TOTALLY VARIANT SETS IN FINITE GROUPS AND VECTOR SPACES

FREDERICK HOFFMAN AND LLOYD R. WELCH

1. Introduction. We are concerned here with the question of which finite groups and vector spaces possess subsets which are moved by every non-identity automorphism (in the vector-space case—non-singular linear transformation). We find that this is the case for all but four finite-dimensional vector spaces (2-, 3-, and 4-dimensional space over Z_2, 2-dimensional space over Z_3), and for all finite groups except for those corresponding to the vector-space exceptions, and the quaternion group of order eight. The question was first posed to the authors, in the vector-space case, by Morris Marx. Leonard Baum suggested the type of argument used in the proof of Lemma 1 of § 2.

Definitions.

1. Let $\mathfrak{S}$ be a subset of the finite group $\mathfrak{G}$, $\mathfrak{S}$ not containing the identity of $\mathfrak{G}$. If $\mathfrak{S}$ has the property that the only automorphism ϕ of $\mathfrak{G}$ with $\mathfrak{S}\phi = \mathfrak{S}$ is the identity automorphism, then $\mathfrak{S}$ is a *totally variant* subset of $\mathfrak{G}$. ($\mathfrak{S}$ is totally variant in $\mathfrak{G}$.)

2. Let $\mathfrak{S}$ be a subset of the vector space V, $\mathfrak{S}$ not containing the zero element of V. If $\mathfrak{S}$ has the property that the only non-singular linear transformation T of V with $\mathfrak{S}T = \mathfrak{S}$ is the identity transformation, then $\mathfrak{S}$ is a totally variant subset of V. We note the following:

(1) The omission of the identity (zero) element from totally variant sets is simply a convenience for proofs.

(2) The complement of a totally variant subset is totally variant.

(3) Any group (vector space) having a totally variant subset has a totally variant generating set.

(4) (Pointed out by E. C. Paige.) The group $\mathfrak{G}$ has a totally variant subset if and only if the right regular representation is a constituent of the permutation representation of the automorphism group of $\mathfrak{G}$ on the power set of $\mathfrak{G}$; i.e., there is an element of the power set whose images under distinct automorphisms are distinct.

2. Preliminary lemmas. We begin by stating some rough results arrived at by counting.

LEMMA 1. *Every vector space of dimension seven or greater over Z_2 has a totally variant subset.*

Received October 24, 1966.

https://doi.org/10.4153/CJM-1968-068-5 Published online by Cambridge University Press

Proof. We shall compute an upper bound for the number of subsets which have at least one non-singular transformation other than the identity leaving them invariant. The bound will be less than the total number of subsets. Therefore there must be at least one totally variant subset.

Let V be of dimension $n \geqslant 7$ over Z_2. The number of non-singular linear transformations of V is

$$l(n) = \prod_{k=0}^{n-1} (2^n - 2^k) = 2^{n^2} \cdot \prod_{k=1}^{n} (1 - 2^{-k}) < 2^{n^2} \cdot \frac{3}{8}.$$

The number of subsets of V left invariant by the non-identity transformation ϕ is $2^{\mathfrak{D}(\phi)}$, where $\mathfrak{D}(\phi)$ is the number of orbits of ϕ. $\mathfrak{D}(\phi)$ can be bounded in terms of the number of fixed points of ϕ. Since the fixed points form a subspace, the number of them must be a power of 2, say 2^k where $k < n$. Since all other orbits must be of length at least two,

$$\mathfrak{D}(\phi) \leqslant 2^k + (2^n - 2^k)/2 = 2^{n-1} + 2^{k-1}.$$

An upper bound for the number of subsets of V which are not totally variant is then

$$l(n) \cdot 2^{\max \mathfrak{D}} = l(n) \cdot 2^{2^{n-1}+2^{n-2}} < \tfrac{3}{8} 2^{n^2} \cdot 2^{3(2^{n-2})}.$$

Since V has 2^{2^n} subsets, V will have a totally variant subset whenever $2^{n^2-1+3(2^{n-2})} < 2^{2^n}$; that is, when $n^2 - 1 < 2^{n-2}$. This is the case when $n \geqslant 8$. When $n = 7$, we use a more careful argument.

