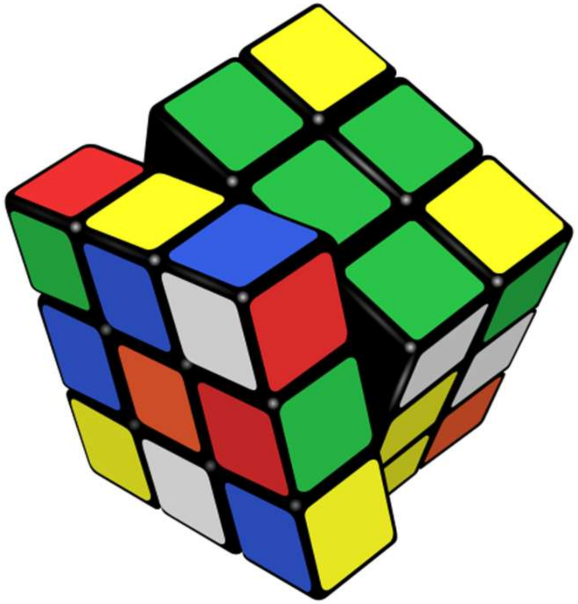
代数系统（三）

子群和群论基本定理

南京大学计算机科学与技术系

内容提要

- 子群的定义及其判定
- 生成子群与元素的阶
- 子群的陪集与划分
- 拉格朗日定理
- 拉格朗日定理的推论



子群的定义

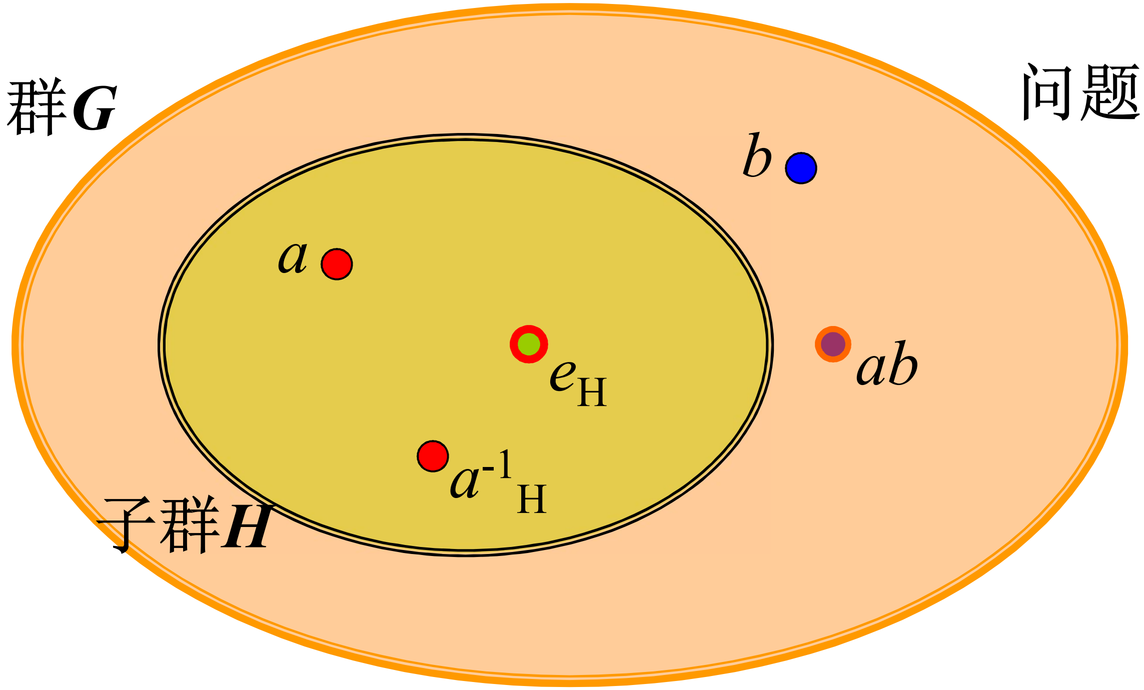
- 设$(G, \circ)$是群，H是G的非空子集，如果H关于G中的运算构成群，即$(H, \circ)$也是群，则H是G的子群。
  - 记作$(H, \circ) \le (G, \circ)$, 简记为 $H \le G$。
- 例子：偶数加系统是整数加群的子群
- 平凡子群 $(G, \circ)$，$(\{e\}, \circ)$

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 – 判定定理一

- **G**是群，**H**是**G**的非空子集。**H**是**G**的子群当且仅当：
  - $\forall a,b\in H,\ ab\in H$, 并且
  - $\forall a\in H,\ a^{-1}\in H$

