PACIFIC JOURNAL OF MATHEMATICS
Vol. 26, No. 2, 1968

KOSTRIKIN'S THEOREM ON ENGEL GROUPS OF PRIME POWER EXPONENT

S. BACHMUTH AND H. Y. MOCHIZUKI

THEOREM **Let $p \geqq 3$ be a prime and $e \geqq 1$ any integer. Then there exists a group $\mathfrak{G}$ which has exponent p^e and Engel length $e(p^e - p^{e-1}) + (p-3)/2$.**

If $e = 1$, this reduces to a Theorem of Kostrikin [2], whose proof employed other methods. Our method yields the additional information, that $\mathfrak{G}$ is a solvable group of class at most $k+1$, where k is the least integer such that $2^{k-1} \geqq p - 2$.

In this paper we give an elementary proof of a theorem due to Kostrikin [2] which states that for any prime $p \geqq 3$, there exists a group of exponent p which has Engel length $(3p-5)/2$. Our proof is conceptually very simple and elementary at least in contrast with Kostrikin's proof, which uses some rather deep results from Lie ring theory [3]. Furthermore, our method establishes that this group has solubility class at most $k+1$ where k is the least integer such that $2^{k-1} \geqq p-2$. (By the solubility class of a group G we mean the least integer k for which $G^{(k)} = 1$, where $G^{(i)}$ is the commutator subgroup of $G^{(i-1)}$ and $G^{(0)} = G$. By the Engel length of G we mean the least positive integer n such that $[a, b; n] = 1$ for all a, b in G, where $[a, b; 1] = [a, b] = aba^{-1}b^{-1}$ and inductively $[a, b; i+1] = [[a, b; i], b]$.)

Our methods actually generalize to groups of prime power exponent. That is, for a given prime $p \geqq 3$ and an integer $e \geqq 1$, there exists a group of exponent p^e which has Engel length $e(p^e - p^{e-1}) + (p-3)/2$. (This contains Kostrikin's Theorem by taking $e = 1$.) Moreover, this group has solubility class at most $k+1$, where k is the least integer such that $2^{k-1} \geqq p-2$. We will however limit our discussion to the case $e = 1$ in the main body of the paper and indicate in an appendix how the same methods and proof yield the above theorem for arbitrary e.

We first give the setting and then an outline of the proof of Kostrikin's Theorem in § 2. The remaining sections give the technical details of the proof until the final section of concluding remarks. Here we discuss possible alternate proofs.

2. Outline of proof.

KOSTRIKIN'S THEOREM. *Let $p \geqq 3$ be a prime. Then there exists a group $\mathfrak{G}$ of exponent p and Engel length $(3p-5)/2$. Furthermore, $\mathfrak{G}$ is of solubility class at most $(k+1)$ where k is the least integer for which $2^{k-1} \geqq (p-2)$.*

We shall construct the group of Kostrikin's Theorem. Let ω be a primitive p^{th} root of unity, and let Z denote the ring of integers. If (p) is the ideal of $Z[\omega]$ generated by $p \in Z$, then we denote the ring $Z[\omega]/(p)$ by $Z_p[\omega]$. An alternative construction of $Z_p[\omega]$ is as follows: Let $Z_p = Z/(p)$ and let $\langle x \rangle$ be a cyclic group of order p. Form the group ring $Z_p\langle x \rangle$ and factor by the ideal generated by $(1 + x + \cdots + x^{p-1}) = (1 - x)^{p-1}$.

We shall call $\omega, \omega^2, \cdots, \omega^{p-1}$ the primitive p^{th} roots of unity. Σ will denote the augmentation ideal of $Z_p[\omega]$, i.e., the ideal generated by $(1 - \omega^i), 1 \leqq i \leqq (p - 1)$. It is well-known that Σ is in fact a principal ideal, generated by any one of the $(1 - \omega^i)$. From [1], we know $\Sigma^{p-1} = 0$ but $\Sigma^{p-2} \neq 0$.

Let $\mathfrak{H}$ be the group of upper triangular $(p - 2) \times (p - 2)$ matrices of $Z_p[\omega]$ generated by

$$A = \begin{bmatrix} \omega & 1 & & & \\ & \omega^2 & & & 0 \\ & & \cdot & & \\ & & & \cdot & \\ 0 & & & & \omega^{p-2} \end{bmatrix}$$

$$B = \begin{bmatrix} \omega & 0 & & & & \\ & \omega^2 & 1 & & & 0 \\ & & \omega^3 & 1 & & \\ & & & \cdot & \cdot & \\ & & & & \cdot & \cdot \\ 0 & & & & & 1 \\ & & & & & \omega^{p-2} \end{bmatrix}$$

We first prove that $\mathfrak{H}$ is a group of exponent p. In fact, we show that in the ring $\mathfrak{R}$ of upper triangular $(p - 2) \times (p - 2)$ matrices each H in $\mathfrak{H}$ satisfies the cyclotomic identity; i.e. if $I =$ identity matrix, $I + H + H^2 + \cdots + H^{p-1} = (I - H)^{p-1} = 0$.