Consider those ϕ that have 2^{n-1} fixed points. Transformations of this type are determined by specifying the subspace of dimension $n - 1$ left fixed and specifying the image of one additional vector. The number of subspaces of dimension $n - 1$ is $2^n - 1$. Thus the number of ϕ with 2^{n-1} fixed points is less than $2^n \cdot 2^n$. All other transformations will have $\mathfrak{D}(\phi) \leqslant 2^{n-1} + 2^{n-3}$, and an upper bound for the number of subsets which are not totally variant is

$$2^{2n} \cdot 2^{2^{n-1}+2^{n-2}} + l(n) \cdot 2^{2^{n-1}+2^{n-3}}.$$

When $n = 7$ and $l(7)$ is replaced by $\frac{3}{8}2^{49}$, the bound is $2^{110} + 3 \cdot 2^{126}$. Since this number is less than 2^{2^7}, the result follows.

LEMMA 2. *Let V be a vector space of dimension four or greater over Z_3. Then V has a totally variant subset.*

Proof. Using notation like that in Lemma 1, with dimension of V again n, we get $l(n) < 2 \cdot 3^{n^2-1}$, $\mathfrak{D}(\phi) < 3^{n-1} + 3^{n-1}$. Thus we are comparing $2 \cdot 3^{n^2-1} \cdot 2^{2 \cdot 3^{n-1}}$ with 2^{3^n}, or 3^{n^2-1} with $2^{3^{n-1}-1}$. For $n \geqslant 4$ there are not enough sets which can fail to be totally variant.

LEMMA 3. *Let V be a vector space of dimension three or greater over* GF(4) *or any finite-dimensional vector space over a field of more than four elements. Then V has a totally variant subset.*

Proof. We remark that the cases of dimension one and of an infinite field are not difficult, and that for a field of k elements, $l(n) < (k-1)k^{n^2-1}$, $\mathfrak{D}(\phi) < \frac{1}{2}(k+1)k^{n-1}$, and that the result follows.

The above lemmas, together with the remark in the proof of Lemma 3, leave us with the vector spaces $V^2(Z_2)$, $V^3(Z_2)$, $V^4(Z_2)$, $V^2(Z_3)$, $V^5(Z_2)$, $V^6(Z_2)$, $V^3(Z_3)$, and $V^2(\mathrm{GF}(4))$. We shall show that the first four do not have totally variant subsets and that the last four do.

LEMMA 4. *$V^2(Z_3)$ does not have a totally variant subset.*

Proof. If we let $Z_3 = \{0, 1, -1\}$, we see easily by relabelling that if none of the following is totally variant, no subset is:

$$\{(1,0)\},$$
$$\{(1,0),(0,1)\}, \qquad \{(1,0),(-1,0)\},$$
$$\{(1,0),(0,1),(1,1)\}, \qquad \{(1,0),(0,1),(-1,-1)\},$$
$$\{(1,0),(0,1),(-1,0)\},$$
$$\{(1,0),(0,1),(1,1),(1,-1)\}, \qquad \{(1,0),(0,1),(1,1),(-1,-1)\},$$
$$\{(1,0),(0,1),(1,1),(-1,0)\}, \qquad \{(1,0),(0,1),(-1,-1),(1,-1)\},$$
$$\{(1,0),(0,1),(-1,-1),(-1,0)\}, \qquad \{(1,0),(0,1),(-1,0),(0,-1)\}.$$

It is not difficult to find a transformation for each set. For example, the transformation ϕ with $(a,b)\phi = (a, a+b)$ fixes $\{(1,0),(0,1),(1,1),(1,-1)\}$.

LEMMA 5. *The vector spaces $V^2(Z_2)$, $V^3(Z_2)$, and $V^4(Z_2)$ do not have totally variant subsets.*

Proof. $V^2(Z_2)$. Any single non-zero element of $V^2(Z_2)$ is fixed by the linear transformation interchanging the other two non-zero elements; hence no subset could be totally variant.

