TRANSITIVE PERMUTATION GROUPS IN WHICH ALL DERANGEMENTS ARE INVOLUTIONS

I. M. Isaacs
Department of Mathematics, University of Wisconsin
Madison, WI 53706 USA
e-mail: isaacs@math.wisc.edu

Thomas Michael Keller
Department of Mathematics, Texas State University
601 University Drive,
San Marcos, TX 78666-4616 USA
e-mail: keller@txstate.edu

Mark L. Lewis
Department of Mathematical Sciences, Kent State University
Kent, OH 44242 USA
e-mail: lewis@math.kent.edu

Alexander Moretó
Departament d'Àlgebra, Universitat de València
46100 Burjassot. València SPAIN
e-mail: Alexander.Moreto@uv.es

Abstract. Let G be a transitive permutation group in which all derangements are involutions. We prove that G is either an elementary abelian 2-group or is a Frobenius group having an elementary abelian 2-group as kernel. We also consider the analogous problem for abstract groups, and we classify groups G with a proper subgroup H such that every element of G not conjugate to an element of H is an involution.

MSC (2000): Primary 20B10; Secondary 20D99

The research of the fourth author was partially supported by the Spanish Ministerio de Ciencia y Tecnología and the Programa Ramón y Cajal.

1 Introduction.

Recall that a permutation without fixed points is called a *derangement.* An easy and well known counting argument shows that every finite transitive permutation group on a set with more than one element must contain a derangement. In fact, it is not hard to show that the number of derangements in a nontrivial transitive permutation group is at least as large as the order of a point stabilizer. (See, for instance [3].)

What are the orders of the derangements in a nontrivial transitive permutation group G? Using the classification of finite simple groups, B. Fein, W. Kantor and M. Schacher [6] have shown that G must contain a derangement of prime-power order. In fact, in most cases, there is a derangement of prime order. (Transitive groups that fail to have a derangement of prime order were studied in [7].)

In this note, we consider transitive permutation groups in which all derangements are involutions. Our main result is the following.

Theorem A. *Let G be a transitive permutation group and suppose that every derangement in G is an involution. Then one of the following holds.*

(i) *G is an elementary abelian 2-group.*

(ii) *G is a Frobenius group whose Frobenius kernel is an elementary abelian 2-group.*

It seems reasonable to ask if an analogous result might be true for groups in which all derangements have some common prime order different from 2. The following shows that if such a result exists, it will necessarily be more complicated. Consider, for example, the semidirect product G of $\mathrm{SL}(2,p)$ with its natural module, and let G act on the right cosets of $\mathrm{SL}(2,p)$. It is not hard to see that if $p > 2$ in this situation, then all derangements have order p. In particular, if $p > 3$, then a transitive group in which all derangements have order p does not even need to be solvable.

If we reinterpret Theorem A in the setting of abstract groups, we can obtain a somewhat sharper result. Given a subgroup H of a finite group G, the elements of G that are not contained in any conjugate of H correspond to the derangements in a permutation group, and so we refer to these elements as the *H-derangements* of G. (If H is proper in G, then H-derangements necessarily exist.) We give necessary and sufficient conditions for all H-derangements to be involutions.

Of course, the case where $H = G$ is without interest. If $|G : H| = 2$, then H is normal in G, and so the set of H-derangements in G is exactly $G - H$. It is well known that in this case, $G - H$ consists of involutions precisely when there is some involution $t \in G - H$ such that conjugation by t inverts the elements of H. This can happen, of course, only if H is abelian.

The following result gives all possibilities when $|G : H| > 2$.

Theorem B. *Let H be a subgroup of a finite group G and assume that $|G : H| > 2$. Then all H-derangements in G are involutions if and only if one of the following holds.*

(i) *G is an elementary abelian 2-group.*

(ii) *G has a normal elementary abelian Sylow 2-subgroup T and $N = H \cap T$ is the core of H in G. Also, G/N is a Frobenius group with complement H/N and kernel T/N.*

We thank Gary Seitz, Ron Solomon and Don White for helpful comments. Most of this work was done while the second, third and fourth authors were visiting the University of Wisconsin, Madison. They thank the Mathematics Department for its hospitality. The research of the second and third authors was done while on sabbatical leave from their universities. They thank their universities for the time on sabbatical.

