Pure Mathematics 理论数学, 2014, 4, 172-178
Published Online September 2014 in Hans. http://www.hanspub.org/journal/pm
http://dx.doi.org/10.12677/pm.2014.45026

Hans汉斯

An Elementary Proof for the Uniqueness (up to Isomorphism) of the Simple Groups of Order 360 and 504

Feng Zhou[1], Haoran Yu[2], Jie Wang[2], Heguo Liu[1*]

[1]Department of Mathematics, Hubei University, Wuhan
[2]Department of Mathematics, Peking University, Beijing
Email: thoufeng@163.com, *ghliu@hubu.edu.cn

Received: Jul. 12th, 2014; revised: Aug. 10th, 2014; accepted: Aug. 19th, 2014

Abstract

Only by using Sylow's theorem, basic permutation computation and linear algebra theory, we prove that a simple group of order 360 is isomorphic to *PSL* (2,9) and a simple group of order 504 is isomorphic to *PSL* (2,8).

Keywords

Sylow's Theorem, Simple Group, *PSL* (2,9), *PSL* (2,8)

360阶和504阶单群的唯一性的初等群论证明

周　峰[1]，于浩然[2]，王　杰[2]，刘合国[1*]

[1]湖北大学数学系，武汉
[2]北京大学数学系，北京
Email: thoufeng@163.com, *ghliu@hubu.edu.cn

收稿日期：2014年7月12日；修回日期：2014年8月10日；录用日期：2014年8月19日

*通讯作者。

摘　要

仅用Sylow定理、最基本的置换计算和线性代数重新证明了360阶单群同构于*PSL* (2,9)及504阶单群同构于*PSL* (2,8)。

关键词

Sylow定理；单群；*PSL* (2,9)，*PSL* (2,8)

1. 引言

本文采用的符号和术语都是标准的，见文献[1]。

我们知道，对 n 阶的非交换单群，当 $n \le 1000$ 时， n 只能是 60、168、360、504、660，并且阶不超过 1000 的非交换单群只有 5 个：60 阶单群 A_5 、168 阶单群 $PSL(2,7)$ 、360 阶单群 A_6 、504 阶单群 $PSL(2,8)$ 和 660 阶单群 $PSL(2,11)$ 。运用 Sylow 定理不难证明 60 阶单群同构于 A_5 ，见文献[2]和[3]。在文献[2]和[3]中，Huppert 和 Smith 分别用不同的初等群论方法证明了 168 阶单群同构于 $PSL(2,7)$ ，而 360 阶单群同构于的 A_6 初等群论证明见[4] [5]，[6]利用文献[2]的方法证明了 660 阶单群同构于 $PSL(2,11)$ 。对于 504 阶单群同构于 $PSL(2,8)$ ，在[5]中，Cole 利用置换群的技巧给出了证明。这样，阶不超过 1000 的非交换单群同构唯一性都有了初等的群论证明。而本文将利用[2]和[6]里的方法，从射影线性群的角度出发，将 360 阶单群及 504 阶单群里的某些元素与射影线性群里的元素对应起来，从而将给定阶的单群嵌入射影线性群里，再通过比较群的阶，重新证明 360 阶单群同构于 $PSL(2,9)$ 及 504 阶单群同构于 $PSL(2,8)$ 。除了 Sylow 定理和最基本的群论知识外，本文是完全自包含的，这个证明对初学者来说是容易理解的，作者希望它对群论教学具有借鉴和启发作用。

2. 360 阶单群同构于 $PSL(2,9)$ 的初等群论证明

证明：设 G 是 360 阶单群。

(1) $n_5(G)=36$ 。由 Sylow 第三定理知 $n_5(G)=1$，6 或 36。由 G 是单群， $n_5(G)$ 不可能为 1。谬设 $n_5(G)=6$ ，由 G 是 360 阶单群， $G \cong A_6$ ，而 $n_5(A_6)=36$ ，矛盾！