$V^3(Z_2)$. If a subset of k elements were totally variant, there would be as many distinct k-element subsets not containing zero as there are non-singular linear transformations of $V^3(Z_2)$—that is, 168. There are no more than 70 distinct subsets of any fixed size.

$V^4(Z_2)$. The numbers here are 20,160 and 6435.

Example 1. Let $\mathrm{GF}(4) = \{1, \alpha, 1+\alpha, 0\}$, with $\alpha^2 = \alpha + 1$. Then the following subset of $V^2(\mathrm{GF}(4))$ is totally variant: $\{(1,0),(\alpha,0),(0,1)\}$.

Example 2. Let $Z_3 = \{1, -1, 0\}$. Then the following subset of $V^3(Z_3)$ is totally variant:

$$\{(1,0,0),(0,1,0),(0,0,1),(1,1,0),(1,0,1),(0,0,-1)\}.$$

https://doi.org/10.4153/CJM-1968-068-5 Published online by Cambridge University Press

The verification of Example 1 consists in noting that $(1, 0)$ is fixed under all linear transformations fixing the set, since $\alpha(1, 0)$ is in the set, while $\alpha(\alpha, 0)$ and $\alpha(0, 1)$ are not. Then, $(\alpha, 0)$ must be fixed, so $(0, 1)$ must be, and any non-singular linear transformation fixing the set is the identity. For the second example, one examines sums of elements in the set to force fixed points.

A method for finding totally variant sets in vector spaces over the field of two elements is considered in the next section.

3. Examples of totally variant sets in $V^n(Z_2)$. The most convenient method of determining whether or not a subset, $\mathfrak{S}$, of $V^n(Z_2)$ is totally variant under linear transformations is to examine the Fourier transform of the characteristic function of $\mathfrak{S}$:

$$f_{\mathfrak{s}}(\lambda) = \frac{1}{2^n}\left[\sum_{v \in V^n - \mathfrak{S}} \chi_\lambda(v) - \sum_{v \in \mathfrak{S}} \chi_\lambda(v)\right].$$

The χ_λ are multiplicative characters on $V^n(Z_2)$ parameterized by the vectors of $V^n(Z_2)$ in the form

$$\chi_\lambda(v) = \begin{cases} 1 & \text{if } \sum \lambda_i v_i = 0, \\ -1 & \text{if } \sum \lambda_i v_i = 1. \end{cases}$$

If the linear transformation, A, leaves $\mathfrak{S}$ invariant, then $(A^t)^{-1}$ must leave $f_{\mathfrak{s}}$ invariant. Therefore $\mathfrak{S}$ will be totally variant if and only if the trivial linear transformation is the only one leaving $f_{\mathfrak{s}}$ fixed.

An example of a totally variant set in $V^6(Z_2)$ is

$$\mathfrak{S} = \left\{\begin{array}{llll} (101101), & (101111), & (000011), & (000100) \\ (100110), & (001000), & (001001), & (001010) \\ (101100), & (001101), & (111100), & (001110) \\ (001111), & (010000), & (010001), & (010010) \\ (010011), & (110100), & (010101), & (010110) \\ (111000), & (111001), & (111010), & (111011) \\ (011100), & (111101), & (011111), & (110000) \\ (110001), & (110010), & (110011), & (110101) \end{array}\right.$$

The Fourier transform of $\mathfrak{S}$ has the property that

$$f_{\mathfrak{s}}(001000) = 3/8,$$
$$f_{\mathfrak{s}}(001101) = f_{\mathfrak{s}}(011101) = f_{\mathfrak{s}}(101111) = 1/4,$$

and

$$f_{\mathfrak{s}}(001011) = f_{\mathfrak{s}}101011) = f_{\mathfrak{s}}(011111) = -1/4.$$

