数量型与有限群结构

SHU LIANG XING YU YOU XIAN QUN JIE GOU

沈如林◎著

中国出版集团
世界图书出版公司

本书获国家自然科学基金项目（编号：11201133）资助

数量型与有限群结构

SHU LIANG XING YU YOU XIAN QUN JIE GOU

沈如林◎著

中国出版集团
世界图书出版公司
广州·上海·西安·北京

图书在版编目(CIP)数据

数量型与有限群结构 / 沈如林著. — 广州:世界图书出版广东有限公司,2015.11
ISBN 978-7-5192-0448-8

Ⅰ.①数… Ⅱ.①沈… Ⅲ.①有限群—研究
Ⅳ.①O152.1

中国版本图书馆 CIP 数据核字(2015)第 275767 号

数量型与有限群结构

策划编辑　刘婕妤
责任编辑　黄　琼
出版发行　世界图书出版广东有限公司
地　　址　广州市新港西路大江冲 25 号
http:// www.gdst.com.cn
印　　刷　北京天正元印务有限公司
规　　格　710mm×1000mm　1/16
印　　张　14.5
字　　数　250 千
版　　次　2016 年 1 月第 1 版　2016 年 1 月第 1 次印刷
ISBN 978-7-5192-0448-8/O·0047
定　　价　46.00 元

目　录

第1章 基本概念及定理

§1.1 引言

群论起源于对代数方程的研究, 它是人们对代数方程求解问题逻辑考察的结果. 群论的早期发展归功于著名数学家Gauss, Cauchy, Abel, Hamilton, Galois等许多人. 群理论被公认为19世纪最杰出的数学成就之一. 最重要的是, 群论不仅开辟了全新的研究领域, 同时对于物理学、化学的发展, 甚至对于20世纪结构主义哲学的产生和发展都产生了巨大的影响. 在有限群及表示论中, 有限性决定了数量关系在这些理论中的极端重要性, 菲尔兹奖获得者Zelmanov 关于限制Burnside 问题的工作说明了这种关系在群论中的重要地位. 另外, 有限群著名定理, 如Lagrange定理, Sylow定理, Burnside 定理和奇阶定理, 都是一些极其美妙的数量性质.

群的数量问题的研究在过去的几十多年里一直非常活跃. 1981年有限单群分类定理完成后, 不少群论学者试图用一些基本的数量关系来刻画有限群. 1987年, 施武杰教授提出了单群的纯数量刻画: 仅用有限群元素阶的集合和有限群的阶来刻画有限单群(见[259-271]); 之后有很多类似的问题被提出, 比如Thompson给出的群阶与共轭类长度集合对单群的刻画猜想. Itô有多篇文章研究群元素共轭类的长度对群的影响(见[140-146]);文献[53-66]讨论了群的共轭类个数对群的影响; 自然数称为有限群的Sylow数, 如果它是某个群的Sylow 子群的个数, 文献[277-278]对Sylow数的相关性质进行了研究.

这些工作都很好地说明了有限群的数量性质本质地反映了群的性质. 有限群中同阶元素的个数是群内部结构的一个基本数量. 例如Alperin-Feit-Thompson定理, 设G 是2-群, 正好包含t 个二阶元. 如果$t \equiv 1 (\bmod 4)$, 则G 循环或者$|G : G'| = 4$ (此时只能为群Z_2^2, 二面体群、半二面体群和广义四元素群). 很多学者对元素个数对群内部结构的影响进行了研究, 见[19-21]. 我们可以用如下型的概念来统一研究.

定义 *设群G 有性质P, 且在性质P下群G对应到一个自然数的集合T_P, 我们称群G 有性质P的数量型T_P.*

本书中的群一般指有限群, 单群都是指有限单群. 我们所使用

的群论的术语和符号是标准的, 参照Robinson 的著作[249], Kurzweil 和Stellmacher 的著作[165] 及徐明耀的著作[305], 未指出的符号可参考本书文献.