(2) 若 $P_1,P_2 \in Syl_3(G)$ 且 $P_1 \ne P_2$ ，则 $P_1 \cap P_2 = 1$ 。谬设 $D = P_1 \cap P_2 > 1$ ，则 $|D|=3$ 。从而 $P_1,P_2 \le N_G(D)$ 。从而 $|N_G(D)| \ge 36$ 。由于 G 是 360 阶单群， $|N_G(D)|=36$ 。不难看出 $N_G(D)/D$ 中之 4 阶子群正规，设 $X \in Syl_2(N_G(D))$ ，则 $XD \lhd N_G(D)$ 。不难看出 $|C_X(D)|=2$ 或 4，且 $C_X(D)=O_2(XD)$ $char$ XD ，从而 $C_X(D) \lhd N_G(D)$ 。若 $|C_X(D)|=2$ ，则 $N_G(D)/C_X(D)$ 中有 9 阶子群正规，进而知 $N_G(D)$ 中 9 阶子群正规，矛盾！若 $|C_X(D)|=4$ ，则 $72 \| N_G(C_X(D))|$ ，矛盾于 G 是 360 阶单群！

(3) $n_3(G)=10$ 。由 Sylow 第三定理知 $n_3(G)=1,4,10$ 或 40。由 G 是 360 阶单群， $n_3(G)$ 不可能为 1 或 4。若 $n_3(G)=40$ ，则由 1、2 知 G 中至少有 $36\times4+40\times8+1=465$ 个元素，矛盾！故 $n_3(G)=10$ 。取定 $P \in Syl_3(G)$ ，则 $|N_G(P)|=36$ 。

(4) G 中无 6 阶元及 10 阶元。谬设 G 中有 6 阶元 x。注意到 G 依共轭作用在 $Syl_3(G)$ 上诱导 G 到 A_{10} 的群嵌入。承 2 知 x^2 引起的置换同形于 $(1)(234)(567)(8,9,10)$ 。从而 x 引起的置换同形于 $(1)(234567)(8,9,10)$ ，是奇置换，矛盾！谬设 G 中有 10 阶元 y，同样注意到 G 依共轭作用在 $Syl_3(G)$ 上诱导 G 到 A_{10} 的群嵌入，且由 3 知 y 引起的置换无不动点。从而 y 引起的置换同形于 $(1,2,3,4,5,6,7,8,9,10)$ ，是奇置换，矛盾！

(5) $P\cong Z_3\times Z_3$ 且 $N_G(P)$ 是 Frobenius 群， P 在 $N_G(P)$ 中的补群是 4 阶循环群。谬设 $P\cong Z_9$。由于 $Aut(Z_9)\cong Z_6$，故 $N_G(P)$ 中有 6 阶元，矛盾于(4)。亦承(4)知 $N_G(P)$ 是 36 阶 Frobenius 群，进一步地， P 在 $N_G(P)$ 中的补群是 4 阶循环群。

(6) P 依共轭正则地作用在 $Syl_3(G)\setminus\{P\}$ 上。从而 $N_G(P)$ 在 $Syl_3(G)$ 上的传递的共轭作用置换同构于 9 元域 $F_9=Z_3[x]/(x^2+1)$ 上的射影空间上的置换群

$$\langle u_\eta=(\infty\mapsto\infty,\xi\mapsto\xi+\eta,\forall\xi\in F_9),n=(\infty\mapsto\infty,\xi\mapsto\bar{x}\xi,\forall\xi\in F_9)\mid\forall\eta\in F_9\rangle。$$

$\begin{pmatrix}0&\eta\\1&1\end{pmatrix},\begin{pmatrix}\bar{x}&0\\0&1\end{pmatrix}$的行列式都是 F_9 中的平方元，故 $N_G(P)$ 嵌入 $PSL(2,9)$。

(7) 首先证明 G 之 Sylow 2-子群同构于 D_8。取定 $Q\in Syl_2(G)$，谬设 Q 交换，由于 G 中有 4 阶循环子群，故 $Q\cong Z_8$ 或 $Z_4\times Z_2$。由 4 知 $N_G(Q)=Q$，且 Q 之任一非单位元 z 都满足 $C_G(z)=Q$，进而 z 在 G 中的共轭类长 $|Cl(z)|=45$。如果 $g\in G,x,y\in Q$ 使得 $y=x^g$。则 $Q=C_G(y)=C_G(x^g)=C_G(x)^g=Q^g$，从而 $g\in N_G(Q)=Q,y=x^g=x$。从而 G 共有 $45\times7=315$ 个 2-元素。G 中至少有 $315+144+80+1=540$ 个元素，矛盾！谬设 $Q\cong Q_8$， 设 n $(n\in N_G(P),\circ(n)=4)$ 诱导的置换是 $(\infty\mapsto\infty,\xi\mapsto\bar{x}\xi,\forall\xi\in F_9)$。 $\exists m\in G$ 使得 $\circ(m)=4,m^{-1}nm=n^{-1},m^2=n^2$。则 m^2 引起的置换的不动点只有 $0,\infty$， m 引起的置换对换 $0,\infty$。从而 m 诱导的置换同形于 $(0,\infty)(1234)(5678)$，是奇置换，矛盾!故 $Q\cong D_8$。

