Can. J. Math., Vol. XXIV, No. 5, 1972, pp. 851–858

THE NUMBER OF GENERATORS OF A LINEAR p-GROUP

I. M. ISAACS

Let G be a finite p-group, having a faithful character χ of degree f. The object of this paper is to bound the number, $d(G)$, of generators in a minimal generating set for G in terms of χ and in particular in terms of f. This problem was raised by D. M. Goldschmidt, and solved by him in the case that G has nilpotence class 2. (See [**1**, Lemma 2.8].) We obtain the following results:

THEOREM A. *Let χ be a faithful character of the p-group, G. Let $f = \chi(1)$ and let s be the number of linear constituents of χ. Then*
(a) $d(G) \leqq (3/p)(f - s) + s$. *Also,*
(b) if $p \geqq 3$ *and G is non-abelian, then* $d(G) \leqq f - p + 3$.

THEOREM B. *Let G be a p-group and let $\chi \in \mathrm{Irr}(G)$ be faithful. Then*

$$d(G) \leqq \frac{f + (f/p) + 2p - 4}{p - 1}.$$

It is shown by examples that the inequalities in Theorem A are best possible, and the one in Theorem B is nearly so.

1. Suppose χ is a faithful character of the p-group, G, and that $\chi = \psi + \lambda$, where λ is linear. Let $N = \mathrm{Ker}\, \psi$ so that λ_N is faithful and hence N is cyclic. It follows that $d(G) \leqq d(G/N) + 1$. By repeated application of this argument, we see that in order to prove Theorem A(a), it suffices to assume that χ has no linear constituents and show that $d(G) \leqq 3f/p$. Observe that part (b) of this theorem follows immediately from (a).

We would like to use reasoning similar to this in order to reduce the problem of bounding $d(G)$ to the situation of Theorem B, namely where χ is irreducible. In general, G is a subdirect product of the irreducible linear groups determined by the irreducible constituents of a faithful character. Unfortunately, if N_1, $N_2 \lhd G$ with $N_1 \cap N_2 = 1$, it does not follow that $d(G) \leqq d(G/N_1) + d(G/N_2)$. In order to overcome this difficulty we need to strengthen the theorem we are trying to prove.

Definition 1. Let G be a p-group and let $U \subseteq G$. Then

$$d_G(U) = d(U/(U \cap \Phi(G))).$$

Received August 30, 1971. This research was supported by NSF Grant GP–29432.

https://doi.org/10.4153/CJM-1972-084-0 Published online by Cambridge University Press

Instead of assuming that χ is faithful on G and bounding $d(G)$, we shall assume $U \lhd G$ and χ is a character of G with χ_U faithful and we shall bound $d_G(U)$. Since $d_G(G) = d(G)$, the new problem includes the old one.

LEMMA 2. *Let G be a p-group with $U \subseteq G$.*

(a) *If $U \subseteq H \subseteq G$, then $d_G(U) \leqq d_H(U)$ and $d_G(U) \leqq d_G(H)$.*

(b) *If $V \subseteq U$ and $V \lhd G$, then $d_G(U) = d_G(V) + d_{G/V}(U/V)$.*

Proof. (a). Since $H/H \cap \Phi(G)$ is elementary, $\Phi(H) \subseteq \Phi(G)$ and $U \cap \Phi(H) \subseteq U \cap \Phi(G)$. It follows that $d_H(U) \geqq d_G(U)$. Also, $d_G(U) = d(U\Phi(G)/\Phi(G)) \leqq d(H\Phi(G)/\Phi(G)) = d_G(H)$.

(b). Let $A = U \cap V\Phi(G)$. Then $U \supseteq A \supseteq U \cap \Phi(G)$ and $d_G(U) = d(U/A) + d(A/(U \cap \Phi(G)))$. Now $A = V(U \cap \Phi(G))$ and hence $A/(U \cap \Phi(G)) \cong V/(V \cap \Phi(G))$. Thus $d(A/(U \cap \Phi(G)) = d_G(V)$. Finally, we have $(U/V) \cap \Phi(G/V) = (U \cap V\Phi(G))/V = A/V$. Therefore, $d_{G/V}(U/V) = d((U/V)/(A/V)) = d(U/A)$. The proof is complete.