设 G是有限群, $x \in G$. $X \in G$, X的中心化子是 $\{g \in G : xg = gx, \forall\ x \in G\}$, 表示成 $C_G(X)$. 如果$X = \{x\}$, 我们可将括号去掉. X在 G中的共轭类表示为x^G. x的指数表示为 $Ind_G(x)$. 我们将 G的导群表示成 G'. Fitting子群表示为 $Fit(G)$. 给定一个素数p, p常规和p异常经常被应用. 我们说一个元素是p常规的等价于说它是一个 p'元, 也就是它的阶不能被p整除; 不是 p'的元说成p异常元. 同样地, 如果 π是一个素数集, 则 π'是不含 π里面元素的素数集. $O_\pi(G)$是 G的最大的阶为一个 π数字的正规子群. 同样, $O^\pi(G)$是 G的因子群 $G/O^\pi(G)$ 为一个π群的最小正规子群. 在群 G中的一个p补指的是 G的以最高阶 p整除G的阶为指数的子群 H. 我们用CFSG表示有限单群的分类定理.

大写字母$G, H, \cdots$表示群.

$Sym(\Omega)$表示集合Ω上的对称群;$Sym(n)$表示n个元素上的对称群, 或简记为S_n.

$|S|$表示集合S中元素的个数.

$H \leqslant G$表示H为群G 的子群.

$H \trianglelefteq G$表示子群H为群G 的正规子群.

$|G : H|$表示子群H在群G 中的指数.

H^g表示子群H在元素G 下的共轭子群, 即$g^{-1}Hg$.

p-群表示阶为素数幂的群.

Z_n表示n阶循环群.

$H \rtimes K$表示正规子群H被群K的可裂扩张.

$O_p(G)$表示G 的所有$Sylow$ p-子群的交.

$\pi_e(G)$表示G 的所有元素阶的集合.

$\tau_e(G)$表示G 的所有同阶元素长度(或个数)的集合.

$s_m(G)$表示G 中m阶元的个数, 简记为s_m.

π表示某个素数集合.

$|n|_\pi$表示n的π-部分, 即素因子为π的n的最大因子, 记$|n|_p$为$|n|_{\{p\}}$.

$p^s \parallel n$表示p^s为n的p-部分.

$\pi(n)$表示群自然数n的素因子的集合. 并记$\pi(G)$为$\pi(|G|)$.

$\gcd(m,n)$, $lcm(m,n)$分别表示整数m,n的最大公因子和最小公倍数, 在不混淆的时候, 简记为(m,n)和$[m,n]$.

§1.2 基本概念及结果

本节中给出群论中基本的概念及结果, 为后面证明引用.

定义 1.1. 称非空集合G为一群, 如果在G上定义一个二元运算, 并且满足

(*a*) 结合律: $a(bc)=(ab)c$, 任意$a,b,c\in G$;

(*b*) 存在单位元素: 存在$1\in G$, 使得对任意$a\in G$, 有$1a=a1=a$;

(*c*) 存在逆元素: 对任意$a\in G$, 存在$a^{-1}\in G$, 使得$aa^{-1}=a^{-1}a=1$.

群G的一个子集H如果对于G中运算构成群, 我们称H为G的群, 记为$H\leqslant G$. 如果$x\in G$, 称集合$Hx=\{hx|h\in H\}$和$xH=\{xh|h\in H\}$分别为子群H在G中的一个右陪集和左陪集. 子群H在G中左(右)陪集的个数叫作H在G中的指数, 记为$|G:H|$. 进一步如果对于任意$x\in G$都有$xH=Hx$, 称H为G的正规子群, 记为$H\trianglelefteq G$.

定理 1.2. (*Lagrange*) 设G为有限群, $H\leqslant G$, 则$|G|=|H||G:H|$.

定理 1.3. (第一同构定理) 设$N\trianglelefteq G$, $M\trianglelefteq G$, 且$N\leqslant M$, 则$M/N\trianglelefteq G/N$, 并且$(G/N)/(M/N)\cong G/M$.

定理 1.4. (第二同构定理) 设$H\trianglelefteq G$, $K\trianglelefteq G$, 则$H\cap K\trianglelefteq H$, 且$HK/K\cong H/(H\cap K)$.

定理 1.5. (N/C-定理) 设$H\leqslant G$, 则$N_G(H)/C_G(H)$同构于$Aut(H)$的一个子群.