(8) 由于 $Q\cong D_8$，故 $\exists t\in G$ 使得 $\circ(t)=2,tnt=n^{-1}$，则 t 对换 $0,\infty$。以下简记 $\bar{x}$ 为 x。则 t 诱导的置换：

$$t:0\mapsto\infty,\infty\mapsto0,1\mapsto1^t,x\mapsto-x1^t,-1\mapsto-1^t,-x\mapsto x1^t,1+x\mapsto(1+x)^t,$$
$$x-1\mapsto-x(1+x)^t,-x-1\mapsto-(1+x)^t,1-x\mapsto x(1+x)^t。$$

由于 t 诱导的是偶置换，故 $1^t=1,-1,x$ 或 $-x$。

若 $1^t=1$，则 $tn:1\mapsto1\mapsto x,x\mapsto-x\mapsto1,-1\mapsto-1\mapsto-x,-x\mapsto x\mapsto-1$， $1^{tn}=x$ 且 $\circ(tn)=2,(tn)n(tn)^{-1}=n^{-1}$，故可以用 tn 替代 t。

若 $1^t=-1$，则 $tn^3:1\mapsto-1\mapsto x,x\mapsto x\mapsto1,-1\mapsto1\mapsto-x,-x\mapsto-x\mapsto-1$，同理以用 tn^3 替代 t。

若 $1^t=-x$，则 $tn^2:1\mapsto-x\mapsto x,x\mapsto-1\mapsto1,-1\mapsto x\mapsto-x,-x\mapsto1\mapsto-1$，同理以用 tn^2 替代 t。

故无妨设 $1^t=x$， $t:1\mapsto x,x\mapsto1,-1\mapsto-x,-x\mapsto-1$。

同理 $(1+x)^t=1+x,1-x,-1-x$ 或 $x-1$。

若 $(1+x)^t=1+x$，则

$$t:0\mapsto\infty,\infty\mapsto0,1\mapsto x,x\mapsto1,-1\mapsto-x,-x\mapsto-1,1+x\mapsto1+x,$$
$$x-1\mapsto1-x,-x-1\mapsto-x-1,1-x\mapsto x-1.$$

考虑平移(P 中某 3 阶元诱导)-1：
$$0\mapsto-1,\infty\mapsto\infty,1\mapsto0,x\mapsto x-1,-1\mapsto1,-x\mapsto-x-1,$$
$$1+x\mapsto x,x-1\mapsto1+x,-x-1\mapsto1-x,1-x\mapsto-x.$$

则 $t(-1)$ (先作用 t，后作用 -1)：
$$0\mapsto\infty,\infty\mapsto-1,1\mapsto x-1,x\mapsto0,-1\mapsto-x-1,-x\mapsto1,$$
$$1+x\mapsto x,x-1\mapsto-x,-x-1\mapsto1-x,1-x\mapsto x+1.$$

即 $(1,x-1,-x)(x,0,\infty,-1,-x-1,1-x,1+x)$，是 21 阶元，但 21 不整除 360，矛盾！

若 $(1+x)^t=1-x$，则
$$t:0\mapsto\infty,\infty\mapsto0,1\mapsto x,x\mapsto1,-1\mapsto-x,-x\mapsto-1,1+x\mapsto1-x,$$
$$x-1\mapsto-x-1,-x-1\mapsto x-1,1-x\mapsto x+1.$$

即 $(0,\infty)(1,x)(-1,-x)(1+x,-x)(x-1,-x-1)$，是奇置换，矛盾！

若 $(1+x)^t=x-1$，则
$$t:0\mapsto\infty,\infty\mapsto0,1\mapsto x,x\mapsto1,-1\mapsto-x,-x\mapsto-1,1+x\mapsto x-1,$$
$$x-1\mapsto x+1,-x-1\mapsto1-x,1-x\mapsto-x-1.$$

即 $(0,\infty)(1,x)(-1,-x)(1+x,x-1)(-x-1,1-x)$，亦是奇置换，矛盾！

从而 $(1+x)^t=-1-x$，$\begin{array}{l} t:0\mapsto\infty,\infty\mapsto 0,1\mapsto x,x\mapsto 1,-1\mapsto -x,-x\mapsto -1,1+x\mapsto -1-x,\\ x-1\mapsto x-1,-x-1\mapsto x+1,1-x\mapsto 1-x. \end{array}$

