THE NUMBER OF GENERATORS OF A LINEAR $p$-GROUP

1. M. ISAACS

Let $G$ be a finite $p$-group, having a faithful character $\chi$ 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 $\chi$ 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 $\chi$ be a faithful character of the $p$-group, $G$. Let $f = \chi(1)$ and let $s$ be the number of linear constituents of $\chi$. Then
(a) $d(G) \leq (3/p)(f - s) + s$. Also,
(b) if $p \geq 3$ and $G$ is non-abelian, then $d(G) \leq f - p + 3$.

**Theorem B.** Let $G$ be a $p$-group and let $\chi \in \text{Irr}(G)$ be faithful. Then
$$d(G) \leq \frac{f + (f/p) + 2p - 4}{p - 1}.$$  

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 $\chi$ is a faithful character of the $p$-group, $G$, and that $\chi = \psi + \lambda$, where $\lambda$ is linear. Let $N = \text{Ker} \psi$ so that $\lambda_N$ is faithful and hence $N$ is cyclic. It follows that $d(G) \leq d(G/N) + 1$. By repeated application of this argument, we see that in order to prove Theorem A(a), it suffices to assume that $\chi$ has no linear constituents and show that $d(G) \leq 3f/p$. 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 $\chi$ 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 $N_1, N_2 \triangleleft G$ with $N_1 \cap N_2 = 1$, it does not follow that $d(G) \leq d(G/N_1) + d(G/N_2)$. 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
$$d_G(U) = d(U/(U \cap \Phi(G))).$$
Instead of assuming that $\chi$ is faithful on $G$ and bounding $d(G)$, we shall assume $U \triangleleft G$ and $\chi$ is a character of $G$ with $\chi_U$ faithful and we shall bound $d_\sigma(U)$. Since $d_\sigma(G) = d(G)$, 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 $d_\sigma(U) \leq d_\sigma(H)$ and $d_\sigma(U) \leq d_\sigma(H)$.
(b) If $V \subseteq U$ and $V \triangleleft G$, then $d_\sigma(U) = d_\sigma(V) + d_\sigma(U/V)$.

**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 $d_\sigma(U) \geq d_\sigma(U)$. Also, $d_\sigma(U) = d(U\Phi(G)/\Phi(G)) \leq d(H\Phi(G)/\Phi(G)) = d_\sigma(H)$.

(b). Let $A = U \cap V\Phi(G)$. Then $U \supseteq A \supseteq U \cap \Phi(G)$ and $d_\sigma(U) = d(U/A) + d(A/(U \cap \Phi(G)))$. Now $A = V(U \cap \Phi(G))$ and hence $A/(U \cap \Phi(G)) \cong V/(V \cap \Phi(G))$. Thus $d(A/(U \cap \Phi(G)) = d\sigma(V)$. Finally, we have $(U/V) \cap \Phi(G/V) = (U \cap V\Phi(G))/V = A/V$. Therefore, $d_\sigma(U/V) = d((U/V)/(A/V)) = d(U/A)$. 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 $N_i \triangleleft G$ for $1 \leq i \leq n$. Then

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

**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 $A \triangleleft G$ be abelian with $G/A$ cyclic. Let $Ag$ be a generator of $G/A$. Then
(a) $G' = \{a^{-1}a^p|a \in A\}$ and
(b) $|G'| |A \cap Z(G)| = |A|$.

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

**Lemma 5.** Let $G$ be a $p$-group with abelian $A \triangleleft G$ such that $G/A$ is cyclic. Let $\chi \in \text{Irr}(G)$ with $\chi(1) = p^e$ and suppose $\chi_A$ is faithful. Then
(a) $d_\sigma(A) \leq e + 1$.

Also,
(b) if $\det \chi_A = 1_A$, then $d_\sigma(A) \leq e$; and
(c) if $A$ has exponent $\leq p^e$ then $d_\sigma(A) \leq e$.

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

Now $\chi_Z = p^e\lambda$ where $\lambda$ 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 $|Z| \leq p^e$, and (b) now follows.
To prove (a), let \( C \) be the cyclic group of automorphisms of \( A \) induced by \( G/A \). Since \( \chi_A \) is faithful, \( C \) permutes the set of linear constituents of \( \chi_A \) faithfully. This action is transitive, and hence regular and \( |C| \leq \chi(1) \). Let \( \theta(a) = \Pi_{g \in G}^a \) for \( a \in A \). Then \( \theta \) is an endomorphism of \( A \) and \( \theta(a) = \theta(a^g) \) for \( g \in G \). It follows that \( G' \subseteq \ker \theta = K \). 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 \( |Z : \theta(A)| \leq |C| \leq p^e \). It follows that \( |K : K \cap \Phi(G)| \leq p^e \) and \( d_\phi(K) \leq e \). Since \( d_\phi(K)(A/K) \leq 1 \), we have \( d_\phi(A) \leq e + 1 \) and the proof is complete.

