Can. J. Math., Vol. XXIX, No. 3, 1977, pp. 541–551

FINITE QUOTIENTS OF THE AUTOMORPHISM GROUP OF A FREE GROUP

ROBERT GILMAN

1. Introduction. Let G and F be groups. A *G-defining subgroup of F* is a normal subgroup N of F such that F/N is isomorphic to G. The automorphism group Aut (F) acts on the set of G-defining subgroups of F. If G is finite and F is finitely generated, one obtains a finite permutation representation of Out (F), the outer automorphism group of F. We study these representations in the case that F is a free group. We denote by F_n a free group on n free generators $x_1, \ldots, x_n$.

THEOREM 1. *Fix $n \geqq 3$. For any prime $p \geqq 5$,* Out (F_n) *acts on the $PSL(2, p)$-defining subgroups of F_n as the alternating or symmetric group, and both cases occur for infinitely many primes.*

COROLLARY 1. *If $n \geqq 3$,* Out (F_n) *is residually finite alternating and residually finite symmetric.*

The meaning of Corollary 1 is that for any $\alpha \in$ Out (F_n) there is a homomorphism ρ from Out (F_n) onto a finite alternating group such that $\rho(\alpha) \neq 1$. E. Grossman proved that for all n, Out (F_n) is residually finite [**9**]. Theorem 1 and Corollary 1 are proved in Section 5. The conclusion of Theorem 1 does not hold for $n = 2$. Out (F_2) acts intransitively on the PSL (2,5)-defining subgroups of F_2 [**12**, § 10; **14**, Proposition 4], and on the PSL (2,7)-defining subgroups of F_2 [**15**, Theorem 1]. We have the following partial extensions of Theorem 1.

THEOREM 2. *If $n \geqq 4$ and G is a finite nonabelian simple group generated by $n - 2$ elements,* Out (F_n) *acts as the alternating or symmetric group on at least one of its orbits on the G-defining subgroups of F_n.*

THEOREM 3. *If G is a finite group of order $g > 1$, and $n \geqq 2 \log_2 (g)$,* Out (F_n) *is transitive on the G-defining subgroups of F_n.*

In connection with Theorem 2 we note that all currently known simple groups seem to be generated by two elements [**8**, § 78]. If G is a finite abelian simple group of order p, the action of Out (F_n) on the G-defining subgroups of F_n is well-known.

A much sharper form of Theorem 3 holds if G is solvable. M. Dunwoody has shown that in this case one need only assume that n is greater than the size of the smallest set of generators of G [**6**]. In [**5**, Theorem 1] he shows that this

Received June 14, 1976 and in revised form, October 8, 1976.

https://doi.org/10.4153/CJM-1977-056-3 Published online by Cambridge University Press

bound is sharp. His discussion in [**6**] of the action of Out (F_3) on the A_5-defining subgroups of F_3 motivated the present work. Theorem 3 is a corollary of a result of F. Cappel, a student of J. Neubuser [**2**].

2. G-vectors. For any group G a *G-vector* of length n is an n-tuple $\boldsymbol{a} = (a_1, \ldots, a_n)$, $a_i \in G$, $1 \leqq i \leqq n$. A *generating G-vector* is one whose entries generate G. G-vectors were introduced in [**12**, Kap. II] in order to define an action of Aut (F_n) which is equivalent to its action on G-defining subgroups of F_n but easier to work with. If $W = x_{i_1}^{\epsilon_1} \ldots x_{i_t}^{\epsilon_t}$ is a word in $x_1, \ldots, x_n$, we define

$$W(\boldsymbol{a}) = a_{i_1}^{\epsilon_1} \ldots a_{i_t}^{\epsilon_t}.$$

Let E be the set of epimorphisms from F_n to G. The direct product Aut (G) $\times$ Aut (F_n) acts on E; for $\alpha \in$ Aut (G) and $\sigma \in$ Aut (F_n) the element (α, σ) sends $\rho \in E$ to the composite $\alpha\rho\sigma^{-1}$. Clearly the action of Aut (F_n) on the Aut (G)-orbits of E is equivalent to its action on G-defining subgroups of F_n. Let $V(G, n)$ be the set of generating G-vectors of length n. The map π sending ρ to $(\rho(x_1), \ldots, \rho(x_n))$ gives a one to one correspondence between E and $V(G, n)$ and induces an action of Aut (G) $\times$ Aut (F_n) on $V(G, n)$ by $\alpha\, \pi(\rho)\, \sigma = \pi(\alpha\, \rho\, \sigma)$.

