FIXED-POINT-FREE p-ELEMENTS IN TRANSITIVE PERMUTATION GROUPS

Á. BERECZKY

ABSTRACT

We give sufficient conditions for a finite permutation group to contain a fixed-point-free permutation of p-power order for a given prime p.

Introduction

It is a well-known fact that a finite transitive permutation group of degree at least two contains a fixed-point-free element. Using the Classification Theorem of finite simple groups, Fein, Kantor and Schacher [3] showed that this element can be taken to have prime-power order; they also gave an interesting application of this fact in number theory. However, the problem of finding sufficient conditions for a transitive permutation group G to have a fixed-point-free p-element for a given prime number p is still almost untouched. Of course, if G has such a p-element, then p divides the degree of G, but the converse is not true (see examples in [2]). Cameron, Frankl and Kantor [2] have formulated the conjecture that if in some sense the p-part dominates in the degree of the group G, then G contains a fixed-point-free p-element. More precisely, if we define the set $\mathscr{A}_p = \{n \in \mathbb{N}$: there is a transitive permutation group of degree n containing no fixed-point-free p-element$\}$, then they conjecture that there exists a function m_p such that if $n = p^a \cdot b$ with $p \nmid b$ and $a \geqslant m_p(b)$, then $n \notin \mathscr{A}_p$.

It is easy to see that if $n = p^a \cdot b$ with $b < p$, then $n \notin \mathscr{A}_p$. It was also established in [2] that $2^a \cdot 3 \notin \mathscr{A}_2$ for all $a \geqslant 2$. (There is a nice example in [3] which illustrates that $p(p+1) \in \mathscr{A}_p$ for any prime p.)

The results of the present paper are summarised in Theorems 1 and 2.

THEOREM 1. *Let p be a prime number and $a \geqslant 2$. Then every transitive permutation group of degree $p^a \cdot (p+1)$ contains a fixed-point-free p-element, that is, $p^a \cdot (p+1) \notin \mathscr{A}_p$.*

THEOREM 2. *Let p be an odd prime number and $a \geqslant 1$. If $p+1 < b < \frac{3}{2}(p+1)$, then every transitive permutation group of degree $p^a \cdot b$ contains a fixed-point-free p-element, that is, $p^a \cdot b \notin \mathscr{A}_p$.*

ACKNOWLEDGEMENT. The author is grateful to Péter P. Pálfy for helpful discussions.

Received 18 April 1994.

1991 *Mathematics Subject Classification* 20B05.

Proof of Theorem 1

We need the following elementary fact.

LEMMA 1.1. *Let $H < G$ be arbitrary groups with H central in G and $|G:H| = p^2$ (p a prime number). Then the commutator subgroup of G is cyclic.*

Proof. Clearly H is normal in G and G/H is abelian, so $G' \leqslant H \leqslant \mathbf{Z}(G)$. If G is abelian, then there is nothing to prove; otherwise, we have $G/H \cong \mathbb{Z}_p \times \mathbb{Z}_p$, and for suitable elements x and y in G, every element of G can be written in the form $x^i y^j h$ with $0 \leqslant i, j \leqslant p-1$, $h \in H$. Using the general identities $[ab, c] = [a, c]^b [b, c]$ and $[a, bc] = [a, c][a, b]^c$, we have $[x^i y^j h_1, x^k y^l h_2] = [x, y]^{il} [y, x]^{jk} = [x, y]^{il-jk}$. Hence $G' = \langle [x, y] \rangle$.

The next lemma plays an important role throughout. It can be verified by an elementary counting argument.