These are the only characters with magnitude at least 1/4. Thus, any transformation on characters which leaves $f_{\mathfrak{s}}$ fixed must leave $\gamma = (001000)$ fixed, permute $\alpha_1 = (001101)$, $\alpha_2 = (011101)$, $\alpha_3 = (101111)$, and permute $\beta_1 = (001011)$, $\beta_2 = (101011)$, $\beta_3 = (011111)$. Now, if $\alpha_i A = \alpha_j$ and $\beta_k A = \beta_k$,

https://doi.org/10.4153/CJM-1968-068-5 Published online by Cambridge University Press

then $(\alpha_i + \beta_k)A = \alpha_j + \beta_k$. If $f_{\mathfrak{S}}$ is to be invariant, then $f_{\mathfrak{S}}(\alpha_i + \beta_k)$ must equal $f_{\mathfrak{S}}(\alpha_j + \beta_k)$. The table of coefficients, $f_{\mathfrak{S}}(\alpha_i + \beta_k)$, is given in Table I. An examination of this table shows that transformations with the above

TABLE I

	β_1	β_2	β_3
α_1	1/8	−1/8	1/8
α_2	−1/8	1/8	−1/8
α_3	1/8	−1/8	−1/8

property must leave $\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3$ fixed. The set of vectors $\{\gamma, \alpha_1, \alpha_3, \beta_1, \beta_2, \beta_3\}$ forms a basis for $V^6(Z_2)$, and therefore the only transformation leaving $f_{\mathfrak{S}}$ fixed is the identity.

An example of a totally variant set in $V^5(Z_2)$ is

$$\mathfrak{S} = \left\{ \begin{array}{llll} (00001), & (00110), & (00111), & (01000) \\ (01010), & (01011), & (01111), & (10010) \\ (10101), & (11001), & (11010), & (11100) \\ (11101), & (11110), & (11111) & \end{array} \right.$$

Its Fourier transform has the property that

$$f_{\mathfrak{S}}(01000) = f_{\mathfrak{S}}(11100) = f_{\mathfrak{S}}(11101) = 5/16$$

and

$$f_{\mathfrak{S}}(10110) = f_{\mathfrak{S}}(11110) = f_{\mathfrak{S}}(10011) = -5/16$$

and these are the only characters with $|f_{\mathfrak{S}}(\lambda)| = 5/16$. Therefore any transformation which leaves $f_{\mathfrak{S}}$ invariant must permute $\alpha_1 = (01000)$, $\alpha_2 = (11100)$, $\alpha_3 = (11101)$ and permute $\beta_1 = (10110)$, $\beta_2 = (11110)$, $\beta_3 = (10011)$. The table for $f_{\mathfrak{S}}(\alpha + \beta)$ is given in Table II. An examination of this table shows

TABLE II

	β_1	β_2	β_3
α_1	−5/16	−5/16	3/16
α_2	−1/16	3/16	−1/16
α_3	3/16	3/16	−1/16

that $\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2$, and β_3 are all fixed points. Since $\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_3$ form a basis for $V^5(Z_2)$, all vectors are fixed and $\mathfrak{S}$ has no non-trivial symmetries.

4. Groups of odd order.

In this section we prove:

THEOREM 1. *Let $\mathfrak{G}$ be a (solvable) group of odd order which does not contain a totally variant subset. Then $\mathfrak{G}$ is the non-cyclic group of order nine.*

The theorem will be proved by induction on the length of a chief series. We need a series of lemmas.

https://doi.org/10.4153/CJM-1968-068-5 Published online by Cambridge University Press

Lemma 1. *Let $\mathfrak{H}$ be a characteristic subgroup of the group $\mathfrak{G}$. Let $\mathfrak{H}$ and $\mathfrak{G}/\mathfrak{H}$ possess totally variant subsets. Then $\mathfrak{G}$ has a totally variant subset.*