定理 1.6. (*Frattini*论断) 设$N\trianglelefteq G$, $P\in Syl_p(N)$, 则$G=N_G(P)N$.

设元素$x,g\in G$, 则元素$g^{-1}xg$称为x的共轭元素, 记为x^g. 子群$H^g=\{h^g|h\in H\}$称为H的共轭子群. 令$[x,y]=x^{-1}y^{-1}xy$, 称为元素x,y的换位

子. 群$\langle[x,y]|x,y\in G\rangle$称为群$G$的换位子群, 记为$G'$. 容易看出$G/G'$为交换群. 设$n\geqslant 2$, 则$G$的$n$次导群,记为$G^{(n)}$, 为$G$的$n-1$次导群的导群. 产生了一个$G$的正规群列：$G\geqslant G'\geqslant G^{(2)}\geqslant G^{(3)}\geqslant\cdots\geqslant G^{(n)}\geqslant\cdots$, 称为$G$的导群列. 如果存在$G^{(n)}=1$, 我们称$G$为可解群. 使得$G^{(n)}=G^{(n-1)}$的最小的$n$称为$G$的导来长.

如果G的一列正规子群：

$$1=N_0\leqslant N_1\leqslant\cdots\leqslant N_d=G \tag{1.1}$$

满足N_i/N_{i-1}为几乎单群, 即同型单群的直积, 我们称为G的主因子列. 如果在(1.1)中仅仅满足N_{i-1}在N_i中正规, $i=1,2,\ldots,d$, 称N_{i-1}是G的次正规子群, 记为$N_{i-1}\lhd\lhd G$. 进一步, 如果N_i/N_{i-1}为单群, 称(1.1)为G的合成因子列. 此时称如上的d分别为G的主列长和合成列长.

定理 1.7. (*Sylow*定理) *设G为有限群, p^n为$|G|$的最大的p幂. 则*

(1) G中存在p^n阶子群, 称为G的Sylow p-子群;

(2) G的所有Sylow子群共轭, 且每个p-子群都包含在某个Sylow p-子群中;

(3) G的所有Sylow子群个数$n_p\equiv 1(\mathrm{mod}\ p)$.

如果Sylow定理是群论中第一个非常重要的定理. 一个子群H称为G的Hall子群, 或者Hall $\pi(H)$-子群, 如果$\gcd(|H|,|G:H|)=1$. 以下为Hall 子群的一些结果.

定理 1.8. (*Hall 定理*) *群G为可解群, 当且仅当G存在Hall π-子群, 这里任意$\pi\subseteq\pi(G)$.*

设群$G\neq 1$, 令$\Phi(G)$为G的所有极大子群之交, 规定$\Phi(1)=1$, 称$\Phi(G)$为G 的Frattini 子群. 本质上$\Phi(G)$为G 中所有非生成元的集合. 明显为G的一个特征子群, 同时它是G中所有非生成元的集合. 如果群G为其所有Sylow子群的直积, 我们叫作幂零群. 当然p-群是幂零群.

定理 1.9. *(1) $\Phi(G)$是幂零群;*

(2) 如果$G/\Phi(G)$是幂零群, 那么G为幂零群;

(3) 设$N\unlhd G$, 那么$\Phi(G)N/N\leqslant\Phi(G/N)$;

(4) 设G为p-群, 则$G/\Phi(G)$为初等交换p-群; 反之, $\Phi(G)$是G的使其商群为初等交换群的最小的正规子群.

定理 1.10. 群G为幂零群等价于下列条件之一:

(1) 对G的每个真正规子群N都有中心$Z(G/N) \neq 1$;

(2) 对G的每个非平凡正规子群N有$[N, G] < N$;

(3) G的每个极大子群是正规的;

(4) 对G的每个非循环正规子群U有$\langle x^U \rangle \neq U, \forall x \in U$;

(5) 对G中任意互素阶元都是交换的.

以下给出著名的奇阶定理.

定理 1.11. (*Feit-Thompson*定理, 奇阶定理) 奇数阶群为可解群.

注意随着单群分类定理的完成, 可解性的判断及其关于可解相关的命题随之解决, 比如Schreier猜想：单群的外自同构群为可解群, 等. 如下给出可解群的一些等价的判断条件.