The induced action is equivalent to the action of Aut (G) $\times$ Aut (F_n) on E whence the action of Aut (F_n) on G-defining subgroups of F_n is equivalent to its action on Aut (G)-orbits of $V(G, n)$. Let $\bar{V}(G, n)$ be the set of Aut (G)-orbits of $V(G, n)$. Write $\boldsymbol{a} \sim \boldsymbol{b}$ if $\boldsymbol{a}$ and $\boldsymbol{b}$ are in the same Aut (F_n)-orbit of $\bar{V}(G, n)$. If $\sigma(x_i) = W_i$, $1 \leqq i \leqq n$ for words W_i in x_j, $1 \leqq j \leqq n$, we have

$$\alpha\, \boldsymbol{a}\, \sigma = (\alpha(W_1(\boldsymbol{a})), \ldots, \alpha(W_n(\boldsymbol{a}))).$$

The elementary automorphisms of F_n are

$$P(i, k)\colon x_i \rightarrow x_k,\ x_k \rightarrow x_i$$
$$\sigma(i)\colon x_i \rightarrow x_i^{-1}$$
$$L(i, k)\colon x_i \rightarrow x_k x_i$$
$$R(i, k)\colon x_i \rightarrow x_i x_k$$

where $1 \leqq i, k, \leqq n$, $i \neq k$, and unmentioned generators are left fixed [**11**, Sec. 3.5]. The effect of these automorphisms on $\boldsymbol{a} \in V(G, n)$ is to interchange any two entries, invert any entry, or multiply one entry by a different one.

The following lemma is used in the proof of Theorem 2 and is the only place we use the simplicity of G in the proof of that theorem.

LEMMA 1. *Let G be a finite nonabelian simple group. Suppose $\boldsymbol{a} = (a_1, \ldots, a_n) \in V(G, n)$ and $G = \langle a_i | i \neq j\rangle$ for some j, $1 \leqq j \leqq n$. For any $c \in G$, there is a word*

$$W(x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n)$$

such that for

$$\beta = W(R(j, 1), \ldots, R(j, j-1), R(j, j+1), \ldots, R(j, n))$$

we have

$$\boldsymbol{a}\beta = (a_1, \ldots, a_{j-1}, a_j c, a_{j+1}, \ldots, a_n)$$

and for any $\boldsymbol{b} = (b_1, \ldots, b_n) \in V(G, n)$ *either* $\boldsymbol{b}\beta = \boldsymbol{b}$ *or there exists* $\alpha \in \mathrm{Aut}(G)$ *such that* $b_i = \alpha(a_i)$, $1 \leqq i \leqq n, i \neq j$.

Proof. For any vector $\boldsymbol{v}$ of length n, let $\boldsymbol{v}'$ be the vector of length $n-1$ obtained by omitting the jth entry of $\boldsymbol{v}$. Let $\boldsymbol{x} = (x_1, \ldots, x_n) \in V(F_n, n)$; the entries of $\boldsymbol{x}'$ generate a free group $F \subseteq F_n$.

Let N be the kernel of the homomorphism $\rho: F \to G$, $\rho(x_i) = a_i$, $1 \leqq i \leqq n$, $i \neq j$; and let M be the intersection of the kernels of all homomorphisms $\mu: F \to G$ with kernel distinct from N. Because G is simple, $F = NM$ and we can find $W = W(\boldsymbol{x}') \in M$ such that $W(\boldsymbol{a}') = \rho(W) = c$. If we define μ by $\mu(x_i) = b_i$, then $W(\boldsymbol{b}') = \mu(W(\boldsymbol{x}')) = 1$ unless μ and ρ have the same kernel in which case $\mu = \alpha\rho$ and $b_i = \alpha(a_i)$, $1 \leqq i \leqq n$, $i \neq j$, for some $\alpha \in \mathrm{Aut}(G)$. Clearly β has the desired effect.

3. Proof of Theorem 3. Let S be a finite set of generators of G and let $\{a_1, \ldots, a_r\} \subseteq S$ be of minimum order such that $\langle a_1, \ldots, a_r \rangle = G$. If $H_i = \langle a_1, \ldots, a_i \rangle$, then H_1 has order at least 2 and the index $|H_{i+1} : H_i| \geqq 2$. Thus G has order $g \geqq 2^r$ whence $r \leqq k$ where k is the greatest integer less than or equal to $\log_2(g)$.

Now pick $a_1 \ldots a_k \in G$ so that $\langle a_1, \ldots, a_k \rangle = G$. For $n \geqq 2k$ define

$$\boldsymbol{w} = (a_1, \ldots, a_k, 1, \ldots, 1) \in V(G, n).$$

Consider any $\boldsymbol{v} \in V(G, n)$; it suffices to reduce $\boldsymbol{v}$ to $\boldsymbol{w}$ by elementary automorphisms of F_n. By the preceding paragraph k of the entries of $\boldsymbol{v}$ generate G. Permute the entries of $\boldsymbol{v}$ so that the last k entries generate G. Multiplying the first k entries by the last k, we can change $\boldsymbol{v}$ so that its first k entries are $a_1, \ldots, a_k$. Now multiplying the last $n-k$ entries by the first k, we can reduce $\boldsymbol{v}$ to $\boldsymbol{w}$.

4. Proof of Theorem 2 and part of Theorem 1. It suffices in the proof of Theorem 2 to show that $\mathrm{Aut}(F_n)$ acts as the alternating or symmetric group on some subset of $\bar{V}(G, n)$. We will show first that $\mathrm{Aut}(F_n)$ acts doubly transitively on one of its orbits and then estimate the degree and minimal degree of the action. At this point a theorem of Bochert [**1**, p. 144] gives the desired result.