LEMMA 1.2. *Let P be a finite p-group, and let $M_1, M_2, \ldots, M_{p+1}$ be maximal subgroups in P. If $P = \bigcup_{i=1}^{p+1} M_i$, then $|P: \bigcap_{i=1}^{p+1} M_i| = p^2$ and $M_i \neq M_j$ for $i \neq j$.*

LEMMA 1.3. *Let $H_1, H_2, \ldots, H_{p+1}$ be subgroups of index at least p^2 in the finite p-group P. Then $P \setminus \bigcup \{H_i^x \mid 1 \leqslant i \leqslant p+1,\ x \in P\} \neq \emptyset$.*

Proof. By way of contradiction, suppose that the conjugacy classes of the subgroups $H_1, H_2, \ldots, H_{p+1}$ cover the whole group P. Let K_i and $M_i (1 \leqslant i \leqslant p+1)$ be subgroups of P with $H_i \leqslant K_i < M_i$, $|P:K_i| = p^2$, $|P:M_i| = p$. Then, obviously,

$$\bigcup \{K_i^x \mid 1 \leqslant i \leqslant p+1,\ x \in P\} = \bigcup \{M_i \mid 1 \leqslant i \leqslant p+1\} = P$$

holds. Applying Lemma 1.2, we obtain that $M_1, M_2, \ldots, M_{p+1}$ are distinct and $N = \bigcap_{i=1}^{p+1} M_i$ is a normal subgroup of index p^2 in P. For $i \neq j$ and $x \in P$, $M_i \cap K_j^x \leqslant M_i \cap M_j = N$, thus M_i is covered by the conjugates of K_i together with N. This means that K_i is not normal in P (that is, it has p conjugates), and again by Lemma 1.2, $N_i = N \cap \bigcap_{x \in P} K_i^x$ has index p^2 in M_i for all $i = 1, 2, \ldots, p+1$. Now $N = \bigcup_{i=1}^{p+1} N_i$, as for any $1 \leqslant i \leqslant p+1$ and $x \in P$, we have $N \cap K_i^x = N_i$. We can use Lemma 1.2 once again: $R = \bigcap_{i=1}^{n+1} N_i$ has index p^2 in N. As an intersection of normal subgroups, R is normal in P, and in the factor group P/R the normal subgroups N_i/R $(1 \leqslant i \leqslant p+1)$ have order p, so each of them is central. It follows that N/R is a central subgroup of index p^2 in P/R. By Lemma 1.1, the commutator subgroup $(P/R)' = P'R/R$ is cyclic and is contained in N/R. Since N is the union of $N_1, N_2, \ldots, N_{p+1}$, for suitable l we have $P'R/R \leqslant N_l/R$, which means $P' \leqslant N_l \leqslant K_l$. We know that K_l is not normal, but this contradicts the fact that a subgroup containing the commutator subgroup is necessarily normal.

Proof of Theorem 1. It was first shown by G. A. Miller [4] that if G is a transitive permutation group of degree n and $p^k \mid n$, then p^k also divides the size of the orbits of any Sylow p-subgroup of G. It follows that if G is any transitive permutation group of degree $p^a \cdot (p+1)$ with $a \geqslant 2$ and P is a Sylow p-subgroup of G, then P has at most $p+1$ orbits with each of size at least p^a. Applying Lemma 1.3, the union of the point-

stabilisers in P cannot be equal to P, hence G has a fixed-point-free permutation of p-power order.

Proof of Theorem 2

From now on we restrict ourselves to odd prime numbers. As we have seen above, the proof of Theorem 1 is based on the fact that if a finite p-group is covered by $p+1$ of its maximal subgroups, then certain conditions necessarily hold. The situation is similar when a finite p-group is covered by less than $\frac{3}{2}(p+1)$ of its maximal subgroups. The relevant result (Lemma 2.2 below) is a consequence of a combinatorial theorem.

THEOREM 2.1 (A. Blockhuis [1]). *If S is a non-trivial blocking set of the projective plane over* GF(p) *(that is, if S intersects every line of the plane but does not contain a line), then the cardinality of S is at least* $\frac{3}{2}(p+1)$.