定理 1.12. 群G为可解群等价于下列条件之一:

(1) G的主因子为初等交换群;

(2) G的合成因子为素数阶群;

(3) 设$N \trianglelefteq G$, N 和G/N可解.

如果群G 为其正规子群N和Sylow p-子群的乘积NP, 并且满足$N \cap P = 1$, 称G 为p-幂零群, N 为G 的正规p-补.

定理 1.13. (*Burnside* p-幂零准则) 设G 为有限群, P为G 的*Sylow* p-子群. 若$N_G(P) = C_G(P)$, 则G 为p-幂零群.

注意运用N/C-定理和Burnside p-幂零准则容易知道, 如果Sylow 2-子群为循环群, 则必然存在正规的2-补.

定理 1.14. (*Frobenius* p-幂零准则) 设G 为有限群, P为*Sylow* p-子群, 则G 为p-幂零群, 当且仅当P 中任何两个元在G 中共轭, 必然在P中共轭.

注意Burnside p-幂零准则是Frobenius p-幂零准则的特殊情形. 如果G 的两子群H, K且$H \leqslant K$, 称K在G 下融合控制H, 如果H中任何两个元素在G 中共轭, 必然在K中共轭. Burnside同时证明如果G 有交换的Sylow p-子群P, 则$N_G(P)$ 融合控制P.

定理 1.15. (*Schur-Zassenhaus Hall-补准则*) *设N 是G 的正规Hall子群, 则N 在G 中存在补子群且任何两个补子群共轭.*

注意在原有的Schur-Zassenhaus Hall-补准则中, 任何两个补子群共轭需要条件N或G/N可解, 但可根据著名的奇阶定理(Feit-Thompson定理)知道这个条件是恒成立的, 故可以去掉. 另外, 以上定理当N为交换群时, 称为Gaschütz定理.

定义 1.16. *设G 为群, Ω为集合. 假定对于所有$g \in G$ 和$\alpha \in \Omega$ 定义一个Ω中唯一元素$\alpha \cdot g$. 如果满足以下条件, 我们称群G 作用在Ω上:*

(*a*) *任意$\alpha \in \Omega$, 有$\alpha \cdot 1 = \alpha$;*

(*b*) *任意$\alpha \in \Omega$, $g, h \in G$, 有$\alpha \cdot (gh) = (\alpha \cdot g) \cdot h$.*

设G 作用在Ω上, 并且只有G 中的单位元满足$\alpha \cdot 1 = \alpha$, 称作用是忠实的;如果对于Ω中的任意两元α, β都存在(唯一)元素G 使得$\beta = \alpha \cdot g$, 称为作用为传递(正则)的;集合$\{g \in G | \alpha \cdot g = \alpha, \forall \alpha \in \Omega\}$称为作用的核. 设$\alpha \in \Omega$, 称集合$\alpha^G = \{\alpha \cdot g | g \in G\}$ 为Ω中包含α的轨道;称集合$G_\alpha = \{g \in G | \alpha \cdot g = \alpha\}$为$\alpha$在$G$ 中的稳定子.

定理 1.17. *设有限群G 作用在有限集Ω上, 则G 同态于Ω上对称群$Sym(\Omega)$的某个子群, 且同态核为作用的核.*

推论 1.18. *设$H \leqslant G$且$|G : H| = n$, 则$G/\bigcap_{g \in G} H^g \leqslant Sym(n)$.*

注意这里子群$\bigcap_{g \in G} H^g$ 也称为H 在G 中的核. 如果群G 作用在Ω上, 置换特征标是定义在G 上的一个整值函数χ为$\chi(g) = |\{\alpha \in \Omega | \alpha \cdot g = \alpha\}|$.

定理 1.19. *群G 作用在有限集Ω上, 并设$\alpha \in \Omega$, 则$|\alpha^G| = |G : G_\alpha|$.*

定理 1.20. (*Cauchy-Frobenius定理*) *设有限群G 作用在有限集Ω上, 则作用的轨道数目为$\frac{1}{|G|} \sum_{g \in G} \chi(g)$, 这里$\chi$为$G$ 的置换特征标.*

定理 1.21. *设有限p-群G作用在集合Ω上, 并设$\Omega_0 = \{\alpha \in \Omega | \alpha \cdot g = \alpha, \forall g \in G\}$, 则$|\Omega| \equiv |\Omega_0| (\mathrm{mod} p)$.*

设群G作用在有限集Ω上且Ω是群, 称群作用在群上. 如果满足$(|G|, |\Omega|) = 1$, 称为互素作用.