For the first part of the proof, we assume only that $n \geqq 3$ and G is generated by $n-1$ elements in order to apply our argument to the proof of Theorem 1. Let $\{a_1, \ldots, a_{n-1}\}$ be a fixed set of generators for G. Let V' be the orbit of

https://doi.org/10.4153/CJM-1977-056-3 Published online by Cambridge University Press

Aut $(G) \times$ Aut (F_n) containing

$$\mathbf{v} = (a_1, \ldots, a_{n-1}, 1)$$

and let $\bar{V}'$ be the set of Aut (G)-orbits of V'.

From [**11**, Sec. 3.5] the elementary automorphisms of F_n generate Aut (F_n), and

$$N = \langle L(i, k), R(i, k) | 1 \leqq i, k \leqq n, i \neq k \rangle$$

is a normal subgroup of Aut (F_n). We claim Aut $(G) \times N$ acts transitively on V'.

Clearly $\mathbf{v}\, \sigma(n) = \mathbf{v}$, and further if i, j, n are distinct,

$$\mathbf{v}\, P(i, j) = \mathbf{v}\, R(n, i)R(i, n)^{-1}R(i, j)R(j, i)^{-1}R(j, n)R(n, j)^{-1},$$

while for $i \neq n$

$$\mathbf{v}\, P(i, n) = \mathbf{v}\, R(n, i)R(i, n)^{-1}.$$

As the transpositions $\{(i, n)\}$ generate the symmetric group on $\{1, 2, \ldots, n\}$, it follows that Aut $(F_n) = N\, C_{\mathrm{Aut}(F_n)}(\mathbf{v})$. Thus our claim is valid.

We will show that N acts doubly transitively on $\bar{V}'$. Let

$$\mathbf{w} = (b_1, \ldots, b_n)$$

be an element of V' not in the Aut (G)-orbit of $\mathbf{v}$. It suffices to show that for a fixed $e \in G$, $e \neq 1$, $\mathbf{w}$ can be reduced to

$$\mathbf{y} = (a_1, \ldots, a_{n-1}, e)$$

by applying elements of Aut (G) or elements of $C_N(\mathbf{v})$. Clearly $y \in V'$. We have $\mathbf{y} = \alpha\, \mathbf{w}\, \delta$, $\alpha \in$ Aut (G), $\delta \in N$. We may assume $\alpha = 1$. Express δ as a word in the $R(i, k)$'s and $L(i, k)$'s. The problem is that some of the $R(i, k)$'s and $L(i, k)$'s do not fix $\mathbf{v}$. Consider the $R(i, k)$'s; the $L(i, k)$'s are handled similarly. For $1 \leqq i < n$, $R(i, n)$ fixes $\mathbf{v}$, and for $1 \leqq i, k, < n$, $i \neq k$,

$$R(i, k) = R(n, k)^{-1}R(i, n)^{-1}R(n, k)R(i, n).$$

Thus we need only show that for any $\mathbf{w}$ chosen as above and i, $1 \leqq i < n$, we can find an element $\beta \in N$ such that $\mathbf{w}\, \beta = \mathbf{w}\, R(n, i)$ and β fixes $\mathbf{v}$. We can do this by Lemma 1 unless $b_i = \alpha(a_i)$, $1 \leqq i \leqq n - 1$, for some $\alpha \in$ Aut (G). Thus we are reduced to dealing with the case

(1) $\quad \mathbf{w} = (a_1, \ldots, a_{n-1}, b) \quad 1 \neq b \neq e.$

At this point we assume the hypothesis of Theorem 2. In particular $n \geqq 4$ and we may suppose $a_{n-1} = 1 = b_{n-1}$. We will reduce $\mathbf{w}$ to $\mathbf{y}$. First of all $R(n - 1, n)R(n, n - 1)^{-1}$ fixes $\mathbf{v}$ and moves $\mathbf{w}$ to

$$\mathbf{u} = \mathbf{w}P(n - 1, n) = (a_1, \ldots, a_{n-2}, b, 1)$$

By Lemma 1 we can find $\beta \in C_N(\boldsymbol{v})$ such that

$$\boldsymbol{u}\beta = (a_1, \ldots, a_{n-2}, b, e)$$

and likewise we can find $\beta' \in C_N(\boldsymbol{v})$ for which $\boldsymbol{u}\beta\beta' = \boldsymbol{y}$.

Now we estimate the degree r and minimal degree s of the action of Aut (F_n) on $\bar{V}'$. The vectors $(a_1, \ldots, a_{n-2}, e, f)e, f \in G$ lie in g^2 distinct Aut (G)-orbits of V' where g is the order of G. Thus $r \geqq g^2$.

