信息安全数学基础

第二部分 第八章 群

中山大学 信息科学与技术学院 计算机科学系

5. 子群

定理

设$(\mathbb{G},\cdot)$是一个群. H是$\mathbb{G}$的子集. 如果H中的元素也能按照运算$\cdot$满足群的定义, 则群$(H,\cdot)$称为$(\mathbb{G},\cdot)$的子群*(subgroup)*, 记作$H\leq\mathbb{G}$.

例如: 已知$(\mathbb{Z},+)$是一个群, 令

$$\mathbb{H}_2=\{\text{全体偶数}\}=\{2k|k\in\mathbb{Z}\}\subseteq\mathbb{Z},$$

很容易验证这个集合对$(\mathbb{Z},+)$中的运算$+$也构成群. 所以$H_2\leq\mathbb{Z}$.
事实上,

$$\mathbb{H}_m=\{mk\ :\ k\in\mathbb{Z}\}\subseteq\mathbb{Z}$$

对$(\mathbb{Z},+)$中的运算$+$都构成群, 所以都有$H_m\leq\mathbb{Z}$.

平凡子群和子群的单位元

- 平凡子群
  仅有一个单位元构成的集合e也是$\mathbb{G}$的子集, 这个子集对$(\mathbb{G},\cdot)$中的运算$\cdot$也构成群, 即为$(\mathbb{G},\cdot)$的子群.
  另外, $(\mathbb{G},\cdot)$本身当然也是$(\mathbb{G},\cdot)$的子群.
  这两个子群称为是$(\mathbb{G},\cdot)$的平凡子群.

- 设H是G的子群, 则H的单位元就是G的单位元.

  证明: 设子群的单位元为e', G的单位元为e,
  对于H中的任意元素$x: e'\cdot x = x$
  这个x自然也属于G中: $e\cdot x = x \Longrightarrow e'\cdot x = e\cdot x$.
  群中元素都有逆元(或者使用群的消去律): $e' = e$ $\diamond$

子群的判断

定理

设H是群G的非空子集, 则如下三个命题等价:

1. H是G的子群.
2. 对于任意$a, b \in H$, 有$ab \in H$和$a^{-1} \in H$.
3. 对于任意$a, b \in H$, 有$ab^{-1} \in H$.

证明:

$(1 \to 2)$: 由定义.

$(2 \to 3)$: 对于任何$a, b \in H$, 由(2)得$b^{-1} \in H$和$ab^{-1} \in H$..

$(3 \to 1)$: 应用(3)可得$aa^{-1} = e \in H$, 所以H中有单位元.

应用(3)可得$a^{-1} = ea^{-1} \in H$, 所以每个元素在H中有逆元.

子群的判断

定理

设H是群G的非空子集, 则如下三个命题等价:

1. H是G的子群.
2. 对于任意$a, b \in H$, 有$ab \in H$和$a^{-1} \in H$.
3. 对于任意$a, b \in H$, 有$ab^{-1} \in H$.

证明:

$(1 \to 2)$: 由定义.

$(2 \to 3)$: 对于任何$a, b \in H$, 由(2)得$b^{-1} \in H$和$ab^{-1} \in H$..

$(3 \to 1)$: 应用(3)可得$aa^{-1} = e \in H$, 所以H中有单位元.

应用(3)可得$a^{-1} = ea^{-1} \in H$, 所以每个元素在H中有逆元.

于是, 对于任意$a, b \in H$, 有$a(b^{-1})^{-1} = ab \in H$.

子群的判断

定理

设H是群G的非空子集, 则如下三个命题等价:

1. H是G的子群.
2. 对于任意$a, b \in H$, 有$ab \in H$和$a^{-1} \in H$.
3. 对于任意$a, b \in H$, 有$ab^{-1} \in H$.

证明:

$(1 \to 2)$: 由定义.

$(2 \to 3)$: 对于任何$a, b \in H$, 由(2)得$b^{-1} \in H$和$ab^{-1} \in H$..

$(3 \to 1)$: 应用(3)可得$aa^{-1} = e \in H$, 所以H中有单位元.