定理 1.22. *设G, H是有限群, 假设G互素作用在H上, 则G固定H的某个Sylow p-子群, 这里p是$|H|$的任意素因子.*

设$Aut(G)$自然的作用在G上, ϕ是群G的自同构, 称ϕ是固定点自由的, 如果$x^{\phi} = x$可以推出$x = 1$.

定理 1.23. *设G为有限群, 如果G有2阶固定点自由自同构, 则G为奇阶交换群.*

定理 1.24. *设G为有限群, 如果G有3阶固定点自由自同构, 则G为类至多为2的幂零群.*

定理 1.25. *设G为有限群, 如果G有素数阶固定点自由自同构, 则G为幂零群.*

运用单群分类定理, 我们可以得到固定点自由的一般结果:

定理 1.26. *设G为有限群, 如果G有一个固定点自由自同构, 则G为可解群.*

定理 1.27. *设G为有限交换群, 假设$H \leqslant Aut(G)$且有形式$K \rtimes \langle \phi \rangle$. 如果对于任意$k \in K$, 元素$k\phi$是固定点自由的或者为素数阶的, 且$|K|$和$|G|$互素, 则$K$固定某个$G$的非平凡元.*

定理 1.28. *(P. Hall) 设G为有限群且$\pi(G)$为$|G|$的素因子集合, 则群G可解当且仅当存在Hall π-子群, 任意$\pi \subseteq \pi(G)$.*

由于两子群交换当且仅当它们乘积仍为子群, 我们可以拿出Sylow子群中不同素数的一组代表$\{P_1, P_2, \cdots, P_k\}$, 如果任意两个都是交换的, 称为$G$的Sylow系. 根据以上Hall定理知道有限群为可解当且仅当存在Sylow系.

设G为有限群且$G \neq 1$, 规定G中极大幂零正规子群为G的Fitting子群, 记为$F(G)$. 令G为非平凡群, 则对于G的任意主列$1 = G_0 < G_1 < G_2 < \cdots < G_n = G$, 有

$$F(G) = \bigcap_{i=1}^{n} C_G(G_i/G_{i-1})$$

其中$C_G(G_i/G_{i-1})$=$\{g \in G | g_i^g G_{i-1} = g_i G_{i-1}, \forall g_i \in G_i\}$. 群$G$说是完全的, 如果$G$的导群$G'$恰等于$G$, 若$G$是完全群, 且$G/Z(G)$为单群, 称$G$为拟单群. 拟单群的同态像仍为拟单群. 如果$G$的子群$K$是次正规且是拟单的, 称为$G$的一个分支. 定义两个特征子群: $E(G) = \langle K | K$为G的分支$\rangle$, $F^*(G) = F(G)E(G)$. 称$F^*(G)$为G的广义Fitting子群. 当然, 如果G可解, 则$F^*(G) = F(G)$.

定理 1.29. $C_G(F^*(G)) \leqslant F^*(G)$.

定理 1.30. 设$E(G) \neq 1$, $K_1, K_2, \cdots, K_n$为所有分支, 设$Z = Z(E(G))$, $Z_i = Z(K_i)$ 且$E_i = K_i Z/Z$, $i = 1, 2, \cdots, n$, 则

(*a*) $E(G)$为$K_1, K_2, \cdots, K_n$的中心积, 特别$Z = Z_1 Z_2 \cdots Z_n$;

(*b*) $Z_i = Z \cap K_i$, $E_i \cong K_i/Z_i$为非交换单群;

(*c*) $E(G)/Z \cong E_1 \times E_2 \times \cdots E_n$.