By Lemma 1 some $\beta \in N$ fixes all elements of $V(G, n)$ except those in the Aut (G)-orbits of $(a_1, \ldots, a_{n-1}, f), f \in G$, whence $s \leqq g$. By the theorem of Bochert referred to above if Aut (F) does not act as the alternating or symmetric group,

$$s \geqq r/3 - 2\sqrt{r}/3.$$

As the righthand side is an increasing function of r for $r \geqq 1$, we have

$$g \geqq g^2/3 - 2g/3$$

whence $g \leqq 5$ which is impossible. This completes the proof of Theorem 2.

5. The proof of Theorem 1 and Corollary 1. First we show that the theorem implies the corollary. It suffices to show that if $\alpha \in$ Aut (F_n), $n \geqq 3$, and α normalizes every PSL $(2,p)$-defining subgroup of F_n for all primes $p > 3$, then α is inner. Let x be a primitive element of F_n, and let R be the normal closure of x in F_n, F_n/R is free on $n - 1$ generators. In [**13**] it is shown that for $n \geqq 2$ F_n is residually PSL $(2,p)$, p a prime > 3. Applying this result to F_n/R, we see that α must normalize R. By [**11**, Theorem 4.11] $\alpha(x)$ is conjugate in F_n to x or x^{-1}. Considering the action of α on the commutator quotient of F_n, we see that either $\alpha(x)$ is conjugate to x for every primitive element x or $\alpha(x)$ is conjugate to x^{-1} for every primitive x. In the first case α is inner by [**9**, Lemma 1]. In the second case the obvious extension of [**9**, Lemma 1] and its proof suffice to show α is inner.

The proof of Theorem 1 rests on explicit knowledge of the lattice of subgroups of PSL $(2,p)$ [**4**, Ch XII; **10**, § 3]. As PSL $(2,p)$ is generated by two elements, Theorem 2 applies to the action of Out (F_n) on PSL $(2,p)$-defining subgroups of F_n when $n \geqq 4$. We will show that the conclusion of Theorem 2 holds when $n = 3$.

Let a and b be the elements of G of order p represented by the matrices

$$(2) \quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

respectively. As $N_G(\langle a \rangle)$ is the unique maximal subgroup of G containing $\langle a \rangle$, $\langle a, b \rangle = G$. Let

$$\boldsymbol{v} = (a, b, 1), \quad \boldsymbol{y} = (a, b, ab),$$

and define V' and $\bar{V}'$ as in the proof of Theorem 2. By the reduction to (1) in the proof of Theorem 2 we need only show for

$$\boldsymbol{w} = (a, b, c) \quad 1 \neq c \neq ab$$

how to reduce $\boldsymbol{w}$ to $\boldsymbol{y}$ be elements of $C_N(v)$. If $c \notin N_G(\langle a\rangle) \cap N_G(\langle b\rangle)$, either $\langle a, c\rangle = G$ or $\langle b, c\rangle = G$. If, however $c \in N_G(\langle a\rangle) \cap N_G(\langle b\rangle)$, then c has matrix representation

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

whence $bcb^{-1} \notin N_G(\langle a\rangle)$; since $\boldsymbol{w} \sim (a, b, bcb^{-1})$, we may assume $\langle a, c\rangle = G$. By Lemma 1,

$$\boldsymbol{u} = \boldsymbol{w}\beta = (a, ab, c)$$

for some $\beta \in C_N(\boldsymbol{v})$. Since 1 is not an eigenvalue of the product of the matrices in (2), no automorphism of G moves b to ab. By Lemma 1,

$$\boldsymbol{t} = \boldsymbol{u}\,\beta' = (a, ab, ab)$$

for some $\beta' \in C_N(\boldsymbol{v})$, and another application of Lemma 1 moves $\boldsymbol{t}$ to $\boldsymbol{y}$.

We have shown that Aut (F_3) acts doubly transitively on one of its $\bar{V}(G,3)$-orbits. As in the proof of Theorem 2, the minimal degree of this action is at most g. Once we show that Aut $(G) \times$ Aut (F_3) acts transitively on $V(G, 3)$, the degree of the action will be the number of G-defining subgroups of F_3. We can then calculate this number by the method of [**9**] and show as in the proof of Theorem 2 that Aut (F_3) acts as the alternating or symmetric group on $\bar{V}'$.

We will show the required transitivity. Let

$$\boldsymbol{v} = (a, b, 1, \ldots, 1)$$

where a and b are chosen as above, and let

$$\boldsymbol{w} = (c_1, \ldots, c_n)$$

be an arbitrary group vector in $V(G, n)$. Suppose first that a proper subset of $S = \{c_1, \ldots, c_n\}$ generates G. By permuting the entries of $\boldsymbol{w}$ we may assume $G = \langle c_2, \ldots, c_n\rangle$. Multiplying the first entry by the others we may assume $c_1 = a$. Now $\langle c_1, c_j\rangle = G$ for some j, $2 \leqq j \leqq n$. We may assume $\langle c_1, c_n\rangle = G$. Now we can achieve $c_2 = b$ and then $c_3 = \ldots = c_n = 1$. Thus in this case we can move $\boldsymbol{w}$ to $\boldsymbol{v}$.

