

离散数学考前复习

第一部分 逻辑

命题逻辑的定义

命题是一个或真或假的陈述句，但不能既真又假

逻辑连接词(逻辑运算符)，真值表

逻辑连接词

- 否定词 NOT Negation \neg
- 合取词 AND Conjunction \wedge
- 析取词 OR Disjunction \vee
- 异或词 XOR Exclusive or \oplus
- 蕴含词 if-then Implication \rightarrow
- 等价词 if and only if Biconditional \leftrightarrow

运算优先级： $\neg > \wedge > \vee > \rightarrow > \leftrightarrow$

真值表

蕴含：只有真 \rightarrow 假为假

等价：同真同假时为真

命题逻辑等价，基本逻辑等价式，逻辑等价的证明

命题逻辑等价

$$p \leftrightarrow q$$

是永真式，称命题p和q是等价的

基本逻辑等价式

几个难记忆的基本逻辑等价式

吸收律

$$p \vee (p \wedge q) \Leftrightarrow p$$

$$p \wedge (p \vee q) \Leftrightarrow p$$

其他

$$(p \rightarrow q) \wedge (p \rightarrow r) \Leftrightarrow p \rightarrow (q \wedge r)$$

$$(p \rightarrow r) \wedge (q \rightarrow r) \Leftrightarrow (p \vee q) \rightarrow r$$

$$(p \rightarrow q) \vee (p \rightarrow r) \Leftrightarrow p \rightarrow (q \vee r)$$

$$(p \rightarrow r) \vee (q \rightarrow r) \Leftrightarrow (p \wedge q) \rightarrow r$$

逻辑等价的证明

两种方式：

1. 画真值表
2. 通过已知的逻辑等价式，证明 $p \leftrightarrow q$ 是永真式

命题逻辑推理:推理法则，形式化推理证明

逻辑蕴含

如果 $p \rightarrow q$ 是永真式，则命题p蕴含q

有效的论证

若每当所有的前提都为真时，结论也为真，则这样的论证称为有效的。也就是等价于下列蕴含式为真。

$$p_1 \wedge p_2 \wedge \dots \wedge p_n \rightarrow q$$

is tautology

推理法则

| | |
|-------|--|
| 附加 | $p \rightarrow (p \vee q)$ |
| 化简 | $(p \wedge q) \rightarrow p$ |
| 合取 | $((p) \wedge (q)) \rightarrow (p \wedge q)$ |
| 假言推理 | $(p \wedge (p \rightarrow q)) \rightarrow q$ |
| 取拒式 | $(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$ |
| 假言三段论 | $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$ |
| 析取三段论 | $((p \vee q) \wedge (\neg p)) \rightarrow q$ |
| 构造两难性 | $((p \rightarrow r) \wedge (q \rightarrow r)) \wedge (p \vee q) \rightarrow r$ |
| 消解 | $((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$ |

形式化论证 Formal Proofs

假定假设是正确的，用一些推论和逻辑等价式来确定结论的正确

如果有这样 $p \rightarrow q$ 的结论形式，我们就能把原问题转换成为下面这个式子：

$$p_1 \wedge p_2 \wedge \dots \wedge p_n \wedge p \Rightarrow q$$

因为

$$(p_1 \wedge p_2 \wedge \dots \wedge p_n) \rightarrow (p \rightarrow q) \Leftrightarrow (p_1 \wedge p_2 \wedge \dots \wedge p_n \wedge p) \rightarrow q$$

是永真式

归谬法：

使用归谬法证明 $p \rightarrow q$ 的步骤：

1. 假设 p 为真， q 为假
2. 证明 $\neg p$ 也为真 \rightarrow 矛盾！

谬误 Fallacies

1. 断定结论的谬误

$((p \rightarrow q) \wedge q) \rightarrow p$ 把此式当作重言式的不正确的论证

2. 否定假设的谬误

$$((p \rightarrow q) \wedge \neg p) \rightarrow \neg q$$

谓词和量词

谓词

一般来说，形为 $P(x_1, x_2, \dots, x_n)$ 的语句是命题函数P在n元组 (x_1, x_2, \dots, x_n) 的值，P也称为谓词。

量词

全称量词 \forall

$\forall x P(x)$ 对论域中任意一个x而言， $P(x)$ 的真值都为真。

$$\forall x P(x) \Leftrightarrow P(x_1) \wedge P(x_2) \wedge \dots \wedge P(x_n)$$