应用(3)可得$a^{-1} = ea^{-1} \in H$, 所以每个元素在H中有逆元.

于是, 对于任意$a, b \in H$, 有$a(b^{-1})^{-1} = ab \in H$.

定理

如果H是群G的有限子集, 且对于任何$a, b \in H$都有$ab \in H$, 则H是G的子群.

子群的交集

定理

设G是一个群, $\{H_i\}_{i\in I}$是G的一族子群, 则$\bigcap_{i\in I} H_i$是G的一个子群.

证明: 对于任意的$a, b \in \bigcap_{i\in I} H_i$, 有

$$a, b \in H_i, i \in I.$$

因为H_i是G的子群,所以, 由上述定理可得

$$ab^{-1} \in H_i, i \in I,$$

进而$ab^{-1} \in \bigcap_{i\in I} H_i$, 再由子群的判断定理可知$\bigcap_{i\in I} H_i$是$G$的一个子群.

$\mathbb{Z}_p^*$的q阶子群

乘法子群: 设G是一个乘法群. 如果G的一个子集合G'本身也构成一个乘法群, 那么称G'是G的子群. 特别地, 如果$|G'| = q$, 则也称G'是G的q阶子群.

$\mathbb{Z}_p^*$的q阶子群

乘法子群: 设G是一个乘法群. 如果G的一个子集合G'本身也构成一个乘法群, 那么称G'是G的子群. 特别地, 如果$|G'| = q$, 则也称G'是G的q阶子群.

- $\mathbb{Z}_7 \setminus \{0\} = \{3^0 = 1, 3^2 = 2, 3^1 = 3, 3^4 = 4, 3^5 = 5, 3^3 = 6\}$关于模7的乘法运算构成一个乘法群. 可以验证, $\mathbb{Z}_7 \setminus \{0\}$的子集合

$$\{2^0 = 1, 2^1 = 2, 2^2 = 4\}$$

关于模7的乘法运算也构成一个乘法群, 它被称为$\mathbb{Z}_7 \setminus \{0\}$的一个乘法子群.

乘法子群: 设G是一个乘法群. 如果G的一个子集合G'本身也构成一个乘法群, 那么称G'是G的子群. 特别地, 如果$|G'| = q$, 则也称G'是G的q阶子群.

- $\mathbb{Z}_7 \setminus \{0\} = \{3^0 = 1, 3^2 = 2, 3^1 = 3, 3^4 = 4, 3^5 = 5, 3^3 = 6\}$关于模7的乘法运算构成一个乘法群. 可以验证, $\mathbb{Z}_7 \setminus \{0\}$的子集合

$$\{2^0 = 1, 2^1 = 2, 2^2 = 4\}$$

  关于模7的乘法运算也构成一个乘法群, 它被称为$\mathbb{Z}_7 \setminus \{0\}$的一个乘法子群.
- $\mathbb{Z}_{11} \setminus \{0\}$关于模11的乘法运算构成一个乘法群. 可以验证, $\mathbb{Z}_{11} \setminus \{0\}$的子集合

$$\{3^0 = 1, 3^1 = 3, 3^2 = 9, 3^3 = 5, 3^4 = 4\}$$

  关于模11的乘法运算也构成一个乘法群.

6. 群的陪集

定义

设$(H,\cdot)$是群$(G,\cdot)$的一个子群, $a \in G$, 称集合

$$aH = \{a \cdot h \,|\, h \in H\}$$

为由a所确定的H在G中的左陪集, a称为aH的代表元素.
类似地, 称集合

$$Ha = \{h \cdot a \,|\, h \in H\}$$

为由a所确定的H在G中的右陪集, a称为Ha的代表元素.