Assume $n \geqq 4$ and let $H = \langle c_1, c_2, c_3\rangle$. By the preceding paragraph we may assume that H is a proper subgroup of G. With the exception of A_5, the proper subgroups of G are all solvable and generated by 2 elements. By [**6**], we see that with the exception of $H \cong A_5$, that $\boldsymbol{u} = (c_1, c_2, c_3)$ can be moved by an element of Aut (F_3) to an H-vector with one entry equal to the identity. It follows that $\boldsymbol{w}$ can be moved to $\boldsymbol{v}$ as before. Once we have dealt with the case $n = 3$, then as $A_5 \cong PSL$ (2,5), this argument will apply to $H \cong A_5$ as well.

Now we deal with the case $n = 3$. Assume there exists an Aut $(G) \times$ Aut (F_3)-orbit, W, of $V(G, 3)$ with $\boldsymbol{v} \notin W$. We will derive a contradiction. Let

$$\boldsymbol{w} = (c, d, e)$$

be an arbitrary element of W, and let H be the subgroup of G generated by two entries of $\boldsymbol{w}$. From the discussion above we know

(i) $H \neq G$.

We claim that H is noncyclic. Suppose $H = \langle c, d\rangle$ and H is cyclic; then $H = \langle cd^i\rangle$ for some integer i and

$$\boldsymbol{w} \sim \boldsymbol{u} = (cd^i, d, e) \in w$$

which is impossible by (i) as $G = \langle cd^i, e\rangle$. Thus we have established

(ii) H is noncyclic.

Now assume that H normalizes a Sylow p-subgroup, P, of G. By (ii) and the structure of $N_G(P)$, $P \subseteq H$ and H/P is cyclic. We assume again that $H = \langle c, d\rangle$; H is a Frobenius group. For some i, $f = cd^i$ generates a complement to P in H and for some j, $g = df^j$ generates P. We have

$$\boldsymbol{w} \sim (f, d, e) \sim \boldsymbol{u} = (f, g, e) \in W.$$

$N_G(P)$ is the unique maximal subgroup of G containing P, and it follows from $G = \langle f, g, e\rangle$ that $e \notin N_G(P)$ and $G = \langle g, e\rangle$ contrary to (i). Hence

(iii) H does not normalize a Sylow p-subgroup of G.

By (i)-(iii), $\langle c, d\rangle$ must be dihedral, elementary abelian of order 4 or isomorphic to A_4, S_4, or A_5. If $d^2 \neq 1$, we wish to move $\boldsymbol{w}$ to (x, y, e) with $y^2 = 1$. In the dihedral case $x = c$, $y = cd$ suffices, while if $H \cong A_4$, either $c^2 = 1$ and we can interchange c and d or $|c| = |d| = 3$ and cd or c^2d is an involution. If $H \cong S_4$ and c and d are both not involutions, the orders of c and d are 3 or 4. If $|c| = |d| = 4$, then $|cd| = 2$ or 3, so we may assume $|c| = 3$, $|d| = 4$. Either $|cd| = 2$ or $|c^2d| = 2$. Finally in the case $H \cong A_5$, we appeal to [**11**, § 10] which says that for some automorphism $x_i \rightarrow w_i(x_1, x_2)$ of F_2, $w_2(c, d)$ will be an involution. As we may extend this automorphism to F_3 by $x_3 \rightarrow x_3$, we can move $\boldsymbol{w}$ to (x, y, e) as desired. Applying the same argument to x and e, we have

(iv) $\boldsymbol{w} \sim \boldsymbol{u} = (x, y, z)$ with $|x| = |y| = 2$.

We let $\boldsymbol{u} = (x, y, z)$ stand for an arbitrary element of W whose first two entries have order 2. Suppose $[x, y] \neq 1$ so that $\langle x, y\rangle$ is dihedral of order at least 6 and $f = xy$ has order at least 3. As

$$\boldsymbol{u} \sim (x, f, z) \in W$$

(i)-(iii) imply that $K = \langle f, z\rangle$ is dihedral or isomorphic to A_4, S_4 or A_5. With the exception of $K \cong A_4$, f is inverted by some $g \in K$. Since g is equal to a word in f and z,

$$(x, f, z) \sim (xg, f, z)$$

But x also inverts f so that $\langle xg, f\rangle$ is abelian. By (ii) $\langle xg, f\rangle$ must be elementary abelian of order 4 contrary to $|f| \geqq 3$. We conclude that

(v) $\langle xy, z\rangle \cong A_4$ or $[x, y] = 1$.

