2^3p 阶群的构造（p为奇质数）

张 远 达

本文讨论 2^3p 阶群 G（p 为奇质数）的构造。结果是：当 $p\neq 3$ 及 7 时，G 共有12型在 $p\equiv 3(\mathrm{mod}\ 4)$时，$G$ 共有 11 型在 $p\equiv 5(\mathrm{mod}\ 8)$时，而 G 共有15型在 $p\equiv 1(\mathrm{mod}\ 8)$时；但当 $p=3$ 时即24阶群共有15型；当 $p=7$ 时即56阶群共有13型。

讨论 2^3p 阶群的构造，我们假定人们已知道 $4p$ 阶群的构造，列表于下：

（表 一）

	型	构造（定义关系）	附注
4p阶群（p为奇质数）	I	$G=\{a\}$, $a^{4p}=1$ （循环群）	
	II	$G=\{a\}\times\{b\}\times\{c\}$, $a^2=b^2=c^p=1=[a,b]=[b,c]=[c,a]$ （初等交换）	
	III	$G=\{a,b\}$, $a^{2p}=b^2=1$, $b^{-1}ab=a^{-1}$	
	IV	$G=\{a,b\}$, $a^{2p}=1$, $b^2=a^p$, $b^{-1}ab=a^{-1}$	
	V	$G=\{a,b,c\}$, $a^p=b^2=1$, $c^2=b$, $b^{-1}ab=a^{-1}$, $cb=bc$, $c^{-1}ac=a^k$, 但 $k^2\equiv -1\ (\mathrm{mod}\ p)$	仅在 $p\equiv 1(\mathrm{mod}\ 4)$时，才出现这一型。
		$G=\{a,b,c\}$, $a^2=b^2=c^3=1$, $c^{-1}ac=b$, $c^{-1}bc=ab=ba$	仅在 $p=3$ 时，才出现这一型，这时 $G\simeq A_4$（四次交代群）

今设群 G 的阶 $o(G)=2^3p$（p 为奇质数）。

为讨论方便，先假定 $p\neq 3$ 且 $p\neq 7$。于是这时有 $(p,(2-1)(2^2-1)(2^3-1))=1$，而 G 为 2-幂零的[1],[2]，即 G 实际上有西洛塔 (sylow-tower)[3]，也就是说如 $M_1\triangleleft G$ 且 $o(M_1)=p$ 之 M_1 必存在（$M_1\triangleleft G$ 表示 M_1 为 G 之正规子群）。因之由 M_1 之循环性以及 G/M_1 之幂零性易知 G 是超可解的（因 G 为循环群 M_1 被超可解群 G/M_1 之扩张），故 G 必有一个指数为 2 的正规子群 A，即 $A\triangleleft G$ 且 $o(A)=2^2p=4p$。于是 A 只能为表一中的型 I ——V。

先讨论型（I） （即 $A=\{a\}$, $a^{4p}=1$）。于是因 G 为 A 被 2 阶（循环）群之扩张，故

这时有 $G=\{a,g\}$, $a^{4p}=1$, $g^2=a^t$, $g^{-1}ag=a^r$, 式中 $r^2\equiv 1\pmod{4p}$ 与 $t(r-1)\equiv o\pmod{4p}$[文献[2]中129页定理21]。但 $r^2\equiv 1\pmod{4p}$有4个解，即 $r\equiv 1,\ -1,\ 2p+1,\ 2p-1\pmod{4p}$。

在 $r\equiv 1\pmod{4p}$时，G 是交换群；又因它已有阶4的元，故交换群 G 只能是次二个可能，即

(i) $G\doteq\{x\}$ 为 $8p=2^3p$ 阶的循环群($x^8=1$)；

(ii) $G=\{x\}\times\{y\}\times\{z\}$ 为 p 阶、4阶、2阶这样三个循环群之直积 ($x^p=y^4=z^2=1=[x,y]=[y,z]=[z,x]$)。

在 $r\equiv -1\pmod{4p}$时，必 $t\equiv o\pmod{2p}$，故 $g^2=1$ 或 $=a^p$，随而 G 又为次二个可能性，如

(iii) $G=\{a,g\}$, $a^p=g^2=1$, $g^{-1}ag=a^{-1}$；

(iv) $G=\{a,g\}$, $a^{4p}=1$, $g^2=a^{2p}$, $g^{-1}ag=a^{-1}$。

在 $r\equiv 2p+1\pmod{4p}$，必有 $t\equiv 0\pmod 2$，故 $t=2(2k+1)$ 或 $t=2^2k$。因 $\frac{p+1}{2}x\equiv -k\pmod p$有解 x，故再令 $g_1=a^xg$ 时就有 $G=\{a,g\}=\{a,g_1\}$, $a^{4p}=1$, $g_1^{-1}ag_1=a^{2p+1}$, $g_1^2=\begin{cases}a^2\ (\text{当 } t=2(2k+1)\text{时}),\\ 1\ (\text{当 } t=4k\text{ 时})。\end{cases}$ 这说明了 G 又仅为次二个可能，如

(v) $G=\{a,g\}$, $a^{2p}=1$, $g^2=1$, $g^{-1}ag=a^{2p-1}$；

(vi) $G=\{a,g\}$, $a^{4p}=1$, $g^2=a^2$, $g^{-1}ag=a^{2p+1}$。

在 $r\equiv 2p-1\pmod{4p}$ 时，必有 $t\equiv 0\pmod p$，故 $g^2=1$、a^p、a^{2p} 或 a^{3p} 只这四个可能。但令 $g_1=ag$ 后又显有 $G=\{a,g\}=\{a,g_1\}$，其中 $g_1^{-1}ag_1=a^{2p-1}$, $g_1^2=a^{2p+t}=\begin{cases}1\ (t=2p\text{ 时}),\\ a^p\ (t=3p\text{ 时})。\end{cases}$ 这说明了 G 仅为次二型，即

(vii) $G=\{a,g\}$, $a^{4p}=1$, $g^2=1$, $g^{-1}ag=a^{2p-1}$；

(viii) $G=\{a,g\}$, $a^{4p}=1$, $g^2=a^p$, $g^{-1}ag=a^{2p-1}$。

再讨论表一中的型(Ⅱ) (即 $A=\{a,b,c\}$, $a^2=b^2=c^p=1=[a,b]=[b,c]=[c,a]$)。于是这时有 $G=\{a,b,c,g\}$，除 a,b,c 间之关系如上述外还有 $g^2=u=a^kb^lc^m$, $g^{-1}xg=x^\sigma$ (每 $x\in A$)，σ 为 A 之自同构，但 $\sigma^2=1$ (A 之恒等自同构)且 $u^\sigma=u$。

因 A 中阶2的元仅为 a、b 与 ab，阶 p 的元仅为 $c^i(i=1,2,\cdots,p)$，故必有

$$\begin{cases}a^\sigma=g^{-1}ag=a^\lambda b^\mu,\\ b^\sigma=g^{-1}bg=a^\delta b^\nu,\\ c^\sigma=g^{-1}cg=c^i(i=1,2,\cdots,p-1),\end{cases}\qquad \text{且}\begin{vmatrix}\lambda & \mu\\ \delta & \nu\end{vmatrix}\not\equiv 0\pmod 2。$$

再利用 $a^{\sigma^2}=a$, $b^{\sigma^2}=b$, $c^{\sigma^2}=c$，又可得：

$$\left.\begin{aligned}&\lambda^2+\mu\delta\equiv 1\\&\nu^2+\mu\delta\equiv 1\\&\mu(\lambda+\nu)\equiv 0\\&\delta(\lambda+\nu)\equiv 0\end{aligned}\right\}\pmod 2 \text{ 及 } i^2\equiv 1 \pmod p.$$

又从 $u=u^\sigma$ 得 $a^kb^lc^m=a^{\lambda k+\delta l}b^{\mu k+\nu l}c^{im}$，于是有

$$\left.\begin{aligned}&(\lambda-1)k+\delta l\equiv 0\\&\mu k+(\nu-1)l\equiv 0\end{aligned}\right\}\pmod 2 \text{ 及 } (i-1)m\equiv 0(\bmod p).$$

由 $i^2\equiv 1(\bmod p)$得：

$i\equiv -1(\bmod p)$，故必 $m\equiv 0(\bmod p)$；或 $i\equiv 1(\bmod p)$，因之 m 可任意；只这二个可能。又从 $\lambda^2+\mu\delta\equiv 1\equiv\nu^2+\mu\delta \pmod 2$ 得 $0\equiv\lambda^2-\nu^2\equiv(\lambda+\nu)^2 \pmod 2$，故或 $\lambda=\nu=0$，或 $\lambda=\nu=1$，也只这二个可能。

在 $i\equiv -1(\bmod p)$时，$m\equiv 0(\bmod p)$。若 $\lambda=\nu=0$，则由 $\begin{vmatrix}\lambda & \mu\\ \delta & \nu\end{vmatrix}\not\equiv 0(\bmod 2)$知 $\mu=\delta=1$，故必 $k\equiv l \pmod 2$，于是 $g^2=u=ab$ 或 $=1$。但在 $g^2=ab$ 时，令 $g_1=ag$ 后，易见 $G=\{a,b,c,g\}=\{a,b,c,g_1\}$中 $g_1^2=1$，$g_1^{-1}ag_1=b$，$g_1^{-1}bg_1=a$，$g_1^{-1}cg_1=c^{-1}$。这也就说明了 $k=l=1$ 的情况可以转化为 $k=l=0$ 来讨论，即可令