We do not directly compute the Engel length of the group $\mathfrak{H}$, but we instead use a form of the Magnus representation in order to increase the solubility class of our group by one. (cf. [4].) Let t_1 and t_2 be indeterminates which commute with all elements of $\mathfrak{R}$. Let $\mathfrak{G}$ be the group of 2×2 matrices over $\mathfrak{R}[t_1, t_2]$ generated by

$$R = \begin{bmatrix} A & t_1 \\ 0 & 1 \end{bmatrix}, \qquad S = \begin{bmatrix} B & t_2 \\ 0 & 1 \end{bmatrix}.$$

We then show $\mathfrak{G}$ satisfies the conditions for Kostrikin's Theorem.

To do this, we first note that $\mathfrak{G}$ is a group of exponent p by observing that if

$$\begin{bmatrix} D & Pt_1 + Qt_2 \\ 0 & 1 \end{bmatrix}$$

is in $\mathfrak{G}$, then

$$\begin{bmatrix} D & Pt_1 + Qt_2 \\ 0 & 1 \end{bmatrix}^p = \begin{bmatrix} D^p & (I + D + \cdots + D^{p-1})(Pt_1 + Qt_2) \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Using the notations $B^D = DBD^{-1}$ and $C_n = [A, B; n]$, we then note that

$$[R, S; (3p-7)/2] = \begin{bmatrix} C_{(3p-7)/2} & P_{(3p-7)/2}t_1 + Q_{(3p-7)/2}t_2 \\ 0 & 1 \end{bmatrix}$$

where

$$P_{(3p-7)/2} = (I - B^{C(3p-9)/2}) \cdots (I - B^{C_2})(I - B^{C_1})(I - B^A)$$

and the form of $Q_{(3p-7)/2}$ is unimportant.

By establishing that $P_{(3p-7)/2} \neq 0$ in $\mathfrak{N}$, we show that

$$[R, S; (3p-7)/2] \neq 1 ,$$

i.e., that $\mathfrak{G}$ has Engel length $\geqq (3p-5)/2$. Almost all the difficulties of the proof is involved in showing $P_{(3p-7)/2} \neq 0$.

In Sections 4, 5 and 6, which are devoted to establishing that $P_{(3p-7)/2}$ is not the zero matrix, we analyze the structure of B^{C_n} and C_n. If $M \in \mathfrak{N}$, let $\bar{M}$ be the $(p-3) \times (p-3)$ matrix obtained from M by deleting the first row and first column of M. Then $\bar{M}_1\bar{M}_2 = \overline{M_1M_2}$, i.e., the first row and first column have no effect on the other rows and colums during multiplication. In § 4, we first study $\bar{B}^{\bar{C}_n}$ and $\bar{C}_n$, the key conclusion here being that $\bar{B}^{\bar{C}_n} \equiv \bar{B}$ modulo Σ^{n+1}. In § 5 we establish the necessary information concerning the first rows of B^{C_n} and C_n. Section 6 is devoted to using these results to analyze the $(p-2)^{\text{th}}$ column of P_n, and in particular the $(1, p-2)$ entry of $P_{(3p-7)/2}$ which proves to be non zero (i.e., not in Σ^{p-1}).

We point out that the proof as it stands is meant only for primes $p \geqq 7$. For $p = 3, 5$, the proof can easily be modified and we omit the details.

Throught the rest of the paper except the last section, we assume $p \geqq 7$.

3. The groups $\mathfrak{H}$ and $\mathfrak{G}$. We first note that any element of $\mathfrak{H}$ is of the following form:

$$H_1 = \begin{bmatrix} \omega^i & & & * \\ & \omega^{2i} & & \\ & & \ddots & \\ 0 & & & \omega^{(p-2)i} \end{bmatrix}$$

where i is relatively prime to p, or

$$H_2 = \begin{bmatrix} 1 & & & * \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{bmatrix} = I + N$$

where N is upper triangular with diagonal entries zero and hence is nilpotent, i.e., $N^{p-2} = 0$.

PROPOSITION 1. *$\mathfrak{H}$ has exponent p. In fact,*

$$I + H + H^2 + \cdots + H^{p-1} = (I - H)^{p-1} = 0$$

for all $H \in \mathfrak{H}$.

