 代数系统也可以用 $\langle A, +, -, *, \dots \rangle$ 表示, 其中 $+, -, *, \dots$ 表示 A 的各个代数运算.

4.6

Example 4. 设 $S = \{1, 2, 3, 4\}$, 定义 S 上的二元运算 \circ 如下:

$$x \circ y = (xy) \pmod{5}, \quad \forall x, y \in S \tag{1}$$

则 $\langle S, \circ \rangle$ 构成一个代数系统.

这里, 运算 \circ 还可用表格的形式来定义, 称为运算表:

\circ	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

从表中可以看出, 运算 \circ 在 S 上是封闭的.

4.7

代数系统

Example 5. 有类似的封闭性质的代数系统, 还有如

- $\langle \mathbb{Z}, + \rangle$, $+$ 表示通常的加法运算.
- $\langle \mathbb{Z}, * \rangle$, $*$ 表示通常的乘法运算.
- $\langle \mathcal{P}(S), \cup, \cap, \sim \rangle$ 等,


这里 \mathbb{Z} 表示整数集合, $\mathcal{P}(S)$ 表示集合 S 的幂集.

4.8

2 运算及其性质

封闭

Definition 6. 设 $*$ 是定义在集合 A 上的二元运算, 如果对任意 $x, y \in A$, 都有 $x * y \in A$, 则称运算 $*$ 在 A 上封闭.

 通俗地讲, 封闭就是和谐、不自相矛盾.

理论、系统都具有这个特点: 基本要求是能自成一体.

4.9

可交换

Definition 7. 设 $*$ 为 A 上的二元运算, 如果对任意 $x, y \in A$, 都有

$$x * y = y * x$$

则称二元运算 $*$ 在 A 上是可交换的.

Example 8. 例如,

- 实数集合上的加法和乘法是可交换的, 但减法不可交换.
- 幂集 $\mathcal{P}(A)$ 上的 \cup, \cap, \oplus (对称差) 都是可交换的, 但是相对补运算 (差运算) 不可交换.

4.10


可交换

Example 9. 设 $A = \{a, b, c, d\}$, 由表

$*$	a	b	c	d
a	a	b	c	d
b	b	d	a	c
c	c	a	b	dd
d	d	c	aa	b

所给的代数运算是否满足交换律?

解: 注意到 $d * c = a$, 而 $c * d = d$, 所以该运算不满足交换律.

 可见满足交换律的运算, 其运算表是对称的.

4.11

可结合

Definition 10. 设 $*$ 为 A 上的二元运算, 如果对于任意的 $x, y, z \in A$ 都有

$$(x * y) * z = x * (y * z),$$

则称运算 $*$ 在 A 上是可结合的.

Example 11. 例如普通的加法和乘法, 在自然数集 \mathbb{N} , 整数集 \mathbb{Z} , 有理数集 \mathbb{Q} , 实数集 \mathbb{R} 和复数集 \mathbb{C} 上都是可结合的. 减法就不满足结合律:

$$(a - b) - c \neq a - (b - c), \quad \text{除非 } c = 0.$$

4.12

可分配

Definition 12. 设 \circ 和 $*$ 是集合 A 上的两个二元运算, 如果对任意的 $x, y, z \in A$, 有

$$x * (y \circ z) = (x * y) \circ (x * z), \quad (2)$$

$$(y \circ z) * x = (y * x) \circ (z * x), \quad (3)$$

则称运算 $*$ 对 \circ 是可分配的.

Example 13. 例如,

- 实数集 \mathbb{R} 上的乘法对加法是可分配的;
- 在幂集 $\mathcal{P}(S)$ 上 \cup 和 \cap 是互相可分配的.

4.13

吸收律

Definition 14. 设 \circ 和 $*$ 是 A 上两个可交换的二元运算, 如果对于任意的 $x, y \in A$ 都有

$$x * (x \circ y) = x, \quad (4)$$

$$x \circ (x * y) = x, \quad (5)$$

则称 \circ 和 $*$ 满足吸收律.

Example 15. 例如幂集 $\mathcal{P}(S)$ 上的 \cup 和 \cap 运算满足吸收律: 任意 $A, B \in \mathcal{P}(S)$, 有

$$A \cup (A \cap B) = A, \quad (6)$$

$$A \cap (A \cup B) = A. \quad (7)$$

4.14

等幂律

Definition 16. 设 \circ 为 A 上的二元运算, 如果对于任意的 $x \in A$ 都有 $x \circ x = x$, 则称运算 \circ 是等幂的, 或称该运算适合等幂律.

Example 17. 例如幂集 $\mathcal{P}(S)$ 上的 \cup 和 \cap 运算满足等幂律: 任意 $A \in \mathcal{P}(S)$, 有

$$A \cup A = A, \quad A \cap A = A.$$

4.15

左幺元, 右幺元, 幺元

Definition 18. 设 \circ 为 A 上的二元运算,

- 如果存在 $e_l \in A$, 使得对任意 $x \in A$ 都有

$$e_l \circ x = x \quad (8)$$

则称 e_l 是 A 中关于 \circ 运算的一个左幺元.

- 如果存在 $e_r \in A$, 使得对任意 $x \in A$ 都有

$$x \circ e_r = x \quad (9)$$

则称 e_r 是 A 中关于 \circ 运算的一个右幺元.

- 若 $e \in A$ 关于 \circ 运算既是左幺元又是右幺元, 则称 e 为 A 上关于 \circ 运算的幺元.

4.16

左幺元, 右幺元, 幺元

Example 19. 在自然数集 \mathbb{N} 上, 0 是加法的幺元, 1 是乘法的幺元.

Example 20. 指出幂集 $\mathcal{P}(S)$ 上, \cup 运算和 \cap 运算的幺元.

解: \cup 运算的幺元是 \emptyset , \cap 运算的幺元是 S .

4.17

Theorem 21. 设 \circ 为 A 上的二元运算, e_l, e_r 分别为 \circ 运算的左幺元和右幺元, 则 $e_l = e_r = e$, 且 e 为 A 上关于 \circ 运算的唯一的幺元.

证: ① 因

$$e_l = e_l \circ e_r \quad (e_r \text{ 为右幺元})$$

$$e_l \circ e_r = e_r \quad (e_l \text{ 为左幺元})$$

所以 $e_l = e_r$.

令 $e_l = e_r = e$, 则 e 是 A 中的幺元.

② 假设 e' 是 A 中的另一个幺元, 则有

$$e' = e \circ e' = e.$$

所以 e 是 A 中关于 \circ 运算的唯一的幺元. □

4.18

Example 22. 设 $S = \{\alpha, \beta, \gamma, \delta\}$, $*$ 运算由下表定义, 指出 $*$ 运算是否有左幺元, 右幺元?

$*$	α	β	δ	γ
α	δ	α	β	γ
β	α	β	δ	γ
δ	α	β	δ	γ
γ	δ	γ	α	β

解: β 和 δ 都是 S 中关于 $*$ 运算的左幺元; $*$ 运算没有右幺元.

4.19

左零元, 右零元, 零元

Definition 23. 设 \circ 为 A 上的二元运算,

- 若存在元素 $\theta_l \in A$ 使得对于任意 $x \in A$ 有

$$\theta_l \circ x = \theta_l \quad (10)$$

则称 θ_l 是 A 上关于 \circ 运算的左零元.

- 若存在元素 $\theta_r \in A$ 使得对于任意 $x \in A$ 有

$$x \circ \theta_r = \theta_r \quad (11)$$

则称 θ_r 是 A 上关于 \circ 运算的右零元.

- 若 $\theta \in A$ 关于 \circ 运算既是左零元又是右零元, 则称 θ 为 S 上关于 \circ 运算的零元.

4.20

左零元, 右零元, 零元

Example 24. 例如自然数集合上 0 是普通乘法的零元, 而加法没有零元.

Example 25. 指出幂集 $\mathcal{P}(S)$ 上, \cup 运算和 \cap 运算的零元.

解: \cup 运算的零元是 S , \cap 运算的零元是 \emptyset .

注意

通俗地讲,

- 幺元是运算中影响最小的元: 运算的结果还是对方;
- 零元是运算中影响最大的元: 运算的结果总是自己.

4.21

Theorem 26. 设 \circ 为 A 上的二元运算, θ_l 和 θ_r 分别为 \circ 运算的左零元和右零元, 则有 $\theta_l = \theta_r = \theta$, 且 θ 是 A 上关于 \circ 运算的惟一零元.

证: 设 θ_l 和 θ_r 分别为 \circ 运算的左零元和右零元, 所以

$$\theta_l = \theta_l \circ \theta_r = \theta_r \quad (12)$$

令 $\theta_l = \theta_r = \theta$, 则 θ 是 A 上关于 \circ 运算的零元.

假设 θ' 也是 A 中的零元, 则有

$$\theta' = \theta \circ \theta' = \theta,$$

所以 θ 是 A 中关于 \circ 运算的惟一的零元. □

Theorem 27. 设 \circ 为 A 上的二元运算, e 和 θ 分别为 \circ 运算的幺元和零元, 如果 A 至少有两个元素, 则 $e \neq \theta$.

证: 用反证法. 假设 $e = \theta$, 则对 $\forall x \in A$ 有

$$x = x \circ e \quad (e \text{ 是幺元})$$

$$= x \circ \theta \quad (e = \theta)$$

$$= \theta \quad (\theta \text{ 是零元})$$

此式说明 A 中只有惟一的元素 θ , 与 A 中至少含有两个元素矛盾. □

左逆元, 右逆元, 逆元

Definition 28. 设 \circ 为 A 上的二元运算, $e \in A$ 为 \circ 运算的幺元, 对于 $x \in A$,

- 如果存在 y_l 使得 $y_l \circ x = e$, 则称 y_l 是 x 的左逆元.
- 如果存在 y_r 使得 $x \circ y_r = e$, 则称 y_r 是 x 的右逆元.
- 若 $y \in S$ 既是 x 的左逆元又是 x 的右逆元, 则称 y 是 x 的逆元 (inverse elements).
 - 如果 x 的逆元存在, 则称 x 是可逆的.
 - 一个元素 x 的逆元通常记为 x^{-1} .
 - 当运算被称为“加法运算”时 (记为 $+$), x 的逆元可记为 $-x$.

Example 29. 例如, 在整数集合 \mathbb{Z} 上, 加法的幺元是 0. 对任何整数, 它的加法逆元都存在, 即它的相反数 $-x$.

注意

对于给定的集合和二元运算来说,

- 如果幺元或零元存在, 一定是惟一的.
- 而逆元能否存在, 与元素有关. 有的元素有逆元, 有的元素没有逆元, 不同的元素对应着不同的逆元.
 - 一个元素的左逆元不一定等于它的右逆元.
 - 一个元素可以有左逆元不一定有右逆元.
 - 甚至一个元素的左 (右) 逆元不一定是惟一的.

Theorem 30. 设 \circ 为 A 上可结合的二元运算, e 为么元. 对 $x \in A$, 若存在左逆元 y_l 和右逆元 y_r , 则有 $y_l = y_r = y$, 且 y 是 x 的唯一的逆元.

证: ① 对于 $x \in A$, 注意到 y_l 和 y_r 是 x 的左、右逆元, 有 $y_l \circ x = e$ 和 $x \circ y_r = e$, 得

$$\begin{aligned} y_l &= y_l \circ e && (e \text{ 是么元}) \\ &= y_l \circ (x \circ y_r) && (y_r \text{ 是 } x \text{ 的右逆元}) \\ &= (y_l \circ x) \circ y_r && (\circ \text{ 为可结合的}) \\ &= e \circ y_r && (y_l \text{ 是 } x \text{ 的左逆元}) \\ &= y_r && (e \text{ 是么元}) \end{aligned}$$

令 $y_l = y_r = y$, 则 y 是 x 的逆元.

证: ② 下面证明逆元的惟一性.

假若 $y' \in A$ 也是 x 的逆元, 则

$$\begin{aligned} y' &= y' \circ e && (e \text{ 是么元}) \\ &= y' \circ (x \circ y) && (y \text{ 是 } x \text{ 的逆元}) \\ &= (y' \circ x) \circ y && (\circ \text{ 为可结合的}) \\ &= e \circ y && (y' \text{ 是 } x \text{ 的逆元}) \\ &= y. && (e \text{ 是么元}) \end{aligned}$$

所以 y 是 x 惟一的逆元. □

设代数系统 $\langle A, * \rangle$, 其中 $A = \{a, b, c\}$, A 上的二元运算 $*$ 定义如表: 试分析 $*$ 运算的封闭性,

$*$	a	b	c
a	a	b	c
b	b	a	c
c	c	c	c

Example 31. 交换性, 等幂性. A 中关于 $*$ 是否有么元和零元? 如有么元, 每个元素是否有逆元? 如有, 求出逆元.

