



第八章 群

刘世霞

shixia@tsinghua.edu.cn

问题解答

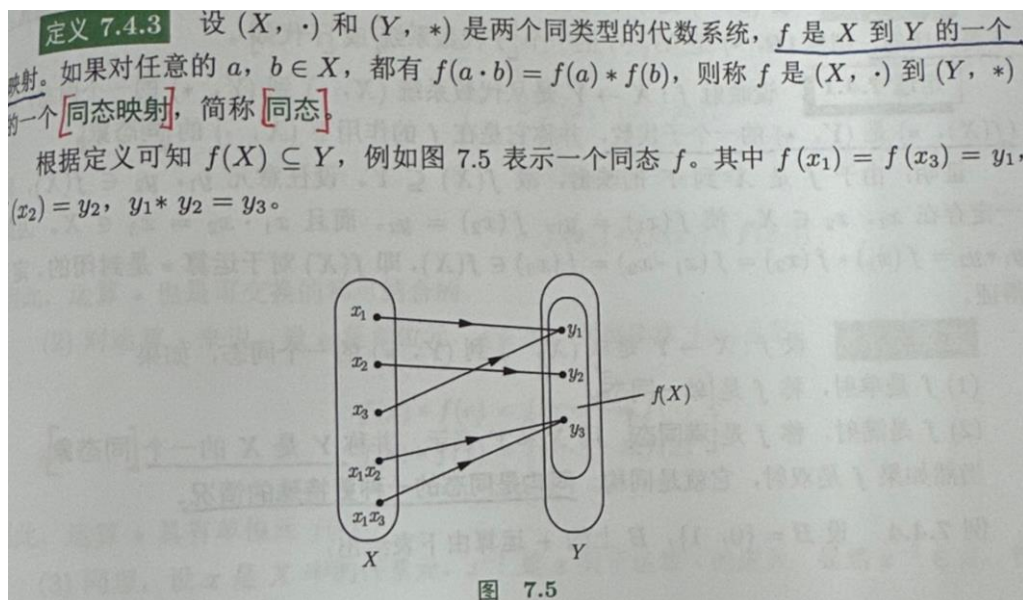


- 证结合律真的要枚举吗，有没有简单的语言证明，谢谢
- 满足结合律怎么证？把每种情况都枚举出来有点太麻烦了
 - 如果只是给了一个运算表，通常只能枚举证明
 - 如果对里面元素的性质有更多了解，可以用数学归纳法等证明，比如整数加法的结合律
- 设 f 是从代数系统 (A, \cdot) 到 $(B, *)$ 的满同态， S 是 A 的非空子集。 $f(S)$ 表示 S 中的元素在 f 下的象的集合，即 $f(S) = \{f(a) \mid a \in S\}$ 那么1.若 (S, \cdot) 是半群，则 $(f(S), *)$ 也是半群。2.若 (S, \cdot) 是么群，则 $(f(S), *)$ 也是么群。这里满同态是必须的吗？书上写的同态，好像也可以吧，因为好像没有涉及到 B
 - 同态就可以

问题解答



- 请问图片中图7.5所表示的 f 为什么是同态？ X 中没有 $x_2 \cdot x_3$ ，而且要是 x_1 和 $x_2 x_3$ 相乘会被映射到什么呢？
 - 这个图不严谨，没有给出 \cdot 和 $*$ 具体的运算表，无法说明 f 是同态
 - 图中信息无法得出 $f(x_1 x_2 x_3)$ 是什么



定义回顾



- **同态**：设 (X, \cdot) 和 $(Y, *)$ 是两个同类型的代数系统， $f: X \rightarrow Y$ 是一个映射。
- 如果 $\forall a, b \in X$ ，恒有 $f(a \cdot b) = f(a) * f(b)$
- 则称 f 是 (X, \cdot) 到 $(Y, *)$ 的一个**同态映射**，简称**同态**。
- 如何判定一个给定的系统是代数系统？
 - 集合是非空的
 - 定义的运算应该满足映射成立条件
 - 所有运算的封闭性

设 A 是非空集合， f_1, f_2, \dots, f_s 分别是 A 的 k_1, k_2, \dots, k_s 元运算， $k_i (i = 1, 2, \dots, s)$ 是正整数。

称集合 A 和运算 f_1, f_2, \dots, f_s 所组成的系统为一个**代数系统**（或一个代数结构），简称为一个**代数**，

教学反馈



03-04/20:29 周一 文 28

速度和节奏略快，希望能把概念讲的更加清晰一些，谢谢老师！

03-01/15:57 周五 文 21

感觉讲的有一些快，下次能不能更突出概念一些

03-02/21:25 周六 文 25

老师讲的很好，可以稍微慢一点点就更好了，谢谢老师。

03-03/17:07 周日 文 14

挺好的，可以再多一些实例吗？

03-02/00:13 周六 文 60

感觉讲的可以适当快一些，今天课上cover的部分看看书20min就自学完了，有些例子和证明比较显然似可以在课上快速带过（



内容回顾：代数系统的概念

定义7.3.3

- 设 A 是非空集合， f_1, f_2, \dots, f_s 分别是 A 的 k_1, k_2, \dots, k_s 元运算， $k_i (i = 1, 2, \dots, s)$ 是正整数。
- 称集合 A 和运算 f_1, f_2, \dots, f_s 所组成的系统为一个**代数系统**（或一个代数结构），简称为一个**代数**，用记号 $(A, f_1, f_2, \dots, f_s)$ 表示。
- 当 A 是有限集合时，也称该系统是**有限代数系统**。
- 两要素
 - 集合和代数运算（封闭的）



关于代数系统 (A, f) ，下面哪些描述是正确的

- ☒ A A 是非空的
- ☒ B f 是映射
- ☒ C 运算满足封闭性
- ☐ D 有单位元



如何判定一个给定的系统是代数系统？

- 集合是非空的
- 定义的运算应该满足映射成立条件
- 所有运算的封闭性



内容回顾：代数系统的概念

- 例： 设 $Z_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$ 是整数模 m 同余所确定的等价类集合， Z_m 上的运算 $+$ 定义如下：

$$\bar{i} + \bar{j} = \overline{(i + j)(\text{mod } m)}$$

则 $(Z_m, +)$ 是代数系统！

我们称该运算为模 m 加法运算。



内容回顾：交换律

- 代数系统 (X, \cdot) 中，如果 $\forall x_i, x_j \in X$,
- 都有 $x_i \cdot x_j = x_j \cdot x_i$ 成立,
- 则称 (X, \cdot) 对于二元运算·适合**交换律**。

$$(M_n(R), +)$$

$$(M_n(R), \times)$$



内容回顾：指数律

定理7.3.1

- 若 (X, \cdot) 对二元运算·适合结合律，则对于任何正整数 m 和 n ，有

$$1. \quad x^m \cdot x^n = x^{m+n}$$

$$2. \quad (x^m)^n = x^{m \times n}$$

指数律！广义结合律



内容回顾：单位元

定义 7.3.4

- 给定一个代数系统 $V = (X, \cdot)$
- 如果 $\exists e_L \in X$, 使得 $\forall x \in X$, 都有 $e_L \cdot x = x$, 则称 e_L 是 X 上关于运算 \cdot 的一个左单位元。
- 若 e 既是左单位元又是右单位元, 则称之为单位元。



内容回顾：逆元

定义 7.3.5

- 设 $V = (X, \cdot)$ 是有单位元 e 的代数系统，对于 $x \in X$,
- 若 $\exists x' \in X$, 使得 $x' \cdot x = e$, 则称 x 是左可逆的, 并称 x' 是 x 的一个左可逆元;
- 若 $\exists x'' \in X$, 使得 $x \cdot x'' = e$, 则称 x 是右可逆的, 并称 x'' 是 x 的一个右逆元;
- 若 x 既是左可逆的又是右可逆的, 则说 x 是可逆元。