2 Simple groups.

Recall that if H is a proper subgroup of G, then G necessarily contains an H-derangement. In this section, we use the classification of simple groups to prove the following.

Theorem 2.1. *Let G be a finite simple group of order exceeding 2 and suppose that $H < G$ is a proper subgroup. Then G contains an H-derangement that is not an involution.*

It certainly would be pleasant to have an elementary and transparent proof of Theorem 2.1. Although it seems reasonable that such a proof might exist, we have been unable to find one, and the argument we present here depends heavily on the simple-group classification. Once we have proved Theorem 2.1, however, we shall have no further need for the classification in this paper.

We begin with an elementary and general result.

Lemma 2.2. *Suppose the group G has a proper subgroup H such that all H-derangements are involutions. If t is one of these involutions, then H and t satisfy the following.*

(i) *t is not conjugate to an element of H.*

(ii) *t is not the square of any element in G.*

(iii) *$\mathbf{C}_G(t)$ is a 2-group.*

(iv) *$|H|$ is divisible by every odd prime divisor of $|G|$.*

Proof. Conclusion (i) is clear. Since t lies in no conjugate of H, it follows that if t is a power of some element $x \in G$, then x also lies in no conjugate of H. Then x is an H-derangement, and so it is an involution. In particular, $x^2 \neq t$ and (ii) follows.

If $\mathbf{C}_G(t)$ is not a 2-group, it contains an element y of some odd prime order p. Then $(ty)^p = t$, and thus t is a power of the element ty, which is not an involution. This contradicts the result of the previous paragraph, and so conclusion (iii) follows.

Finally, if p is an odd prime divisor of $|G|$, then G contains an element u of order p. Since u is not an involution, it must lie in some conjugate of H, and thus p divides $|H|$, proving (iv). $\square$

We say that a group G satisfies $(*)$ if there exist a subgroup $H < G$ and an involution $t \in G$ such that conclusions (i)–(iv) of Lemma 2.2 hold. Since the assertion of Theorem 2.1 is clearly valid if G has prime order $p > 2$, it suffices to prove that no nonabelian simple group satisfies $(*)$.

First, we show that there are relatively few simple groups having an involution that satisfies conclusion (iii) of Lemma 2.2. The following summarizes the information that we need from the classification.

Lemma 2.3. *Assume that G is a nonabelian simple group and that $t \in G$ is an involution such that $\mathbf{C}_G(t)$ is a 2-group. Then G is one of the following.*

(i) $\mathrm{PSL}(2, q)$, *where* $q > 5$ *is a Fermat prime, a Mersenne prime, or* 9.

(ii) $\mathrm{PSL}(2, 2^f)$, *where* $f \geq 2$.

(iii) $\mathrm{PSL}(3, 2^f)$, *where* $f \geq 1$.

(iv) $\mathrm{PSU}(3, 2^f)$, *where* $f \geq 2$.

(v) $\mathrm{Sp}(4, 2^f)$, *where* $f \geq 1$.

(vi) $\mathrm{Sz}(2^f)$, *where* $f \geq 3$ *is odd.*

Proof. We can check using the Atlas [4] that neither the Tits group nor any of the sporadic simple groups has an involution whose centralizer is a 2-group. Also, if $t \in \mathrm{Alt}(n)$ is an involution, where $n \geq 7$, then either t can be written as a product of at least four disjoint transpositions or else t fixes at least three points. In either case, the centralizer of t in G contains an element of order 3. It follows that we need to consider only simple groups of Lie type.