解: 这些运算性质可直接从运算表看出:

- $*$ 运算是封闭的, 因为表中每个元素都属于 A .
- $*$ 运算可交换, 因运算表关于主对角线对称.
- $*$ 运算不等幂, 因运算表主对角线有的元素与所在行列表头元素不同.
- $*$ 运算有零元 c , 因为 c 所在行列中的元素都是与它相同.
- $*$ 运算有么元 a , 因为 a 所在行列中的元素依次与表头行列一致.
- a 和 b 均以自身为逆元, 因为 a, b 所在行和列交汇处的元素为么元.

Example 32. 设 $\mathbb{N}_k = \{0, 1, 2, \dots, k-1\}$, 在 \mathbb{N}_k 定义运算 $+_k$ 如下: 对任意 $x, y \in \mathbb{N}_k$

$$x +_k y = \begin{cases} x + y, & x + y < k \\ x + y - k, & x + y \geq k \end{cases}$$

试分析 \mathbb{N}_k 中的每个元素是否有逆元? 如有, 求出逆元.

解: 因为对任意 $x \in \mathbb{N}_k$, $x + 0 = x < k$, 所以

$$x +_k 0 = 0 +_k x = x + 0 = x,$$

故 0 是幺元.

对任意 $x \in \mathbb{N}_k$, 令 $x +_k y = 0$, 分两种情况讨论:

- (1) 如果 $x + y < k$, 按运算 $+_k$ 的定义, 有 $x +_k y = x + y = 0$, 因 $x, y \in \mathbb{N}_k$, 可知 $x = y = 0$, 因此 0 以自身为逆元;
- (2) 如果 $x + y \geq k$, 则有 $x +_k y = x + y - k = 0$, 解出 $y = k - x$. 即每个非 0 元素 x 都有逆元 $k - x$. □

4.28

从运算表看运算的性质

对代数系统 $\langle A, * \rangle$, 其二元运算 $*$ 的性质可以根据运算表表现出来:

- 运算 $*$ 具有封闭性, 当且仅当运算表中的每个元素都属于 A .
- 运算 $*$ 具有可交换性, 当且仅当运算表关于主对角线是对称的.
- 运算 $*$ 具有等幂性, 当且仅当运算表的主对角线上的每一元素与它所在行(列)的表头元素相同.
- A 中关于运算 $*$ 具有零元, 当且仅当该元素所对应的行和列中的元素都与该元素相同.
- A 中关于运算 $*$ 具有幺元, 当且仅当该元素所对应的行和列依次与运算表的行和列相一致.
- 设 A 中关于运算 $*$ 具有幺元, a 和 b 互逆, 当且仅当位于 a 所在行和 b 所在列的元素及 b 所在行和 a 所在列的元素都是幺元.

4.29

3 半群

广群 & 半群

Definition 33. 如果集合 S 上的二元运算 $*$ 是封闭的, 则称代数系统 $\langle S, * \rangle$ 为广群 (groupoid). 也称为群坯.

Definition 34. 如果集合 S 上的二元运算 $*$ 是封闭的, 并且满足结合律, 则称代数系统 $\langle S, * \rangle$ 为半群 (semigroup).

4.30

Example 35. 设 $S = \{a, b, c\}$, 定义 S 上的运算 $*$ 如表所示, 验证 $\langle S, * \rangle$ 是否为半群.

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

解: 从运算可看出运算 $*$ 是封闭的.

另外 a, b, c 皆为左幺元, 所以, 对任意 $x, y, z \in S$, 均有

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

所以 $*$ 运算是可结合的. 从而 $\langle S, * \rangle$ 是半群. □

4.31

例 36 代数系统 $\langle \mathbb{N}^+, - \rangle$ 和 $\langle \mathbb{R}, / \rangle$ 是半群吗? 这里 \mathbb{N}^+ 为正整数集, \mathbb{R} 为实数集, $-$ 和 $/$ 是普通的减法和除法.

4.32

子半群

Theorem 36. 设 $\langle S, * \rangle$ 为一半群, $B \subseteq S$ 且 $*$ 在 B 上封闭, 那么 $\langle B, * \rangle$ 也是一个半群. 通常称 $\langle B, * \rangle$ 为 $\langle S, * \rangle$ 的子半群.

证明思路: 结合律在 B 上仍成立.

Example 37. 普通乘法运算在某些集合上构成 $\langle \mathbb{R}, \times \rangle$ 的子半群. 例如:

- $\langle [0, 1], \times \rangle$;
- $\langle [0, 1), \times \rangle$;
- $\langle \mathbb{Z}, \times \rangle$.

4.33

Theorem 38. 设 $\langle S, * \rangle$ 为一个半群, 如果 S 是一个有限集合, 则必有 $a \in S$, 使得 $a * a = a$.

证: 因 $\langle S, * \rangle$ 是半群, $\forall b \in S$, 由 $*$ 的 因为 $p \geq 1$, 所以 $\exists k \geq 1$, 使得 封闭性可知

$$kp \geq i$$

$b * b \in S$, 记 $b^2 = b * b$ 对于 $b^{kp} \in S$, 有
 $b^2 * b = b * b^2 \in S$, 记 $b^3 = b^2 * b = b * b^2$

$$\begin{aligned} b^{kp} &= b^p * b^{kp} \\ &= b^p * (b^p * b^{kp}) \end{aligned}$$

4.34

因 S 是一个有限集合, 所以 $\exists j > i$, 使

$$\begin{aligned} &= b^{2p} * b^{kp} \\ &= b^{2p} * (b^p * b^{kp}) \\ &= \dots \end{aligned}$$

$$b^i = b^j$$

令 $p = j - i$, 即 $j = p + i$, 代入上式得

$$= b^{kp} * b^{kp}$$

$$b^i = b^p * b^i$$

所以, $b^q = b^p * b^q$, $q \geq i$.

所以, 存在 $a = b^{kp}$, 使 $a * a = a$.

Definition 39. 含有幺元的半群, 称为独异点 (monoid), 或亚群, 含幺半群.

4.35

Theorem 40. 设 $\langle S, * \rangle$ 是一个独异点, 则在关于运算 $*$ 的运算表中任何两行或两列都是不相同的.

证: 设 S 中关于 $*$ 运算的 幺元是 e .

$\forall a, b \in S$, 且 $a \neq b$ 时, 有

4.36

$$e * a = a \neq b = e * b, \tag{13}$$

$$a * e = a \neq b = b * e. \tag{14}$$

所以, 在 $*$ 的运算表中 不可能有两行或两列是 相同的. \square

$*$	\dots	a	\dots	b	\dots
\vdots	\dots	\vdots	\dots	\vdots	\dots
e	\dots	a	\dots	b	\dots
\vdots	\dots	\vdots	\dots	\vdots	\dots
$*$	\dots	e	\dots		
\vdots	\dots	\vdots	\dots		
a	\dots	a	\dots		
\vdots	\dots	\vdots	\dots		
b	\dots	b	\dots		
\vdots	\dots	\vdots	\dots		

Example 41. 设 \mathbb{Z} 是整数集合, m 是任意正整数, Z_m 是由模 m 的同余类组成的同余类集, 在 Z_m 上定义两个二元运算 $+_m$ 和 \times_m 分别如下:

对于任意的 $[i], [j] \in Z_m$

$$[i] +_m [j] = [(i + j) \pmod{m}] \quad (15)$$

$$[i] \times_m [j] = [(i \times j) \pmod{m}] \quad (16)$$

试证明在这两个二元运算的运算表中任何两行或两列都是不相同的.

证: 考察代数系统 $\langle Z_m, +_m \rangle$ 和 $\langle Z_m, \times_m \rangle$, 先分三步证明 $\langle Z_m, +_m \rangle$ 是独异点, 再利用定理的结论:

- (1) 证明两个运算在 Z_m 上封闭;
- (2) 证明两个运算满足结合律;
- (3) 证明 $[0]$ 是 $\langle Z_m, +_m \rangle$ 的幺元, $[1]$ 是 $\langle Z_m, \times_m \rangle$ 的幺元.

本例题的实例见表 5-3.2 和表 5-3.3.

Theorem 42. 设 $\langle S, * \rangle$ 是一个独异点, 对于任意 $a, b \in S$, 若 a, b 均有逆元, 则

- (1) $(a^{-1})^{-1} = a$;
- (2) $a * b$ 有逆元, 且 $(a * b)^{-1} = b^{-1} * a^{-1}$.

证: ① 因 a^{-1} 和 a 为互为逆元, 直接得到结论.

② 必须证明两种情况:

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

和

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

利用结合律容易得出.

4 群与子群

群

Definition 43. 称代数系统 $\langle G, * \rangle$ 为群 (group), 如果

- (1) 运算 $*$ 是封闭的.
- (2) 运算 $*$ 是可结合的.
- (3) 存在幺元 e .
- (4) 每一元素 x 都有逆元 x^{-1} .

上述四个条件, 依次得到概念: 广群 \rightarrow 半群 \rightarrow 独异点 \rightarrow 群.

Example 44. 例如,

- $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{Q}^+, * \rangle$, $\langle \mathbb{R} - \{0\}, * \rangle$ 都是群, 这里, $+$ 和 $*$ 表示数的加法和乘法, \mathbb{Z} 表示整数集, \mathbb{Q}^+ 表示正有理数集, \mathbb{R} 表示实数集.

– $\langle \mathbb{Z}, + \rangle$ 的幺元为 0, 逆元 $x^{-1} = -x$.

– $\langle \mathbb{Q}^+, * \rangle$ 的幺元为 1, 逆元 $x^{-1} = 1/x$.

- $\langle \mathbb{R} - \{0\}, * \rangle$ 的幺元为 1, 逆元 $x^{-1} = 1/x$.

• $\langle \mathbb{N}, + \rangle, \langle \mathbb{R}, * \rangle$ 不是群.

- \mathbb{N} 中除幺元 0 外, 其余元素无逆元.

- \mathbb{R} 中 0 无逆元.

4.40

Example 45. $R = \{0^\circ, 60^\circ, 120^\circ, 180^\circ, 240^\circ, 300^\circ\}$, $*$ 是 R 上的二元运算, $a * b$ 表示先旋转 a 再旋转 b 的角度, 并规定旋转 360° 等于原来的状态. 验证 $\langle R, * \rangle$ 是一个群.

$*$	0°	60°	120°	180°	240°	300°
0°	0°	60°	120°	180°	240°	300°
60°	60°	120°	180°	240°	300°	0°
120°	120°	180°	240°	300°	0°	60°
180°	180°	240°	300°	0°	60°	120°
240°	240°	300°	0°	60°	120°	180°
300°	300°	0°	60°	120°	180°	240°

解: 验证 $\langle R, * \rangle$ 满足

(1) 运算 $*$ 封闭;

(2) 满足结合律: $(a * b) * c$ 和 $a * (b * c)$ 的旋转角度为 $a + b + c \pmod{360^\circ}$.

(3) 有幺元 0° ;

(4) 元素都有逆元: $60^\circ, 120^\circ, 180^\circ$ 分别与 $300^\circ, 240^\circ, 180^\circ$ 互逆. □

4.41

有限群, 有限群的阶数, 无限群

Definition 46. 设 $\langle G, * \rangle$ 是一个群.

• 若 G 为有限集, 则称 $\langle G, * \rangle$ 为有限群 (finite group); 此时 G 的元素个数称为该有限群的阶数 (order), 记为 $|G|$.

• 若 G 为无限集, 称 $\langle G, * \rangle$ 为无限群 (infinite group).

4.42

Theorem 47. 群中不可能有零元.

证: 设 $\langle G, * \rangle$ 为群.

① 当群的阶为 1 时, 它的惟一元素视作幺元 e .

② 设 $|G| > 1$ 且群有零元 θ . 那么群中任何元素 $x \in G$, 都有

$$x * \theta = \theta * x = \theta \neq e.$$

所以, 零元 θ 就不存在逆元, 与 $\langle G, * \rangle$ 是群的假设矛盾. □

4.43

Theorem 48. 设 $\langle G, * \rangle$ 为群, 对于 $a, b \in G$, 必存在 $x \in G$, 使得关于 x 的方程 $a * x = b, x * a = b$ 都有惟一解.

证: ① 先证解的存在性.

