Illinois Journal of Mathematics
Volume 45, Number 3, Fall 2001, Pages 1051–1060
S 0019-2082

COUNTING INVOLUTIONS

MICHAEL ASCHBACHER, ULRICH MEIERFRANKENFELD, AND BERND STELLMACHER

ABSTRACT. Some results are established which are useful in determining the order of a finite group with one class of involutions, given knowledge of the centralizer of an involution. An application is provided to illustrate the results. The main tool is a lemma of H. Bender on counting involutions.

0. Introduction

There are a number of results on finite groups that are proved by counting involutions; the Brauer-Fowler Theorem [4] and the Thompson Order Formula (see 45.6 in [1]) are perhaps the two most important examples. In a less well known paper [2], Bender introduces an involution counting technique useful in analyzing small groups where more traditional local analysis is often ineffective. In particular Bender's approach can sometimes be used to calculate the order of a group with one class of involutions; we recall that the Thompson Order Formula does not apply to such groups.

In this note we use Bender's approach to prove:

THEOREM 1. *Assume M is a nontrivial TI-subgroup of the finite group G, let $M^* = N_G(M)$, and assume $M^* = MC_{M^*}(z)$ for some involution $z \in M^*$ and $C_G(x)$ is of odd order for each $x \in M^\#$. Then one of the following holds:*

(1) $M \trianglelefteq G$.
(2) $n(G) \leq |G : M|$, *where $n(G)$ denotes the number of involutions in G.*
(3) $G \cong PGL_2(m)$ *or* $L_2(m)$ *for some power m of some prime p, M is an elementary abelian p-group of order m, and $m \equiv 1 \mod 4$ if $G \cong L_2(m)$.*
(4) $G \cong L_2(2^e)$ *for some integer $e > 1$ and M is cyclic of order $2^e + 1$.*

Received September 18, 2000; received in final form October 5, 2001.
2000 *Mathematics Subject Classification.* 20D05.
The first author's work was partially supported by NSF-9901367.

(5) *There exists a positive integer d such that G is the split extension of an elementary abelian group of order 2^{2d} by M^*, and M^* is dihedral of order $2(2^d+1)$.*

See [1] for the definition of basic notation and terminology. For example, T is a *TI-subgroup* of G if distinct conjugates of T in G intersect trivially; $O(G)$ is the largest normal subgroup of G of odd order; $G^\# = G - \{1\}$ is the set of nontrivial elements of G.

Notice that if conclusion (2) holds then $|M| \leq |C_G(t)|$ for each involution t in G, while if G has one class of involutions then conclusion (2) of Theorem 1 is equivalent to $|M| \leq |C_G(z)|$.

The next lemma provides subgroups to which Theorem 1 can be applied. It is a slight variation on the penultimate theorem in [3]. Given a group G, define the *commuting graph* of G to be the graph Δ with vertex set $G^\#$ and g adjacent to h if $gh = hg$. Write $d(g,h)$ for the distance from g to h in Δ and let $\Delta^i(g) = \{h \in \Delta : d(g,h) = i\}$.

LEMMA 2. *Let G be a finite group, z an involution in G, and $1 \neq x$ an element of G inverted by z. Assume:*

(i) $d(z,x) \geq 3$.
(ii) *If $d(z,x) = 3$ then z inverts no member of $\Delta^2(z) \cap \Delta(x)$.*

Set $M = C_G(x)$. Then:

(1) *$M = C_G(y)$ for each $y \in M^\#$, so $d(z,x) = \infty$.*
(2) *M is a TI-subgroup of G.*
(3) *M is abelian of odd order and inverted by z.*
(4) *$M^* = N_G(M)$ is a Frobenius group with kernel M and complement $C_{M^*}(z)$.*
(5) *M is a Hall subgroup of G.*

In a group G with one class of involutions, if one has good control over the centralizer of an involution then one can usually obtain strong information about the centralizers of elements at distance 1 from involutions, and hence also some information about elements at distance 2. Lemma 2 and Theorem 1 supply information about centralizers of elements at distance greater than 2 that are inverted by involutions.

