doi: 10.3969/j. issn. 1007-2861. 2010. 06. 017

有限群 Sylow 子群的个数的一个注记

沈如林[1], 史江涛[2], 邵长国[3], 施武杰[4]

(1. 湖北民族学院 数学系,湖北 恩施 445000;2. 北京大学 数学科学学院,北京 100871;
3. 上海大学 理学院,上海 200444;4. 苏州大学 数学科学学院,江苏 苏州 215006)

摘要: 推广张继平关于 Sylow 数的研究结果,证明有限群 Sylow r-子群的个数为 $2p^n$,p 为奇素数且 $n\geqslant 1$,当且仅当 $2p^n=1+r^{2m}$.

关键词: 有限群;有限单群;极大子群;Sylow 数

中图分类号: O 152.1　　**文献标志码**: A　　**文章编号**: 1007-2861(2010)06-0639-04

A Note on Number of Sylow Subgroups of Finite Groups

SHEN Ru-lin[1], SHI Jiang-tao[2], SHAO Chang-guo[3], SHI Wu-jie[4]

(1. Mathematical Department, Hubei University for Nationalities, Enshi 445000, Hubei, China;
2. School of Mathematical Sciences, Peking University, Beijing 100871, China;
3. College of Sciences, Shanghai University, Shanghai 200444, China;
4. School of Mathematical Sciences, Suzhou University, Suzhou 215006, Jiangsu, China)

Abstract: The result of Zhang Jiping on the Sylow number of finite groups was generalized, and prove that the number of Sylow r-subgroup is $2p^n$, where p is odd prime and $n\geqslant 1$, if and only if $2p^n=1+r^{2m}$.

Key words: finite groups; finite simple groups; maximal subgroups; Sylow number

Sylow 定理是有限群理论的一个非常重要的定理. 设有限群 G 的 Sylow r-子群的个数为 n_r,我们称 n_r 为有限群 G 的 Sylow r-数. 由 Sylow 定理可知,一个数量关系为 $n_r\equiv 1(\mathrm{mod}\ r)$,但反之满足模 r 余 1 的数并不一定就是 Sylow r-数. 例如,Hall[1] 利用有限群的模表示证明了 22 不是 Sylow 3-数,21 不是 Sylow 5-数,$n=1+3p$ 不是 Sylow p-数($p\geqslant 7$). 关于 Sylow 数对有限群本身的影响,张继平[2] 进行了系统研究,证明了 Huppert 猜想. 现在提出一个有趣的问题:哪些正整数可以成为一个 Sylow 数[1-2]? 显然任何的奇数都是一个 Sylow 2-数,因为在二面体群 D_{2n}(n 奇数)中,Sylow 2-数恰为 n. 而对于哪些偶数为 Sylow 数,还是一个未解决的问题. 文献[2]给出了一个未证明的结果:数 $2p$(p 奇素数)为 Sylow r-数当且仅当 $2p=1+r^{2m}$. 本研究继续文献[1-2]的工作,推广并得到以下定理.

定理 1　有限群 G 的 Sylow r-子群的个数为 $2p^n$,当且仅当 $2p^n=1+r^{2m}$.

注:对于丢番图方程 $2p^n=1+r^{2m}$($n>1$, $m>0$)的解,若 $n>2$ 且是偶数,则除了 $p=13$, $r=239$, $m=1$, $n=4$ 以外,没有其他解[3]. 若 $n=2$,这是 Pell 数列中的素数问题,到底有多少? 这是一个著名的未解

收稿日期:2009-04-29
基金项目:国家数学天元基金资助项目(11026195);中国博士后科学基金资助项目(20100470136,20100480582);河南省科技计划资助项目(94300510100)
通信作者:沈如林(1977~),男,博士,研究方向为有限群. E-mail:shenrulin@hotmail.com

决的问题. 若 $n>1$ 是奇数,容易看出该方程没有解.

