关于 $p(kp+1)(kp+2)$ 阶的单群

洪 加 威

(北京市科学技术局)

摘　　要

本文证明了：对于任何一个正整数 n 存在一个正整数 m，使得对任何正整数 $k \leqslant n$ 及任何素数 $p \geqslant m$，阶为 $p(kp+1)(kp+2)$ 的单群都必须同构于 $LF(2, p+1)$ 或 $LF(2, 2p+1)$.

按照 R. Brauer 的一个结果[1]，$p(p+1)(p+2)$ 阶的单群必须同构于 $LF(2, p+1)$，$p+1=2^r$. 1956 年，O. Nagai[2] 证明了：如果 p-Sylow 子群的中心化子就等于自身，那末 $p(2p+1)(2p+2)$阶的单群必须同构于 $LF(2, 2p+1)$. 作者将在另一文[1]中证明定理 1.

定理 1. 阶为 $p(kp+\delta)(kp+2\delta)$ $(\delta = \pm 1, k \leqslant 5)$ 的单群必须同构于:

i) $LF(2, p+1)$, 当 $k=1, \delta=1, p=2^r-1$;

ii) $LF(2, p-1)$, 当 $k=1, \delta=-1, p=2^r+1$;

iii) $LF(2, 2p+1)$, 当 $k=2, \delta=1, p=\frac{1}{2}(q^r-1)$;

iv) $LF(2, 2p-1)$, 当 $k=2, \delta=-1, p=\frac{1}{2}(q^r+1)$;

v) $LF(2, 7)$, 当 $k=3, \delta=-1, p=3$.

于是，我们可以提出，对于任何正整数 n，确定全部 $p(kp+1)(kp+2)$ (其中 $k \leqslant n$)阶单群的工作能够在有限步之内完成吗？作者在老师段学复教授的指导下，证明了下列的定理 2.

定理 2. 对于任何一个正整数 n，存在一个正整数 m，使得对任何正整数 $k \leqslant n$ 及任何素数 $p \geqslant m$，阶为 $p(kp+1)(kp+2)$ 的单群都必须同构于 $LF(2, p+1)$ 或 $LF(2, 2p+1)$.

在这个定理的证明中，我们将看到：确定全部 $p(kp+1)(kp+2)$ (其中 $k \leqslant n$)阶单群的工作，是能够在有限步之内完成的.

证明的大致步骤如下：令 G 是 $g=p(kp+1)(kp+2)$ 阶的单群，P 是 G 的一个 p-Sylow 子群，$N=\mathfrak{N}_G(P)$ 是 P 在 G 中的正规化子. 我们首先证明（见第一节）、对于充分大的 p，$[N:1]=2p$，N 是非交换的，因此，P 是 G 的一个特殊子群，G 是一个(#)群(参看 Harada[3])。根据 Harada 关于(#)群的结果，对于充分大的 p，在 G 的第一个 p-指标块 $B_1(p)$ 中，有一个 $a=kp+1$ 级不可约指标 χ_1，$\frac{1}{2}(p-1)$ 个 $b=kp+2$ 级不可约例外指标 χ_2^σ 和主指标 χ_0.

本文 1972 年 6 月 10 日收到.

1) "阶为 $p(kp+\delta)(kp+2\delta)$, $(\delta=\pm 1, k\leqslant 5)$ 的单群"一文将在《科学通报》发表.

G的元素被分成三部分：p-元素；$(kp+1)$-元素和$(kp+2)$-元素(见第二节)．然后证明对于充分大的p，$a=kp+1$必须是一个素数方幂q^c(见第三节)，并且对于充分大的p，必须有$c=1$或$k=q-1$(见第四节)．对于$c=1$，我们立刻得到$k=2$，$G\cong LF(2,2p+1)$．对于$k=q-1$，我们证明对于充分大的素数p，q-Sylow 子群Q是初等交换q-群，因此是一个 T. I. 集合，$[G:\mathfrak{N}_G(Q)]=kp+2$(见第五节)．最后证明(见第六节)，对于充分大的$p$，$k\leqslant 2$．当$k=1$时，$G\simeq LF(2,p+1)$；当$k=2$时，$G\simeq LF(2,2p+1)$．

一、$\mathfrak{N}_G(P)$ 的阶等于 $2p$

假定p是一个足够大的素数．在这个假定之下，我们将证明：任何一个 p-Sylow 子群的正规化子的阶等于$2p$．$|\mathfrak{N}_G(P)|=2p$．

引理 1. 令G是一个有限群，S是G的一个子群，$N=\mathfrak{N}_G(S)$是S在G中的正规化子．假定S在N内对于G弱封闭．那末，在G的以N的陪集为文字的置换表示中，S恰好保持一个文字不动．

证．假定Nx是被S保持不动的一个陪集，那末，对任何$s\in S$，我们有

$$Nxs=Nx,\quad xsx^{-1}\in N,$$

所以

$$xSx^{-1}\subseteq N.$$

因为S在N内是弱封闭的，故$xSx^{-1}=S$．因此，$x\in\mathfrak{N}_G(S)=N$，也就是说，恰好只有陪集$N\cdot 1$是被S保持不动的．