设 a 的逆元 a^{-1} , 令

$$x = a^{-1} * b, \quad (\text{构造一个解})$$

则

$$\begin{aligned} a * x &= a * (a^{-1} * b) \\ &= (a * a^{-1}) * b \\ &= e * b \\ &= b. \end{aligned}$$

证: ② 再证解惟一性.

若另有解 x_1 满足 $a * x_1 = b$, 则

$$a^{-1} * (a * x_1) = a^{-1} * b$$

即

$$x_1 = a^{-1} * b. \quad \square$$

4.44

Theorem 49. 设 $\langle G, * \rangle$ 为群, 那么, 对任意 $a, x, y \in G$,

$$a * x = a * y \Rightarrow x = y \quad (17)$$

$$x * a = y * a \Rightarrow x = y \quad (18)$$

因此, 群中消去律成立.

证: 设 $a * x = a * y$, 且 a 的逆元是 a^{-1} , 则有

$$\begin{aligned} a^{-1} * (a * x) &= a^{-1} * (a * y) \\ (a^{-1} * a) * x &= (a^{-1} * a) * y && \text{(结合律)} \\ e * x &= e * y \\ x &= y. \end{aligned}$$

4.45

同理可证 (18) 式. □

置换

Definition 50. 设 S 是一个非空集合, 从集合 S 到 S 的一个双射称为 S 的一个置换.

Example 51. 设 $S = \{a, b, c, d\}$. $f: S \rightarrow S$, $f(a) = b$; $f(b) = d$; $f(c) = a$; $f(d) = c$. 这个置换可以表示成如下形式:

$$\begin{pmatrix} a & b & c & d \\ b & d & a & c \end{pmatrix}$$

4.46

Theorem 52. 设 $\langle G, * \rangle$ 为群, 那么, 运算表中的每一行或每一列都是群 G 的元素的置换.

证: 先证运算表中的任一行或任一列所含 G 中的一个元素不可能多于一次.

用反证法: 设 $a \in G$ 对应的行有两个元素都是 c , 即

$$a * b_1 = a * b_2 = c, \quad \text{且 } b_1 \neq b_2.$$

*	...	b_1	...	b_2	...
⋮	...	⋮	...	⋮	...
a	...	c	...	c	...
⋮	...	⋮	...	⋮	...

由消去律得 $b_1 = b_2$. 这与 $b_1 \neq b_2$ 矛盾.

再证 G 中每一个元素必出现一次.

证: 考察对应于元素 $a \in G$ 的那一行, 设 b 是 G 中的任意一个元素, 则 $a^{-1} * b \in G$, 它必出现在运算表的顶行.

*	...	$a^{-1} * b$...
⋮	...	⋮	...
a	...	b	...
⋮	...	⋮	...

由于

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

所以 b 必定出现在运算表中对应于 a 的那一行.

综上所述: $\langle G, * \rangle$ 的运算表中每一行都是 G 的元素的一个置换, 且每一行都是不同的. 对于列的证明类似. □

4.47

等幂元

Definition 53. 代数系统 $\langle G, * \rangle$ 中, 如果存在 $a \in G$, 有 $a * a = a$, 则称 a 为运算 $*$ 的等幂元.

4.48

等幂元

Theorem 54. 在群 $\langle G, * \rangle$ 中, 除幺元 e 之外, 不可能有任何别的等幂元.

证: 因为 $e * e = e$, 所以 e 是等幂元.

现设 $a \in G$, $a \neq e$ 且 $a * a = a$, 则有

$$\begin{aligned}
 a &= e * a \\
 &= (a^{-1} * a) * a \\
 &= a^{-1} * (a * a) \\
 &= a^{-1} * a && \text{(已假设 } a * a = a) \\
 &= e.
 \end{aligned}$$

与假设 $a \neq e$ 相矛盾. □

4.49

子群

Definition 55. 设 $\langle G, * \rangle$ 是群, $S \subseteq G$, S 非空. 如果 $\langle S, * \rangle$ 也是群, 则称 $\langle S, * \rangle$ 为 $\langle G, * \rangle$ 的子群 (subgroup).

Definition 56. 设 $\langle G, * \rangle$ 为群, $\langle S, * \rangle$ 为 G 的子群, 如果 $S = \{e\}$ 或 $S = G$, 那么称 $\langle S, * \rangle$ 为 $\langle G, * \rangle$ 的平凡子群.

简言之, $\langle \{e\}, * \rangle$ 和 $\langle G, * \rangle$ 是群 $\langle G, * \rangle$ 的两个平凡子群.

G 还可能其它的子群, 称为 G 的真子群. 例如, 偶数全体构成整数加群的一个真子群.

Example 57. $\langle \mathbb{Z}, + \rangle$ 是一个群, 设 $\mathbb{Z}_E = \{x \mid x = 2n, n \in \mathbb{Z}\}$, 证明 $\langle \mathbb{Z}_E, + \rangle$ 是 $\langle \mathbb{Z}, + \rangle$ 的一个子群.

证: 本题的实质是要证明 $\langle \mathbb{Z}_E, + \rangle$ 是群. 按群的定义证明如下:

- (1) 证明 $+$ 运算在 \mathbb{Z}_E 上封闭: 任取 $x, y \in \mathbb{Z}_E$, 可设 $x = 2n_1, y = 2n_2$, 其中 $n_1, n_2 \in \mathbb{Z}$. 那么 $x + y = 2(n_1 + n_2) \in \mathbb{Z}_E$, 故运算封闭.
- (2) 因 $+$ 运算在 \mathbb{Z} 上可结合, 而 $+$ 运算在 \mathbb{Z}_E 上封闭, 所以, $+$ 运算在 \mathbb{Z}_E 上可结合.
- (3) 因 $\langle \mathbb{Z}, + \rangle$ 的幺元 0 在 \mathbb{Z}_E 中, 所以 $\langle \mathbb{Z}_E, + \rangle$ 有幺元 0 .
- (4) 对任意 $x = 2n \in \mathbb{Z}_E$, 有 $2n + 2(-n) = 0$, 而 $-n \in \mathbb{Z}$, 即 $2(-n) \in \mathbb{Z}_E$. 这说明 \mathbb{Z}_E 中的任意元素有逆元.

所以 $\langle \mathbb{Z}_E, + \rangle$ 是群, 又因 $\mathbb{Z}_E \subseteq \mathbb{Z}$, 所以 $\langle \mathbb{Z}_E, + \rangle$ 是群 $\langle \mathbb{Z}, + \rangle$ 的子群. \square

Theorem 58. 设 $\langle G, * \rangle$ 为群, $\langle S, * \rangle$ 为 $\langle G, * \rangle$ 的子群, 那么, $\langle G, * \rangle$ 中的幺元 e 必定也是 $\langle S, * \rangle$ 中的幺元.

证: 已知 $\langle G, * \rangle$ 中的幺元 e , 设 $\langle S, * \rangle$ 中的幺元为 e_1 .

对于任意一个元素 $x \in S \subseteq G$, 必有

$$e_1 * x = x = e * x.$$

则由消去律有,

$$e_1 = e. \quad \square$$

Theorem 59. 设 $\langle G, * \rangle$ 为群, S 为 G 的非空子集, 如果对于任意元素 $a, b \in S$, 有 $a * b^{-1} \in S$, 则 $\langle S, * \rangle$ 必定是 $\langle G, * \rangle$ 的子群.

证: 分四步证明:

- (1) 先证 G 中的幺元 e 也是 S 中的幺元:
对任意元素 $a \in S \subseteq G$, $e = a * a^{-1} \in S$ 且 $a * e = e * a = a$, 即 e 也是 S 中的幺元.
- (2) 其次证 S 中的每一个元素都有逆元:
对任意元素 $a \in S$ 中, 因为 $e \in S$, 所以 $e * a^{-1} \in S$, 即 $a^{-1} \in S$.

(3) 然后证明 $*$ 在 S 中是封闭的:

对任意元素 $a, b \in S, b^{-1} \in S$, 而 $b = (b^{-1})^{-1}$. 所以

$$a * b = a * (b^{-1})^{-1} \in S. \quad (19)$$

(4) 结合律是保持的.

因此, $\langle S, * \rangle$ 是 $\langle G, * \rangle$ 的子群. □

4.53

Theorem 60. 设 $\langle G, * \rangle$ 为群, B 为 G 的非空子集, 如果 B 是一个有限集, 那么, 只要运算 $*$ 在 B 上封闭, $\langle B, * \rangle$ 必定是 $\langle G, * \rangle$ 的子群.

证: 先证幺元的存在性.

设任意元素 $b \in B$, 若 $*$ 在 B 上封闭, 则元素 $b^2 = b * b, b^3 = b^2 * b, b^4 = b^3 * b, \dots$, 都在 B 中.

由于是有限集, 所以必存在正整数 i 和 j ($i < j$), 使得

$$b^i = b^j, \quad \text{即 } b^i = b^i * b^{j-i}. \quad (20)$$

可见 $e = b^{j-i}$ 是 $\langle G, * \rangle$ 中的幺元, 且该幺元也在子集 B 中.

再证任意 $b \in B$ 存在逆元.

如果 $j - i > 1$, 则由 $e = b^{j-i} = b * b^{j-i-1}$, 可知 b^{j-i-1} 是 b 的逆元, 且 $b^{j-i-1} \in B$;

如果 $j - i = 1$, 则 (20) 式为 $b^i = b^i * b$, 可知 b 是幺元, 而幺元是以自身为逆元的.

综上, $\langle B, * \rangle$ 是 $\langle G, * \rangle$ 的一个子群. □

4.54

5 阿贝尔群和循环群

阿贝尔群

Definition 61. 如果群 $\langle G, * \rangle$ 中的二元运算 $*$ 是可交换的, 则称该群为阿贝尔群 (Abelian group), 也叫交换群 (commutative group).

4.55

Example 62. 证明 1, 2, 3, 4 阶群都是交换群.

解: 群 $\langle G, * \rangle$ 的运算表中的每行 (列) 都是 G 中元素的一个置换. 因此很容易得出 1, 2, 3, 4 阶群的运算表, 不论其元素是什么, 只要它们构成群, 其群表的形式是固定不变的.

$*$	1
1	1

$*$	1	2
1	1	2
2	2	1

$*$	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

由群表可知, 1, 2, 3, 4 阶群都是交换群.

4.56

四阶群 $\langle \{1, 2, 3, 4\}, * \rangle$ 的群表有四种形式:

*	1	2	3	4	*	1	2	3	4
1	1	2	3	4	1	1	2	3	4
2	2	4	1	3	2	2	1	4	3
3	3	1	4	2	3	3	4	1	2
4	4	3	2	1	4	4	3	2	1

*	1	2	3	4	*	1	2	3	4
1	1	2	3	4	1	1	2	3	4
2	2	1	4	3	2	2	3	4	1
3	3	4	2	1	3	3	4	1	2
4	4	3	1	2	4	4	1	2	3

Theorem 63. 群 $\langle G, * \rangle$ 是阿贝尔群的充分必要条件是: 对任意 $a, b \in G$, 有

$$(a * b) * (a * b) = (a * a) * (b * b). \quad (21)$$

证: 充分性. 对任意 $a, b \in G$, 如果 $(a * b) * (a * b) = (a * a) * (b * b)$, 那么,

$$\begin{aligned} a^{-1} * (a * b) * (a * b) * b^{-1} &= a^{-1} * (a * a) * (b * b) * b^{-1}, \\ (a^{-1} * a) * (b * a) * (b * b^{-1}) &= (a^{-1} * a) * (a * b) * (b * b^{-1}), \quad (\text{结合律}) \\ b * a &= a * b. \end{aligned}$$

这说明 $*$ 运算是可交换的.

必要性. 若群 $\langle G, * \rangle$ 是交换群, 则对任意 $a, b \in G$, 有

$$\begin{aligned} (a * b) * (a * b) &= a * (b * a) * b \\ &= a * (a * b) * b \\ &= (a * a) * (b * b). \end{aligned} \quad \square$$

幂 (乘方)

- 在一个群 $\langle G, * \rangle$ 里, 结合律是成立的. 所以

$$a_1 * a_2 * \cdots * a_n$$

有意义, 是 G 的某一个元.

- $a * a * \cdots * a$ 当然也是 G 的一个元, 记为

$$\underbrace{a * a * \cdots * a}_{n \uparrow} = a^n, \quad n \text{ 是正整数.}$$

叫做 a 的 n 次幂 (或 n 次方). 并且规定

$$a^0 = e, \quad (22)$$

$$a^{-n} = (a^{-1})^n, \quad (n \text{ 是正整数}). \quad (23)$$

- 对任意的整数 n, m 容易算出

$$a^n * a^m = a^{n+m}, \quad (24)$$

$$(a^n)^m = a^{nm}. \quad (25)$$

循环群

Definition 64. 如果群 $\langle G, * \rangle$ 有元素 a , 使得 G 中任意元素都可表示成 a 的幂, 即

$$G = \{a^k \mid k \text{ 为任意整数}\}. \quad (26)$$

则称该群为循环群 (cyclic group). a 称为循环群 G 的生成元.