1　极大子群指数为 $2p^n$ 的单群

一个 q^m-1 的素因子 q_m 称本原素因子,如果 q_m 不整除 q^n-1(任意 $n<m$). 由 Zsigmondy 定理[4]知,如果 $m>2$ 且 $(q,m)\neq(2,6)$,则本原素因子 q_m 一直存在. 记 $|n|_p$ 为数 n 的 p-部分.

首先,给出极大子群的指数为素数幂的单群[5].

引理 1　设 G 是非交换有限单群,$H<G$ 且 $|G:H|=p^n$,则下列结论成立:

(1) $G=A_m$, $H\cong A_{m-1}$,其中 $m=p^n$;

(2) $G=L_m(q)$, H 是直线或超平面的稳定化子, 于是 $|G:H|=\dfrac{q^m-1}{q-1}$,其中 m 为素数;

(3) $G=L_2(11)$, $H\cong A_5$;

(4) $G=M_{23}$ 且 $H\cong M_{22}$,或者 $G=M_{11}$ 且 $H\cong M_{10}$;

(5) $G=U_4(2)\cong S_4(3)$, H 是指数为 27 的抛物子群.

引理 2　G 是域 $GF(q)(q=r^f)$ 上的典型单群,设 C_i 是文献[6]中定义的极大子群类,$1\leqslant i\leqslant 8$. 如果 $H\in C_i$,则

(1) 存在一个数 $c\in C$(其中 C 参见表 1),使得 r^c-1 的每个本原素因子整除 $|G:H|$;

(2) 若 $(G,|G:H|)\neq\left(A_n(q),\dfrac{q^{n+1}-1}{q-1}\right)$, 则 $p\mid|G:H|$ 或存在 $c_1,c_2\in C(c_1\neq c_2)$,使得 $r^{c_i}-1(i=1,2)$ 的每个本原素因子整除 $|G:H|$;

(3) 若 $p=2$ 且 $|G:H|_2=2$, 则 $(G,H)=(L_2(4),S_3)$.

表 1　有限群 Sylow 子群的个数的一个标记

Table 1　A note on the number of Sylow subgroups of finite groups

G	C
$A_n(q)(n\geqslant 2)$	$nf,(n+1)f$
$C_n(q)(n\geqslant 3)$	$nf,2nf,2(n-1)f$
${}^2A_{2k}(q)(k\geqslant 2)$	$2(2k+1)f,4kf,2(2k-1)f,2kf$
${}^2A_n(q)(n\geqslant 3)$	$2(k+1)f,4kf,2(2k+1)f,4(k+1)f$
$B_n(q)(n\geqslant 3)$	$nf,2nf,2(n-1)f$
$D_n(q)(n\geqslant 4)$	$nf,2(n-1)f,2(n-2)f$
${}^2D_n(q)(n\geqslant 4)$	$2nf,(n-1)f,2(n-1)f$

证明　直接从文献[6]中的表 3.5 A-F 及第 4 章计算可以得出以上结论. 以下以 $G=A_n(q)$ 的 C_2 型极大子群为例来计算(其他的类型更为简单). 由文献[4]中的第四章计算知

$$H_{\overline{\Omega}}\cong\left[\frac{(q-1)^{t-1}(q-1,m)}{(q-1,n+1)}\right].$$

$$L_m(q)^t.\ [(q-1,m)^{t-1}].S_t,$$

式中,$n+1=mt$ 且 $t\geqslant 2$. 由于 H 为 C_2 型,故 $H=H_{\overline{\Omega}}\cap A_n(q)$.

现考虑 H 的 Sylow r-子群的阶,明显 $|H|_r=|L_m(q)|_r^t\cdot|S_t|_r$,因此,

$$|H|_r=r^{\frac{m(m-1)ft}{2}+\left(\left[\frac{t}{r}\right]+\left[\frac{t}{r2}\right]+\left[\frac{t}{r2}\right]+\cdots\right)}<r^{\frac{m(m-1)ft}{2}+\frac{t}{r-1}},$$

显然,$|A_n(q)|_p=q^{\frac{n(n+1)}{2}}=r^{\frac{mt(mt-1)f}{2}}$.

