ON NON-HURWITZ GROUPS AND NON-CONGRUENCE SUBGROUPS OF THE MODULAR GROUP

by JEFFREY COHEN

(Received 19 April, 1979; revised 10 December, 1979)

In this note homomorphisms of $(2, 3, n) = \langle x, y : x^2 = y^3 = (xy)^n = 1\rangle$ into $\mathrm{PSL}_3(q)$ are considered. Of particular interest is $(2, 3, 7)$ whose finite factors are referred to as Hurwitz groups. It is known (see [**3**]) that for certain q, $\mathrm{PSL}_2(q)$ is a Hurwitz group, so that one might suppose that $\mathrm{PSL}_3(q)$ is a natural place to search for new Hurwitz groups. This intuition turns out to be ill-founded, for as we shall see all Hurwitz subgroups of $\mathrm{PSL}_3(q)$ have already been discovered in [**3**].

If n is allowed to assume the value ∞, a well-known result asserts that $\mathrm{PSL}_2(\mathbb{Z})$, the modular group, is obtained. Letting G_n denote the principal congruence subgroup at level n, it is almost obvious that the only simple non-abelian composition factors of $\mathrm{PSL}_2(\mathbb{Z})/G_n$ are $\mathrm{PSL}_2(p)$ for p a prime divisor of n. Thus, any maximal normal subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ with simple non-abelian factor not isomorphic to some $\mathrm{PSL}_2(p)$ must be a non-congruence group. That not all non-congruence groups arise in this way was established in [**5**]. We shall find non-congruence subgroups of the modular group by showing that $\mathrm{PSL}_3(q)$ and $\mathrm{PSU}_3(q^2)$ are with several exceptions factors of $\mathrm{PSL}_2(\mathbb{Z})$. The $\mathrm{PSL}_3(q)$ result is due to Garbe but it emerges naturally in this paper.

1. Hurwitz Subgroups of $\mathrm{PSL}_3(q)$. We recall the standard imbedding $\mathrm{PGL}_2(\bar{F}_p) \xrightarrow{\phi} \mathrm{PSL}_3(\bar{F}_p)$,

$$\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right\} \to \left\{(ad-bc)^{-3}\begin{bmatrix} a^2 & 2ab & b^2 \\ ac & ad+bc & bd \\ c^2 & 2cd & d^2 \end{bmatrix}\right\},$$

where $\{A\}$ denotes the coset of A.

THEOREM 1. *Let $\bar{F}_p$ denote the algebraic closure of* $\mathrm{GF}(p)$ *and suppose G is a Hurwitz subgroup of* $\mathrm{PSL}_3(\bar{F}_p)$. *Then either*

(i) $G \simeq \mathrm{PSL}_2(7)$

or

(ii) $G \simeq \begin{cases} \mathrm{PSL}_2(p) & \text{if } p \equiv \pm 1 (\mathrm{mod}\ 7), \\ \mathrm{PSL}_2(p^3) & \text{otherwise.} \end{cases}$

Proof. Suppose $A, B \in \mathrm{PSL}_3(\bar{F}_p)$ and that

$$\begin{cases} A^7 = B^3 = (AB)^2 = I & \text{if} \quad p \neq 7, \\ A^3 = B^7 = (AB)^2 = I & \text{if} \quad p = 7. \end{cases}$$

By varying the choice of coset representatives one may assume without loss of generality that the matrices representing the elements of orders 2 and 7 have the same orders. We shall show that the same is true of the matrix representing the element of order 3. In characteristic 3 this is an immediate consequence of the fact that there exist no non-trivial cube roots of unity. If the characteristic $p \neq 3$, then any matrix representative M of $\{A\}$ or $\{B\}$ of order 9 is similar to a diagonal matrix D of unit determinant with ninth roots of unity on the diagonal. It is immediate that D has only two distinct field elements on the diagonal, one of which is the fourth power of the other. Thus, M has a two-dimensional eigenspace associated with some ninth root of unity. The matrix representative N of order 2 also has such a subspace since N is similar to

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix} \text{ if } p \neq 2, \qquad \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{ if } p = 2. \tag{1}$$