**Lemma 6.** Let \( G \) be a p-group with \( \chi \in \text{Irr}(G) \) and \( \chi(1) = p \). Let \( U \triangleleft G \) and suppose \( \chi_U \) is faithful. Then
(a) \( d_\phi(U) \leq 3 \). Also,
(b) \( d_\phi(U) \leq 2 \) if \( U \) is abelian, \( \det \chi_U = 1_U \) or \( U \) has exponent \( p \), and
(c) \( d_\phi(U) \leq 1 \) if \( U \) is abelian and either \( \det \chi_U = 1_U \) or \( U \) has exponent \( p \).

**Proof.** Use induction on \( |G| \). If there exists \( H \leq G \) with \( U \subseteq H \) and \( \chi_U \) irreducible, then the result follows since \( d_\phi(U) \leq d_\phi(H) \). Supposing, then, that \( U \subseteq G \), we may assume that the restriction of \( \chi \) to every maximal subgroup containing \( U \) is reducible. It follows that \( \chi \) 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 \( \lambda \) is a faithful linear character of \( U \). In this case \( U \) is cyclic and \( d_\phi(U) \leq 1 \).

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

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

**Theorem 7.** Let \( G \) be a p-group, \( \chi \in \text{Irr}(G) \) and \( U \triangleleft G \) with \( \chi_U \) faithful. Let \( \chi(1) = f \) and let \( r \) be the number of (not necessarily distinct) irreducible constituents of \( \chi_U \). Set \( b = (f + (f/p) + 2p - 4)/(p - 1) \). Then:
(a) \( d_\phi(U) \leq b \).
(b) If \( r > 1 \), then
\[
d_\phi(U) \leq b - \frac{(r/p) - 1}{p - 1} - 1.
\]
(c) If \( \det \chi_U = 1_U \), the inequalities in (a) and (b) may be replaced by strict inequalities.
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 $f \geq p^2$.

If $r = 1$, then $\chi_U$ is irreducible and since $d_\phi(U) \leq d_\psi(U)$, 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 $\chi_H$ is irreducible. Since $|H| |G| < |G| |G|$, the inductive hypothesis applies and we conclude that $d_\phi(H) \leq b - 1$ with strict inequality if $\det \chi = 1_G$. It follows that $d_\phi(G) = 1 + d_\phi(H) \leq b$, 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, $H \supset U$. If $\chi_H$ 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 $\theta_i$ 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 $f \geq p^2$, $\theta_1(1) \geq p$ and there exists a maximal subgroup, $W$, of $H$ with $(\theta_1)_W$ reducible. It follows that $U \not\leq W$. Let $\lambda$ be a linear character of $H$ with kernel $W$ and let $\psi = \lambda^g$ and $V = U \cap \text{Ker } \psi$. Then $V \subseteq U \cap W \subseteq U$. Also, $\phi(H) \subseteq W$ and $\phi(H) < G$, so that $\phi(H) \subseteq \text{Ker } \psi$ and consequently, $U/V$ is elementary abelian. If $\psi$ is reducible, then $W < G$, $W = \text{Ker } \psi$ and $U/V$ is cyclic. If $\psi$ 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 $d_{\phi/V}(U/V) = 1$, and thus this is true in either case.

Since $V \subseteq U$, the theorem applies to bound $d_\phi(V)$. Since $\chi_V$ has at least $p^2$ irreducible constituents, we have $d_\phi(V) \leq b - 2$, with strict inequality if $\det \chi_U = 1_G$. Now $d_\phi(U) = d_\phi(V) + d_{\phi/V}(U/V) = 1 + d_\phi(V)$ and thus the theorem holds.

Finally, we assume that $r \geq p^2$ and again choose a maximal $H \supset U$. As before, we may assume that $\chi_H = \theta_1 + \ldots + \theta_p$. Let $\lambda_i = \det \theta_i$, let $\psi = \lambda_1^2$ and let $V = U \cap \text{Ker } \psi$. If $\psi$ is reducible then $\text{Ker } \psi = \text{Ker } \lambda_1$, $U/V$ is cyclic and $d_{\phi/V}(U/V) = 1$. If $\psi$ 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 $d_{\phi/V}(U/V) \leq 2$. Now let $\psi_H = \Pi_{\lambda_i} = \det \chi_H$ and hence if $\det \chi_U = 1_U$, it follows that $d_{\phi/V}(U/V) = 1_{(U/V)}$ and $d_{\phi/V}(U/V) \leq 1$ by Lemma 6(c).