例1: 设$G=\{e,g,g^2,\ldots,g^{11}\}$, $H=\{e,g^4,g^8\}$, 显然H是G的子群.
作出H在G中的所有右陪集:
$He=\{e,g^4,g^8\}=H, Hg=\{g,g^5,g^9\}, Hg^2=\{g^2,g^6,g^{10}\}, Hg^3=\{g^3,g^7,g^{11}\},$
$Hg^4=\{g^4,g^8,e\}, Hg^5=\{g^5,g^9,g\}, Hg^6=\{g^6,g^{10},g^2\}, Hg^7=\{e^7,g^{11},g^3\},$
$Hg^8=\{g^8,e,g^4\}, Hg^9=\{g^9,g,g^5\}, Hg^{10}=\{g^{10},g^2,g^6\}, Hg^{11}=\{g^{11},g^3,g^7\}.$

例1: 设$G=\{e,g,g^2,\ldots,g^{11}\}$, $H=\{e,g^4,g^8\}$, 显然H是G的子群.
作出H在G中的所有右陪集:
$He=\{e,g^4,g^8\}=H, Hg=\{g,g^5,g^9\}, Hg^2=\{g^2,g^6,g^{10}\}, Hg^3=\{g^3,g^7,g^{11}\},$
$Hg^4=\{g^4,g^8,e\}, Hg^5=\{g^5,g^9,g\}, Hg^6=\{g^6,g^{10},g^2\}, Hg^7=\{e^7,g^{11},g^3\},$
$Hg^8=\{g^8,e,g^4\}, Hg^9=\{g^9,g,g^5\}, Hg^{10}=\{g^{10},g^2,g^6\}, Hg^{11}=\{g^{11},g^3,g^7\}.$

- 在实际中, 可以令$G=\mathbb{Z}_{13}^*$, 而$g=2$是模13的一个原根.
- 从这个例子中可以看出, 陪集的代表元不唯一.

例2: 设$n>1$是整数, 则$H=n\mathbb{Z}$是$(\mathbb{Z},+)$的子群, 子集

$$a+n\mathbb{Z}=\{a+nk\,|\,k\in\mathbb{Z}\}$$

是$H=n\mathbb{Z}$的左陪集, 该陪集为实际为模n的一个剩余类.

子群陪集的基本性质

设H是G的子群.

- $aH = H \iff a \in H$.
- $b \in aH \iff a^{-1} \cdot b \in H$.

子群陪集的基本性质

设H是G的子群.

- $aH = H \iff a \in H$.
- $b \in aH \iff a^{-1} \cdot b \in H$.
  如果$b \in aH$, 则存在$h \in H$使得$b = a \cdot h, a^{-1} \cdot b = a^{-1} \cdot (a \cdot h) = h \in H$;
  反之, 设$a^{-1} \cdot b \in H$, 则$a \cdot (a^{-1} \cdot b) \in aH$,即$b \in aH$.
- $b \in Ha$当且仅当$b \cdot a^{-1} \in H$.
- $|aH| = |H|$, 即H在G中的任意陪集大小相等.

子群陪集的基本性质

设H是G的子群.

- $aH = H \iff a \in H$.
- $b \in aH \iff a^{-1} \cdot b \in H$.
  如果$b \in aH$, 则存在$h \in H$使得$b = a \cdot h, a^{-1} \cdot b = a^{-1} \cdot (a \cdot h) = h \in H$;
  反之, 设$a^{-1} \cdot b \in H$, 则$a \cdot (a^{-1} \cdot b) \in aH$,即$b \in aH$.
- $b \in Ha$当且仅当$b \cdot a^{-1} \in H$.
- $|aH| = |H|$, 即H在G中的任意陪集大小相等.
  一方面, 由aH的定义可见aH中元素个数必不大于H的元素个数即$|aH| \leq |H|$.
  另一方面, 对于任意的$h_1, h_2 \in H, h_1 \neq h_2$, 必有$a \cdot h_1 \neq a \cdot h_2$(群$G$有消去律),
  即$|aH| \geq |H|$, 故$|aH| = |H|$.
- 对于任意的$a \in H$, 有$aH = H = Ha$.

