Pure Mathematics 理论数学, 2022, 12(10), 1702-1706
Published Online October 2022 in Hans. http://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2022.1210184

Hans汉斯

群中元素乘积的阶的定理推广

李雅月

云南师范大学数学学院，云南 昆明

收稿日期：2022年9月18日；录用日期：2022年10月17日；发布日期：2022年10月24日

摘　要

讨论了群G中两个元素a，b乘积的阶等于$\frac{mn}{(m,n)^2}$的情况。给出了群中元素a，b不可交换时，元素乘积的阶的一类计算问题。在相对较大的范围内，对已有定理进行了推广。

关键词

群，元素，乘积，阶

Generalization of the Theorem for the Product Order of Elements in Group

Yayue Li

School of Mathematics, Yunnan Normal University, Kunming Yunnan

Received: Sep. 18th, 2022; accepted: Oct. 17th, 2022; published: Oct. 24th, 2022

Abstract

In this paper, we discuss the case that the order of the product of two elements a, b in group G is equal to $\frac{mn}{(m,n)^2}$. This paper presents a class of computational problems for the order of the product of elements in a group when $ab \neq ba$. In a relatively large range, the existing theorems are extended.

Keywords

Group, Element, Product, Order

文章引用: 李雅月. 群中元素乘积的阶的定理推广[J]. 理论数学, 2022, 12(10): 1702-1706.
DOI: 10.12677/pm.2022.1210184

在[1]中我们知道若群 G 中元素 a 的阶是 m，而 b 的阶是 n，则当 $ab=ba$，且 $(m,n)=1$ 时，有 $|ab|=mn$。

这个定理对于求群中元素乘积的阶起着非常重要的作用。当然，也存在一定的局限性，如果 $ab\neq ba$ 或 $(m,n)\neq 1$ 时，ab 的阶就不一定等于 nm。这时我们可以思考，a 和 b 之间满足什么条件时，乘积 ab 的阶与元素 a，b 的阶之间也存在着某些联系。

引理 1 [1]. 设 a 是群 G 的元素，a 的阶是 n，则 $a^m=e\Leftrightarrow n\mid m$。

引理 2 [2]. 设 a,b 为群 G 中两个元素，$|a|=|b|=m$，且存在 $k\in N$，使得 $a=b^k$，那么 $|ab|=\dfrac{m}{(m,k+1)}$。

引理 3 [2]. 设 a,b 为群 G 中的两个元素，$|a|=|b|=m$，若存在 $s,t\in N$ 使得 $a^s=b^t$，则当 $s\mid(m+1)$ 时，有 $|ab|=\dfrac{m}{\left(m,\dfrac{m+1}{s}t+1\right)}$。

引理 4 [3]. 设 a,b 为群 G 中的两个元素，$|a|=m,|b|=n,m\neq n$，则当 $ab=ba$ 时一定存在 $|ab|\mid[m,n]$，$\dfrac{[m,n]}{(m,n)}\mid|ab|$，其中 $[m,n]$ 是 m 与 n 的最小公倍数。

引理 5 [4]. 设 a，b 为群 G 中的两个元素，$|a|=m,|b|=n,m\neq n$，那么当 $ab=ba$，而且 $(m,n)\mid\dfrac{n}{(m,n)}$ 或者 $(m,n)\mid\dfrac{m}{(m,n)}$ 成立时，有 $|ab|=[m,n]$。

根据引理 4，我们可知当 $|a|=m,|b|=n,m\neq n,ab=ba$ 时，可设 $|ab|=\dfrac{mn}{(m,n)^2}k$，其中 $1\le k\le d$，且 $k\mid d,d=(m,n)$，即在引理 5 的条件下可求出 $|ab|=\dfrac{mn}{(m,n)}(k=d)$ 的这种情况。接下来我们可以思考 a，b 之间存在什么关系时，可以求出 $|ab|=\dfrac{mn}{(m,n)^2}(k=1)$。

定理 1. 设 a，b 为群 G 中的两个元素，$|a|=m,|b|=n,(m,n)=d,ab=ba,a^{m_1}=b^{n_1}$ 且 $d\mid(m_1+n_1)$，其中 $m=m_1d,n=n_1d$，那么 $|ab|=\dfrac{mn}{(m,n)^2}$。