(ix) $G=\{a,b,c,g\}$，$a^2=b^2=c^p=1=[a,b]=[a,c]=[b,c]$，$g^2=1$，

$g^{-1}ag=b$，$g^{-1}bg=a$，$g^{-1}cg=c^{-1}$。

如果这时是 $\lambda=\nu=1$，则 $\mu\delta\equiv 0 \pmod 2$；因而或 $\mu=0$，$\delta=1$；或 $\mu=1$，$\delta=0$；或 $\mu=\delta=0$；共三种情况。由于元素 a,b 在群 G 内地位的对称性，可知 $\mu=0$，$\delta=1$ 与 $\mu=1$，$\delta=0$ 给出同一型的群，因之只需研究 $\mu=0$，$\delta=1$ 与 $\mu=\delta=0$ 这二款。

当 $\mu=\delta=0$ 时，k 与 l 可任意，由是 $g^{-1}ag=a$，$g^{-1}bg=b$，$g^{-1}cg=c^{-1}$，而 $g^2=1$，a,b 或 ab 共四种可能。且由于元素 a,b 在 G 内地位的对称性又知 $g^2=a$ 与 $g^2=b$ 这二款无本质上的差异。然令 $a_1=ab$ 后又易知 $A=\{a\}\times\{b\}\times\{c\}=\{a_1\}\times\{b\}\times\{c\}$，且 $a_1^2=1$，$g^2=ab=a_1$，又说明了只需研究 $g^2=1$ 与 $g^2=ab$ 这二款，也就是说又有次二个可能的类型：

(x) $G=\{a,b,c,g\}$，$a^2=b^2=c^p=1=[a,b]=[a,c]=[b,c]$，$g^2=1$，

$g^{-1}ag=a$，$g^{-1}bg=b$，$g^{-1}cg=c^{-1}$；

(xi) $G=\{a,b,c,g\}$，$a^2=b^2=c^p=1=[a,b]=[a,c]=[b,c]$，

$g^2=ab$(或$=a,b$)，$g^{-1}ag=a$，$g^{-1}bg=b$，$g^{-1}cg=c^{-1}$。

当 $\mu=0$，$\delta=1$ 时，有 $g^{-1}ag=a$，$g^{-1}bg=ab$，$g^{-1}cg=c^{-1}$ 及 $g^2=a^k$（这时由 $(\lambda-1)k+\delta l\equiv 0(\bmod 2)$得 $l\equiv 0(\bmod 2)$，故 $g^2=1$ 或 $=a$。但在 $g^2=a$ 时令 $g_1=bg$ 后，就有 $G=\{a,b,c,g\}=\{a,b,c,g_1\}$，其中 $g_1^2=1$，$g_1^{-1}ag_1=a$，$g_1^{-1}bg_1=ab$，$g_1^{-1}cg_1=c^{-1}$。这说明了

只需考虑 $g^2=1$ 即可。然在 $g^2=1$ 时令 $a_1=ab$ 又得 $G=\{a,b,c,g\}=\{a_1,b,c,g\}$，而有定义关系：

$a_1^2=b^2=c^p=1=[a_1,b]=[a_1,c]=[b,c]$，$g^2=1$，$g^{-1}a_1g=b$，$g^{-1}bg=a_1$，$g^{-1}cg=c^{-1}$，即 G 变成了(ix)型。

总之，在 $i\equiv-1(\mathrm{mod}\ p)$时，$G$ 之型只有三个，如(ix)，(x)，(xi)型。

再讨论 $i\equiv1(\mathrm{mod}\ p)$。这时，仍如上述需分别考虑 $\lambda=0=\nu$ 及 $\lambda\equiv1=\nu$ 二款。在 $\lambda=\nu=0$ 时有 $\mu=\delta=1$，因而 $k\equiv l\ (\mathrm{mod}\ 2)$，故或 $k=l=1$，或 $k=l=0$。于是 $g^{-1}ag=b$，$g^{-1}bg=a$，$g^{-1}cg=c$，$g^2=c^m$ 或 $=abc^m(m$ 任意)；故令 $g_1=ac^xg$ 后，显见 $G=\{a,b,c,g\}=\{a,b,c,g_1\}$，式中 $g_1^{-1}ag_1=b$，$g_1^{-1}bg_1=a$，$g_1^{-1}cg_1=c$，而 $g_1^2=c^{m+2x}$（在 $g^2=abc^m$ 时）或 $=abc^{m+2x}$（在 $g^2=c^m$ 时）；且对某一 m 言当 x 跑遍模 p 的完全剩余系时，$2x+m$ 也跑遍之，故恒有 x 使 $m+2x\equiv0(\mathrm{mod}\ p)$，即在 $g^2=abc^m$ 形时可选 g_1 使 $g_1^2=1$，而在 $g^2=c^m$ 时，首先就直接令 $g_1=c^xg$ 可知 $g_1^2=1$。总之可以适当地选 g 使 $G=\{a,b,c,g\}$而有：

$a^2=b^2=c^p=1=[a,b]=[a,c]=[b,c]$，$g^2=1$，$g^{-1}ag=b$，$g^{-1}bg=a$，$g^{-1}cg=c$。

这时再令 $g'=acg$，又得 $G=\{a,b,c,g'\}$，而有 $g'^2=abc^2$，因而由 $o(abc^2)=2p$ 知 $o(g')=4p$。说明了 G 有阶为 $4p$ 的元素，故 G 有 $4p$ 阶的循环正规子群，问题已变为讨论过了的款(Ⅰ)，即表一中的型Ⅰ.

所以在研究 $i\equiv1(\mathrm{mod}\ p)$时，就只需研究 $\lambda=1=\nu$ 的情形。因而如前述的理由一样得知这时应分别考虑 $\mu=0$，$\delta=1$ 与 $\mu=\delta=0$ 两种现象。

在 $\mu=0$，$\delta=1$ 时（必有 $l=0$，k 任意），$G=\{a,b,c,g\}$，式中 $a^2=b^2=c^p=1=[a,b]=[a,c]=[b,c]$，$g^{-1}ag=a$，$g^{-1}bg=ab$，$g^{-1}cg=c$，$g^2=a^kc^m$。再令 $g_1=a^sb^tc^xg$ 时又有 $G=\{a,b,c,g_1\}$，其中仍有 $g_1^{-1}ag_1=a$，$g_1^{-1}bg_1=ab$，$g_1^{-1}cg_1=c$，但 $g_1^2=a^{k+t}c^{2x+m}$；于是选 t 使 $k+t\equiv0(\mathrm{mod}\ 2)$并选 x 使 $2x+m\equiv0\ (\mathrm{mod}\ p)$，则 $g_1^2=1$。这就是说可适当地选 G 之一生成元 g 使 $g^2=1$。于是再令 $g'=bc^{p+1/2}g$，得 $g'^2=ac$，故从 $o(ac)=2p$ 知 $o(g')=4p$，说明了 G 有阶为 $4p$ 的元素，又回到了已讨论过的款(Ⅰ)。

因而只需考虑 $\mu=\delta=0$（故 k,l 都得任意），即 $G=\{a,b,c,g\}$，$a^2=b^2=c^p=1=[a,b]=[a,c]=[b,c]$，$g^{-1}ag=a$，$g^{-1}bg=b$，$g^{-1}cg=c$，$g^2=a^kb^lc^m$，故 G 是交换群。这时，由于$(a^sb^tc^rg)^2=c^{2r}g^2=a^kb^lc^{m+2r}$，可知 G 中元素之阶最大者为 $4p$ 或 $2p$，因而 G 可能为在讨论(Ⅰ)款时已讨论过了的(ii)型外尚有次型：

(xii) $G=\{a\}\times\{b\}\times\{c\}\times\{g\}$，$a^2=b^2=g^2=c^p=1=[a,b]=[a,c]=[a,g]=[b,c]=[b,g]=[c,g]$（$8p$ 阶初等交换群）。

再次，讨论表一中的型(Ⅲ)，即 $A=\{a,b\}$，$a^{2p}=b^2=1$，$b^{-1}ab=a^{-1}$。于是，这时有 $G=\{a,b,g\}$，且尚有关系式 $g^{-1}ag=a^\sigma$，$g^{-1}bg=b^\sigma$，σ 为 A 之自同构，而 σ^2 等于由 A 之元 u 所诱导的 A 之内自同构，但 $g^2=u$，且 $u^\sigma=g^{-1}ug=u$。因 A 中凡阶 $2p$ 之元为 a^k 形，$(k,2p)=1$，其个数 $=\varphi(2p)=p-1$，于是必有

$$\begin{cases} g^{-1}ag(=a^\sigma)=a^k,\ (k,2p)=1,\\ g^{-1}bg(=b^\sigma)=a^tb,\\ g^2(=u)=a^s\ \text{或}=a^sb. \end{cases}$$

但由 $a^{k^2}=a^{\sigma^2}=u^{-1}au=\begin{cases}a\text{（在 }g^2=u=a^s\text{ 时）},\\ a^{-1}\text{（在 }g^2=u=a^sb\text{ 时）},\end{cases}$ 得 $k^2\equiv 1\pmod{2p}$ 在 $g^2=u=a^s$ 时，或 $k^2\equiv -1\pmod{2p}$在 $g^2=u=a^sb$ 时。由于$\left(\frac{-1}{p}\right)=-1$，即 -1 为 p 之二次非剩余，在 $p\equiv 3\pmod 4$时，故这时只能是 $g^2=u=a^s$；然 $p\equiv 1\pmod 4$时，有 $g^2=a^s$ 或 $g^2=a^sb$ 均可能。为简单计，先讨论 $p\equiv 3\pmod 4$，于是 $g^2=a^s$，$k\equiv\pm 1\pmod{2p}$，即 $g^{-1}ag=a$ 或 $=a^{-1}$。但在 $g^{-1}ag=a^{-1}$ 时若令 $g_1=bg$，就有 $G=\{a,b,g\}=\{a,b,g_1\}$，而具关系式：

$$\begin{cases}g_1^{-1}ag_1=a,\\ g_1^{-1}bg_1=a^\lambda b,\\ g_1^2=a^{-(s+\lambda)}.\end{cases}$$