Finally to illustrate how Theorem 1 and Lemma 2 can be applied, we give a short, elementary proof of the following well known result:

THEOREM 3. *Let G be a finite group containing an involution z such that $T = C_G(z)$ is dihedral of order 8. Then one of the following holds:*

(1) *$G = TO(G)$.*
(2) *$G \cong S_4 \cong PGL_2(3)$.*
(3) *$G \cong S_5 \cong PGL_2(5)$.*

(4) $G \cong L_3(2) \cong PSL_2(7)$.
(5) $G \cong A_6 \cong PSL_2(9)$.

Bender gives a similar proof of a slightly weaker result in [2]. Theorem 1 makes possible only a small simplification in Bender's treatment, but such simplifications become more crucial in larger examples.

Local characterizations like Theorem 2 of small groups in the existing literature typically involve extensive use of exceptional character theory and block theory. In addition to supplying simplified proofs for such results, another advantage to an approach involving involution counting is the elimination or reduction in appeals to character theory.

1. A lemma of Bender

Let G be a finite group and $\mathcal{J}$ the set of involutions in G. For $S \subseteq G$, let $n(S) = |\mathcal{J} \cap S|$ be the number of involutions in S. Following Bender in [2], given a subgroup M of G, define

$$f = f(G, M) = \frac{n(G)}{|G : M|} - 1.$$

Observe:

LEMMA 1.1. *$n(G) > |G : M|$ iff $f(G, M) > 0$.*

Write G/M for the coset space of cosets Mg, $g \in G$, and represent G by right multiplication on G/M.

Again following Bender, given a nonnegative integer m, define

$$b_m = b_m(G, M) = |\{C \in G/M - \{M\} : n(C) = m\}|.$$

Observe that for each m, M acts on the set of cosets C of M with $n(C) = m$.

The following lemma of Bender in [2] is one of the fundamental tools in this paper; its proof is easy and elementary.

LEMMA 1.2 (Bender). *Assume $M \leq G$ with $n(G) > |G : M|$. Then*

$$b_1 = f^{-1}(n(M) + \sum_{i>1}(i-1)b_i - 1 - b_0) - 1 - b_0 - \sum_{i>1} b_i.$$

2. The proof of Theorem 1

Throughout this section we assume the hypotheses of Theorem 1. Continue the notation of the previous section. In addition, for $x \in G$ let $I(x)$ be the set of involutions in G inverting x. Set $m = |M|$. Recall $m_2(G)$ is the 2-rank of G; that is, $m_2(G) = k$, where 2^k is the maximal order of an elementary abelian 2-subgroup of G.

LEMMA 2.1.

(1) *M is abelian of odd order and inverted by z.*
(2) *$I(y) \subseteq Mz = z^M$ for all $y \in M^\#$.*
(3) *$\mathcal{J} \cap M^* = z^M$.*
(4) *$m_2(M^*) = 1$.*
(5) *$C_{M^*}(z)$ is a complement to M in M^* and $[z, M^*] = M$.*

Proof. Let $W = C_G(M)$. By hypothesis $C_G(y)$ is of odd order for each $y \in M^\#$, so m is odd, W is of odd order, and $C_M(i) = 1$ for each involution $i \in M^*$. Thus (1) holds. If $i \in I(y)$ then $i \in M^*$ as M is TI. Then i inverts M, so $zi \in W$. Hence as $|W|$ is odd, $i \in z^W$. But by hypothesis, $M^* = MC_{M^*}(z)$, so $W = MC_W(z)$, and hence $i \in z^M = Mz$. Therefore (2) holds. Further as $C_M(i) = 1$ for each $i \in \mathcal{J} \cap M^*$, (2) implies (3). As $m_2(M\langle z\rangle) = 1$, (3) implies (4). As $M^* = MC_{M^*}(z)$ and $C_M(z) = 1$, (5) holds. □

LEMMA 2.2.