亦即 $\xi\mapsto\frac{\overline{x}}{\xi},\forall\xi\in F_9\cup\{\infty\}$。可由 $\begin{pmatrix}0 & \overline{x}\\ 1 & 0\end{pmatrix}$ 诱导。由于 $-\overline{x}$ 是 F_9 中之平方元，故 $\langle N_G(P),t\rangle$ 嵌入 $PSL(2,9)$。由于 $72\left|\langle N_G(P),t\rangle\right|$，从而 $G=\langle N_G(P),t\rangle$，$G$ 可嵌入 $PSL(2,9)$ 中，再比较群的阶，得 $G\cong PSL(2,9)$。

3. 关于 $PSL(2,8)$

为了讨论 504 阶单群的唯一性，我们从 $PSL(2,8)$ 的元素和 Sylow 子群入手。

首先注意到 $PSL(2,8)\cong SL(2,8)$，我们通过弄清 $SL(2,8)$ 的结构来得到 $PSL(2,8)$ 的相关信息。

(1) $g_1=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ 是 $SL(2,8)$ 的单位元。

(2) $g_2=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ 为 $SL(2,8)$ 的一个 2 阶元，若有 $g=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in SL(2,8)$ 使 $gg_2=g_2g$，则 $\begin{pmatrix}a & a+b\\ c & c+d\end{pmatrix}=\begin{pmatrix}a & b+d\\ c & d\end{pmatrix}$，因此 $a=d$，$c=0$，$g=\begin{pmatrix}a & b\\ 0 & a\end{pmatrix}$。考虑到 $g\in SL(2,8)$，$a^2=1$，此时 $a=1$，$g=\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}$，$b\in F_8$，$\left|C_{SL(2,8)}(g_2)\right|=8$，$g_2$ 所在的共轭类长为 63。

(3) x^3+x+1 为 F_2 上不可约多项式，不妨设 $F_8=\{a+b\eta+c\eta^2\mid a,b,c\in F_2\text{且}\eta^3=1+\eta\}$，令 $s\in F_8^*$，则 s 为 7 阶元。当 $s=\eta$ 时，$s^{-1}=1+\eta^2$；当 $s=\eta^2$ 时，$s^{-1}=1+\eta+\eta^2$；当 $s=1+\eta$ 时，$s^{-1}=\eta+\eta^2$。令 $g_3=\begin{pmatrix}\eta & 0\\ 0 & 1+\eta^2\end{pmatrix}$，$g_4=\begin{pmatrix}\eta^2 & 0\\ 0 & 1+\eta+\eta^2\end{pmatrix}$，$g_5=\begin{pmatrix}1+\eta & 0\\ 0 & \eta+\eta^2\end{pmatrix}$，易知 g_3，g_4，g_5 均为 7 阶元，若有 $g=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in SL(2,8)$ 使 $gg_3=g_3g$，则 $\begin{pmatrix}a\eta & b+b\eta^2\\ c\eta & d+d\eta^2\end{pmatrix}=\begin{pmatrix}\eta a & \eta b\\ c+c\eta^2 & d+d\eta^2\end{pmatrix}$，此时 $b=c=0$，因此 $g=\begin{pmatrix}a & 0\\ 0 & d\end{pmatrix}$，其中 $ad=1$。容易得到 $\left|C_{SL(2,8)}(g_3)\right|=7$，$g_3$ 所在的共轭类长 72，同样的计算可得 g_4，g_5 所在的共轭类长分别为 72。

(4) F_8 上首一 2 次的常数项为 1 的不可约多项式有

$$x^2+x+1,\quad x^2+\eta x+1,\quad x^2+\eta^2x+1,\quad x^2+(\eta+\eta^2)x+1$$

四个多项式对应的相伴矩阵分别为

$$g_6=\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix},\quad g_7=\begin{pmatrix}0 & 1\\ 1 & \eta\end{pmatrix},\quad g_8=\begin{pmatrix}0 & 1\\ 1 & \eta^2\end{pmatrix},\quad g_9=\begin{pmatrix}0 & 1\\ 1 & \eta+\eta^2\end{pmatrix}$$