说明了 $k\equiv -1\pmod{2p}$可转化为 $k\equiv 1\pmod{2p}$ 来讨论，即可设 $G=\{a,b,g\}$，$a^{2p}=1=b^2$，$b^{-1}ab=a^{-1}$，$g^{-1}ag=a$，$g^{-1}bg=a^\lambda b$，$g^2=a^s(=u)$；于是再由 $b^{\sigma^2}=u^{-1}bu$ 得 $a^{2\lambda}b=a^{-2s}b$，$\lambda+s\equiv 0\pmod p$。

苟若 s 为奇数，则元素 g^2 的阶 $o(g^2)=2p$（$p\nmid s$ 时）或 $=2$（$p\mid s$ 时），因而 $o(g)=4p$（$p\nmid s$ 时）或 $=4$（$p\mid s$ 时）；但由 $o(g)=4$（$p\mid s$ 时）以及 $ga=ag$ 与 $o(a^2)=p$ 即得 $o(a^2g)=4p$，说明了 G 有阶 $4p$ 的元素，问题又回到了款（1）。

所以我们只需研究 s 为偶数，即 $s=2s_1$。当 $p\mid s_1$ 时，$g^2=1$。当 $p\nmid s_1$ 时，选 x_1 使 $s_1x_1\equiv 1\pmod p$且可令 x_1 为奇数（$\because x_1$ 与 $p+x_1$ 中必有一为奇数）；故再由 $(s_1+p)x_1\equiv 1\pmod p$及 s_1 与 s_1+p 中有一是奇数，则知有奇数 x 使 $xx_1\equiv 1\pmod p$，因而 $(x,2p)=1$，故令 $a_1=a^x$ 时就有 $G=\{a_1,b,g\}$，$a_1^{2p}=1=b^2$，$b^{-1}a_1b=a_1^{-1}$，$g^{-1}a_1g=a_1$，$g^{-1}bg(=a^sb)=a_1^{\lambda x_1}b$，$g^2(=a^s)=a_1^s$。这无异乎是说在 s 为偶数时，我们可以限制在 $s=0$ 及 $s=2$ 来讨论，也就是说：$G=\{a,b,g\}$，式中 $a^{2p}=1=b^2$，$b^{-1}ab=a^{-1}$，$g^{-1}ag=a$，$g^{-1}bg=a^\lambda b$，$g^2=1$ 或 $=a^2$。

然在 $g^2=a^2$ 时，有 $g^{p-1}=a^{p-1}$，故令 $g_1=a^{p-1}g$ $(=g^p)$ 后又有 $G=\{a,b,g_1\}$，其中 $g_1^{-1}ag_1=a$，$g_1^{-1}bg_1=a^{\lambda+2}b$，$g_1^2=1$，说明了 $s=2$ 也可以转化为 $s=0$ 来讨论，即可限制为 $g^2=1$。于是再从 $g^{-1}bg=a^\lambda b$ 得 $b=g^{-2}bg^2=g^{-1}(a^\lambda b)g=a^{2\lambda}b$，$\lambda\equiv 0\pmod p$，故 $\lambda=0$ 或 $=p$，即：

（1）′：$G=\{a,b,g\}$，$a^{2p}=1=b^2$，$b^{-1}ab=a^{-1}$，$g^2=1$，$g^{-1}ag=a$，$g^{-1}bg=b$；

或

（2）′：$G=\{a,b,g\}$，$a^{2p}=1=b^2$，$b^{-1}ab=a^{-1}$，$g^2=1$，$g^{-1}ag=a$，$g^{-1}bg=a^pb$。

设（4）′为真，就令 $a_1=a^p$，$a_2=a^{p+1}$，于是 $a_1a_2=a$，$G=\{a,b,g\}=\{a_1,a_2,b,g\}=\{g,a_1,a_2,b\}$，而有：

$$g^2=a_1^2=a_2^p=1=[g,a_1]=[g,a_2]=[a_1,a_2],\ b^2=1,\ b^{-1}gb=g,\ b^{-1}a_1b=a_1,$$

$$b^{-1}a_2b=a_2^{-1},$$

这恰与(x)型完全一致（将这里的 g, a_1, a_2, b 分别看做(x)型中的 a, b, c, g）。

若（2）′为真，仍令 $a_1 = a^p$，$a_2 = a^{p+1}$，就有 $G = \{a, b, g\} = \{a_1, a_2, b, g\} = \{a_1 g, g, a_2, b\} = \{h, g, a_2, b\}$，式中 $h = a_1 g$，而有定义关系：

$$h^2 = g^2 = a_2^p = 1 = [h, g] = [h, a_2] = [g, a_2],\ b^2 = 1,\ b^{-1}hb = g,\ b^{-1}gb = h,$$

$$b^{-1}a_2 b = a_2^{-1},$$

这恰与(ix)型完全一致（将这里的 h, g, a_2, b 分别看做(ix)型中的 a, b, c, g）。

总之，是说明了：在 $p \equiv 3 \pmod 4$ 时，除了上面已述过了的(i)——(xii)型外，不会再产生新的群 G。故需探索的是 $p \equiv 1 \pmod 4$，这时由于 $\left(\frac{-1}{p}\right) = 1$ 知 $k^2 \equiv -1 \pmod{2p}$ 确有解，因而可能 $g^2 = a^s$，也可能 $g^2 = a^s b$。在 $g^2 = a^s$ 时，与刚在上面讨论的完全一样，不会产生与(i)——(xii)型相异的群。但在 $g^2 = a^s b$ 时，$k^2 \equiv -1 \pmod{2p}$ 有二解；再令 $b_1 = a^s b$，就有 $G = \{a, b, g\} = \{a, b_1, g\}$，式中

$$a^{2p} = 1 = b_1^2,\ b_1^{-1}ab_1 = a^{-1},\ g^{-1}ag = a^k,\ g^{-1}b_1 g = a^{(k-1)s+\lambda}b_1,\ g^2 = b_1.$$

这说明了可以限制在 $s = 0$ 的情况来讨论，也就是说可令 $G = \{a, b, g\}$，式中

$a^{2p} = 1 = b^2$，$b^{-1}ab = a^{-1}$，$g^{-1}ag = a^k$，$g^{-1}bg = a^\lambda b$，$g^2 = b$（$= u$）；因而 $k^2 \equiv -1 \pmod{2p}$。于是利用 $u^\sigma = g^{-1}ug = u$ 又知 $\lambda \equiv 0 \pmod{2p}$，故 $g^{-1}ag = a^k$，$g^{-1}bg = b$，$g^2 = b$，但 $k^2 \equiv -1 \pmod{2p}$；并因 $k^2 \equiv -1 \pmod{2p}$ 之二解 k_1, k_2 有关系式 $k_1 + k_2 \equiv 0 \pmod{2p}$，故从 $g^{-1}ag = a^{k_2}$ 而令 $g_1 = bg$ 后就有 $G = \{a, b, g\} = \{a, b, g_1\}$，具定义关系 $g_1^{-1}ag_1 = a^{k_1}$，$g_1^{-1}bg_1 = b$，$g_1^2 = b$。这说明了 $k^2 \equiv -1 \pmod{2p}$ 之二个解 k_1 与 k_2 所产生的群没有本质上的差异，群 G 为唯一型，是：

(xiii) $G = \{a, b, g\}$，$a^{2p} = b^2 = 1$，$b^{-1}ab = a^{-1}$，$g^{-1}ag = a^k$，$g^{-1}bg = b$，$g^2 = b$，但 $k^2 \equiv -1 \pmod{2p}$，而 $p \equiv 1 \pmod 4$。

又再次，讨论表一中的款（N），即 $A = \{a, b\}$，$a^{2p} = 1$，$b^2 = a^p$，$b^{-1}ab = a^{-1}$。于是 $G = \{a, b, g\}$，尚有 $g^{-1}ag = a^\sigma$，$g^{-1}bg = b^\sigma$，σ 为 A 之自同构，但 σ^2 等于用 A 之元 u 所诱导的 A 之内自同构，$g^2 = u$ 且 $u^\sigma = g^{-1}ug = u$。

由 $A = \{a\} + \{a\}b$ 之陪集 $\{a\}b$ 中每元的阶 $= 4$。故必 $g^{-1}ag\ (= a^\sigma) = a^k$，$(k, 2p) = 1$，$g^{-1}bg\ (= b^\sigma) = a^\lambda b$，$g^2\ (= u) = a^s$ 或 $= a^s b$。

由 $a^{k^2} = a^{\sigma^2} = u^{-1}au = \begin{cases} a & (\text{在 } g^2 = a^s \text{ 时}) \\ a^{-1} & (\text{在 } g^2 = a^s b \text{ 时}) \end{cases}$，得 $k^2 \equiv 1 \pmod{2p}$ 是在 $g^2 = a^s$ 时，或 $k^2 \equiv -1 \pmod{2p}$ 是在 $g^2 = a^s b$ 时。

先讨论 $g^2 = a^s$（当 $p \equiv 3 \pmod 4$ 时也只能是 $g^2 = a^s$）。于是 $k^2 \equiv 1 \pmod{2p}$，$k \equiv \pm 1 \pmod{2p}$。但在 $k \equiv -1 \pmod{2p}$ 时（即 $g^{-1}ag = a^{-1}$），令 $g_1 = bg$ 后就有 $G = \{a, b, g_1\}$，并具 $g_1^{-1}ag_1 = a$，$g_1^{-1}bg_1 = a^\lambda b$，$g_1^2 = a^{p-(s+\lambda)}$，这说明了可把 $k \equiv -1 \pmod{2p}$ 转化为 $k \equiv 1 \pmod{2p}$，即适当地可选 g 使 $G = \{a, b, g\}$ 中 $g^{-1}ag = a$，$g^{-1}bg = a^\lambda b$，$g^2 = a^s$。

