

HALL SUBGROUPS OF M -GROUPS NEED NOT BE M -GROUPS

HIROSHI FUKUSHIMA

(Communicated by Jonathan I. Hall)

ABSTRACT. In this paper, we shall give examples of M -groups that have Hall subgroups that are not M -groups.

1. INTRODUCTION

A character of a finite group G is monomial if it is induced from a linear character of a subgroup of G . A group G is an M -group if all its complex irreducible characters (the set $\text{Irr}(G)$) are monomial.

In the 1960s, Dornhoff [3] proved that normal Hall subgroups of M -groups are M -groups, and conjectured that normal subgroups of M -groups are M -groups. In the early 1970s, Dade [1] and van der Waall [6] independently showed that normal subgroups of M -groups need not be M -groups. In [5], Isaacs asked whether Hall subgroups of M -groups need be M -groups. In this paper, we shall give examples of M -groups that have Hall subgroups that are not M -groups.

Let $N \triangleleft G$ and $\theta \in \text{Irr}(N)$. We write $C_G(\theta)$ to denote the stabilizer of θ in G . We also write $\text{Irr}(G|\theta) = \{\chi \in \text{Irr}(G) \mid [\chi_N, \theta] \neq 0\}$.

2. PRELIMINARY LEMMAS

We begin with some preliminary lemmas.

Lemma 2.1. *Let E be an extra-special p -group, let σ be an automorphism of E of order q where $q \neq p$ is a prime, and let $G = E\langle\sigma\rangle$. If σ acts irreducibly on $E/Z(E)$, then G is not an M -group.*

Proof. We know that $|E| = p^{2n+1}$ for some positive integer n . This implies that the nontrivial irreducible p -modules for σ must have dimension $2n$, and thus, σ must centralize $Z(E)$. For any nonlinear character $\psi \in \text{Irr}(E)$, we see that $\psi(1) = p^n$ and ψ is invariant under the action of σ . By Corollary 6.28 of [4], ψ has an extension $\chi \in \text{Irr}(G)$.

We claim that χ is not monomial. Suppose χ were monomial. Then there would be a subgroup $H \subseteq G$ and a linear character $\lambda \in \text{Irr}(H)$ so that $\lambda^H = \chi$. We see that $|G : H| = \chi(1) = p^n$. It follows that $|H| = p^{n+1}q$, and so by conjugating, we may assume that $\sigma \in H$. This implies that $H \cap E/Z(E)$ is a σ -submodule of $E/Z(E)$, but this is a contradiction, since $Z(E) \subset H \cap E \subset E$ and $E/Z(E)$ is

Received by the editors June 23, 2003 and, in revised form, October 29, 2003.
2000 *Mathematics Subject Classification.* Primary 20C15.

irreducible under the action of σ . Therefore, we conclude that χ is not monomial, and hence, G is not an M -group. \square

Lemma 2.2. *Let N be a normal subgroup of G , and let φ be a linear character of N . Write T for the stabilizer of φ in G , and assume that φ extends to $\hat{\varphi} \in \text{Irr}(T)$. Given a character $\eta \in \text{Irr}(T/N)$, the character $(\hat{\varphi}\eta)^G$ is monomial if and only if η is monomial. Furthermore, every character in $\text{Irr}(G|\varphi)$ is monomial if and only if T/N is an M -group.*

Proof. By Gallagher's theorem, we know that $\hat{\varphi}\eta \in \text{Irr}(T|\varphi)$, and by Clifford's theorem, $\chi = (\hat{\varphi}\eta)^G$ is irreducible. Using Lemma 4.1 of [2] (or Problem 6.11 of [4]), we see that χ is monomial if and only if $\hat{\varphi}\eta$ is monomial. Suppose S is a subgroup of T and $\sigma \in \text{Irr}(S)$ so that $\sigma^T = \eta$. It is known that $(\hat{\varphi}_S\sigma)^T = \hat{\varphi}\eta$ (see Problem 5.3 of [4]). It follows that $\hat{\varphi}\eta$ is monomial if and only if η is monomial. The last conclusion is an immediate consequence of the previous one, and this proves the lemma. \square