Since G is simple, the $\langle x, z\rangle$-conjugates of y generate G, and likewise x does not commute with some $\langle x, z\rangle$-conjugate, y_1, of y. Thus

$$\boldsymbol{u} \sim \boldsymbol{u}_1 = (x, y_1, z)$$

with $|x| = |y_1| = 2$ and $[x, y_1] \neq 1$. Consequently $|xy_1| \geqq 3$ and by (v) $\langle xy_1, z\rangle \cong A_4$. We must have $|xy_1| = 3$ and $|(xy_1)^j z| = 2$ for some j. Hence

$$\boldsymbol{u}_1 \sim \boldsymbol{u}_2 = (x, y_1, z_1)$$

with $|z_1| = 2$. By (v) G is a quotient of

$$G_1 = \langle x, y_1, z_1 | x^2, y_1^2, z_1^2, (xy_1)^3, (xz_1)^m, (y_1z_1)^n\rangle$$

with m and n each equal to 2 or 3. If $m = 2$ or $n = 2$, then G_1 has order 12 or 24 by [**3**, § 4.3]. But $|G| \geqq 60$, so we must have $|xz_1| = |y_1z_1| = 3$ (in which case G_1 has infinite order). Now

$$\boldsymbol{u}_2 \sim (x, y_1, y_1z_1) \in W$$

so (v) implies $\langle xy_1, y_1z_1\rangle \cong A_4$. Further $|y_1z_1| = 3$ and $|xy_1y_1z_1| = |xz_1| = 3$. But then $|xy_1(y_1z_1)^{-1}| = 2$; and as $|y_1| = |z_1| = 2$, $(y_1z_1)^{-1} = z_1y_1$. We have $|xy_1z_1y_1| = 2$. In other words x commutes with

$$z_2 = y_1z_1y_1 = y_1z_1y_1^{-1}.$$

But

$$\boldsymbol{u}_2 \sim (x, y_1, z_2) \in W$$

with $|x| = |y_1| = |z_2| = |xz_2| = 2$, $|xy_1| = 3$, $|y_1z_2| = |z_1y_1| = 3$ gives a contradiction as above.

Our results so far guarantee that Aut (F_n) acts as the alternating or symmetric group on $\bar{V}(G, n)$. By [**11**, Sec. 3.5] $\langle\sigma(1)\rangle$ covers the commutator quotient of Aut (F_n). By Dirichlet's theorem on primes, Theorem 3 will be proved once we show that the sign (as a permutation) of $\sigma = \sigma(1)$ is odd if $p \equiv 1 \pmod{80}$ and even if $p \equiv 17 \pmod{80}$. We will count the number of points of $\bar{V}(G, n)$ moved by σ and divide by 2. The Aut (G)-orbit of $\boldsymbol{w} = (c_1, \ldots, c_n)$ is fixed by σ exactly when there is an automorphism α of G with $\alpha(c_1) = c_1^{-1}$, $\alpha(c_i) = c_i$ $2 \leqq i \leqq n$. Since $\langle c_1, \ldots, c_n\rangle = G$, $\boldsymbol{w}$ determines α.

First we count the number $\psi(G)$ of generating G-vectors $\boldsymbol{w}$ which are not fixed by σ; i.e., the number of $\boldsymbol{w}$'s with $|c_1| > 2$. The number of H-vectors of this type for a group H is $f(H)|H|^{n-1}$ where $f(H)$ is the number of elements of H of order at least 3. To calculate $\psi(G)$ we use the Möbius inversion of P. Hall [**9**] and obtain a sum over the subgroups of G.

$$\psi(G) = \Sigma\mu(H)f(H)|H|^{n-1}$$

where μ is given in [**10**, § 3.9]. Combining terms corresponding to conjugate subgroups, we obtain

(3) $\psi(G) = \Sigma' a_H f(H)|H|^{n-1}$

where the sum is carried out over conjugacy classes of subgroups as in [**10**, Theorem 3.9]. As it will suffice to determine $\psi(G)$ modulo $8g$, we may ignore terms in (3) which are divisible by $8g$. If we note that a_H is always divisible by $|G : H|$ (as it must be by [**7**, Corollary 2]), and $n \geqq 3$, we may ignore any H for which 8 divides $f(H)|H|$. By inverting elements of H we see that $f(H)$ is even whence we may ignore terms corresponding to H's of even order.

We obtain

$$(4)\quad \begin{array}{l} \psi(G) \equiv 4g \pmod{8g} \quad \text{if } p \equiv 1 \pmod{80} \\ \psi(G) \equiv 0 \pmod{8g} \quad \text{if } p \equiv 17 \pmod{80}. \end{array}$$

Among the $\psi(G)$ vectors not fixed by σ will be some which are in an Aut (G)-orbit fixed by σ. Let $\theta(G)$ be the number of these vectors; $\theta(G)$ is the number of generating G-vectors

$$\boldsymbol{w} = (c_1, c_2, \ldots, c_n)$$

for which $|c_1| > 2$ and there is an automorphism $\alpha \in$ Aut (G) inverting c_1 and centralizing c_i, $2 \leqq i \leqq n$. The Aut (G)-orbit of $\boldsymbol{w}$ has size $2g = |\text{Aug } (G)|$, and all its vectors are moved by σ. Thus σ is a product of $(\psi(G) - \theta(G))/4g$ disjoint transpositions. We will show $\theta(G) \equiv 0 \pmod{8g}$ when $n \geqq 4$. For $n = 3$, similar but harder computation gives the same result. We identify Aut (G) with PGL $(2,p)$ and think of G as a subgroup of Aut(G).