引理 2. 设U和V都是群，$[U:1]=u$，$[V:1]=v$，$(u,v)=1$．如果$C=U\times V$在一组文字上有一个忠实的置换表示，而且这一组文字被U分成r个传递区，那末

$$v\leqslant r!$$

证略．

引理 3. 令G是一个g阶单群，$g=pg'$，$(p,g')=1$．P是G的一个 p-Sylow 子群，$N=\mathfrak{N}_G(P)$，$[G:N]=1+rp$．令$C=\mathfrak{C}_G(P)$是P的中心化子，$C=V\times P$，$[V:1]=v$．则有

$$v\leqslant r!$$

证．考虑G的以$1+rp$个N的陪集为文字的置换表示．因为P是N的特征子群，所以它在N内弱封闭．根据引理 1，P恰恰保持一个文字不动．又因为G是单群，故表示是忠实的，C在rp个文字上有一个忠实的表示，而这rp个文字又被P分成r个传递区．因此，根据引理 2，$v\leqslant r!$

引理 4. 设$m>0$是一个整数，并设单群G的阶为$g=fp(up+1)$，$f\leqslant m$，$u\leqslant mp$．P是一个 p-Sylow 子群，$N=\mathfrak{N}_G(P)$．假定p充分大，则N的阶等于fp．

证．设$[G:N]=1+rp$，$[N:1]=p(sp+a)$，$0\leqslant a<p$．那末，

$$p(sp+a)(rp+1)=pf(up+1),$$

所以

$$a\equiv f(\mathrm{mod}\ p),\quad a=f.$$

因此，$srp+fr+s=fu$，$m^2p\geqslant fu\geqslant srp$，我们就得到

$$m^2\geqslant sr.$$

如果$s=0$，那末$[N:1]=pa=fp$，引理就成立了．因此，我们不妨设$s\neq 0$，$m^2\geqslant sr\geqslant r$．

考虑以 N 的陪集为文字的置换表示. 令 $C = \mathfrak{C}_G(P) = V \times P$. 我们有 $[N:C] \mid (p-1)$ 以及 $[N:C] \mid (sp+f)$, 因此,

$$[N:C] \mid (p-1, sp+f) = (p-1, s+f),$$

所以

$$[N:C] \mid (s+f), \quad [N:1] \mid (s+f) \cdot [C:1],$$

$$p(sp+f) \mid (s+f) \cdot p \cdot [V:1],$$

$$[V:1] \geqslant (sp+f)/(s+f).$$

但是, $V \lhd N$, $([V:1], p) = 1$. 根据引理 3,

$$[V:1] \leqslant r!,$$

所以

$$(sp+f)/(f+s) \leqslant r!, \quad sp \leqslant r!(f+s),$$

$$p \leqslant r!(1+f/s) \leqslant r!(1+f) \leqslant (m^2)!(1+m).$$

因此,当 p 充分大时必须有 $s=0$, 这就证明了引理 4.

在这里, 单群 G 的阶 $g = p(kp+1)(kp+2) = fp(up+1)$. 其中 $u = \frac{1}{2}(k^2p+3k) \leqslant k^2p$, $f=2$, p 是充分大的. 根据引理 4, 我们断言 $[N:1] = 2p$. 如果 N 是交换的, 容易证明在 G 中存在一个 $(kp+1)(kp+2)$ 阶的正规子群. 因此 N 是非交换的, P 是一个 G 的特殊子群[3], G 是一个(廿)群[3].

二、$B_1(p)$ 的指标

根据 K. Harada 的结果[3], 在 G 的指标块 $B_1(p)$ 中, 有一个 a 级不可约指标 χ_1, $\frac{1}{2}(p-1)$ 个 b 级不可约例外指标 χ_2^σ 和主指标 χ_0, 它们的级数满足

$$1 + a\delta = b\delta, \quad \delta = \pm 1,$$

$$a \equiv \delta \pmod{p}, \quad g = pabd.$$

这里 d 是某个整数, $d \equiv 1 \pmod{p}$. 我们可以写成

$$a = sp + \delta, \quad b = sp + 2\delta, \quad d = tp + 1,$$

这里 s 和 t 是适当的整数. 于是有

$$(tp+1)(sp+\delta)(sp+2\delta) = (kp+1)(kp+2).$$

因此,当 p 充分大时,则 $t=0$, $d=1$, $\delta=1$, $s=k$. 所以

$$g = pab, \quad a = kp+1, \quad b = kp+2.$$

根据(廿)群的性质, G 中所有非单位元素分成三类: p-元素, $(kp+1)$-元素和 $(kp+2)$-元素. $(kp+1)$-元素的总数是 $kp(kp+2)$.

从文献[4,5]可知, $B_1(p)$ 的指标如表 1.