LEMMA 2.2. *If P is a finite p-group, $k < \frac{3}{2}(p+1)$ a positive integer, and $M_1, M_2, \ldots, M_k$ maximal subgroups in P for which $\bigcup_{i=1}^{k} M_i = P$, then we can choose $p+1$ out of these k subgroups such that their union also equals P.*

Proof. Let us first notice that since every maximal subgroup of P contains the Frattini subgroup $\Phi(G)$, we can replace P with its factor group $G/\Phi(G)$, that is, we may assume that P is a vector space over GF(p). Now we use induction on the dimension of P. If $\dim P = 2$, then there is nothing to prove, for in this case the number of maximal subspaces in P is $p+1$. In the case $\dim P = 3$, apply the dual statement of Theorem 2.1 for the projective plane determined by P. Since $k < \frac{3}{2}(p+1)$, there are $p+1$ subgroups among $M_1, \ldots, M_k$ such that they correspond to $p+1$ lines of the projective plane through a common point. These lines then cover the whole plane, that is, these $p+1$ subgroups cover P. Now let $d > 3, \dim P = d$, and suppose that the statement is true for all vector spaces (over GF(p)) with dimension less than d. Since the number of maximal subspaces in P, $p^{d-1}+p^{d-2}+\ldots+p+1$, is greater than k, there exists a maximal subspace V in P such that $V \neq M_i$ for all $1 \leqslant i \leqslant k$. Then $V \cap M_i$ $(1 \leqslant i \leqslant k)$ are maximal subspaces in V and

$$V = V \cap P = V \cap (\bigcup_{i=1}^{k} M_i) = \bigcup_{i=1}^{k} (V \cap M_i),$$

hence by the induction hypothesis we may assume that $V = \bigcup_{i=1}^{p+1} (V \cap M_i)$. Now Lemma 1.2 yields $|V : \bigcap_{i=1}^{p+1} (V \cap M_i)| = p^2$, therefore $U = V \cap (\bigcap_{i=1}^{p+1} M_i)$ is a subspace of codimension 3 in P. Let v be any vector in $P \setminus \bigcup_{i=1}^{p+1} M_i$. For $V_1 = \langle U, v \rangle$, we have

$$V_1 \cap M_1 = V_1 \cap M_2 = \ldots = V_1 \cap M_{p+1} = U, \quad V_1 = \bigcup_{i=1}^{k} (V_1 \cap M_i) = \bigcup_{i=p+1}^{k} (V_1 \cap M_i).$$

Since $k-p$ is strictly less than $p+1$, $V_1 \leqslant M_j$ necessarily holds for a suitable j. This argument shows that P is also covered by those of the subgroups $M_1, M_2, \ldots, M_k$ which contain U. However, the proposition holds for G/U as $\dim G/U = 3$, completing the proof.

Proof of Theorem 2. By way of contradiction, suppose that for some $a \geqslant 1$ and $p+1 < b < \frac{3}{2}(p+1)$, there exists a set Ω of cardinality $n = p^a \cdot b$ and a transitive permutation group G acting on Ω, which does not contain a fixed-point-free p-element. This means that none of the Sylow p-subgroups of G contain fixed-point-free permutations. Let us first notice that if G_α is an arbitrary stabiliser and $S \in \mathrm{Syl}_p(G)$,

then $S \cap G_\alpha \in \mathrm{Syl}_p(G_\alpha)$. Namely, by Miller's Lemma (see the proof of Theorem 1), any orbit of S has size at least p^a. We may assume that each of them has size exactly p^a, because in the other case the number of S-orbits would be at most $1+(p^a b-p^{a+1})/p^a = b-p+1 \leqslant p$, and it means that the stabilisers in S are contained in at most p maximal subgroups, contradicting the assumption, according to which S is covered by the stabilisers. Thus $|S:S\cap G_\alpha| = p^a$, and so

$$|G_\alpha : S \cap G_\alpha| = \frac{|G:S\cap G_\alpha|}{|G:G_\alpha|} = \frac{|G:S|\cdot|S:S\cap G_\alpha|}{|G:G_\alpha|} = \frac{|G:S|}{b},$$

and this is not divisible by p. Let $\mathscr{P}_i$ denote the set of subgroups of G containing an intersection of a Sylow p-subgroup and a point-stabiliser as a subgroup of index p^i. We shall prove the following two statements by induction on i:

(a) $Q_1 Q_2 \in \mathscr{P}_i \Rightarrow Q_1$ and Q_2 are conjugate in G;

(b) $Q \in \mathscr{P}_i \Rightarrow |N_G(Q):Q|$ is not divisible by p^2.

