Pure Mathematics 理论数学, 2013, 3, 241-243
http://dx.doi.org/10.12677/pm.2013.34036 Published Online July 2013 (http://www.hanspub.org/journal/pm.html)

An Elementary Proof that the Simple Group of Order 660 Is Isomorphism to $PSL(2,11)$*

Feng Zhou[1], Tao Xu[2], Heguo Liu[1]

[1]College of Mathematics and Information Science, Hubei University, Wuhan
[2]College of Science, Hebei University of Engineering, Handan
Email: thoufeng@163.com, gtxutao@163.com, ghliu@hubu.edu.cn

Received: May 29th, 2013; revised: Jun. 14th, 2013; accepted: Jun. 21st, 2013

Abstract: In this paper, we will only use Sylow's theorem to prove that the simple group of order 660 is isomorphic to $PSL(2,11)$.

Keywords: Sylow's Theorem; Simple Group; $PSL(2,11)$

660 阶单群同构于 $PSL(2,11)$ 的初等群论证明*

周 峰[1]，徐 涛[2]，刘合国[1]

[1]湖北大学数学与计算机科学学院，武汉
[2]河北工程大学理学院，邯郸
Email: thoufeng@163.com, gtxutao@163.com, ghliu@hubu.edu.cn

收稿日期：2013 年 5 月 29 日；修回日期：2013 年 6 月 14 日；录用日期：2013 年 6 月 21 日

摘 要：本文仅用 Sylow 定理证明了 660 阶单群一定同构于 $PSL(2,11)$。

关键词：Sylow 定理；单群；$PSL(2,11)$

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，对阶为 n 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 $PSL(2,5)$、168 阶单群 $PSL(2,7)$、360 阶单群 $PSL(2,9)$、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 $PSL(2,5)$，见文献[1]和文献[2]。在文献[1]和文献[2]中，Smith 和 Huppert 分别用群论的不同方法证明了 168 阶单群同构于 $PSL(2,7)$。在文献[3]中，Isaacs 用特征标的理论证明了 360 阶单群同构于 $A_6\cong PSL(2,9)$，对这个看似简单的结果至今还没有见到纯粹的群论证明。值得指出的是，在文献[4]第八章的练习 8.12 中，Rotman 希望运用初等群论证明 360 阶单群同构于 A_6，但他给出的提示“360 阶单群只有 6 个 Sylow 5-子群”是错误的，因为 360 阶单群的 Sylow 5-子群的个数一定是 36。在本文中，我们借用文献[2]的思想，利用初等群论的方法证明了下面的结果。

*资助项目：湖北省高层次人才工程基金(070-016533)。

2. 主要定理及证明

定理：660 阶单群同构于 $PSL(2,11)$。

证明：设 G 是 660 阶单群，此时 $|G| = 660 = 2^2\times3\times5\times11$。首先证明 G 的 Sylow 11-子群的个数 $n_{11}(G)=12$，Sylow 5-子群的个数 $n_5(G)=66$。设 P 是 G 的 Sylow 11-子群，由 Sylow 定理知 $n_{11}(G)\equiv1(\bmod 11)$ 和 $n_{11}(G)=|G:N_G(P)|$，因此 $n_{11}(G)=1$ 或 12。注意到 G 是单群，于是 $n_{11}(G)=12$，进而 $|N_G(P)|=55=5\times11$。下证 $N_G(P)$ 包含 11 个 Sylow 5-子群，根据 Sylow 定理得到 $n_5(N_G(P))=1$ 或 11。若 $N_G(P)$ 只有 1 个 Sylow 5-子群 Q，则 $Q\lhd N_G(P)$，从而 $N_G(P)\subseteq N_G(Q)$，即有 $|G:N_G(Q)|$ 整除 $|G:N_G(P)|=12$，因为 $n_5(G)\equiv1(\bmod 5)$，所以 $n_5(G)\neq12$，即 $|G:N_G(Q)|\le6$，由此得到 $|G|$ 整除 $6!$，矛盾。因此 $N_G(P)$ 包含 11 个 Sylow 5-子群。根据 Sylow 定理得到 G 的 Sylow 5-子群的个数 $n_5(G)=1,6,11$ 或 66。由 G 是单群可以得到 $n_5(G)\neq1$ 或 6，若 $n_5(G)=11$，则 $N_G(P)$ 包含 G 的全部 Sylow 5-子群，而 $N_G(P)$ 可由这些 Sylow 5-子群生成，这将有 $N_G(P)\lhd G$，矛盾于 G 是单群，所以 $n_5(G)=66$。