（注意：这里a^{-1}是a在**G**中的逆元，当**H**确定为群后，它也是a在**H**中的逆元）

- 证明
  - 必要性显然（注意群中逆元素的唯一性）
  - 充分性：只须证明**G**中的单位元也一定在**H**中，它即是**H**的单位元素。

子群的判定－判定定理二

- **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：

$$\mathrm{H} = \{a^k \mid k\text{是整数}\}$$

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
  - 利用判定定理二：

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

群中元素的阶

- 定义（元素的阶）

设$(G, *)$为群，$n \in Z$，$a \in G$，以下定义a^n:

若$n \geq 0$，则a^n已在上讲定义。

若$n < 0$，则$a^n = (a^{-n})^{-1}$。

若$(\exists n \in \mathbb{N}^+)(a^n = e)$，则称$a$的阶(order)是有穷的且记$a$的阶$|a| = min\{n > 0 \mid a^n = e\}$。

若$\neg(\exists n \in \mathbb{N}^+)(a^n = e)$，则称$a$的阶是无穷的，且记$a$的阶$|a| = \infty$。

性质:

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

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

群中元素的阶（续）

- 例

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

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

在$(\mathbb{Z}_6, +_6)$中，$|0| = 1$

元素	0	1	2	3	4	5
阶	1	6	3	2	3	6

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

群中元素的阶（续）

- 定理（元素的阶的性质）

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

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

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

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

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

群中元素的阶（续）

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

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

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

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

$\therefore a^r = e$

$\because r < m$

$\therefore r = 0$，从而$k = q \times m$，故$m \mid k$。

"$\Leftarrow$"，设$|a| = r$

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

群中元素的阶（续）

(2)令$|a|=r$

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

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

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

Case 1: ab的阶有穷，设为r

从而$(ab)^{r+1}=a(ba)^r b$

从而$ab=a(ba)^r b$，故$(ba)^r=e$

故ba的阶有穷，设为r'，由(1)知$r' \mid r$

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

因此$|ab|=|ba|$.

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

群中元素的阶（续）

-
- 例题：设$\langle G,*\rangle$为群，试证明：若$|G|=n$，则

  G中阶大于2的元素有偶数个

证明：

对于$a\in G$，若$|a|>2$，则$a\neq a^{-1}$，若不然，则$a=a^{-1}$，从而$a^2=e$，故$|a|\leq 2$与$|a|>2$矛盾！因此我们有$|a|>2\rightarrow a\neq a^{-1}$，故$G$中阶$>2$的元素$a$与其逆$a^{-1}$成对出现，因此$G$有偶数个阶$>2$的元素。

群的中心

- 设G是群，构造G的子集C如下：

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

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$a, b \in C$, (即$ax=xa$, $bx=xb$对G中一切x成立)，

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

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

左(右)陪集及其表示

- 若**H**是群**G**的一个子群，$\boldsymbol{a}$是**G**中的任意一个元素，定义：$\boldsymbol{a}\mathbf{H} = \{\, \boldsymbol{ah} \mid \boldsymbol{h} \in \mathbf{H} \,\}$
- $\boldsymbol{a}\mathbf{H}$称为**H**的一个左陪集
  - 由群的封闭性可知，$\boldsymbol{a}\mathbf{H}$也是**G**的子集
  - $\forall \boldsymbol{h} \in \mathbf{H}.\ \boldsymbol{ah} \in \mathbf{H}$ *iff* $\boldsymbol{a} \in \mathbf{H}$
- 相应地可定义右陪集

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：$a \in a\mathrm{H}$
  - $\forall a,b \in \mathrm{G}$, $a\mathrm{H}=b\mathrm{H}$或者$a\mathrm{H}\cap b\mathrm{H}=\varnothing$
    - 假设$a\mathrm{H}\cap b\mathrm{H}\neq\varnothing$, 即存在$c\in a\mathrm{H}\cap b\mathrm{H}$, 令$c=ah_1=bh_2$,
    - 则$a=bh_2h_1^{-1}$, 从而$a\mathrm{H}\subseteq b\mathrm{H}$，
    - 同理可得： $b\mathrm{H}\subseteq a\mathrm{H}$. 所以 $a\mathrm{H}=b\mathrm{H}$
- 注意：a, b属于同一左陪集

  iff $a\in b\mathrm{H}$且$b\in a\mathrm{H}$

  iff $b^{-1}a\in\mathrm{H}$

陪集与划分（续）

-
- 定理（陪集与划分）：设$\langle H,*\rangle < \langle G,*\rangle$，

(1) $eH = H$

(2) $\cup\{aH|a \in G\} = G$

(3) $\forall a,b \in G$，$aH = bH$ 或者 $aH \cap bH = \emptyset$

(4) $\{aH|a \in G\}$为$\boldsymbol{G}$之划分

陪集与划分（示例）

- 令$H = \{2n|n \in \mathbb{Z}\}$，$\langle H, +\rangle < \langle \mathbb{Z}, +\rangle$，$a \in \mathbb{Z}$，

