

## 第七讲陪集、拉格朗日定理

陈建文

October 23, 2022

**定义1.** 设 $G$ 为一个群,  $G$ 的任意子集称为群子集。在 $2^G$ 中借助于 $G$ 的乘法引入一个代数运算, 称为群子集的乘法:  $\forall A, B \in 2^G$ ,

$$AB = \{ab | a \in A \text{ 且 } b \in B\}$$

$\forall g \in G, A \in 2^G, \{g\}A$ 简写为 $gA$ , 即 $gA = \{ga | a \in A\}$ 。

**定义2.** 设 $H$ 为群 $G$ 的一个子群,  $a \in G$ , 则集合 $aH$ 称为子群 $H$ 的一个左陪集,  $Ha$ 称为 $H$ 的一个右陪集。

**定理1.** 设 $H$ 为群 $G$ 的一个子群, 则 $\forall a \in G, aH = H$ 的充分必要条件是 $a \in H$ 。

证明.  $\Leftarrow$  设 $aH = H$ , 则 $a = ae \in aH = H$ 。

$\Rightarrow$  设 $a \in H$ , 则 $\forall g \in aH, \exists h \in H, g = ah \in H; \forall h \in H, h = a(a^{-1}h) \in aH$ 。  $\square$

**定理2.** 设 $H$ 为群 $G$ 的一个子群, 则 $\forall a, b \in G, aH = bH$ 的充分必要条件是 $a^{-1}b \in H$ 。

证明.  $\Leftarrow$  设 $aH = bH$ , 则 $b = be \in bH = aH$ , 从而 $\exists h \in H$ 使得 $b = ah$ , 于是,  $a^{-1}b = h \in H$ 。

$\Rightarrow$  设 $a^{-1}b \in H$ , 则 $\forall g \in aH, \exists h \in H$ , 使得 $g = ah = b((b^{-1}a)h) = b((a^{-1}b)^{-1}h) \in bH$ , 从而 $aH \subseteq bH$ ; 由 $a^{-1}b \in H$ 可得 $b^{-1}a \in H$ , 从而 $bH \subseteq aH$ 。  $\square$

**定理3.** 设 $H$ 为群 $G$ 的一个子群, 则 $\forall a, b \in G, aH = bH$ 或者 $aH \cap bH = \phi$ 。

证明. 如果 $aH \cap bH \neq \phi$ , 设 $f \in aH \cap bH$ , 则 $\exists h, h'$ 使得 $f = ah = bh'$ , 于是 $a^{-1}b = hh'^{-1} \in H$ , 从而 $aH = bH$ 。  $\square$

**定理4.** 设 $H$ 为群 $G$ 的一个子群, 则 $\forall a, b \in G, |aH| = |bH|$ 。

证明. 令 $\phi: aH \rightarrow bH, \forall h \in H, \phi(ah) = bh$ , 则易验证 $\phi$ 为双射, 所以 $|aH| = |bH|$ 。  $\square$

**定理5.** 设 $H$ 为群 $G$ 的一个子群, 则 $H$ 的所有左陪集构成的集合为 $G$ 的一个划分。

证明. 首先, 不同的左陪集互不相交。其次,  $\forall a \in G, a \in aH$ , 所以 $G = \bigcup_{a \in G} aH$ 。因此,  $H$ 的所有左陪集构成的集族为 $G$ 的一个划分。  $\square$

**定义3.** 设 $H$ 为群 $G$ 的一个子群, 如果 $H$ 的所有不同的左陪集的个数为有限数 $j$ , 则称 $j$ 为 $H$ 在 $G$ 中的指数, 记为 $j = [G : H]$ , 否则称 $H$ 在 $G$ 中的指数为无穷大。

**定理6.** 设 $G$ 为一个有限群,  $H$ 为 $G$ 的一个子群, 则 $|G| = |H| \cdot [G : H]$ 。

证明.  $H$ 在 $G$ 中的所有不同的左陪集构成的集族为 $G$ 的一个划分, 每个左陪集均含有 $n$ 个元素。因此,  $|G| = n|G : H|$ 。□

**推论1.** 有限群中每个元素的阶都能整除该有限群的阶。

证明. 设 $G$ 为一个 $N$ 阶群,  $a$ 为 $G$ 的一个阶为 $n$ 的元素, 则由 $a$ 生成的 $G$ 的子群 $\langle a \rangle$ 的阶也为 $n$ , 由Lagrange定理,  $n|N$ 。□

**推论2.** 如果群 $G$ 的阶为素数, 则 $G$ 为一个循环群。

因为 $p$ 为素数, 所以 $p \geq 2$ 。于是,  $G$ 中至少有一个非单位元素 $a$ 。 $a$ 的阶整除 $p$ , 但 $p$ 为素数, 所以 $a$ 的阶为 $p$ 。因此,  $G = \langle a \rangle$ 。