定理

设aH, bH是任意两个H在G中的左陪集. 或者有$aH = bH$或者有$aH \cap bH = \Phi$

证明: 如果$aH \cap bH \neq \phi$, 则存在$f \in aH \cap bH$, 即存在$h_1, h_2 \in H$使得

$$f = a \cdot h_1 = b \cdot h_2,$$

所以$a = b \cdot h_2 \cdot h_1^{-1}$. 任取$x \in aH$, 则存在$h_3 \in H$使得

$$x = a \cdot h_3 = (b \cdot h_2 \cdot h_1^{-1}) \cdot h_3 = b \cdot (h_2 \cdot h_1^{-1} \cdot h_3) \in bH,$$

即$aH \subseteq bH$. 反之, 任取$x \in bH$, 则存在$h_4 \in H$使得

$$x = b \cdot h_4 = (a \cdot h_1 \cdot h_2^{-1}) \cdot h_4 = a \cdot (h_1 \cdot h_2^{-1} \cdot h_4) \in bH,$$

即$bH \subseteq aH$. $\diamond$

定理

设H是G的子群, 则群G可以表示为不相交的左(右)陪集的并集.

指标和商集

定义

子群H在群G中左(右)陪集的个数称为H在G中的指标, 或指数, 记作$[G:H]$.

定义

子群H在群G中不同左(右)陪集构成的集合$\{aH|a\in G\}$, 称为H在G中商集, 记作G/H.

例: 设$n>1$是整数, 则$H=n\mathbb{Z}$是$(\mathbb{Z},+)$的子群, 模n的一个剩余类

$$a+n\mathbb{Z}=\{a+nk\,|\,k\in\mathbb{Z}\}$$

是$H=n\mathbb{Z}$的左陪集. 显然, 子群H在群$(\mathbb{Z},+)$中左陪集的个数为n, 即$[G:H]=n$. 此外, 子群H在群$(\mathbb{Z},+)$中的商集G/H实际上是模n的完全剩余类.

Lagrange定理及其推论

定理（拉格朗日(Lagrange)）

设G是有限群, $H \leq G$, 则
$$|G| = |H|[G:H]$$

证明: 设$[G:H]=m$, 于是存在$a_1, a_2, \cdots, a_m \in G$使得$G=\bigcup_{i=1}^{m} a_i H$, 且$a_i H \cap a_j H = \Phi$, 其中$i \neq j$. 而每一个陪集的元素个数均为$|a_i H| = |H|$, 所以

$$|G| = \sum_{i=1}^{m} |H| = m|H| = |H|[G:H].$$

推论

设H为有限群G的子群, $|G|=n$且$|H|=m$, 则$m \mid n$, 即有限群的任意子群的阶数是该有限群的阶数的因数. 特别地, 任何素数阶的群不可能有非平凡子群.

子群的一些其他性质

定理

设H, K是交换群G的两个子群, 则H和K的笛卡尔积HK也是G的子群, 并且HK的阶满足$|HK| = |H||K|/|H \cap K|$.

定理

设H, K是G的两个子群, 则$H \cap K$在群H中左(右)陪集的个数, 即$H \cap K$在群H中的指标不超过子群K在群G中的指标，也即$[H : H \cap K] \leq [G : K]$. 如果$[G : K]$是有限的, 则$[H : H \cap K] = [G : K]$当且仅当$G = HK$.

定理

设H, K是G的两个子群, 如果它们在群G中的指标是有限的，则$[G : H \cap K]$也是有限的, 并且

$$[G : H \cap K] \leq [G : H][G : K].$$

进一步，等号成立当且仅当$G = HK$.

7. 正规子群

定义（正规子群）

设G是群, $H \leq G$, 如果对于任意的$g \in G$都有

$$gH = Hg,$$

则称H是G的正规子群, 或者不变子群, 记作$H \trianglelefteq G$.

7. 正规子群

定义 (正规子群)

设G是群, $H \leq G$, 如果对于任意的$g \in G$都有

$$gH = Hg,$$

则称H是G的正规子群, 或者不变子群, 记作$H \trianglelefteq G$.

- 如果G是交换群, 则G的任何子群都是正规子群.

定义（正规子群）

设G是群, $H \leq G$, 如果对于任意的$g \in G$都有

$$gH = Hg,$$

则称H是G的正规子群, 或者不变子群, 记作$H \trianglelefteq G$.

