群与子群

离散数学一代数结构

南京大学计算机科学与技术系

内容提要

- 群的定义
- 群方程及其解
- 群与消去律
- 群中元素的阶
- 子群的定义及其判定
- 有限群的子群的判定
- 拉格朗日定理

群的定义

- 满足下列性质的代数系统(S, ∘ , *e*) 称为群:
  - ∘ 是S上的二元运算，满足结合律
    - 对任意 $x, y, z \in S$，$(x \circ y) \circ z = x \circ (y \circ z)$
  - *e*是单位元素
    - 对任意 $x \in S$, $e \circ x = x \circ e = x$ //单位元素有时记为1_S
  - 每个元素均有逆元素
    - 对任意 $x \in S$,存在S中的元素x^*， $x \circ x^* = x^* \circ x = e$
    - // 称x^*是x的逆元素，一般记为x^{-1}
- 如果还满足交换律：交换群(阿贝尔群)

群的例子

- **整数加群: (Z,+)**
  - 加法可结合；单位元素0；a的逆元素为$(-a)$
- **剩余加群: $(Z_n, +_n)$ $(n\geq 2)$**
  - $Z_n=\{0,1,2,\ldots,n-1\}$, $a+_n b$=<$a+b$除以n的余数>
  - 剩余加满足结合律；0是单位元；
  - 任何元素均可逆
    - 0的逆元素为0
    - a的逆元素为n-a (a=1,…n-1)

群的例子

- 非零实数乘法群: (*R*-{0},•)
  - 乘法可结合；单位元素1；*x*的逆元素为1/*x*
  - 注意：实数集与乘法不构成群
- 每行每列恰好有一个1，其它元素均为0的所有n×n阶矩阵 以及矩阵乘法构成群
  - 矩阵乘法可结合；
  - 单位元是主对角元素全为1而其它元素全为0的矩阵；
  - 根据线性代数知识可知这样的矩阵是可逆矩阵。

集合上的置换

- 在集合{1,2,3}上可以定义6个一一对应的函数:

$$e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\quad \alpha=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\quad \beta=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

$$\gamma=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\quad \delta=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\quad \varepsilon=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

有限集合上的一一对应的函数称为置换。

群S_3

- $<\{e,\alpha,\beta,\gamma,\delta,\varepsilon\}, \circ>$构成群，其中“∘”是函数复合。

$\circ$	e	α	β	γ	δ	ε
e	e	α	β	γ	δ	ε
α	α	β	e	δ	ε	γ
β	β	e	α	ε	γ	δ
γ	γ	ε	δ	e	β	α
δ	δ	γ	ε	α	e	β
ε	ε	δ	γ	β	α	e

运算表

例如：

$\delta\circ\gamma(1) = \gamma(\delta(1)) = \gamma(3) = 2$

$\delta\circ\gamma(2) = \gamma(\delta(2)) = \gamma(2) = 3$

$\delta\circ\gamma(3) = \gamma(\delta(3)) = \gamma(1) = 1$

即：$\delta\circ\gamma = \alpha$

群方程及其解

- 群方程：
  - $a \circ x = b$ 和 $y \circ a = b$ 称为群方程
- 群方程的解：
  - $\mathbf{a \circ x = b \Rightarrow a \circ (a^{-1} \circ b) = b}$
  - $\mathbf{y \circ a = b \Rightarrow (b \circ a^{-1}) \circ a = b}$
- 群方程的解是唯一的
  - 假设$\mathbf{a \circ x_1 = b = a \circ x_2}$
  - 等号两边同时左乘$\mathbf{a^{-1}}$, 得 $\mathbf{x_1 = a^{-1} \circ b = x_2}$

群的第二定义

- 代数系统(G, ∘)满足结合律，且形如a∘x=b 和 y∘a=b 的方程均有唯一解，则(G, ∘)是群。
- 证明要点

(1) 任取G中的元素b, y∘b=b 有唯一解，设为e, 易证e是(G,∘)中的*左单位元素*：对任意的a∈G，b ∘x=a有唯一解，设为c，则 e∘a= e∘b∘c= b∘c=a

(2) 对任意的a∈G，y∘a=e有唯一解，记为a'(*"准左逆元素"*)

(3) 则a'也是a的 *"准右逆元素"*：y∘a'=e有唯一解，设为a", 则 a∘a'= e∘(a∘a')= (a"∘a')∘(a∘a')=e

(4) e也是*右单位元素*：对任意的a∈G，a∘e= a∘(a'∘a)=a

综合(1)-(4), e是(G,∘)的单位元素，而任意元素a的逆元素即a'