COROLLARY 3. *Let G be a p-group and let $U = N_0 \supseteq N_1 \supseteq \ldots \supseteq N_n = 1$ where $N_i \lhd G$ for $1 \leqq i \leqq n$. Then*

$$d_G(U) = \sum_{i=1}^{n} d_{G/N_i}(N_{i-1}/N_i).$$

Proof. Repeated application of part (b) of the lemma yields the result.

Next, we wish to establish appropriate bounds when $\chi(1) = p$. The following lemma is well known and is stated here without proof.

LEMMA 4. *Let $A \lhd G$ be abelian with G/A cyclic. Let Ag be a generator of G/A. Then*

(a) $G' = \{a^{-1}a^g | a \in A\}$ *and*

(b) $|G'|\,|A \cap \mathbf{Z}(G)| = |A|$.

If χ is a character of a group, G, then det χ is the linear character of G obtained by taking the determinant of any representation of G which affords χ.

LEMMA 5. *Let G be a p-group with abelian $A \lhd G$ such that G/A is cyclic. Let $\chi \in \mathrm{Irr}(G)$ with $\chi(1) = p^e$ and suppose χ_A is faithful. Then*

(a) $d_G(A) \leqq e + 1$.

Also,

(b) *if* det $\chi_A = 1_A$, *then $d_G(A) \leqq e$, and*

(c) *if A has exponent $\leqq p^e$ then $d_G(A) \leqq e$.*

Proof. Let $Z = \mathbf{Z}(G) \cap A$. By Lemma 4, we have $|A : G'| = |Z|$. Since χ is irreducible, we have $Z(\mathrm{Ker}\ \chi)/\mathrm{Ker}\ \chi$ is cyclic and thus Z is cyclic since χ_A is faithful. If $|Z| \leqq p^e$, then $|A/(A \cap \Phi(G))| \leqq |A:G'| \leqq p^e$ and $d(A) \leqq e$. Therefore, (c) follows.

Now $\chi_Z = p^e\lambda$ where λ is a faithful character of Z. We have det $\chi_Z = \lambda^{p^e}$ and hence if det $\chi_Z = 1_Z$, it follows that $|Z| \leqq p^e$, and (b) now follows.

To prove (a), let C be the cyclic group of automorphisms of A induced by G/A. Since χ_A is faithful, C permutes the set of linear constituents of χ_A faithfully. This action is transitive, and hence regular and $|C| \leqq \chi(1)$. Let $\theta(a) = \Pi_{\sigma \in C} a^\sigma$ for $a \in A$. Then θ is an endomorphism of A and $\theta(a) = \theta(a^g)$ for $g \in G$. It follows that $G' \subseteq \operatorname{Ker} \theta = K$. It is clear that $\theta(A) \subseteq Z$ and since $|A : K| = |\theta(A)|$ and $|A : G'| = |Z|$, we have $|K : G'| = |Z : \theta(A)|$ and $A/K \cong \theta(A)$ is cyclic. If $Z = \langle z \rangle$, then $\theta(z) = z^{|C|}$ and hence $|Z : \theta(A)| \leqq |C| \leqq p^e$. It follows that $|K : K \cap \Phi(G)| \leqq p^e$ and $d_G(K) \leqq e$. Since $d_{G/K}(A/K) \leqq 1$, we have $d_G(A) \leqq e + 1$ and the proof is complete.

LEMMA 6. *Let G be a p-group with $\chi \in \operatorname{Irr}(G)$ and $\chi(1) = p$. Let $U \lhd G$ and suppose χ_U is faithful. Then*

(a) $d_G(U) \leqq 3$. *Also,*

(b) $d_G(U) \leqq 2$ *if U is abelian,* $\det \chi_U = 1_U$ *or U has exponent p, and*

(c) $d_G(U) \leqq 1$ *if U is abelian and either* $\det \chi_U = 1_U$ *or U has exponent p.*

Proof. Use induction on $|G|$. If there exists $H \subset G$ with $U \subseteq H$ and χ_H irreducible, then the result follows since $d_G(U) \leqq d_H(U)$. Supposing, then, that $U \subset G$, we may assume that the restriction of χ to every maximal subgroup containing U is reducible. It follows that χ vanishes on $G - U\Phi(G)$ and hence $[\chi_{U\Phi(G)}, \chi_{U\Phi(G)}] = |G : U\Phi(G)|$. If $|G : U\Phi(G)| > p$, then $[\chi_U, \chi_U] = p^2$ and $\chi_U = p\lambda$, where λ is a faithful linear character of U. In this case U is cyclic and $d_G(U) \leqq 1$.