表 1. $B_1(p)$ 的指标

g_i	1	ab	ab	$\cdots$	ab	t_1pb	t_2pb	$\cdots$	t_jpb				
阶	1	p	p	$\cdots$	p	s_1	s_2	$\cdots$	s_j				
χ_0	1	1	1	$\cdots$	1	1	1	$\cdots$	1	1	1	$\cdots$	1
χ_1	$kp+1$	1	1	$\cdots$	1	0	0	$\cdots$	0	-1	-1	$\cdots$	-1
$\chi_{\sigma^1}^2$	$kp+2$	η_0	η_1	$\cdots$	η_{t-1}	1	1	$\cdots$	1	0	0	$\cdots$	0
$\chi_2^{\sigma^2}$	$kp+2$	η_1	η_2	$\cdots$	η_0	1	1	$\cdots$	1	0	0	$\cdots$	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$		$\vdots$
$\chi_2^{\sigma^t}$	$kp+2$	η_{t-1}	η_0	$\cdots$	η_{t-2}	1	1	$\cdots$	1	0	0	$\cdots$	0

这里 $t=\frac{1}{2}(p-1)$, $\chi_2^{s_1}$, $\chi_2^{s_2}$, $\cdots$, $\chi_2^{s_t}$ 是 t 个不同的 p-共轭指标. 令 ϵ 是 1 的 p 次本原根, γ 是模 p 的一个本原根,

$$\epsilon_0=\epsilon^{\gamma^0},\ \epsilon_1=\epsilon^{\gamma^1},\ \cdots,\ \epsilon_{p-2}=\epsilon^{\gamma^{p-2}},\ \epsilon_{p-1}=\epsilon^{\gamma^{p-1}}=\epsilon^{\gamma^0}=\epsilon_0.$$

$$\eta_0=\epsilon_0+\epsilon_t,\ \eta_1=\epsilon_1+\epsilon_{t+1},\ \cdots,\ \eta_{t-1}=\epsilon_{t-1}+\epsilon_{2t-1},$$

$s_1, s_2, \cdots, s_t$ 是 $kp+1$ 的某些因子.

引理 5. 假设 q 是一个不等于 p 的素数, $q\mid g$. 那末, 存在 q-最高块 $B_s(q)$, $\cdots$, $B_l(q)$, 使得

$$B_1(q)\cup B_s(q)\cup\cdots\cup B_l(q)\supseteq B_1(p).$$

证. 因为 G 是一个单纯(非)群, 所有级数与 p 互素的指标都包含在 $B_1(p)$ 中. 显然, $\chi_0\in B_1(p)\cap B_1(q)$. 首先, 我们假定 $\chi_1\notin B_1(p)\cap B_1(q)$, 则 $B_1(p)\cap B_1(q)$ 由 χ_0 和某些 χ_2^σ 组成. 我们把 σ 分成两个集合: 如果 $\chi_2^\sigma\in B_1(p)\cap B_1(q)$, 就令 $\sigma\in\Delta$; 否则就令 $\sigma\in\Delta'$. 令 y 是一个 p 阶元, 设 $q^c\| g$, 我们有

$$\chi_0(1)\chi_0(y)+\sum_{\sigma\in\Delta}\chi_2^\sigma(1)\chi_2^\sigma(y)\equiv 0(\mathrm{mod}\ q^c).$$

从表 1 得知, $\chi_2^\sigma(y)=\nu_{i_\sigma}$, 对于不同的 σ, i_σ 是互不相同的. 我们有

$$1+\chi_2(1)\sum_{\sigma\in\Delta}\eta_{i_\sigma}\equiv 0(\mathrm{mod}\ q^c).$$

但是, $1+\eta_0+\eta_1+\cdots+\eta_{t-1}=0$, 因此

$$-\left(\sum_{\sigma\in\Delta}\eta_{i_\sigma}+\sum_{\sigma\in\Delta'}\eta_{i_\sigma}\right)+\chi_2(1)\sum_{\sigma\in\Delta}\eta_{i_\sigma}\equiv 0(\mathrm{mod}\ q^c),$$

故

$$-\frac{1}{q^c}\sum_{\sigma\in\Delta'}\eta_{i_\sigma}+\frac{\chi_2(1)-1}{q^c}\sum_{\sigma\in\Delta}\eta_{i_\sigma}$$

是一个代数整量. 如果 $\sigma\neq\tau$, 那末 $i_\sigma\neq i_\tau$, 被包含在 η_{i_σ} 和 η_{i_τ} 中的 ϵ 的方幂也就完全不同. 但是 $\epsilon_0, \epsilon_1, \cdots, \epsilon_{p-1}$ 构成一组基, 在域 $R(\epsilon)$ 中, 每一个代数整量都是 ϵ 的整多项式, 因此我们得到:

1) Δ' 是空集,

2) $(\chi_2(1)-1)/q^c=\chi_1(1)/q^c$ 是一个整数. 于是 χ_1 被包含在一个 q-最高块之中.

如果我们置 $B_s(q)=\{\chi_1\}$, 立刻得到

$$B_1(q)\cup B_s(q)\supseteq B_1(p).$$

现在, 我们假定 $\chi_1\in B_1(p)\cap B_1(q)$. 用同样的方法, 我们得到

$$1+\chi_1(1)+\chi_2(1)\sum_{\sigma\in\Delta}\eta_{i_\sigma}\equiv 0(\mathrm{mod}\ q^c),$$

$$(-1-\chi_1(1))\left(\sum_{\sigma\in\Delta}\eta_{i_\sigma}+\sum_{\sigma\in\Delta'}\eta_{i_\sigma}\right)+\chi_2(1)\sum_{\sigma\in\Delta}\eta_{i_\sigma}\equiv 0(\mathrm{mod}\ q^c).$$