Lemma 2.3. *Let p be an odd prime so that 3 divides $p+1$. Let E be an extra-special p -group of order p^5 and exponent p . Then E has an automorphism σ of order 3 with centralizer $Z(E)$, and E has a maximal abelian subgroup A that is normal in E and σ -invariant. If G is the semi-direct product $E\langle\sigma\rangle$, then G is an M -group.*

Proof. We know that 3 divides $p^2 - 1$. We can view E as the central product of E_1 and E_2 where E_1 and E_2 are both extra-special groups of order p^3 and exponent p . Since 3 divides $p^2 - 1$, it follows that E_1 and E_2 each have an automorphism of order 3 with each having centralizer $Z = Z(E)$. Applying these to the central product, we get the automorphism σ of E with order 3 and centralizer Z . We let $T = \langle\sigma\rangle$, and we note that $C_E(T) = Z$. It suffices to find an abelian T -invariant subgroup $A \subseteq E$ of index p^2 . (Note that this will prove that G is an M -group.)

Let U/Z be an irreducible T -submodule of E/Z . Then U/Z has order p^2 since 3 does not divide $p - 1$. If U is abelian, then we are done, so we assume U is nonabelian. Let $V = C_E(U)$. Then $U \cap V = Z$, and E/Z is the direct sum of the irreducible modules U/Z and V/Z . Note that V must be nonabelian.

Take x to be an element of U that does not lie in Z , and write $y = x^\sigma$. Then x and y generate U , so they do not commute. Let $z = [x, y]$, and observe that $Z = \langle z \rangle$. Then $y^\sigma \in x^{-1}y^{-1}Z$.

Let r be an element of V that does not lie in Z , and write $s = r^\sigma$. We see that r and s generate V , so they do not commute, and hence, $[r, s]$ is a nonidentity element of Z . We see that $s^\sigma \in r^{-1}s^{-1}Z$. Suppose that $[r, s] = z^{-1}$. We observe that $(xr)^\sigma = ys$, and we compute $[xr, ys] = [x, y][r, s] = zz^{-1} = 1$. Also, $(ys)^\sigma \in (x^{-1}y^{-1})(r^{-1}s^{-1})Z = (xr)^{-1}(ys)^{-1}Z \subseteq \langle xr, ys \rangle$. We conclude that $\langle xr, ys \rangle$ is a σ -invariant abelian subgroup of E of index p^2 , and we will be done.

The idea is to choose r properly. We pick any element $v \in V - Z$, and let $w = v^\sigma$. Note that $w^\sigma \in v^{-1}w^{-1}Z$. We know that $[v, w] = z^a$ for some integer a with $1 \leq a \leq p - 1$. We consider elements of the form $v^i w^j$, and we see that $(v^i w^j)^\sigma Z = w^i v^{-j} w^{-j} Z = v^{-j} w^{i-j} Z$. It follows that

$$[v^i w^j, (v^i w^j)^\sigma] = [v^i w^j, v^{-j} w^{i-j}] = (z^a)^{i(i-j)-j(-j)} = z^{a(i^2-ij+j^2)}.$$

We need to show that as i and j vary over Z/pZ , the quantity $i^2 - ij + j^2$ takes on all values in Z/pZ .

For any value $b \in Z/pZ$, we consider the equation $i^2 - ij + j^2 = b$. We take the equation $i^2 - ij + j^2 - b = 0$, and we solve for i . By the quadratic formula, we can do this if the discriminant is a square. The discriminant is $j^2 - 4(j^2 - b) = 4b - 3j^2$. We want to find k so that $4b - 3j^2 = k^2$. As j and k vary through the p possible values in Z/pZ , we see that $4b - 3j^2$ and k^2 each take on $(p+1)/2$ different values. Since there are only p possible values in Z/pZ , there must be an overlap between these two sets. We now fix b so that $ab = -1$ modulo p . The work we have just done shows that we can find i and j so that $i^2 - ij + j^2 = b$ modulo p . We take $r = v^i w^j$, and we see that $s = r^\sigma$. The work we did earlier shows that $[r, s] = z^{a(i^2 - ij + j^2)} = z^{ab} = z^{-1}$. We now conclude that E has a normal σ -invariant subgroup of index p^2 , so the lemma is proved. \square