内容回顾：消去律

- 定义：代数系统 $V = (X, \cdot)$ 上的二元运算 \cdot ，如果对 $\forall a, b, c \in X$ 且 $a \neq 0$

$$ab = ac \quad \Rightarrow \quad b = c$$

$$ba = ca \quad \Rightarrow \quad b = c$$

运算 \cdot 满足消去律！



内容回顾：同类型

定义7.4.1

- 设 $V_1 = (X, o_1, o_2, \dots, o_r)$ 和 $V_2 = (Y, \bar{o}_1, \bar{o}_2, \dots, \bar{o}_r)$ 是两个代数系统，若 o_i 和 \bar{o}_i 都是 k_i 元运算，且 $k_i (i = 1, 2, \dots, r)$ 是正整数
- 则说代数系统 V_1 和 V_2 是同类型的。

$$(\{a, b\}, \bullet)$$

\bullet	a	b
a	a	b
b	b	a

$$(\{0, 1\}, \times)$$

\times	0	1
0	0	1
1	1	0



内容回顾：同构

定义7.4.2

- 设 (X, \cdot) 和 $(Y, *)$ 是两个同类型的代数系统,
 $f: X \rightarrow Y$ 是一个双射。
- 如果 $\forall a, b \in X$, 恒有 $f(a \cdot b) = f(a) * f(b)$
- 则称 f 是 (X, \cdot) 到 $(Y, *)$ 的一个**同构映射**, 并称
 (X, \cdot) 与 $(Y, *)$ **同构**, 用 $X \cong Y$ 表示。



内容回顾：同构

- 另外设 $Y = \{a, b, c, d\}$ ，并定义 Y 上的运算如下：

\cdot	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

- (Y, \cdot) 与 $(Z_4, +)$ 是同类型的代数系统。现定义 $f: Z_4 \rightarrow Y$ 如下： $f: \bar{0} \rightarrow a, \bar{1} \rightarrow b, \bar{2} \rightarrow c, \bar{3} \rightarrow d$ ，可以判断 f 是同构映射，因此 $Z_4 \cong Y$



内容回顾：同态

- 定义7.4.3：设 (X, \cdot) 和 $(Y, *)$ 是两个同类型的代数系统， $f: X \rightarrow Y$ 是一个映射。
- 如果 $\forall a, b \in X$ ，恒有 $f(a \cdot b) = f(a) * f(b)$
- 则称 f 是 (X, \cdot) 到 $(Y, *)$ 的一个同态映射，简称同态。
- 定义7.4.6：代数系统 (X, \cdot) 上的同态映射
$$f: X \rightarrow X$$
- 称为自同态，若 f 是同构映射，则称之为自同构。



内容回顾： 8.1 半群

定义8.1.1

- 设 S 是非空集合， \cdot 是 S 上的一个二元运算，如果 \cdot 满足结合律，则代数系统 (S, \cdot) 称为半群(semigroup)。
- 换句话说，如果对于任意的 $a, b, c \in S$ ，若 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ 成立，则称 (S, \cdot) 为半群。

封结



内容回顾： 8.1 半群

- 例： $(R, +)$

$$\forall a, b, c \in R \quad (a + b) + c = a + (b + c)$$

半群！

- 例： $(R, -)$

$$\forall a, b, c \in R \quad (a - b) - c \neq a - (b - c)$$



内容回顾： 8.1 半群

定义8.1.2

- 若半群 (M, \cdot) 中有单位元 e 存在，则称 (M, \cdot) 是一个**含幺半群**或简称**幺群**。
- 幺群有时会用三元组 (M, \cdot, e) 表示，方便起见，简称 M 为幺群，并常用 ab 表示 $a \cdot b$ ，称为 a 与 b 的乘积。

封结幺



内容回顾： 8.1 半群

- 例： $(R, +)$

$$\forall a, b, c \in R \quad (a + b) + c = a + (b + c)$$

$$\forall a \in R \quad a + 0 = 0 + a = a$$

半群！

么群！



内容回顾： 8.1 半群

定义8.1.3

- 设 (M, \cdot, e) 是一个么群，若 \cdot 适合交换律，则称 M 是交换么群。

- 例： $(R, +)$

$$\forall a, b, c \in R \quad (a + b) + c = a + (b + c)$$

$$\forall a \in R \quad a + 0 = 0 + a = a$$

半群！

么群！

交换么群！



内容回顾： 8.1 半群

定理8.1.1

- 如果二元运算 \cdot 适合结合律，那么也适合广义结合律。
 - 根据定理显见

$$a^n a^m = a^{n+m} \quad (a^m)^n = a^{mn}$$

其中定义 $a^0 = e$ ，即 M 中的单位元。

- 如果 a 是 M 中的一个可逆元，那么一定有 $a^{-1} \in M$ ，于是 $a^{-1} a^{-1} \cdots a^{-1}$ (n 个) 可以表示成

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

因此上式中的 m, n 在整数范围内取值都是成立的。

若 a 可逆，则 a^n 也可逆



内容回顾： 8.1 半群

定义8.1.4

- 设 (M, \cdot, e) 是一个幺群，若存在一个元素 $g \in M$ ，使得任意的 $a \in M$ ， a 都可以写成 g 的方幂形式，即 $a = g^m$ （ m 是非负整数），则称 (M, \cdot, e) 是一个**循环幺群**，并且称 g 是 M 的一个**生成元**。



8.1 半群

- 例: $(R, +)$

$$\forall a, b, c \in R \quad (a + b) + c = a + (b + c)$$

$$\forall a \in R \quad a + 0 = 0 + a = a$$

半群! 么群! 交换么群! 循环么群? ×

- 例: $(N, +)$

循环么群? √



内容回顾： 8.1 半群

定理8.1.2 循环幺群是可交换幺群

- 证明：

设 g 是循环幺群中的一个生成元，则对任意 $a, b \in M$ ，有 $a = g^m, b = g^n, (m, n \geq 0)$

由于二元运算适合结合律，因此

$$ab = g^m g^n = g^{m+n} = g^n g^m = ba$$

所以循环幺群是可交换的。



内容回顾： 8.1 半群

定义8.1.5

- 设 (S, \cdot) 是一个半群, $T \subseteq S$, 在运算 \cdot 的作用下如果 T 是封闭的, 则称 (T, \cdot) 是 (S, \cdot) 的**子半群**。

定义8.1.6

- 设 (M, \cdot, e) 是一个幺群, $T \subseteq M$, 在运算 \cdot 的作用下如果 T 是封闭的, 且 $e \in T$, 则称 (T, \cdot, e) 是 (M, \cdot, e) 的**子幺群**。



内容回顾： 8.1 半群

定义8.1.7

- 设 (A, \cdot) 、 $(B, *)$ 是两个半群。 $f: A \rightarrow B$ 是 A 到 B 的映射， $\forall a, b \in A$, 若 $f(a \cdot b) = f(a) * f(b)$ 成立，则称 f 是从半群 A 到半群 B 的同态映射，简称同态。若 f 分别是单射、满射和双射时，分称 f 是单同态、满同态和同构。



内容回顾： 8.1 半群

定理8.1.3

- 设 f 是从代数系统 (A, \cdot) 到 $(B, *)$ 的~~满~~同态， S 是 A 的非空子集。 $f(S)$ 表示 S 中的元素在 f 下的象的集合，即 $f(S) = \{f(a) | a \in S\}$
- 那么
 1. 若 (S, \cdot) 是半群，则 $(f(S), *)$ 也是半群。
 2. 若 (S, \cdot) 是么群，则 $(f(S), *)$ 也是么群。

在满同态下，半群和么群的性质保留



内容回顾： 8.1 半群

推论

- 设 f 是从半群 (A, \cdot) 到代数系统 $(B, *)$ 的满同态,
 (S, \cdot) 是 (A, \cdot) 的子半群。
- 则有
 1. $(B, *)$ 是半群。
 2. $(f(S), *)$ 是 $(B, *)$ 的子半群。