(This is established by Jordan form considerations.) It is now evident that M and N have a common eigenvector v so that $(MN)^{18}v = v$ which entails that 18 divides 7. Thus, M cannot exist. Suppose $|\omega| = n$, $\omega \in \mathrm{GF}(q)$ where

$$n = \begin{cases} 7 & \text{if } \quad p \neq 7, \\ 3 & \text{if } \quad p = 7, \end{cases} \tag{2}$$

Then after a similarity transformation one can assume that

$$A = \begin{bmatrix} \omega^{-1} & 0 & 0 \\ 0 & \omega^{-i} & 0 \\ 0 & 0 & \omega^{-j} \end{bmatrix} \tag{3}$$

where (I) $i = 2$, $j = 4$ and $p \neq 7$, or (II) $i = -1$, $j = 0$. From (1) it follows that $AB + I$ is of rank one so that

$$AB = \begin{bmatrix} tx-1 & ux & vx \\ ty & uy-1 & vy \\ tz & uz & vz-1 \end{bmatrix}. \tag{4}$$

We therefore have

$$B = \begin{bmatrix} \omega(tx-1) & \omega ux & \omega vx \\ \omega^i ty & \omega^i(uy-1) & \omega^i vy \\ \omega^j tz & \omega^j uz & \omega^j(vz-1) \end{bmatrix}. \tag{5}$$

The characteristic polynomial of B is $(x-1)^3$ or $x^3 - 1$ according to whether p is equal to 7 or not, so that computing it directly from B yields:

$$\left.\begin{aligned} \omega tx + \omega^i uy + \omega^j vz &= \omega + \omega^i + \omega^j(+3), \\ (\omega^{i+1} + \omega^{j+1})tx + (\omega^{i+1} + \omega^{i+j})uy + (\omega^{j+1} + \omega^{i+j})vz &= \omega^{i+1} + \omega^{j+1} + \omega^{i+j}(+3), \\ tx + uy + vz &= 2. \end{aligned}\right\} \tag{6}$$

In Case (I) let $\alpha=\omega+\omega^2+\omega^4$, so that the determinant Δ of the coefficient matrix is $2\alpha+1$ which is non-zero since $\alpha^2+\alpha+2=0$. In Case (II)

$$\Delta=2(\omega-\omega^{-1})+(\omega^{-2}-\omega^2).$$

If $\Delta=0$, then $\omega+\omega^{-1}=2$, which is incompatible with $|\omega|=7$. If $p\neq 7$, by Cramer's rule we have

$$\begin{aligned}\Delta tx&=\omega^2(\omega^{i+j-2}+1)(\omega^i-\omega^j),\\ \Delta uy&=\omega^{2i+1}(\omega^{j-1}-1)(\omega^{j+1-2i}+1),\\ \Delta vz&=\omega^{2j+1}(1-\omega^{i-1})(\omega^{i+1-2j}+1).\end{aligned}$$

Therefore, tx and uy never vanish and $vz=0$ is possible only in Case (3B) with $p=2$. In this situation if $v=z=0$, then $\langle A,B\rangle$ is isomorphic to a subgroup of $SL_2(\bar{F}_2)$, so that by [**3**], $\langle A,B\rangle\simeq PSL_2(8)$. (If $p=7$ one checks that $txuyvz\neq 0$ similarly.) If $p=2$, by applying the automorphism which maps each matrix into the transpose of its inverse (if necessary) one can assume that $z\neq 0$. Hence the one-dimensional vector space $\begin{pmatrix}x\\y\\z\end{pmatrix}$ determines B uniquely. Let B' denote the result of priming all unknowns in B. To show that $\langle A,B\rangle$ is $GL_3(\bar{F}_q)$ conjugate to $\langle A,B'\rangle$, it suffices to produce C that centralizes A and is such that the range of $CABC^{-1}$ is spanned by $\begin{pmatrix}x'\\y'\\z'\end{pmatrix}$. This is effected by taking

$$C=\begin{bmatrix}x'x^{-1}&0&0\\0&y'y^{-1}&0\\0&0&z'z^{-1}\end{bmatrix}.$$

We have shown that A determines the isomorphism type of $\langle A,B\rangle$ independent of t,u,v,x,y,z. Now by [**3**], the matrix

$$\begin{bmatrix}\omega&0\\0&\omega^{-1}\end{bmatrix}$$

can be taken as part of a $(2,3,7)$ triple, so that an application of ϕ yields that $\langle A,B\rangle$ is isomorphic to a subgroup of $PSL_2(\bar{F}_q)$. In [**3**] it is shown that any such Hurwitz group is given by (ii) in Case II. To see that $PSL_2(7)$ is generated in Case I, use the following presentation found in [**2**]:

$$PSL_2(7)=\langle x,y\colon x^2=y^3=(xy)^7=[x,y]^4=1\rangle.$$

It is worth noting that in characteristic 0, $\langle A,B\rangle$ is isomorphic to $(2,3,7)$ or $PSL_2(7)$.