Under the assumption that $U \subset G$, the remaining case is where $|G : U\Phi(G)| = p$, G/U is cyclic, and U is abelian. In this case, Lemma 5 yields $d_G(U) \leqq 2$ and $d_G(U) \leqq 1$ if $\det \chi_U = 1_U$ or U has period p.

The only remaining case is where $U = G$. Here χ is faithful, and there exists an abelian subgroup A of index p (since χ is a monomial character). By the earlier cases, $d_G(A) \leqq 2$ and $d_G(A) \leqq 1$ if $\det \chi_A = 1_A$ or A has exponent p. The result now follows since $d_G(G) = d_G(A) + 1$.

2. In this section we prove Theorems A and B by working with irreducible characters, χ, of G which are faithful upon restriction to $U \lhd G$. In order to obtain the desired bound we introduce another parameter and prove a somewhat stronger theorem.

THEOREM 7. *Let G be a p-group, $\chi \in \operatorname{Irr}(G)$ and $U \lhd G$ with χ_U faithful. Let $\chi(1) = f$ and let r be the number of (not necessarily distinct) irreducible constituents of χ_U. Set $b = (f + (f/p) + 2p - 4)/(p - 1)$. Then:*

(a) $d_G(U) \leqq b$.

(b) *If $r > 1$, then*

$$d_G(U) \leqq b - \frac{(r/p) - 1}{p - 1} - 1.$$

(c) *If* $\det \chi_U = 1_U$, *the inequalities in* (a) *and* (b) *may be replaced by strict inequalities.*

https://doi.org/10.4153/CJM-1972-084-0 Published online by Cambridge University Press

Proof. Use induction on $|U|\,|G|$. First note that if $f = 1$, then $b > 1$ and U is cyclic and the theorem holds. If $f = p$, then $b = 3$. In this case the theorem follows from Lemma 6. We therefore assume that $f \geqq p^2$.

If $r = 1$, then χ_U is irreducible and since $d_G(U) \leqq d_U(U)$, we are done by induction if $U < G$. Assume then, that $U = G$ and let H be a maximal subgroup of G, chosen so that χ_H is reducible. Since $|H|\,|G| < |G|\,|G|$, the inductive hypothesis applies and we conclude that $d_G(H) \leqq b - 1$ with strict inequality if $\det \chi = 1_G$. It follows that $d_G(G) = 1 + d_G(H) \leqq b$, again with strict inequality if $\det \chi = 1_G$. The theorem is now proved in this case.

Now suppose $r = p$. Choose a maximal subgroup, $H \supseteq U$. If χ_H is irreducible, we are done by applying the inductive hypothesis to H. We may assume, then, that $\chi_H = \theta_1 + \ldots + \theta_p$, where the θ_i are conjugate irreducible characters of H. Since we are assuming $r = p$, we have $(\theta_i)_U$ irreducible for all i. On the other hand, since $f \geqq p^2$, $\theta_1(1) \geqq p$ and there exists a maximal subgroup, W, of H with $(\theta_1)_W$ reducible. It follows that $U \nsubseteq W$. Let λ be a linear character of H with kernel W and let $\psi = \lambda^G$ and $V = U \cap \operatorname{Ker} \psi$. Then $V \subseteq U \cap W \subset U$. Also, $\Phi(H) \subseteq W$ and $\Phi(H) \lhd G$, so that $\Phi(H) \subseteq \operatorname{Ker} \psi$ and consequently, U/V is elementary abelian. If ψ is reducible, then $W \lhd G$, $W = \operatorname{Ker} \psi$ and U/V is cyclic. If ψ is irreducible, there is a corresponding irreducible character $\hat{\psi}$ of G/V and $\hat{\psi}_{(U/V)}$ is faithful. It follows from Lemma 6(c) that $d_{G/V}(U/V) = 1$, and thus this is true in either case.

Since $V \subset U$, the theorem applies to bound $d_G(V)$. Since χ_V has at least p^2 irreducible constituents, we have $d_G(V) \leqq b - 2$, with strict inequality if $\det \chi_U = 1_U$. Now $d_G(U) = d_G(V) + d_{G/V}(U/V) = 1 + d_G(V)$ and thus the theorem holds.