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

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

Let $r_i$ be the number of irreducible constituents of $(\theta_i)_{N_{i-1}}$ and observe that $r_i \geq r/p \geq p$. Let $\hat{\theta}_i$ be the irreducible character of $H/N_i$ corresponding to $\theta_i$ for $1 \leq i \leq p$. We have $\hat{\theta}_i(N_{i-1}/N_{i-1})$ is faithful and has trivial determinant since $N_{i-1} \subseteq V \subseteq \text{Ker } \psi \subseteq \text{Ker } \lambda_i$. 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 $f \geq p^2$ and $r/p \geq r/p^2 \geq 1$, the quantity on the right is an integer and we conclude
\[ d_{H/N_1}(N_{i-1}/N_i) \leq \frac{(f/p) + (f/p^2) + 2p - 4}{p - 1} - \frac{(r/p^2) - 1}{p - 1} - 2. \]
Therefore we have
\[ d_\sigma(V) \leq \frac{f + (f/p) + 2p^2 - 4p - (r/p) - p - 2p}{p - 1} = \frac{f + (f/p) - p - (r/p)}{p - 1} = b - \frac{(r/p) - 1}{p - 1} - 3. \]
Combining this inequality with $d_{\sigma|V}(U/V) \leq 2$ and $d_{\sigma|V}(U/V) \leq 1$ if $\det \chi_V = 1_V$, 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 $f \geq p$, we have
\[ \frac{f + (f/p) + 2p - 4}{p - 1} \leq \frac{3f}{p}. \]

Proof of Theorem A. It has already been noted that it suffices to prove (a), and that, only when $\chi$ has no linear constituents. Let $\chi_1, \chi_2, \ldots, \chi_n$ be the distinct irreducible constituents of $\chi$ and let $K_i = \ker \chi_i$ and $N_i = \bigcap_{j=1}^i K_j$.

Then by Corollary 3, $d(G) = \sum d_{\sigma|N_i}(N_{i-1}/N_i)$ where $N_0 = G$. By Theorem 7 applied to $G/N_i$, we have $d_{\sigma|N_i}(N_{i-1}/N_i) \leq 3\chi_i(1)/p$. It follows that $d(G) \leq 3\chi(1)/p$ 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 $U < G$ be abelian. Suppose $\chi \in \text{Irr}(G)$ with $\chi(1) = f$ and $\chi_U$ faithful. Then $d_\sigma(U) \leq (f - 1)/(p - 1) + 1$.

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 $A < G$, $A$ abelian, $G/A$ cyclic, $\chi \in \text{Irr}(G)$, $\chi_A$ faithful, $\chi(1) = p^e$ and $d_\sigma(A) = e + 1$. The example is as follows.
Let \( A = \langle x_1 \rangle \times \langle x_2 \rangle \times \ldots \times \langle x_{e+1} \rangle \), where the order, \( o(x_i) = p^e \). Define an automorphism, \( \sigma \), of \( A \) by
\[
x_i^\sigma = x_{i+1}^p \text{ for } 1 \leq i \leq e
\]
and \( x_{e+1}^\sigma = x_{e+1} \). We claim that \( o(\sigma) \leq p^e \). Let \( Z = \langle x_{e+1} \rangle \). Then \( \sigma \) 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 \( a^{-1}\theta \in Z \) for all \( a \in A \).

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

Let \( G \) be the semi-direct product, \( A \times \langle \sigma \rangle \). It is clear that \( G' = \Phi(A) \) and hence \( |A : G'| = p^{e+1} \). By Lemma 4, \( |A \cap Z(G)| = p^{e+1} \). However, since \( \langle \sigma \rangle \) acts faithfully on \( A \), we have \( Z(G) \subseteq A \). Since \( Z \subseteq Z(G) \) and \( |Z| = p^{e+1} \), it follows that \( Z(G) = Z \) is cyclic. Therefore, \( G \) has a faithful irreducible character \( \chi \) with \( \chi(1) \leq |G : A| \leq p^e \). 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 \( p^k \), \( k \geq 1 \). There exists an abelian \( p \)-group, \( U \), on which \( E \) acts so that
(a) \( C_U(E) \) is cyclic
and
(b) \( d(U/[U, E]) = (p^k - 1)/(p^e - 1) + 1 \).