As we have noted, $\boldsymbol{w}$ determines α uniquely and $\langle \alpha, c_1 \rangle = D$ is a dihedral subgroup of Aut (G). For each choice of α and c_1 we obtain a group vector $\boldsymbol{w}$ by choosing $c_i \in C_G(\alpha)$, $2 \leqq i \leqq n$. If $\boldsymbol{w}$ is not a generating G-vector, then $\langle c_i | 1 \leqq i \leqq n \rangle$ lies in a maximal subgroup of G and $\langle \alpha, c_i | 1 \leqq i \leqq n \rangle$ lies in a maximal subgroup of Aut (G). To count the number of generating group vectors corresponding to the pair (α, c_1) we count the number of sequences $c_2, \ldots, c_n$ in $C_G(\alpha)$ such that $\langle c_i | 2 \leqq i \leqq n \rangle$ is not contained in $C_{H \cap G}(\alpha)$ for any maximal subgroup H of Aut (G) containing D. We divide the enumeration into cases according to the value of $m = |c_1|$. Define $q = (p - 1)/2$ and $r = (p + 1)/2$ so that $g = 2pqr$.

Suppose $p \neq m > 5$. D lies in a unique maximal subgroup H of Aut (G) and H is dihedral of order $4q$ if m divides q or dihedral of order $4r$ if m divides r. (The maximal subgroups of Aut (G) are the normalizers of the maximal subgroups of G, and their structure is determined by knowledge of the subgroups of PSL $(2,p^2)$ and the fact that PSL $(2,p^2)$ has a subgroup isomorphic to PGL $(2,p)$.) Suppose $|H| = 4q$. H contains $\varphi(m)$ elements of order m, where φ is Euler's function. There are pr choices for H (of order $4q$) and $2q$ involutions in $H - Z(H)$. These divide into 2 H-conjugacy classes each of order q. From the involutions in a single H-conjugacy class we obtain $q\varphi(m)$ pairs (α, c_1). For each pair we may choose $c_2, \ldots, c_n$ in $|C_G(\alpha)|^{n-1} - |C_{H \cap G}(\alpha)|^{n-1}$ ways. As

$|H \cap G|$ is even and $n \geqq 4$, the number of choices of $c_2, \ldots, c_n$ is divisible by 4, and the number of generating group vectors we obtain is congruent to 0 modulo $16q$. From the rp choices for H, then the total number of generating group vectors we obtain is congruent to zero modulo $16rpq = 8g$. The same conclusion holds if $m > 5$ and m divides r.

Suppose $p \neq m = 5$. D lies in a unique dihedral group H of order $4q$ or $4r$ and if $D \subseteq G$, D also lies in two icosahedral groups K_1 and K_2. The argument of the previous paragraph gives 0 (mod $8g$) $\boldsymbol{w}$'s once we show that for a fixed α and c_1, the number of choices of $c_2, \ldots, c_n$ is divisible by 8. If α is outer, the desired conclusion follows exactly as before. If α is inner, $\langle c_2, \ldots, c_n \rangle$ must not lie in $C_{H \cap G}(\alpha)$ or $C_{K_i}(\alpha)$, $i = 1, 2$. We can calculate the number of choices for $c_2, \ldots, c_n$ by Möbius inversion on the lattice of subgroups consisting of $C_G(\alpha)$ and all intersections of $C_{H \cap G}(\alpha)$ and $C_{K_i}(\alpha)$, $i = 1, 2$. The answer will be a linear combination of the orders of the groups in the lattice raised to the power $n - 1$. As $\langle \alpha \rangle$ is the minimum element of this lattice and $n \geqq 4$, our answer will be divisible by 8.

Next we suppose $m = 4$. D lies in a unique maximal dihedral subgroup H. If M is any maximal subgroup of Aut (G) containing D, $Z(D) \subseteq C_{M \cap G}(\alpha)$ implies $|C_{M \cap G}(\alpha)|$ is even and the argument of the previous paragraph with $Z(D)$ in place of $\langle \alpha \rangle$ shows that the number of choices of $c_2, \ldots, c_n$ is divisible by 4. We again obtain 0 (mod $4g$) $\boldsymbol{w}$'s.

Consider $m = 3$. D lies in a unique H dihedral of order $4q$ or $4r$. If $D \nsubseteq G$ and $p \equiv \pm 3 \pmod 8$, D lies in two octahedral groups. If $D \subseteq G$, D lies in two octahedral subgroups of G if $p \equiv \pm 1 \pmod 8$. When $D \subseteq G$, (that is when α lies in the H-conjugacy class of involutions in $H \cap G - Z(H)$) we obtain as in the case $p \neq m = 5$, 0 (mod $8g$) generating group vectors. Suppose $D \nsubseteq G$ and $|H| = 4q$. From the rp choices for H and q choices for $\alpha \in H - G$, we have $(rp)(q)\varphi(3) = g$ pairs (α, c_1). If $p \equiv \pm 1 \pmod 8$, H is the only maximal subgroup of Aut (G) containing D and we obtain 0 (mod $8g$) generating vectors as before. However if $p \equiv \pm 3 \pmod 8$, D lies in two octahedral subgroups J_1, J_2 of Aut (G). Let $E_i = C_{J_i \cap G}(\alpha)$, $i = 1, 2$. $|E_i| = 2$ and $J_i = \langle D, E_i \rangle$. We have $E_1 \neq E_2$ else $J_1 = J_2$ and $E_i \nsubseteq C_H(\alpha)$ else $J_i \subseteq H$. By Möbius inversion the number of choices for $c_2, \ldots, c_n$ is

