

信息安全数学基础

第二部分 第八章 群

中山大学 计算机学院

5. 子群

定理

设 (G, \cdot) 是一个群. H 是 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 (G, \cdot) 的子群(subgroup), 记作 $H \leq G$.

例如: 已知 $(\mathbb{Z}, +)$ 是一个群, 令

$$H_2 = \{\text{全体偶数}\} = \{2k \mid k \in \mathbb{Z}\} \subseteq \mathbb{Z},$$

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,

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

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 G 的子集, 这个子集对 (G, \cdot) 中的运算 \cdot 也构成群, 即为 (G, \cdot) 的子群.

另外, (G, \cdot) 本身当然也是 (G, \cdot) 的子群.

这两个子群称为是 (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: $e \cdot x = x \implies e' \cdot x = e \cdot x$.

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 \rightarrow 2): 由定义.

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

(3 \rightarrow 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 \rightarrow 2): 由定义.

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

(3 \rightarrow 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 \rightarrow 2): 由定义.

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

(3 \rightarrow 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.

\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.

- $\mathbb{Z}_{11} \setminus \{0\}$ 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

$$aH = \{a \cdot h \mid h \in H\}$$

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

$$Ha = \{h \cdot a \mid h \in H\}$$

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 $G = \{e, g, g^2, \dots, g^{11}\}$, $H = \{e, g^4, g^8\}$, 显然 H 是 G 的子群.

作出 H 在 G 中的所有右陪集:

$$\begin{aligned} He &= \{e, g^4, g^8\} = H, Hg = \{g, g^5, g^9\}, Hg^2 = \{g^2, g^6, g^{10}\}, Hg^3 = \{g^3, g^7, g^{11}\}, \\ Hg^4 &= \{g^4, g^8, e\}, Hg^5 = \{g^5, g^9, g\}, Hg^6 = \{g^6, g^{10}, g^2\}, Hg^7 = \{g^7, g^{11}, g^3\}, \\ Hg^8 &= \{g^8, e, g^4\}, Hg^9 = \{g^9, g, g^5\}, Hg^{10} = \{g^{10}, g^2, g^6\}, Hg^{11} = \{g^{11}, g^3, g^7\}. \end{aligned}$$

例1: 设 $G = \{e, g, g^2, \dots, g^{11}\}$, $H = \{e, g^4, g^8\}$, 显然 H 是 G 的子群.

作出 H 在 G 中的所有右陪集:

$$\begin{aligned} He &= \{e, g^4, g^8\} = H, Hg = \{g, g^5, g^9\}, Hg^2 = \{g^2, g^6, g^{10}\}, Hg^3 = \{g^3, g^7, g^{11}\}, \\ Hg^4 &= \{g^4, g^8, e\}, Hg^5 = \{g^5, g^9, g\}, Hg^6 = \{g^6, g^{10}, g^2\}, Hg^7 = \{g^7, g^{11}, g^3\}, \\ Hg^8 &= \{g^8, e, g^4\}, Hg^9 = \{g^9, g, g^5\}, Hg^{10} = \{g^{10}, g^2, g^6\}, Hg^{11} = \{g^{11}, g^3, g^7\}. \end{aligned}$$

- 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

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

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

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

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

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

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 的完全剩余系.

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 $a_1, a_2, \dots, a_m \in G$ 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.

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 $\{e\}$.

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 $a \in G \setminus H$, 则 $aH \cap H = Ha \cap H = \Phi$, 从而 $G = H \cup aH = H \cup Ha$, 再由陪集性质的 $aH = G \setminus H = Ha$, 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 $aH \in Ha \Rightarrow ah = h_1a \Rightarrow aha^{-1} = h_1 \in H$.

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

正规子群的判断

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 $H \trianglelefteq G$

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.