当 s 为奇数时，若 $p \nmid s$，则 $o(g) = 4p$；若 $p \mid s$，则 $o(g) = 4$，因而 $o(a^2 g) = 4p$；总之，说明了 G 有阶 $4p$ 的元素，又回到了款（I）。故只需考虑 s 为偶数，这时若

$p \mid \frac{s}{2}$，则 $g^2=1$；若 $p \nmid \frac{s}{2}$，则选 x_1 使 $\frac{s}{2}x_1 \equiv 1 \pmod{p}$，且可令 x_1 是奇数（$\because x_1$ 与 $p+x_1$ 中有一为奇数），由是再据 $\left(\frac{s}{2}+p\right)x_1 \equiv 1 \pmod{p}$ 以及 $\frac{s}{2}$ 与 $\frac{s}{2}+p$ 中有一为奇数，可知有奇数 x 使 $xx_1 \equiv 1 \pmod{p}$，因而 $xx_1 \equiv 1 \pmod{2p}$，于是令 $a_1=a^x$ 后显有 $G=\{a_1, b, g\}$，式中 $a_1^{2p}=1$，$b^2=a_1^p(=a^{px}=a^p)$，$b^{-1}a_1b=a_1^{-1}$，$g^{-1}a_1g=a_1$，$g^{-1}bg=a_1^{\lambda x_1}b$，$g^2(=a^s=a^{sx_1x}=a_1^{sx_1}=a_1^{2\cdot(s/2)x_1})=a_1^2$。总之，说明了 s 为偶数时，我们只需探索 $s=0$ 与 $s=2$ 这两情况。然在 $s=2$（即 $g^2=a^2$）时，$g^{p-1}=a^{p-1}$，故令 $g_1=g^p=a^{p-1}g$，又得 $G=\{a, b, g_1\}$，式中 $g_1^2=a^{2(p-1)}g^2=1$，说明了 $s=2$ 也可以转化为 $s=0$ 去替代。这无异乎是说可令 $G=\{a, b, g\}$ 中 $a^{2p}=1$，$b^2=a^p$，$b^{-1}ab=a^{-1}$，$g^{-1}ag=a$，$g^{-1}bg=a^\lambda b$，$g^2=1$。由是再利用 $b^{\sigma^2}=u^{-1}bu=b$ 得 $a^{2\lambda}b=b$，$\lambda \equiv 0 \pmod{p}$，因而只有下列两个可能：

(1)″：$g^{-1}ag=a$，$g^{-1}bg=b$，$g^2=1$；

(2)″：$g^{-1}ag=a$，$g^{-1}bg=a^pb$，$g^2=1$。

再令 $a_1=a^p$，$a_2=a^{p+1}$，则 $a=a_1a_2$，$G=\{a, b, g\}=\{a_1, a_2, b, g\}=\{h, a_2, b, g\}$（但 $h=a_1g$）。

若（1）″为真，改写 $G=\{h, g, a_2, b\}$ 后，有定义关系：

$$h^2=g^2=a_2^p=1=[h, g]=[h, a_2]=[g, a_2],\ b^2=hg,\ b^{-1}hb=h,$$

$$b^{-1}gb=g,\ b^{-1}a_2b=a_2^{-1}.$$

这恰与(xi)型完全一致（将这里的 h, g, a_2, b 分别看做那里的 a, b, c, g。）

若（2）″为真，令 $b_1=gb$ 后就有 $G=\{h, g, a_2, b_1\}$，具定义关系：$h^2=g^2=a_2^p=1=[h, g]=[h, a_2]=[g, a_2]$，$b_1^2=1$，$b_1^{-1}hb_1=g$，$b_1^{-1}gb_1=h$，$b_1^{-1}a_2b_1=a_2^{-1}$。这又恰与(ix)型完全一致。

总之，在 $p \equiv 3 \pmod{4}$ 时，除上述的(i)——(xii)型外，表一中的(Ⅳ)款再不会产生新的群。

可是，在 $p \equiv 1 \pmod{4}$ 时，尚需研究 $k^2 \equiv -1 \pmod{2p}$ 即 $g^2=a^sb$。这时，$k^2 \equiv -1 \pmod{2p}$ 有二解 k_1, k_2，且又有 $k_1+k_2 \equiv 0 \pmod{2p}$。如 $g^{-1}ag=a^{k_2}$，令 $g_1=bg$ 后就得 $G=\{a, b, g\}=\{a, b, g_1\}$，式中 $g_1^{-1}ag_1=a^{k_1}$，$g_1^{-1}bg_1=a^\lambda b$，$g_1^2=a^{p+\lambda-s}b$，这说明 $g^{-1}ag=a^{k_2}$ 与 $g^{-1}ag=a^{k_1}$ 将互相转化，因而没有必要来区分 k_1 或 k_2。但令 $b_1=a^sb$ 后又有：$G=\{a, b, g\}=\{a, b_1, g\}$，并具定义关系 $a^{2p}=1$，$b_1^2=a^p$，$b_1^{-1}ab_1=a^{-1}$，$g^{-1}ag=a^k$，$g^{-1}b_1g(=a^{\lambda+ks}b)=a^{\lambda+(k-1)s}b_1$，$g^2=b_1$。这又说明了可不损普遍性得令 $g^2=a^sb$ 中的 $s=0$，即 $g^2=b$；于是再由 $u^\sigma=g^{-1}ug=u=g^2=b$ 可知 $g^{-1}bg=b$，即 $\lambda \equiv 0 \pmod{2p}$，因而可能有次型：

(xiv) $G=\{a, b, g\}$，$a^{2p}=1$，$b^2=a^p$，$b^{-1}ab=a^{-1}$，$g^2=b$，$g^{-1}ag=a^k$，

$g^{-1}bg=b$，

但 $k^2 \equiv -1 \pmod{2p}$，而 $p \equiv 1 \pmod{4}$。

最后，讨论表一中的(Ⅴ)款 即 $A=\{a, b, c\}$，而具定义关系 $a^p=1=b^2, b^{-1}ab=a^{-1}$，

$a^2=b$, $c^{-1}bc=b$, $c^{-1}ac=a^k$, 但 $k^2\equiv -1 \pmod p$。——当然是在 $p\equiv 1 \pmod 4$ 时。因 $G=\{a,b,c,g\}$ 中尚有

$$\left.\begin{aligned} g^{-1}ag&=a^\sigma\\ g^{-1}bg&=b^\sigma\\ g^{-1}cg&=c^\sigma \end{aligned}\right\},\ \sigma \text{ 为 } A \text{ 之自同构，} \sigma^2 \text{ 等于 } A \text{ 之 } u \text{ 所诱导的 } A \text{ 之内自同构，} g^2=u=a^tb^lc^mc\in A,\ u^\sigma=u,$$

但 $l=0,1$; $m=0,1$; $t=0,1,2,\cdots,p-1$; 且 $A=\{a\}+\{a\}b+\{a\}c+\{a\}bc$ 中凡属陪集 $\{a\}b$ 之元的阶均为 2，属陪集 $\{a\}c$ 与 $\{a\}bc$ 的元之阶全为 4；故必

$$\begin{cases} g^{-1}ag(=a^\sigma)=a^i\ (i=1,2,\cdots,p-1),\\ g^{-1}bg(=b^\sigma)=a^\lambda b,\\ g^{-1}cg(=c^\sigma)=a^\mu c \text{ 或 } =a^\mu bc. \end{cases}$$

首先可断言 $g^{-1}cg\ (=c^\sigma)=a^\mu bc$ 是不可能的：因若 $c^\sigma=a^\mu bc$，则由 $c^{-1}ac=a^k$ 得 $(c^\sigma)^{-1}a^bc^\sigma=(a^\sigma)^k$，即 $a^{ik}=a^{-ik}$，$ik\equiv 0(\bmod p)$，显非所许。故只能够是 $g^{-1}cg(=c^\sigma)=a^\mu c$。

再利用 $a^{i^2}=a^{\sigma^2}=u^{-1}au=c^{-m}b^{-l}a^{-t}aa^tb^lc^m=a^{(-1)^lk^m}$，得知 $i^2\equiv(-1)^lk^m \pmod p$。于是 $m=1$ 可导致 $i^2\equiv(-1)^lk$，$i^4\equiv k^2\equiv -1(\bmod p)$，$i^8\equiv 1(\bmod p)$，即在模 p 之既约剩余类群 C_p 中 i 的阶为 8，故 $8|(p-1)$，因而在 $p\equiv 5 \pmod 8$ 时由于 $8\nmid(p-1)$ 则知 $m\neq 1$，只能是 $m=0$。为简单计，暂时先讨论 $p\equiv 5(\bmod 8)$。

既然 $p\equiv 5(\bmod 8)$，故必 $m=0$，因而 $i^2\equiv(-1)^l(\bmod p)$，$i^4\equiv 1 \pmod p$，即 i 之 4 次幂已为模 p 之既约剩余类群 C_p 之单位元，于是由于 C_p 为 $p-1$ 阶循环群，故 C_p 中 4 次幂为单位元的元素之个数恰等于 4，然 $\{k\}$ 又是 C_p 之唯一的一个 4 阶子群，因之不得不有整数 r 使 $i\equiv k^r(\bmod p)$。再选 s 使 $r+s\equiv 0 \pmod 4$，并令 $g_1=c^sg$，则 $G=\{a,b,c,g\}=\{a,b,c,g_1\}$ 而具定义关系：

$$a^p=1=b^2,\ b^{-1}ab=a^{-1},\ c^2=b,\ c^{-1}bc=b,\ c^{-1}ac=a^k,$$

但 $k^2\equiv -1(\bmod p)$，以及

$$g_1^{-1}ag_1=a,\ g_1^{-1}bg_1=a^\lambda b,\ g_1^{-1}cg_1=a^\mu c,\ g_1^2=c^sa^tb^l(a^\mu c)^s=c^sa^tb^lc^sa^{\mu k(1+k+\cdots+k^{s-1})}=c^{2s}a^{tk^s}b^la^{\mu k(1+k+\cdots+k^{s-1})}=b^{s+l}a^{tk^s+(-1)^l\mu k(1+k+\cdots+k^{s-1})}=a^tb^l \text{ 形。}$$