Proof. Since $I - H^p = (I - H)^p$, we need only show $H \in \mathfrak{H}$ satisfies the cyclotomic identity. Suppose H is of type H_1. Then, the characteristic polynomial of H over $Z_p[\omega]$ divides

$$\prod_{i=1}^{p-1} (x - \omega^i) = 1 + x + x^2 + \cdots + x^{p-1} .$$

By the Cayley-Hamilton Theorem $I + H + \cdots + H^{p-1} = 0$.

If $H = I + N$, $N^{p-2} = 0$, then we have that $[I - (I + N)]^{p-1} = N^{p-1} = 0$. This completes the proof.

Elements of $\mathfrak{G}$ have the form

$$\begin{bmatrix} D & Pt_1 + Qt_2 \\ 0 & 1 \end{bmatrix}$$

where $D \in \mathfrak{H}$ and $P, Q \in \mathfrak{R}$.

We can easily show by induction that

$$\begin{bmatrix} D & Pt_1 + Qt_2 \\ 0 & 1 \end{bmatrix}^i = \begin{bmatrix} D^i & (1 + D + \cdots + D^{i-1})(Pt_1 + Qt_2) \\ 0 & 1 \end{bmatrix}$$

Putting $i = p$ and applying Proposition 1 we immediately have.

PROPOSITION 2. *$\mathfrak{G}$ has exponent p.*

The generators R and S of $\mathfrak{G}$ where described in § 2. We now examine the form of a commutor $[R, S; n]$. Recall that $B^D = DBD^{-1}$, $D \in \mathfrak{H}$, and $C_n = [A, B; n]$.

PROPOSITION 3.

$$[R, S] = \begin{bmatrix} C_1 & (I - B^A)t_1 + (A - C_1)t_2 \\ 0 & 1 \end{bmatrix}$$

and, in general, for $n \geqq 2$,

$$[R, S; n] = \begin{bmatrix} C_{n-1} & P_n t_1 + Q_n t_2 \\ 0 & 1 \end{bmatrix}$$

where

$$P_n = (I - B^{C_{n-1}}) \cdots (I - B^{C_1})(I - B^A) .$$

Proof. By straightforward computation and an induction argument.

REMARK. We will also use the notation $P_1 = (I - B^A)$.

PROPOSITION 4. *Let k be the least integer for which $2^{k-1} \geqq (p - 2)$. Then $\mathfrak{H}$ is of solubility class at most k, and $\mathfrak{G}$ is of solubility class at most $(k + 1)$.*

Proof. If we can show that $\mathfrak{H}$ has solubility class at k, then the use of the Magnus representation increases the solubility class by 1, so that $\mathfrak{G}$ has solubility class at most $(k + 1)$. (cf. [4].)

To prove that $\mathfrak{H}$ has solubility class at most k, we must show $\mathfrak{H}^{(k)} = 1$. If $M = (x_{ij}) \in \mathfrak{R}$, then for fixed j, we define the diagonal of M consisting of the entries $x_{i,i+j}$, $1 \leqq i \leqq (p - 2) - j$, as the j^{th} upper diagonal. Let $\mathscr{M}$ be the ideal in $\mathfrak{R}$ of all matrices with main diagonal consisting of zeros. Then it is well-known that $\mathscr{M}^n$ consists entirely of matrices whose j^{th} upper diagonal entries are all zero, $1 \leqq j \leqq (n - 1)$.

$\mathfrak{H}^{(1)}$ consists of matrices of form $I + M$, $M \in \mathscr{M}$. We assert that $\mathfrak{H}^{(k)}$ consists entirely of matrices of form $I + M$, $M \in \mathscr{M}^{2^{k-1}}$. Suppose the assertion is true for k. If M is in $\mathscr{M}^{2^k}$ and B is any element of $\mathfrak{H}^{(k)}$, then since $\mathscr{M}$ is an ideal, $B(I + M)B^{-1} = I + BMB^{-1}$, where BMB^{-1} is in $\mathscr{M}^{2^k}$. Also if M_1, M_2 are in $\mathscr{M}^{2^k}$ then $(I + M_1)(I + M_2) = I + M_3$ where $M_3 \in \mathscr{M}^{2^k}$. Thus, since $\mathfrak{H}^{(k+1)}$ is generated as a normal subgroup of H by all commutators $[x, y]$ for x, y in $\mathfrak{H}^{(k)}$, to complete our induction assertion, we need only show $[I + M_1, I + M_2] \equiv I \bmod \mathscr{M}^{2^k}$

with $I + M_1$ and $I + M_2$ in $\mathfrak{H}^{(k)}$, i.e., M_1 and M_2 in $\mathscr{A}^{2k-1}$. But since $(I + M)^{-1} = (I - M + M^2 - \cdots)$ for M in $\mathscr{A}$, we have $(I + M_i)^{-1} \equiv I - M_i \bmod \mathscr{A}^{2k}$ for M_i in $\mathscr{A}^{2k-1}$. Hence,

$$[I + M_1, I + M_2] \equiv (I + M_1)(I + M_2)(I - M_1)(I - M_2) \equiv I \bmod \mathscr{A}^{2k}.$$

This proves our assertion.