COROLLARY 1. *$PSL_3(q)$ is a Hurwitz group if and only if $q=2$.*

2. $\mathrm{PSL}_3(q)$ **and** $\mathrm{PSU}_3(q^2)$ **as Modular Group Factors.** In this section $\mathrm{GF}(q)$ is the field of $p^r = q$ elements and $\mathrm{GF}(q) = \mathrm{GF}(p)(\alpha, \beta)$ with p a prime number. Let

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \qquad B = \begin{bmatrix} 1 & \beta & \alpha \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix},$$

so that $A^3 = B^2 = I$ and the projective order n of AB is determined by its characteristic polynomial given by

$$f(x) = x^3 - \alpha x^2 + \beta x - 1.$$

If r is even we denote $x^{\sqrt{q}}$ by $\bar{x}$ and also denote the homomorphism induced on $\mathrm{GL}_3(q)$ by "bar". Finally, round brackets shall denote vectors and square brackets projective points.

Proposition 1. *Suppose $(x-\sigma) \nmid f(x)$ where $\sigma^6 = 1$. Then $\langle A, B\rangle$ fixes no projective point. Dually $\langle A, B\rangle$ fixes no projective line.*

Proof. Negate. The fixed points of B are

$$x = \begin{bmatrix} \beta \\ -2 \\ 0 \end{bmatrix}, \qquad y = \begin{bmatrix} \alpha \\ 0 \\ -2 \end{bmatrix}, \qquad z = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \quad \text{if } p \neq 2,$$

$$x = \begin{bmatrix} \alpha \\ \beta \\ 0 \end{bmatrix}, \qquad z = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \quad \text{if } p = 2.$$

Clearly $Az \neq z$, so that there exist $t, u \in \mathrm{GF}(q)$ with

$$A(tx + uy) = tx + uy.$$

Since the eigenvalues of A are (not necessarily primitive) cube roots of unity this entails that if $p \neq 2$,

$$\begin{pmatrix} -2t \\ -2u \\ t\beta + u\alpha \end{pmatrix} = (\sqrt[3]{1})^i \begin{pmatrix} t\beta + u \\ -2t \\ -2u \end{pmatrix} \qquad (i \in \{0, 1, 2\}).$$

Hence if $p \neq 2$, $\sqrt[3]{1}\beta + (\sqrt[3]{1})^2\alpha = -2$. The same result is obtained when $p = 2$. Thus

$$f(x) = (x + \sqrt[3]{1})(x^2 - (\alpha + \sqrt[3]{1})x - (\sqrt[3]{1})^2),$$

contrary to hypothesis. The dual proposition is proven similarly by using the fixed lines of B:

$$\hat{x} = [2, \beta, \alpha], \; \hat{y} = [0, 1, 0], \; \hat{z} = [0, 0, 1].$$

If $\hat{x}A=\hat{x}$, then $\beta=\sqrt[3]{1}\alpha$, so that

$$f(x)=(x-\sqrt[3]{1})(x^2+(\sqrt[3]{1}-\alpha)x+(\sqrt[3]{1})^2),$$

contrary to assumption. Since $[0,t,u]A\neq[u,0,t]$ we aré done.

Proposition 2. *Let r be even. Then $\langle A,B\rangle$ fixes a non-zero unitary form if and only if $\bar{\alpha}=\beta$. In this case, the form is non-degenerate if and only if*

$$\alpha^3+\bar{\alpha}^3-6\alpha\bar{\alpha}+8\neq 0.$$

In particular, this occurs if $\alpha^{q+1}=1$ and $|\alpha|\nmid 6$.