这说明了我们可以适当地选 g 使 $G=\{a,b,c,g\}$ 中 a,b,c 间之关系如 $a^p=b^2=1$，$c^2=b$，$b^{-1}ab=a^{-1}$，$c^{-1}bc=b$，$c^{-1}ac=a^k(k^2\equiv -1(\bmod p)$，因而是在 $p\equiv 1(\bmod 4)$ 时)外，尚得令

$$g^{-1}ag=a,\ g^{-1}bg=a^\lambda b,\ g^{-1}cg=a^\mu c \text{ 及 } g^2\ (=u)=c^tb^l.$$

由是再利用 $a^{\sigma^2}=u^{-1}au$ 得 $g^{-2}ag^2=b^{-l}ab^l$，$a=a^{(-1)^l}$，$(-1)^l\equiv 1(\bmod p)$，不得不有 $l=0$，故 $g^2=a^t$；再令 $g'=a^xg$，使 $2x+t\equiv 0(\bmod p)$，则 $G=\{a,b,c,g'\}$ 而有 $g'^{-1}ag'=a$，$g'^{-1}bg'=a^{\lambda-2x}b$，$g'^{-1}cg'=a^{\mu-x(1+k)}c$，$g'^2=1$。这无异乎是说还可适当地选 g，使

$$g^{-1}ag=a,\ g^{-1}bg=a^\lambda b,\ g^{-1}cg=a^\mu c,\ g^2=1.$$

象这样选了 g 后，再利用 $b^{\sigma^2}=u^{-1}bu$ 得 $a^{2\lambda}b=b$，$\lambda\equiv 0(\bmod p)$，即 $g^{-1}bg=b$；由是又有

$$b = g^{-1}bg = b^{\sigma} = (c^{\sigma})^{-1}b^{\sigma}c^{\sigma} = a^{-2\mu k}b,$$

故 $\mu \equiv 0 \pmod{p}$，即 $g^{-1}cg = c$。这就是说，$G = \{a, b, c, g\}$ 中 $a^p = 1 = b^2$，$b^{-1}ab = a^{-1}$，$c^2 = b$，$c^{-1}bc = b$，$c^{-1}ac = a^k$（$k^2 \equiv -1 \pmod{p}$，因而是在 $p \equiv 1 \pmod{4}$ 时），$g^{-1}ag = a$，$g^{-1}bg = b$，$g^{-1}cg = c$，$g^2 = 1$。

并注意 k 可限制取奇数（$\because (p-k)^2 \equiv k^2 \equiv -1 \pmod{p}$），故有 $k^2 = -1 \pmod{2p}$。再令 $a_1 = ag$，则 $0(a_1) = 2p$，且从 $g^2 = 1$ 知 $g^{p-1} = 1$，因而 $a_1^p = a^p g^p = g^p = g$，故 $G = \{a, b, c, g\} = \{a_1, b, c, g\} = \{a_1, b, c\}$，其中 $a_1^{2p} = 1 = b^2$，$b^{-1}a_1 b = a_1^{-1}$，$c^{-1}a_1 c = a_1^k$，$c^{-1}bc = b$，$c^2 = b$。这说明了它恰与(xiii)型的群一致（把这里的 a_1, b, c 分别看做那里的 a, b, g）。这也是说在 $p \equiv 1 \pmod{4}$ 时如出现 $p \equiv 5 \pmod{8}$，那末除前述各种类型的群以外再不会产生新的群。

于是只剩下 $p \equiv 1 \pmod{4}$ 中 $p \equiv 1 \pmod{8}$ 的情况需要探索。令 $g^2 = u = a^l b^l c^m (l = 0, 1;\ m = 0, 1;\ t = 0, 1, 2, \cdots, p-1)$ 后，分 $m = 0$ 与 $m = 1$ 两小款讨论。在 $m = 0$ 时，完全同上面一样不会再有新群产生。故只需考虑 $m = 1$。这也是说 $G = \{a, b, c, g\}$，式中 $a^p = 1 = b^2$，$b^{-1}ab = a^{-1}$，$c^2 = b$，$c^{-1}bc = b$，$c^{-1}ac = a^k (k^2 \equiv -1 \pmod{p})$，$g^{-1}ag = a^i (i = 1, 2, \cdots, p-1)$，$g^{-1}bg = a^{\lambda}b$，$g^{-1}cg = a^{\mu}c$，$g^2 = a^t b^l c (t = 0, 1, \cdots, p-1;\ l = 0, 1)$。

今再分别讨论 $l = 0$ 与 $l = 1$。

先讨论 $l = 0$。这时，$g^2 = a^t c$，$i^4 \equiv -1 \pmod{p}$ 而 $i^8 \equiv 1 \pmod{p}$。由于这时 $a^{t2} = (a^t)^i = g^{-2}ag^2 = c^{-1}ac = a^k$，得知 $i^2 \equiv k$，$i^3 \equiv ik \pmod{p}$，故因在模 p 之既约剩余类群 C_p 中 $o(i) = 8$ 就知道 $i^3 \not\equiv 1 \pmod{p}$，于是 $ik \not\equiv 1 \pmod{p}$，因而 $(1 - ik)x + t \equiv 0 \pmod{p}$ 有解 x，故再令 $g_1 = b^x g$ 时有：

$$G = \{a, b, c, g\} = \{a, b, c, g_1\},$$

其中 $g_1^2 = a^{(1-ik)x+t}c = c$，$g_1^{-1}ag_1 = a^i$，$g_1^{-1}bg_1 = b^{\lambda - 2ix}b$，$g_1^{-1}cg_1 = a^{\mu - x(1+k)i}c$；这说明了可以适当地选 g 使 $G = \{a, b, c, g\}$ 中 $g^2 = c$，$g^{-1}ag = a^i$ 且有 $g^{-1}bg = a^{\lambda}b$ 及 $g^{-1}cg = a^{\mu}c$ 形。

于是再从 $u^{\sigma} = v$ 得 $g^{-1}cg = c$，$\mu \equiv 0 \pmod{p}$，因而又由 $b^{\sigma} = (c^{\sigma})^2$ 得 $a^{\lambda}b = c^2 = b$，$\lambda \equiv 0 \pmod{p}$，即 $G = \{a, b, c, g\}$ 中除 a, b, c 之关系外尚有

$$g^{-1}ag = a^i,\ g^{-1}bg = b,\ g^{-1}cg = c,\ g^2 = c \qquad (1)$$

故待决定的是 i。因在模 p 之既约剩余类群 C_p 中元 i 的阶为 8，故 $\{i\}$ 为循环群 C_p 中唯一的一个 8 阶子群，于是 C_p 中阶 8 之元仅为 i，i^3，i^5 与 i^7 共四个，这说明了(1)式中的 i 得取 i，i^3，i^5，或 i^7，即

$g^{-1}ag = a^i$，或 $= a^{i^3}$，或 $= a^{i^5}$，或 $= a^{i^7}$。

然在 $g^{-1}ag = a^i$ 时，若令 $g_1 = gc$，$g_2 = gc^2$，$g_3 = gc^3$，则 $G = \{a, b, c, g\} = \{a, b, c, g_\alpha\} (\alpha = 1, 2, 3)$，而 $g_\alpha^{-1}bg_\alpha = b$，$g_\alpha^{-1}cg_\alpha = c$，$g_\alpha^2 = c^{2\alpha+1}$ 以及 $g_\alpha^{-1}ag_\alpha = a_{ik}{}^{\alpha} = a_i{}^{2\alpha+1} (\alpha = 1, 2, 3)$。当 $\alpha = 2$ 时，$G = \{a, b, c, g_2\}$ 中 $g_2^2 = c^5 = c$；然在 $\alpha = 1$ 或 $= 3$ 时，由于 $G = \{a, b, c_1, g_\alpha\} (c_1 = c^{-1})$ 中 $a^p = b^2 = 1$，$b^{-1}ab = a^{-1}$，$c_1^2 = b$，$c_1^{-1}bc_1 = b$，$c_1^{-1}ac_1 = a^{k^2}$（$(k^2)^2 \equiv -1 \pmod{p}$），$g_\alpha^2 = c_1$，$g_\alpha^{-1}ag_\alpha = a^{i^{2\alpha+1}}$，$g_\alpha^{-1}bg_\alpha = b$，$g_\alpha^{-1}c_1 g_\alpha = c_1$。

这与(1)完全一样，只是以 c_1 代 c，以 g_α 代 g，而以 i 换为 $i^{2\alpha+1}$。这足以说明(1)中的

i 怎样去变化都无关紧要，只要它在 C_p 内的阶等于 8 就行了。这也是说 G 之型是唯一的，即

(xv) $G=\{a, b, c, g\}$, $a^p=b^2=1$, $b^{-1}ab=a^{-1}$, $c^2=b$, $c^{-1}bc=b$, $c^{-1}ac=a^k$（但 $k^2\equiv -1 \pmod p$），且 $g^2=c$, $g^{-1}bg=b$, $g^{-1}cg=c$, $g^{-1}ag=a^i$，但 $i^8\equiv 1 \pmod p$ 而 $i^4\equiv -1 \pmod p$。注意这时 $p\equiv 1 \pmod 8$。