因此

$$\frac{1}{q^c}(-1-\chi_1(1)+\chi_2(1))\sum_{\sigma\in\Delta}\eta_{i_\sigma}-\frac{1}{q^c}(1+\chi_1(1))\sum_{\sigma\in\Delta'}\eta_{i_\sigma}=-\frac{1}{q^c}\chi_2(1)\sum_{\sigma\in\Delta'}\eta_{i_\sigma}$$

是一个代数整量. 如果 Δ' 是空集, 那末 $B_1(q)\supseteq B_1(p)$. 如果确有某些 σ 属于 Δ', 那末 $q^c\mid\chi_2(1)$, 每一个 χ_2^σ 构成一个 q-最高块, 把它们取作 $B_s(q)$, $\cdots$, $B_l(q)$, 就有

$$B_1(q)\cup B_s(q)\cup\cdots\cup B_l(q)\supseteq B_1(p).$$

三、a 是一个素数方幂 ($a = q^c$)

我们用 $\pi(s)$ 标记在 s 中出现的不同素因子的个数. 任给两个正整数 s 与 t, s 一定有这样的因子: 它的每个素因子都在 t 中出现. 把 s 的这种因子中的最大者记为 s_t.

引理 6. 假定 G 是一个单群, $|G| = g = pabd$, $|\mathfrak{N}_G(P)| = 2p$. 那末

$$\pi(a) < 2\ln ad_a/\ln 2p,$$
$$\pi(d) < 2\ln dd_d/\ln 2p.$$

证. 假定 $r^i \| a$, 根据引理 5, $\frac{1}{2}(p-1)$ 个 b 级例外指标全都属于 $B_1(r)$, 因此 $B_1(r)$ 至少包含有 $\frac{1}{2}(p+1)$ 个指标. 但是,如果 $r^{i_0} \| g$, 根据 R. Brauer 和 Feit 的结果[6], 在 $B_1(r)$ 中至多有 $\frac{1}{4} r^{2i_0}$ 个不可约指标,所以

$$\frac{1}{2}(p+1) \leqslant \frac{1}{4} r^{2i_0}.$$

现在, a 中出现有 $\pi(a)$ 个不同的素数 $r_1, r_2, \cdots, r_{\pi(a)}$, 因此

$$\left[\frac{1}{2}(p+1)\right]^{\pi(a)} \leqslant \left(\frac{1}{4}\right)^{\pi(a)} r_1^{2i_{01}} \cdot r_2^{2i_{02}} \cdots r_{\pi(a)}^{2i_{0\pi(a)}}.$$

这里 $r_j^{i_{0j}} \| g$. 显然, $r_j^{i_{0j}} \| ad$, $r_j^{i_{0j}} \| ad_a$. 因此

$$\left[\frac{1}{2}(p+1)\right]^{\pi(a)} \leqslant \left(\frac{1}{4}\right)^{\pi(a)} (ad_a)^2,$$

所以

$$(2p)^{\pi(a)} < (ad_a)^2,$$
$$\pi(a) < 2\ln ad_a/\ln 2p.$$

第二个不等式可以同样证明.

我们已经证明了 $\lim\limits_{p\to\infty} d = 1$,所以

$$\lim_{p\to\infty}(2\ln ad_a/\ln 2p) = \lim_{p\to\infty}(2\ln a/\ln 2p) = \lim_{p\to\infty}(2\ln(kp+1)/\ln 2p) = 2.$$

于是,当 p 充分大时, $\pi(a) \leqslant 2$. 也就是说, a 中最多包含两个不同的素因子,我们假定

$$a = kp + 1 = q^m \cdot r^n.$$

如果 $m \geqslant 1$, $n \geqslant 1$, 假定在 G 中有 μ 个 q^m-类, 它们的代表元素是 $x_1, x_2, \cdots, x_\mu$, 每类分别包含有 $u_1 pb, u_2 pb, \cdots, u_\mu pb$ 个元素. 还假定在 G 中有 ν 个 r^n-类, 它们的代表元素是 $y_1, y_2, \cdots, y_\nu$, 每类分别包含 $v_1 pb, v_2 pb, \cdots, v_\nu pb$ 个元素. 假定 x_i 恰和 s_{ij} 个与 y_j 共轭的元素交换,且 y_j 恰和 t_{ij} 个与 x_i 共轭的元素相交换. 显然

$$u_i s_{ij} = v_j t_{ij}.$$

如果 G 中元素 z 的阶是 $q^{m_1} r^{n_1}$, $m_1 > 0$, $n_1 > 0$, 我们就称 z 为一个混合元素. 显然, 其 q-部分共轭于 x_i, 且 r-部分又共轭于 y_j 的混合元素的总数是

$$u_i pbs_{ij} = v_j pbt_{ij}.$$

假定有 i_0, j_0, 使得 $s_{i_0 j_0} \neq 0$, 那末 $t_{i_0 j_0} \neq 0$. 在这种情形, $\mathfrak{N}(x_{i_0})$ 中存在一个 r 阶的元素, 因此,我们能假定在 $\mathfrak{N}(x_{i_0})$ 中的 r-Sylow 子群的阶是 r^{n_1}, $n_1 > 0$.