可选取 F_{64}^* 的一个生成元 ε 使 $\varepsilon^7+\varepsilon^{-7}=\eta$，此时 $\varepsilon^{14}+\varepsilon^{-14}=\eta^2$，$\varepsilon^{21}+\varepsilon^{-21}=1$ 且 $\varepsilon^{28}+\varepsilon^{-28}=\eta^4=\eta+\eta^2$，因此 g_6，g_7，g_8，g_9 均可表成形如 $\begin{pmatrix}0 & 1\\ 1 & r+r^{-1}\end{pmatrix}$ 的矩阵。

若有 $g=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in SL(2,8)$ 使 $g\begin{pmatrix}0 & 1\\ 1 & r+r^{-1}\end{pmatrix}=\begin{pmatrix}0 & 1\\ 1 & r+r^{-1}\end{pmatrix}g$ 则 $\begin{pmatrix}b & a+b(r+r^{-1})\\ d & c+d(r+r^{-1})\end{pmatrix}=\begin{pmatrix}c & d\\ a+d(r+r^{-1}) & b+d(r+r^{-1})\end{pmatrix}$，$g=\begin{pmatrix}a & b\\ b & a+b(r+r^{-1})\end{pmatrix}$，另外，

$ad-bc=a\left(a+b\left(r+r^{-1}\right)\right)-b^2=\left(a+br\right)\left(a+br^{-1}\right)=1$。令 $\Omega=\left|\left\{(a,b)\mid ad-bc\neq 0\right\}\right|$，由于 $(a,b)\neq(0,0)$ 当且仅当 $ad-bc\neq 0$，因此 $|\Omega|=8^2-1=63$。令 $\Omega_1=\left|\left\{(a,b)\mid ad-bc=1\right\}\right|$，若 $ad-bc=\alpha\in F_8$ (其中 $\alpha\neq 0,1$)，F_8 里的每个元都是平方元，故存在 $\beta\in F_8$ 使 $\alpha=\beta^2$，此时 $ad-bc=\left(a+br\right)\left(a+br^{-1}\right)=\beta^2$，$\left(a\beta^{-1}+b\beta^{-1}r\right)\left(a\beta^{-1}+b\beta^{-1}r^{-1}\right)=1$，此时 (a,b) 的取法种数为 $|\Omega_1|$。因此 $|\Omega_1|=\dfrac{|\Omega|}{7}=9$，即 $\left|C_{SL(2,8)}\left(g_6\right)\right|=\left|C_{SL(2,8)}\left(g_7\right)\right|=\left|C_{SL(2,8)}\left(g_8\right)\right|=\left|C_{SL(2,8)}\left(g_9\right)\right|=9$，$g_6$，$g_7$，$g_8$，$g_9$ 所在的共轭类长都是 56。

综上所述，考虑到 g_2、g_3、g_4、g_5、g_6、g_7、g_8 和 g_9 具有不同的迹，它们彼此不相似，而 $1+63+72+72+72+56+56+56+56=504=\left|SL(2,8)\right|$，这说明我们已经找出了 $SL(2,8)$ 的所有共轭类，综合(1)、(2)、(3)、(4)，我们得到 $SL(2,8)$ 的元素的信息(如表 1)。

由于 $PSL(2,8)\cong SL(2,8)$，所以 $PSL(2,8)$ 也具有同样的共轭类。

现在，我们能够很快证明 $PSL(2,8)$ 是一个单群。事实上，任取 $PSL(2,8)$ 的正规子群 N，N 的阶整除 504，且 $|N|=1+63x_1+72x_2+56x_3$，其中 $x_1=0$ 或 1，$x_2=0$、1、2 或 3，$x_3=0$、1、2、3 或 4。不难验证 $|N|=1$ 或 504，即 $N=1$ 或 $PSL(2,8)$，$PSL(2,8)$ 是单群。

(5) 令 $P=\left\langle\begin{pmatrix}1&a\\0&1\end{pmatrix}\mid a\in F_8\right\rangle$，此时 P 为初等 Abel 群且 $P\in Syl_2\left(PSL(2,8)\right)$，由于 $g_3=\begin{pmatrix}\eta&0\\0&1+\eta^2\end{pmatrix}$ 为 $PSL(2,8)$ 的 7 阶元且 $g_3^{-1}\begin{pmatrix}1&a\\0&1\end{pmatrix}g_3=\begin{pmatrix}1&a\left(1+\eta^2\right)^2\\0&1\end{pmatrix}\in P$，故 7 整除 $\left|N_{PSL(2,8)}(P)\right|$，再考虑到 8 整除 $\left|N_{PSL(2,8)}(P)\right|$ 及 $PSL(2,8)$ 是单群，所以 $\left|N_{PSL(2,8)}(P)\right|=56$，$PSL(2,8)$ 的 Sylow 2-子群的个数 $n_2=9$。