Thus when $2^{k-1} \geqq (p - 2)$, $\mathfrak{H}^{(k)} = 1$, and the solubility class of $\mathfrak{H}$ is k. This completes the proof of Proposition 4.

4. **The forms of $\bar{C}_n$ and $\bar{B}^{\bar{C}_n}$.** We recall that

$$A = \begin{bmatrix} \omega & 1 & & & & \\ & \omega^2 & & & & \\ & & \omega^3 & & & \\ & & & \ddots & & \\ & 0 & & & \ddots & \\ & & & & & \omega^{p-2} \end{bmatrix},$$

$$B = \begin{bmatrix} \omega & 0 & & & & \\ & \omega^2 & 1 & & & \\ & & \omega^3 & 1 & & \\ & & & \ddots & \ddots & \\ & 0 & & & \ddots & 1 \\ & & & & & \omega^{p-2} \end{bmatrix}.$$

Thus

$$A^{-1} = \begin{bmatrix} \omega^{p-1} & -\omega^{p-3} & & & & \\ & \omega^{p-2} & & & & \\ & & \omega^{p-3} & & & \\ & & & \ddots & & \\ & 0 & & & \ddots & \\ & & & & & \omega^2 \end{bmatrix},$$

$$B^{-1} = \begin{bmatrix} \omega^{p-1} & 0 & \cdot & \cdot & \cdot & 0 \\ & \omega^{p-2} & -u_{23} & u_{24} & -u_{25} \cdots & -u_{2,p-2} \\ & & \omega^{p-3} & -u_{34} & u_{35} \cdots & \\ & & & \ddots & & \\ & & 0 & & \ddots & \\ & & & & & \omega^2 \end{bmatrix}.$$

where the (i, j) entry of $B^{-1}, j \geqq i \geqq 2$, is

$$(-1)^{i+j}u_{ij} = (-1)^{i+j}\omega^{(p+i)+(p-i-1)+\cdots+(p-i)} .$$

We also compute

$$B^A = \begin{bmatrix} \omega & (1-\omega^{p-1}) & \omega^{p-3} & & & & \\ & \omega^2 & \omega^{p-1} & & 0 & & \\ & & \omega^3 & \omega^{p-1} & & & \\ & & & \cdot & \cdot & & \\ & 0 & & & \cdot & \cdot & \\ & & & & & \cdot & \omega^{p-1} \\ & & & & & & \omega^{p-2} \end{bmatrix} .$$

We next observe by a direct computation that

$$C_1 = B^A B^{-1} = I + N_1$$

where $N_1 = (c_{ij}^{(1)})$ has (i, j) entry $c_{12}^{(1)} \equiv 0 \pmod{\Sigma}$, $c_{13}^{(1)} \equiv 1 \pmod{\Sigma}$ and for $j > i \geqq 2$,

$$c_{ij}^{(1)} = (-1)^{i+j}(\omega^i u_{ij} - \omega^{p-1}u_{i+1,j}) \equiv 0 \pmod{\Sigma} . \tag{4.1}$$

LEMMA 1. *For $2 \leqq i < j < (p-2)$, we have $c_{i+1,j+1}^{(1)} = \omega^{i-j}c_{ij}^{(1)}$.*

Proof.

$$\begin{aligned} c_{i+1,j+1}^{(1)} &= (-1)^{(i+1)+(j+1)}(\omega^{i+1}\omega^{(p-i-1)+(p-i-2)+\cdots+(p-j-1)} \\ &\quad - \omega^{p-1}\omega^{(p-i-2)+(p-i-3)+\cdots+(p-j-1)}) \\ &= (-1)^{i+j}(\omega^{i+1}\omega^{(p-j-1)}\omega^{-(p-i)}\omega^{(p-i)+(p-i-1)+\cdots+(p-j)} \\ &\quad - \omega^{p-1}\omega^{-(p-i-1)}\omega^{(p-j-1)}\omega^{(p-i-1)+(p-i-2)+\cdots+(p-j)}) \\ &= (-1)^{i+j}\omega^{i-j}(\omega^i u_{ij} - \omega^{p-i}u_{i+1,j}) . \end{aligned}$$

This completes the proof.