可以证明, r^{n-n_1} 是共轭于 x_{i_0} 的元素的总数的一个因子

$$r^{n-n_1} \mid u_{i_0} pb, \quad r^{n-n_1} \mid u_{i_0}.$$

在 G 中，与 x_{i_0} 交换的 r^n-元素的总数是 $\sum_j s_{i_0 j}$，因此

$$r^{n_1} - 1 \leqslant \sum_j s_{i_0 j}.$$

所以

$$\begin{aligned}\sum_i u_{i_0 i} pbs_{i_0 j} &\geqslant pbr^{n-n_1} \sum_j s_{i_0 j} \\ &\geqslant pbr^{n-n_1}(r^{n_1} - 1) \\ &\geqslant pbr^{n-n_1}(r^{n_1} - r^{n_1-1}) \\ &= pbr^n \cdot \left(\frac{r-1}{r}\right).\end{aligned}$$

同样，可以证明

$$\sum_i v_{j_0 i} pbt_{ij_0} \geqslant pbq^m \left(\frac{q-1}{q}\right).$$

容易看到，如果 $l = \sum_i \sum_j u_i pbs_{ij} = \sum_i \sum_j v_j pbt_{ij}$，则有 $kpb > l$. 但

$$l \geqslant \sum_j u_{i_0 j} pbs_{i_0 j} \geqslant pbr^n \left(\frac{r-1}{r}\right),$$

$$l \geqslant \sum_i v_{j_0 i} pbt_{ij_0} \geqslant pbq^m \left(\frac{q-1}{q}\right).$$

因此，

$$(kpb)^2 > l^2 \geqslant (pb)^2 r^n q^m \left(\frac{r-1}{r}\right)\left(\frac{q-1}{q}\right)$$

$$\geqslant \frac{1}{3}(pb)^2 q^m r^n.$$

所以 $$k^2 > \frac{a}{3} > \frac{1}{3} kp, \quad 3k > p.$$

所以，对充分大的 p，不存在混合元素，也就是说，$s_{ij} = t_{ij} = 0$. 因此，一个 q 阶的共轭类至少包含 pbr^n 个元素，一个 r 阶的共轭类至少包含 pbq^m 个元素. 于是

$$kpb \geqslant q^m pb + r^n pb,$$

$$k \geqslant q^m + r^n \geqslant 2\sqrt{q^m r^n} = 2\sqrt{a},$$

所以 $$kp + 1 \leqslant \frac{1}{4} k^2, \quad p \leqslant \frac{1}{4} k.$$

这就证明了：当 p 充分大时，$a = q^c$ 是一个素数方幂.

四、$k = q - 1$ 或 $k = 2$, G 同构于 $LF(2, 2p+1)$

引理 7. 对于固定的 k，如果 $kp + 1 = q^c$，那末 p 是有界的. 除非 $k = q - 1$ 或 $c = 1$.

证. 假定 $k \neq q - 1$，$c \neq 1$，我们将证明 p 是有界的.

由

$$kp = q^c - 1 = (q-1)(q^{c-1} + \cdots + q + 1),$$

如果 $p \mid (q-1)$，那末

$$(q^{c-1} + \cdots + q + 1) \mid k.$$

于是 $q^c < k^2$, p 就是有界的了.

因此我们能够假定 $p \nmid (q-1)$. 那末

$$p \mid (q^{c-1} + \cdots + q + 1), \quad (q-1) \mid k.$$

于是 q 是有界的. 假定 d 是使得 $q^d \equiv 1 (\mathrm{mod}\, k)$ 成立的最小正整数,那末 $d \mid c$, $c = de$, e 是某个整数. 我们有

$$kp = q^{de} - 1 = (q^d - 1)(q^{d(e-1)} + \cdots + q^d + 1).$$

如果 $p \mid (q^d - 1)$, 则

$$(q^{d(e-1)} + \cdots + q^d + 1) \mid k.$$

当 $e = 1$ 时, $c = d \leqslant \varphi(k)$, φ 表示欧拉函数; 既然 q 是有界的,当然 q^c 和 p 也都是有界的. 当 $e \neq 1$ 时,我们有 $q^{d(e-1)} < k$, $q^c = q^{de} < k^2$. 所以 q^c 和 p 都是有界的.

因此,我们能够假定 $p \nmid (q^d - 1)$. 那末

$$p \mid (q^{d(e-1)} + \cdots + q^d + 1),$$

$$(q^d - 1) \mid k.$$

因为 $q^d \equiv 1 (\mathrm{mod}\, k)$, 我们得到 $k = q^d - 1$, 故 $d \neq 1$. 我们有

$$kp = q^{de} - 1 = (q^e - 1)(q^{e(d-1)} + \cdots + q^e + 1).$$

如果 $p \mid (q^e - 1)$, 则有

$$(q^{e(d-1)} + \cdots + q^e + 1) \mid k, \quad q^e = q^{de} < k^2,$$

q^e 和 p 都是有界的. 因此,我们假定 $p \nmid (q^e - 1)$, 于是

$$p \mid (q^{e(d-1)} + \cdots + q^e + 1), \quad (q^e - 1) \mid k = q^d - 1.$$

于是, $e \leqslant d$,

$$q^e = q^{de} \leqslant q^{d \cdot d} = (k+1)^d \leqslant (k+1)^{\varphi(k)} \leqslant (k+1)^k.$$

因此, $p = (q^e - 1)/k$ 有界. 引理 7 证毕.