考虑 G 在 $Syl_{11}(G)$ 上的共轭作用。由于 $n_{11}(G)=12$，可设

$$Syl_{11}(G)=\{P=P_\infty,P_0,P_1,\cdots,P_{10}\}$$

并用 $\{\infty,GF(11)\}$ 表示被置换的数码集合。设 $P=\langle u\rangle$，则 $u\in N_G(P_\infty)$，所以 u 保持 P_∞ 不动。因为 $u\notin N_G(P_i)\ (0\le i\le10)$，所以 u 变动了 $GF(11)$ 的每个元，因为 u 是 G 的一个 11 阶元，适当调整数码的排列顺序，u 共轭作用在 $Syl_{11}(G)$ 上引起的置换总可以写成 $(\infty)(0,1,2,\cdots,10)$ 的形式。显然 u 对应的映射为 $x\mapsto x+1$，其中 $x\in\{\infty,GF(11)\}$，这是一个线性分式映射。

设 $N_G(P)=\langle u,n\rangle$，其中 u 是一个 11 阶元，n 是一个 5 阶元。由 $n\in N_G(P)$ 得到 n 保持 P_∞ 不动。因为 $3^5\equiv1(\bmod 11)$，所以对所有的 $x\in GF(11)$，n 对应的映射为 $x\mapsto3x$，这是一个线性分式映射。

设 $N=\langle n\rangle$ 是 G 的一个 Sylow 5-子群，记 $H:=N_G(N)$，则 $|G:H|=n_5(G)=66$，从而 $|H|=10=2\times5$，于是 H 有一个 2 阶元 t。由于 $N\lhd H$，t 共轭作用在 N 上，诱导了 N 的一个自同构，注意到 t 为 2 阶元，因此 $n^t=n$ 或 $n^t=n^{-1}$。

若 $n^t=n$，则 n 与 t 可交换，nt 是一个 10 阶元，即 H 含有 10 阶元，此时 H 是循环群，所以 G 的所有 Sylow 5-子群 $N_i\ (1\le i\le66)$ 的正规化子 H_i 都是循环群，且 $H_i\neq H_j$ 当且仅当 $N_i\neq N_j\ (1\le i,j\le66)$。$H_i$ 含有 $\varphi(10)=4$ (φ 为欧拉函数)个 10 阶元，而 G 含有 66 个 Sylow 5-子群，因此所有正规化子共含有 $4\times66=264$ 个 10 阶元。

根据 Sylow 定理可以得到 G 的 Sylow 3-子群的个数 $n_3(G)=1,4,10,22,55$ 或 220。注意到 G 是单群，因此 $n_3(G)\neq1$ 或 4。若 $n_3(G)\ge10$，则 G 至少有 $2\times10=20$ 个 3 阶元。因为 $n_{11}(G)=12$，所以 G 有 10×12=120 个 11 阶元，又 $n_5(G)=66$，故 G 有 $4\times66=264$ 个 5 阶元。综上我们得到 G 中 10 阶元、3 阶元、11 阶元和 5 阶元的总个数至少有 $264+20+120+264=668$ 个，而 $668>660=|G|$，矛盾。因此 $n^t=n^{-1}$。