定理 1.31. (有限单群分类定理, *CFSG*) 有限单群为以下群之一:

(*a*) 素数阶循环群Z_p;

(*b*) 交错群A_n $(n \geqslant 5)$;

(*c*) 16族*Lie*型单群:

(c1) *Chevalley* 群$A_n(q)$, $B_n(q) n > 1$, $C_n(q) n > 2$, $D_n(q) n > 3$;

(c2) $E_6(q)$, $E_7(q)$, $E_8(q)$, $F_4(q)$, $G_2(q)$;

(c3) *Steinberg* 群 ${}^2A_n(q^2) n > 1$, ${}^2D_n(q^2) n > 3$, ${}^2E_6(q^2)$, ${}^3D_4(q^3)$;

(c4) *Suzuki* 群${}^2B_2(2^{2n+1})$;

(c5) *Ree* 群, *Tits* 群${}^2F_4(2^{2n+1})$;

(c6) *Ree* 群${}^2G_2(3^{2n+1})$.

(*d*) 26个散在单群(*Sporadic groups*):

(d1)*Mathieu* 单群M_{11}, M_{12}, M_{22}, M_{23}, M_{24};

(d2)*Janko* 单群J_1, J_2, J_3, J_4;

(d3)*Conway* 单群Co_1, Co_2, Co_3;

(d4)*Fischer* 单群Fi_{22}, Fi_{23}, Fi'_{24};

(d5)*Higman-Sims* 单群HS;

(d6)*McLaughlin* 单群McL;

(d7)*Held* 单群He;

(d8)*Rudvalis* 单群Ru;

(d9)*Suzuki* 散在单群Suz;

(d10)*O'Nan* 单群$O'N$;

(d11)*Harada-Norton* 单群HN;

(d12)*Lyons* 单群Ly;

(d13)*Thompson* 单群Th;

(d14)小魔群B;

(d15)*Fischer-Griess*大魔群M.

定理 1.32. (有限非交换单群的阶) 设S为非交换单群, 则S的阶由表1.1和表1.2给出.

表1.1: 散在单群S 的阶

S	S的阶	S	S的阶
M_{11}	$2^4 3^2 \cdot 5 \cdot 11$	M_{12}	$2^6 3^3 \cdot 5 \cdot 11$
M_{22}	$2^7 3^2 \cdot 5 \cdot 7 \cdot 11$	M_{23}	$2^7 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$
M_{24}	$2^{10} 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	J_1	$2^3 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$
J_2	$2^7 3^3 \cdot 5^2 \cdot 7$	J_3	$2^7 3^5 \cdot 5 \cdot 17 \cdot 19$
J_4	$2^{21} 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$	Ru	$2^{14} 3^3 5^3 \cdot 7 \cdot 13 \cdot 29$
He	$2^{10} 3^3 5^2 7^3 11$	McL	$2^7 3^6 5^3 \cdot 7 \cdot 11$
HN	$2^{14} 3^6 5^6 \cdot 7 \cdot 11 \cdot 19$	HiS	$2^9 3^2 5^3 \cdot 7 \cdot 11$
Suz	$2^{13} 3^7 5^2 \cdot 7 \cdot 11 \cdot 13$	Co_1	$2^{21} 3^9 5^4 7^2 \cdot 11 \cdot 13 \cdot 23$
Co_2	$2^{18} 3^6 5^3 \cdot 7 \cdot 11 \cdot 23$	Co_3	$2^{10} 3^7 5^3 \cdot 7 \cdot 11 \cdot 23$
Fi_{22}	$2^{17} 3^9 5^2 \cdot 7 \cdot 11 \cdot 13$	Fi_{23}	$2^{18} 3^{13} 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$
Fi'_{24}	$2^{21} 3^{16} 5^2 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$	$O'N$	$2^9 3^4 7^3 5 \cdot 11 \cdot 19 \cdot 31$
LyS	$2^8 3^7 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$	M, F_1	$2^{46} 3^{20} 5^9 7^6 11^2 13^3 \cdot 17 \cdot 19 \cdot 23$ $\cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$
B, F_2	$2^{41} 3^{13} 5^6 7^2 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47$	Th, F_3	$2^{15} 3^{10} 5^6 7^2 \cdot 13 \cdot 19 \cdot 31$