  $aH = \{2n + a|n \in \mathbb{Z}\}$，$(2k)H = H$，

  $(2k+1)H = \mathbb{Z} - H$，$\{0H, 1H\}$$\mathbb{Z}$的一个划分。

- $\langle \mathbb{Z}_6, \oplus_6\rangle$为群，令$H = \{0,3\}$，$\langle H, \oplus_6\rangle < \langle \mathbb{Z}_6, \oplus_6\rangle$

  ，$H0 = H$，$H1 = \{1,4\}$，$H2 = \{2,5\}$

  $H3 = H, H4 = \{4,1\} = H1, H5 = \{5,2\} = H2$

  $\{H0, H1, H2\}$是$\mathbb{Z}_6$的一个划分。

左陪集关系

- 设H是群G的子群，定义G上的二元关系R如下：
  $\forall a,b\in G$, $(a,b)\in R$当且仅当$b^{-1}a\in H$
- R是G上的等价关系
  - 自反性：$\forall a\in G$, $a^{-1}a=e$
  - 对称性：注意$a^{-1}b=(b^{-1}a)^{-1}$
  - 传递性：如果$b^{-1}a\in H$, $c^{-1}b\in H$, 则
    $$c^{-1}a=c^{-1}(bb^{-1})a=(c^{-1}b)(b^{-1}a)\in H$$
- $[a]_R=aH$：$x\in[a]_R \Leftrightarrow aRx \Leftrightarrow x^{-1}a=h\in H \Leftrightarrow x=ah^{-1}\in aH$

Lagrange 定理

- 引理（陪集的势）

  设$\langle H,*\rangle < \langle G,*\rangle$，$a \in G$，则$H \approx aH \approx Ha$

- 证明：

  令$\sigma: H \to aH$为$\sigma(h) = ah$，由消去律可知

  τ, σ为1-1，易见σ亦为满射，故$H \approx aH$。

  同理可证$H \approx Ha$。

Lagrange 定理（续）

- $\{aH \mid a \in G\}$ 是G的一个划分。
- 对有限群G，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（右）陪集的个数，称为H在G中的指数，记为$[G:H]$

Lagrange 定理（续）

- Lagrange定理：设$\langle G,*\rangle$为有限群，$\langle H,*\rangle < \langle G,*\rangle$，则 $|G| = |H| \cdot [G:H]$

- 证明：由于$|G|$有穷，故$[G:H]$有穷且设为N，从而有$a_1,\cdots,a_N \in G$使$\{a_iH|1 < i \leq N\}$为G之划分，故$G = \cup_{i=1}^{N} Ha_i$；由引理，对任意i,j，$|Ha_i| = |Ha_j| = |H|$ $\therefore |G| = |H| \cdot N$即$|G| = |H| \cdot [G:H]$. □

Lagrange 定理（续）

- 推论1：设$\langle G,*\rangle$为有限群，$a \in G$，则$|a|$为$|G|$的因子。

- 证明*：$\because \big\langle \langle a\rangle,* \big\rangle \le \langle G,*\rangle \therefore |\langle a\rangle|$为$|G|$的因子，又由于$|a|$有穷，故$|\langle a\rangle| = |a|$，故$|a|$为$|G|$的因子. $\square$

Lagrange 定理（续）

- **推论2***：设$\langle G,*\rangle$为p阶群，若p为质数，则

$(\exists a \in G)(\langle a\rangle = G)$

证：设$|G| = p$为素数，可以取$a \neq e$，$a \in G$,由上推论知

$|\langle a\rangle|$为$|G|$的因子，$\because |\langle a\rangle| \geq 2 \ \therefore |\langle a\rangle| = p$

故$G = \langle a\rangle$

拉格朗日定理的应用

- **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$\langle b\rangle$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**。
    - 如果没有**3**阶元素，即$\forall x\in G$, $x^2=e$, 那么$\forall x, y\in G$, $xy=(yx)^2(xy)=yx$, 即**G**是交换群。
    - 因此$\{e,a,b,ab\}$构成**4**阶子群，但**4**不能整除**6**，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。