The next lemma gives the information about $\bar{C}_n$ and $\bar{B}^{\bar{C}_n}$ that we will need.

LEMMA 2. *Let $C_n = I + N_n$ where $N_n = (c_{ij}^{(n)})$.*
(a) *$\bar{B}^{\bar{C}_n} \equiv \bar{B} \pmod{\Sigma^{n+1}}$ for all n.*
(b) *$\bar{C}_n \equiv I \pmod{\Sigma^n}$ for all n.*
(c) *For $2 \leqq i < (p-2)$, $c_{i+j,j+1}^{(n)} = \omega^{i-j}c_{ij}^{(n)} \pmod{\Sigma^{n+1}}$.*

Proof. For $n = 1$, part (c) is Lemma 1 and part (b) follows from (4.1). We shall prove (b) and (c) by an induction argument. Assume (b) and (c) hold for n. We first prove that (a) is true.

$$\begin{aligned}\bar{C}_n^{-1} &= (I - \bar{N}_n + \bar{N}_n^2 - \bar{N}_n^3 + \cdots) \\ &\equiv (I - \bar{N}_n) \pmod{\Sigma^{n+1}}\end{aligned}$$

since $\bar{N}_n^k \equiv 0 \pmod{\Sigma^{kn}}$. (Here we are using the obvious fact that N_n has only nonzero entries above the main diagonal and hence is nilpotent.) Thus,

$$\begin{aligned}\bar{B}^{\bar{C}_n} &\equiv (I + \bar{N}_n)B(I - \bar{N}_n) \pmod{\Sigma^{n+1}} \\ &\equiv \bar{B}\bar{N}_n\bar{B} - \bar{B}\bar{N}_n \pmod{\Sigma^{n+1}}\end{aligned}$$

since $\bar{N}_n B \bar{N}_n \equiv \pmod{\Sigma^{2n}}$. Hence to prove (a) we must show

$$\bar{N}_n\bar{B} - \bar{B}\bar{N}_n \equiv 0 \pmod{\Sigma^{n+1}} .$$

For $j \geqq (i+1)$, the (i,j) entry of $\bar{N}_n\bar{B}$ is $(c^{(n)}_{i+1,j} + \omega^{j+1}c^{(n)}_{i+1,j+1})$, and the (i,j) entry of $\bar{B}\bar{N}_n$ is $(\omega^{i+1}c^{(n)}_{i+1,j+1} + c^{(n)}_{i+2,j+1})$. Thus, for $j \geqq i+1$, the (i,j) entry of $\bar{N}_n\bar{B} - \bar{B}\bar{N}_n$ is

$$(c^{(n)}_{i+1,j} - c^{(n)}_{i+2,j+1}) + (\omega^{j+1} - \omega^{i+1})c^{(n)}_{i+1,j+1} .$$

But by our induction hypothesis for part (c), we have

$$(c^{(n)}_{i+1,j} - c^{(n)}_{i+2,j+1}) \equiv (1 - \omega^{i-j+1})c^{(n)}_{i+1,j}$$

and this is in Σ^{n+1} since our induction hypothesis for part (b) is that all entries of $\bar{N}_n$ are in Σ^n. Similarly

$$(\omega^{j+1} - \omega^{i+1})c^{(n)}_{i+1,j+1} \in \Sigma^{n+1}$$

since by hypothesis all entries of $\bar{N}_n$ are in Σ^n. Thus, the (i,j) entry of $\bar{N}_n\bar{B} - \bar{B}\bar{N}_n$ is in Σ^{n+1}, and hence $\bar{B} \equiv \bar{B}^{\bar{C}_n} \pmod{\Sigma^{n+1}}$. Thus for a fixed n, (b) and (c) implies (a).

We now show that (b) is true for $n+1$. We first note that

$$\begin{aligned}\bar{C}_{n+1} &= \bar{B}^{\bar{C}_n}\bar{B}^{-1} \\ &\equiv I + \bar{N}_n - \bar{B}\bar{N}_n\bar{B}^{-1} \pmod{\Sigma^{n+1}} .\end{aligned}$$