存在量词 \exists

$\exists x P(x)$ 在论域中存在一个x使 $P(x)$ 的真值为真

$$\exists x P(x) \Leftrightarrow P(x_1) \vee P(x_2) \vee \dots \vee P(x_n)$$

量词的否定

$$\neg \forall x P(x) \Leftrightarrow \exists x \neg P(x)$$

$$\neg \exists x P(x) \Leftrightarrow \forall x \neg P(x)$$

逻辑等价

量词相关逻辑等价式 PPT或课本

嵌套量词

- 嵌套量词->出现在其他量词作用域内的量词

- 量词的顺序是重要的
- 嵌套量词的否定

量词有关推理法则

- 全称量词消去
- 全称量词引入
- 存在量词消去
- 存在量词引入

第二部分 集合论+函数

集合的基本概念及表示方法

一组对象形成集合，集合中的对象也叫做集合中的元素或成员

集合用大写字母表示，元素用小写字母表示

集合的描述：

- 花括号表示
- 集合构造符号 $U, Q, Z, S = \{x | P(x)\}$
- 文氏图

集合之间的关系

- 子集
- 集合相等
- 真子集

集合的势(基数)：集合中不同元素的多少

集合的幂集：集合S所有子集的集合

笛卡尔积

集合运算及运算性质

并、交、差、补集、对称差

重要运算性质

$$A - B = A \cap \bar{B}$$

集合恒等式

函数

函数的定义

一个从集合A到集合B的函数f: $A \rightarrow B$

$$\forall a(a \in A \rightarrow \exists b(b \in B \wedge f(a) = b))$$

A叫做定义域，B叫做伴域

如果 $f(a)=b$ ，那么a叫做b的原像，b叫做a的像

函数的类型

一对一函数

函数f称为一对一的或单射的，当且仅当对于f定义域中的所有的x,y, $f(x)=f(y)$

蕴含 $x=y$

也就是说，原像是唯一的

映上函数

从A到B的函数f叫做映上的或满射，当且仅当对每个 $b \in B$,有元素 $a \in A$ 使得 $f(a)=b$

一一对应函数

一一对应函数，或双射函数，指的是又是射又是满射的函数

逆映射

令f为从集合A到集合B的一一对应，f的反函数是这样的函数，它指派给B中元素y的是A中使得 $f(x) = y$ 唯一元素x。f的反函数用 f^{-1} 表示，于是在 $f(x) = y$ 时 $f^{-1}(y) = x$)

函数的复合

函数本质上是二元关系,所以可以象二元关系的复合那样来定义函数的复合.

定理: 设 $f: A \rightarrow B$, $g: B \rightarrow C$, 则

若f,g是满射, 则 $g \circ f$ 是满射。

若f,g是单射, 则 $g \circ f$ 是单射。

若f,g是一一映射, 则 $g \circ f$ 是一一映射。

集合的基数 Cardinality

有限集的基数就是有限集中元素的个数

集合等势

设A、B为任意两个集合，如果存在从A到B的双射，则称A与B等势

无限集可以与其真子集等势

定理：

- 等势关系是一个等价关系
- 无限集必与它的一个真子集等势（有限集与无限集的根本区别）

等势关系是一个等价关系，对每个等价类给出一个标志，该标志就是集合的势

与自然数集 N 的集合等势的集合势为 \aleph_0

与 $(0,1)$ 等势的集合的势为 \aleph

设 A, B 是两个集合，若 $A \subset B$ 且 A 与 B 的某子集等势，则称 A 的势小于 B 的势，记为 $|A| < |B|$.

用 $|A| \leq |B|$ 表示“ $|A|$ 小于或等于 $|B|$ ”

定理：

- $|A| \leq |B| \Leftrightarrow$ 存在 A 到 B 的单射
- 设 A, B, C 为任意集合，则
 - 1) $|A| \leq |A|$
 - 2) $|A| \leq |B|, |B| \leq |C| \Rightarrow |A| \leq |C|$
 - 3) $|A| \leq |B|, |B| \leq |A| \Rightarrow |A| = |B|$
- (三歧定理) 对任意集合 A 与 B ， $|A| < |B|$ ， $|B| < |A|$ ， $|A| = |B|$ 中恰有一个成立
- 对任意集合 A ，必有 $|A| < |2^A|$

第三部分 关系

关系的基本概念，表示方法

关系的基本概念

设 A, B 为任意两个集合，称笛卡儿积 $A \times B$ 的子集 R 为集合 A 到 B 的一个二元关系。若 $(x, y) \in R$ ，则称 x 与 y 有关系 R ，记为 xRy