From the above line of reasoning, it follows that $\mathscr{P}_i = \varnothing$ for $i > a$, $\mathscr{P}_i \cap \mathscr{P}_j = \varnothing$ for $i \neq j$, and $\mathscr{P}_a = \mathrm{Syl}_p(G)$, so (a) and (b) clearly hold for $i \geqslant a$.

Let $Q_1, Q_2 \in \mathscr{P}_0$, $Q_1 = G_\alpha \cap S_1$, $Q_2 = G_\beta \cap S_2$, where $\alpha, \beta \in \Omega$ and $S_1, S_2 \in \mathrm{Syl}_p(G)$. Since G is transitive, there is a $g \in G$ such that $G_\alpha = G_\beta^g$. Then $Q_2^g = G_\alpha \cap S_2^g$ is also a Sylow p-subgroup in G_α, hence for suitable $h \in G_\alpha$ we have $Q_2^{gh} = Q_1$.

Next we show that for $Q \in \mathscr{P}_0$, p^2 does not divide $|N_G(Q):Q|$. If this were not true, we could choose a Sylow p-subgroup S containing Q with $|N_S(Q):Q| \geqslant p^2$. Let Ω_1, $\Omega_2, \ldots, \Omega_b$ denote the orbits of S on Ω, and for each $1 \leqslant t \leqslant b$ let Q_t be the stabiliser in S of a point belonging to Ω_t. Without loss of generality, we may make the assumption that $Q = Q_1$. Since S has no fixed-point-free element, the conjugates of $Q_1, Q_2, \ldots, Q_b$ (by elements in S) cover the whole of S, so there should be at least $p+1$ distinct subgroups in the set $\{Q_1, Q_2, \ldots, Q_b\}$. Q has at least p^2 fixed points in Ω_1 as $|N_S(Q):Q| \geqslant p^2$, therefore Q_2 must also have at least p^2 fixed points in Ω (for they are conjugate in G). Now if $|N_S(Q_2):Q_2| = p$, then Q_2 cannot have more than p fixed points in each Ω_j, so it has fixed points in at least p distinct S-orbits. Hence we may assume $Q_2 = Q_3 = \ldots = Q_{p+1}$, contrary to the above observation that there are at least $p+1$ distinct ones among the subgroups $Q_1, Q_2, \ldots, Q_b$. Thus we have proved that $|N_S(Q_2):Q_2| \geqslant p^2$, and similarly $|N_S(Q_t):Q_t| \geqslant p^2$ holds for all $t \leqslant b$. Therefore, for any t, Q_t has at most $|S:Q_t|/p^2$ distinct conjugates in S, hence the union of all the conjugates of the subgroups $Q_1, Q_2, \ldots, Q_b$ in S contains at most $b\cdot|Q|\cdot|S:Q|/p^2 = b\cdot|S|/p^2$ elements. This contradiction shows that (b) holds for $i = 0$.

Let us now turn to the proof of the induction step. Let $1 \leqslant j < a$ be a positive integer, and suppose that (a) and (b) are true for all $i \leqslant j-1$. For any $Q_1, Q_2 \in \mathscr{P}_j$, there exist $Q_3, Q_4 \in \mathscr{P}_{j-1}$ such that $Q_3 < Q_1$ and $Q_4 < Q_2$. Using (a) for $i = j-1$, $Q_4^g = Q_3$ for a suitable $g \in G$. Now Q_3 is a subgroup of index p in both Q_2^g and Q_1, thus taking (b) for $i = j-1$ into consideration, Q_2^g and Q_1 are Sylow p-subgroups in $N_G(Q_3)$. Hence there exists an element $h \in N_G(Q_3)$ such that $Q_2^{gh} = Q_1$. Thus assertion (a) is verified for $i = j$.