- 如果G是交换群, 则G的任何子群都是正规子群.
- 任何群都有两个平凡的正规子群: G和$\{e\}$.

7. 正规子群

定义 (正规子群)

设G是群, $H \leq G$, 如果对于任意的$g \in G$都有

$$gH = Hg,$$

则称H是G的正规子群, 或者不变子群, 记作$H \trianglelefteq G$.

- 如果G是交换群, 则G的任何子群都是正规子群.
- 任何群都有两个平凡的正规子群: G和$\{e\}$.
- 指数为2的子群必为正规子群.

7. 正规子群

定义（正规子群）

设G是群, $H \leq G$, 如果对于任意的$g \in G$都有

$$gH = Hg,$$

则称H是G的正规子群, 或者不变子群, 记作$H \trianglelefteq G$.

- 如果G是交换群, 则G的任何子群都是正规子群.
- 任何群都有两个平凡的正规子群: G和$\{e\}$.
- 指数为2的子群必为正规子群.
  设G是群, $H \leq G$, 且$[G:H] = 2$, 取$a \in G \backslash H$, 则$aH \cap H = Ha \cap H = \Phi$, 从而$G = H \cup aH = H \cup Ha$, 再由陪集性质的$aH = G \backslash H = Ha$, 可知$H \trianglelefteq G$.

正规子群的性质

定理

设H是G的正规子群, 则如下命题等价:

1. $\forall a \in G$, 有$aH = Ha$
2. $\forall a \in G, \forall h \in H$, 有$aha^{-1} \in H$
3. $\forall a \in G$, 有$aHa^{-1} \subseteq H$
4. $\forall a \in G$, 有$aHa^{-1} = H$

证明:

$(1 \Rightarrow 2:)$ $\forall a \in G, \forall h \in H$, 有$aH \in Ha \Rightarrow ah = h_1 a \Rightarrow aha^{-1} = h_1 \in H$.

$(2 \Rightarrow 3:)$ $aha^{-1} \in H \Rightarrow aHa^{-1} \subseteq H$.

$(3 \Rightarrow 4:)$ 由$\forall a \in G$, 有$aHa^{-1} \subseteq H$, 因而有$a^{-1}H(a^{-1})^{-1} \subseteq H$, 即$a^{-1}Ha \subseteq H$.
所以, 对于任意的$h \in H$, 有$a^{-1}ha = h_1 \in H$, 进而有$h = ah_1a^{-1} \in aHa^{-1}$,
于是$H \subseteq aHa^{-1}$, 因此$aHa^{-1} = H$.

$(4 \Rightarrow 1:)$ $aHa^{-1} = H \Rightarrow (aHa^{-1})a = Ha \Rightarrow aH = Ha$.

例:设

$$G = \left\{ \begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix} \mid r, s \in \mathbb{Q}, r \neq 0 \right\}$$

$$H = \left\{ \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \mid s \in \mathbb{Q} \right\}$$

G对矩阵乘法构成群, 判断H是否为正规子群.

任取

$$a = \begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix} \in G, \quad h = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \in H$$

有

$$aha^{-1} \in \begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} r^{-1} & -r^{-1}s \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & rt \\ 0 & 1 \end{pmatrix} \in H$$

所以$H \trianglelefteq G$

商集G/H

定义

设$H \trianglelefteq G$, 则G关于H的左陪集的集合与G关于H的右陪集的集合相等, 称为G关于H的陪集集合, 记作G/H, 即$G/H = \{aH \mid a \in G\} = \{Ha \mid a \in G\}$.

定理

设$H \trianglelefteq G$, 则G/H关于乘法$(aH) \cdot (bH) = (ab)H$构成群. G/H也被称为G对正规子群H的商群.

证: 子集的乘法是关于G/H的满足封闭性和结合律的二元运算. G/H中有单位元H. 对于任意的$aH \in G/H$, 有逆元$a^{-1}H$. 综上所述, G/H关于子集的乘法构成群.