Proof. Let $\mathfrak{S}_1$, $\mathfrak{S}_2$ be totally variant subsets of $\mathfrak{H}$ and $\mathfrak{G}/\mathfrak{H}$ respectively, with $\mathfrak{S}_2$ generating $\mathfrak{G}/\mathfrak{H}$. Let $\bar{\mathfrak{S}}_2 \subseteq \mathfrak{G}$ be a set of coset representatives for $\mathfrak{S}_2$. Then $\mathfrak{T} = \mathfrak{S}_1 \cup \bar{\mathfrak{S}}_2$ is a totally variant subset of $\mathfrak{G}$. For, let ϕ be an automorphism of $\mathfrak{G}$ with $\mathfrak{T}\phi = \mathfrak{T}$. Since $\mathfrak{H}$ is characteristic, $\mathfrak{S}_1\,\phi = \mathfrak{S}_1$. Thus $\phi|\mathfrak{H}$ is the identity. Let $\bar{\phi}$ be the automorphism induced by ϕ on $\mathfrak{G}/\mathfrak{H}$. Since $\bar{\mathfrak{S}}_2\phi = \bar{\mathfrak{S}}_2$, $\mathfrak{S}_2\bar{\phi} = \mathfrak{S}_2$, so $\bar{\phi}$ is the identity. In particular, ϕ is the identity on $\bar{\mathfrak{S}}_2$. Since elements of the form SH, $S \in \bar{\mathfrak{S}}_2$, $H \in \mathfrak{H}$, generate $\mathfrak{G}$, ϕ is the identity on $\mathfrak{G}$, and the lemma is proved.

Lemma 2. *Let $\mathfrak{H}$ be a characteristic subgroup of the group $\mathfrak{G}$. Let $\mathfrak{H}$ contain a totally variant subset, and let $\mathfrak{G}/\mathfrak{H}$ be non-cyclic of order nine. Then $\mathfrak{G}$ contains a totally variant subset.*

Proof. Let $\mathfrak{S}$ be a totally variant subset of $\mathfrak{H}$. Let $A\mathfrak{H}$, $B\mathfrak{H}$ be generators of $\mathfrak{G}/\mathfrak{H}$. Let S be an element of $\mathfrak{S}$. Then $\mathfrak{T} = \{A, B, AS\} \cup \mathfrak{S}$ is totally variant. For, suppose $\mathfrak{T}\phi = \mathfrak{T}$ for some ϕ, an automorphism of $\mathfrak{G}$. Then we immediately note that $\mathfrak{S}\phi = \mathfrak{S}$, since $\mathfrak{H}$ is characteristic, so $\phi|\mathfrak{H}$ is the identity. Then we note that $B\phi = B$, since $\mathfrak{T}$ contains two representatives of the coset $A\mathfrak{H}$ and only one of the coset $B\mathfrak{H}$. Since $A\cdot S = AS$, $(A\phi)(S\phi) = (AS)\phi$, or $(A\phi)\cdot S = (AS)\phi$. Since $AS\cdot S \neq A$ ($\mathfrak{G}$ is of odd order), we are forced to conclude that $A\phi = A$, so that ϕ is the identity on $\mathfrak{G}$.

Lemma 3. *Let $\mathfrak{H}$ be a characteristic subgroup of $\mathfrak{G}$ with $\mathfrak{H}$ and $\mathfrak{G}/\mathfrak{H}$ each non-cyclic of order nine. Then $\mathfrak{G}$ has a totally variant subset.*

Proof. Let A_1, B_1 generate $\mathfrak{H}$, and $A_2\mathfrak{H}$, $B_2\mathfrak{H}$ generate $\mathfrak{G}/\mathfrak{H}$. Then $\mathfrak{T} = \{A_1, B_1, A_1A_2, A_2, B_2\}$ is totally variant. For, suppose $\mathfrak{T}\phi = \mathfrak{T}$ for some ϕ, an automorphism of $\mathfrak{G}$. Since $\mathfrak{H}$ is characteristic, $\{A_1, B_1\}\phi = \{A_1, B_1\}$, $\{A_1A_2, A_2\}\phi = \{A_1A_2, A_2\}$, and $B_2\phi = B_2$. If $A_2\phi = A_1A_2$, then $(A_1A_2)\phi = A_2$. This, together with the chain of equalities $(A_1A_2)\phi = (A_1\phi)(A_2\phi) = (A_1\phi)A_1A_2$, implies that $A_1\phi = A_1^{-1}$. Since $\mathfrak{H}$ is such that neither A_1 nor B_1 can satisfy this implication, $A_2\phi = A_2$. It readily follows that $A_1\phi = A_1$. Thus ϕ is the identity on a set of generators for $\mathfrak{G}$; hence ϕ is the identity on $\mathfrak{G}$.