Example 65. 所有复数

$$e^{\frac{2k\pi i}{n}} = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}, \quad (k = 0, 1, 2, \dots, n-1) \quad (27)$$

作为一个 n 阶有限循环群, $e^{\frac{2\pi i}{n}}$ 是它的一个生成元.

4.60

Example 66. 全体整数的集合 \mathbb{Z} 关于普通加法构成一个群, 我们把它称为整数加群. 试说明整数加群 $\langle \mathbb{Z}, + \rangle$ 是循环群.

解: 群 $\langle \mathbb{Z}, + \rangle$ 的幺元是 0. 任意 $a \in \mathbb{Z}$, 其逆元为 $-a$.

这个群的全体的元都是 1 的乘方. (假如把 \mathbb{Z} 的代数运算不用 $+$ 而用 $*$ 来表示, 就很容易明白了.)

假定 m 是任意正整数, 则

$$m = \underbrace{1 + 1 + \dots + 1}_m = \underbrace{1 * 1 * \dots * 1}_m = 1^m$$

所以, 对任意 $m \in \mathbb{Z}$, 有

$$m = \begin{cases} \underbrace{1 + 1 + \dots + 1}_m = 1^m, & m > 0, \\ 0 = 1^0, & m = 0, \\ \underbrace{(-1) + (-1) + \dots + (-1)}_{|m|} = (-1)^{|m|} = (1^{-1})^{|m|} = 1^m, & m < 0. \quad \square \end{cases}$$

4.61

Example 67. 设 $G = \{\alpha, \beta, \gamma, \delta\}$, 定义 G 上的运算 $*$ 如下表, 说明 $\langle G, * \rangle$ 是循环群.

*	α	β	δ	γ
α	α	β	δ	γ
β	β	α	γ	δ
δ	δ	γ	β	α
γ	γ	δ	α	β

- (1) 由运算表可知运算封闭;
- (2) 可验证运算 $*$ 是可结合的;
- (3) α 是幺元;
- (4) β, γ, δ 的逆元分别是 β, δ, γ .

所以, $\langle G, * \rangle$ 是群.

γ, δ 都是生成元:

$$\begin{aligned}\gamma^1 &= \gamma, & \gamma^2 &= \beta, \\ \gamma^3 &= \beta * \gamma = \delta, \\ \gamma^4 &= \delta * \gamma = \alpha; \\ \delta^1 &= \delta, & \delta^2 &= \beta, \\ \delta^3 &= \beta * \delta = \gamma, \\ \delta^4 &= \gamma * \delta = \alpha.\end{aligned}$$

β 不是生成元:

$$\begin{aligned}\beta^1 &= \beta, & \beta^2 &= \alpha, \\ \beta^3 &= \alpha * \beta = \beta, \\ \beta^4 &= \beta * \beta = \beta^2 = \alpha.\end{aligned}$$

□

4.62

Theorem 68. 循环群是阿贝尔群.

证: 设 $\langle G, * \rangle$ 是循环群, 生成元是 a .

对任意 $x, y \in G$, 可令 $x = a^r, y = a^s$. r, s 为整数. 那么

$$\begin{aligned}x * y &= a^r * a^s \\ &= a^{r+s} \\ &= a^{s+r} \\ &= a^s * a^r \\ &= y * x.\end{aligned}$$

交换律满足, 这就证明了循环群 $\langle G, * \rangle$ 是阿贝尔群.

□

4.63

Theorem 69. 设 a 是 n 阶有限循环群 $\langle G, * \rangle$ 的生成元, 则 $a^n = e$, 且

$$G = \{a, a^2, a^3, \dots, a^{n-1}, a^n = e\}$$

其中, e 是么元, n 是使 $a^n = e$ 的最小正整数. (称 n 为元素 a 的阶.)

证: (用反证法) 假定 $a^m = e$, m 是正整数, 且 $m < n$.

按所设, G 中任一元素皆可表示成 a^k , 令 $k = mg + r$, 其中 g 是整数, $0 \leq r < m$. 于是

$$a^k = a^{mg+r} = (a^m)^g * a^r = a^r$$

这说明 G 中任一元素皆可表示成 a^r , 从而 G 中至多只有 m 个不同的元素, 与 $|G| = n (> m)$ 矛盾.

剩下的问题是要证明 $a, a^2, a^3, \dots, a^{n-1}, a^n$ 是不同的元素.

假设 $a^i = a^j, 1 \leq i < j \leq n$, 那么

$$e = a^i * a^{-i} = a^j * a^{-i} = a^{j-i}, 1 \leq j-i < n.$$

按假设, n 是使 $a^n = e$ 的最小正整数, 所以 $a^i = a^j$ 不可能.

□

4.64

有限循环群的典型例子

整数集合 \mathbb{Z} 按同余关系 $R = \{ \langle a, b \mid a \equiv b \pmod{n} \rangle \}$, 划分为 n 个等价类 (模 n 的剩余类):

$$[0] = \{ \dots, -2n, -n, 0, n, 2n, \dots \}; \quad (28)$$

$$[1] = \{ \dots, -2n+1, -n+1, 1, n+1, 2n+1, \dots \}; \quad (29)$$

.....

$$[n-1] = \{ \dots, -n-1, -1, n-1, 2n-1, 3n-1, \dots \}. \quad (30)$$

令 $G = \{ [0], [1], [2], \dots, [n-1] \}$, 规定“加法”运算:

$$[a] \oplus [b] = [a+b] \quad (31)$$

则 $\langle G, \oplus \rangle$ 是一个群 (模 n 的剩余类加群).

4.65

有限循环群的典型例子

\oplus	[0]	[1]	...	[n-2]	[n-1]
[0]	[0]	[1]	...	[n-2]	[n-1]
[1]	[1]	[2]	...	[n-1]	[0]
\vdots	\vdots	\vdots		\vdots	\vdots
[n-1]	[n-1]	[0]	...	[n-3]	[n-2]

易见 G 的么元 $e = [0]$, 且 $[1]$ 是 G 的一个生成元.

任意 $[i] \in G$, 有

$$[i] = \underbrace{[1] \oplus [1] \oplus \dots \oplus [1]}_i \triangleq [1]^i,$$

显然,

$$G = \{ [1], [1]^2, [1]^3, \dots, [1]^{n-1}, [1]^n = [0] = e \}.$$

4.66

Example 70. 设 G 刚好包含 $x^3 = 1$ 的三个根:

$$1, \quad \varepsilon_1 = \frac{-1 + \sqrt{-3}}{2}, \quad \varepsilon_2 = \frac{-1 - \sqrt{-3}}{2}.$$

对于普通乘法来说, G 构成一个群. 为什么? 是循环群吗?

解: ① $\langle G, \times \rangle$ 是一个群:

(1) 运算封闭. 注意, 其中

$$\varepsilon_1^2 = \frac{1 + (-3) - 2\sqrt{-3}}{4} = \frac{-1 - \sqrt{-3}}{2} = \varepsilon_2, \quad \varepsilon_2^2 = \varepsilon_1.$$

(2) 满足结合律.

(3) 么元是 1.

(4) 逆元存在: ε_1 与 ε_2 互逆; 么元 1 的逆元是自己.

② 是循环群: ε_1 与 ε_2 都是生成元. □

可见, 循环群的生成元可以是不惟一的.

4.67

7 陪集和拉格朗日定理

陪集与拉格朗日定理

这一节的主要内容是利用群 G 的一个子群 H 来作一个分类, 并得到相应的定理.

相关的定义和结论, 都可以用“整数的模 n 剩余类加群”作为原型来理解.

陪集

Definition 71. 设 $\langle H, * \rangle$ 为 $\langle G, * \rangle$ 的子群, $a \in G$. 集合

$$aH \triangleq \{a * h \mid h \in H\}, \quad (32)$$

$$Ha \triangleq \{h * a \mid h \in H\}, \quad (33)$$

分别称为由 a 确定的 H 在 G 中的左陪集和右陪集.

a 称为代表元素.

注

- 群的每个子集不见得都是群. 子群的陪集是群论中的一个重要内容, 由这一概念可以引导出一个重要结果, 即拉格朗日定理. 它指出群与其子群之间存在的一个重要关系.
- 这里只就左陪集进行讨论, 右陪集也有类似的结论.

Theorem 72 (拉格朗日定理). 设 $\langle H, * \rangle$ 为 $\langle G, * \rangle$ 的子群, $a, b \in G$, 那么

(1) $R = \{\langle a, b \rangle \mid a \in G, b \in G \text{ 且 } a^{-1} * b \in H\}$ 是 G 中的一个等价关系. 对于 $a \in G$, 若记 $[a]_R = \{x \mid x \in G \text{ 且 } \langle a, x \rangle \in R\}$, 则

$$[a]_R = aH \quad (34)$$

(2) 如果 $\langle G, * \rangle$ 为有限群, $|G| = n$, $|H| = m$, 那么 $m|n$ (即 H 的阶整除 G 的阶).

证: ① 先证关系 R 是等价关系.

- 关系 R 是自反的:

对于任意 $a \in G$, 必有 $a^{-1} \in G$, 使

$$a^{-1} * a = e \in H.$$

所以 $\langle a, a \rangle \in R$.

$$R = \{\langle a, b \rangle \mid a \in G, b \in G \text{ 且 } a^{-1} * b \in H\}$$

- 关系 R 是对称的:

若 $\langle a, b \rangle \in R$. 则 $a^{-1} * b \in H$, 因为 H 是 G 的子群, 故

$$(a^{-1} * b)^{-1} = b^{-1} * a \in H$$

所以, $\langle b, a \rangle \in R$.

- 关系 R 是传递的:

若 $\langle a, b \rangle \in R$, $\langle b, c \rangle \in R$. 则 $a^{-1} * b \in H$, $b^{-1} * c \in H$, 所以

$$a^{-1} * b * b^{-1} * c = a^{-1} * c \in H$$

则 $\langle a, c \rangle \in R$.

对于 $a \in G$, 有 $b \in [a]_R \Leftrightarrow \langle a, b \rangle \in R \Leftrightarrow a^{-1} * b \in H \Leftrightarrow b \in aH$. 因此

$$[a]_R = aH.$$

拉格朗日定理

② 由于 R 是 G 中的一个等价关系, 所以必定将 G 划分成不同的等价类 $[a_1]_R, [a_2]_R, \dots, [a_k]_R$, 使得

$$G = \bigcup_{i=1}^k [a_i]_R = \bigcup_{i=1}^k a_i H \quad (a_i \in G)$$

若 $h_1, h_2 \in H$, 且 $h_1 \neq h_2$, $a \in G$, 那么 $a * h_1 \neq a * h_2$. 所以

$$|a_i H| = |H| = m, \quad i = 1, 2, \dots, k.$$

因此

$$n = |G| = \left| \bigcup_{i=1}^k a_i H \right| = \sum_{i=1}^k |a_i H| = k \cdot m.$$

所以 H 阶的整除 G 的阶, 即 $m|n$. □

4.72

拉格朗日定理的推论

推论 1

任何质数阶¹的群不可能有非平凡子群.

证: (反证法) 假设质数阶群 $\langle G, * \rangle$ 有非平凡子群 $\langle H, * \rangle$.

根据拉格朗日定理, 则 $|H|(1 < |H| < |G|)$ 是 $|G|$ 的因子, 与 $|G|$ 为质数矛盾. □

4.73

推论 2

设 $\langle G, * \rangle$ 为 n 阶有限群, e 是群 $\langle G, * \rangle$ 的幺元. 那么

- (1) 对于任意 $a \in G$, a 的阶² 必是 n 的因子, 且必有 $a^n = e$;
- (2) 如果 n 为质数, 则 $\langle G, * \rangle$ 必是循环群.

证: ① 若 $a \in G$, a 的阶数为 m , 则循环群 $\langle \{a, a^2, \dots, a^m\}, * \rangle$ 是 G 的子群.

根据拉格朗日定理, $m|n$. 令 $n = mk$, 则

$$a^n = a^{mk} = (a^m)^k = e^k = e.$$

② 令 $\langle G', * \rangle = \langle \{a, a^2, \dots, a^m\}, * \rangle$, 则 G' 是 G 的循环子群.