Finally, we assume that $r \geqq p^2$ and again choose a maximal $H \supseteq U$. As before, we may assume that $\chi_H = \theta_1 + \ldots + \theta_p$. Let $\lambda_i = \det \theta_i$, let $\psi = \lambda_1{}^G$ and let $V = U \cap \operatorname{Ker} \psi$. If ψ is reducible then $\operatorname{Ker} \psi = \operatorname{Ker} \lambda_1$, U/V is cyclic and $d_{G/V}(U/V) = 1$. If ψ is irreducible, then as before we let $\hat{\psi}$ be the corresponding irreducible character of G/V. Since $\hat{\psi}_{(U/V)}$ is faithful and U/V is abelian, Lemma 6(b) yields $d_{G/V}(U/V) \leqq 2$. Now $\det \psi_H = \Pi \lambda_i = \det \chi_H$ and hence if $\det \chi_U = 1_U$, it follows that $\det \hat{\psi}_{(U/V)} = 1_{(U/V)}$ and $d_{G/V}(U/V) \leqq 1$ by Lemma 6(c).

Now let $K_j = \operatorname{Ker} \theta_j$ and let $N_i = V \cap \bigcap_{j=1}^{i} K_j$. Set $N_0 = V$ and note that $N_p = 1$ since χ_V is faithful. By Corollary 3,

$$d_G(V) \leqq d_H(V) = \sum_{i=1}^{p} d_{H/N_i}(N_{i-1}/N_i).$$

Let r_i be the number of irreducible constituents of $(\theta_i)_{N_{i-1}}$ and observe that $r_i \geqq r/p \geqq p$. Let $\hat{\theta}_i$ be the irreducible character of H/N_i corresponding to θ_i for $1 \leqq i \leqq p$. We have $\hat{\theta}_{i(N_{i-1}/N_i)}$ is faithful and has trivial determinant since $N_{i-1} \subseteq V \subseteq \operatorname{Ker} \psi \subseteq \operatorname{Ker} \lambda_i$. It follows by the inductive hypothesis that

$$d_{H/N_i}(N_{i-1}/N_i) < \frac{(f/p) + (f/p^2) + 2p - 4}{p - 1} - \frac{(r_i/p) - 1}{p - 1} - 1.$$

Since $f \geqq p^2$ and $r_i/p \geqq r/p^2 \geqq 1$, the quantity on the right is an integer and we conclude

$$d_{H/N_i}(N_{i-1}/N_i) \leqq \frac{(f/p) + (f/p^2) + 2p - 4}{p - 1} - \frac{(r/p^2) - 1}{p - 1} - 2.$$

Therefore we have

$$d_G(V) \leqq \frac{f + (f/p) + 2p^2 - 4p}{p - 1} - \frac{(r/p) - p}{p - 1} - 2p$$
$$= \frac{f + (f/p) - p - (r/p)}{p - 1} = b - \frac{(r/p) - 1}{p - 1} - 3.$$

Combining this inequality with $d_{G/V}(U/V) \leqq 2$ and $d_{G/V}(U/V) \leqq 1$ if $\det \chi_U = 1_U$, yields (b) and (c) in this case. The proof of the theorem is now complete.

Observe that Theorem B is a special case of Theorem 7(a) and has therefore now been proved. Also note that if $f \geqq p$, we have

$$\frac{f + (f/p) + 2p - 4}{p - 1} \leqq \frac{3f}{p}.$$

Proof of Theorem A. It has already been noted that it suffices to prove (a), and that, only when χ has no linear constituents. Let $\chi_1, \chi_2, \ldots, \chi_n$ be the distinct irreducible constituents of χ and let $K_j = \operatorname{Ker} \chi_j$ and $N_i = \bigcap_{j=1}^{i} K_j$. Then by Corollary 3, $d(G) = \Sigma\, d_{G/N_i}(N_{i-1}/N_i)$ where $N_0 = G$. By Theorem 7 applied to G/N_i, we have $d_{G/N_i}(N_{i-1}/N_i) \leqq 3\chi_i(1)/p$. It follows that $d(G) \leqq 3\chi(1)/p$ as desired.

We end this section with a corollary of Theorem 7. The bound given here will be shown to be sharp.

COROLLARY 8. *Let G be a p-group and let $U \lhd G$ be abelian. Suppose $\chi \in \operatorname{Irr}(G)$ with $\chi(1) = f$ and χ_U faithful. Then $d_G(U) \leqq (f - 1)/(p - 1) + 1$.*

Proof. If $f = 1$, U is cyclic. Otherwise, apply Theorem 7(b) with $r = f$.