3. THE CONSTRUCTION

We suppose that p and q are distinct odd primes so that p divides $q - 1$ and 3 divides $p + 1$. Then $q = 1 + pk$ for some integer k . Hence $(q^p - 1)/(q - 1) = 1 + q + \dots + q^{p-1} \equiv 1 + (1 + pk) + \dots + (1 + (p - 1)pk) = p + ((p - 1)p^2 k/2) \pmod{p^2}$. Thus $(q^p - 1)/(q - 1) = pr$, where $r \equiv 1 \pmod{p}$. In particular, $(p, r) = 1$. Next we claim that 3 does not divide r . It is known that the gcd of $q - 1$ and $(q^p - 1)/(q - 1)$ must divide p , so if 3 divides $q - 1$, then 3 will not divide $(q^p - 1)/(q - 1)$. On the other hand, we know that the order of q modulo 3 must divide 2 , so if 3 does not divide $q - 1$, then the order of q modulo 3 is 2 . Since 2 does not divide p , it cannot be that q^p is congruent to 1 modulo 3 , so 3 does not divide $(q^p - 1)/(q - 1)$.

We mention that there exist pairs of primes with the properties mentioned in the previous paragraph. One such pair of primes is $p = 5$ and $q = 11$. Observe that $(11^5 - 1)/(11 - 1) = 5 \cdot 3221$.

Let F be the finite field of order q^p . Take V to be the additive group of F , so V is an elementary abelian q -group. Let N be the subgroup of order $(q^p - 1)/(q - 1) = pr$ in the multiplicative group of F . Multiplication in F provides a natural action of N on V via automorphisms. The orbits in this action correspond to the cosets of the subgroup of order $q - 1$ in the multiplicative group of F . Fix $s, t \in N$ so that $o(s) = p$ and $o(t) = r$, and note that $N = \langle st \rangle$. Let a be a generator for the Galois group of F over the field of order q so that a has order p . The Galois action provides a natural action for a on V and N . Note that the fixed field for a is the field of order q , so each orbit of N on V is stabilized by a . Since p divides $q - 1$, it follows when s is viewed as an element of F that s lies in the fixed field, so a will centralize s .

Let Q be an extra-special p -group of order p^5 and exponent p . Let Z be the center of Q , and suppose that Z is generated by z . We can fix the generators of Q to be x_0, y_0, x_1, y_1 so that $x_0^p = y_0^p = x_1^p = y_1^p = z^p = 1$ and $[x_0, y_0] = [x_1, y_1] = z$. We define $Q_0 = \langle x_0, y_0 \rangle$ and $Q_1 = \langle x_1, y_1 \rangle$. Let K be an elementary abelian group of order p^2 that is generated by x_2 and y_2 . It is not difficult to see that $E = Q \times K$ has an automorphism σ of order 3 that centralizes Z and is defined by

$$x_0^\sigma = y_0, y_0^\sigma = x_0^{-1}y_0^{-1}, x_1^\sigma = y_1, y_1^\sigma = x_1^{-1}y_1^{-1}, x_2^\sigma = y_2, y_2^\sigma = x_2^{-1}y_2^{-1}.$$

We define M to be the semi-direct product arising from σ acting on E .

We set $U = V \langle t \rangle$. We define an action of Q on U whose kernel is Q_0 by $u^{x_1} = u^a$ and $u^{y_1} = u^s$ for all $u \in U$. We define an action of K on U by $u^{x_2} = u^{a^{-1}}$ and $u^{y_2} = u^s$ for all $u \in U$. We set $U_0 = U \times U^\sigma \times U^{\sigma^2}$. We define an action of M

on U_0 by $(u^{\sigma^i})^x = u^{(\sigma^i x \sigma^{-i})\sigma^i}$ for all $u \in U, x \in M$, and $i = 1, 2$. Our group G is the resulting semi-direct product of M acting on U_0 . Observe that $|U| = q^p r$ and $|M| = p^7 3$, so $|G| = q^{3p} r^3 p^7 3$. Take $V_0 = V \times V^\sigma \times V^{\sigma^2}$, and let H be the semi-direct product of M acting on V_0 . We see that $|H| = q^{3p} p^7 3$ and $|G : H| = r^3$, so H is a Hall subgroup of G . (Obviously, q does not divide r , the choice of p precludes p from dividing r , and we showed that 3 does not divide r ; so $(r^3, q^{3p} p^7 3) = 1$.) We will show that G is an M -group and H is not an M -group. Also, we take L to be the semi-direct product of M acting on $\langle t \rangle \times \langle t^\sigma \rangle \times \langle t^{\sigma^2} \rangle$. Observe that L acts coprimely on V_0 .