群与消去律

- 群满足消去律：
  - 设(G, ∘)是群，对任意a,b,c∈G

    若a∘b=a∘c, 则b=c

    若b∘a=c∘a, 则b=c
- 正整数集与普通乘法构成的代数系统满足结合律和消去律，但它*不是*群。

有限群与消去律

- **设G是有限集合，代数系统(G, ∘)满足结合律和消去律，则(G, ∘)是群**
  - **证明要点：**

设$G=\{a_1,a_2,a_3,\ldots,a_n\}$，对G中任意给定的元素$a_i$,考虑集合$a_iG=\{a_i\circ a_1, a_i\circ a_2, a_i\circ a_3, \ldots, a_i\circ a_n\}$。注意$a_iG$是G的子集（运算封闭），同时又与G等势（消去律），所以：$a_iG=G$。这意味着方程$a\circ x=b$ 有唯一解。(*Why?*)

类似地可证方程$y\circ a=b$也有唯一解。

因此：(G, ∘)是群

群G中元素a的阶

- 元素的乘幂：
  - $a^0 = e$ （e是单位元素）
  - $a^{n+1} = a^n \circ a$ (n是非负整数)
  - $a^{-k} = (a^{-1})^k$ (k为正整数)
- 定义：
  - 等式 $a^k = e$ 成立的最小正整数k称为a的阶（周期），记为$|a|=k$。如果这样的k不存在，a为无限阶元。

群G中元素*a*的阶（性质）

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

有限群的运算表

- 回顾“逻辑或”与“布尔和”的运算表

∨	F	T
F	F	T
T	T	T

+	0	1
0	0	1
1	1	1

  - 如果不考虑符号的形式及其含义，则两者没有差别。
- 群表中的每行或每列均为群中所有元素的一种排列。
  - 有一行和一列与标题行/列相同

子群的定义

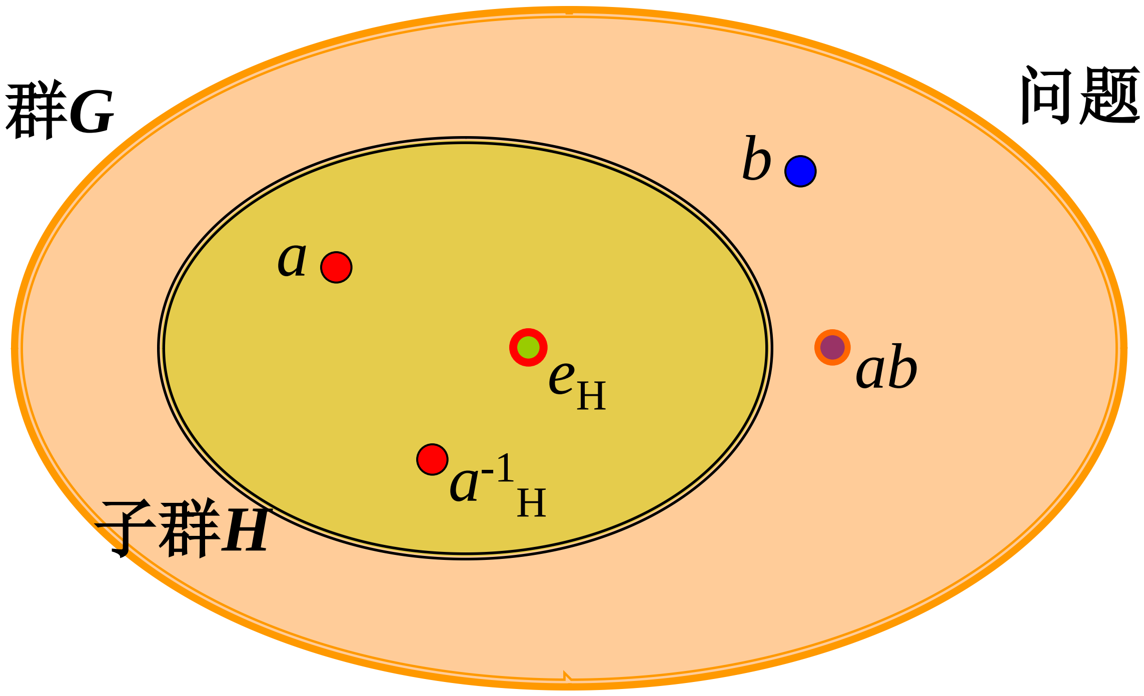
- 设(G, ∘)是群，H是G的非空子集，如果H关于G中的运算构成群，即(H, ∘)也是群，则H是G的子群。
  - 记作(H, ∘) ≤ (G, ∘), 简记为 H≤G。
- 例子：偶数加系统是整数加群的子群
- 平凡子群

注意：结合律在G的子集上均成立。

关于子群定义的进一步思考

问题1：e_H是否一定是e_G?　　$e_H\, e_H = e_H \rightarrow e_H = e_G$

问题2：*ab*应该在哪儿?