3. In this section we discuss some examples.

THEOREM 9. *The bounds given in Theorem* A *are sharp.*

Proof. Let H be the central product of a non-abelian group of order p^3 with a cyclic group of order p^2. Then $d(H) = 3$ and H has a faithful irreducible character of degree p. Now let G be the direct product of $(f - s)/p$ copies of H and s copies of a cyclic group of order p. Then $d(G) = 3(f - s)/p + s$ and G has a faithful character of degree f.

The direct product of one copy of H with $f - p$ cyclic groups of order p shows that the bound in (b) is the best possible.

THEOREM 10. *The bound given in Lemma* 5(a) *is sharp.*

Proof. We need an example of a p-group G with $A \lhd G$, A abelian, G/A cyclic, $\chi \in \operatorname{Irr}(G)$, χ_A faithful, $\chi(1) = p^e$ and $d_G(A) = e + 1$. The example is as follows.

https://doi.org/10.4153/CJM-1972-084-0 Published online by Cambridge University Press

Let $A = \langle x_1 \rangle \times \langle x_2 \rangle \times \ldots \times \langle x_{e+1} \rangle$, where the order, $o(x_i) = p^i$. Define an automorphism, σ, of A by

$$x_i^\sigma = x_i x_{i+1}^p \text{ for } 1 \leqq i \leqq e$$

and $x_{e+1}^\sigma = x_{e+1}$. We claim that $o(\sigma) \leqq p^e$. Let $Z = \langle x_{e+1} \rangle$. Then σ acts on A/Z and this is the situation corresponding to the case $e - 1$. By induction, then, $\sigma^{p^{e-1}}$ acts trivially on A/Z. Let $\theta = \sigma^{p^{e-1}}$ so that $a^{-1}a^\theta \in Z$ for all $a \in A$.

Now let $\bar{A} = A/\Omega_1(A)$. Then σ acts on $\bar{A}$ and this too is the situation corresponding to $e - 1$. Thus θ is trivial on $\bar{A}$ and $a^{-1}a^\theta \in \Omega_1(A) \cap Z$ for all $a \in A$. If $a^\theta = ay$, then $y^p = 1$ and $y^\theta = y$ so that $a^{\theta p} = ay^p = a$, and $o(\sigma) \leqq p^e$ as claimed.

Let G be the semi-direct product, $A \rtimes \langle \sigma \rangle$. It is clear that $G' = \Phi(A)$ and hence $|A : G'| = p^{e+1}$. By Lemma 4, $|A \cap \mathbf{Z}(G)| = p^{e+1}$. However, since $\langle \sigma \rangle$ acts faithfully on A, we have $\mathbf{Z}(G) \subseteq A$. Since $Z \subseteq \mathbf{Z}(G)$ and $|Z| = p^{e+1}$, it follows that $\mathbf{Z}(G) = Z$ is cyclic. Therefore, G has a faithful irreducible character χ with $\chi(1) \leqq |G : A| \leqq p^e$. Finally, since $G' = \Phi(A)$, it follows that $d_G(A) = d(A) = e + 1$. By Lemma 5(a), $\chi(1) = p^e$ and the proof is complete.

THEOREM 11. *Let E be an elementary abelian p-group of order p^k, $k \geqq 1$. There exists an abelian p-group, U, on which E acts so that*

(a) $\mathbf{C}_U(E)$ *is cyclic*

and

(b) $d(U/[U, E]) = (p^k - 1)/(p - 1) + 1$.

Before proving Theorem 11, we discuss some consequences. Let G be the semi-direct product $U \rtimes E$. Then we have $G' = [U, E]$ and $G/G' \cong U/[U, E] \times E$. It follows that $d_G(U) = d(U/[U, E]) = (p^k - 1)/(p - 1) + 1$ and that $d(G) = d_G(U) + k$. Now $\mathbf{Z}(G) \cap U = \mathbf{C}_U(E)$ is cyclic, and thus there exists $\chi \in \mathrm{Irr}(G)$ with $\mathbf{C}_U(E) \cap \mathrm{Ker}\,\chi = 1$. It follows that χ_U is faithful. Let $f = \chi(1)$ so that $f \leqq |G : U| = p^k$. On the other hand, Corollary 8 asserts that $d_G(U) \leqq (f - 1)/(p - 1) + 1$. It follows that $f = p^k$. At this point we have proved

COROLLARY 12. *The bound of Corollary 8 is sharp.*

In the above situation, $f = |G : U|$ and it follows that U is a maximal abelian subgroup of G. Therefore, $\mathbf{C}_U(E) = \mathbf{Z}(G)$ and hence χ is faithful. Let $b = b(f)$ be the bound given in Theorem B. If $f = p$ or p^2, we see that $d(G) = b$. Although the above group, G, does not prove that the bound, b, is sharp; it does show that it is not far wrong, since for $f > 1$ we have $d(G) > pb/(p + 1)$.