设 $a = kp + 1 = q^e$, 当 p 充分大时,我们有

$k = q - 1$ 或 $e = 1$. 假定 $e = 1$, 那末

$$g = pq(kp + 2), \quad q = kp + 1,$$

则有

$$q^3 > g.$$

根据 R. Brauer 和 W. F. Reynolds 的结果[7], G 同构于 $LF(2, q)$ 或 $LF(2, q-1)$. 因为 $q - 1 = kp$, 不是 2 的方幂,群 $LF(2, q-1)$ 不是解. 如果 $G \cong LF(2, q)$, 那末

$$g = \frac{1}{2} q(q-1)(q+1) = pq(q+1),$$

$$q = 2p + 1, \quad k = 2.$$

从现在起,我们假定 $k = q - 1$.

五、q-Sylow 子群 Q 是一个初等 Abelian q-群

令 x 是一个 q^e-元素,那末与 x 共轭的元素的总数是 upb. 这里 u 是 q 的一个方幂, $u = q^i$. 考虑到 $k = q - 1$ 以及 $k \geqslant q^i$,我们得到 $i = 0$. 因此,每个 q^e-元素属于某个 q-Sylow 子群的中心,每个 q-非正则类恰好包含 pb 个元素.

我们考虑 $N = \mathfrak{N}_G(Q) \supseteq Q$. 如果 $N = Q$, 根据 H. Wielandt 的一个定理(见文献[8, Satz

2])，对于任何一个Q的正规子群Q_0，只要Q/Q_0是交换的，就存在G的一个正规子群G_0，使得

$$G/G_0 \cong Q/Q_0.$$

我们取Q的某个极大子群作为Q_0，因为G是单群，故$N = Q$是不可能的，所以$N \supset Q$.

我们将要证明存在一个Q的p阶自同构，它仅仅保持单位元不变．为了这个目的，我们将证明$p|[N:Q]$．考虑以N的陪集为文字的置换表示，假定这个表示的指标是χ．因为$[G:N] = \chi(1)$，所以我们想要证明$p \nmid \chi(1)$.

设$p|\chi(1)$．我们知道χ包含χ_0恰好一次，因此χ必须还包含某个$B_1(p)$的指标.

情形1．如果χ包含某个$b = kp + 2$级指标，它就必须包含所有的$\frac{1}{2}(p-1)$个b级的p-共轭指标．因此

$$\chi(1) \geqslant 1 + \frac{1}{2}(p-1)(kp+2).$$

但，$\chi(1) = [G:N]$，$[G:Q] = p(kp+2)$．令$\omega = [N:Q]$，就有

$$\omega = [G:Q]/[G:N]$$
$$\leqslant p(kp+2)\Big/\Big(1 + \frac{1}{2}(p-1)(kp+2)\Big) \xrightarrow[p\to\infty]{} 2.$$

因此，当p充分大时，$\omega \leqslant 2$．我们已证明了$\omega \neq 1$，所以$\omega = 2$，Q有一个2阶自同构，它仅仅保持单位元不变．根据R. Brauer和K. Fowler的一个定理(见文献[9，定理(4B)])，Q是交换的．因为q^r-元素只和q^r-元素以及单位交换，Q是一个T. I集合．q-Sylow子群的总数是

$$kp(kp+2)/(q^r - 1) = kp + 2.$$

于是，$[N:1] = p(kp+1) = 2(kp+1)$，这是不可能的，因此$\chi$不能包含$b$级的指标.

情形2．χ包含u个a级指标，因此

$$\chi(1) = 1 + u(kp+1) + sp.$$

因为我们假定了$p|\chi(1)$，所以

$$p|(1+u), \quad u \geqslant p-1,$$
$$\chi(1) \geqslant 1 + (p-1)(kp+1),$$
$$\omega = p(kp+2)/\chi(1) \leqslant \frac{p(kp+2)}{1+(p-1)(kp+1)} \xrightarrow[p\to\infty]{} 1.$$

所以，当p充分大时，$\omega = 1$，这是不可能的．因此，$p \nmid \chi(1)$．存在一个Q的p阶自同构，它仅仅保持单位元不变.

现在假定$Q = Q_0 \supset Q_1 \supset Q_2 \supset \cdots \supset Q_l = 1$．这里$Q_i$是$Q$的特征子群．我们把$l$称为这个特征链的长度.

引理8. 如果q-群Q有一个p阶自同构τ仅仅保持单位元不变，l是Q的某个特征链的长度，则有

$$l \leqslant \ln[Q:1]/\ln(p+1).$$

证．假定特征链是

$$Q = Q_0 \supset Q_1 \supset Q_2 \supset \cdots \supset Q_l = 1.$$

我们将要证明$[Q_{i-1}:Q_i] \geqslant p+1$.

对于任意的x_1，$x_2 \in Q_i$，如$x_1(x_1^{-1})^\tau = x_2(x_2^{-1})^\tau$，那末$x_2^{-1}x_1 = (x_2^{-1}x_1)^\tau$，因此，$x_2^{-1}x_1 = 1$，

$x_1 = x_2$. 因此，如果 $x_1 \neq x_2$，就有 $x_1(x_1^{-1})^\tau \neq x_2(x_2^{-1})^\tau$. 故所有 Q_i 的元素都能写成 $x(x^{-1})^\tau$ $(x \in Q_i)$ 的形式.