- 关系 R 是一个集合

- $R \subseteq A \times B$

$$R = \{(a, b) | a \in A, b \in B, aRb\}$$

关系的表示方法

- 列出所有有序对
- 集合表示语言
- 二维表格
- 关系矩阵
- 有向图

关系的性质

自反、反自反、对称、反对称、传递

对称+传递->自反

关系的运算

关系是 $A \times B$ 的子集，可以按照两个集合组合的方式来组合两个A到B的关系

集合运算

交、并、补、差、对称差

通过关系矩阵运算

关系的合成

$$R = \{(a, b) | a \in A, b \in B, aRb\}$$

$$S = \{(b, c) | b \in B, c \in C, bSc\}$$

$$SoR = \{(a, c) | a \in A, c \in C, \exists b(b \in B \wedge aRb \wedge bSc)\}$$

$$SoR \neq RoS$$

如何计算？

- 定义
- 关系矩阵相乘

关系的幂

$$R^n = \begin{cases} R & \text{if } n=1 \\ R^{n-1} \circ R & \text{if } n>1 \end{cases}$$

定理

集合A上的关系R是传递的，当且仅当对 $n=1, 2, 3, \dots$ 有

$$R^n \subseteq R$$

关系的逆

$$R = \{(a, b) | a \in A, b \in B, aRb\}$$

$$R^{-1}(R^c) = (b, a) | (a, b) \in R, a \in A, b \in B$$

几个有关的运算律

$$(S \circ T)^{-1} = T^{-1} \circ S^{-1}$$

关系的闭包

自反闭包 Reflexive Closure

R是A上的关系，R的自反闭包，记作 $r(R)$

$$r(R) = R \cup I_A$$

如何计算自反闭包？主对角线上全改为1

$$R \text{ 是自反关系} \iff R = R \cup I_A$$

对称闭包 Symmetric Closure

R是A上的关系，R的对称闭包，记作 $s(R)$

$$s(R) = R \cup R^{-1}$$

$$R \text{ 是对称关系} \iff R = R \cup R^{-1}$$

传递闭包Transitive Closure

R的传递闭包是包含R的最小的具有传递性的关系

如何计算？

A为有限集， $|A|=n$ ，则

$$t(R) = \bigcup_{i=1}^n R_i$$

定理：R是集合A上的关系，则

- 若R是自反的，则 $s(R)$ 和 $t(R)$ 都是自反的
- 若R是对称的，则 $r(R)$ 和 $t(R)$ 都是对称的
- 若R是传递的，则 $r(R)$ 是传递的

$t(R) = R$. 关系R的传递闭包等于连通性关系R.

传递闭包的计算->沃舍尔算法

等价关系，等价类，划分

等价关系

满足下列三个条件的关系，称为等价关系

- 自反的
- 对称的
- 传递的

一些术语

a和b等价

$(a, b) \in R, R$ 是一个等价关系

x 关于 R 的等价类

R 为集合 A 上的等价关系，对于每个 $x \in A$ ，作集合

$$[x]_R = \{y \in A | xRy\}$$

等价类

R 是 A 上的等价关系， $a \in A$ ，一切与 a 等价的元素构成的 A 的子集，叫做 a 的 R -等价类，记作 $[a]_R$ 或 $[a]$

a 称为 $[a]_R$ 的代表元

R 是 A 上的等价关系， R 的所有等价类构成的集合叫做 A 对 R 的商集，记作 A/R

定理

1. 如果 R_1, R_2 是 A 上的等价关系，那么 $R_1 \cap R_2$ 也是 A 上的等价关系
2. 如果 R_1, R_2 是 A 上的等价关系，则 $R_1 \cup R_2$ 在 A 上有自反和对称的关系
3. 如果 R_1, R_2 是 A 上的等价关系，则 $(R_1 \cup R_2)^*$ 是 A 上的等价关系
4. R 是集合上的等价关系，则

$$aRb \iff [a] = [b] \iff [a] \cap [b] \neq \emptyset$$

划分

$\{A_1, A_2, \dots, A_n\}$ 是集合 A 的子集集合，该集合构成 A 的划分，当且仅当

- $A_i \neq \emptyset$
- $A_i \cap A_j = \emptyset$, when $i \neq j$
- A 中的任意元素 a ，存在 i 使得 $a \in A_i$

