NIS2312-01 2023-2024 Fall

信息安全的数学基础 (1)

Answer 8

2023 年 10 月 19 日

假设 H, K 是有限群 G 的子群. 证明:

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

解: 设 $|H| = n$ 和 $|K| = m$, 我们有

$$\begin{bmatrix} h_1k_1 & h_1k_2 & \cdots & h_1k_m \\ h_2k_1 & h_2k_2 & \cdots & h_2k_m \\ h_nk_1 & h_nk_2 & \cdots & h_nk_m \end{bmatrix},$$

共计 $|H| \cdot |K|$ 个元素 (不考虑元素是否重复).

注意到有 $|HK| \leq |H| \cdot |K|$, 出现这一情况是由于可能存在 $h, h' \in H, k, k' \in K$ 满足 $h \neq h'$, $k \neq k'$ 和 $hk = h'k'$. 此时我们有 $k(k')^{-1} = h^{-1}h' \in H \cap K$, 故此时对于任意 $t = k(k')^{-1} = h^{-1}h' \in H \cap K$, 有 $k = t^{-1}k'$ 和 $h' = ht$. 因此, $hk = htt^{-1}k = (ht)(t^{-1}k) = h'k'$. 换句话说, 上述矩阵中元素, 每个元素均重复了 $|H \cap K|$ 次, 故我们有结论 $|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$.