1 群论

Statement:有限群的元素的阶数是有限的

Proof: 设 G 是个有限群, $a \in G$

反证法: 设 $a \in G, a^m \neq e(m = 1, 2, 3, ...)$. 由于群的封闭性, a^m 在群中, 当 m 取不同数字的时候我们会得出无穷多个 a^m 都在群中, 这样就导出了矛盾. ■

1.1 陪集

Definition: 陪集

若 G 为群, H 为其子群, g 是 G 中的元素, 则

- $gH = \{gh \mid h \in H\}$ 是H在G中的左陪集.
- $Hg = \{hg \mid h \in H\}$ 是H在G中的右陪集.

由定义, G的陪集一定是G的子集(由群的封闭性), 但不一定构成群, 因为大多数情况下没有单位元(见下).

Example: $G = (\mathbb{Z}/4\mathbb{Z}, +), H = \{0, 2\}$ then

$$H + 1 = \{1, 3\} = H + 3 = \{3, 1\}$$

$$2 + H = \{2, 0\} = 0 + H = \{0, 2\}$$

我们看出, 用同一个陪集中的元素生成陪集得到的陪集都是相等的, 下面我们就来证明这个定理.

Collorary: 如果 $a \in Hb$, 那么 $Ha = Hb$. (很重要)

Proof:

$$a \in Hb \Rightarrow a = h_m b \Rightarrow b = h_m^{-1} a$$

若$h_a, h_b \in H$, 有$h_c \in H = h_a h_b$ (群的定义)

取 $\forall x \in Ha$. 存在 $x = h_n a = h_n(h_m b) = (h_n h_m)b = h_i b \in Hb$. 因此 $Ha \subset Hb$.

取 $\forall y \in Hb$. 存在 $y = h_p b = h_p h_m^{-1} a = h_j a \in Ha$. 因此 $Hb \subset Ha$.

因此

$$Ha = Hb$$

■

Collorary's Collorary: He 是唯一有单位元的陪集. 根据上述结论, 任何其他有单位元的陪集都和 He 相等, 所以只有陪集He是G的子群.

1.1.1 陪集的集合是群的分割

令 H 是 G 的子群. 则 $\{Ha \mid a \in G\}$ 是 G 的一个分割. (分割的意思是说, 这些集合的并集是 G, 且取任意的两个(不同的)集合,它们的交集为空).

Proof:

首先证明这些陪集的并集是G. 因为 $e \in H, ea = a$, 所以 $\forall a[a \in G \Rightarrow a \in Ha]$, 这说明了在 Ha 中至少有元素 a, 所以$\cap \{Ha \mid a \in G\} = G$.

其次证明任取两个不同的集合,它们的交集为空. 我们用反证法.

设两个不同的陪集 Ha, Hb 的交集不为空, 取 $x \in Ha \cap Hb$. 由陪集的定义可知 $x = h_m a = h_n b$. 同时左乘 h_m 的逆元素可得:

$$a = h_m^{-1} h_n b$$

$$(h_m^{-1} h_n) \in H \ (\text{子群是群, 群的定义})$$

$$a \in Hb \Rightarrow Ha = Hb$$

这就导出了矛盾, 所以, 两个不同陪集的交集一定为空.

1.1.2 陪集的等长性

由陪集的定义 $Ha = \{ha \mid h \in H\}(a \in G)$, Ha 的元素个数和 H 的一样. 所以 H 与Ha 之间可以建立一个一一对应的关系(也可以从证明双射的角度出发来证明元素个数相同).

1.1.3 Lagrange's Theorem

Theorem: Lagrange's Theorem

令 G 是有限群, H 是其子群. 有 $\text{ord}(H) \mid \text{ord}(G)$.

因为陪集的两个性质, 这个定理就变得很显然了.

$|G| = |Ha_1| + |Ha_2| + ... + |Ha_n| = n\ |H|$

注意, 这个定理的逆定理是不一定成立的. 比方说一个 8 阶群的子群肯定是 1,2,4 或 8 阶的, 但 4 阶的群不一定是其子群.

1.1.4 Langrage's Theorem 的简单应用

Langrage's Theorem 同样揭示了 p 阶群(p 是质数)没有非平凡子群, 且是循环群.

Theorem: 关于 p 阶群

p 阶群 G 是循环群, 且所有非单位元元素都是 G 的生成元.

Proof:

$|G| = p$, 取 $a \in G/\{e\}$ 则 a 的阶不可能为 1. 令 $|a| = m$, 使用 Langrage's Theorem, 则 $m \mid p$. 因为 p 是质数且 $m \neq 1$, 有 $m = p$ 所以 $< a >= G$

它还能证明一个有限群中元素的阶整除群的阶, 即 $a \in G, \text{ord}(a) \mid \text{ord}(G)$.

我们知道一个元素的阶定义就是这个元素生成的群的阶数, 因为这个元素在群 G 中, 所以生成的群 K 是 G 的子群, 利用 Langrage's Theorem 原命题得证.