R 为集合 A 上的等价关系， R 的等价类构成 S 的划分

给定S的划分，存在等价关系R，以集合 A_i , $i=1, 2, \dots$ 作为它的等价类

n元素的集合上有多少个不同的等价关系

$$B(0) = B(1) = 1$$
$$B(n+1) = \sum_{k=0}^n C_n^k B(k), n \geq 1$$

偏序关系及偏序集

偏序关系

一个关系R是集合S上的偏序关系，则它满足：

- 自反的
- 反对称的
- 传递的

(S,R)叫做偏序集 poset或partial Ordering

可比与不可比

在偏序集(S,R)中，若元素a, b存在 aRb 或 bRa ，则称a,b可比

否则称a,b不可比

若偏序集中每一对元素都是可比的，那么S叫做全序集或线序集，R叫做全序或线序，一个全序也叫做链

字典序

词典排序是在两个偏序集的笛卡尔乘积上定义的偏序集。

哈塞图 Hasse Diagrams

用于描述偏序关系的一种方式

如何构造？

- 构造偏序关系的有向图
- 去掉所有的环
- 去掉冗余的边
- 一走所有有向边上的箭头

链和反链

偏序关系 (A, \leq) , $B \subseteq A$, 如果 (B, \leq) 是一个全序集, 则 B 叫做 (A, \leq) 的链
链的长度= $|B|$

$B \subseteq A$, 对于 B 中任意不同的两个元素 a, b , $(a, b), (b, a)$ 都不属于关系 \leq , 则 B 叫做 (A, \leq) 的反链

极大(Maximum)元和极小(Minimal)元

a 在偏序集 (A, \leq) 中是极大(小)的, 当不存在 $b \in A$, 使得 $a \leq b (b \leq a)$

最大(Greatest)元和最小(Least)元

a 是偏序集 (A, \leq) 中的最大元素, 当所有的 $b \in A$, 有 $b \leq a$, 最小元素类似
最大元, 最小元如果存在, 则是唯一的

上界和下界

A 为 S 的子集, 如果 a 是 S 的元素使得对所有元 $b \in A$, 有 $b \leq a$, 那么 a 叫做 A 的一个上界

下界定义类似

最小上界和最大下界

设 $\langle P, \leq \rangle$ 是偏序集, $A \subseteq P$, 若 a 是 A 的上界, 且对 A 的任意上界 b , 有 $a \leq b$, 则称 a 为 A 的最小上界(上确界), 若 a 是 A 的下界, 且对 A 的任意下界 b , 有 $b \leq a$, 则称 a 为 A 的最大下界(下确界)

良序集 Well-ordered Sets

偏序集 (A, R) ，若 A 的非空子集均有最小元，则称其为良序集

良序集一定是全序集，反之不然。

格 Lattices

如果一个偏序集的每对元素都有最小上界和最大下界，就称这个偏序集为格
所有的全序都是格，但并非所有的偏序集都是格

拓扑排序 Topological Sorting

从一个偏序构造一个相容的全序叫做拓扑排序

代数系统

运算

设 A 是一个集合， $A \times A$ 到 A 的映射称为 A 上的二元运算。一般地， A^n 到 A 的映射称为 A 上的 n 元运算。

运算的结果

设 f 是 A 上的 n 元运算，对任意的 $x_1, x_2, \dots, x_n \in A$ ， $f(\langle x_1, x_2, \dots, x_n \rangle)$ 称作 x_1, x_2, \dots, x_n 在 f 下的运算结果，并简记为 $f(x_1, x_2, \dots, x_n)$

运算封闭

设 f 是 A 上的 n 元运算， $S \subseteq A$ ，如果对 $x_1, x_2, \dots, x_n \in S$ ，恒有 $f(x_1, x_2, \dots, x_n) \in S$ ，则称 S 对运算 f 是封闭的。运算 f 在 S 上是封闭的。

运算表

有限集的运算可以用一个表来表示

运算律

结合律、交换律、左分配律、右分配律、左消去律、右消去律

代数系统

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

子代数系统

设 $\langle A, * \rangle$ 是代数系统, $S \subseteq A$, 如果 S 对 $*$ 封闭, 则称 $\langle S, * \rangle$ 为 $\langle A, * \rangle$ 的子代数.

单位元

掌握概念 左、右单位元, 单位元

定理: 设代数系统 $\langle A, \circ \rangle$ 中既有左单位元 e_l , 又有右单位元 e_r , 则 $e_l = e_r$.