证明：不妨设 $|ab|=p$，则 $(ab)^p=e$，因为 $ab=ba$，所以

$$(ab)^{pm}=a^{pm}b^{pm}=b^{pm}=e$$

因为 $|b|=n$ 由引理 1 得

$$n\mid pm\Rightarrow\frac{n}{(m,n)}\mid p\frac{m}{(m,n)}$$

由 $\left(\dfrac{n}{(m,n)},\dfrac{m}{(m,n)}\right)=1$，所以

$$\frac{n}{(m,n)} \mid p \tag{1}$$

又因为$|a|=m$且$(ab)^{pn}=a^{pn}b^{pn}=a^{pn}=e$，所以$m \mid pn \Rightarrow \frac{m}{(m,n)} \mid p\frac{n}{(m,n)}$

$$\left(\frac{n}{(m,n)},\frac{m}{(m,n)}\right)=1 \Rightarrow \frac{m}{(m,n)} \mid p \tag{2}$$

由(1)和(2)式，$\left(\frac{n}{(m,n)},\frac{m}{(m,n)}\right)=1$

$$\frac{mn}{(m,n)^2} \mid p \tag{3}$$

另一方面，已知$a^{m_1}=b^{n_1}$

$$(ab)^{\frac{mn}{(m,n)^2}}=(ab)^{m_1n_1}=a^{m_1n_1}b^{m_1n_1}=b^{n_1^2}b^{m_1n_1}=b^{n_1(n_1+m_1)}$$

由$d \mid (m_1+n_1)$，不妨设$n_1+m_1=kd$，所以

$$(ab)^{\frac{mn}{(m,n)^2}}=b^{n_1(n_1+m_1)}=b^{n_1dk}=b^{nk}=e$$

根据引理 1 得

$$p \mid \frac{mn}{(m,n)^2} \tag{4}$$

所以，由(3)与(4)得

$$p=\frac{mn}{(m,n)^2}，\text{即}|ab|=\frac{mn}{(m,n)^2}$$

特别的，当$|a|=2\cdot p_1,|b|=2\cdot p_2,ab=ba,a^{p_1}=b^{p_2}$，其中$p_1,p_2$为不相等的奇素数，那么$|ab|=\frac{mn}{(m,n)^2}$。

例如，在模 30 的剩余类加群Z_{30}中，[3]的阶为 10，[5]的阶为 6，且$5[3]=3[5]$，则$(10,6)=2,m_1=5,n_1=3,2 \mid (5+3),[3]+[5]=[8]$的阶为$15=\frac{10\times 6}{2^2}$。

我们知道若群 G 中$|a|=m,|b|=n,ab=ba$，且$(m,n)=1$时，有$|ab|=mn$。如果a,b不可以交换或者这两个元素的阶不互素时，ab乘积的阶就不能直接求出等于nm。此时，我们可以思考当$ab\neq ba$时，如果两个元素 a，b 之间满足$(n,2k)=2k,ab=b^{2k-1}a^{-1}$，元素 a，b 乘积的阶的问题。定理 2 就是对这一问题的研究。

定理 2. 设a,b为群 G 的两个元素，$|a|=m,|b|=n,(n,2k)=2k,(m,n)=1$，且$ab=b^{2k-1}a^{-1}$，那么$|ab|=\frac{n}{k}$。

证明：首先，当$ab=b^{2k-1}a^{-1}$

$$(ab)^h=\begin{cases}b^{hk} & h\text{为偶数}\\ b^{hk+(k-1)}a^{-1} & h\text{为奇数}\end{cases} \tag{5}$$