Hence, to prove (b) holds for $(n+1)$ we must show that

$$\bar{N}_n - \bar{B}\bar{N}_n\bar{B}^{-1} \equiv 0 \pmod{\Sigma^{n+1}} .$$

For $j \geqq (i+1)$ the (i,j) entry of $\bar{B}\bar{N}_n\bar{B}^{-1}$ is

$$\begin{aligned}&\sum_{k=i+1}^{(j-1)} (\omega^{i+1}c^{(n)}_{i+1,k+1} + c^{(n)}_{i+2,k+1})(-1)^{k+j}u_{k+1,j+1} \\ &\quad + \omega^{p-j-1}(\omega^{i+1}c^{(n)}_{i+1,j+1} + c^{(n)}_{i+2,j+1}) = \omega^{p-j+i}c^{(n)}_{i+1,j+1} \\ &\quad + \sum_{k=i+1}^{j-2} [(-1)^{k+j}u_{k+1,j+1}\omega^{i+1}c^{(n)}_{i+1,k+1} + (-1)^{k+j+1}u_{k+2,j+1}c^{(n)}_{i+2,k+2}] \\ &\quad + (\omega^{p-j-1}c^{(n)}_{i+2,j+1} - u_{j,j+1}\omega^{i+1}c^{(n)}_{i+1,j}) .\end{aligned}$$

By the induction hypothesis, all the summands after the first term have the form

$$\begin{aligned}\pm(uc_{i+1,l} - vc_{i+2,l+1}) &\equiv \pm(u - v\omega^{i-l+1}) \\ &\equiv 0 \,(\mathrm{mod}\, \Sigma^{n+1}) ,\end{aligned}$$

where u and v are powers of ω. Thus, the (i, j) entry of $\bar{B}\bar{N}_n\bar{B}^{-1}$ is just $\omega^{p-j+i}c^{(n)}_{i+1,j+1} \,(\mathrm{mod}\, \Sigma^{n+1})$. Hence for $j \geqq i + 1$, the (i, j) entry of $(\bar{N}_n - \bar{B}\bar{N}_n\bar{B}^{-1})$ is

$$c^{(n)}_{i+1,j+1} - \omega^{p-j+i}c^{(n)}_{i+1,j+1} \equiv 0 \,(\mathrm{mod}\, \Sigma^{n+1}) .$$

The proof of (b) of Lemma 1 is now complete.

To prove (c), we first note that we actually have

$$\bar{C}_{n+1} \equiv I + \bar{N}_n - \bar{B}\bar{N}_n\bar{B}^{-1} \,(\mathrm{mod}\, \Sigma^{2n})$$

since the neglected terms all contain at least two factors of $\bar{N}_n$. Thus if $n \geqq 2$, we have

$$\bar{C}_{n+1} \equiv I + \bar{N}_n - \bar{B}\bar{N}_n\bar{B}^{-1} \,(\mathrm{mod}\, \Sigma^{n+2}) .$$

Suppose, therefore, that $n = 1$.

Recomputing $\bar{B}^{\bar{c}_1}$ modulo Σ^3, we have

$$\begin{aligned}\bar{B}^{\bar{c}_1} &\equiv (I + \bar{N}_1)\bar{B}(I - \bar{N}_1 + \bar{N}_1^2) \,(\mathrm{mod}\, \Sigma^3) \\ &\equiv \bar{B} + \bar{N}_1\bar{B} - \bar{B}\bar{N}_1 - (\bar{N}_1\bar{B} - \bar{B}\bar{N}_1)\bar{N}_1 \,(\mathrm{mod}\, \Sigma^3) .\end{aligned}$$

Since in the proof of part (a) we showed $(\bar{N}_1\bar{B} - \bar{B}\bar{N}_1) \equiv 0 \,(\mathrm{mod}\, \Sigma^2)$, we see that $\bar{B}^{\bar{c}_1} \equiv (\bar{B} + \bar{N}_1\bar{B} - \bar{B}\bar{N}_1) \,(\mathrm{mod}\, \Sigma^3)$ and hence

$$\bar{C}_2 \equiv I + \bar{N}_1 - \bar{B}\bar{N}_1\bar{B}^{-1} \,(\mathrm{mod}\, \Sigma^3) .$$

Thus for all integers n, we have

$$\bar{C}_{n+1} \equiv I + \bar{N}_n - \bar{B}\bar{N}_n\bar{B}^{-1} \,(\mathrm{mod}\, \Sigma^{n+2}) .$$

In the range $(p - 3) > j > i$, $\bar{N}_n - \bar{B}\bar{N}_n\bar{B}$ has (i, j) entry,

$$\begin{aligned}&(c^{(n)}_{i+1,j+1} - \omega^{p-j+i}c^{(n)}_{i+1,j+1}) \\ &\quad - \sum_{k=i+1}^{j-2} [(-1)^{k+j}u_{k+1,j+1}\omega^{i+1}c^{(n)}_{i+1,k+1} + (-1)^{k+j+1}u_{k+2,j+1}c^{(n)}_{i+2,k+2}] \\ &\quad - (\omega^{p-j-1}c^{(n)}_{i+2,j+1} - u_{j,j+1}\omega^{i+1}c^{(n)}_{i+1,j}) .\end{aligned}$$