推论: 代数系统 $\langle A, \circ \rangle$ 中的单位元如果存在, 则必定唯一.

逆元

逆元的概念

定理: 设 e 是代数系统 $\langle A, * \rangle$ 的单位元, $*$ 满足结合律, 如果 $a \in A$ 的左逆元 b 及右逆元 c 均存在, 则 $b = c$.

推论: 设 $\langle A, * \rangle$ 是有单位元的代数系统, $*$ 满足结合律. 如果 $a \in A$ 的逆元存在, 则必定唯一.

幂等元

设 $\langle A, * \rangle$ 是一个代数系统, 如果 $a \in A$ 满足 $a * a = a$, 称 a 为 A 的幂等元.

同态和同构

对 $\langle A, * \rangle, \langle B, \circ \rangle$, $f: A \rightarrow B$, 如果 f 保持运算, 即:

$$\forall x, y \in A \text{ 有 } f(x * y) = f(x) \circ f(y)$$

称 f 为 $\langle A, * \rangle$ 到 $\langle B, \circ \rangle$ 的同态映射(同态)

同态和同构

设 $\langle A, * \rangle$, $\langle B, \circ \rangle$ 为两个代数系统, $f: A \rightarrow B$ 为 A 到 B 的同态.

如果 f 是单射, 称 f 为单同态

如果 f 为满射, 称 f 为满同态, 称 B 是 A 在 f 下的同态象, 记为 $f: A \sim B$

如果 f 是双射, 称 f 为同构映射(同构), 这时称 A 与 B 在 f 映射下同构. 记为 $f: A \cong B$

定理

f 是 $\langle A, * \rangle$ 到 $\langle B, \cdot \rangle$ 的同态,

g 是 $\langle B, \cdot \rangle$ 到 $\langle C, \triangle \rangle$ 的同态, 则

$g \circ f$ 是 $\langle A, * \rangle$ 到 $\langle C, \triangle \rangle$ 的同态.

且当 f, g 均为单同态、满同态、同构时, $g \circ f$ 也必是单同态、满同态、同构.

满同态保持结合律、交换律、单位元、逆元、幂等元

自同态, 自同构

设 $\langle A, * \rangle$ 为一个代数系统, $\langle A, * \rangle$ 到自身的同态称为 A 的自同态, $\langle A, * \rangle$ 到自身的同构称为 A 的自同构

半群

满足结合律的代数系统叫做半群

半群的运算通常叫做乘法

a^n 表示 n 个 a 做运算的结果

半群满足指数律

$$\begin{aligned}a^m a^n &= a^{m+n} \\ (a^m)^n &= a^{mn}\end{aligned}$$

可交换半群

满足交换律的半群

可交换半群中有另一指数律:

$$(ab)^n = a^n b^n$$

可交换半群中的运算常用加法记号表示

指数律形式

$$\begin{aligned}ma + na &= (m + n)a \\ m(na) &= (mn)a\end{aligned}$$

么半群

有单位元的半群

用加法记号时, 单位元常用0表示, 称为零元

么半群若存在逆元, 由于满足结合律, 其逆元必唯一

么半群中, 用 a^{-1} 表示 a 的唯一逆元

当采用加法记号时, 逆元常记作 $-a$, 叫做 a 的负元

子半群

设 $\langle S, \circ \rangle$ 为一半群, 若 $T \subseteq S$ 在 S 的运算 \circ 下也构成半群, 则称 $\langle T, \circ \rangle$ 为 $\langle S, \circ \rangle$ 的子半群.

实际上, 只要 $T \subseteq S$ 对运算 \circ 封闭, 则 $\langle T, \circ \rangle$ 即为 $\langle S, \circ \rangle$ 的子半群

$\langle S, * \rangle$ 有单位元 e , $\langle S, * \rangle$ 的子半群未必有单位元, 即使有的话, 也未必等于 e

设 S 是么半群, 若 T 是 S 的子半群, 且 S 的单位元 $e \in T$, 则称 T 是 S 的子么半群.