Lemma 3.1. *H is not an M -group.*

Proof. Let $A = Q_0 \langle x_1 x_2, y_1 y_2^{-1} \rangle$. It is not difficult to see that A is the kernel of the action of E on $\text{Irr}(V)$. Furthermore, since E/A is abelian, it must have a regular orbit in $\text{Irr}(V)$. So we can find a character $\lambda \in \text{Irr}(V)$ with $C_E(\lambda) = A$. Let $\varphi = \lambda \times \lambda^\sigma \times \lambda^{\sigma^2}$. We see that $C_E(\varphi) = A \cap A^\sigma \cap A^{\sigma^2}$. It follows that $Q_0 \subseteq C_E(\varphi)$. Also, A is not σ -invariant, so $|E : C_E(\varphi)| > |E : A| = p^2$. We obtain $|C_E(\varphi) : Q_0| < p^2$, and we conclude that $C_E(\varphi) = Q_0$. Since σ will stabilize φ , we have $C_M(\varphi) = Q_0 \langle \sigma \rangle$, and $C_M(\varphi)$ is not an M -group by Lemma 2.1.

Let T be the stabilizer of φ in H . It follows that $T = V_0 C_M(\varphi)$. Since $(|V_0|, |T : V_0|) = 1$, we know φ extends to $\hat{\varphi} \in \text{Irr}(T)$. Since $T/V_0 \cong C_M(\varphi)$, we can find a character $\eta \in \text{Irr}(T/V_0)$ that is not monomial. We know that $(\hat{\varphi}\eta)^H$ is irreducible, and it is not monomial by Lemma 2.2. Therefore, H is not an M -group. \square

Lemma 3.2. *G is an M -group.*

Proof. Using Lemma 2.3, it is not difficult to show that $M \cong G/U_0$ is an M -group. To show G is an M -group, it suffices to show that every character in $\text{Irr}(G)$ whose kernel does not contain U_0 is monomial.

Suppose $\chi \in \text{Irr}(G)$ and U_0 is not contained in $\text{Ker}(\chi)$. For now, we will assume that V_0 is contained in $\text{Ker}(\chi)$. Let φ be an irreducible constituent of χ_{U_0} , and notice that $\varphi \in \text{Irr}(U_0/V_0)$. Let T be the stabilizer of φ in G , and observe that $(|U_0 : V_0|, |T : U_0|) = 1$, so φ extends to $\hat{\varphi} \in \text{Irr}(T)$. By Lemma 2.2, it suffices to prove that T/U_0 is an M -group. If 3 does not divide $|T : U_0|$, then T/U_0 is a p -group, and we are done. Thus, we may assume that 3 divides $|T : U_0|$, and by conjugating, we may assume that $\sigma \in T$. This implies that $\varphi = \nu \times \nu^\sigma \times \nu^{\sigma^2}$ for some character $\nu \in \text{Irr}(U/V)$. Observe that $T = U_0 C_M(\varphi)$ and $C_M(\varphi) = C_E(\varphi) \langle \sigma \rangle$. Furthermore, we have $C_E(\varphi) = C_E(\nu) \cap C_E(\nu)^\sigma \cap C_E(\nu)^{\sigma^2} = C_E(\nu) \cap C_E(\nu)^\sigma$. It is not difficult to see that $|E : C_E(\nu)| = p$ and $C_E(\nu) \cap C_E(\nu)^\sigma$ is an extra-special p -group of order p^5 . Thus, $C_M(\varphi)$ is an M -group by Lemma 2.3.