Lemma 4. *Let $\mathfrak{H}$ be a characteristic subgroup of $\mathfrak{G}$. Let $\mathfrak{H}$ be non-cyclic of order nine, and let $\mathfrak{G}/\mathfrak{H}$ possess a totally variant subset. Then $\mathfrak{G}$ has a totally variant subset.*

Proof. Let A, B generate $\mathfrak{H}$ and let $\mathfrak{S}$ be a totally variant set in $\mathfrak{G}/\mathfrak{H}$. Assume the identity element not in $\mathfrak{S}$. Let $\bar{\mathfrak{S}} \subset \mathfrak{G}$ be a set of coset representatives for $\mathfrak{S}$. Let $S \in \bar{\mathfrak{S}}$. If $\mathfrak{T} = \{A, B, AS\} \cup \bar{\mathfrak{S}}$, then $\mathfrak{T}$ is totally variant. For, suppose ϕ is an automorphism of $\mathfrak{G}$ with $\mathfrak{T}\phi = \mathfrak{T}$. Since $\mathfrak{H}$ is characteristic, ϕ induces $\bar{\phi}$ on $\mathfrak{G}/\mathfrak{H}$. But $\mathfrak{S}\bar{\phi} = \mathfrak{S}$ and $\mathfrak{S}$ is totally variant;

https://doi.org/10.4153/CJM-1968-068-5 Published online by Cambridge University Press

therefore $\bar{\phi}$ is the identity on $\mathfrak{G}/\mathfrak{H}$ and cosets are invariant under ϕ. Since the members of $\mathfrak{T} - \{A, B, S, AS\}$ lie in distinct cosets (other than $A\mathfrak{H}$ and $S\mathfrak{H}$), it follows that ϕ is the identity on $\mathfrak{T} - \{A, B, S, AS\}$. Consider the coset $S\mathfrak{H}$ which has two members, AS and S, of $\mathfrak{T}$. If $S\phi = AS$, then, by the invariance of $S\mathfrak{H}$ and $\mathfrak{T}$, $AS\phi = S$. Now

$$A\phi = (AS \cdot S^{-1})\phi = (AS)\phi \cdot (S^{-1})\phi = S \cdot (AS)^{-1} = A^{-1},$$

which is impossible. On the other hand, if $S\phi = S$, then $(AS)\phi = AS$ and $A\phi = (AS \cdot S^{-1})\phi = AS \cdot S^{-1} = A$. As B is the only remaining element, $B\phi = B$ and ϕ is shown to be the identity on a set of generators, completing the argument.

Proof of the theorem. We prove by induction on the length of a chief series for a solvable group $\mathfrak{G}$ of odd order. Let $\mathfrak{G} = \mathfrak{G}_0 \supset \mathfrak{G}_1 \supset \ldots \supset \mathfrak{G}_n = \{1\}$ be a chief series for $\mathfrak{G}$. Assume $\mathfrak{G}$ is not the non-cyclic group of order nine. Then, if $n = 1$, $\mathfrak{G}$ has a totally variant subset, by the results of § 2. ($\mathfrak{G}$ must be elementary abelian; hence a vector space over a prime field.) So, assume the theorem for groups with chief series of length less than n. Then, if one lets $\mathfrak{H} = \mathfrak{G}_1$, the assumption leads us to the case of one of the Lemmas 1–4, and the theorem follows. (We use the fact that $\mathfrak{G}/\mathfrak{H}$ is elementary abelian.)

5. Abelian groups.

In this section we prove:

THEOREM 2. *The only abelian groups which do not possess totally variant subsets are the elementary abelian groups of order* 4, 8, 16, *and* 9.

By the results of the previous section, we actually can restrict attention to groups of even order. We first note that the only abelian 2-groups other than those listed above which could fail to have totally variant subsets are non-elementary and of order 2^2, 2^3, 2^4, 2^5, or 2^6 (by the counting arguments of § 2). We leave to the reader the verification that all the possible groups here have such subsets. (In one case of 2^6 one may wish to use the example for $V_5(Z^2)$ in the construction.)