群

群的相关概念

设 $\langle G, * \rangle$ 为么半群，如果 $\forall a \in G$ ， a 的逆元 a^{-1} 均存在，则称 $\langle G, * \rangle$ 为群。

一个代数系统 $\langle G, * \rangle$ 满足下列条件，则称之为群：

- 结合律成立 (半群)
- G 中具有单位元 (么半群)
- G 中任意元素 a ，都存在 $a^{-1} \in G$ 是 a 的逆元

有限群

当群 G 中只含有有限个元素时，称其为有限群，否则称其为无限群

有限群 G 的元素个数称为群 G 的阶，并规定无限群 G 的阶为 ∞ 。群 G 的阶也记为 $|G|$ 。

交换群

满足交换律的群叫做交换群，也叫做Abel群

群的基本性质

定理1：重点

设 $\langle G, * \rangle$ 为群，则

- (1) G 中消去律成立.
- (2) 单位元 e 是 G 中唯一幂等元

定理2：

设 $\langle G, * \rangle$ ， $\langle H, \circ \rangle$ 是群， f 是 G 到 H 的同态。若 e 为 G 的单位元，则 $f(e)$ 为 H 的单位元，且 $\forall a \in G$ ，有

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

定理3:

设 $\langle G, * \rangle$ 是群, $\langle H, \circ \rangle$ 是任意代数系统, 若存在 G 到 H 的满同态, 则 $\langle H, \circ \rangle$ 必为群.

证明: 满同态保持结合律, 交换律, 单位元, 逆元

定理4:

设 $\langle G, * \rangle$ 是一个半群, 且

(1) G 中有一左单位元 e , 使任意 G 中元素 a

$$ea = a$$

(2) G 中任一元素 a , 均有一“左逆元”

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

则 G 为群

证明: 证明左逆元也是右逆元, 再证明左单位元也是右单位元

定理5:

设 $\langle G, * \rangle$ 是半群, 如果 $\forall a, b \in G$, 方程

$$ax = b$$

$$ya = b$$

在 G 中总有解, 则 G 是群

定理6:

满足消去律的有限半群必为群

定理7:

有限群的运算表中，每一行(列)都是G中元素的一个全排列

子群与元素的周期

子群的相关概念

设 $\langle G, * \rangle$ 是一个群， $H \subseteq G$ ，如果H在G的运算下也构成群，则称 $\langle H, * \rangle$ 为 $\langle G, * \rangle$ 的子群。

任何群G都有两个平凡子群： $\{e\}$ ， G ，其它子群称为真子群。

子群相关性质

定理1：

设H是群G的子群，则H的单位元 e' 就是G的单位元 e 。对 $a \in H$ ， a 在H中的逆元 a' 就是 a 在G中的逆元 a^{-1} 。

定理2：

H是群 $\langle G, * \rangle$ 的非空子集，则H是G的子群 当且仅当

- $\forall a, b \in H$ 有 $a * b \in H$
- $\forall a \in H$ ， a 在G中的逆元 $a^{-1} \in H$ 。

推论：

设 $\langle G, * \rangle$ 为群，S是G的非空子集，则

S是G的子群 $\Leftrightarrow \forall a, b \in S$ $a * b^{-1} \in S$ 。

元素的周期

设G是群， $a \in G$ ，若存在正整数n，使 $a^n = e$ ，则将满足该条件的最小正整数n称为a的周期（阶），若这样的n不存在，称a的周期为 ∞ 。

表示方法：

用 $|a|$ 表示a的周期（阶）。并将周期（阶）为n的元素称为n阶元素

元素周期的性质

定理：

设 G 是一个群， $a \in G$ ，

(1) a 的周期等于 a 生成的循环子群 $\langle a \rangle$ 的阶，即

$$|a| = |\langle a \rangle|$$

(2) 若 a 的周期为 $n < \infty$ ，则

$$a^m = e \Leftrightarrow n | m.$$

推论：

设 G 为群， $a \in G$ ，若 a 的周期为 n （或等价地说 $\langle a \rangle$ 的阶为 n ），则

$$\langle a \rangle = \{a^0, a^1, \dots, a^{n-1}\}$$

循环群

循环群相关概念

设 G 是一个群，如果存在 $a \in G$ ，使 $G = \langle a \rangle = \{a^i \mid i \in \mathbb{Z}\}$ ，称 G 为由 a 生成的循环群， a 称为其生成元。

循环群相关性质

定理1：

设 $\langle G, * \rangle$ 是一个循环群，若 G 是无限群，则

$$\langle G, * \rangle \cong \langle \mathbb{Z}, + \rangle$$

若 G 是 n 阶群，则

$$\langle G, * \rangle \cong \langle \mathbb{Z}_n, +_n \rangle$$

定理2：循环群的子群必为循环群

定理3: 设 $\langle G, * \rangle$ 是 n 阶循环群, m 是正整数且 $m \mid n$, 则 G 中存在唯一一个 m 阶子群.