Tables 4.5.1 and 4.5.2 of [8] list all involutions and their centralizers for the groups of Lie type in odd characteristic. One sees from those tables that the only simple groups of Lie type in odd characteristic that have an involution whose centralizer is a 2-group are the groups of the form $\mathrm{PSL}(2, q)$ with q a Fermat prime, a Mersenne prime, or 9. All of these groups except $PSL(2, 5)$ appear in case (i) of the lemma, and since $PSL(2, 5) \cong PSL(2, 4)$, that group occurs in case (ii).

Unfortunately, we have found no corresponding tables for simple groups of Lie type in characteristic 2, but the information we need about the centralizers of involutions in these groups is contained in the long paper [1]. (Also, see [2]). It is possible to deduce our result by sifting through the data in those papers. $\square$

It is now easy to complete the proof of Theorem 2.1 by showing that a nonabelian simple group cannot satisfy $(*)$.

Theorem 2.4. *No nonabelian simple group satisfies* $(*)$.

Proof. Suppose G is a nonabelian simple group that satisfies $(*)$. Thus G has a proper subgroup H and an involution t that satisfy conclusions (i)-(iv) of Lemma 2.2, and in particular, we see that G must be one of the groups that appear in the statement of Lemma 2.3.

We begin by noting that with the exception of the groups $Sp(4, 2^f)$ of case (v) of Lemma 2.3, each of the simple groups mentioned in that lemma has a unique conjugacy class of involutions. But (as is well known) the Sylow 2-subgroups of all groups in cases (i), (iii), (iv) and (vi) of Lemma 2.3 contain elements of order 4, and it follows that all of the involutions in these simple groups are squares. None of these groups, therefore, can be our group G, which satisfies $(*)$.

Suppose G is one of the groups named in case (ii) of Lemma 2.3. Then as we have mentioned, G has a unique class of involutions, and it follows that the subgroup H contains no involution, and so it has odd order. Since G is $PSL(2, 2^f)$, we can use Dickson's classification of the subgroups of these groups (see Hauptsatz II.8.27 of [9]) to deduce that each subgroup of odd order of G has order dividing either $2^f - 1$ or $2^f + 1$, and so each such subgroup has order coprime to one of these two numbers. By $(*)$, however, we know, that $|H|$ is divisible by every odd prime divisor of $|G|$, and this is a contradiction since both $2^f + 1$ and $2^f - 1$ divide $|G|$, and these numbers exceed 1.

The only remaining possibility is that G is $\mathrm{Sp}(4, 2^f)$ with $f \geq 1$. Although $\mathrm{Sp}(4, 2^f)$ has three conjugacy classes of involutions, only one of these classes contains elements whose centralizers are 2-groups. To complete the proof, we show that the involutions in that class are squares in $\mathrm{Sp}(4, 2^f)$, and thus conclusion (ii) of Lemma 2.2 fails.

According to Table IV.1 of [5], the matrix

$$t = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

is a representative of the class of involutions whose centralizer is a Sylow 2-subgroup of $\mathrm{Sp}(4, 2^f)$. Looking at Table IV.1 of [5], we see that

$$s = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

is another element of $\mathrm{Sp}(4, 2^f)$. An easy computation shows that $s^2 = t$, and this completes the proof. $\square$

3 The main results.

The following contains the information we need to prove Theorems A and B.

Theorem 3.1. *Let $H < G$ and suppose that all H-derangements in G are involutions. Writing N to denote the core in G of H, we have the following.*

(i) *Conjugation by an H-derangement inverts the elements of N.*

(ii) *G/N has an elementary abelian normal Sylow 2-subgroup T/N.*

(iii) *H/N is a complement for T/N in G/N.*

(iv) *If $T < G$, then G/N is a Frobenius group with kernel T/N and complement H/N.*

Proof. To prove (i), suppose that $t \in G$ is an H-derangement, and let $x \in N$. Since t lies in no conjugate of H and x lies in every conjugate of H, it follows that xt lies in no conjugate of H, and thus by hypothesis, xt is an involution. Then $1 = xtxt = xx^t$, and so t inverts x, as wanted.