Proof. Let H denote a unitary form, so that

$$H=\begin{bmatrix} a & b & c\\ \bar{b} & d & e\\ \bar{c} & \bar{e} & f\end{bmatrix}.$$

From $\bar{A}'HA=H$ it follows that $a=d=f$ and $b=\bar{c}=e$. Now

$$0=\bar{B}'HB-H=\begin{bmatrix} 0 & \beta a-2b & \alpha a-2\bar{b}\\ * & * & \alpha\bar{\beta}a-\bar{\beta}\bar{b}-\alpha\bar{b}\\ * & * & *\end{bmatrix}$$

so that $\bar{\alpha}=\beta$. One easily checks that if $\bar{\alpha}=\beta$, then the form H is fixed:

$$H=\begin{bmatrix} 2 & \bar{\alpha} & \alpha\\ \alpha & 2 & \bar{\alpha}\\ \bar{\alpha} & \alpha & 2\end{bmatrix}.$$

Taking the determinant of H establishes the remainder of this proposition.

Proposition 3. *Suppose that $\langle A,B\rangle$ is isomorphic to a subgroup of $\mathrm{PSL}_2(q)$. If $p=2$, further assume that $\langle A,B\rangle$ fixes no projective point or line. Then $(x-\sqrt[3]{1})\mid f(x)$.*

Proof. By [**1**] and [**4**], any subgroup of $\mathrm{PSL}_3(q)$ isomorphic to $\mathrm{PSL}_2(q)$ either fixes a projective point or line or fixes a conic. (The fixing of projective objects occurs only when $p=2$.) Thus one can map $\langle A,B\rangle$ by an automorphism (induced by conjugating by an element of $\mathrm{GL}_3(q)$) into the image of ϕ. Without loss of generality, $\phi^{-1}(AB)$ is upper triangular, i.e.

$$\phi^{-1}(AB)=\begin{bmatrix}\omega & *\\ 0 & \omega^{-1}\end{bmatrix}.$$

Applying ϕ gives the result.

Theorem 2. *Suppose $\mathrm{PSL}_3(p^s)$ has no element of order n for $s<r$. Further suppose $8<n\equiv\pm1 \pmod 6$ and $(x-\sigma)\nmid f(x)$ where $\sigma^6=1$. Then $\langle A,B\rangle$ is isomorphic to $\mathrm{PSL}_3(q)$ or $\mathrm{PSU}_3(\sqrt{q})$.*

Proof. Let $G = \langle A, B\rangle$. We shall refer to Mitchell's list in **[3]** of the subgroups of $\mathrm{PSL}_3(q)$ for q odd. The even characteristic case is handled analogously using **[1]**. Since n is not divisible by 2 or 3, G has trivial abelianization. Thus G is not of Types 3, 4, 7, 9 or 10. By Proposition 1, G is not of Types 1 or 2. Proposition 3 and the fact that G has no abelianization yield that G is not of type 5. Since $n > 8$, groups of types 11–14 are excluded. Finally since $\mathrm{PSL}_3(p^s)$ has no element of order n, G is not isomorphic to this type 6 group.

COROLLARY 2 (Garbe). *$\mathrm{PSL}_3(q)$ is a $(2, 3, n)$-group where*

$$n = \frac{q^2+q+1}{(q^2+q+1, 3)} \quad \textit{and} \quad q \neq 4.$$

Proof. Choose an element $\omega \in \mathrm{GF}(q^3)$ of order q^2+q+1 and let

$$f(x) = (x-\omega)(x-\omega^q)(x-\omega^{q^2}).$$

$\langle A, B\rangle$ cannot be the unitary group since this group has no element of order n.

THEOREM 3. *Suppose $\sqrt{q} \notin \{2, 5, 8, 17\}$ and that*

$$n = \begin{cases} \dfrac{\sqrt{q}+1}{(\sqrt{q}+1, 3)} & \textit{if } \sqrt{q} \equiv 1 \pmod 4, \\[2ex] \dfrac{2(\sqrt{q}+1)}{(\sqrt{q}+1, 3)} & \textit{otherwise.} \end{cases}$$

Then $\mathrm{PSU}_3(q)$ is a $(2, 3, n)$-group.