(1) *Mz is the unique coset C of M such that $n(C) > 1$.*
(2) *$n(Mz) = m$.*

Proof. Suppose $C \in G/M$ with $n(C) > 1$. Then there are distinct involutions $i, j \in C$. Then $ij \in M^\#$ is inverted by i and j, so by 2.1(2), $i, j \in I(ij) \subseteq Mz$; that is $C = Mz$, so (1) holds. Part (2) follows from parts (1) and (2) of 2.1. □

During the remainder of the section we assume that neither conclusion (1) nor conclusion (2) of Theorem 1 hold. Thus $n(G) > |G : M|$ and $G \neq M^* = N_G(M)$. Let $a = |M^* : M|$, $r = |C_G(z)|/a$ and $N = |G : M^*|$. Observe $a = |C_{M^*}(z)|$.

Recall the definition of the parameters $b_i = b_i(G, M)$ from the previous section.

LEMMA 2.3.

(1) $b_1 = f^{-1}(m - (b_0 + 2)) - (b_0 + 2)$.
(2) $b_0 < m - 2$.

Proof. As $n(G) > |G : M|$, we can apply 1.1 to conclude $f > 0$ and appeal to 1.2. By 2.2, $b_i = 0$ except when i is 0, 1, or m; also $n(M) = 0$ and $b_m = 1$. Thus (1) follows from 1.2. As $b_1 \geq 0$, (1) implies (2). □

LEMMA 2.4. *Let $g \in G - M^*$ and set $D = M^* \cap M^{*g}$. Then:*

(1) *$n(Mg) = 1$ and $n(M^*g) = a$.*
(2) *D is a complement to M in M^* inverted by the involution $t \in Mg$, D contains a unique involution i, and $D = C_{M^*}(i)$.*
(3) *$M \cap M^{*g} = 1$.*

(4) $N - 1 = m(r-1)$.
(5) $|G| = Nma = (m(r-1)+1)ma$.
(6) $b_1 = am(r-1)$.

Proof. If $n(Mg) \neq 1$ then $n(Mg) = 0$ by 2.2(1). However as $M \cap M^g = 1$, the orbit on G/M of Mg under M is of length m, so $b_0 \geq m$, contrary to 2.3(2). Further M^*g is the union of a cosets of M, so $n(M^*g) = a$, establishing (1).

Next by 2.1(3), $z^G \cap M^* = z^{M^*}$, so $C_G(z)$ is transitive on the set Γ of fixed points of z on G/M^* (see 5.21 in [1]). Thus $|\Gamma| = |C_G(z) : C_{M^*}(z)| = |C_G(z)|/a = r$. Let $\mathcal{U} = M^*g \cap \mathcal{J}$; by (1), $\mathcal{U}$ is of order a. Thus for $j \in \mathcal{U}$, the set U of elements of D inverted by j is $\{uj : u \in \mathcal{U}\}$ of order a. By (1), $\mathcal{U}$ is a set of coset representatives for M in M^*g, so as $M^*j = M^*g$ and $D \leq M^*$, we conclude:

$$M^* = \bigcup_{u \in \mathcal{U}} Muj = MU = MD.$$

In particular D is of even order, so as j acts on D, D contains an involution i centralizing j. Now by 2.1(5), i inverts M, so $M \cap D = [M \cap D, i]$. Also by 2.1(5) applied to M^{*g}, $[M \cap D, i] \leq [M^{*g}, i] \leq M^g$, so $M \cap D \leq M \cap M^g = 1$. Thus D is a complement to M in M^*, so $|D| = a = |U|$ and hence $D = U$. As $D = U$, D is inverted by j, so D is abelian. Thus $D \leq C_{M^*}(i)$, so $D = C_{M^*}(i)$ and as $m_2(M^*) = 1$, i is the unique involution in D. Therefore (2) and (3) hold.

For each $g \in G - M^*$, $M^* \cap M^{*g}$ is the stabilizer in M^* of $M^*g \in G/M^*$, so by (2), M^*g is fixed by a unique involution of M^*. Thus by 2.1(3), $G/M^* - \{M^*\}$ is partitioned by the m sets $\mathrm{Fix}_{G/M^*}(z^x) - \{M^*\}$, $x \in M$. This establishes (4).