Observe that the canonical homomorphism $G \to G/N$ maps the set of H-derangements in G onto the set of (H/N)-derangements in G/N, and so the latter set consists of involutions. It follows that to prove (ii), (iii) and (iv), we can replace G by G/N, and so we can assume $N = 1$.

We work next to prove (ii) and (iii) by induction on $|G|$. Note that G is nontrivial since H is proper, and so we can choose a maximal normal subgroup M of G. Suppose first that $MH < G$, and write $K = MH$. Then all K-derangements in G are H-derangements, and hence they are involutions. Reasoning as we did in the previous paragraph, we see that all (K/M)-derangements in the simple group G/M are involutions. Since $K/M < G/M$, we conclude by Theorem 2.1 that $|G/M| = 2$, and so $K = M \lhd G$.

Now fix a K-derangement t and observe that $G = \langle K, t\rangle$ since $|G : K| = 2$ and $t \notin K$. By assertion (i), with K in place of both H and N, we see that t inverts the elements of K. It follows that K is abelian and that t normalizes every subgroup of K. Thus $H \lhd \langle K, t\rangle = G$, and so $H = N = 1$. Every nonidentity element of G, therefore, is an H-derangement, and hence is an involution. In this case, G is an elementary abelian 2-group, and conclusions (ii) and (iii) hold with $T = G$.

We can now assume that $MH = G$, and we write $D = M \cap H$, so that $D < M$. Let L be the core in M of D, and note that $L \subseteq D \subseteq H$. Since M normalizes L and $MH = G$, it follows that all G-conjugates of L are H-conjugates, and hence they lie in H. We conclude that L is contained in all conjugates of H, and so $L \subseteq N = 1$.

Now H normalizes D and since $MH = G$ it follows that all G-conjugates of D are M-conjugates. If x is a D-derangement in M, therefore, then x lies in no G-conjugate of D, and hence it lies in no G-conjugate of H. This shows that all D-derangements in M are H-derangements, and hence they are involutions. We can thus apply the inductive hypothesis in M, with D in place of H. Since the core of D in M is trivial, we know that a Sylow 2-subgroup T of M is elementary abelian and normal in M, and hence it is normal in G. By the inductive hypothesis, we also know that D complements T in M, and so $TD = M$. Then $G = MH = TDH = TH$. Since T is abelian and normal in G, it follows that $T \cap H \lhd G$. But H has trivial core in G, and hence $T \cap H = 1$.

At this point, we know that the Sylow 2-subgroup T of M is elementary abelian and normal in G, and that it is complemented in G by H. To complete the proof of (ii) and (iii), it suffices to show that T is a full Sylow 2-subgroup of G, or equivalently, that H has odd order.

Suppose that $|H|$ is even and choose an involution $s \in H$. Since $T \lhd G$ and $TH = G$, we see that $\mathbf{C}_H(T) \lhd G$, and thus $\mathbf{C}_H(T) = 1$. We can therefore choose an element $t \in T$ that fails to commute with s. Let $x = st$, and observe that since s and t are noncommuting involutions, $x^t = x^{-1}$ and x has order $o(x) > 2$. By hypothesis, therefore, x is not an H-derangement, and so it lies in some conjugate H^g of H. Now $[x,t] = x^{-1}x^t = x^{-2} \in H^g$ and also $[x,t] \in T$ since $T \lhd G$. Then $x^{-2} \in T \cap H^g = (T \cap H)^g = 1$, and this is a contradiction since we know that $o(x) > 2$. It follows that $|H|$ is odd, as wanted.