To complete the proof of the theorem the following lemmas will suffice. Lemma 1 is given more generally than needed here for use in the next section.

LEMMA 1. *Let $\mathfrak{G}$ be generated by subgroups $\{\mathfrak{H}_i\colon i = 1, \ldots, k\}$, of relatively prime orders. If each $\mathfrak{H}_i$ contains a totally variant subset, so does $\mathfrak{G}$.*

Proof. If the set $\mathfrak{S}_i$ is a totally variant generating set in $\mathfrak{H}_i$, for each i, then

$$\mathfrak{S} = \bigcup_{i=1}^{k} \mathfrak{S}_i$$

is clearly totally variant, since any automorphism fixing $\mathfrak{S}$ fixes each $\mathfrak{S}_i$ because of the relative primeness of the orders. This forces such an automorphism to be the identity on each of the $\mathfrak{H}_i$, hence on $\mathfrak{G}$.

https://doi.org/10.4153/CJM-1968-068-5 Published online by Cambridge University Press

LEMMA 2. *Let $\mathfrak{G}$ be the direct product of $\mathfrak{H}$ and $\mathfrak{K}$, with $\mathfrak{H}$ elementary abelian of order 2^2, 2^3, or 2^4, $\mathfrak{K}$ a group of odd order with totally variant subset. Then $\mathfrak{G}$ has a totally variant subset.*

Proof. Let $\mathfrak{S}$ be a totally variant subset of $\mathfrak{K}$.

Case 1. Let $\mathfrak{H}$ be generated by A and B. Let $S \in \mathfrak{S}$. Let $\mathfrak{T} = \{A, BS\} \cup \mathfrak{S}$. Obviously, by considering orders, any automorphism ϕ of $\mathfrak{G}$ fixing $\mathfrak{T}$ fixes A, fixes BS, and fixes $\mathfrak{S}$. Thus ϕ is the identity on $\mathfrak{K}$ and on a set of generators for $\mathfrak{H}$. Hence $\mathfrak{T}$ is totally variant in $\mathfrak{G}$.

Case 2. Let $\mathfrak{H}$ be generated by A, B, and C. Let K_1, K_2 be two distinct non-identity elements of $\mathfrak{K}$. If $\mathfrak{T} = \{A, B, BK_1, CK_2\} \cup \mathfrak{S}$, we see, again by considering orders, that any automorphism ϕ of $\mathfrak{G}$ giving $\mathfrak{T}$ fixes $\mathfrak{S}$ and the pairs $\{A, B\}$ and $\{BK_1, CK_2\}$. Thus ϕ is the identity on $\mathfrak{K}$. Since $B \cdot K_1 = BK_1$, $B\phi \cdot K_1 \phi = (BK_1)\phi$, so $B\phi \cdot K_1 = (BK_1)\phi$. We see immediately that ϕ must fix A, B, BK_1, and CK_2. These, together with $\mathfrak{K}$, generate $\mathfrak{G}$, Thus ϕ is the identity; $\mathfrak{T}$ is totally variant in $\mathfrak{G}$.

Case 3. Let $\mathfrak{H}$ be generated by A, B, C, and D. Let K_1, K_2 be two distinct elements of $\mathfrak{K}$. If $\mathfrak{T} = \{A, B, BK_1, CK_2, DK_1\} \cup \mathfrak{S}$, the argument of Case 2, together with the remark that ϕ is the identity on $\mathfrak{K}$ implies $(CK_2)\phi \neq DK_1$, shows $\mathfrak{T}$ to be totally variant.

LEMMA 3. *Let $\mathfrak{G}$, $\mathfrak{H}$, $\mathfrak{K}$ be as in Lemma 2, except that we now let $\mathfrak{K}$ be the non-cyclic group of order nine. Then $\mathfrak{G}$ has a totally variant subset.*

Proof. Let $\mathfrak{K}$ be generated by E and F. We consider the same cases as in Lemma 2, and list totally variant subsets, leaving verification to the reader.

Case 1. $\mathfrak{T} = \{A, BE, F\}$.