设函数 $g(t):=\dfrac{1}{2}mt(mt-1)f-\dfrac{1}{2}mt(m-1)\cdot f-\dfrac{t}{p-1}$,由于 $t\geqslant 2$ 且 $p\geqslant 2$,故 $g(t)\geqslant m^2f-2$. 如果 $m\geqslant 2$ 或 $f\geqslant 2$,则 $g(t)\geqslant 0$,故 $|A_n(q)|_p>|H|_p$,以上结论成立. 如果 $m=1$ 且 $f=1$,则 $|A_n(q)|_p=p^{\frac{t(t-1)}{2}}$,而 $|H|_r=|S_t|_r=r^{\left[\frac{t}{r}\right]+\left[\frac{t}{r2}\right]+\left[\frac{t}{r2}\right]+\cdots}<r^t$,明显如果 $t\geqslant 3$,则 $|A_n(q)|_r\geqslant r^t>|H|_r$,以上结论成立. 若 $t=2$,则 $|A_n(q)|_r=r$, 但 $|H|_r=r^{\left[\frac{2}{r}\right]+\left[\frac{2}{r2}\right]+\left[\frac{2}{r2}\right]+\cdots}\leqslant r$,且当且仅当 $p=2$,等式成立,即此时 $A_n(q)=L_2(2)$,但这不是单群,即有 $|A_n(q)|_p>|H|_p$,以上结论成立. 用同样的方法讨论函数 $g(t)\geqslant 1$ 的情况,可以得到结论(2)成立. 对于(3), $p=2$ 且 $|G:H|_2=2$,因此,需要解方程

$$1+\frac{m(m-1)ft}{2}+\left(\left[\frac{t}{2}\right]+\left[\frac{t}{2^2}\right]+\left[\frac{t}{2^2}\right]+\cdots\right)=\frac{mt(mt-1)f}{2}.$$

类似以上的讨论,可以得到解 G 只能是 $L_2(4)$ 且 $H=S_3$.

下面给出极大子群指数为 $2p^n$ 的单群的分类.

定理 2　设 G 是非交换有限单群,H 是 G 的极大子群且 $|G:H|=2p^n$,则有以下结论:

(1) $G=A_m$, $H=A_{m-1}$,其中 $m=2p^n$;

(2) $G=L_2(r^{2^m})$ 且 $1+r^{2^m}=2p^n$, H 为 1 维子空间的稳定子;

(3) $G=U_4(3)$,$H=L_3(4)$,且 $|G:H|=2\cdot 3^4$;

(4) $G=U_3(5)$,$H=A_7$,且 $|G:H|=2\cdot 5^2$;

(5) $G=M_{22}$,$H=L_3(4)$,且 $|G:H|=2\cdot 11$.

证明　设 G 是非交换单群,H 为 G 的极大子群且 $|G:H|=2p^n$,这里 p 为奇素数且 $n\geqslant 1$. 分以下 4

种情形考虑.

情形 1: G 为散在单群.

设 G 不是大魔群 M 时, G 的所有极大子群 H 在文献[7-11]中列出,容易得出结论成立. 假设 G 是大魔群 M 时,文献[7,12]列举了所有的局部极大子群和 2-局部极大子群 H,容易得出结论成立. 如果 H 不是局部极大子群,则 H 的所有根在文献[12]中已给出,容易看出 $|G:H|\neq 2p^n$.

情形 2: G 为交错单群 $A_m(m\geqslant 5)$.