不妨设$|ab|=p$，由$(n,2k)=2k \Rightarrow \frac{n}{k}$是偶数

由(5)式得

$$(ab)^{\frac{n}{k}} = b^n = e$$

根据引理 1 得

$$p \mid \frac{n}{k} \tag{6}$$

接下来证：$\frac{n}{k} \mid p$

若 p 为偶数：$(ab)^p = b^{pk} = e$，由引理 1 得

$$n \mid pk \Rightarrow \frac{n}{k} \mid p$$

若 p 为奇数：$(ab)^p = b^{pk+(k-1)}a^{-1} = e$，从而

$$a = b^{pk+(k-1)} \Rightarrow a^m = b^{m[pk+(k-1)]} = e$$

由引理 1 得

$$n \mid m\left[pk+(k-1)\right]$$

因为 $(m,n)=1$

$$n \mid \left[pk+(k-1)\right]$$

分析 $pk+(k-1)$ 的奇偶性，可知 $pk+(k-1)$ 只能为奇数，且 n 为偶数，不能整除奇数；矛盾

从而

$$\frac{n}{k} \mid p \tag{7}$$

由(6)与(7)得

$$p = \frac{n}{k} \text{ 即 } |ab| = \frac{n}{k}$$

定理 3. 设 a，b 为群 G 的两个元素 $|a|=n, |b|=\ln$，存在 $k \in N$，使 $a = b^k$，则 $|ab| = \frac{\ln}{(\ln, k+1)}$。

证：设 $|ab| = p, d = (\ln, k+1)$，则 $1 = \left(\frac{\ln}{d}, \frac{k+1}{d}\right)$

$$(ab)^p = b^{(k+1)p} = e \Rightarrow \ln \mid (k+1)p \Rightarrow \frac{\ln}{d} \mid \frac{k+1}{d}p \Rightarrow \frac{\ln}{d} \mid p \tag{8}$$

又因为

$$(ab)^{\frac{\ln}{d}} = b^{\frac{(k+1)\ln}{d}} = e \Rightarrow p \mid \frac{\ln}{d} \tag{9}$$

由(8)与(9)得：

$$p = \frac{\ln}{d} = \frac{\ln}{(\ln, k+1)}$$

定理 4. 设 a，b 为群 G 的两个元素 $|a|=n, |b|=\ln$，若存在 $s,t \in N$，使得 $a^s = b^t$，且 $s \mid (n+1)$，那么

$|ab|=\dfrac{\ln}{\left(\ln,\dfrac{n+1}{s}t+1\right)}$。

证：因为 $a^s=b^t$，且 $s\mid(n+1)\Rightarrow\dfrac{n+1}{s}$ 是整数

$$\left(a^s\right)^{\frac{n+1}{s}}=\left(b^t\right)^{\frac{n+1}{s}}\Leftrightarrow a^{n+1}=b^{\frac{n+1}{s}t}\Leftrightarrow a=b^{\frac{n+1}{s}t}$$

由定理 3 得

$$|ab|=\frac{\ln}{\left(\ln,\dfrac{n+1}{s}t+1\right)}$$

例如，在模 36 的剩余类加群 Z_{36} 中，[24]的阶为 3，[3]的阶为 12，且 $2[24]=16[3],s=2,t=16,2\mid(3+1)$。所以，$[24]+[3]=[27]$ 的阶 $4=\dfrac{12}{\left(12,16\times\dfrac{3+1}{2}+1\right)}=\dfrac{12}{(12,33)}$。[9]和[27]的阶都为 4，且 $[27]=3[9]$ 及 $s=1,t=3,1\mid(4+1)$。所以，$[9]+[27]=[36]$ 的阶为 $1=\dfrac{4}{\left(4,3\times\dfrac{4+1}{1}+1\right)}=\dfrac{4}{(4,16)}$ 成立。

定理 3，定理 4 是对引理 2，引理 3 的结论进行了推广。引理 2，3 中元素 a，b 的阶一定要满足相等，但定理 3，4 不止可以解决元素 a，b 的阶相等的情形，还可以解决部分元素 a，b 的阶不相等时，元素 a，b 乘积的阶的计算问题。

参考文献

[1] 杨子胥. 近世代数[M]. 北京: 高等教育出版社, 2011.

[2] 杨冰. 关于群中乘积元素的阶[J]. 大学数学, 2005, 21(5): 125-128.

[3] 张远达. 有限群构造(上册) [M]. 北京: 科学出版社, 1982.

[4] 廖小莲, 刘葵, 陈国华. 关于群中乘积元素的阶[J]. 高等数学研究, 2011, 14(2): 17-19.