Finally, we assume that V_0 is not contained in the kernel of χ . Let δ be an irreducible constituent of χ_{V_0} . Let S be the stabilizer of δ in G . Again, $(|V_0|, |S : V_0|) = 1$, so δ extends to $\hat{\delta} \in \text{Irr}(T)$, and we see using Lemma 2.2 that it suffices to show that S/V_0 is an M -group. If 3 does not divide $|S : V_0|$, then $S/(S \cap U_0)$ is a p -group and $(S \cap U_0)/V_0$ is abelian. By Theorem 6.23 of [4], this will force S/V_0 to be an M -group. We suppose that 3 does not divide $|S : V_0|$, and by conjugating, we may assume that $\sigma \in S$. This implies that $\delta = \lambda \times \lambda^\sigma \times \lambda^{\sigma^2}$ for some nonprincipal character $\lambda \in \text{Irr}(V)$.

We know that $\langle t \rangle$ acts Frobeniusly on V , so no nonidentity element in $\langle t \rangle$ will stabilize λ . It follows that $C_{\langle t \rangle E}(\lambda)$ is a p -subgroup, so we can find an element

$h \in \langle t \rangle$ so that $A = C_{\langle t \rangle E}(\lambda^h) \subseteq E$. Recall that the orbits in V under the action of $\langle t \rangle E$ have size pr . It is not difficult to see that the orbits in V have the same size, so $|\langle t \rangle E : A| = pr$, and hence, A has index p in E .

Let $\delta' = \lambda^h \times (\lambda^\sigma)^{h^\sigma} \times (\lambda^{\sigma^2})^{h^{\sigma^2}}$ and observe that $\delta' = \delta^{(h, h^\sigma, h^{\sigma^2})}$. Observe that $C_E(\delta') = A \cap A^\sigma \cap A^{\sigma^2} = A \cap A^\sigma$. We note that A is not σ -invariant so $A \cap A^\sigma \subset A$. On the other hand, A is normal in E of index p , so $A \cap A^\sigma$ will be normal in E of index p^2 , and $|A \cap A^\sigma| = p^5$. Since K is not contained in A , we have $K \times Q_0 \neq A \cap A^\sigma$, and we conclude that $C_E(\delta') = A \cap A^\sigma$ is an extra-special group of order p^5 . Now, $C_M(\delta') = C_L(\delta')$ is a conjugate of $C_L(\delta)$ that lies in M , so $C_M(\delta') = C_E(\delta')\langle \sigma \rangle$, and $C_M(\delta')$ is an M -group by Lemma 2.3. It follows that $S/V_0 \cong C_M(\delta)$ is an M -group. This proves the theorem. \square

4. ANOTHER CONSTRUCTION

We observe that Lemma 2.3 is still true if E is replaced by a central product of two quaternion groups of order 8. We can change the construction in Section 3 by taking $p = 2$ and q to be an odd prime so that $q + 1 = 2r$ where r is relatively prime to 6. (The first such prime $q = 13$.) We take Q to be the central product of two quaternion groups of order 8, and we make the appropriate changes in the generators of Q . The rest of the argument will go through for this construction.

ACKNOWLEDGMENTS

I wish to thank Mark L. Lewis for his many helpful suggestions, both for revising my presentation and generalizing the example. I also wish to thank Masayuki Wajima for providing me his preprint.

REFERENCES

- [1] E.C.Dade. Normal subgroups of M -groups need not be M -groups. *Math. Z.* 133(1973), 313-317. MR 0325748 (48:4094)
- [2] E.C.Dade. Monomial characters and normal subgroups. *Math. Z.* 178(1981), 401-420. MR 0635210 (83e:20014)
- [3] L.Dornhoff. M -groups and 2-groups. *Math. Z.* 100(1967), 226-256. MR 0217174 (36:265)
- [4] I.M.Isaacs. Character theory of finite groups. Academic Press, San Diego, California, 1976. MR 0460423 (57:417)
- [5] I.M. Isaacs, Primitive characters, normal subgroups, and M -groups, *Math. Z.* 177(1981), 267-284. MR 0612879 (82f:20026)
- [6] R.W.Van der Waall. On the embedding of minimal non- M -groups. *Indag. Math.* 36(1974), 157-167. MR 0352237 (50:4724)

DEPARTMENT OF MATHEMATICS, FACULTY OF EDUCATION, GUNMA UNIVERSITY MAEBASHI,
 GUNMA 371-8510, JAPAN
E-mail address: fukusima@edu.gunma-u.ac.jp