如果 $m\leqslant 13$,直接根据文献[7]知,结论成立. 假定 $m>13$,设 H 是 G 的极大子群且 $|G:H|=2p^n$,如果 $\frac{m}{2}<p\leqslant m$,则 $|G:H|=2p$. 当然, G 可以看成是次数为 $2p$ 的本原置换群. 该本原置换群由 Liebeck 和 Saxl[13]完全分类,则有 $G=A_{2p}$,或 A_c,这里 $\frac{c(c-1)}{2}=2p$. 容易看出, $c=4,5$,故结论成立. 如果 $p\leqslant\frac{m}{2}$,因为 $m>13$,故可以取不超过 m 的最大和次大的素数 q 和 r. 当然, q 和 r 都不整除 $|G:H|$, 由文献[14]的定理 4 知,存在 k 满足 $q\leqslant k\leqslant m$,使得 $A_k\lhd H\leqslant S_k\times S_{m-k}$. 显然 H 满足文献[15]中第 366 页的结论(a),故 $H=A_m\cap(S_k\times S_{m-k})$,于是 $|A_m:H|=\frac{m!}{k!\ (m-k)!}$,因此,有 $\frac{m!}{k!\ (m-k)!}=2p^n$. 根据文献[5]的定理 2.1 知, $p^n\leqslant m$. 如果 $k\geqslant 2$, 而 $m>13$,则 $\frac{m!}{k!\ (m-k)!}\geqslant\frac{1}{2}m(m-1)>2p^n$,不可能. 故 $k=1$ 且 $m=2p^n$,结论成立.

情形 3: G 为在空间 $V(n,q)$ 上的典型单群,这里 $q=r^f$.

当 $G=A_1(q),A_2(q),B_2(q),{}^2A_2(q),{}^2A_3(q)$,根据文献[16]第 387 页的讨论,有 $G={}^2A_3(3)$, ${}^2A_2(5)$ 或 $G=A_1(q)$ 且 $|G:H|=q+1$ 或 $q(q\pm1)$,只要 $q+1=2p^n$ 或 $q(q\pm1)=2p^n$. 而 $\gcd(q,q\pm1)=1$,故对于第 2 个方程,有 $q=2$ 或 $q\pm1=2$,即 $q=1,2,3$,显然此时 G 不是单群. 对于方程 $q+1=2p^n$,即 $r^f+1=2p^n$, 如果 $f=2^m\cdot l$ 且 l 为奇数,则 $r^f+1=r^{2^m\cdot l}=(1+r^{2^m})(r^{2^m(l-1)}-r^{2^m(l-2)}+\cdots+1)$. 显然 r 为奇数,故 $2\mid 1+r^{2^m}$,如果 $l>1$,则有 $p\mid r^{2^m(l-1)}-r^{2^m(l-2)}+\cdots+1$,由 Zsigmondy 定理知,存在本原素因子 r_l 使得 r_l 不是 $1+r^{2^m}$ 的因子,故 $1+r^{2^m}=2$,矛盾. 因此 $l=1$,即 $1+r^{2^m}=2p^n$. 由引理 2 中的结论(3),假定表 1 中 $r^c-1\neq 2^6-1$,明显 $r_c>2$. 由单群的极大子群结构定理[6], G 的每个极大子群都在 $\bigcup_{i=1}^{8}C_i$ 或 S 中. 对于 C_i 型的极大子群,如果 $(G,|G:H|)\neq\left(A_{m-1}(q),\frac{q^m-1}{q-1}\right)$,则由引理 2 知,结论成立. 如果 $(G,|G:H|)=\left(A_{m-1}(q),\frac{q^m-1}{q-1}\right)$,则 $\frac{q^m-1}{q-1}=2p^n$. 但 $\frac{q^m-1}{q-1}=q^{m-1}+q^{m-2}+\cdots+1$,这样 q 是奇数且 m 是偶数. 若 $m=de$ 且 $d,e>1$,于是

$$2p^n=\frac{q^{de}-1}{q-1}=\frac{(q^{d(e-1)}+q^{d(e-2)}+\cdots+1)(q^e-1)}{q-1}.$$

但 $q^{d(e-1)}+q^{d(e-2)}+\cdots+1$ 和 $\frac{q^e-1}{q-1}$ 都大于 2 且存在不同的本原素因子,矛盾. 所以 $m=2$,即 $G=L_2(q)$. 其他情况讨论与 $G=A_1(q)$ 一致,故结论成立.

如果 $H\in S$,则由文献[16],只需将 $2^a\cdot 3^b$ 换成 $2p^n$ 即可,结论成立.