The proof of (b) is like that in the case $i = 0$. We may make the assumption $j \leqslant a-2$, because the case $j = a-1$ is trivial. Suppose that $|N_G(Q):Q|$ is divisible by p^2 for some Q in $\mathscr{P}_j$. Then there is a Sylow p-subgroup S in G containing Q with $|N_S(Q):Q| \geqslant p^2$. Let $\Omega_1, \Omega_2, \ldots, \Omega_b$ denote the orbits of S on Ω, for $t = 1, 2, \ldots, b$, let R_t be the stabiliser in S of a point belonging to Ω_t, and let Q_t be the subgroup

of S containing R_t as a subgroup of index p^j. (We remark that Q_t is unique, for if $Q_t, Q_t' \geqslant S$, $|Q_t:R_t| = |Q_t':R_t| = p^j$ and $Q_t \neq Q_t'$, then $T = Q_t \cap Q_t' \in \mathscr{P}_l$ for some $l < j$; $T < N_S(T) \cap Q_t$, $T < N_S(T) \cap Q_t'$, so it follows that $|N_S(T):T| > p$, hence p^2 divides $|N_G(T):T|$, contradicting the induction hypothesis.) Without loss of generality, we may also make the assumption that $Q = Q_1$.

We show that the size of any orbit of the subgroup Q_t is at least p^j, and if Q_t has an orbit of size p^j in Ω_t, then for a suitable $\alpha \in \Omega_t$ we have $G_\alpha \cap S \leqslant Q_t$. Namely, for $\alpha \in \Omega$, the size of the Q_t-orbit containing α is equal to

$$\frac{|Q_t|}{|Q_t \cap G_\alpha|} = p^j \frac{|S \cap G_\alpha|}{|Q_t \cap G_\alpha|} \geqslant p^j,$$

and equality holds if and only if $S \cap G_\alpha \leqslant Q_t$. Observe that Q_t cannot have more than one conjugate in S with the property that its orbit containing a fixed $\alpha \in \Omega_t$ has size p^j. For if $Q_t^{s_1}$ and $Q_t^{s_2}$ $(s_1, s_2 \in S)$ are such conjugates, then $Q_t^{s_1}$ and $Q_t^{s_2}$ would both contain $S \cap G_\alpha$ as a subgroup of index p^j, and we noticed above that this implies $Q_t^{s_1} = Q_t^{s_2}$. On the other hand, since S is transitive on Ω_t, for each $\alpha \in \Omega_t$ there is a conjugate of Q_t in S with the property that its orbit containing α has size p^j. So if we denote by r the number of Q_t-orbits on Ω_t of size p^j, then

$$|S:N_S(Q_t)| \cdot r \cdot p^j = |\Omega_t|,$$

$$r = \frac{|\Omega_t|}{p^j |S:N_S(Q_t)|} = \frac{|\Omega_t| \cdot |N_S(Q_t):Q_t|}{p^j \cdot |S:Q_t|} = |N_S(Q_t):Q_t|.$$

It follows from the assumption $|N_S(Q):Q| \geqslant p^2$ that Q has at least p^2 orbits of size p^j on Ω_1. Hence Q_2 (as a conjugate of Q) has also at least p^2 orbits of size p^j on Ω. Now if $|N_S(Q_2):Q_2| = p$, then using the result of the previous paragraph, it follows that Q_2 has orbits of size p^j on at least p members of the set $\{\Omega_1, \Omega_2, \ldots, \Omega_b\}$, and in this case we may assume that $Q_2 = Q_3 = \ldots = Q_{p+1}$. Now the conjugates of $Q_1, Q_2, \ldots, Q_b$ (by elements in S) cannot cover the subgroup S, hence neither do the conjugates of $R_1, R_2, \ldots, R_b$. This contradiction indicates that $|N_S(Q_2):Q_2| \geqslant p^2$ necessarily holds, and similarly we have $|N_S(Q_t):Q_t| \geqslant p^2$ for all positive integers $t \leqslant b$. Now for any t, Q_t has at most $|S:Q_t|/p^2$ different conjugates in S, therefore the union of the conjugates of the subgroups $Q_1, Q_2, \ldots, Q_b$ (by elements in S) contains at most $b \cdot |Q| \cdot |S:Q|/p^2 = b \cdot |S|/p^2$ elements. From this, it follows again that the conjugates of $R_1, R_2, \ldots, R_b$ by elements in S cannot cover the whole of S. This contradiction shows that the assumption $p^2 \mid |N_G(Q):Q|$ was false.