半群、幺群、子半群的同态象，仍然是半群、幺群、子半群！



第八章 群

8.1 半群

8.2 群、群的基本性质

8.3 循环群 群的同构

8.4 变换群和置换群 Cayley定理

8.5 陪集和群的陪集分解 Lagrange定理

8.6 正规子群与商群

8.7 群的同态、同态基本定理

8.8 群的直积



8.2 群、群的基本性质

定义8.2.1

- 设 G 是非空集合， \cdot 是 G 上的二元运算，若代数系统 (G, \cdot) 满足
 1. 适合结合律，即 $\forall a, b, c \in G$, 有 $(ab)c = a(bc)$
 2. 存在单位元 e ，使得 $\forall a \in G, ae = ea = a$
 3. G 中的元素都是可逆元。即 $\forall a \in G$, 都 $\exists a^{-1} \in G$, 使得 $aa^{-1} = a^{-1}a = e$
- 则称代数系统 (G, \cdot) 是一个群，或记为 (G, \cdot, e) 。
- 为了方便起见，常用 G 表示群 (G, \cdot, e)



群的定义：封闭性、结合律、么元、逆

封闭么逆 \rightarrow 凤姐咬你





8.2 群、群的基本性质

定义8.2.2

- 设 (G, \cdot, e) 是含幺半群， e 是其单位元，如果 $\forall a \in G$ ，都 $\exists a^{-1} \in G$ ，使得

$$aa^{-1} = a^{-1}a = e$$

成立，则称 G 是一个群。

- G 是所有元素都可逆的含幺半群。



常用代数系统的比较

封

封闭

封闭么

封闭么逆

凤姐咬你

非空集合+
代数运算

非空集合+代数运
算+结合律

非空集合+代数运算+
结合律+单位元

非空集合+代数运算+
结合律+单位元+逆元

代数系统

半群

含么半群

群



下面哪个代数系统是群？

- ☒ A $(\mathbb{Q}, +), (\mathbb{Z}, +), (\mathbb{R}, +)$
- ☒ B $(\mathbb{R} - \{0\}, *)$
- ☒ C $(\mathcal{P}(S), \oplus)$
- ☐ D $(\mathbb{N}, +)$
- ☒ E $(\mathbb{Z}_n, +_n)$

提交



实例

- $(\mathbb{Q}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$ ✓ 逆元 $-x$
- $(\mathbb{R} - \{0\}, *)$ ✓ 逆元?
- $(\mathcal{P}(S), \oplus)$ ✓ 逆元?
- $(\mathbb{N}, +)$ ✗
- $(\mathbb{Z}_n, +_n)$ ✓

幂集:

单位元: 空集

逆元: 自身

逆元:

$$x = 0, \quad x^{-1} = 0;$$

$$x \neq 0, \quad x^{-1} = n - x$$



实例

- 设 $R = \{0^\circ, 60^\circ, 120^\circ, 180^\circ, 240^\circ, 300^\circ\}$ 表示在平面上几何图形绕形心顺时针旋转角度的六种可能情况，设 \star 是 R 上的二元运算，对于 R 中任意两个元素 a 和 b , $a \star b$ 表示平面图形连续旋转 a 和 b 得到的总旋转角度。并规定旋转 360° 等于原来的状态，就看作没有经过旋转。验证 $\langle R, \star \rangle$ 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：由题意， R 上的二元运算 \star 的运算表如上所示，由表知，运算 \star 在 R 上是**封闭的**。

对于任意 $a, b, c \in R$ ， $(a \star b) \star c$ 表示将图形依次旋转 a, b 和 c ，而 $a \star (b \star c)$ 表示将图形依次旋转 b, c 和 a ，而总的旋转角度都是 $a+b+c \pmod{360}$ ，因此 $(a \star b) \star c = a \star (b \star c)$ ，即 \star 运算满足结合性。

0^0 是么元。

60^0 ， 120^0 ， 180^0 逆元分别是 300^0 ， 240^0 ， 180^0

因此 (R, \star) 是个群



练习

- 已知：在整数集 I 上的二元运算 $*$ 定义为： $a, b \in I$,

$$a * b = a + b - 2$$

证明： $(I, *)$ 为群。

单位元： 2
逆元： $x^{-1} = 4 - x$

1. 非空集合
2. 运算时封闭的
3. 满足结合律
4. 有单位元
5. 有逆元



群和消去律之间的关系

- 1) 群满足消去律；2) 有限半群若其上的运算满足消去律，则一定是群
- 消去律：代数系统 $V = (X, \cdot)$ 上的二元运算 \cdot ，如果对 $\forall a, b, c \in X$ 且 $a \neq 0$

$$ab = ac \quad \Rightarrow \quad b = c$$

$$ba = ca \quad \Rightarrow \quad b = c$$

有限半群上的运算若满足消去律，则为群



- 对于有限半群 $G = \{x_1, \dots, x_n\}$ ，考察集合 $x_1 G = \{x_1 x_1, \dots, x_1 x_n\}$ 。由封闭性有 $x_1 G \subset G$ ，由消去律知 $\{x_1 x_1, \dots, x_1 x_n\}$ 两两不同，故 $x_1 G = G$ 。同理 $G = G x_1$
- 由 $x_1 G = G$ ，故存在元素 x_r 满足 $x_1 x_r = x_1$ 。下证 x_r 为右单位元。对任意 $x \in G$ 由 $G = G x_1$ 有 $x = x' x_1$ ，进而 $x x_r = x' x_1 x_r = x' x_1 = x$ 故为右单位元。同理可证存在左单位元 x_l ，可证单位元存在且唯一。
- 再利用 $G = x_1 G = G x_1$ 且 G 中有单位元，立得 x_1 存在左逆元和右逆元，进而 x_1 可逆。由 x_1 一般性知 G 所有元素均可逆。

定理 7.3.2

- 若代数系统 $V = (X, \cdot)$ 既有左单位元 e_L ，又有右单位元 e_R ，则 $e = e_L = e_R$ 是 X 的唯一的单位元。



无限半群上的运算若满足消去律，那么该半群是一定为群。

☐ A 对

☒ B 错

无限半群的反例：正整数乘法组成的半群



8.2 群、群的基本性质

定义8.2.3

- 若群 G 的二元运算满足交换律, 即 $\forall a, b \in G$, 都有 $ab = ba$
- 则称 G 是交换群, 或阿贝尔 (Abel) 群。
- 满足交换律的群是交换群!



8.2 群、群的基本性质

笑话

- 有人问一个法国四年级小朋友， $3+4$ 等于几？回答：不知道。
- 那 $4+3$ 等于几？还是回答不知道。
- 那你小学都学了些什么呀？我知道 $3+4=4+3$ 。
- 为什么呀？
- 因为加法是一个Abel群。



例题

- 设 $G = \{ e, a, b, c \}$ ， G 上的运算由下表给出

适合结合律，有单位元，每个元素都有逆元素

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

特征：

1. 满足交换律
2. 每个元素都是自己的逆元
3. a, b, c 中任何两个元素运算结果都等于剩下的第三个元素

克莱因（Klein）四元群，也是可交换群



定义：平凡群、有限群、无限群

- 只含单位元的群称为**平凡群**
 $(\{0\}, +)$ 是平凡群
- 规定集合 G 的基数为群 (G, \cdot) 的阶，当阶为某一整数时，该群为**有限群**；否则为**无限群**。

例

- $(Q^*, \cdot, 1)$ ，其中 Q^* 是非0有理数，对于任意 $a \in Q$ ，都有 $1/a \in Q$ ，使 $a \cdot (1/a) = (1/a) \cdot a = 1$ 。
因此 $(Q^*, \cdot, 1)$ 是**无限群**。