如前述, m 是 n 的一个因子, 已知 n 为质数, 故 $n = m$, 或 $m = 1$.

- 若 $n = m$, 则 $G = G'$. G' 是循环群, 所以 G 是循环群.
- 若 $m = 1$, 则 $a = e$, 而 a 是 G 中的任意一个元素, 所以 $G = \{e\}$, 是循环群. □

4.74

Example 73. 在 $X = \mathbb{R} - \{0, 1\}$ 定义 6 个函数:

$$\begin{aligned} f_1(x) &= x; & f_2(x) &= x^{-1}; & f_3(x) &= 1 - x; \\ f_4(x) &= (1 - x)^{-1}; & f_5(x) &= (x - 1)x^{-1}; & f_6(x) &= x(x - 1)^{-1}. \end{aligned}$$

则 $\langle F, \circ \rangle$ 是群, 这里 $F = \{f_1, f_2, f_3, f_4, f_5, f_6\}$, “ \circ ” 是函数的复合运算. 试求 $\langle F, \circ \rangle$ 的所有子群.

解: 先写出运算表.

¹质数, 即素数: 大于 1 而无真因数的自然数.

²元素 a 的阶, 是满足 $a^t = e$ 的最小正整数 t .

\circ	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_4	f_3	f_6	f_5
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_2	f_5	f_1	f_3
f_5	f_5	f_3	f_6	f_1	f_4	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

比如,

$$\begin{aligned} f_2(f_3(x)) &= (f_3(x))^{-1} \\ &= (1-x)^{-1} \\ &= f_4(x), \end{aligned}$$

所以 $f_2 \circ f_3 = f_4$. 再如,

$$\begin{aligned} f_3(f_2(x)) &= 1 - f_2(x) \\ &= 1 - x^{-1} \\ &= (x-1)x^{-1} \\ &= f_5(x), \end{aligned}$$

所以 $f_3 \circ f_2 = f_5$. 因 $|F| = 6$, $\langle F, \circ \rangle$ 的子群只能是 1, 2, 3, 6 阶群.

- 平凡子群: $\langle \{f_1\}, \circ \rangle, \langle F, \circ \rangle$.
- 2 阶子群: $\langle \{f_1, f_2\}, \circ \rangle, \langle \{f_1, f_3\}, \circ \rangle, \langle \{f_1, f_6\}, \circ \rangle$.
- 3 阶子群: $\langle \{f_1, f_4, f_5\}, \circ \rangle$.

注意这里

- f_1 是幺元;
- f_2, f_3, f_6 的阶为 2;
- f_4, f_5 的阶为 3.

□

4.75

Example 74. (续前例) 令 $H = \{f_1, f_4, f_5\}$, $\langle H, \circ \rangle$ 是 $\langle F, \circ \rangle$ 的子群. 求 $F = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ 中的各元素所确定的 H 在 F 中的所有左陪集.

$$\begin{aligned} f_1H &= \{f_1, f_4, f_5\}, & f_2H &= \{f_2, f_3, f_6\}, \\ f_3H &= \{f_2, f_3, f_6\} = f_2H, & f_4H &= \{f_1, f_4, f_5\} = f_1H, \\ f_5H &= \{f_1, f_4, f_5\} = f_1H, & f_6H &= \{f_2, f_3, f_6\} = f_2H. \end{aligned}$$

从此例看到,

- 由群 $\langle F, \circ \rangle$ 的子群 $\langle H, \circ \rangle$ 所确定的所有不同左陪集 $(\{f_1, f_4, f_5\}, \{f_2, f_3, f_6\})$ 中只有一个是子群;
- 任意两个左陪集要么相等, 要么相交为空.

□

4.76

8 同态与同构

Example 75. 设 α, β, γ 是带正电荷的粒子, δ, ε 是中性粒子, ζ 是带负电荷的粒子, 下表描述了这些粒子间相互作用的结果:

\otimes	α	β	γ	δ	ε	ζ
α	α	β	α	α	γ	δ
β	β	α	γ	β	γ	ε
γ	α	γ	α	β	γ	ε
δ	α	β	β	δ	ε	ζ
ε	γ	γ	γ	ε	ε	ζ
ζ	δ	ε	ε	ζ	ζ	ζ

令 $A = \{\alpha, \beta, \gamma, \delta, \varepsilon, \zeta\}$, 则 $\langle A, \otimes \rangle$ 是一个代数系统.

$*$	1	0	-1
1	1	1	0
0	1	0	-1
-1	0	-1	-1

如果只考虑带电粒子的正负特性, 则这些粒子相互作用的结果可用另一个系统 $\langle B, * \rangle$ ($B = \{1, 0, -1\}$) 概括地描述. 建立从 A 到 B 的映射 f ,

$$f(x) = \begin{cases} 1, & x \in \{\alpha, \beta, \gamma\}, \\ 0, & x \in \{\delta, \varepsilon\}, \\ -1, & x \in \{\zeta\}. \end{cases}$$

对任意 $a_1, a_2 \in A$, 有

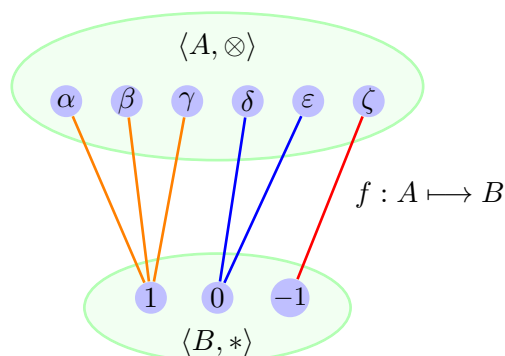
$$f(a_1 \otimes a_2) = f(a_1) * f(a_2)$$

例如, $f(\beta \otimes \zeta) = f(\varepsilon) = 0$, $f(\beta) * f(\zeta) = 1 * (-1) = 0$. 所以,

$$f(\beta \otimes \zeta) = f(\beta) * f(\zeta).$$

这时, 称 f 为代数系统 $\langle A, \otimes \rangle$ 到 $\langle B, * \rangle$ 的一个同态.

$$f(\alpha) = f(\beta) = f(\gamma) = 1, f(\delta) = f(\varepsilon) = 0, f(\zeta) = -1:$$



例如,

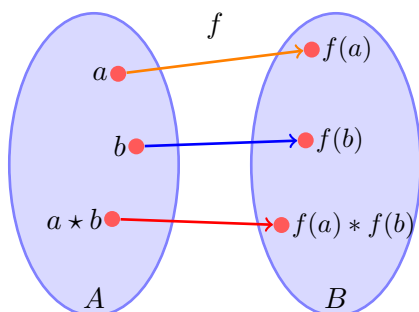
$$\beta \otimes \zeta = \varepsilon, \quad 1 * (-1) = 0;$$

$$f(\beta \otimes \zeta) = f(\varepsilon) = 0 = 1 * (-1) = f(\beta) * f(\zeta).$$

同态

Definition 76. 设 $\langle A, \star \rangle$ 和 $\langle B, * \rangle$ 是两个代数系统, \star 和 $*$ 分别是 A 和 B 上的二元运算. 如果存在映射 $f: A \rightarrow B$, 对任意 $a_1, a_2 \in A$, 有

$$f(a_1 \star a_2) = f(a_1) * f(a_2) \quad (35)$$



- (1) 称 f 是 $\langle A, \star \rangle$ 到 $\langle B, * \rangle$ 的一个同态映射 (homomorphism), 简称同态;
- (2) 称 $\langle A, \star \rangle$ 同态于 $\langle B, * \rangle$, 记作 $A \sim B$;
- (3) 称 $\langle f(A), * \rangle$ 为 $\langle A, \star \rangle$ 的一个同态象 (image under homomorphism). 其中

$$f(A) = \{x \mid x = f(a), a \in A\} \subseteq B. \quad (36)$$

4.79

同态

注

- 普通的映射讨论的是两个集合 A 和 B 的关系;
- 同态讨论的是与代数运算也发生关系的映射. 即两个代数系统之间的联系.
- 若 f 是 $\langle A, \star \rangle$ 到 $\langle B, * \rangle$ 的一个同态映射, 则任意 $a_1, a_2 \in A$, 只要

$$a_1 \rightarrow b_1, \quad a_2 \rightarrow b_2, \quad (37)$$

就有

$$a_1 \star a_2 \rightarrow b_1 * b_2. \quad (38)$$

4.80

Example 77. 记 $B = \{1, -1\}$. 对代数系统 $\langle \mathbb{Z}, + \rangle$ 和 $\langle B, \times \rangle$ (普通的加法和乘法),

(1) $f_1: \quad a \rightarrow 1, \quad (a \text{ 是 } \mathbb{Z} \text{ 的任一元})$

是一个 \mathbb{Z} 到 B 的同态映射. 因为任意 $a_1, a_2 \in \mathbb{Z}$, 有

$$a_1 \rightarrow 1, \quad a_2 \rightarrow 1,$$

$$a_1 + a_2 \rightarrow 1 = 1 \times 1.$$

(2) $f_2: \quad a \rightarrow +1, \quad (\text{若 } a \text{ 是偶数})$

$$a \rightarrow -1, \quad (\text{若 } a \text{ 是奇数})$$

则 f_2 是一个 \mathbb{Z} 到 B 的 (满射的) 同态映射. 例如, 若 a_1 奇, a_2 偶, 则

$$a_1 \rightarrow -1, \quad a_2 \rightarrow +1,$$

$$a_1 + a_2 \rightarrow -1 = (-1) \times (+1).$$

4.81

同态映射可能不惟一.

(a) $\langle A, \star \rangle$			(b) $\langle B, \oplus \rangle$			(c) $\langle C, \ast \rangle$		
\star	a	b	\oplus	偶	奇	\ast	0°	180°
a	a	b	偶	偶	奇	0°	0°	180°
b	b	a	奇	奇	偶	180°	180°	0°

同构

Definition 78. 设 f 是 $\langle A, \star \rangle$ 到 $\langle B, \ast \rangle$ 一个同态,

- (1) 如果 f 是 A 到 B 的满射, 则称 f 是 $\langle A, \star \rangle$ 到 $\langle B, \ast \rangle$ 满同态 (或同态满射).
- (2) 如果 f 是 A 到 B 的入射 (即单射), 则称 f 是 $\langle A, \star \rangle$ 到 $\langle B, \ast \rangle$ 单一同态.
- (3) 如果 f 是 A 到 B 的双射 (即一一映射), 则称 f 为同构映射, 并称 $\langle A, \star \rangle$ 与 $\langle B, \ast \rangle$ 同构 (isomorphism), 记作 $A \cong B$.

Example 79. 设 $A = \{1, 2, 3\}$, $\bar{A} = \{4, 5, 6\}$. A 与 \bar{A} 的代数运算 \star 与 \ast 分别为

\star	1	2	3	\ast	4	5	6
1	3	3	3	4	6	6	6
2	3	3	3	5	6	6	6
3	3	3	3	6	6	6	6

那么 $1 \rightarrow 4, 2 \rightarrow 5, 3 \rightarrow 6$

是一个 A 与 \bar{A} 间的同构映射. 因为

$$a \star b = 3 \rightarrow 6 = \bar{a} \ast \bar{b}.$$

$\Rightarrow A$ 同 \bar{A} 没有什么本质上的区别, 惟一的区别只是命名的不同而已.

Example 80. 代数系统 $\langle B, \oplus \rangle$, 和 $\langle C, \ast \rangle$ 都是与 $\langle A, \star \rangle$ 同构的:

研究同构的意义

假定对于代数运算 \circ 与 $\bar{\circ}$ 来说, A 与 \bar{A} 同构. 那么

- 对于代数运算 \circ 与 $\bar{\circ}$ 来说, A 与 \bar{A} 这两个集合, 抽象地来看, 没有什么区别 (只有命名上的不同).
- 若一个集合有一个只与这个集合的代数运算有关的性质, 那么另一个集合有一个完全相同的性质. (比如结合律, 交换律等.)

Example 81. 设 \mathbb{R} 是实数集, \mathbb{R}_+ 为正实数集合, 说明代数系统 $\langle \mathbb{R}_+, \cdot \rangle$ 与 $\langle \mathbb{R}, + \rangle$ 是同构的. ($+$, \cdot 是普通的加法, 乘法.)