Thus assertions (a) and (b) are verified for all $i \geqslant 0$.

From now on let S be a fixed Sylow p-subgroup in G, and let $\Omega_1, \Omega_2, \ldots, \Omega_b$ be the orbits of S on Ω. For any $1 \leqslant t \leqslant b$, let R_t denote the stabiliser in S of a point in Ω_t and M_t the maximal subgroup of S containing R_t. (We know that M_t is unique.) Obviously, M_t contains S_β, the stabiliser of β in S for all $\beta \in \Omega_t$ (because it is conjugate to R_t in S). Since S has no fixed-point-free elements, it follows that $S = \bigcup_{t=1}^{b} M_t$. Applying Lemma 2.2, we may assume that $S = \bigcup_{t=1}^{p+1} M_t$, and by Lemma 1.2, $N = \bigcap_{t=1}^{p+1} M_t$ is a (normal) subgroup of index p^2 in S.

Next we show that the subgroups $M_1, M_2, \ldots, M_b$ are distinct. They are certainly conjugate to each other in G (as elements in $\mathscr{P}_{a-1}$). Since $S = \bigcup_{t=1}^{p+1} M_t$, $M_1, M_2, \ldots, M_{p+1}$ are distinct. Since the cardinality of the set $\{M_{p+2}, \ldots, M_b\}$ is less than $p+1$, we may assume that $M_1 \neq M_j$ for all $j \geqslant 2$. From this it follows that $\Omega_2, \Omega_3 \ldots, \Omega_b$ do not split into smaller orbits under the action of M_1, so there are only p M_1-orbits of size

p^{a-1}. Now this property also holds for $M_2, M_3, \ldots, M_b$ (for they are conjugate to M_1 in G), and thus $M_i \neq M_j$ for $i \neq j$. It is a trivial consequence that none of the subgroups $M_{p+2}, \ldots, M_b$ contains N.

Let s be an arbitrary element in $N_G(S)$. Then s permutes the subgroups $M_1, M_2, \ldots, M_b$ (by conjugation) because they are the only maximal subgroups of S containing at least one of its point-stabilisers. The sets $\{M_1, M_2, \ldots, M_{p+1}\}$ and $\{M_1^s, M_2^s, \ldots, M_{p+1}^s\}$ intersect in more than one element, therefore $N^s = N$, so the conjugation by elements in $N_G(S)$ leaves the set $\{M_1, M_2, \ldots, M_{p+1}\}$ invariant. We shall complete our proof by showing that, on the other hand, $N_G(S)$ acts transitively on the set $\{M_1, M_2, \ldots, M_b\}$. To see this, let $1 \leqslant i < j \leqslant b$ and $g \in G$ such that $M_i^g = M_j$. Since both S and S^g contain M_j as a maximal subgroup, they are Sylow p-subgroups in $N_G(M_j)$. Thus we have $S^{gh} = S$ for a suitable $h \in N_G(M_j)$, and gh moves M_i into M_j. This final contradiction completes the proof of Theorem 2.

References

1. A. BLOCKHUIS, 'On the size of a blocking set in $PG(2,p)$', *Combinatorica* (1) 14 (1994) 111–114.
2. P. J. CAMERON, P. FRANKL and W. M. KANTOR, 'Intersecting families of finite sets and fixed-point-free 2-elements', *European J. Combin.* 10 (1989) 149–160.
3. B. FEIN, W. M. KANTOR and M. SCHACHER, 'Relative Brauer groups II', *J. Reine Angew. Math.* 328 (1981) 39–57.
4. G. A. MILLER, 'A fundamental theorem with respect to transitive substitution groups', *Bull. Amer. Math. Soc.* 9 (1903) 543–544.

Department of Algebra and Number Theory
Eötvös University Budapest
H-1088 Budapest
Múzeum Krt. 6–8
Hungary

Current address
Department of Mathematics
University of Florida
Gainesville, FL 32611
USA