**推论3.** 设 $G$ 为一个群, 则 $\forall a \in G, a^{|G|} = e$ 。

证明. 设 $a$ 的阶为 $n$ , 则 $n|N$ , 于是 $a^N = (a^n)^{(N/n)} = e^{(N/n)} = e$ 。□

**例.** 证明: 阶小于等于5的群为交换群。

证明. 设 $G$ 为一个 $p$ 阶群,  $p \leq 5$ 。如果 $p = 1$ , 则 $G = \{e\}$ 为一个交换群。当 $p = 2, 3, 5$ 时,  $p$ 为素数,  $G$ 为循环群, 从而为交换群。以下证明当 $p = 4$ 时,  $G$ 也为一个交换群。此时,  $G$ 中每个元的阶整除4, 所以 $G$ 中每个元素的阶为1, 2或4。如果 $G$ 中有一个阶为4的元素 $a$ , 则 $G = \langle a \rangle$ , 从而为交换群。如果 $G$ 中每个元素的阶都不为4, 则 $G$ 中每个非单位元素的阶都为2。于是,  $\forall x, y \in G, x^2 = e, y^2 = e, (xy)^2 = e$ 。由 $(xy)^2 = e$ 得 $xyxy = e$ , 两边同时左乘 $x$ , 右乘 $y$ , 可得 $yx = xy$ , 故 $G$ 为交换群。□

**定理7.** 设 $H$ 为群 $G$ 的一个子群,  $S_l$ 为 $H$ 的所有左陪集构成的集合,  $S_r$ 为 $H$ 的所有右陪集构成的集合, 则 $|S_l| = |S_r|$ 。

**定理8.** 设 $p$ 为素数, 整数 $a$ 与 $p$ 互素, 则 $a^{p-1} \equiv 1 \pmod{p}$ 。

证明. 以下证明 $S_p \setminus \{[0]\} = \{[1], [2], \dots, [p-1]\}$ 对于乘法运算“ $\cdot$ ”构成一个群。

其中的乘法运算“ $\cdot$ ”定义为:  $\forall i, j \in Z, [i] \cdot [j] = [ij]$ 。

$\forall i, j, i', j' \in Z$ , 果 $[i] = [i'], [j] = [j']$ , 则 $[ij] = [i'j']$ , 这验证了“ $\cdot$ ”为一个运算。

$\forall i, j, k \in Z, ([i] \cdot [j]) \cdot [k] = [ij] \cdot [k] = [(ij)k], [i] \cdot ([j] \cdot [k]) = [i] \cdot [jk] = [i(jk)], ([i] \cdot [j]) \cdot [k] = [i] \cdot ([j] \cdot [k])$ , 这验证了乘法运算满足结合律。

$\forall i \in Z, [1] \cdot [i] = [i]$ , 这验证了 $[1]$ 为左单位元。

$\forall i \in Z, [i] \neq [0]$ , 则 $(i, p) = 1$ , 从而 $\exists s, t \in Z, si + tp = 1$ , 于是 $p|(si - 1)$ , 所以 $[si] = [1]$ , 即 $[s][i] = [1]$ , 这说明 $[i]$ 有左逆元。

以上验证了 $S_p \setminus \{[0]\}$ 对于乘法运算“ $\cdot$ ”构成一个群。

$\forall a \in Z$ , 如果 $a$ 与 $p$ 互素, 则 $[a] \in S_p \setminus \{[0]\}$ , 从而 $[a]^{p-1} = [1], a^{p-1} \equiv 1 \pmod{p}$ 。□

RSA算法:

- (1) 随机选择两个大的素数 $p$ 和 $q$ ;
- (2) 计算 $n = pq$ ;
- (3) 选择数 $e$ , 使得 $e$ 与 $(p-1)(q-1)$ 互素;
- (4) 计算数 $d$ , 使得对于某个整数 $k$ ,  $ed = 1 + k(p-1)(q-1)$ ;
- (5) 将 $(e, n)$ 作为公钥发布, 保留私钥 $(d, n)$ 。

设待加密的明文为 $M$ ,  $M < n$ 。

加密过程:  $C = M^e \bmod n$ ;

解密过程:  $M = C^d \bmod n$ 。

**定理9.** 在以上描述的RSA算法中,  $(M^e \bmod n)^d \bmod n = M$ 。

证明. 由于 $(M^e \bmod n)^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$ , 因此只需证 $M^{ed} \bmod n = M$ 。当 $M$ 与 $p$ 互素时,

$$\begin{aligned} & M^{ed} \bmod p \\ &= M^{1+k(p-1)(q-1)} \bmod p \\ &= M(M^{p-1})^{k(q-1)} \bmod p \\ &= M(1)^{k(q-1)} \bmod p \\ &= M \bmod p \end{aligned}$$

于是 $M^{ed} \equiv M \pmod{p}$ 。当 $p|M$ 时, 该式显然也成立。

同理可证 $M^{ed} \equiv M \pmod{q}$ , 进一步可得 $M^{ed} \equiv M \pmod{pq}$ , 即 $M^{ed} \equiv M \pmod{n}$ , 从而 $M^{ed} \bmod n = M \bmod n = M$ 。□

课后作业题:

**练习1.** 证明: 六阶群里必有一个三阶子群。

**练习2.** 设 $p$ 为一个素数, 证明: 在阶为 $p^m$ 的群里一定含有一个 $p$ 阶子群, 其中 $m \geq 1$ 。

**练习3.** 在三次对称群 $S_3$ 中, 找一个子群 $H$ , 使得 $H$ 的左陪集不等于 $H$ 的右陪集。

**练习4.** 设 $H$ 为群 $G$ 的一个子群, 如果左陪集 $aH$ 等于右陪集 $Ha$ , 即 $aH = Ha$ , 则 $\forall h \in H, ah = ha$ 一定成立吗?