解: 为说明 $\langle \mathbb{R}_+, \cdot \rangle$ 与 $\langle \mathbb{R}, + \rangle$ 是同构的, 必须建立 \mathbb{R}_+ 到 \mathbb{R} 的双射 f , 并且对任意 $x_1, x_2 \in \mathbb{R}_+$, 有

$$f(x_1 \cdot x_2) = f(x_1) + f(x_2). \quad (39)$$

可令 $f: \mathbb{R}_+ \rightarrow \mathbb{R}$, $f(x) = \ln x$, 则 f 是 \mathbb{R}_+ 到 \mathbb{R} 的双射, 且

$$\begin{aligned} f(x_1 \cdot x_2) &= \ln(x_1 \cdot x_2) \\ &= \ln x_1 + \ln x_2 \\ &= f(x_1) + f(x_2). \end{aligned}$$

所以, 代数系统 $\langle \mathbb{R}_+, \cdot \rangle$ 与 $\langle \mathbb{R}, + \rangle$ 是同构的. \square

先算后映 = 先映后算

自同态 & 自同构

Definition 82. 设 $\langle A, * \rangle$ 是代数系统,

- (1) 如果 f 是 $\langle A, * \rangle$ 到 $\langle A, * \rangle$ 的一个同态, 则称 f 为自同态.
- (2) 如果 g 是 $\langle A, * \rangle$ 到 $\langle A, * \rangle$ 的一个同构, 则称 g 为自同构.

4.86

Example 83. 设 $A = \{1, 2, 3\}$, 代数运算 $*$ 由下表给定.

$*$	1	2	3
1	3	3	3
2	3	3	3
3	3	3	3

那么

$$f: 1 \rightarrow 2, 2 \rightarrow 1, 3 \rightarrow 3 \quad (40)$$

是一个对于 $*$ 来说的 A 的自同构.

4.87

Theorem 84. 设 G 是代数系统的集合, 则 G 中代数系统间的同构关系是等价关系.

证: ① 设任意 $\langle A, * \rangle \in G$, 令 $f: A \mapsto A, f(a) = a, a \in A$. 从而

$$\langle A, * \rangle \cong \langle A, * \rangle.$$

即同构关系是自反的.

② 设 $\langle A, * \rangle \cong \langle B, * \rangle$, 那么存在双射 $f: A \mapsto B$, 故 $f^{-1}: B \mapsto A$ 也是双射, 所以

$$\langle B, * \rangle \cong \langle A, * \rangle.$$

因而该关系是对称的.

③ 设 $\langle A, * \rangle \cong \langle B, * \rangle, \langle B, * \rangle \cong \langle C, \oplus \rangle$, 则存在双射 $f: A \mapsto B$ 和 $g: B \mapsto C$, 那么 $g \circ f: A \mapsto C$ 也是双射, 所以

$$\langle A, * \rangle \cong \langle C, \oplus \rangle.$$

因而该关系是传递的.

因此, 同构关系是等价关系. □

4.88

Theorem 85. 设 f 是代数系统 $\langle A, * \rangle$ 到 $\langle B, * \rangle$ 的同态映射, 如果 $\langle A, * \rangle$ 是半群 (独异点, 群), 则同态象 $\langle f(A), * \rangle$ 也是半群 (独异点, 群).

证: 以群为例进行证明.

① $*$ 运算在 $f(A)$ 上封闭.

因 f 是同态, 所以 $f(A) \subseteq B$. 对任意 $b_1, b_2 \in f(A)$, 有 $a_1, a_2 \in A$, 使得 $f(a_1) = b_1, f(a_2) = b_2$, 那么

$$b_1 * b_2 = f(a_1) * f(a_2) = f(a_1 * a_2) \in f(A),$$

② $*$ 运算在 $f(A)$ 上可结合.

对任意 $b_1, b_2, b_3 \in f(A)$, 有 $a_1, a_2, a_3 \in A$, 使得 $f(a_1) = b_1, f(a_2) = b_2, f(a_3) = b_3$, 那么

$$\begin{aligned} b_1 * (b_2 * b_3) &= f(a_1) * (f(a_2) * f(a_3)) \\ &= f(a_1) * f(a_2 * a_3) \\ &= f(a_1 * (a_2 * a_3)) \\ &= f((a_1 * a_2) * a_3) \\ &= f(a_1 * a_2) * f(a_3) \\ &= (f(a_1) * f(a_2)) * f(a_3) \\ &= (b_1 * b_2) * b_3. \end{aligned}$$

③ 存在幺元.

设 e 是 $\langle A, \star \rangle$ 的幺元, 对任意 $b \in f(A)$, 有 $a \in A$, 使得 $f(a) = b$, 那么

$$b * f(e) = f(a) * f(e) = f(a * e) = f(a) = b.$$

同时,

$$b * f(e) = f(a * e) = f(e * a) = f(e) * f(a) = f(e) * b.$$

所以, $f(e)$ 是 $\langle f(A), * \rangle$ 的幺元.

④ 任意元素有逆元.

对任意 $b \in f(A)$, 有 $a \in A$, 使得 $f(a) = b$, 因 $\langle A, \star \rangle$ 是群, 则 a 有逆元 a^{-1} , 且 $f(a^{-1}) \in f(A)$, 那么

$$\begin{aligned} f(a) * f(a^{-1}) &= f(a * a^{-1}) = f(e) \\ f(e) &= f(a^{-1} * a) = f(a^{-1}) * f(a). \end{aligned}$$

因 $f(e)$ 是 $\langle f(A), * \rangle$ 的幺元, 所以 $f(a^{-1})$ 是 $f(a)$ 的逆元.

所以任意 $b = f(a) \in f(A)$ 有逆元, 即 $f(a)^{-1} = f(a^{-1})$.

由上述, $\langle f(A), * \rangle$ 是群. □

4.89

注

从前述的证明中, 我们可以看到:

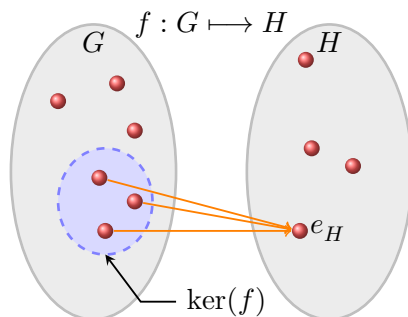
- 若 e 是 A 的幺元, 则 $f(e)$ 是 $f(A)$ 的幺元; (A 是独异点, 或群.)
- 若 x^{-1} 是 x 的逆元, 则 $f(x^{-1})$ 是 $f(x)$ 的逆元. (A 是群.)

4.90

Definition 86. 设 f 是群 $\langle G, \star \rangle$ 到群 $\langle H, * \rangle$ 的一个同态映射, e_H 是 $\langle H, * \rangle$ 的幺元, 令

$$\ker(f) = \{x \mid x \in G \text{ 且 } f(x) = e_H\}$$

称 $\ker(f)$ 是同态映射 f 的核, 简称同态核 (kernel of homomorphism).



Theorem 87. 设 f 是群 $\langle G, \star \rangle$ 到群 $\langle H, \star \rangle$ 的一个同态映射, 则 f 的同态核 K 是 G 的子群. (即 $\langle K, \star \rangle$ 是 $\langle G, \star \rangle$ 的子群)

证: ① 对任意 $k_1, k_2 \in K$, 有

$$f(k_1 \star k_2) = f(k_1) \star f(k_2) = e_H \star e_H = e_H. \quad (41)$$

所以 $k_1 \star k_2 \in K$, 所以 \star 运算在 K 上封闭.

② 进而可知 \star 运算在 K 上可结合.

③ 又因 f 是群 $\langle G, \star \rangle$ 到群 $\langle H, \star \rangle$ 的同态映射, 根据前述定理,

$$e_H = f(e). \quad (42)$$

这说明 $e \in K$, e 也是 K 的幺元.

④ 对任意 $k \in K$, $f(k) = e_H$.

$$f(k^{-1}) = (f(k))^{-1} = (e_H)^{-1} = e_H. \quad (43)$$

所以 $k^{-1} \in K$, 即 K 中任意元素有逆元. 从而 K 是 G 的子群.

4.92

同余关系 & 同余类

Definition 88. 设 $\langle A, \star \rangle$ 是一个代数系统, R 是 A 上的等价关系. 如果 $\langle a_1, a_2 \rangle, \langle b_1, b_2 \rangle \in R$ 时, 有

$$\langle a_1 \star b_1, a_2 \star b_2 \rangle \in R, \quad (44)$$

则称 R 为 A 上关于运算 \star 的同余关系.

由该同余关系将 A 划分成的等价类叫做同余类.

4.93

Example 89. 给定代数系统 $\langle \mathbb{Z}, + \rangle$ 和 \mathbb{Z} 上的模 k 等价关系 R , 证明 R 是 \mathbb{Z} 上关于运算 $+$ 的同余关系.

证: 设 $\langle a, b \rangle, \langle c, d \rangle \in R$, 那么可令:

$$a - b = kn_1, \quad c - d = kn_2, \quad n_1, n_2 \in \mathbb{Z}, \quad (45)$$

所以,

$$(a - b) + (c - d) = k(n_1 + n_2), \quad n_1 + n_2 \in \mathbb{Z}$$

$$\Leftrightarrow (a + c) - (b + d) = k(n_1 + n_2)$$

$$\Leftrightarrow \langle a + c, b + d \rangle \in R.$$

按定义, R 是 \mathbb{Z} 上关于运算 $+$ 的同余关系. □

4.94

Example 90. 给定代数系统 $\langle A, \star \rangle$, $A = \{a, b, c, d\}$, 运算 \star 定义如下表, 给定 A 上的等价关系 $R = \{\langle a, a \rangle, \langle b, b \rangle, \langle c, c \rangle, \langle d, d \rangle, \langle a, b \rangle, \langle b, a \rangle, \langle c, d \rangle, \langle d, c \rangle\}$, 分析 R 是否为 A 上关于运算 \star 的同余关系.

\star	a	b	c	d
a	a	a	d	c
b	b	a	d	a
c	c	b	a	b
d	c	d	b	a

证: $\langle a, b \rangle, \langle c, d \rangle \in R$, 但

$$\langle a \star c, b \star d \rangle = \langle d, a \rangle \notin R,$$

按定义, R 不是同余关系. □

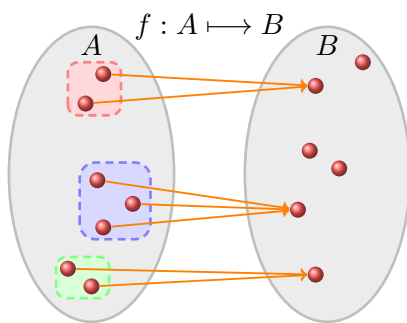


Figure 1: 同余关系 —— 特殊的等价关系

- 从同余关系的定义可知, 同余关系首先是等价关系.
- 同余关系与代数系统上的运算有关, 所以等价关系不一定是同余关系.

Theorem 91. 设 $\langle A, \star \rangle$ 是一个代数系统, R 是 A 上的同余关系. $B = \{A_1, A_2, \dots, A_r\}$ 是由 R 诱导的 A 的一个划分, 那么必存在新的代数系统 $\langle B, \ast \rangle$, 它是 $\langle A, \star \rangle$ 的同态象.

本定理证明线索:

- (1) 在 B 上建立运算 \ast ;
- (2) 证 $\langle A, \star \rangle$ 与 $\langle B, \ast \rangle$ 满同态, 即要构造一个满射 $f: A \rightarrow B$, 使

$$f(x \star y) = f(x) \ast f(y).$$

证: 在 B 上定义二元运算 \ast : 对任意 $A_i, A_j \in B$, 任取 $a_1 \in A_i, a_2 \in A_j$, 如果 $a_1 \star a_2 \in A_k$, 则定义 $A_i \ast A_j = A_k$.

因 R 是 A 上的同余关系, 所以上述定义的 $A_i \ast A_j = A_k$ 是惟一的.

其次, 作映射 $f: A \rightarrow B, f(a) = A_i, a \in A_i$. 显然 f 是满射.

对任意 $x, y \in A$, 则 x, y 应属于某一分块, 可设 $x \in A_i, y \in A_j$, 这里 $1 < i, j < r$; 同时, $x \star y$ 必属于 B 中的某个同余类, 不妨设 $x \star y \in A_k$. 于是

$$f(x \star y) = A_k = A_i \ast A_j = f(x) \ast f(y).$$

因此, f 是由 $\langle A, \star \rangle$ 到 $\langle B, \ast \rangle$ 的满同态, 即 $\langle B, \ast \rangle$ 是 $\langle A, \star \rangle$ 的同态象. □

4.96

Theorem 92. 设 f 是 $\langle A, \star \rangle$ 到 $\langle B, \ast \rangle$ 的同态映射, 定义 A 上的二元关系 R :

$$\langle a, b \rangle \in R \text{ 当且仅当 } f(a) = f(b).$$

则 R 是 A 上的同余关系.