Proof. Choose $\alpha \in \mathrm{GF}(q)$ with $|\alpha| = \sqrt{q}+1$ and let

$$f(x) = (x-\alpha)(x^2+\bar{\alpha}).$$

Since AB is a nonderogatory matrix, it follows that $|\{AB\}| = n$. By Proposition 2, $\langle\{A\}, \{B\}\rangle$ fixes a non-degenerate unitary form. As above we shall use Mitchell's (and Hartley's) lists. Since $n \geq 8$ (with strict inequality in characteristic 5), groups of types 8–12 are excluded as possibilities for $\langle\{A\}, \{B\}\rangle$. Types 1 and 2 are excluded by Proposition 1, while type 5 groups are excluded by Proposition 3. Since groups of types 6–8 contain no element of order n, we are reduced to showing that $\langle\{A\}, \{B\}\rangle$ fixes no triangle. If $\langle\{A\}, \{B\}\rangle$ does fix some triangle, then its vertices are fixed points of $(AB)^2$. These are

$$W_1 = \begin{bmatrix} 1 \\ -\alpha \\ \alpha^2 \end{bmatrix}, \quad W_2 = \begin{bmatrix} 1 \\ -\sqrt{-\bar{\alpha}} \\ -\bar{\alpha} \end{bmatrix}, \quad W_3 = \begin{bmatrix} 1 \\ \sqrt{-\bar{\alpha}} \\ -\bar{\alpha} \end{bmatrix}.$$

https://doi.org/10.1017/S0017089500004419 Published online by Cambridge University Press

If

$$\begin{bmatrix} -\alpha \\ \alpha^2 \\ 1 \end{bmatrix} = AW_1 = W_2 = \begin{bmatrix} 1 \\ -\sqrt{-\bar{\alpha}} \\ -\bar{\alpha} \end{bmatrix},$$

then $-\alpha^2\bar{\alpha} = -\sqrt{-\bar{\alpha}}$, so that $\alpha^{2\sqrt{q}+4} = -\alpha^{\sqrt{q}}$ which yields that

$$\alpha^3 = \alpha^{2\sqrt{q}+2+3} = -\alpha^{\sqrt{q}+1} = -1$$

which is incompatible with $|\alpha| = n$. Similarly A does not map W_1 to W.

If $\sqrt{q} = 5$, let $\alpha = -\sqrt{-2} - 1$ so that $|AB| = 8$. Then by the preceding argument $\langle\{A\}, \{B\}\rangle$ is either $\mathrm{PSU}_3(q)$ or is isomorphic to M_{10}. A computation yields that $10\,|\{(AB)^2A^{-1}B^{-1}\}| = 10$ and this implies that $\mathrm{PSU}_3(q)$ is the group generated, since M_{10} has no element of order 10. Similarly using the following data one checks that $\mathrm{PSU}_3(q)$ is a modular group factor:

$\sqrt{q}$	α satisfies	$\lvert\{AB\}\rvert$
8	$\alpha^6 + \alpha + 1 = 0$	21
17	$\alpha^2 - 5 = 0$	91

Now $\mathrm{PSU}_3(4)$ has a normal Sylow 3-subgroup, so that if $x, y \in \mathrm{PSU}_3(4)$ satisfy $x^2 = y^3 = 1$, then in the factor group $\bar{x}^2 = \bar{y} = 1$. But the factor has order 8, so that $\langle x, y\rangle$ is a proper subgroup of $\mathrm{PSU}_3(4)$. Summarizing we obtain

COROLLARY 3. *$\mathrm{PSU}_3(q)$ is a factor of the modular group if and only if $\sqrt{q} \neq 2$.*

ACKNOWLEDGEMENT. The author would like to thank Dr. M. Marsden for performing the final two computations in this work. Thanks are also due to the referee for his scepticism and helpful suggestions.

REFERENCES

1. W. W. Hartley, Ternary collineation groups, *Ann. of Math.* **27** (1925), 140–158.

2. John Leech, Generators for certain normal subgroups of (2, 3, 7), *Proc. Cambridge Philos. Soc.* **61** (1965), 321–332.

3. A. M. Macbeath, Generators of the linear fractional groups, *Proceedings of a Symposium of Pure Mathematics in Number Theory*, Vol. XII, Houston (1967), 14–32.

4. H. H. Mitchell, Ternary linear groups, *Trans. Amer. Math. Soc.* **12** (1911), 207–242.

5. Morris Newman, Maximal normal subgroups of the modular group, *Proc. Amer. Math. Soc.* **19** (1968), 1138–44.

UNIVERSITY OF PITTSBURGH
PITTSBURGH
PENNSYLVANIA 15260