实例：判断群的阶

- $\langle \mathbb{Z}, + \rangle$ 和 $\langle \mathbb{R}, + \rangle$ 是
 - 无限群
- $\langle \mathbb{Z}_n, \cdot \rangle$ 是
 - 有限群，也是 n 阶群.
- Klein四元群是
 - 4阶群
- 上述群都是交换群

8.2 群、群的基本性质



• **定理8.2.1:** 设 G 是一个群, 则

1. G 中的单位元唯一。

定理7.3.2

2. G 中每个元素都有唯一的逆元。 **定理7.3.3**

3. 指数律成立: 即 $\forall a \in G, m, n$ 是任意整数, 有

$$a^m a^n = a^{m+n} \quad (a^m)^n = a^{mn} \quad \text{定理7.3.1}$$

4. 若 $ab = ba$, 则 $(ab)^n = a^n b^n$

定理7.3.1

• 若 (X, \cdot) 对二元运算 \cdot 适合结合律, 则对于任何正整数 m 和 n , 有

1. $x^m \cdot x^n = x^{m+n}$

2. $(x^m)^n = x^{m \times n}$



8.2 群、群的基本性质

定理8.2.2

- 设半群 (G, \cdot) 有一个左单位元 e , 且对 $\forall a \in G$, 都有左逆元 $a^{-1} \in G$, 使得 $a^{-1}a = e$ 成立, 则 G 是群。

- 证明: 因为

$$\begin{aligned} ae &= \underline{e} \underline{a} \underline{e} = ((\underline{a^{-1}})^{-1} \underline{a^{-1}}) \overset{\text{red arc}}{a} (\underline{a^{-1}a}) = (a^{-1})^{-1} (\underline{a^{-1}a}) (\underline{a^{-1}a}) \\ &= (a^{-1})^{-1} (ea^{-1})a = ((a^{-1})^{-1} a^{-1})a = ea = a \end{aligned}$$

- 所以 e 也是右单位元。



8.2 群、群的基本性质

定理8.2.2

设半群 (G, \cdot) 有一个左单位元 e , 且对 $\forall a \in G$, 都有左逆元 $a^{-1} \in G$, 使得 $a^{-1}a = e$ 成立, 则 G 是群。

证明 (续)

- 以下证 a^{-1} 也是 a 的右逆元
- 设 a' 是 a^{-1} 的左逆元, 于是有

$$aa^{-1} = eaa^{-1} = (a'a^{-1})aa^{-1} = a'(a^{-1}a)a^{-1} = (a'e)a^{-1} = a'a^{-1} = e$$

- 因此 G 是群!



8.2 群、群的基本性质

定理8.2.2

- 设半群 (G, \cdot) 有一个左单位元 e , 且对 $\forall a \in G$, 都有左逆元 $a^{-1} \in G$, 使得 $a^{-1}a = e$ 成立, 则 G 是群。
- 注意: 定理中“ $a^{-1}a = e$ ”中的 e 必须为一固定的左单位元。否则存在反例:
此时 a, b 均是左单位元, 但不构成群

$$S = \{a, b\}$$

	a	b
a	a	b
b	a	b

8.2 群、群的基本性质



- 定理8.2.3: 设 (G, \cdot) 是半群, 如果对 G 中任意两个元素 a, b , 方程 $ax = b$ 和 $ya = b$ 在 G 中都有解, 则 G 是一个群。
- 证明:
 - $\because \forall a, b \in G, \quad ya = b$ 有解
 - $\therefore \forall a \in G, \quad ya = a$ 有解, 不妨设某个解为 e $ea = a$
 - 对方程 $ax = b$, 设 x' 是其中的一个解, 那么
$$\forall b \in G \quad eb = e(ax') = (ea)x' = ax' = b$$
所以 e 就是左单位元;
 - 此外, $\forall a \in G, ya = e$ 有解 y' , 所以 y' 是 a 的左逆元。
 - 由定理8.2.2, G 是群。

定理8.2.2

设半群 (G, \cdot) 有一个左单位元 e , 且对 $\forall a \in G$, 都有左逆元 $a^{-1} \in G$, 使得 $a^{-1}a = e$ 成立, 则 G 是群。



例题

- 设群 $G=(P(\{a,b\}),\oplus)$, 其中 \oplus 为对称差. 解下列群方程

$$\{a\} \oplus X = \emptyset, \quad Y \oplus \{a,b\} = \{b\}$$

- 解

$$X = \{a\}^{-1} \oplus \emptyset = \{a\} \oplus \emptyset = \{a\},$$

$$Y = \{b\} \oplus \{a,b\}^{-1} = \{b\} \oplus \{a,b\} = \{a\}$$



例题

- 设 $G = (\{a_1, a_2, \dots, a_n\}, \cdot)$ 是 n 阶群, 令

$$a_i G = \{a_i \cdot a_j \mid j=1, 2, \dots, n\}$$

证明 $a_i G = G$.

证 由群中运算的封闭性有 $a_i G \subseteq G$. 假设 $a_i G \subset G$, 即 $|a_i G| < n$.

必有 $a_j, a_k \in G$ 使得

$$a_i \cdot a_j = a_i \cdot a_k \quad (j \neq k)$$

由消去律得 $a_j = a_k$, 与 $|G| = n$ 矛盾.



8.2 群、群的基本性质

定理8.2.4

- 设 G 是一个群, $\forall a, b \in G$ 恒有

$$(a^{-1})^{-1} = a, \quad (ab)^{-1} = b^{-1}a^{-1}$$

- 证明:

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

$$\because (ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = e$$

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



8.2 群、群的基本性质

定义8.2.4

- 设 a 是 G 中的一个元素，若有正整数 k 存在，使 $a^k = e$ ，则满足 $a^k = e$ 的最小正整数 k 称为元素 a 的阶（或周期），记为 $O < a >$ ，并称 a 是有限阶元素。

- 例： (Z_6, \cdot)

设 $Z_6 = \{\bar{0}, \bar{1}, \dots, \bar{5}\}$ ，是 Z_6 上的模6加法运算。

$$O < \bar{1} > = 6$$

$$O < \bar{3} > = 2$$



请计算群 $(\mathbb{Q} - \{0\}, *)$ 中各元素的阶
其中 \mathbb{Q} 是有理数



8.2 群、群的基本性质

定理8.2.5

• 设 a 是群 G 中的一个 r 阶元素， k 是正整数，则

1. $a^k = e$ ，当且仅当 $r|k$

2. $O \langle a \rangle = O \langle a^{-1} \rangle$

3. $r \leq |G|$



8.2 群、群的基本性质

定理8.2.5

- 设 a 是群 G 中的一个 r 阶元素, k 是正整数, 则
 1. $a^k = e$, 当且仅当 $r|k$
- 证明:
 - 充分性: $r|k$, 则 $k = rm$, 得 $a^k = a^{rm} = (a^r)^m = e^m = e$
 - 必要性: 若 $a^k = e$, $k = pr + q (0 \leq q < r)$, 得 $a^k = a^q = e$
 - r 是 a 的阶, 所以 $q = 0$, 故 $r|k$



8.2 群、群的基本性质

- 定理8.2.5: 设 a 是群 G 中的一个 r 阶元素, k 是正整数, 则 $2. \quad 0 < a > = 0 < a^{-1} >$
- 证明:
 - 设 $0 < a > = r, 0 < a^{-1} > = r'$
 - 定理8.2.1得 $(a^{-1})^r = (a^r)^{-1} = e$, 所以 $r' | r$
 - 同理, $r | r'$, 故 $r = r'$