Before proving Theorem 11, we need the following counting lemma.

LEMMA 13. *Let n and k be positive integers and let N be the number of k-tuples, $(x_1, \ldots, x_k)$ of integers, $0 \leqq x_i \leqq n$, such that $\Sigma x_i \equiv 0 \bmod n$. Then*

$$N = \frac{(n + 1)^k - 1}{n} + 1.$$

Proof. We count the k-tuples with $\Sigma x_i \equiv 0 \bmod n$ according to the number, r, of entries equal to n. If $r = k$, there is one such k-tuple. If $r < k$, the number of k-tuples with the required property is $\binom{k}{r}F(r)$ where $F(r)$ is the number of $(k - r)$-tuples, $(y_1, \ldots, y_{k-r})$, where $0 \leqq y_i \leqq n - 1$ and $\Sigma y_i \equiv 0 \bmod n$.

We may identify the n^{k-r} $(k - r)$-tuples of integers y_i, $0 \leqq y_i \leqq n - 1$ with the elements of the direct product of $k - r$ cyclic groups of order n. Under this identification, the tuples, $(y_1, \ldots, y_{k-r})$, with $\Sigma y_i \equiv 0 \bmod n$, correspond to the elements of the kernel of a homomorphism onto the cyclic group of order n. It follows that $F(r) = n^{k-r-1}$ and

$$N = 1 + \sum_{r=0}^{k-1} \binom{k}{r} n^{k-r-1}$$

$$= 1 + \frac{1}{n}((n + 1)^k - 1),$$

as desired.

Proof of Theorem 11. We shall construct U as an (additive) subgroup of the group ring $R[E] = A$, where $R = \mathbf{Z}/p^{k+1}\mathbf{Z}$. Now E acts on A by right multiplication and $\mathbf{C}_A(E) = R(\sum_{x \in E} x)$, a cyclic group. Therefore, it suffices to find a subgroup $U \subseteq A$ which is invariant under E (i.e., U must be an ideal) such that $d(U/[U, E]) = (p^k - 1)/(p - 1) + 1$.

First we observe that for $x \in E$, we have $(x - 1)^p = p\sum_{i=1}^{p-1} r_i(x - 1)^i$ for suitable $r_i \in R$. This is so because of the polynomial identity $X^p - (X + 1)^p + 1 = p\sum_{i=1}^{p-1} m_i X^i$ where $m_i = -\binom{p}{i}/p \in \mathbf{Z}$. Substituting $x - 1$ for X yields the required result.

Next we establish some notation. Let $\{x_1, \ldots, x_k\}$ be a fixed set of generators for E. Let $\mathscr{S} = \{(m_1, \ldots, m_k) | m_i \in \mathbf{Z}, 0 \leqq m_i \leqq p - 1\}$. If $s = (m_1, \ldots, m_k) \in \mathscr{S}$, we write $\sum s$ for $\sum m_i$ and $(x - 1)^s$ for $(x_1 - 1)^{m_1}(x_2 - 1)^{m_2} \ldots (x_k - 1)^{m_k} \in A$.

We claim that $\{(x - 1)^s | s \in \mathscr{S}\}$ is an R-basis for A. Since $|\mathscr{S}| = p^k = |E|$, it suffices to show that if $\sum_{s \in \mathscr{S}} r_s(x - 1)^s = 0$ with $r_s \in R$, then all $r_s = 0$. Suppose, then, that some $r_s \neq 0$. By multiplying the dependence by the highest power of p which fails to annihilate all of the coefficients, we may assume that $pr_s = 0$ for all $s \in \mathscr{S}$. Now, among all $s \in \mathscr{S}$ with $r_s \neq 0$, choose one, say $s_0 = (m_1, \ldots, m_k)$, with $\sum s_0$ minimal. Let $t = (p - 1 - m_1, \ldots, p - 1 - m_k) \in \mathscr{S}$ and multiply the dependence by $(x - 1)^t$. Observe that $r_s(x - 1)^s (x - 1)^t = 0$ if $s \neq s_0$. This is so because if $s \neq s_0$ and $r_s \neq 0$, then $\sum s \geqq \sum s_0$ and hence some entry (say the ith) in the k-tuple, s, is strictly larger than the corresponding entry in s_0. It follows that $(x - 1)^s(x - 1)^t \in (x_i - 1)^p A \subseteq pA$. Since $pr_s = 0$, it follows that $r_s(x - 1)^s(x - 1)^t = 0$. We now have