证: 先证 R 是 A 上的等价关系:

- 对任意 $a \in A$, 因 $f(a) = f(a)$, 所以 $\langle a, a \rangle \in R$;
- 若 $\langle a, b \rangle \in R$, 则 $f(a) = f(b)$, 亦有 $f(b) = f(a)$, 所以 $\langle b, a \rangle \in R$;
- 若 $\langle a, b \rangle \in R, \langle b, c \rangle \in R$, 则 $f(a) = f(b), f(b) = f(c)$, 于是 $f(a) = f(c)$, 所以 $\langle a, c \rangle \in R$.

其次, 若 $\langle a, b \rangle \in R, \langle c, d \rangle \in R$, 则

$$f(a \star c) = f(a) \ast f(c) = f(b) \ast f(d) = f(b \star d).$$

所以, $\langle a \star c, b \star d \rangle \in R$. 故 R 是 A 上的同余关系. □

4.97

9 环与域

环与域

本节讨论具有两个运算的代数系统 $\langle A, \oplus, * \rangle$. 它可视为 $\langle A, \oplus \rangle$ 和 $\langle A, * \rangle$ 组合而成的代数系统. 我们把第一个运算 \oplus 称为“加法”; 把第二个运算 $*$ 称为“乘法”.

例如实数集上具有加和乘运算的代数系统 $\langle \mathbb{R}, +, \cdot \rangle$.

环

Definition 93. 设 $\langle A, \oplus, * \rangle$ 是代数系统, 如果

- (1) $\langle A, \oplus \rangle$ 是阿贝尔群;
- (2) $\langle A, * \rangle$ 是半群.
- (3) 运算 $*$ 对 \oplus 是可分配的. 即对任意 $a, b, c \in A$, 有

$$a * (b \oplus c) = (a * b) \oplus (a * c), \quad (46)$$

$$(b \oplus c) * a = (b * a) \oplus (c * a). \quad (47)$$

则称 $\langle A, \oplus, * \rangle$ 是环 (ring).

注

- 为了方便, 常称环 $\langle A, \oplus, * \rangle$ 的第一个运算 \oplus 为“加法”, 并记为 $+$;
- 用 θ 表示加法幺元, 用 $-a$ 表示 a 的加法逆元, 将 $a + (-b)$ 记为 $a - b$;
- 称第二个运算 $*$ 为“乘法”, 并记为 \circ .

Theorem 94. 设 $\langle A, +, \circ \rangle$ 是环, 用 θ 表示加法幺元, 用 $-a$ 表示 a 的加法逆元, 将 $a + (-b)$ 记为 $a - b$. 则对任意 $a, b, c \in A$, 有

(1) $a \circ \theta = \theta \circ a = \theta$, (加法幺元是乘法零元)

(2) $a \circ (-b) = (-a) \circ b = -(a \circ b)$,

(3) $(-a) \circ (-b) = a \circ b$,

(4) $a \circ (b - c) = a \circ b - a \circ c$,

(5) $(b - c) \circ a = b \circ a - c \circ a$.

(以下依次来证明...)

①
$$a \circ \theta = \theta \circ a = \theta.$$

证: 因为 θ 是加法幺元, $\forall x \in A$, 有 $\theta + x = x$. 所以

$$\begin{aligned} a \circ \theta &= a \circ (\theta + \theta), & (\theta \text{ 是加法幺元}) \\ &= a \circ \theta + a \circ \theta. & (\text{分配律}) \end{aligned}$$

上式等价于

$$a \circ \theta + \theta = a \circ \theta + a \circ \theta.$$

由消去律, 得

$$\theta = a \circ \theta.$$

同理可证 $\theta \circ a = \theta$.

$$\textcircled{2} \quad a \circ (-b) = (-a) \circ b = -(a \circ b).$$

证: $a \circ (-b) = -(a \circ b)$ 可理解为 $a \circ b$ 的加法逆元是 $a \circ (-b)$. 证明如下:

$$\begin{aligned} a \circ b + a \circ (-b) &= a \circ (b + (-b)) && \text{(分配律)} \\ &= a \circ \theta \\ &= \theta. && \text{(结论 ①)} \end{aligned}$$

所以

$$a \circ (-b) = -(a \circ b).$$

同理可证 $a \circ (-b) = -(a \circ b)$.

4.103

$$\textcircled{3} \quad (-a) \circ (-b) = a \circ b$$

证: 由结论 $\textcircled{2}$, 及: $(a^{-1})^{-1} = a$, 得

$$\begin{aligned} (-a) \circ (-b) &= -(a \circ (-b)) && \text{(结论 ②)} \\ &= -(- (a \circ b)) && \text{(结论 ②)} \\ &= a \circ b. && ((a^{-1})^{-1} = a) \end{aligned}$$

4.104

$$\textcircled{4} \quad a \circ (b - c) = a \circ b - a \circ c.$$

证:

$$\begin{aligned} a \circ (b - c) &= a \circ (b + (-c)) \\ &= a \circ b + a \circ (-c) && \text{(分配律)} \\ &= a \circ b + (- (a \circ c)) && \text{(结论 ②)} \\ &= a \circ b - a \circ c. \end{aligned}$$

结论 $\textcircled{5}$ 同理. □

4.105

交换环 & 含幺环

Definition 95. 设 $\langle A, +, \circ \rangle$ 是环,

(1) 如果 $\langle A, \circ \rangle$ 是可交换的, 则称 $\langle A, +, \circ \rangle$ 是交换环 (commutative ring).

(2) 如果 $\langle A, \circ \rangle$ 含有幺元, 则称 $\langle A, +, \circ \rangle$ 是含幺环 (ring with unity).

注

- 以上定义针对的是乘法 \circ ;
- 对含幺环, $\langle A, \circ \rangle$ 是独异点;
- 一般, 一个环未必有一个乘法幺元. 例如 $\mathbb{Z}_E = \{\text{所有偶数}\}$, 对普通加法和乘法构成一个环, 但是没有乘法幺元.

4.106

零因子

Definition 96. 设 $\langle A, +, \circ \rangle$ 是环, 如果存在 $a, b \in A$, 且 $a \neq \theta, b \neq \theta$, 使得 $a \circ b = \theta$, 则称 $\langle A, +, \circ \rangle$ 是含零因子环. a 和 b 称为零因子.

注

- 零因子: “两个非零的数相乘等于零”;
- 强调这个概念, 是因为

$$a \circ b = 0 \Rightarrow a = 0 \text{ 或 } b = 0 \quad (48)$$

这一条普通的计算规则, 在一般的环里并不一定成立;

- 一个环当然可以没有零因子, 比如整数环;
- 显然, 在而且只在一个没有零因子的环里, (48) 式才会成立.

4.107

Theorem 97. 一个环 $\langle A, +, \circ \rangle$ 没有零因子, 当且仅当乘法满足消去律, 即

$$c \neq \theta, c \circ a = c \circ b \Rightarrow a = b.$$

$$c \neq \theta, a \circ c = b \circ c \Rightarrow a = b.$$

证: 设 $c \circ a = c \circ b$ 且 $c \neq \theta$, 则

$$\begin{aligned} c \circ (a - b) &= c \circ a - c \circ b = c \circ a + (-c \circ b) \\ &= c \circ a + (-c \circ a) \\ &= \theta. \end{aligned}$$

若环 $\langle A, +, \circ \rangle$ 无零因子, 由上式及 $c \neq \theta$, 得

$$a - b = \theta,$$

两边加 b , 得 $a = b$. 另一式类似可证. 即证消去律成立.

反之, 设 $a \neq \theta, a \circ b = \theta$, 因 $a \circ \theta = \theta$, 得

$$a \circ b = a \circ \theta,$$

若消去律成立, 得 $b = \theta$. 这说明 $\langle A, +, \circ \rangle$ 无零因子. □

4.108

零因子

Example 98. 一个数域 F 上的一切 $n \times n$ 矩阵对于矩阵的加法和乘法来说, 构成一个环. 这个环有幺元, 即单位矩阵. 当 $n \geq 2$ 时, 这个环是非交换环, 有零因子 (或者说, 不满足消去律).

以上我们认识了一个环可能满足的三种附加条件: (1) 乘法满足交换律, (2) 存在幺元, (3) 零因子不存在 (满足消去律). 一个环当然可以满足其中的一个或多个附加条件. 同时满足以上三个条件的环, 称为整环.

4.109

整环

Definition 99. 设 $\langle A, +, \circ \rangle$ 是环, 如果

- (1) $\langle A, \circ \rangle$ 是可交换的;
- (2) $\langle A, \circ \rangle$ 含有幺元;
- (3) $\langle A, \circ \rangle$ 无零因子 (或满足消去律):

$$a \circ b = \theta \Rightarrow a = \theta \text{ 或 } b = \theta. \quad (49)$$

则称 $\langle A, +, \circ \rangle$ 是整环.



环 + 乘法幺元 + 乘法可交换 + 乘法消去律 = 整环

4.110

整环

Example 100. 整数环 $\langle \mathbb{Z}, +, \cdot \rangle$ 是整环, 因 $\langle \mathbb{Z}, \cdot \rangle$ 可交换, 有幺元 1, 且无零因子 (即不可能有两个非零的数相乘等于零).

4.111

域

上面我们提到了三个附加条件:

- (1) 乘法满足交换律,
- (2) 存在幺元,
- (3) 零因子不存在 (满足消去律).

还有一个附加条件没有提到, 即逆元的存在性.

注意到零元 θ 是没有逆元的, 即不存在元素 a 使得 $\theta \circ a = a \circ \theta = e$. 我们看这个新的附加条件:

- (4) 每一个不等于零元的元有一个逆元.

4.112

域

注意附加条件 (4) 成立必有附加条件 (3) 成立, 即, 若环中每一个不等于零元的元有一个逆元, 则零因子不存在 (满足消去律). 因为

$$a \neq \theta, a \circ b = \theta \Rightarrow a^{-1} \circ a \circ b = b = \theta.$$

一个环如果满足附加条件 (1), (2), (4), 则称为域.

4.113

域

Definition 101. 设 $\langle A, +, \circ \rangle$ 是代数系统, 如果

- (1) $\langle A, + \rangle$ 是阿贝尔群;
- (2) $\langle A - \{\theta\}, \circ \rangle$ 是阿贝尔群;
- (3) 运算 \circ 对 $+$ 是可分配的,

则称 $\langle A, +, \circ \rangle$ 是域 (field).

Example 102. • $\langle \mathbb{R}, +, \circ \rangle, \langle \mathbb{Q}, +, \circ \rangle, \langle \mathbb{C}, +, \circ \rangle$ 都是域.

- 但 $\langle \mathbb{Z}, +, \circ \rangle$ 是整环而不是域,
因 $\langle \mathbb{Z} - \{0\}, \circ \rangle$ 不是群: 整数除 ± 1 之外, 均无乘法逆元.
- 此例说明整环不一定是域.

4.114

域 V.S. 整环

两者的定义区别在于

整环	$\langle A, \circ \rangle$ 是可交换含幺半群, 且无零因子;
域	$\langle A - \{\theta\}, \circ \rangle$ 是阿贝尔群.

事实上, 域的概念是在整环中增加了“除了零元外, 每个元都有逆元”这个条件.

Theorem 103. 域一定是整环.

4.115

Theorem 104. 有限整环一定是域.

证: 设 $\langle A, +, \circ \rangle$ 是有限整环, 则 $\langle A, \circ \rangle$ 是可交换的含么半群, 要证 $\langle A, +, \circ \rangle$ 是域, 只须证任意非零元 c , 都有乘法逆元.

事实上, 若 $a, b \in A$, 且 $a \neq b$, 则 $a \circ c \neq b \circ c$ (否则, 因 $\langle A, \circ \rangle$ 无零因子, 由消去律而导致 $a = b$).

又因运算 \circ 封闭, 从而有 $A \circ c = A$.

用 e 表示乘法么元. 由 $A \circ c = A$, 则存在 $d \in A$, 使得 $d \circ c = e$.

故 d 是 c 的乘法逆元, 这说明 $\langle A - \{\theta\}, \circ \rangle$ 是阿贝尔群. \square

4.116

同态映射

可以将同态概念推广到具有两个运算的代数系统.