定理8.2.1

- 设 G 是一个群, 则

1. G 中的单位元唯一。

¹ 定理7.3.2

2. G 中每个元素都有唯一的逆元。

² 定理7.3.3

3. 指数律成立: 即 $\forall a \in G, m, n$ 是任意整数, 有

$$a^m a^n = a^{m+n} \quad (a^m)^n = a^{mn} \quad \text{定理7.3.1} \quad \text{³}$$

4. 若 $ab = ba$, 则 $(ab)^n = a^n b^n$



8.2 群、群的基本性质

定理8.2.5

- 设 a 是群 G 中的一个 r 阶元素, k 是正整数, 则

$$3. \quad r \leq |G|$$

- 思路: 证明 e, a, \dots, a^{r-1} 是不同的元素
- 证明:

设 $e = a^0$, 且 a, \dots, a^{r-1} 中 $a^i = a^j$, 其中 $0 \leq i < j < r$

$a^{j-i} = e$, 即 $0 < j - i < r$, 与 a 的阶是 r 相矛盾

e, a, \dots, a^{r-1} 是 G 中不同的元素,

$r \leq |G|$ 。



实例

- **例5** 设 G 是群, $a, b \in G$ 是有限阶元. 证明
- (1) $O \langle b^{-1}ab \rangle = O \langle a \rangle$ (2) $O \langle ab \rangle = O \langle ba \rangle$

证 (1) 设 $O \langle a \rangle = r$, $O \langle b^{-1}ab \rangle = t$, 则有

$$\begin{aligned}(b^{-1}ab)^r &= \underbrace{(b^{-1}ab)(b^{-1}ab)\dots(b^{-1}ab)}_{r\uparrow} \\ &= b^{-1}a^r b = b^{-1}eb = e\end{aligned}$$

从而有 $t \mid r$.

另一方面, 由 $a = (b^{-1})^{-1}(b^{-1}ab)b^{-1}$ 可知 $r \mid t$. 从而有 $O \langle b^{-1}ab \rangle = O \langle a \rangle$.



实例

(2) 设 $0 < ab > = r$, $0 < ba > = t$, 则有

$$\begin{aligned}(ab)^{t+1} &= \underbrace{(ab)(ab)\dots(ab)}_{t+1\text{个}} \\ &= a \underbrace{(ba)(ba)\dots(ba)}_{t\text{个}} b \\ &= a(ba)^t b = aeb = ab\end{aligned}$$

由消去律得 $(ab)^t = e$, 从而可知, $r \mid t$.
同理可证 $t \mid r$. 因此 $0 < ab > = 0 < ba >$



关于群的元素阶，下列说法正确的是

- ☒ A 有限群的元素阶都是有限的
- ☐ B 所有元素的阶都是有限的群必为有限群
- ☒ C 存在无限群，其元素的阶都是有限的
- ☐ D 存在无限群，其元素的阶都是无限的



解答

- A: 有限群的元素的阶都是有限的
- B: 所有元素的阶都是有限的群必为有限群
- C: 存在无限群，其元素的阶都是有限的
- D: 存在无限群，其元素的阶都是无限的

解答

- A 正确，否则无限阶元的若干次幂就构成了一个无限集合
- B 错误 C正确，如 $(P(M), \oplus)$ ：除单位元外所有元素阶均为2的群
- D 错误，单位元的阶只能为1



8.2 群、群的基本性质

定义8.2.5

- 设 H 是群 G 的一个非空子集，若 H 对于 G 的运算仍然构成群，则称 H 是 G 的一个子群，记为 $H \leq G$ 。
 - $G, \{e\}$ 都是群，称为 G 的平凡子群。
 - 如果 G 的子群 $H \neq G$ ，则称 H 为 G 的真子群，记为 $H < G$
- 例
 - $(\mathbb{Z}, +, 0)$ 是一个群，设 T 是正整数 m 整倍数的集合，则 $(T, +, 0)$ 是 $(\mathbb{Z}, +, 0)$ 的一个子群。
 - 设 G 是全体 $n \times n$ 阶实可逆矩阵的集合，它对矩阵乘法构成群。令 H 是行列式值为1的矩阵的集合，则 $H < G$ 。

8.2 群、群的基本性质



- **定理8.2.6** H 是 G 的子群的充要条件是：

1. H 对 G 的乘法运算是封闭的，即 $\forall a, b \in H$ ，都有 $ab \in H$
2. H 中有单位元 e' ，且 $e' = e$
3. $\forall a \in H$ ，都有 $a^{-1} \in H$ ，且 a^{-1} 是 a 在 G 中的逆元

- 证明

- H 是子群，所以 H 对 G 的运算封闭，并存在单位元 e'
 G 中， $e'e = e'$ ， H 中 $e'e' = e'$ ，故 $e'e = e'e'$ ， $e' = e$
- 任取 $a \in H$ ，要证都有 $a^{-1} \in H$
设 a 在 H 中的逆元是 a' ，在 G 中的逆元是 a^{-1}
 $aa^{-1} = e = e' = aa'$ ，故 $a^{-1} = a'$ ，必要性得证
- 充分性是显然的，定理得证



8.2 群、群的基本性质

- 定理8.2.7 G 的非空子集 H 是 G 的子群的充要条件是 $\forall a, b \in H$, 都有 $ab^{-1} \in H$
- 证明
 - 需要证明 H 满足子群充要条件:
封闭性、单位元、逆元素
 - $\forall a, b \in H$, $ab^{-1} \in H$, 故 $\forall a \in H$, 令 $b = a$, 则 $e = aa^{-1} \in H$ (单位元)
 - $\forall b \in H$, $b^{-1} = eb^{-1} \in H$ (逆元)
 - $\forall a, b \in H$, $b^{-1} \in H$, 故 $ab = a(b^{-1})^{-1} \in H$ (封闭性)
- 证毕!



设 H_1, H_2 是 G 的两个子群, 则 $H = H_1 \cap H_2$

- ☒ A 是群 G 的子群
- ☐ B 不是群 G 的子群
- ☐ C 与 G 没有关系



8.2 群、群的基本性质

- 例：设 H_1, H_2 是 G 的两个子群，则 $H = H_1 \cap H_2$ 也是 G 的子群。
- 证明：
 - G 单位元 $e \in H_1, H_2$ ，所以 $e \in H$ ，即 H 非空。
 - 任设 $a, b \in H$ ，则 $a, b \in H_1$ ， $a, b \in H_2$ ，由定理8.2.7有 $ab^{-1} \in H_1$ ， $ab^{-1} \in H_2$ ，因此 $ab^{-1} \in H$ ，
 - 所以 H 是 G 的子群。

证明集合是非空的是非常必要的第一步

定理8.2.7 G 的非空子集 H 是 G 的子群的充要条件是 $\forall a, b \in H$ ，都有 $ab^{-1} \in H$



8.2 群、群的基本性质

- 例：设 a 是群 G 中的任一元素，则 $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$ 是 G 的子群。
- 证明：
 - $a^0 = e \in \langle a \rangle$ ，所以 $\langle a \rangle$ 非空。
 - 任取 $a^m, a^n \in \langle a \rangle$ ，有 $a^m(a^n)^{-1} = a^m a^{-n} = a^{m-n} \in \langle a \rangle$
 - 由定理8.2.7， $\langle a \rangle \leq G$ 。



关于子群的说法，下面说法正确的是

$$HH = \{h_1 h_2 | h_1 \in H, h_2 \in H\}$$

A

对于群 G 和其子群 H ，有 $HH = H$

B

对于群 G 和其子集 H ，若 $HH = H$ ，则 H 是 G 的子群

C

存在群 G 是其两个真子群的并

D

存在群 G 是其三个真子群的并

提交

解答



$$HH = \{h_1 h_2 \mid h_1 \in H, h_2 \in H\}$$

- 对于群 G 和其子群 H , 有 $HH = H$ ✓
 - 子群的运算具有封闭性, 故 $HH \subseteq H$ 。又 $H = eH \subseteq HH$, 故 $H = HH$
- 对于群 G 和其子集 H , 若 $HH = H$, 则 H 是 G 的子群 ✗
 - $G = (\mathbb{Q} - \{0\}, *)$, H 为全体奇数, 其满足 $HH = H$ 但不构成子群
- 存在群 G 是其两个真子群的并 ✗
 - 反证, 假设 $G = H \cup K$, H, K 是 G 的真子群
 - 存在 $h \in H, h \notin K$; $k \in K, k \notin H$
 - 此时 $hk \notin H$ (否则 $k = h^{-1}(hk) \in H$) 同理 $hk \notin K$, 则 $hk \notin G$, 矛盾
- 由存在群 G 是其三个真子群的并 ✓
 - $G = K_4 = \{e, a, b, c\}, H_1 = \{e, a\}, H_2 = \{e, b\}, H_3 = \{e, c\}$



总结：群的性质

性质1 设 (G, \cdot) 为群，则 $\forall a \in G$ ， a 的左逆元也是 a 的右逆元.