表1.2: 交错单群及Lie型单群S的阶

S	条件	S的阶
A_n	$n \geqslant 5$	$\frac{n!}{2}$
$A_n(q)$	$n \geqslant 1, q$为素数幂	$\frac{q^{\frac{1}{2}n(n+1)}}{(n+1,q-1)} \prod_{i=1}^{n}(q^{i+1}-1)$
$B_n(q)$	$n \geqslant 2, q$为素数幂	$\frac{q^{n^2}}{(2,q-1)} \prod_{i=1}^{n}(q^{2i}-1)$
$C_n(q)$	$n \geqslant 3, q$为素数幂	$\frac{q^{n^2}}{(2,q-1)} \prod_{i=1}^{n}(q^{2i}-1)$
$D_n(q)$	$n \geqslant 4, q$为素数幂	$\frac{q^{n(n-1)}(q^n-1)}{(4,q^n-1)} \prod_{i=1}^{n-1}(q^{2i}-1)$
$E_6(q)$	q为素数幂	$\frac{q^{36}}{(3,q-1)} \prod_{i\in\{2,5,6,8,9,12\}}(q^i-1)$
$E_7(q)$	q为素数幂	$\frac{q^{63}}{(2,q-1)} \prod_{i\in\{2,5,6,8,10,12,14,18\}}(q^i-1)$
$E_8(q)$	q为素数幂	$q^{120} \prod_{i\in\{2,8,12,14,18,20,24,30\}}(q^i-1)$
$F_4(q)$	q为素数幂	$q^{24} \prod_{i\in\{2,6,8,120\}}(q^i-1)$
${}^2A_n(q^2)$	$n \geqslant 2, q$为素数幂	$\frac{q^{\frac{1}{2}n(n+1)}}{(n+1,q+1)} \prod_{i=1}^{n}(q^{i+1}+(-1)^i)$
${}^2D_n(q^2)$	$n \geqslant 4, q$为素数幂	$\frac{q^{n(n-1)}(q^n+1)}{(4,q^n+1)} \prod_{i=1}^{n-1}(q^{2i}-1)$
${}^2E_6(q^2)$	q为素数幂	$\frac{q^{36}}{(3,q+1)} \prod_{i\in\{2,5,6,8,9,12\}}((-q)^i-1)$
${}^3D_4(q^2)$	q为素数幂	$q^{12}(q^8+q^4+1)(q^6-1)(q^2-1)$
${}^2B_2(q)$	$q=2^{2n+1}, n \geqslant 1$	$q^2(q^2+1)(q^2-1)$
${}^2F_4(q)$	$q=2^{2n+1}, n \geqslant 1$	$q^{12}(q^6+1)(q^4-1)(q^3+1)(q-1)$
${}^2F_4(2)'$	$q=2^{2n+1}, n \geqslant 1$	$2^{12}(2^6+1)(2^4-1)(2^3+1)(2-1)/2=17971200$
${}^2G_2(q)$	$q=3^{2n+1}, n \geqslant 1$	$q^3(q^3+1)(q-1)$

以下给出一些数论的结果.

定理 1.33. *(Zsigmondy定理)[311] 设q是大于1的自然数, p是q^n-1的本原素因子, 即$p \mid q^n-1$, 但是对于任何$1 \leqslant i \leqslant n-1$, 有$p \nmid q^i-1$. 如果$n>1$, 且$n, q$不满足以下的两种情况, 则$q^n-1$存在本原素因子.*

(i) $n=2$ 且$q=2^k-1$ (k是自然数);

(ii) $n=6, q=2$.

定义 1.34. 引理1.33中的素数p叫作q^n-1的本原素因子, 且记作q_n, q模p的方次数为n, 记作$exp_p(q)$.

明显q_n-1能被n整除, 则有$q_n \geqslant n+1$. 一个本原素数q_n称为大本原素数, 如果满足$q_n > n+1$或者$q_n^2 \mid q^n-1$. 以下是W. Feit给出了大本原素数的存在性, 见[97].

定理 1.35. 设q, n是大于1的整数, 则q^n-1存在大本原素数, 除了如下几种情形:

(i) $n=2$且$q=2^s3^t-1$, 这里s为某个自然数, $t=0,1$;

(ii) $q=2$且$m=4,6,10,12,18$;

(iii) $q=3$且$m=4,6$;

(iv) $(q,n)=(5,6)$.

如上大本原素数的存在性在研究有理群的时候起到关键作用, 见[99].