Case 2. $\mathfrak{T} = \{A, B, E, BE, CF\}$.

Case 3. $\mathfrak{T} = \{A, B, E, BE, CE, DF\}$.

LEMMA 4. *Let $\mathfrak{G}$ be the direct product of subgroups $\mathfrak{H}$ and $\mathfrak{K}$, $\mathfrak{H}$ non-cyclic of order nine, $\mathfrak{K}$ of order not divisible by three, and containing a totally variant subset. Then $\mathfrak{G}$ has a totally variant subset.*

Proof. Let $\mathfrak{H}$ be generated by A and B, and let $\mathfrak{K}$ have totally variant subset $\mathfrak{S}$. If $S \in \mathfrak{S}$, then $\{A, BS\} \cup \mathfrak{S}$ is totally variant in $\mathfrak{G}$.

Proof of the theorem. It is clear that any abelian group which is not one of the exceptional cases of the theorem can be shown to have a totally variant subset by the application of at most two of the above lemmas.

6. Non-abelian groups of even order; conclusion. We note that Lemma 1 of § 5 can be used to show that any group whose Sylow subgroups have totally variant subsets has a totally variant subset. Thus the results of § 4 applied to p-groups of odd order force all groups of odd order, except the

https://doi.org/10.4153/CJM-1968-068-5 Published online by Cambridge University Press

elementary abelian group of order nine, to have totally variant subsets, without using the fact that all such groups are solvable. For groups of even order, there are other possibilities. These can be limited to only a few cases by counting arguments. These arguments are greatly facilitated by the use of the tables of Hall and Senior **(2)**.

For two-groups, we have the following two lemmas.

LEMMA 1. *The quaternion group of order eight has no totally variant subset.*

Proof. We let $\mathfrak{G} = \{1, -1, i, j, k, -i, -j, -k\}$ with

$$i^2 = j^2 = k^2 = -1, \qquad ij = -ji = k,$$

$$jk = -kj = i, \qquad ki = -ik = j.$$

We note that it suffices to consider subsets of three or fewer elements, not containing 1 or -1, which are fixed by all automorphisms, to eliminate all possibilities for totally variant sets. Once this observation is made, we simply note that:

1. Any individual element is fixed by a non-identity automorphism.

2. Any two of the elements of order four may be interchanged by a non-identity automorphism.

3. The following are the only three-element sets we need consider: $\{i, j, k\}$, $\{i, -i, j\}$; and it is clear that each of these is fixed by a non-identity automorphism.

LEMMA 2. *The group of Lemma* 1 *is the only non-abelian two-group without a totally variant subset.*

Proof. We only indicate the method of proof here. By using the tables in **(2)**, to count automorphisms we reduce the problem to a small number of cases (fewer than thirty). An examination of subgroups of index two enables us to use Lemma 1 of § 4 to reduce to fewer than ten cases. These remaining cases are taken individually. We give one example: Let $\mathfrak{G}$ be of order 16, generated by $\{A_2, A_3, B_2\}$, with $[A_2, A_3] = A_2^2 = A_3^2 = B_1$, B_1 and B_2 each of order two and generating the centre of $\mathfrak{G}$. Then the set $\{A_2, A_3, B_1 A_2, B_2 A_2, B_2\}$ is totally variant.

THEOREM 3. *The only finite groups which fail to have totally variant subsets are the exceptions in Theorems* 1 *and* 2, *and the quaternion groups of order eight.*

Proof. Again we only indicate the proof. We point out that we have only to consider groups of even order with "bad" two- or three-Sylow subgroups. The number we have to look at can be made quite small by counting arguments. For the cases which remain, the arguments are similar to those of § 4.

https://doi.org/10.4153/CJM-1968-068-5 Published online by Cambridge University Press

References

1. M. Hall, *The theory of groups* (Macmillan, New York, 1959).
2. M. Hall and J. K. Senior, *The groups of order* 2^n ($n \leqslant 6$) (Macmillan, New York, 1964).

Institute for Defense Analyses,
Princeton, N.J.

https://doi.org/10.4153/CJM-1968-068-5 Published online by Cambridge University Press