性质2 设 (G, \cdot) 为群，则 G 的左单位元 e 也是右单位元.

性质3 设 (G, \cdot) 为群，则 $\forall a, b \in G$ ，方程 $a \cdot x = b$ 和 $y \cdot a = b$ 在 G 中的解唯一.



总结：群的性质

性质4 设 (G, \cdot) 为群，则

(1) $\forall a \in G, (a^{-1})^{-1} = a;$

(2) $\forall a, b \in G, (a \cdot b)^{-1} = b^{-1} \cdot a^{-1}.$

性质5 群 (G, \cdot) 中的乘法满足消去律，即 $\forall a, b, c \in G$ 有

(1) 若 $a \cdot b = a \cdot c$ ，则 $b = c$ (左消去律)

(2) 若 $b \cdot a = c \cdot a$ ，则 $b = c$ (右消去律)



总结：群的性质

性质6 设 G 为群，则 G 中的幂运算满足：

- (1) $\forall a \in G, a^n a^m = a^{n+m}, n, m \in \mathbb{Z}$
- (2) $\forall a \in G, (a^n)^m = a^{nm}, n, m \in \mathbb{Z}$
- (3) 若 G 为交换群，则 $(ab)^n = a^n b^n$.

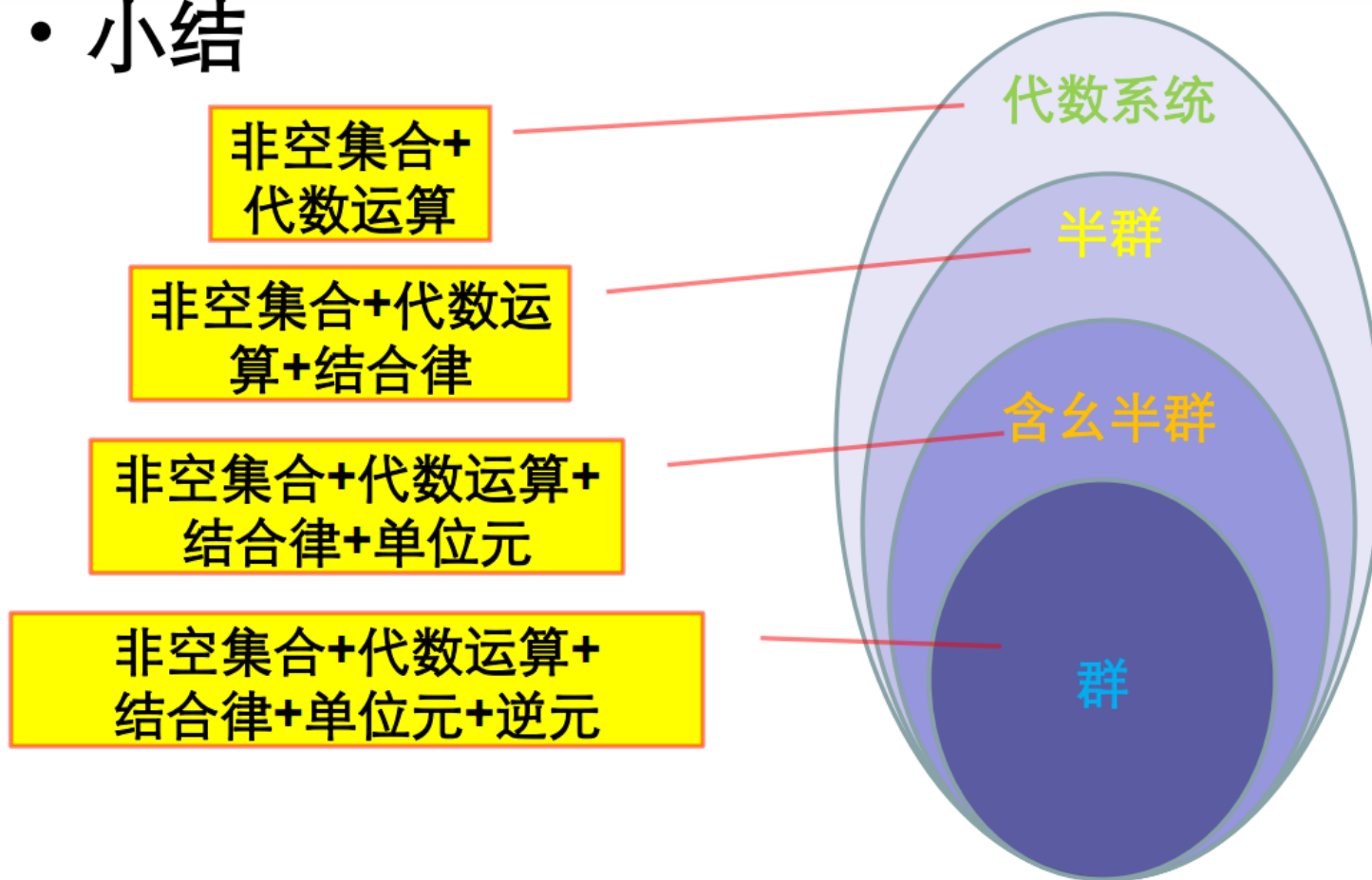
性质7 G 为群， $a \in G$ 且 $|a| = r$. 设 k 是整数，则

- (1) $a^k = e$ 当且仅当 $r \mid k$.
- (2) $\langle a^{-1} \rangle = \langle a \rangle$.



8.2 群、群的基本性质

• 小结





关于无限群，下面说法正确的是

- ☐ A 存在无限群，其只有有限个子群
- ☒ B 存在无限群，其每个元素的阶都有限
- ☒ C 存在无限群，除一个元素外，其余所有元素的阶都无限
- ☒ D 存在无限群，除两个元素外，其余所有元素的阶都无限

提交

解答



- 存在无限群，其只有有限个子群 ✗
 - 若存在无限阶元 a ，则 $\langle a \rangle, \langle a^2 \rangle, \langle a^3 \rangle, \dots$ 均为不同子群，有无限个
 - 若不存在无限阶元，记 $S = \{\langle x \rangle | x \in G\}$ ，即每个元素生成的子群。不存在无限阶元意味着 $\langle x \rangle$ 均为有限集。若 G 只有有限个子群，则 $G = \cup S$ 为有限个有限集的并，必为有限集，矛盾
- 存在无限群，其每个元素的阶都有限 ✓
 - $(P(\mathbb{N}), \oplus)$
- 存在无限群，除一个元素外，其余所有元素的阶都无限 ✓
 - $(\mathbb{Z}, +)$
- 存在无限群，除两个元素外，其余所有元素的阶都无限 ✓
 - $(\mathbb{Q} - \{0\}, *)$