$$0 = r_{s_0}(x - 1)^{s_0}(x - 1)^t = r_{s_0}(x - 1)^{p-1} \ldots (x_k - 1)^{p-1}.$$

This is a contradiction, since 1 is clearly in the support of $(x_1 - 1)^{p-1} \ldots (x_k - 1)^{p-1}$ and $r_{s_0} \neq 0$.

We now use this basis for A to construct two subgroups. For $s \in \mathscr{S}$, let $l(s) = l$ be the unique integer such that $l(p-1) \leqq \sum s < (l+1)(p-1)$ and let $m(s) = m$ be the unique integer such that $m(p-1) < \sum s \leqq (m+1)(p-1)$. Note that $0 \leqq l(s) \leqq k$ and $-1 \leqq m(s) \leqq k-1$. Also $l(s) = m(s)$ unless $\sum s$ is a multiple of $(p-1)$, in which case $m(s) = l(s) - 1$. Now set

$$U = \{p^{k-l(s)}(x-1)^s | s \in \mathscr{S}\}$$

and

$$V = \{p^{k-m(s)}(x-1)^s | s \in \mathscr{S}\}.$$

It is clear that U is the direct sum of the cyclic groups generated by the given set of generators of U and V is the sum of the subgroups of these cyclic groups generated by the generators of V. It follows that $d(U/V)$ is equal to the number of the generators of U which do not lie in V. This is exactly the number of $s \in \mathscr{S}$ with $\sum s \equiv 0 \mod p-1$. By Lemma 13, we have $d(U/V) = (p^k - 1)/(p-1) + 1$.

The proof will be complete when we show $[U, E] = V$ because it then follows automatically that U is E-invariant. Now if $s, s' \in \mathscr{S}$ with $\sum s = 1 + \sum s'$, then $m(s) = l(s')$. If $s \neq (0, 0, \ldots, 0)$, we can choose i, and $s' \in \mathscr{S}$ with $(x-1)^s = (x-1)^{s'}(x_i - 1)$ and $\sum s = 1 + \sum s'$. Thus $p^{k-m(s)}(x-1)^s = p^{k-l(s')}(x-1)^{s'}(x_i-1)$. It follows that every generator of V is of the form $u(x_i - 1)$ for some generator u of U. (If $s = (0, 0, \ldots, 0)$, then $p^{k-m(s)}(x-1)^s = 0$.) Therefore, $V \subseteq [U, E]$. The generators u which arise this way are exactly those which correspond to $s' \in \mathscr{S}$ where the ith entry of s' is $< p-1$. For each such u, we therefore have $u(x_i - 1) \in V$.

All that remains now in order to prove that $[U, E] \subseteq V$ is to show that $p^{k-l(s)}(x-1)^s(x_i-1) \in V$ whenever the ith entry of s is equal to $p-1$. Recall that

$$(x_i - 1)^p = p \sum_{j=1}^{p-1} r_j (x_i - 1)^j,$$

and thus it follows that

$$(x-1)^s(x_i - 1) = p \sum_{j=1}^{p-1} r_j (x-1)^{s_j}$$

where $s_j \in \mathscr{S}$ and $\sum s_j = j + \sum s - (p-1) > \sum s - (p-1)$. Therefore $m(s_j) \geqq l(s) - 1$ and

$$p^{k-l(s)}(x-1)^s(x_i-1) = \sum_{j=1}^{p-1} r_j p^{k-l(s)+1}(x-1)^{s_j} \in V.$$

The proof of the theorem is now complete.

Reference

1. D. M. Goldschmidt, *2-Signalizer functors on finite groups*, J. Algebra *21* (1972), 321–340.

University of Wisconsin,
Madison, Wisconsin