$$|C_G(\alpha)|^{n-1} - |C_{H \cap M}(\alpha)|^{n-1} - 2.2^{n-1} + 2$$

which is congruent to 2 (mod 8). We obtain in this case $2g$ (mod $8g$) generating group vectors, and we obtain the same result if $|H| = 4r$.

In summary if $\theta_p(G)$ is the number of $\boldsymbol{w}$'s with $m = p$ and $\theta_p'(G)$ is the number with $m \neq p$, we have

$$(5) \quad \begin{aligned} \theta_p'(G) &\equiv 0 \pmod{8g} \quad \text{if } p \equiv \pm 1 \pmod 8 \text{ and } n \geqq 4, \\ \theta_{p'}(G) &\equiv 2g \pmod{8g} \quad \text{if } p \equiv \pm 3 \pmod 8 \text{ and } n \geqq 4. \end{aligned}$$

It remains to calculate $\theta_p(G)$. We have $m = p$, and D lies in a unique maximal subgroup H of Aut (G). H is the normalizer of a Sylow p-subgroup

$\langle c_1 \rangle$ of G and is a Frobenius group with $H/\langle c_1 \rangle$ cyclic of order $2q$. H has one class of involutions, which has size p. From the $2r$ choices for H we have $2rp\varphi(p)$ choices of the pair (α, c_1) we may choose $c_2, \ldots, c_n$ in $|C_G(\alpha)|^{n-1} - |C_{H \cap G}(\alpha)|^{n-1}$ ways we have

$$\theta_p(G) = 2rp(p-1)[(2q)^{n-1} - q^{n-1}]$$

whence

$$(6) \quad \theta_p(G) \equiv 0 \pmod{4g} \quad \text{if } p \equiv 1 \pmod 4.$$

By (4), (5), (6) the following table is correct for $p \equiv 1$ or 17 (mod 80) and $n \geqq 4$.

Sign of σ as a permutation on $\bar{V}(PSL(2, p), n)$, $n \geqq 3$

Congruence of p (mod 8)		1	3	5	7
Congruence of p (mod 5)	± 1	-1	1	$(-1)^{n-1}$	1
	± 2	1	-1	$(-1)^n$	-1

For $p = 5$ the sign of σ is $(-1)^n$.

References

1. H. Bochert, *Ueber die Classe der transitiven Substitutionengruppen*, Math. Ann. *49* (1897), 131–144.
2. F. Cappel, *Diplomarbeit* (Aachen, 1974).
3. H. S. M. Coxeter and W. O. J. Moser, *Generators and relations for discrete groups* (Springer Verlag, New York, 1965).
4. L. E. Dickson, *Linear groups with an exposition of the Galois field theory* (Dover Publications Inc., New York, 1958).
5. M. J. Dunwoody, *On T-systems of groups*, J. Australian Math. Soc. *3* (1963), 172–179.
6. ——— *Nielsen transformations*, in Computational Problems in Abstract Algebra, J. Leech ed. (Pergamon Press, Oxford and New York, 1969).
7. R. Gilman, *A combinatorial identity with applications to representation theory*, Illinois J. Math. *17* (1972), 347–351.
8. D. Gorenstein ed., *Reviews on finite groups* (Amer. Math. Soc., Providence, R.I., 1974).
9. E. Grossman, *On the residual finiteness of certain mapping class groups*, J. London Math. Soc. (2) *9* (1974), 160–164.
10. P. Hall, *The Eulerian functions of a group*, Quarterly J. Math. *7* (1936), 134–151.
11. W. Magnus, A. Karrass, and D. Solitar, *Combinatorial group theory* (Interscience Publishers, New York, 1966).
12. B. H. Neumann and H. Neumann, *Zwei Klassen Charakterischer Untergruppen und ihre Faktorgruppen*, Math. Nachr. *4* (1950), 106–125.
13. A. Peluso, *A residual property of free groups*, Comm. Pure Appl. Math. *19* (1966), 435–437.
14. D. Stork, *Structure and applications of Schreier coset graphs*, Comm. Pure Appl. Math. *24* (1971), 797–805.
15. ——— *The action of the automorphism group of F_2 upon the A_6 and $PSL(2, 7)$—defining subgroups of F_2*, Trans. Amer. Math. Soc. *172* (1972), 111–117.

Stevens Institute of Technology,
Castle Point Station,
Hoboken, New Jersey