假若 $[Q_{i-1}:Q_i] \leqslant p$，那末 $(Q_i x)^\tau = Q_i x$. 对某个 $x \in Q_{i-1}$，$x \notin Q_i$ 成立. 这时，$x^\tau = xy$，$y \in Q_i$. 令 $y = z(z^{-1})^\tau$，$z \in Q_i$. 我们有

$$(xz)^\tau = x^\tau z^\tau = xy \cdot z^\tau = x \cdot z(z^{-1})^\tau \cdot z^\tau = xz.$$

τ 保持 xz 不变，所以 $xz = 1$. 但是 $x \notin Q_i$，$z \in Q_i$，这是不可能的，因此 $[Q_{i-1}:Q_i] \geqslant p+1$. 我们立即得到

$$[Q:1] \geqslant (p+1)^l,$$
$$l \leqslant \ln[Q:1]/\ln(p+1).$$

在我们的情形，

$$\lim_{p\to\infty} \ln[Q:1]/\ln(p+1) = \lim_{p\to\infty} \ln(kp+1)/\ln(p+1) = 1,$$

故当 p 充分大时，$l = 1$. 也就是说，不存在 Q 的真特征子群. 因此，$\mathfrak{C}(Q) = Q$，Q 是交换的. $Q^q = 1$，Q 是初等 Abelian q-群，且 Q 是一个 T. I 集合，$[G:N] = kp+2$.

六、$k \leqslant 2$, G 同构于 $LF(2, p+1)$ 或 $LF(2, 2p+1)$

我们将证明当 p 充分大以后，就有 $k \leqslant 2$，并且 $G \cong LF(2, p+1)$ 或 $LF(2, 2p+1)$.

令 $N = \mathfrak{N}_G(Q)$，$[N:1] = pq^c$. 令 P 是 N 的一个 p-Sylow 子群. 每一个 P 中的非单位元素都在 Q 中产生一个 p 阶的自同构 τ. 每一个 Q 的元素都能写成形状 $x(x^{-1})^\tau$，$x \in Q$. 因此 N 的换位子群就是 Q. N/Q 的 p 个线性指标就是 N 的全部线性指标. P 在 N 中的正规化子的阶是 p 或者 $2p$. 如果它是 $2p$，那末 $q = 2$. 根据 Sylow 定理，$q^{c-1} \equiv 1 \pmod p$. 但是 $q^c = kp+1$，故 $q^c = kp+1 \equiv 2 \pmod p$，或 $1 \equiv 2 \pmod p$，这是不可能的. 因此 P 在 N 中的正规化子就是 P.

因为 Q 是交换的，并且 $([Q:1]-1)/[N:Q] = k$，故在 N 中恰有 k 个 q-类，容易看到，在 N 中恰有 $p-1$ 个 p-类. 因此，在 N 中恰有 $p+k$ 个共轭类.

假定 N 的 p-最高块的指标的级数是 $h_1 p, \cdots, h_j p$. 在 $B_1(p)$ 中，有 p 个线性指标，于是我们有 $j+p$ 个不可约指标，所以 $j = k$. 我们有

$$(h_1 p)^2 + (h_2 p)^2 + \cdots + (h_k p)^2 + p = [N:1] = p(kp+1),$$
$$h_1^2 + h_2^2 + \cdots + h_k^2 = k, \quad h_1 = h_2 = \cdots = h_k = 1.$$

于是，N 有 p 个线性指标 $\omega^1, \omega^2, \cdots, \omega^p = \omega^0$ 和 k 个 p 级指标 $\varphi_1, \varphi_2, \cdots, \varphi_k$. 下面是 N 的指标表.

表 2. N 的指标表

阶	1	p	p	$\cdots$	p	q	q	$\cdots$	q
ω^0	1	1	1	$\cdots$	1	1	1	$\cdots$	1
ω^1	1	ϵ	ϵ^2	$\cdots$	ϵ^{p-1}	1	1	$\cdots$	1
ω^2	1	ϵ^2	ϵ^4	$\cdots$	ϵ^{p-2}	1	1	$\cdots$	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$		$\vdots$
ω^{p-1}	1	ϵ^{p-1}	ϵ^{p-2}	$\cdots$	ϵ	1	1	$\cdots$	1
φ_1	p	0	0	$\cdots$	0	α_{11}	α_{12}	$\cdots$	α_{1k}
φ_2	p	0	0	$\cdots$	0	α_{21}	α_{22}	$\cdots$	α_{2k}
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$		$\vdots$
φ_k	p	0	0	$\cdots$	0	α_{k1}	α_{k2}	$\cdots$	α_{kk}