Finally, to prove (iv), assume that $T < G$. To show that G is a Frobenius group with kernel T and complement H as required, it suffices to show that no nonidentity element of T commutes with any nonidentity element of H. We suppose, therefore, that h and t commute, where $1 \neq t \in T$ and $1 \neq h \in H$. Since $o(t) = 2$ and $o(h) > 2$, we see that $o(th) > 2$. Then th is not an H-derangement, and hence it lies in some conjugate of H. This is a contradiction, however, since $|H|$ is odd but $o(th)$ is even. $\square$

The following is Theorem A.

Corollary 3.2. *Let G be a transitive permutation group and suppose that every derangement in G is an involution. Then one of the following occurs:*

(i) *G is an elementary abelian 2-group.*

(ii) *G is a Frobenius group whose Frobenius kernel is an elementary abelian 2-group.*

Proof. We can assume that G is nontrivial, and thus a point stabilizer H is a proper subgroup. Also, the core of H in G is trivial, and so the result follows by conclusion (iv) of Theorem 3.1. □

Finally, we prove Theorem B, which we restate.

Theorem 3.3. *Let H be a subgroup of a finite group G and assume that $|G : H| > 2$. Then all H-derangements in G are involutions if and only if one of the following holds.*

(i) *G is an elementary abelian 2-group.*

(ii) *G has a normal elementary abelian Sylow 2-subgroup T and $N = H \cap T$ is the core of H in G. Also, G/N is a Frobenius group with complement H/N and kernel T/N.*

Proof. If (i) holds, then obviously all H-derangements are involutions, so we assume now that (ii) holds. It is well known that a Frobenius group is the union of its kernel and all conjugates of its complement, and it follows that every H-derangement in G lies in T. These H-derangements are therefore involutions, as required.

Conversely, suppose that all H-derangements in G are involutions and let N be the core of H in G. We know by Theorem 3.1 that G/N has a normal elementary abelian Sylow 2-subgroup T/N and that if $T < G$, then G/N is a Frobenius group with kernel T/N and complement H/N. In particular, $T \cap H = N$, and so to complete the proof, it suffices to show that T is an elementary abelian 2-group.

Since $T \triangleleft G$ and $N \triangleleft G$, it follows that the intersection of each conjugate of H with T is N. All elements of $T - N$, therefore, are H-derangements and hence are involutions. To complete the proof, therefore, it suffices to show that $x^2 = 1$ for every element $x \in N$.

Now $|T/N| = |G : H| > 2$, and thus we can choose elements $s, t \in T - N$ lying in different cosets of N. Writing $u = st^{-1}$, we see that u also lies in $T - N$, and so s, t and u are H-derangements. If $x \in N$, therefore, it follows by conclusion (i) of Theorem 3.1 that each of s, t and u inverts x. Then $x^{-1} = x^u = x^{st^{-1}} = x$, and so $x^2 = 1$. as required. $\square$

References

[1] M. Aschbacher and G. M. Seitz, "Involutions in Chevalley groups over fields of even order", *Nagoya Math. J.* **63** (1976), 1–91.

[2] M. Aschbacher and G. M. Seitz, "Corrections to 'Involutions in Chevalley groups over fields of even order' ", *Nagoya Math. J.* **72** (1978), 135–136.

[3] P. J. Cameron, A. M. Cohen, "On the number of fixed point free elements in a permutation group", *Discrete Math.* **106/107** (1992), 135–138.

[4] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of Finite Groups,* Oxford University Press, London, 1984.

[5] H. Enomoto, "The characters of the finite symplectic group $\mathrm{Sp}(4, q), q = 2^f$", *Osaka J. Math.* **9** (1972), 75–94.

[6] B. Fein, W. Kantor, M. Schacher, "Relative Brauer groups. II", *J. Reine Angew. Math.* **328** (1981), 39–57.

[7] M. Giudici, "Quasiprimitive groups with no fixed point free elements of prime order", *J. London Math. Soc.* **67** (2003), 73–84.

[8] D. Gorenstein, R. Lyons, and R. Solomon, *The Classification of the Finite Simple Groups 3*, American Mathematical Society, Providence, 1998.

[9] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin 1967.