于是再剩下的仅 $m=1$ 时 $l=1$ 的情况需探索。说具体些，$G=\{a, b, c, g\}$, $a^p=b^2=1$, $b^{-1}ab=a^{-1}$, $c^2=b$, $c^{-1}bc=b$, $c^{-1}ac=a^k(k^2\equiv -1 \pmod p)$, $g^{-1}ag=a^i(i=1, 2, \cdots, p-1)$, $g^{-1}bg=a^\lambda b$, $g^{-1}cg=a^\mu c$, $g^2=a^t bc(t=0, 1, \cdots, p-1)$。当然应限制在 $p\equiv 1 \pmod 8$ 的情况下。

注意 $a^{i^2}=(g^{-1}ag)^i=g^{-1}a^ig=g^{-2}ag^2=c^{-1}b^{-1}abc=a^{-k}$ 得导出 $i^2\equiv -k \pmod p$, $i^4\equiv k^2\equiv -1 \pmod p$, $i^8\equiv 1 \pmod p$，即在模 p 之既约剩余类群 C_p 中 $o(i)=8$，故 $i^3\equiv -ik \not\equiv 1 \pmod p$，即 $(1+ik, p)=1$，故有整数 x 使 $(1+ik)x+t\equiv 0 \pmod p$；再令 $g_1=a^x g$，显有 $G=\{a, b, c, g\}=\{a, b, c, g_1\}$，其中 $g_1^{-1}ag_1=a^i$, $g_1^{-1}bg_1=a^{\lambda-2ix}b$, $g_1^{-1}cg_1=a^{\mu-ix(1+k)}c$ 以及 $g_1^2=a^{t+x(1+ik)}bc=bc$。这无异乎是说可适当地选取 g 使

$$g^{-1}ag=a^i,\ g^2=bc \text{ 以及 } g^{-1}bg=a^\lambda b \text{ 与 } g^{-1}cg=a^\mu c.$$

再利用 $b=c^{-1}bc=g^{-2}bg^2=g^{-1}(g^{-1}bg)g=g^{-1}a^\lambda bg=a^{(i+1)\lambda}b$，知 $(i+1)\lambda\equiv 0 \pmod p$，故由 $i^4\equiv -1 \pmod p$ 得 $i+1\not\equiv 0 \pmod p$，因而不得不有 $\lambda\equiv 0 \pmod p$，即 $g^{-1}bg=b$。由是又从 $c^2=b$ 得 $(g^{-1}cg)^2=g^{-1}bg=b$，故 $b=(a^\mu c)^2=a^{\mu(1-k)}b$，$\mu(1-k)\equiv 0 \pmod p$，故必 $\mu\equiv 0 \pmod p$，即 $g^{-1}cg=c$。这说明了 $G=\{a, b, c, g\}$ 中 g 可适当选取使 $g^{-1}ag=a^i$, $g^{-1}bg=b$, $g^{-1}cg=c$, $g^2=bc$。

然因 $A=\{a, b, c\}=\{a, b, c_1\}$，式中 $c_1=bc$，故 $G=\{a, b, c_1, g\}$ 而具定义关系：

$$a^p=b^2=1,\ b^{-1}ab=a^{-1},\ c_1^2=b,\ c_1^{-1}bc_1=b,\ c_1^{-1}ac_1=a^{-k}((-k)^2\equiv -1 \pmod p),$$

$$g^2=c_1,\ g^{-1}bg=b,\ g^{-1}c_1g=c_1,\ g^{-1}ag=a^i;$$

这恰与(xv)型完全一致（把这里的 a, b, c_1, g 分别看做那里的 a, b, c, g）。总之，说明了在 $m=1$ 时，$l=1$ 与 $l=0$ 对群 G 之型言没有本质上的差异，故在 $p\equiv 1 \pmod 8$ 时，有且仅有十五个群。

再计算上述(i)——(xv)型各群中元之阶分布的情况，易见它们两两互异，故证得了下面的定理 1。

定理 1 2^3p 阶群(p 为奇质数，且 $p\neq 3, 7$)在：(a) $p\equiv 3 \pmod 4$时，共有12个；

(b) $p\equiv 5 \pmod 8$时，共有14个；

(c) $p\equiv 1 \pmod 8$时，共有15个。

它们的构造见次表二。

（表 二）

	种类	构 造（定 义 关 系）	备 注
2^3p 阶群（p 为奇质数，且 $p\neq 3$，也 $\neq 7$）	(1)	$G=\{a\}$, $a^{8p}=1$ （循环群）	不论 p 若何即 $p\equiv 1$ 或 $\equiv 3 \pmod 4$ 时
	(2)	$G=\{a\}\times\{b\}\times\{c\}$, $a^p=b^4=c^2=1=[a,b]=[a,c]=[b,c]$ （交换群）	
	(3)	$G=\{a\}\times\{b\}\times\{c\}\times\{d\}$, $a^p=b^2=c^2=d^2=1=[a,b]=[a,c]=[a,d]=[b,c]=[b,d]=[c,d]$ （初等交换群）	
	(4)	$G=\{a,b\}$, $a^{4p}=1=b^2$, $b^{-1}ab=a^{-1}$	
	(5)	$G=\{a,b\}$, $a^{4p}=1$, $b^2=a^{2p}$, $b^{-1}ab=a^{-1}$	
	(6)	$G=\{a,b\}$, $a^{4p}=1=b^2$, $b^{-1}ab=a^{2p+1}$	
	(7)	$G=\{a,b\}$, $a^{4p}=1$, $b^2=a^2$, $b^{-1}ab=a^{2p+1}$	
	(8)	$G=\{a,b\}$, $a^{4p}=1=b^2$, $b^{-1}ab=a^{2p-1}$	
	(9)	$G=\{a,b\}$, $a^{4p}=1$, $b^2=a^p$, $b^{-1}ab=a^{2p-1}$	
	(10)	$G=\{a,b,c,g\}$, $a^2=b^2=c^p=1=[a,b]=[a,c]=[b,c]$, $g^2=1$, $g^{-1}ag=b$, $g^{-1}bg=a$, $g^{-1}cg=c^{-1}$.	
	(11)	$G=\{a,b,c,g\}$, $a^2=b^2=c^p=1=[a,b]=[a,c]=[b,c]$, $g^2=1$, $g^{-1}ag=a$, $g^{-1}bg=b$, $g^{-1}cg=c^{-1}$.	
	(12)	$G=\{a,b,c,g\}$, $a^2=b^2=c^p=1=[a,b]=[a,c]=[b,c]$, $g^2=ab$(或 a 或 b), $g^{-1}ag=a$, $g^{-1}bg=b$, $g^{-1}cg=c^{-1}$	
	(13)	$G=\{a,b,g\}$, $a^{2p}=1=b^2$, $b^{-1}ab=a^{-1}$, $g^{-1}ag=a^k$, $g^{-1}bg=b$, $g^2=b$, 但 $k^2\equiv -1 \pmod{2p}$	在 $p\equiv 5 \pmod 8$ 时
	(14)	$G=\{a,b,g\}$, $a^{2p}=1$, $b^2=a^p$, $b^{-1}ab=a^{-1}$, $g^{-1}ag=a^k$, $g^{-1}bg=b$, $g^2=b$, 但 $k^2\equiv -1 \pmod{2p}$	
	(15)	$G=\{a,b,c,g\}$, $a^p=b^2=1$, $b^{-1}ab=a^{-1}$, $c^2=b$, $c^{-1}bc=b$, $c^{-1}ac=a^k$, $g^2=c$, $g^{-1}bg=b$, $g^{-1}ag=a$, $g^{-1}ag=a^i$, 但 $k^2\equiv -1 \pmod p$, $i^4\equiv -1 \pmod p$.	在 $p\equiv 1 \pmod 8$ 时

在定理 1 中至所以要限制在 $p\neq 7$及 $p\neq 3$，为的是保证 G 之超可解性。现在转而来讨论 $p=7$及 $p=3$的情况。先讨论 $p=7$，即 G 为56阶群：$O(G)=2^3\cdot 7$。这时由于$7\nmid(2-1)(2^2-1)(2^3-1)$，则知 G 不必恒有西洛塔，因而 G 有为非超可解群的可能性；但G 之可解性说明 G 或有指数为 2 的正规子群 A，或G 有指数为7的正规子群B。

先讨论有 $A\lhd G$ 使$[G:A]=2$的 G。这时 $O(A)=2^2\cdot 7=28$，于是根 Hölder 定理(文献[2]之129 页定理 21)不难获知 A 只能是次之四个类型，即为表一中的型(Ⅰ)，(Ⅱ)，(Ⅳ)(Ⅵ)。——只要将表一中之 p 代换为7。故与证上面定理 1 一样，可知在(Ⅰ)款时有八个互不同构的56阶群 G，即前述的(i)—(viii)型共 8 个（令其中之 $p=7$）。在(Ⅱ)款时，也与证定理 1 完全一样，有四个新的互不同构的56阶群即前述的(ix)—(xii) 型共四个（以 7 代 p）。在(Ⅲ)与(Ⅳ)款时，也与讨论定理 1 一样；而且因$7\equiv 3\ (\mathrm{mal}4)$，故没有象那里的(xiii)型与(xiv)型，即除(i)—(xii) 型外不再有新群。这就证明了：只要56阶群含有指数为 2 的正规子群，那末 G 就只能是前述的(i)—(xii) 型（以7代 p）。

故需要讨论的是56阶群 G 没有指数 2 的正规子群。于是从 G 之可解性可知这时 G 必有指数为7之正规子群 B，即 $B\lhd G$ 且$[G:B]=7$，故 $O(B)=8$，于是 B 为 G 之唯一的一个西洛 2 - 子群。但 B 又只能为次之五个型：