Next $|G : M^*| = N$ and $|M^*| = ma$, so (5) follows from (4). Similarly $|G : M| = aN$, while by (1), $|G : M| = a + b_1$. Then (4) implies (6). □

LEMMA 2.5.

(1) *Either*
  (i) *for some integer* $e > 2$, $C_G(z) \cong E_{2^e}$, $a = 2$, *and* $r = 2^{e-1}$,
  or
  (ii) $r = 2$ *and* $C_{M^*}(z)$ *is inverted by an involution in* $C_G(z) - C_{M^*}(z)$.
(2) *In case* (i):
  (a) $|G| = 2m(m(2^{e-1}-1)+1)$.
  (b) $|G : C_G(z)| = m(m(2^{e-1}-1)+1)/2^{e-1}$.
  (c) $|\mathcal{J}| = m(2^e - 1)$.
(3) *In case* (ii):
  (a) $|G| = m(m+1)a$.
  (b) $|G : C_G(z)| = m(m+1)/2$.
  (c) $|\mathcal{J}| = m(a+1)$.

Proof. If $C_G(z) \leq M^*$ then $r = 1$, so $N = 1$ by 2.4(4), contradicting $G \neq M^*$. Thus there is $g \in C_G(z) - M^*$. Let $A = M^* \cap M^{*g}$; then $C_{M^*}(z) = A$ by 2.4(2). By 2.4(1), there is an involution $t \in Mg$, and by 2.4(2), t inverts A. Further $g \in C_M(z)t = \{t\}$, so each element of $C_G(z) - A$ is an involution inverting A. Thus (1)(ii) holds if $r = 2$. If $r > 2$ there exists $h \in C_G(z) - A$ with $hg \notin A$. Thus hg inverts and centralizes A, so A is of exponent 2, and then $A = \langle z \rangle$ by 2.1(4), so (1)(i) holds. Hence (1) is established.

Observe that as $|C_G(z)| = ar$, $|G : C_G(z)| = Nm/r$ by 2.4(5). Also by 2.4(1) and 2.4(6), $|\mathcal{J}| = n(M) + b_1 = m + am(r-1)$. Then (2) and (3) are easy calculations, given 2.4. □

LEMMA 2.6. *Assume case* (ii) *of* 2.5(1) *holds and let* $A = C_{M^*}(z)$. *Then:*

(1) G *is 2-transitive on* G/M^* *and* M *is regular on* $G/M^* - \{M^*\}$.
(2) A *is cyclic and semiregular on* M.
(3) $a = (m-1)/2$ *or* $m - 1$.
(4) m *is a power of a prime* p *and* M *is an elementary abelian* p*-group.*
(5) *If* $a = m-1$ *then* G *has two classes of involutions and* $G \cong PGL_2(m)$.
(6) *If* $a = (m-1)/2$ *then* G *has one class of involutions and* $G \cong L_2(m)$ *with* $m \equiv 1 \mod 4$.

Proof. By 2.5(3), $|G : M^*| = m + 1$, while by 2.4(3), M is semiregular on $G/M^* - \{M^*\}$, so (1) holds. Suppose $1 \neq X \leq A$ with $1 \neq C_M(X)$. As $C_M(z) = 1$, $z \notin X$, so as $m_2(A) = 1$, X is of odd order. By (1), $C_M(X)$ is regular on $\mathrm{Fix}(X) - \{M^*\}$ and by 2.5(2) there is an involution $t \in G - M^*$ inverting X, so $C_{M^t}(X)$ is regular on $\mathrm{Fix}(X) - \{M^*t\}$. Thus $Y = \langle C_M(X), C_{M^t}(X) \rangle$ is 2-transitive on $\mathrm{Fix}(X)$ and $Y \leq C_G(X)$. Thus there is $g \in C_G(X)$ with cycle (M^*, M^*t). This is impossible as $A\langle t \rangle$ is the global stabilizer of this set and each $g \in At$ inverts X, so $g \notin C_G(X)$ as X is of odd order. Thus A is semiregular on M, so as A is abelian, A is cyclic; that is (2) holds.