既然 Q 是一个 T. I 集合，φ_i 在 Q 以外的值为 0，因此 $\varphi_1, \varphi_2, \cdots, \varphi_k$ 是例外指标[10]，一定有 k 个 G 的不可约指标 $\phi_1, \phi_2, \cdots, \phi_k$，使得

$$\phi_i = \pm \varphi_i + u\Phi + \Omega.$$

这里 $\Phi = \varphi_1 + \varphi_2 + \cdots + \varphi_k$，$\Omega$ 是 N 的某些线性指标的和. 我们有 $\phi_1(1) = \phi_2(1) = \cdots = \phi_k(1)$，但是 $\phi_1, \phi_2, \cdots, \phi_k$ 在 q 阶元上有不同的值，因此 $\phi_i \notin B_1(p)$. ϕ_i 是属于 p-最高类的，所以它在 p 阶元上的值为 0. 如果 x 是一个 p 阶元，

$$0 = \phi_i(x) = \pm \varphi_i(x) + u\Phi(x) + \Omega(x),$$

所以

$$\Omega(x) = 0.$$

我们可写成

$$\Omega = v\Omega_0, \quad \Omega_0 = \omega^0 + \omega^1 + \cdots + \omega^{p-1}.$$

$$\phi_i = \pm \varphi_i + u\Phi + v\Omega_0, \quad i = 1, 2, \cdots, k.$$

假定还有另外的 p-最高类指标 ϕ，利用例外指标的性质，考虑到 $\phi(x) = 0$ 对 $x \in P$ 成立，我们可写成

$$\phi = t\Phi + s\Omega_0.$$

容易看到，χ_1 包含 ω^0 一次并且不再包含别的线性指标了，因此

$$\chi_1 = \omega^0 + \Phi.$$

χ_2^σ 包含两个线性指标 $\omega^{t\sigma}$, $\omega^{j\sigma}$，

$$\chi_2^\sigma = \omega^{t\sigma} + \omega^{j\sigma} + \Phi.$$

令 α 是 G 的正则表示的指标，β 是 N 的正则表示的指标，则有

$$\alpha = (kp + 2)\beta.$$

每一个线性指标在 β 中出现一次，因此 β 包含 p 个线性指标，α 包含 $(kp + 2)p$ 个线性指标. 但是

$$\alpha = 1 + (kp + 1)\chi_1 + \sum_\sigma (kp + 2)\chi_2^\sigma + \sum_\psi \psi(1)\psi,$$

这里 ψ 跑遍所有 p-最高类指标. 指标 $1 + (kp + 1)\chi_1 + \sum_\sigma (kp + 2)\chi_2^\sigma$ 包含了 $1+(kp+1)+\frac{1}{2}(p-1)(kp+2)\cdot 2 = p(kp+2)$ 个线性指标，即 α 中的全部线性指标. 因此，$\sum_\psi \psi(1)\psi$ 不再包含线性指标. 也就是说，

$$v = 0, \ s = 0.$$

$$\phi_i = \pm \varphi_i + u\Phi,$$

$$\phi = t\Phi.$$

令 G 中的实类数为 k_1，G 中二阶元的总数为 m. 根据 R. Brauer 和 K. Fowler 的结果(见文献 [9, 定理 (2J)])，我们有

$$k_1 - 1 \geqslant m(m + 1)/g.$$

显然，$m \geqslant p(kp + 1)$，因此

$$\begin{aligned} k_1 - 1 &\geqslant p(kp + 1)(p(kp + 1) + 1)/p(kp + 1)(kp + 2) \\ &= (p(kp + 1) + 1)/(kp + 2). \end{aligned}$$

令非例外的 p-最高类指标的总数为 f，就有

$$1 + 1 + \frac{1}{2}(p - 1) + k + f \geqslant (p(kp + 1) + 1)/(kp + 2).$$

可见，当 p 充分大时，$f>0$. 也就是说，确实存在一个 G^* 的不可约指标 ϕ，使 $\phi=t\Phi$，

$$\phi(1)=t\Phi(1)=tkp.$$

因为 ϕ 是不可约的，故 $\phi(1)\mid g$，

$$tkp\mid p(kp+1)(kp+2),$$

$$k\mid 2,\quad k=1 \quad 或 \quad k=2.$$

当 $k=1$ 时根据 R. Brauer[1] 的结果，$G\cong LF(2,p+1)$；当 $k=2$ 时，我们已证明 p-Sylow 子群的中心化子就等于自身，故 Nagai[2] 的结果可以使用，$G\cong LF(2,2p+1)$.

参 考 文 献

[1] Brauer, R., 1943 *Ann. of Math.*, **44**, 57—79.
[2] Nagai, O., 1956 *Osaka Math. J.*, **8**, 107—117.
[3] Harada, K., 1967 *Ill. J. Math.*, **11**, 647—659.
[4] Brauer, R., 1942 *Amer. J. Math.*, **64**, 401—420.
[5] Brauer, R. and Tuan, H. F., 1945 *Bull. Amer. Math. Soc.*, **51**, 756—766.
[6] Brauer, R. and Feit, W., 1959 *Proc. Nat. Acad. Sci.*, **45**, 361—365.
[7] Brauer, R. and Reynolds, W. F., 1958 *Ann. of Math.*, **68**, 713—720.
[8] Wielandt, H., 1940 *J. Reine und Angew. Math.*, **182**, 180—193.
[9] Brauer, R. and Fowler, K., 1955 *Ann. of Math.*, **62**, 565—583.
[10] Feit, W., 1960 Institute on Finite Groups, at California, pp. 67—70.