第八章 群

8.1 半群

8.2 群、群的基本性质

8.3 循环群 群的同构

8.4 变换群和置换群 Cayley定理

8.5 陪集和群的陪集分解 Lagrange定理

8.6 正规子群与商群

8.7 群的同态、同态基本定理

8.8 群的直积



RSA密码系统

- RSA公钥加密算法是1977年由罗纳德·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman）一起提出的。1987年首次公布，RSA就是他们三人姓氏开头字母拼在一起组成的
- RSA是目前最有影响力的公钥加密算法，它能够抵抗到目前为止已知的绝大多数密码攻击，已被ISO推荐为公钥数据加密标准



RSA密码系统

- RSA算法的主要思想：当 p 和 q 是一个大素数的时候，从它们的积 pq 去分解因子 p 和 q ，这是一个公认的数学难题。
- RSA的主要运算是取自 Z_n 中的指数运算
- Z_n 是整数模 n 的同余类的加法群，在本节课中，我们将会学到 Z_n 是一种循环群。

http://baike.baidu.com/link?url=1TWtkiuBAZ5iXFYB-FtnyCeTsDny6T2TQZUSoztBOXEV9Cr1VnKoxRLBPbWvhRtHWuq4EUVmecfSvKBWuYnZ_K



8.3 循环群 群的同构

定义8.3.1

- 若群 G 中存在一个元素 a ，使得 G 中的任意元素 g ，都可以表示成 a 的幂的形式，即
$$G = \{a^k | k \in \mathbb{Z}\},$$
- 则称 G 是循环群，记作 $G = \langle a \rangle$ ， a 称为 G 的生成元。

由一个元素生成的群



内容回顾：循环么群

定义8.1.4

- 设 (M, \cdot, e) 是一个么群，若存在一个元素 $g \in M$ ，使得任意的 $a \in M$ ， a 都可以写成 g 的方幂形式，即 $a = g^m$ （ m 是非负整数），则称 (M, \cdot, e) 是一个**循环么群**，并且称 g 是 M 的一个**生成元**。



8.3 循环群 群的同构

- 思考：

- 循环群和循环幺群的区别是什么？

- 例：

$$(N, +)$$

$$(Z_m, \cdot) \quad Z_m = \{\overline{0}, \overline{1}, \dots, \overline{m-1}\}$$

是否有逆元



思考

- 生成元的阶与循环群元素数相互关系？

相等



8.3 循环群 群的同构

定义

- 对于循环群 $G = \langle a \rangle$, 若生成元 a 的阶数 $|a| = n$, 也可记为 $O(a)$, 则 $G = \langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$, 称为 **n 阶循环群**;
- 若 $|a|$ 不存在, 则 $G = \langle a \rangle = \{e, a, a^{-1}, a^2, a^{-2}, \dots\}$ 也是无限的, 称为 **无限阶循环群**



下面说法是否正确？

所有的循环群都同构于 $(\mathbb{Z}, +)$ 或 $(\mathbb{Z}_n, +)$

当 $o(a) = \infty$ 时, $G \cong (\mathbb{Z}, +)$ 无限循环群

当 $o(a) = n$ 时, $G \cong (\mathbb{Z}_n, +)$ n 阶循环群



关于循环群的一个结论

- 所有的循环群都同构于 $(\mathbb{Z}, +)$ 或 $(\mathbb{Z}_n, +)$
- 当 $o(a)=\infty$ 时, $G \cong (\mathbb{Z}, +)$ 无限循环群
- 当 $o(a)=n$ 时, $G \cong (\mathbb{Z}_n, +)$ n 阶循环群



8.3 循环群 群的同构

- 思考：
 - 循环群的生成元有几个？
 - 例：

$$(Z, +) \quad 1, -1$$

$$(Z_6, \cdot) \quad Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$$

$$\begin{array}{llll} (\bar{5})^0 = \bar{0} & (\bar{5})^2 = \bar{4} & (\bar{5})^4 = \bar{2} & (\bar{5})^6 = \bar{0} \\ (\bar{5})^1 = \bar{5} & (\bar{5})^3 = \bar{3} & (\bar{5})^5 = \bar{1} & \end{array}$$



关于循环群 $G = \langle a \rangle$ 的生成元，下面哪些说法是正确的？

- ☒ A 若 $o\langle a \rangle = \infty$ ，则 G 中只有生成元 a 或 a^{-1}
- ☒ B 若 $o\langle a \rangle = \infty$ ，则 a^{-1} 是生成元
- ☒ C 若 $o\langle a \rangle = n$ ，则 G 中有 $\varphi(n)$ 个生成元，其中 $\varphi(n)$ 是欧拉函数
- ☐ D 若 $o\langle a \rangle = n$ ，则 G 中只有生成元 a 或 a^{-1}



8.3 循环群 群的同构

定理8.3.1

- 设 $G = \langle a \rangle$, 则
 - 1. 若 $o\langle a \rangle = \infty$, 则 G 中只有生成元 a 或 a^{-1}
 - 2. 若 $o\langle a \rangle = n$, 则 G 中有 $\varphi(n)$ 个生成元
 - 其中 $\varphi(n)$ 是欧拉函数, 它表示小于 n 且与 n 互素的正整数个数。



8.3 循环群 群的同构

定理8.3.1 若 $o\langle a \rangle = \infty$ ，则 G 中只有生成元 a 或 a^{-1}

• 证明：

- 当 $o\langle a \rangle = \infty$ 时，显然 a 是生成元。同时， $\forall a^k \in G$ ， $a^k = (a^{-1})^{-k}$ ，因此 a^{-1} 也是 G 的一个生成元
- 假设还有另外一个生成元 b ，则不妨设 $b = a^j$
- 由于 b 也是生成元，则 a 可以写为 $a = b^t$
- 则必有 $a = b^t = (a^j)^t = a^{jt}$ ，由消去律， $a^{jt-1} = e$
- a 为无限阶，则必有 $jt - 1 = 0$ ，故只能有 $j = t = 1$ 或 $j = t = -1$



8.3 循环群 群的同构

定理8.3.1 若 $o\langle a \rangle = n$ ，则 G 中有 $\varphi(n)$ 个生成元

• 证明（续）：

- 当 $o\langle a \rangle = n$ 时，若 $G = \langle a \rangle = \langle a^r \rangle$ ，则存在 p 使 $a = (a^r)^p$ ，即 $a^{rp-1} = e$
- 故存在 q ，使得 $rp - 1 = qn$ 裴蜀定理
- 即 $(r, n) = 1$ 证毕！

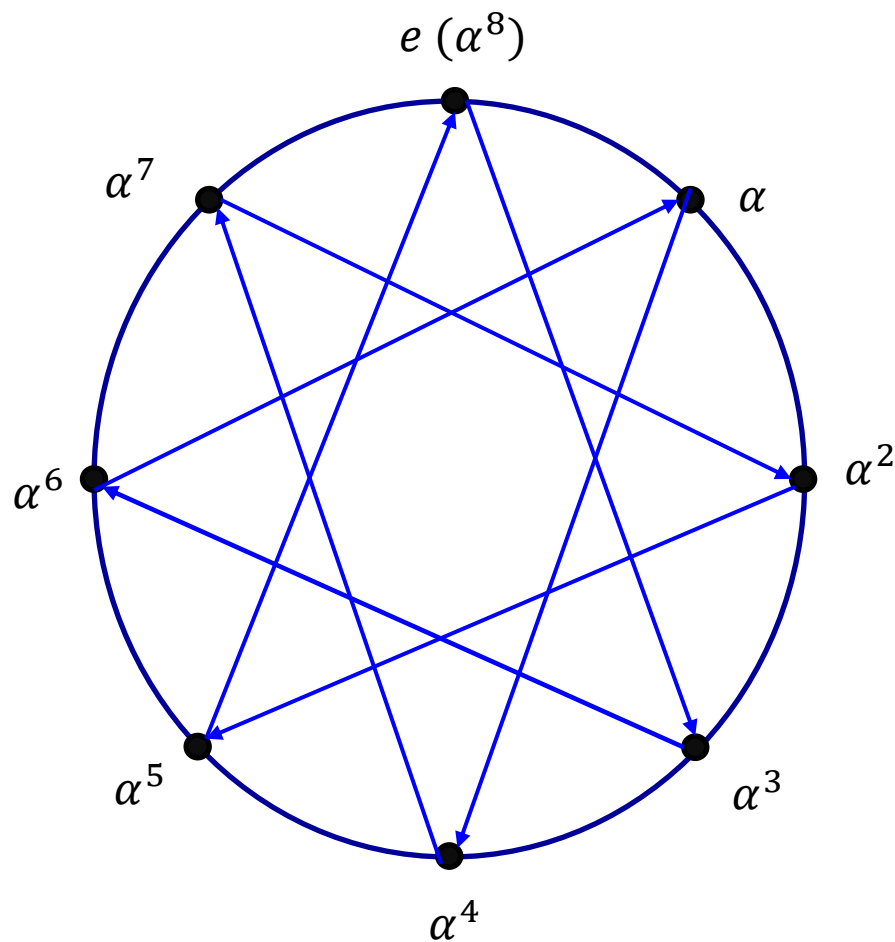
裴蜀定理： a, b 互质的充分必要条件是存在整数 x, y 使 $ax+by=1$