(Ⅰ)′：$B=\{a\}$，$a^8=1$（8 阶循环群）；

(Ⅱ)′：$B=\{a\}\times\{b\}$，$a^4=b^2=1=[a,b]$——(2, 1)型交换群；

(Ⅲ)′：$B=\{a\}\times\{b\}\times\{c\}$，$a^2=b^2=c^2=1=[a,b]=[a,c]=[b,c]$（初等交换群）；

(Ⅳ)′：$B=\{a,b\}$，$a^4=1$，$b^2=a^2$，$b^{-1}ab=a^{-1}$（四元数群）；

(Ⅴ)′：$B=\{a,b\}$，$a^4=b^2=1$，$b^{-1}ab=a^{-1}$（二面体群）。

因 G 为 B 被 7 阶循环群之扩张，且 G 中凡阶 7 的元又不在 B 内，故对 G 之任一个阶7之元 g（$O(g)=7$），应有陪集分解：

$$G=B+Bg+Bg^2+Bg^3+Bg^4+Bg^5+Bg^6$$

且 $g^{-1}xg=x^\sigma$（每 $x\ni B$）中 σ 为 B 的自同构，而 $\sigma^7=1$ 为恒等自同构。

在(Ⅰ)′款时，因 B 之自同构群为 $\varphi(8)=4$ 阶的，故欲 $\sigma^7=1$，必 $\sigma=1$，即 $g^{-1}ag=a$，$G=\{a,g\}$为交换群，于是从 $O(a)=8$，$O(g)=7$及 $ag=ga$ 即知 $O(ag)=56$，故 $G=\{ag\}$是环循的，这与 G 没有指数 2 之正规子群的假定相矛盾。所以(Ⅰ)′款不成立。

若 B 为(Ⅱ)′款，即 $B=\{a\}\times\{b\}$，$a^4=b^2=1=[a,b]$，则因 B 之 Frattini 子群$\Phi(B)=\{a^2\}$是 2 阶的，故 $B/\Phi(B)$为4阶初等交换群，因而 $B/\Phi(B)$ 之自同构群 $\mathbf{A}(B/\Phi(B))$ 为6阶的且与三次对称群 $\mathbf{S}_3$ 同构。但由于 $O(\mathbf{A}(B))\mid O(\Phi B)^4\cdot O(\mathbf{A}(B/\Phi(B)))=24$（[1]元274页3.17Satg），可知欲 $\sigma^7=1$成立，也不得不有 $\sigma=1$，随而 G 是交换的，易知 G 有指数为 2 之正规子群，与题设相抵，不可，所以(Ⅱ)′款也不真。

又因四元数群之自同构群与四次对称群 $\mathbf{S}^4$ 同构（[2]元148 页），二面体群之自同构群仍为二面体群（[4]之98页 Ex.4），故它们的阶分别为24与8，于是在(Ⅳ)′或(Ⅴ)′款时，B 之自同构 σ 具性质 $\sigma^7=1$时亦必 $\sigma=1$，即 $g^{-1}ag=a$，$g^{-1}bg=b$，因而 $O(ag)=4\times 7=28$．不得不有$\{ag\}\lhd G$（$\because[G:\{ag\}]=2$），仍说明了 G 有指数 2 的正规子群，与假设相抵，不可。

于是，唯一的可能性是 B 为(Ⅲ)′款，即 B 为8阶初等交换群。因而有 $G=\{a, b, c, g\}$，

其中 $a^2=b^2=c^2=1=[a, b]=[a, c]=[b, c]$，且 $\begin{cases} g^{-1}ag=a^{\sigma_g}, \\ g^{-1}bg=b^{\sigma_g}, \\ g^{-1}cg=c^{\sigma_g}, \end{cases}$

但 σ_g 为 $B=\{a\}\times\{b\}\times\{c\}$ 之自同构，而有 $\sigma_g^7=1$。因而

$$\begin{cases} g^{-1}ag=a^{\sigma_g}=a^{\lambda_{11}}b^{\lambda_{12}}c^{\lambda_{13}}, \\ g^{-1}bg=c^{\sigma_g}=a^{\lambda_{21}}b^{\lambda_{22}}c^{\lambda_{23}}, \\ g^{-1}cg=c^{\sigma_g}=a^{\lambda_{31}}b^{\lambda_{32}}c^{\lambda_{33}}, \end{cases} \quad \text{而有矩阵 } \Delta_g=\begin{pmatrix} \lambda_{11}\lambda_{12}\lambda_{13} \\ \lambda_{21}\lambda_{22}\lambda_{23} \\ \lambda_{31}\lambda_{32}\lambda_{33} \end{pmatrix}$$

其行列式 $\det\Delta_g\not\equiv 0(mod2)$。因 p^n 阶初等交换 p-群 H 的自同构群 $\mathbf{A}(H)$ 与具有 p 个元的有限域 K_p 上的 n 级全体线性群 $GL(n, K_p)$ 同构，故有 $\mathbf{A}(B)\cong GL(3, K_2)$，且这同构对应关系当然包含着有 σ_g 与 Δ_g 相对应；于是由 $\sigma_g^7=1$ 即得 $\Delta_g^7\equiv\begin{pmatrix} 1&0&0 \\ 0&1&0 \\ 0&0&1 \end{pmatrix}$ (mod2)，再注意 $O(g^i)=7(i=1, 2, 3, 4, 5, 6)$，又知由 g^i 所决定的 B 之自同构 $\sigma_{g^i}(=\sigma_g^i)$ 的阶亦为7，即

$$\begin{cases} g^{-i}ag^i=a^{\lambda_{11}^{(i)}\lambda_{12}^{(i)}\lambda_{13}^{(i)}}, \\ g^{-i}bg^i=c^{\lambda_{21}^{(i)}\lambda_{22}^{(i)}\lambda_{23}^{(i)}}, \\ g^{-i}cg^i=a^{\lambda_{31}^{(i)}\lambda_{32}^{(i)}\lambda_{33}^{(i)}}, \end{cases}$$

而应有

$$\begin{pmatrix} \lambda_{11}^{(i)}\lambda_{12}^{(i)}\lambda_{13}^{(i)} \\ \lambda_{21}^{(i)}\lambda_{22}^{(i)}\lambda_{23}^{(i)} \\ \lambda_{31}^{(i)}\lambda_{32}^{(i)}\lambda_{33}^{(i)} \end{pmatrix}^7=\begin{pmatrix} 1&0&0 \\ 0&1&0 \\ 0&0&1 \end{pmatrix}(\text{mod}2)$$

实际上还有

$$\begin{pmatrix} \lambda_{11}^{(i)}\lambda_{12}^{(i)}\lambda_{13}^{(i)} \\ \lambda_{21}^{(i)}\lambda_{22}^{(i)}\lambda_{23}^{(i)} \\ \lambda_{31}^{(i)}\lambda_{32}^{(i)}\lambda_{33}^{(i)} \end{pmatrix}\equiv\Delta_g^i(\text{mod}2)，\text{及 } \lambda_{\alpha\beta}^{(1)}=\lambda_{\alpha\beta}.$$

显然，又有 $G=\{a, b, c, g\}=\{a, b, c, g^2\}=\cdots=\{a, b, c, g^6\}$。

注意：G 为8阶初等交换群 B 被7阶循环群之扩张（且已假定这扩张 G 无指数2之子群）。下面我们将证明这样的扩张是唯一地存在，为此，就只需要证明：对任何的

$$A=\begin{pmatrix}\mu_{11}\mu_{12}\mu_{13}\\ \mu_{21}\mu_{22}\mu_{23}\\ \mu_{31}\mu_{32}\mu_{33}\end{pmatrix}\in GL(3,K_2)$$

当其阶为 7，即 $A^7\equiv\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$(mod2)时，我们能在上述的 $G=\{a,b,c,g^i\}$ 中找得正规子群 B 的另一组生成元 a_1,b_1,c_1，即 $B=\{a_1\}\times\{b_1\}\times\{c_1\}$，$a_1^2=b_1^2=?=1=[a_1,b_1]=[a_1,c_1]=[b_1,c_1]$，因而 $G=\{a_1,b_1,c_1,g^i\}$，能有

$$\begin{cases}g^{-i}a_1g^i=a_1^{\mu_{11}}b_1^{\mu_{12}}c_1^{\mu_{13}}\\ g^{-i}b_1g^i=a_1^{\mu_{21}}b_1^{\mu_{22}}c_1^{\mu_{23}}\\ g^{-i}c_1g^i=a_1^{\mu_{31}}b_1^{\mu_{32}}c_1^{\mu_{33}}\end{cases}$$

就行了。

但 a_1,b_1,c_1 存在的充要条件是 $\begin{cases}a_1=a^\alpha b^\beta c^\gamma\\ b_1=a^\mu b^\nu c^\delta\\ c_1=a^\xi b^\zeta c^\eta\end{cases}$ 中的矩阵 $P=\begin{pmatrix}\alpha&\beta&\gamma\\ \mu&\nu&\delta\\ \xi&\zeta&\eta\end{pmatrix}$为满秩的，即 $det\ P\equiv1(mod2)$。于是由

$$g^{-i}a_1g^i=\begin{cases}=a_1^{\mu_{11}}b_1^{\mu_{12}}c_1^{\mu_{13}}=a^{\alpha\mu_{11}+\mu\mu_{12}+\xi\mu_{13}}b^{\beta\mu_{11}+\nu\mu_{12}+\zeta\mu_{13}}c^{\gamma\mu_{11}+\delta\mu_{12}+\eta\mu_{13}},\\ =(g^{-i}ag^i)^\alpha(g^{-i}bg^i)^\beta(g^{-i}cg^i)^\gamma\end{cases}$$

$$=a^{\lambda_{11}^{(i)}\alpha+\lambda_{21}^{(i)}\beta+\lambda_{31}^{(i)}\gamma}b^{\lambda_{12}^{(i)}\alpha+\lambda_{22}^{(i)}\beta+\lambda_{32}^{(i)}\gamma}c^{\lambda_{13}^{(i)}\alpha+\lambda_{23}^{(i)}\beta+\lambda_{33}^{(i)}\gamma},$$