(6) 由于 $PSL(2,8)$ 有 9 阶元，故 $PSL(2,8)$ 的 Sylow 3-子群 Q 为循环群，Q 包含 6 个 9 阶元，而 $PSL(2,8)$ 含有 56×3 个 9 阶元，我们得到 $PSL(2,8)$ 的 Sylow 3-子群的个数 $n_3=\dfrac{56\times 3}{6}=28$，$\left|N_{PSL(2,8)}(Q)\right|=18$。

(7) $PSL(2,8)$ 的 Sylow 7-子群 R 为循环群，R 包含 6 个 7 阶元，而 $PSL(2,8)$ 含有 72×3 个 7 阶元，我们得到 $PSL(2,8)$ 的 Sylow 7-子群的个数 $n_7=\dfrac{72\times 3}{6}=36$，$\left|N_{PSL(2,8)}(R)\right|=14$。

综上所述，我们得到 $PSL(2,8)$ 的 Sylow 子群 P 的如下信息：

素数	$\|P\|$	P 的结构	$\left\|Syl_p\left(PSL(2,8)\right)\right\|$	$\left\|N_{PSL(2,8)}(P)\right\|$
2	8	初等 Abel 群	9	56
3	9	循环群	28	18
7	7	循环群	36	14

这些信息有助于我们弄清 504 阶单群的 Sylow 子群及其正规化子的结构。

Table 1. The classes of $SL(2,8)$
表 1. $SL(2,8)$的共轭类

阶	1	2	7	7	7	3	9	9	9
代表元	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	g_9

共轭类长	1	63	72	72	72	56	56	56	56

4. 504 阶单群同构于 $PSL(2,8)$ 的初等群论证明

证明：设 G 是 504 阶单群，此时 $|G|=504=2^3\times3^2\times7$。

(1) $n_7(G)=36$。令 $R\in Syl_7(G)$，由 Sylow 定理知 $n_7(G)=1(\mathrm{mod}\,7)$ 和 $n_7(G)=|G:N_G(R)|$，因此 $n_5(G)=1,8$ 或 36。注意到 G 为单群，$n_5(G)=8$ 或 36。谬设 $n_7(G)=8$，则 $|N_G(R)|=63$，$N_G(R)$ 为 G 的指数为 8 的子群，这时容易验证 G 嵌入 A_8。容易知道 A_8 的 7 阶元有 $C_8^7\times6!$ 个，A_8 的 Sylow 7-子群有 $\frac{C_8^7\times6!}{6}=8\times5!$ 个，进一步地，$|N_{A_8}(R)|=\frac{8!/2}{8\times5!}=21$，而 $|N_G(R)|=63$，这是不可能的！所以只能有 $n_7(G)=36$，$|N_G(R)|=14$，这时，G 有 $(7-1)\times36=216$ 个 7 阶元。

(2) $n_3(G)=28$。取 $P\in Syl_3(G)$，由 Sylow 定理 $n_3(G)=1,4,7$ 或 28。注意到 G 是单群，所以 $n_3(G)=7$ 或 28。谬设 $n_3(G)=7$，则 G 同构于 A_7 的一个子群，而 $|A_7|=2520=5\times504$，故 G 是 A_7 的指数为 5 的子群，此时 $A_7/\bigcap_{x\in A_7}G^x\le A_5$，$G$ 是单群，只能有 $\bigcap_{x\in A_7}G^x=G$，即 $G\lhd A_7$，此时 A_7 的 7 阶元全部在 G 里，而 A_7 含有 $6!=720$ 个 7 阶元，G 含有 216 个 7 阶元，矛盾！于是只能有 $n_3(G)=28$，$|N_G(P)|=18$。