By 2.5(3), $|\mathcal{J}| = m(a+1)$ and $|z^G| = m(m+1)/2$, so $m(m+1)/2 \leq m(a+1)$, and hence $a \geq (m-1)/2$. But by (2), a divides $m - 1$, so (3) holds. Further if $a = (m-1)/2$ then $\mathcal{J} = z^G$, so G has one class of involutions and $m \equiv 1 \mod 4$ as a is even. If $a = m - 1$, then A is regular on $M^\#$, so G is sharply 3-transitive on G/M^* by (1). In any event, A is irreducible on M, so (4) holds.

In each case G is determined up to isomorphism by a result of Zaussenhaus [6], but we do not need Zaussenhaus' result. Rather we argue as follows:

Suppose $a = m - 1$. Regard M as an s-dimensional vector space over $\mathbf{F}_p$; then A is a cyclic subgroup of $GL(M)$ regular on $M^\#$, so A is determined up to conjugation in $GL(M)$. Hence $M^* = MA$ and its action on $\Omega = G/M^*$ are determined up to equivalence. Let $S = \mathrm{Sym}(\Omega)$. In particular a generator x of A is an a-cycle on $\Omega - \{M^*\}$, so $C_S(A) = A \times \langle \tau \rangle$, where τ is a transposition

in S with cycle (M^*, M^*t), and $N_S(A) = \langle\tau\rangle \times B$, where $B = N_S(A)_{M^*}$ is the split extension of A by $\mathrm{Aut}(A)$. Thus A is of index 2 in a unique dihedral subgroup D of S such that $D \not\leq B$. Therefore $G = \langle M^*, t\rangle = \langle M^*, D\rangle$ is determined up to conjugation in S. Then as $PGL_2(m)$ satisfies the hypotheses of G, it follows that $G \cong PGL_2(m)$, so (5) holds.

So assume $a = (m-1)/2$. Then G has one class of involutions and satisfies the hypotheses of Theorem 3.5 in Chapter 13 of [5]. Then that result says $G \cong L_2(m)$, so (6) holds. □

LEMMA 2.7. *Assume case* (i) *of* 2.5(1) *holds. Then:*

(1) *Either*
   (a) *G has one class of involutions, $m = 2^e+1$, and $|G| = 2^e(2^{2e}-1)$, or*
   (b) *G has more than one class of involutions, $m = 2^d+1$, and $|G| = 2^{2d+1}(2^d+1)$, where $d = e-1$.*

(2) *If G has one class of involutions then $G \cong L_2(2^e)$.*

(3) *If G has more than one class of involutions then $G = RM^*$, where $R = O_2(G) \cong E_{2^{2d}}$.*

(4) *M is cyclic.*

Proof. By 2.5(2),

$$\frac{m(m(2^d-1)+1)}{2^d} = |z^G| \leq |\mathcal{J}| = m(2^{d+1}-1),$$

so

$$m(2^d-1) \leq 2^d(2^{d+1}-1) - 1 = (2^d-1)(2^{d+1}+1),$$

and hence

$$(*) \qquad m \leq 2^{d+1}+1 = 2^e+1.$$

Indeed, if G has one class of involutions then the inequality in $(*)$ is an equality, so $m = 2^e+1$ and hence $|G| = 2^e(2^{2e}-1)$ by 2.5(2), so (1)(a) holds in this case. Further $C_G(z) \cong E_{2^e}$ in 2.5(1).i, so as G has one class of involutions, $C_G(i) \cong E_{2^e}$ for each $i \in \mathcal{J}$. Therefore (2) holds by Exercise 16.1 in [1]. In particular the unique subgroup of G of order 2^e+1 is cyclic, so (4) holds.

Thus we may assume G has more than one class of involutions. Then the inequality in $(*)$ is strict; that is, $m < 2^e+1$. However by 2.5(2),

$$|G : C_G(z)| = \frac{m(m(2^d-1)+1)}{2^d},$$

so

$$0 \equiv m(2^d-1)+1 \equiv 1-m \mod 2^d,$$

and hence $m = 2^d+1$. Thus (1)(b) holds by 2.5(2).