得

$$(\mu_{11},\mu_{12},\mu_{13})\begin{pmatrix}\alpha&\beta&\gamma\\ \mu&\nu&\delta\\ \xi&\zeta&\eta\end{pmatrix}\equiv(\alpha,\beta,\gamma)\begin{pmatrix}\lambda_{11}^{(i)}\lambda_{12}^{(i)}\lambda_{13}^{(i)}\\ \lambda_{21}^{(i)}\lambda_{22}^{(i)}\lambda_{23}^{(i)}\\ \lambda_{31}^{(i)}\lambda_{32}^{(i)}\lambda_{33}^{(i)}\end{pmatrix}(\text{mod}2)$$

同理，由 $g^{-i}b_1g^i$ 与 $g^{-i}c_1g^i$ 又分别可得

$$(\mu_{21},\mu_{22},\mu_{23})\begin{pmatrix}\alpha&\beta&\gamma\\ \mu&\nu&\delta\\ \xi&\zeta&\eta\end{pmatrix}\equiv(\mu,\nu,\delta)\begin{pmatrix}\lambda_{11}^{(i)}\lambda_{12}^{(i)}\lambda_{13}^{(i)}\\ \lambda_{21}^{(i)}\lambda_{22}^{(i)}\lambda_{23}^{(i)}\\ \lambda_{31}^{(i)}\lambda_{32}^{(i)}\lambda_{33}^{(i)}\end{pmatrix}(\text{mod}2)$$

与

$$(\mu_{31},\mu_{32},\mu_{33})\begin{pmatrix}\alpha&\beta&\gamma\\ \mu&\nu&\delta\\ \xi&\zeta&\eta\end{pmatrix}\equiv(\xi,\zeta,\eta)\begin{pmatrix}\lambda_{11}^{(i)}\lambda_{12}^{(i)}\lambda_{13}^{(i)}\\ \lambda_{21}^{(i)}\lambda_{22}^{(i)}\lambda_{23}^{(i)}\\ \lambda_{31}^{(i)}\lambda_{32}^{(i)}\lambda_{33}^{(i)}\end{pmatrix}(\text{mod}2)$$

合并上面三个式子就得到了矩阵间的关系是：

$$\begin{pmatrix}\mu_{11}\mu_{12}\mu_{13}\\ \mu_{21}\mu_{22}\mu_{23}\\ \mu_{31}\mu_{32}\mu_{33}\end{pmatrix}\begin{pmatrix}\alpha & \beta & \gamma\\ \mu & \nu & \delta\\ \xi & \zeta & \eta\end{pmatrix}\equiv\begin{pmatrix}\alpha & \beta & \gamma\\ \mu & \nu & \delta\\ \xi & \zeta & \eta\end{pmatrix}\begin{pmatrix}\lambda_{11}^{(i)}\lambda_{12}^{(i)}\lambda_{13}^{(i)}\\ \lambda_{21}^{(i)}\lambda_{22}^{(i)}\lambda_{23}^{(i)}\\ \lambda_{31}^{(i)}\lambda_{32}^{(i)}\lambda_{33}^{(i)}\end{pmatrix}(\mathrm{mod}2)$$

即 $P^{-1}AP\equiv\Delta_0^i(mod2)$。

这就说明了我们要解决的问题转化成了这样一个问题，即：给了 $GL(3,K_2)$ 中的两个矩阵 A 与 Δ（阶均为 7）后，要证明在 $GL(3,K_2)$ 中必有一矩阵 P 使等式 $P^{-1}AP=\Delta^i$ 成立的 $i(i=1,2,3,4,,5,6)$一定存在。下面就来证明 P 与 i 的存在性。

事实上，因域 K_2 仅有二元，即 0 与 1，故从 $\Delta\in GL(3,K_2)$知 $det\Delta=1$，且 Δ 之特征多项式 $f(\lambda)=det(\lambda E-\Delta)=\lambda^3+\lambda^2+\lambda+1$，或 $=\lambda^3+\lambda^2+1$，或 $=\lambda^3+\lambda+1$，或λ^3+1，只这四个可能。但 $\Delta^7=E$ 又说明了Δ 的最小多项式 $m(\lambda)$为 λ^7+1之因式（指在域 K_2 内而言，下同），然 λ^7+1 与其导函数 λ^6 无公共根，故 λ^7+1无重根，因而 $m(\lambda)$ 亦无重根。于是 $det(\lambda E-\Delta)=f(\lambda)=\lambda^3+\lambda^2+\lambda+1=(\lambda+1)^3$ 时由 $m(\lambda)\mid f(\lambda)$ 即得 $m(\lambda)=\lambda+1$，因之 $\Delta=E$，与 Δ 之阶为 7 的假定反不可。当 $f(\lambda)=\lambda^3+1$ 时因有 $O=f(\Delta)=\Delta^3+E$，就得到 $\Delta_3=E$，故再由 $\Delta^7=E$就必有 $\Delta=E$，不可（理由同上）。于是，仅为次之二个可能：
$det(\lambda E-\Delta)=f(\lambda)=\lambda^3+\lambda^2+1$ 或 $=\lambda^3+\lambda+1$。

但不论为何，都易证 $f(\lambda)$与导函数 $f'(\lambda)$无公共根，故 $f(\lambda)$无重根，因之这时不得不有 $m(\lambda)=f(\lambda)$，由是 Δ 的有理标准形 (classical canonical form) 是：

$$C=\begin{pmatrix}0 & 1 & \\ 1 & 0 & 0\\ & 1 & 1\end{pmatrix}\text{当 } f(\lambda)=\lambda^3+\lambda^2+1\text{时}$$

或

$$D=\begin{pmatrix}0 & 1 & \\ 1 & 0 & 1\\ & 1 & 0\end{pmatrix}\text{当 } f(\lambda)=\lambda^3+\lambda+1\text{时。}$$

同理，A 之有理标准形也是 C 或 D，只这二个可能。

于是，当 A 与 Δ 之有理标准形同为 C 或同为 D 时，即在 $GL(3,K_2)$内 A 与 Δ 都和 C（或 D）相似，那末 A 与 Δ 必互为相似，即有 $P\in GL(3,K_2)$使 $P^{-1}AP=\Delta$。

苟若 A 与 Δ 之有理标准形一为 C，一为 D 时，如令为 $R^{-1}AR=C$，$S^{-1}\Delta S=D$（R，$S\in GL(3,K_2)$），则易证从 $O=f(\Delta)=\Delta^3+\Delta+E$ 得 $O=\Delta^3(\Delta_3+\Delta+E)=(\Delta^3)^3+\Delta^7+\Delta^6=(\Delta^3)^3+(\Delta^3)^2+E$，即阶 7 之矩阵 Δ^3 适合方程 $\lambda^3+\lambda^2+1=0$，由于它无重根且在域 K_2 内既约，马上得知 Δ^3 之最小多项式不得不为 $\lambda^3+\lambda^2+1$，因而 Δ^3 之有理标准形亦必为

$C=\begin{pmatrix}0&1&\\1&0&0\\&1&1\end{pmatrix}$，即有 $T\in GL(3,K_2)$ 使 $T^{-1}\Delta^3T=C$，于是 $R^{-1}AR=T^{-1}\Delta^3T$，故 $P^{-1}AP=\Delta^3$（$P=RT^{-1}\in GL(3,K_2)$）。对于 $R^{-1}AR=D$ 及 $S^{-1}\Delta S=C$ 之情况亦可类似地推出相应的结果：事实上，由 $O=f(\Delta)=\Delta^3+\Delta^2+E$，得知 $O=\Delta^2+\Delta^3+E=(\Delta^3)^3+(\Delta^3)+E$，说明阶为7之矩阵 Δ^3 满足方程 $\lambda^3+\lambda+1=0$，但由于这方程无重根且在域 K_2 内既约，则知 Δ^3 之最小多项式就是 $\lambda^3+\lambda+1$，故 Δ^3 之有理标准形为 $\begin{pmatrix}0&0&1\\1&0&1\\0&1&0\end{pmatrix}=D$，即有 $Q\in GL(3,K_2)$ 使 $Q^{-1}\Delta^3Q=D$。于是，由 $R^{-1}AR=D$ 得 $P^{-1}AP=\Delta^3$，但 $P=RQ^{-1}\in GL(3,K_2)$。

于是，不论 Δ_0 怎样选取，只要 $\Delta_0^7\equiv\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}\pmod 2$，群 G 之型是唯一的。今选 $\Delta_0=\begin{pmatrix}0&0&1\\1&0&0\\0&1&1\end{pmatrix}$，得次型：

(xiii)′：$G=\{a,b,c,g\}$，$a^2=b^2=c^2=g^7=1=[a,b]=[a,c]=[b,c]$，$g^{-1}ag=c$，$g^{-1}bg=a$，$g^{-1}cg=bc$。

故又得到

定理2。56阶群有13个，其构造见表三。

（表三）

56 = $2^3\cdot7$ 阶群 G	种类	构造（定义关系）
	(1) | (12)	表二中的(1)——(12)，只将 $p=7$ 代换之。
	(13)	$G=\{a,b,c,g\}$，$a^2=b^2=c^2=[a,b]=[a,c]=[b,c]=g^7=1$， $g^{-1}ag=c$，$g^{-1}bg=a$，$g^{-1}cg=bc$

最后，来讨论 $p=3$ 的情况。即 $O(G)=2^3\cdot3=24$。G 之可解性保证了 G 有指数2或3之正规子群。若有 $A\triangleleft G$ 使 $[G:A]=2$，则 $O(A)=12$，于是 A 只能是表一中的Ⅰ，Ⅱ，Ⅲ（以 $p=3$ 代之）及

(V)′：$A\cong A_4$（四次交代群），即 $A=\{a,b,c\}$，$a^2=b^2=c^3=1$，