(3) G 的任意两个不同的 Sylow 3-子群有平凡的交。选取不同的 $A,B\in Syl_3(G)$。谬设 $D=A\cap B>1$，则 $|D|=3$ 且 $A,B\le N_G(D)$，显然 A,B 都是 $N_G(D)$ 的 Sylow 3-子群，$N_G(D)$ 的 Sylow 3-子群个数 $n_3(N_G(D))>1$ 且 9 整除 $|N_G(D)|$。又 $|AB|=\frac{|A||B|}{|A\cap B|}=27$，$|N_G(D)|\ge|AB|=27$。考虑到 G 的真子群指数大于 7，不难验证 $|N_G(D)|=36$ 或 63。如 $|N_G(D)|=63$，$N_G(D)$ 的 Sylow 7-子群正规，而 G 的 Sylow 7-子群的正规化子为 14 阶，这是不可能的！如 $|N_G(D)|=36$，$N_G(D)/D$ 是 12 阶群，$N_G(D)/D$ 的 Sylow 3-子群肯定不是正规的，由 Sylow 定理知，$N_G(D)/D$ 包含 4 个 Sylow 3-子群，它包含 8 个 3 阶元，故 $N_G(D)/D$ 的 Sylow 2-子群是正规的。设 T/D 是 $N_G(D)/D$ 的 Sylow 2-子群，$T\lhd N_G(D)$，取 T 的 Sylow 2-子群 X，X 是 4 阶群，$T=DX$。从 $X/C_X(D)\le Aut(G)=Z_2$ 知，$1<C_X(D)\le Z(T)$，$Z(T)$ 是 T 的中心。当 $|C_X(D)|=2$ 时，$C_X(D)$ 是 $Z(T)$ 的 Sylow 2-子群，故 $C_X(D)\lhd N_G(D)$，$N_G(D)/C_X(D)$ 是 18 阶群，它有正规的 Sylow 3-子群，这将导致 $N_G(D)$ 含有正规的 Sylow 3-子群，矛盾，因此只能有 $C_X(D)=X$。当 $C_X(D)=X$ 时，T 是 12 阶 Abel 群，X 是 T 的特征子群，$X\lhd N_G(D)$。又取 G 的包含 X 的 Sylow 2-子群 C，当然 $X\lhd C$，从而 $\langle A,B,C\rangle\le N_G(X)$，$|N_G(X)|$ 能被 $|A|\cdot|C|=72$ 整除，$|G:N_G(X)|=1$ 或 7，这是不可能的！因此 $D=1$，这表明 G 的任意两个不同的 Sylow 3-子群有平凡的交，G 含有 $(9-1)\times28=224$ 个 3-元。

(4) $n_2(N_G(R))=7$。取 $R\in Syl_7(G)$，$|N_G(R)|=14$，谬设 $N_G(R)$ 的 Sylow 2-子群正规，则 $N_G(R)$ 为 14 阶循环群，含 $\varphi(14)=6$ 的 14 阶元，故 G 一共包含 $36\times6=216$ 个 14 阶元，而 G 含有 216 个 7 阶元，224 个 3-元，$216+216+224>504$，矛盾！因此 $N_G(R)$ 的 Sylow 2-子群的个数 $n_2(N_G(R))=7$。

(5) G 所含的 2-元均为 2 阶元。考虑 $N_G(R)$ 作用在 $Syl_7(G)$，$N_G(R)$ 含有一个 7 阶子群并含有 7 个 2 阶子群，其中任意 2 阶元将 7 阶元映到它的逆，任意 7 阶元在 $Syl_7(G)$ 上引起的置换为 5 个不相交轮换的乘积，我们可以得到这个 2 阶元刚好在其中 3 个轮换中各有一个不动点，这样，这个 2 阶元刚好有 4 个不动点。此时，这个 2 阶元所在的共轭类长为 $\frac{36}{4}\times7=63$，我们得到 63 个共轭的 2 阶元。由于 G 含有 216 个 7 阶元，224 个 3-元，剩下 $504-216-224-1=63$ 个非单位元，所以这 63 个非单位元全为 2 阶元，并且它们彼此共轭。