Let $i \in \mathcal{J} - z^G$; then i inverts no element of $M^\#$ as M is a TI-subgroup of G and all involutions in M^* are in z^G. Indeed, as $|G| = (2^d+1)2^{2d+1}$ and M

is a TI-subgroup, all elements in $G^\#$ of odd order are in conjugates of M, so i inverts no element of $G^\#$ of odd order. Let $R = O_2(G)$; it follows from the Baer-Suzuki Theorem (see 39.6 in [1]) that $i \in R$. As $C_G(x)$ is of odd order for each $x \in M^\#$, M is semiregular on R. Thus if V is a nontrivial M-chief section on R, $|V^\#| \equiv 0 \mod 2^d + 1$, so $|V| \geq 2^{2d}$. Then as $|G| = 2^{2d}|M^*|$, it follows that $R \cong E_{2^{2d}}$ and M^* is a complement to R in G. Thus (3) holds. Finally as M is abelian and semiregular on R, (4) holds. □

Observe that 2.5–2.7 complete the proof of Theorem 1.

3. The proof of Lemma 2

In this section we assume the hypotheses of Lemma 2. By (i), $C_M(z) = 1$, so z inverts M and (3) holds. Let $y \in M^\#$. Then $d(z, y) \geq d(z, x) - 1$, so if $d(z, x) > 3$ then $d(z, y) \geq 3$. On the other hand, if $d(z, x) = 3$ then as z inverts y, $d(z, y) \geq 3$ by (ii). As M is abelian, $M \leq C_G(y)$ and as $d(z, y) \geq 3$, z inverts $C_G(y)$, so $C_G(y)$ is abelian. Thus $C_G(y) \leq M$, so (1) holds. Then (1) implies (2).

Let i be an involution in M^*. By (1), $C_M(i) = 1$, so i inverts M. Thus $iz \in C_G(M) = M$, so $i \in Mz$. Thus $\mathcal{J} \cap M^* = Mz = z^M$, so $C_{M^*}(z)$ is a complement to M in M^* by a Frattini argument. Further for $r \in C_{M^*}(z)^\#$, $C_M(r) = 1$ by (1), so (4) holds. Finally by (4), M is a Hall subgroup of M^*, while for $p \in \pi(M)$ and $P \in \mathrm{Syl}_p(M)$, $N_G(P) \leq M^*$ by (2), so $P \in \mathrm{Syl}_p(G)$. Thus (5) holds.

This completes the proof of Lemma 2.

4. The proof of Theorem 3

In this section we assume the hypotheses of Theorem 3. As $\langle z \rangle = Z(T)$ is characteristic in T and $T \in \mathrm{Syl}_2(C_G(z))$, $T \in \mathrm{Syl}_2(G)$. Let A_1 and A_2 be the two 4-subgroups of T and let $G_i = N_G(A_i)$. If z is strongly closed in T with respect to G, then applying Thompson transfer to the cyclic subgroup of index 2 in T, $O^2(G)$ has cyclic Sylow 2-subgroups. Therefore (1) holds (see 39.2 in [1]). Thus we may assume $z^g \in A_1 - \langle z \rangle$.

As $\langle z \rangle = [T, A_1]$ and $\langle z^g \rangle = [T^g, A_1]$, $H = \langle T, T^g \rangle \leq G_1$ and H induces $L_2(2)$ on A_1. Thus as $A_1 = C_G(A_1)$, $G_1 = H \cong S_4$. If A_1 is strongly closed in T with respect to G, then by Thompson transfer, $O^2(G_1) = O^2(G) \cap G_1$. Let $L = O^2(G)$. Then $A_1 \in \mathrm{Syl}_2(L)$ and L has one class of involutions with $C_L(z) = A_1 \cong E_4$. It follows from Exercise 16.1 in [1] that $L \cong A_4$ or A_5, and then that (2) or (3) holds. Thus we may assume A_1 is not strongly closed in T with respect to G, so G has one class of involutions and by symmetry, $G_2 \cong S_4$.