We want to show that multiplying this entry by ω^{i-j} gives us the $(i + 1, j + 1)$ entry.

$$\omega^{i-j}c^{(n)}_{i+1,j+1}(1 - \omega^{p-j+i}) = c^{(n)}_{i+2,j+2}(1 - \omega^{p-j+i}) ,$$

by our induction hypothesis. We next compute

$$\begin{aligned}\omega^{i-j}u_{k+1,j+1}\omega^{i+1}c^{(n)}_{i+1,k+1} &= \omega^{i-j}\omega^{(p-k-1)+(p-k-2)+\cdots+(p-j-1}\omega^{i+1}c^{(n)}_{i+1,k+1}\\ &= \omega^{i-j}\omega^{-k-1}\omega^{(p-k-2)+\cdots+(p-j-2)}\omega^{j+2}\omega^{i+1}c^{(n)}_{i+1,k+1}\\ &= u_{k+2,j+2}\omega^{i+2}\omega^{i-k}c^{(n)}_{i+1,k+1}\\ &= u_{k+2,j+2}\omega^{i+2}c^{(n)}_{i+2,k+2}\ .\end{aligned}$$

Similarly, we find that

$$\begin{aligned}\omega^{i-j}u_{k+2,j+1}c^{(n)}_{i+2,k+2} &= \omega^{i-j}\omega^{(p-k-2)+(p-k-3)+\cdots+(p-j-1)}c^{(n)}_{i+2,k+2}\\ &= \omega^{i-j}\omega^{-k-2}u_{k+3,j+2}\omega^{j+2}c^{(n)}_{i+2,k+2}\\ &= u_{k+3,j+2}\omega^{i-k}c^{(n)}_{i+2,k+2}\\ &= u_{k+3,j+2}c^{(n)}_{i+3,k+3}\ .\end{aligned}$$

Thus,

$$\begin{aligned}&\omega^{i-j}\sum_{k=i+1}^{j-2}\left[(-1)^{k+j}u_{k+1,j+1}\omega^{i+1}c^{(n)}_{i+1,k+1} + (-1)^{k+j+1}u_{k+2,j+1}c^{(n)}_{i+2,k+2}\right]\\ &= \sum_{k=i+2}^{j-1}\left[(-1)^{k+j+1}u_{k+1,j+2}\omega^{i+2}c^{(n)}_{i+2,k+1} + (-1)^{k+j+2}u_{k+2,j+2}c^{(n)}_{i+3,k+2}\right]\ .\end{aligned}$$

Finally, computing in a similar manner, we see that

$$\omega^{i-j}(\omega^{p-j-1}c^{(n)}_{i+2,j+1} - u_{j,j+1}\omega^{i+1}c^{(n)}_{i+1,j}) = (\omega^{p-j-2}c^{(n)}_{i+3,j+2} - u_{j+1,j+2}\omega^{i+2}c^{(n)}_{i+2,j+1})\ .$$

Combining these results, we see that ω^{i-j} times the (i, j) entry of $\bar{N}_n - \bar{B}\bar{N}_n\bar{B}^{-1}$ is indeed the $(i+1, j+1)$ entry. Thus, (c) of Lemma 2 is proved.

5. The first rows of C_n and B^{C_n}. With the help of Lemma 2, we will prove

LEMMA 3. *Let* $C_n = I + N_n$, $N_n = (c^{(n)}_{ij})$. *Then the first row of* N_n *has the following form*:

$$\begin{aligned}c^{(n)}_{12} \equiv 0 \pmod{\Sigma^n},\ c^{(n)}_{13} \equiv 0 \pmod{\Sigma^{n-1}},\ \cdots,\ c^{(n)}_{1j}\\ \equiv 0 \pmod{\Sigma^{n-j+2}},\ \cdots,\ c^{(n)}_{1,n+1} \equiv 0 \pmod{\Sigma}\ ,\end{aligned}$$

and

$$c^{(n)}_{1,n+2} \equiv 1 \pmod{\Sigma},\ 1 \leqq n \leqq (p-4)\ .$$

As a corollary of Lemma 3 we have

LEMMA 4. *For* $1 \leqq n \leqq (p-5)$, *the first row of* B^{C_n} *has the following form*: *The* (i, j) *entry is* $\equiv 0 \pmod{\Sigma^{n-j+3}}$ *for* $1 \leqq j \leqq (n+2)$ *and the* $(1, n+3)$ *entry is* $\equiv 1 \pmod{\Sigma}$.