(6) $n_2(G)=9$。令 $P\in Syl_2(G)$，由于 G 所含的 2-元均为 2 阶元，因此 P 为初等 Abel 群。由 Sylow

定理知 $n_2(G)=1(\mathrm{mod}\,2)$ 和 $n_2(G)=|G:N_G(P)|$，因此 $n_2(G)=1,3,7,9,21$ 或 63。注意到 G 为单群，$n_2(G)=9,21$ 或 63。谬设 $n_2(G)=21$，则 $|N_G(P)|=2^3\times 3$。由 Sylow 定理得 $n_3(N_G(P))=1$ 或 4，$N_G(P)$ 最多含有 $4\times(3-1)=8$ 个 3 阶元，但 $P\lhd N_G(P)$，$N_G(P)$ 含有 7 个 2-元，$8+7+1<24$，这表明 $N_G(R)$ 一定包含 6 阶元，由前面的讨论知这是不可能的！谬设 $n_2(G)=63$，则 $|N_G(P)|=8$。取不同的 2 阶元 $x,y\in P$，由前面的讨论，有 $a\in G$ 使 $y=x^a$，考虑到 P 为初等 Abel 群，$P=C_G(y)$，而 $C_G(y)=C_G(x^a)=C_G(x)^a$，故 $P=C_G(x)^a$，即 $P^{a^{-1}}=C_G(x)$，而 $P=C_G(x)$，因此 $P^{a^{-1}}=P$，$a^{-1}\in N_G(P)=P$，这就得到了 $y=x^a=x$，矛盾！这时只能有 $n_2(G)=9$，$|N_G(P)|=56$。

(7) 首先证明 $n_7(N_G(P))=8$。由于 G 含有 63 个 2 阶元，9 个 Sylow 2-子群，因而 G 的不同的 Sylow 2-子群交平凡，由于 $|N_G(P)|=56=2^3\times 7$，谬设 $n_7(N_G(P))=1$，则 $N_G(P)$ 有 $\varphi(56)=24$ 个 56 阶元，故 G 一共包含 $24\times 9=216$ 个 56 阶元，而 G 含有 216 个 7 阶元，224 个 3-元，$216+216+224>504$，矛盾！因此 $N_G(P)$ 的 Sylow 7-子群的个数 $n_7(N_G(P))=8$。

从而 $N_G(P)$ 在 $Syl_2(G)$ 上的传递的共轭作用置换同构于 8 元域 $F_8=Z_2[x]/(x^3+x+1)$ 上的射影空间上的置换群

$$\langle u_\eta=(\infty\mapsto\infty,\xi\mapsto\xi+\eta,\forall\xi\in F),n=(\infty\mapsto\infty,\xi\mapsto\bar{x}\xi,\forall\xi\in F)\,|\,\forall\eta\in F_8\rangle$$

设 $\langle n\rangle$ 是 $N_G(P)$ 的 7 阶子群，则 $|N_G(\langle n\rangle)|=14$，取 2 阶元 $t\in N_G(\langle n\rangle)$，由于 t 与 n 不交换，故 $n^t=n^{-1}$，按照[6]同样的方法，可得 t 作用在 $Syl_2(G)$ 上的置换为 $\xi\mapsto\frac{1^t}{\xi}$，由 $F_8=Z_2[x]/(x^3+x+1)$ 里的所有元都是平方元及

$$PSL(2,8)=\left\{\alpha:x\mapsto\frac{ax+b}{cx+d}\,|\,a,b,c,d\in F_8,ad-bc\text{是}F_8^*\text{中的平方数}\right\}$$

所以 u、n、t 对应的线性分式映射属于 $PSL(2,8)$。

令 $A=\langle u,n,t\rangle$，A 作为 G 的子群可嵌入 $PSL(2,8)$，其中 $\langle u,n\rangle$ 为 56 阶群且 t 为不属于 $\langle u,n\rangle$ 的 2 阶元，故 $|G:\langle u,n,t\rangle|<9$，即 A 是 G 的指数小于 9 的子群，再注意到 G 为单群，于是 $G=A$，故 G 可嵌入 $PSL(2,8)$，而 $|G|=|PSL(2,8)|$，因此 $G\cong PSL(2,8)$。

基金项目

国家自然科学基金(11371124)、湖北省高层次人才工程基金(070-016533)。

参考文献 (References)

[1] Isaacs, I.M. (2008) Finite group theory. American Mathematical Society, Providence.

[2] Huppert, B. (1967) Endliche gruppen. Springer-Verlag, Berlin, Heidelberg, New York.

[3] Smith, G. and Tabachnikova, O. (2000) Topics in group theory. Springer-Verlag, Berlin, Heidelberg, New York.

[4] 周峰, 徐行忠, 廖军, 刘合国 (2014) 360 阶单群同构于 A_6 的初等群论证明. *理论数学*, **1**, 31-37.

[5] Cole, F.N. (1893) Simple groups as far as order 660. *American Journal of Mathematics*, **15**, 303-315.

[6] 周峰, 徐涛, 刘合国 (2013) 660 阶单群同构于 *PSL*(2,11)的初等群论证明. *理论数学*, **4**, 241-243.