循环群中，若某元素的幂次与 n 互素，则可以作为另一生成元！



8.3 循环群 群的同构

例





群的同构

定义8.3.2

- 设 (G, \cdot) 和 $(G', *)$ 是两个群,
 $f: G \rightarrow G'$ 是双射, 如果 $\forall a, b \in G$ 都有
$$f(ab) = f(a) * f(b)$$
- 则称 f 是 G 到 G' 的一个同构, 记作 $G \cong G'$

群同构的充分条件: 1. 双射 2. 保持运算!



8.3 循环群 群的同构

- 思考：

循环群 G 的子群 H 是否仍然是循环群？ **YES!**

分析：子群 H 的生成元？

G 的子群 H ，可以写为 $H = \{e, a^{k_1}, a^{k_2}, \dots, a^{k_m}, \dots\}$

不妨设 H 所有元素的幂次中， k_1 是最小值

则对于 H 中其他元素 a^{k_m} 幂次进行分析，一定有 $k_m = l \cdot k_1 + r$ ，其中 $0 \leq r < k_1$ 。

$$\text{故 } a^{k_m} = a^{r+l \cdot k_1} = a^r a^{l \cdot k_1} \quad \longrightarrow \quad a^r = a^{k_m} (a^{l \cdot k_1})^{-1} \longrightarrow$$

$$a^r \in H$$

$$r = 0$$

最小次幂是生成元



8.3 循环群 群的同构

- 思考：

G 为循环群时， G 的子群是什么特征？

- 若 G 为无限循环群：

假设子群 H 生成元是 a^k ，则该生成元的阶数一定为 ∞

否则若存在正整数 q ，使得 $(a^k)^q = e$ ，将说明 a 为有限阶元，矛盾！

- 若 G 为无限循环群，则其非平凡子群也为无限循环群！



8.3 循环群 群的同构

- 思考：

G 为循环群时， G 的子群是什么特征？

- 若 G 为 n 阶循环群：

假设子群 H 生成元是 a^{k_1} ，设其阶数为 d

由于 $(a^{k_1})^n = (a^n)^{k_1} = (e)^{k_1} = e$ （定理8.2.5）

则必定有 $d|n$

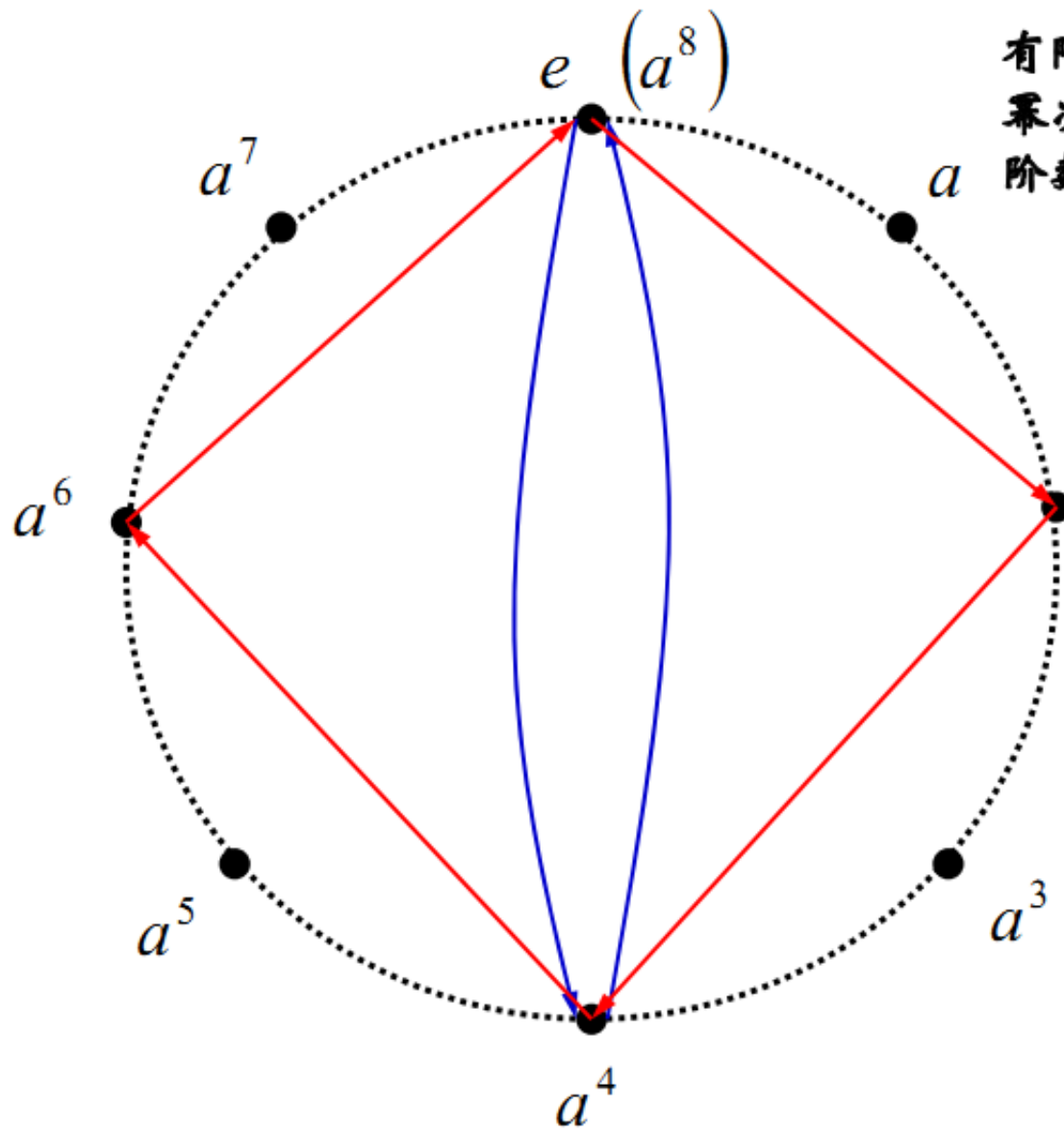
- 若 G 为 n 阶循环群，则其子群生成元阶数为 n 因数！

定理8.2.5 设 a 是群 G 中的一个 r 阶元素， k 是正整数，则

1. $a^k = e$ ，当且仅当 $r|k$



8.3 循环群 群的同构



有限循环群中，
幂次与 n 互质，可做生成元
阶数为 n 因数，可做子群生成元

$$\begin{aligned} a &= (a^r)^p \\ a^{rp-1} &= e \\ rp - 1 &= qn \end{aligned}$$



谢谢
shixia@tsinghua.edu.cn