Definition 105. 设 $\langle A, +, \circ \rangle$ 和 $\langle B, \oplus, \odot \rangle$ 是两个代数系统, 对任意 $a, b \in A$, 如果映射 $f: A \rightarrow B$ 满足

$$(1) f(a + b) = f(a) \oplus f(b),$$

$$(2) f(a \circ b) = f(a) \odot f(b),$$

则称 f 是 $\langle A, +, \circ \rangle$ 到 $\langle B, \oplus, \odot \rangle$ 的一个同态映射.

称 $\langle f(A), \oplus, \odot \rangle$ 是 $\langle A, +, \circ \rangle$ 的同态象.

4.117

Example 106. 设 $\langle \mathbb{N}, +, \cdot \rangle$ 是一个代数系统, \mathbb{N} 是自然数集, $+$ 和 \cdot 是普通的加法和乘法运算, 并设代数系统 $\langle \{\text{偶}, \text{奇}\}, \oplus, \odot \rangle$, 其运算表如下:

\oplus	偶	奇
偶	偶	奇
奇	奇	偶

\odot	偶	奇
偶	偶	偶
奇	偶	奇

容易验证映射

$$f(n) = \begin{cases} \text{偶}, & \text{若 } n = 2k, k = 0, 1, 2, \dots \\ \text{奇}, & \text{若 } n = 2k + 1, k = 0, 1, 2, \dots \end{cases}$$

是由 $\langle \mathbb{N}, +, \cdot \rangle$ 到 $\langle \{\text{偶}, \text{奇}\}, \oplus, \odot \rangle$ 的同态映射.

4.118

Theorem 107. 任一环的同态象是一个环.

证: 设 $\langle A, +, \circ \rangle$ 是一个环, 且 $\langle B, \oplus, \odot \rangle$ 是关于同态映射 f 的同态象.

由 $\langle A, +, \circ \rangle$ 是阿贝尔群, 则同态象 $\langle B, \oplus \rangle$ 是群; 容易验证 \oplus 也满足交换律, 所以 $\langle B, \oplus \rangle$ 是阿贝尔群.

由 $\langle A, \circ \rangle$ 是半群, 则同态象 $\langle B, \odot \rangle$ 也是半群.

证: 对于任意的 $b_1, b_2, b_3 \in B$, 必有相应的 a_1, a_2, a_3 , 使得

$$f(a_i) = b_i, \quad (i = 1, 2, 3)$$

于是

$$\begin{aligned}
b_1 \odot (b_2 \oplus b_3) &= f(a_1) \odot (f(a_2) \oplus f(a_3)) \\
&= f(a_1) \odot f(a_2 + a_3) \\
&= f(a_1 \cdot (a_2 + a_3)) \\
&= f((a_1 \cdot a_2) + (a_1 \cdot a_3)) \\
&= f(a_1 \cdot a_2) \oplus f(a_1 \cdot a_3) \\
&= (f(a_1) \odot f(a_2)) \oplus (f(a_1) \odot f(a_3)) \\
&= (b_1 \odot b_2) \oplus (b_1 \odot b_3).
\end{aligned}$$

同理可证 $(b_2 \oplus b_3) \odot b_1 = (b_1 \odot b_2) \oplus (b_1 \odot b_3)$.

因此, $\langle B, \oplus, \odot \rangle$ 是一个环. □

练习

已知一个环 $\langle \{a, b, c, d\}, +, \cdot \rangle$, 它的运算由下表给出:

+	a	b	c	d	·	a	b	c	d
a	aa	b	c	d	a	a	a	a	a
b	b	c	d	aa	b	a	c	a	c
c	c	d	aa	b	c	a	a	a	a
d	d	aa	b	c	d	a	c	a	c

它是一个交换环吗? 它有乘法幺元吗? 这个环中的零元是什么? 并求出每个元素的加法逆元.

解:

- (1) 因为 \cdot 的运算表是对称的, 所以环 $\langle \{a, b, c, d\}, +, \cdot \rangle$ 是交换环;
- (2) 没有乘法幺元;
- (3) 环中的零元是 a ;
- (4) 由 $+$ 运算表可见: a 和 c 以自身为加法逆元; b 和 d 互为加法逆元. □

阿贝尔 & 世界知名数学大奖

阿贝尔 —— 天才与贫困



阿贝尔 (Niels Henrik Abel, 1802–1829), 挪威数学家.

1821 年入 Christiania 大学 (今挪威 Oslo 大学).

1824 年, 他解决了用根式求解五次方程的不可能性问题, 由此引入可交换群 (也称阿贝尔群) 的概念.

为了能有更多的读者, 他的论文以法文写成 (也送给了 C. F. 高斯), 但是在外国数学家中没有引起反响.

阿贝尔 —— 天才与贫困



1825 年, 他去柏林, 结识了 A. L. 克雷尔 (August Leopold Crelle, 1780–1856), 并成为好友.

1826 年, 他鼓励克雷尔创办了数学刊物《纯数学与应用数学杂志》, 这个杂志是世界上第一个专门从事数学研究的定期刊物. 该杂志的前三卷刊登了阿贝尔 22 篇论文, 使欧洲数学家开始注意他的工作.

1826 年阿贝尔到巴黎, 遇见了 A. M. 勒让德和 A. L. 柯西等著名数学家. 他写了一篇关于椭圆积分的论文, 提交给法国科学院, 不幸未得到重视, 他只好又回到柏林.

克雷尔为他谋求教授职位, 没有成功. 1827 年阿贝尔贫病交迫地回到了挪威, 靠做家庭教师维生.

1829 年 4 月 6 日, 阿贝尔因肺结核去世, 在世二十六年零八个月.

4.122

阿贝尔 —— 天才与贫困

阿贝尔去世后两天, 克雷尔来信说, 阿贝尔将被任命为柏林大学的数学教授.

他与 Évariste Galois (1811–1832) 的英才早逝, 是数学史上的悲剧. 此后荣誉和褒奖接踵而至.



阿贝尔在数学方面的成就是多方面的. 和雅可比同时奠定了椭圆函数论的基础, 得出了阿贝尔定理. 还有阿贝尔积分, 阿贝尔函数以及关于

正项级数收敛的阿贝尔判别法等研究成果.

4.123

阿贝尔奖 The Abel Prize³

挪威政府捐出二亿挪威克朗 (约三千二百万美元) 的基金, 于 2002 年 (阿贝尔诞辰 200 周年) 设立了“阿贝尔奖”.

该奖每年颁发一次, 奖金为 600 万挪威克朗 (约 95 万美元). 这是一个专门针对数学专业的奖项, 是目前国际上专业数学奖中奖金金额最大的奖项之一.

- 2003: **Jean-Pierre Serre**,⁴ Collège de France.
- 2004: **Sir Michael Francis Atiyah**, University of Edinburgh; **Isadore M. Singer**, Massachusetts Institute of Technology.
- 2005: **Peter D. Lax**, Courant Institute of Mathematical Sciences, New York University.

³阿贝尔奖官方网址: <http://www.abelprisen.no/en/>.

⁴Jean-Pierre Serre, 1926 年生于法国, 1954 年获菲尔兹奖, 2000 年获沃尔夫奖.

- 2006: **Lennart Carleson**,⁵ Royal Institute of Technology, Sweden.
- 2007: **Srinivasa S. R. Varadhan**, Courant Institute of Mathematical Sciences, New York University.

世界知名数学大奖

奖项	首颁时间	颁发频度	所在国家或组织	奖金额
菲尔兹奖	1932 年	4 年	IMU	15000 加元
沃尔夫奖	1978 年	1 年	以色列	10 万美元
克拉福德奖 ⁶	1982 年	1 年	瑞典	50 万美元
阿贝尔奖	2003 年	1 年	挪威	600 万挪威克朗
邵逸夫奖	2004 年	1 年	中国	100 万美元

菲尔兹 Fields Prize⁷

1924 年, 在多伦多举行的国际数学家大会 (International Congress of Mathematicians, ICM) 上, 提议创设一项数学奖, 这次会议余下的钱用来建立这个奖的基金.

菲尔兹奖在每 4 年一届的 ICM 上颁发, 奖品包含一枚金质奖章和 15,000 加元 (约 13,000 美元⁸). 奖项的名称是纪念 J. C. Fields 教授, 他是位加拿大数学家, 曾任 1924 年数学家大会秘书长.

菲尔兹奖有一项特别的规定: 获奖者年龄必须不超过 40 岁.

华裔菲尔兹奖得主:

- 1982: Shing-Tung Yau (丘成桐).
- 2006: Terence Tao (陶哲轩).

沃尔夫奖 The Wolf Prizes⁹

沃尔夫奖是世界上具有较高学术声望的多学科国际奖.

1976 年由以色列议会设立, 1978 年首次颁奖. 沃尔夫科学基金会是在 Ricardo Wolf 及其夫人 Francisca Subirana Wolf 的倡导下设立的, 基金来自 Ricardo Wolf 及其家族一千万美元的捐赠.

沃尔夫基金会设有: 数学、物理、化学、医学、农业五个奖 (1981 年增设艺术奖). 通常每年颁发一次, 每个奖的奖金数额为 10 万美元.

华裔沃尔夫奖得主:

- 1978, 物理: 吴健雄 (1912–1997, 生于江苏, 哥伦比亚大学教授.)
- 1983, 数学: 陈省身 (1911–2004, 生于浙江, 加州大学伯克利分校教授.)

⁵Lennart Carleson, 1992 年获沃尔夫奖. 1978–1982 年 IMU 主席.

⁶克拉福德奖主要分三个部分: Astronomy and Mathematics, Geosciences, Biosciences. 依次每年颁发其中之一, 所以, 事实上数学奖要约 6 年颁发一次.

⁷菲尔兹奖官方网址: <http://www.mathunion.org/Prizes/Fields/index.html>.

⁸美元兑加拿大元的比价约为 1 : 1.13 (2006/11/29).

⁹沃尔夫奖官方网址: <http://www.wolfund.org.il/wolfpriz.html>.

- 1991, 农业: 杨祥发 (1932 年生于台湾, 加州大学戴维斯分校教授.)
- 2004, 农业: 袁隆平 (1930 年生于北京, 中国工程院院士.)
- 2004, 医学: 钱永健 (1952 年生于纽约, 加州大学圣地亚哥分校教授.)

克拉福德奖 The Crafoord Prize

The Crafoord Prize in astronomy and mathematics, biosciences, geosciences or polyarthritis research is awarded by the Royal Swedish Academy of Sciences annually according to a rotating scheme. The prize sum of USD 500,000 makes the Crafoord one of the world's largest scientific prizes.

Anna-Greta and Holger Crafoord's Fund was established in 1980 and the first prize was awarded in 1982. The prize is intended to promote international basic research in the disciplines:

- Astronomy and Mathematics,
- Geosciences,
- Biosciences, with particular emphasis on ecology and
- Polyarthritis (rheumatoid arthritis).

克拉福德奖 The Crafoord Prize

These disciplines are chosen so as to complement those for which the Nobel Prizes are awarded. The recipients are worthy scientists who receive the prize in accordance with a set scheme:

- Year 1 Astronomy and Mathematics
- Year 2 Geosciences
- Year 3 Biosciences
- Year 4 Astronomy and Mathematics

The prize in polyarthritis is awarded only when a special committee has shown that scientific progress in this field has been such that an award is justified.

The laureates are announced in mid-January each year, and the prize is presented in April on "Crafoord Day". It is received from the hand of His Majesty the King of Sweden.

克拉福德奖 The Crafoord Prize¹⁰

数学奖得奖者:

- 1982: Vladimir, Igorevich Arnold, Louis Nirenberg.
- 1988: Pierre Deligne, Alexander Grothendieck.
- 1994: Simon Donaldson, Shing-Tung Yau (丘成桐).
- 2001: Alain Connes.

¹⁰克拉福德奖官方网址: <http://www.crafoordprize.se/>.

邵逸夫奖 The Shaw Prize¹¹

邵逸夫奖是由香港著名的电影制作人邵逸夫先生于 2002 年 11 月创立. 首届的颁奖礼在 2004 年 9 月 7 日在香港举行.

邵逸夫奖设有数学奖、天文学奖、生命科学与医学奖, 共三个奖项, 每个奖项一百万美元奖金; 它是个国际性奖项, 由邵逸夫奖基金会有限公司管理.

数学奖得奖者:

- 2004 年: 陈省身.
- 2005 年: Andrew J. Wiles.
- 2006 年: 吴文俊, David Mumford.
- 2007 年: Robert Langlands and Richard Taylor.
- 2008 年: Vladimir Arnold and Ludwig Faddeev.
- 2009 年: Simon K Donaldson and Clifford H Taubes.
- 2010 年: Jean Bourgain.

¹¹邵逸夫奖官方网址: <http://www.shawprize.org/en/index.html>.