Suppose $x \in G^\#$ is of odd order and inverted by an involution. As G has one class of involutions, we may assume z inverts x. As $C_G(z)$ is a 2-group, $d(z, y) = \infty$ for each $y \in G^\#$ of odd order. Thus we conclude from Lemma 2

that $X = C_G(x)$ is a TI-subgroup of odd order inverted by z and satisfies the hypotheses of the group "M" in Theorem 1. Therefore by Theorem 1, either $|X| \le |C_G(z)| = 8$, or G satisfies one of conclusions (3)–(5) of Theorem 1. In the latter case as G has one class of involutions and $C_G(z) \cong D_8$, we conclude (4) or (5) holds. Thus we may assume $|C_G(x)| = 3$ or 5 for each $x \in G^\#$ of odd order inverted by an involution. In particular if $X_i \in \mathrm{Syl}_3(G_i)$ then as X_i is inverted by an involution in T, $X_i = C_G(X_i)$, so $N_G(X_i) = N_{G_i}(X_i) \cong S_3$.

Let $M = G_1$; as $|M| > |T|$, we may apply 1.2 to M. As G has one class of involutions,

$$f = \frac{|G:T|}{|G:M|} - 1 = \frac{|M|}{|T|} - 1 = 2.$$

Further if $y \in M^\#$ then either $N_G(\langle y\rangle) \le M$, or y is one of the six involutions in $M - A_1$. Thus if u is an involution in $G - M$ then $n(Mu) > 1$ iff u centralizes one of these six involutions y, in which case $\langle y\rangle = M \cap M^u$, so $n(Mu) = 2$. Hence $b_m = 0$ for $m > 2$ and $b_2 = 6$. Then as $n(M) = 9$, it follows from 1.2 that

$$\begin{aligned} b_1 &= f^{-1}(n(M) + b_2 - b_0 - 1) - b_2 - b_0 - 1 \\ &= \frac{9 + 6 - b_0 - 1}{2} - 6 - b_0 - 1 = \frac{-3b_0}{2}. \end{aligned}$$

Thus as $b_1 \ge 0$, we conclude $b_1 = b_0 = 0$. Therefore $|G : M| = 1 + b_2 = 7$. Now we conclude $G \cong L_3(2)$ by any one of a number of means. For example, G is 2-transitive on G/G_i for $i = 1, 2$, so the coset geometry of G on the family $\{G_1, G_2\}$ is a projective plane of order $|G_i : G_1 \cap G_2| - 1 = 2$. As it is an elementary exercise to show there is a unique plane of order 2, $G = L_3(2)$ is the group of automorphisms of that plane.

This completes the proof of Theorem 3.

References

[1] M. Aschbacher, *Finite group theory*, Cambridge Univ. Press, Cambridge, 1986.
[2] H. Bender, *Finite groups with large subgroups*, Illinois J. Math. **18** (1974), 223–228.
[3] R. Brauer, *On the structure of groups of finite order*, Proc. Inter. Cong. Math., Amsterdam (1954), North-Holland, Amsterdam, 1957, pp. 209–217.
[4] R. Brauer and K. Fowler, *Groups of even order*, Ann. of Math. **62** (1955), 565–583.
[5] D. Gorenstein, *Finite groups*, Harper and Row, New York, 1968.
[6] H. Zaussenhaus, *Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen*, Hamburg Abh. **11** (1936), 17–40.

Michael Aschbacher, Department of Mathematics, California Institute of Technology, Pasadena, CA 91125, USA
E-mail address: asch@its.caltech.edu

Ulrich Meierfrankenfeld, Department of Mathematics, Michigan State University, East Lansing, MI 48824, USA
E-mail address: meier@math.msu.edu

Bernd Stellmacher, Mathematisches Seminar, Universität Kiel, Ludwig-Meyn Str. 4, D-24098 Kiel, Germany
E-mail address: stellmacher@math.uni-kiel.de