2　定理的证明

由文献[1]知,任何有限群 G 的 Sylow r-数是两种类型数的乘积:① 非交换单群的 Sylow r-数;② 素数幂 q^t 满足 $q^t\equiv 1(\bmod\ r)$. 因此,若 Sylow r-数为 $2p^n$,可以假定 G 为非交换单群. 设 G 的 Sylow r-子群为 R, N 为 $N_G(R)$. 取包含 N 的极大子群为 H. 由于 $|G:N|=2p^n$,故 $|G:H|=p^a$ 或 $2p^b$,这里 $a,b\geqslant 1$. 如果 $|G:H|=p^a$,由引理 1 知, $\gcd(p,|H|)=1$,这样 $a=n$. 故 $|H:N|=2$,于是 $N\lhd H$,这样 $H\leqslant N_G(N)=N_G(N_G(R))=N_G(R)$,有 $H=N$,矛盾. 如果 $|G:H|=2p^b$,同样由定理 2 知, $\gcd(p,|H|)=1$,这样 $b=n$,即 $H=N$,这说明 $N_G(R)$ 是 G 的极大子群. 由定理 2,可以分以下几种情形进行讨论:

(1) $G=A_{2p^n}$ 且 $N\cong A_{2p^n-1}$,此时 $N=N_G(R)\cong A_{2p^n-1}$ 为单群,即 $R\lhd A_{2p^n-1}$,矛盾;

(2) $G=L_2(r^{2^m})$ 且 $1+r^{2^m}=2p^n$,此时易知 $L_2(2^{2^m})$ 的 Sylow r-子群为 $1+r^{2^m}$,故结论成立;

(3) $G=U_4(3),U_3(5),M_{22}$,则 H 为单群,明显不可能.

参考文献:

[1] HALL M. On the number of Sylow subgroups of a finite group [J]. J Algebra, 1967, 7:363-371.

[2] ZHANG J. Sylow numbers of finite groups [J]. J Algebra, 1995, 176:111-123.

[3] BENNETT M A. Powers in recurrence sequences: Pell equation [J]. Trans Amer Math Soc, 2005, 357(4): 1675-1691.

[4] ZSIGMONDY K. Zur theorie der potenzreste [J]. Monatsh Math und Phys, 1892, B3:265-284.

[5] GURALNICK R. Subgroups of prime power index in a simple groups [J]. J Algebra, 1983, 81:304-311.

[6] KLEIDMAN P, LIEBECK M. The subgroup structure of the finite classical groups [M]. Cambridge: Cambridge University Press, 1990.

[7] CONWAY J H, CURTIS R T, NORTON S P, et al. Atlas of finite groups [M]. Oxford and New York: Oxford University Press, 1985.

[8] KLEIDMAN P, PARKER R A, WILSON R A. The maximal subgroups of the Fischer Group Fi_{23} [J]. J Proc London Math Soc, 1989, 39(2):89-101.

[9] KLEIDMAN P, WILSON R A. The maximal subgroups of J_4 [J]. Proc London Math Soc, 1988, 56(3):484-510.

[10] LINTON S A, WILSON R A. The maximal subgroups of the Fischer groups Fi_{24} and Fi'_{24} [J]. Proc London Math Soc, 1991, 65(3):113-164.

[11] WILSON R A. The maximal subgroups of the Baby Monster I [J]. J Algebra, 1999, 211:1-14.

[12] NORTON S P, WILSON R A. Anatomy of the Monster II [J]. Proc London Math Soc, 2002, 84(3):581-598.

[13] LIEBECK M, SAXL J. Primitive permutation groups containing an element of large prime order [J]. J London Math Soc, 1985, 2031:237-249.

[14] LIEBECK M, PREAGER C E, SAXL J. Transitive subgroups of primitive permutation groups [J]. J Algebra, 2000, 234:291-361.

[15] LIEBECK M, PREAGER C E, SAXL J. A classification of the maximal subgroups of the finite alternation and symmetric groups [J]. J Algebra, 1987, 111:365-383.

[16] LI X, XU M. The primitive permutation groups of degree $2^a \cdot 3^b$ [J]. Arch Math, 2006, 86:385-391.

(编辑:孟庆勋)