下证 t 在 $\{\infty,GF(11)\}$ 上引起的置换为

$$(0,\infty)(1,1^t)(3,3^{-1}1^t)(9,9^{-1}1^t)(5,5^{-1}1^t)(4,4^{-1}1^t)。$$

因为 G 在 $\{\infty,GF(11)\}$ 上传递，任意一个点的稳定子群阶为 55，t 为 2 阶元，所以 t 没有不动点，因此 t 对换 n 的不动点 0 和 ∞。由 $n^t=n^{-1}$ 和 $x^n=3x$ 可得 $(3x)^t=x^{nt}=x^{tn^{-1}}$，又 $x^{n^{-1}}=3^{-1}x$，故 $x^{tn^{-1}}=3^{-1}x^t$，从而 $(3x)^t=3^{-1}x^t$。在 $(3x)^t=3^{-1}x^t$ 中分别取 $x=1,3,3^2,3^3$，我们可得置换

$$(0,\infty)(1,1^t)(3,3^{-1}1^t)(9,9^{-1}1^t)(5,5^{-1}1^t)(4,4^{-1}1^t),$$

显然 t 对应的映射为 $x\mapsto x^{-1}1^t$，其中 $x\in\{\infty,GF(11)\}$，这是一个线性分式映射。

综上所述，我们找到了 G 里的 3 个元素 u，n，t 分别对应线性分式映射 $x\mapsto x+1$，$x\mapsto3x$，$x\mapsto x^{-1}1^t$，

其中 $x \in \{\infty, GF(11)\}$。容易验证 $\det u = 1$ 和 $\det n = 3$，而 $GF(11)$ 中的平方剩余为 1，3，4，5，9，所以 $\det u$ 和 $\det n$ 是 $GF(11)$ 中的平方剩余。下证 1^t 不是 $GF(11)$ 中的平方剩余。由于 t 在 $\{\infty, GF(11)\}$ 上引起的置换为

$$(0,\infty)(1,1^t)(3,3^{-1}1^t)(9,9^{-1}1^t)(5,5^{-1}1^t)(4,4^{-1}1^t),$$

t 没有不动点，故

$$1 \neq 1^t,\ 3 \neq 3^{-1}1^t,\ 9 \neq 9^{-1}1^t,\ 5 \neq 5^{-1}1^t,\ 4 \neq 4^{-1}1^t 。$$

进而

$$1 \neq 1^t,\ 1^t \neq 9,\ 1^t \neq 4,\ 1^t \neq 3,\ 1^t \neq 5 。$$

这表明 1^t 不是 $GF(11)$ 中的平方剩余。又 -1 不是 $GF(11)$ 中的平方剩余，于是根据两个非平方剩余的乘积是平方剩余，得到 $\det t = -1^t$ 是 $GF(11)$ 中的平方剩余。因

$$PSL(2,11) = \left\{ \alpha : x \mapsto \frac{ax+b}{cx+d} \mid a,b,c,d \in GF(11), ad-bc\text{是}GF(11)^*\text{中的平方数} \right\},$$

容易看到 u，n，t 对应的线性分式映射属于 $PSL(2,11)$。

令 $A = \langle u,n,t \rangle$，其中 u，n，t 分别是 11 阶元，5 阶元，2 阶元。因为 $2 \times 5 \times 11 = 110$ 整除 $|A|$，所以 $|G:A| \leq 6$，注意到 G 是单群，于是 $G = A$。故 G 同构于 $PSL(2,11)$ 的一个子群，而 $|G| = |PSL(2,11)|$，因此 $G \cong PSL(2,11)$。

参考文献 (References)

[1] G. Smith, O. Tabachnikova. Topics in group theory. Berlin: Springer-Verlag, 2000.
[2] B. Huppert. Enliche gruppen I. Berlin, Heidelberg, New York: Springer-Verlag, 1967.
[3] I. M. Isaacs. Character theory of finite groups. New York: Academic Press, 1976.
[4] J. Rotman. An introduction to the theory of groups. Berlin: Springer-Verlag, 1994.
[5] I. M. Isaacs. Finite group theory. Providence: American Mathematical Society, 2008.