子群的判定

- **G是群，H是G的非空子集。H是G的子群当且仅当：**

  $\forall a,b \in H,\ ab^{-1} \in H$

- 证明
  - 必要性易见
  - 充分性：
    - 单位元素：因为**H**非空，任取**$a \in H$, $e = aa^{-1} \in H$**
    - 逆元素：**$\forall a \in H$**, 因为**$e \in H$**, 所以 **$a^{-1} = ea^{-1} \in H$**
    - 封闭性：**$\forall a,b \in H$**, 已证**$b^{-1} \in H$**，所以**$ab = a(b^{-1})^{-1} \in H$**

子群的判定 – 有限子群

- G是群，H是G的非空有限子集。H是G的子群当且仅当：

  $\forall a,b \in H,\ ab \in H$

- 证明. 必要性显然. 下证充分性，只须证明逆元素性
  - 若H中只含G的单位元，H显然是子群。
  - 否则，任取H中异于单位元的元素a, 考虑序列

    $a, a^2, a^3, \ldots$

    注意：该序列中各项均为有限集合H中的元素，因此，必有正整数i, j(j>i), 满足：$a^i=a^j$, 因此：

    $a^{-1}=a^{j-i-1} \in H$

生成子群

- **设G是群，$a \in G$，构造G的子集H如下：**

$$H = \{a^k \mid k\text{是整数}\}$$

则H构成G的子群，称为a生成的子群 $\langle a \rangle$

- **证明：**
  - **H非空：a在H中**
  - **利用判定定理：**

$$\forall a^m, a^n \in H,\ a^m(a^n)^{-1} = a^{m-n} \in H$$

群的中心

- 设G是群，构造G的子集C如下：

$$C = \{ a \in G \mid \forall x \in G,\ ax=xa \}$$

则C构成G的子群，称为G的中心

证明：

- C非空：单位元在C中
- 利用判定定理二：即证明对任意的a,b∈C, (即ax=xa, bx=xb对G中一切x成立)，

$$(ab^{-1})x=x(ab^{-1}) \text{ 也对G中一切x成立}$$

$$(ab^{-1})x = a(b^{-1}(x^{-1})^{-1}) = a(x^{-1}b)^{-1} = a(bx^{-1})^{-1} = a(xb^{-1}) = x(ab^{-1})$$

左(右)陪集及其表示

- **若H是群G的一个子群，a是G中的任意一个元素，定义集合aH如下：**

$$aH=\{ah|h\in H\}$$

- **aH称为H的一个左陪集**
  - **由群的封闭性可知，aH也是G的子集**
  - **($\forall h\in H.\ ah\in H$)当且仅当$a\in H$**
- **相应地可定义右陪集**

陪集的例子

- 设（I, +）是整数加群，I_3={…-3, 0, 3, 6, 9,…}是一个子群，则$2I_3$={… -1, 2, 5, 8, 11,…}是一个左陪集。

注意：实际上$2I_3=5I_3$。

- S_3={(1), (12),(13),(23),(123),(132)}, H={(1),(12)}是一个子群，(13)H={(13), (132)}是一个左陪集。

注意: (13)H≠H(13)={(13)(123)}

陪集与划分

- 设H是群G的子群，则H的所有左陪集构成G的划分
  - G中任意元素a一定在某个左陪集中：$a \in aH$
  - $\forall a,b \in G$, $aH=bH$或者$aH \cap bH=\varnothing$
    - 假设$aH \cap bH \neq \varnothing$, 即存在$c \in aH \cap bH$, 令$c=ah_1=bh_2$,
    - 则$a=bh_2h_1^{-1}$, 从而$aH \subseteq bH$，
    - 同理可得：$bH \subseteq aH$. 所以 $aH=bH$
- 注意：a, b属于同一左陪集

  $\Leftrightarrow$ $a \in bH$且$b \in aH$

  $\Leftrightarrow$ $b^{-1}a \in H$

拉格朗日定理

- 每个左陪集与相应的子群等势
  - 对任意的左陪集aH, f :H→aH

    ∀h∈H, f(h)=ah是双射
- 拉格郎日定理-有限群的子群的一个必要条件
  - 设G是有限群，H是G的子群，则|H|能整除|G|
- 注意：对有限群，每个陪集元素个数有限且相同，并等于|H|, 于是|G|=k|H|, k是左陪集的个数，称为H在G中的指数，记为[G:H]

拉格朗日定理的重要推论

- 有限群G中任何元素的阶一定是|G|的整除因子
  - 注意：$|\langle a\rangle|$=a的阶
- 若G是质数阶的群，则必有$a\in G$, 满足：$\langle a\rangle=G$
  - 除单位元素外，G中任何元素的生成子群即G本身

拉格朗日定理推论的应用

- 6阶群G必含3阶子群
- 证明
  - 如果G中有6阶元素a, 则b=aa是3阶元素，因此⟨b⟩是3阶子群
  - 如果G中没有6阶元素，则根据拉格朗日定理的推论，G中元素的阶只可能是1,2或3。
    - 如果也没有3阶元素，即$\forall x \in G$, $x^2=e$, 因此， $\forall x, y \in G$, $xy=(yx)^2(xy)=yx$, 即G是可交换群。因此{e,a,b,ab}构成4阶子群，但4不能整除6，这与拉格朗日定理矛盾。
  - 所以G中必含3阶元素*a*, 即由*a*生成的子群是3阶子群。

作业

- pp.202-204
  - 15-22
  - 24