Before proving Theorem 11, we discuss some consequences. Let \( G \) be the semi-direct product \( U \times \langle \sigma \rangle \). Then we have \( G' = [U, E] \) and \( G/G' \cong U/[U, E] \times E \). It follows that \( d_G(A) = d(U/[U, E]) = (p^k - 1)/(p^e - 1) + 1 \) and that \( d(G) = d_0(U) + k \). Now \( Z(G) \cap U = C_U(E) \) is cyclic, and thus there exists \( \chi \in \text{Irr}(G) \) with \( C_U(E) \cap \text{Ker} \chi = 1 \). It follows that \( \chi_U \) is faithful. Let \( f = \chi(1) \) so that \( f \leq |G : U| = p^k \). On the other hand, Corollary 8 asserts that \( d_G(U) \leq (f - 1)/(p^e - 1) + 1 \). 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, \( C_U(E) = Z(G) \) and hence \( \chi \) 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, \(0 \leq x_i \leq n\), such that \( \sum x_i \equiv 0 \mod n \). Then
\[
N = \frac{(n + 1)^k - 1}{n} + 1.
\]

https://doi.org/10.4153/CJM-1972-084-0 Published online by Cambridge University Press
Proof. We count the $k$-tuples with $\sum x_i \equiv 0 \bmod n$ 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 $0 \leq y_i \leq n - 1$ and $\sum y_i \equiv 0 \bmod n$.

We may identify the $n^{k-r}$ $(k - r)$-tuples of integers $y_i$, $0 \leq y_i \leq n - 1$ 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 $\sum y_i \equiv 0 \bmod n$, correspond to the elements of the kernel of a homomorphism onto the cyclic group of order $n$. It follows that $F(r) = \binom{k-r}{r}$ and

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

as desired.

Proof of Theorem 11. We shall construct $U$ as an (additive) subgroup of the group ring $R[E] = A$, where $R = \mathbb{Z}/p^{k+1}\mathbb{Z}$. Now $E$ acts on $A$ by right multiplication and $C_A(E) = R(\sum x \in kA)$, 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 $d(U/\langle U, E \rangle) = (p^k - 1)/(p - 1) + 1$.

First we observe that for $x \in E$, we have $(x - 1)^p = p \sum r_i (x - 1)^i$ for suitable $r_i \in R$. This is so because of the polynomial identity $X^p - (X + 1)^p + 1 = p \sum m_i X^i$ where $m_i = - \binom{i}{p}/p \in \mathbb{Z}$. 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 $\mathcal{S} = \{ (m_1, \ldots, m_k) | m_i \in \mathbb{Z}, 0 \leq m_i \leq p - 1 \}$. If $s = (m_1, \ldots, m_k) \in \mathcal{S}$, we write $s$ for $\sum m_i$ and $(x - 1)^s$ for $(x_1 - 1)^{s_1} (x_2 - 1)^{s_2} \ldots (x_k - 1)^{s_k} \in A$.

We claim that $\{ (x - 1)^s | s \in \mathcal{S} \}$ is an $R$-basis for $A$. Since $|\mathcal{S}| = p^k = |E|$, it suffices to show that if $\sum s \in \mathcal{S}$ $r_s (x - 1)^t = 0$ 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 $s \in \mathcal{S}$. Now, among all $s \in \mathcal{S}$ with $r_s \neq 0$, choose one, say $s_0 = (m_1, \ldots, m_k)$, with $\sum s_0$ minimal. Let $t = (p - 1 - m_1, \ldots, p - 1 - m_k) \in \mathcal{S}$ 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 $\sum t \geq \sum s_0$ and hence some entry (say the $i$th) in the $k$-tuple, $s$, is strictly larger than the corresponding entry in $s_0$. It follows that $(x - 1)^t (x - 1)^t \in (x - 1)^p A \subseteq pA$. 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 $s \in \mathcal{S}$, let $l(s) = l$ be the unique integer such that $l(p - 1) \leq \sum s < (l + 1)(p - 1)$ and let $m(s) = m$ be the unique integer such that $m(p - 1) < \sum s \leq (m + 1)(p - 1)$. Note that $0 \leq l(s) \leq k$ and $-1 \leq m(s) \leq k - 1$. Also $l(s) = m(s)$ unless $\sum s$ is a multiple of $(p - 1)$, in which case $m(s) = l(s) - 1$. Now set

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

and

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

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 $s \in \mathcal{S}$ 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 $s, s' \in \mathcal{S}$ with $\sum s = 1 + \sum s'$, then $m(s) = l(s')$. If $s \neq (0, 0, \ldots, 0)$, we can choose $i$, and $s' \in \mathcal{S}$ 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 $s' \in \mathcal{S}$ where the $i$th 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 $i$th 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

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

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

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

The proof of the theorem is now complete.

**Reference**


*University of Wisconsin,*

*Madison, Wisconsin*