Proof of Lemma 4. We are assuming the truth of Lemma 3. We

first note that $C_n^{-1} \equiv (I - N_n) \pmod{\Sigma^n}$ since $N_n^k \equiv 0 \pmod{\Sigma^{n+1}}$ for $k \geqq 2$ by Lemma 2. Moreover, since our matrices are triangular, the $(1, 2)$ entry of C_n^{-1} is $-c_{12}^{(n)}$. Therefore,

$$B^{C_n} \equiv (I + N_n)B(I - N_n) \pmod{\Sigma^n}$$

and for the $(1, 2)$ entries we get equality rather than congruence. (This congruence is not good enough for the $(1, 2)$ entry since we must show that the $(1, 2)$ entry is $\equiv 0 \pmod{\Sigma^{n+1}}$.) In fact, we can say

$$B^{C_n} \equiv B + (N_nB - BN_n) \pmod{\Sigma^n}$$

where again the $(1, 2)$ entries of both sides are equal. This is because $N_nBN_n \equiv 0 \pmod{\Sigma^n}$ and N_nBN_n has the $(i, i + 1)$ entries all zero.

For $(p - 2) \geqq j \geqq 2$, N_nB has $(1, j)$ entry $(c_{1,j-1}^{(n)} + \omega^j c_{1,j}^{(n)})$ and BN_n has the $(1, j)$ entry $\omega c_{1,j}^{(n)}$. Therefore, $N_nB - BN_n$ has $(1, j)$ entry, $(n + 2) \geqq j \geqq 2$,

$$c_{1,j}^{(n)} + (\omega^j - \omega)c_{1,j}^{(n)} \equiv 0 \pmod{\Sigma^{n-j+3}} ,$$

and $(1, n + 3)$ entry

$$c_{1,n+2}^{(n)} + (\omega^{n+3} - \omega)c_{1,n+3}^{(n)} \equiv 1 \pmod{\Sigma}$$

by Lemma 3. Since for $j \geqq 2$, the $(1, j)$ entry of B is zero, we have proved Lemma 4.

Proof of Lemma 3. C_1 (described in § 4) satisfies Lemma 3. For an induction argument we assume that the lemma holds for n.

From the proof of Lemma 4,

$$C_{n+1} = B^{C_n}B^{-1} \equiv I + N_n - BN_nB^{-1} \pmod{\Sigma^n}$$

where the $(1, 2)$ entries of both sides are equal. An easy calculation (since only 2×2 triangular matrices are involved) shows that the $(1, 2)$ entry is $(1 - \omega^{p-1})c_{12}^{(n)}$ and hence by induction is in Σ^{n+1}. For $(n + 2) \geqq j > 2$, BN_nB^{-1} has $(1, j)$ entry

$$(-1)^j\omega c_{12}^{(n)}u_{2j} + (-1)^{j+1}\omega c_{13}^{(n)}u_{3j} + \cdots + (-1)\omega c_{1,j-1}^{(n)}u_{j-1,j} + \omega^{p-j+1}c_{1,j}^{(n)}$$
$$\equiv \omega^{p-j+1}c_{1,j}^{(n)} \pmod{\Sigma^{n-j+3}} ,$$

by our induction hypothesis. Thus, for $(n + 2) \geqq j \geqq 3$, the $(1, j)$ entry of $(N_n - BN_nB^{-1})$ is

$$(1 - \omega^{p-j+1})c_{1,j}^{(n)} \equiv 0 \pmod{\Sigma^{n-j+3}} ,$$

the $(1, n + 3)$ entry of BN_nB^{-1} is

$$\equiv -\omega u_{j-1,j}c_{1,n+2}^{(n)} + \omega^{p-n-2}c_{1,n+3}^{(n)} \pmod{\Sigma} ,$$

and hence the $(1, n+3)$ entry of $(N_n - BN_nB^{-1})$ is

$$\equiv \omega u_{j-1,j} c_{1,n+2}^{(n)} + (1 - \omega^{p-n-2}) c_{1,n+3}^{(n)} \equiv 1 \pmod{\Sigma} ,$$

since $c_{1,n+2}^{(n)} \equiv 1 \pmod{\Sigma}$. Our proof is therefore complete.

6. **Proof of Kostrikin's theorem ($P_{(3p-7)/2} \neq 0$).** The results of the two previous sections has afforded us with just enough information about $(I - B^{C_i})$ so that we can now determine the relevant information about

$$P_n = \prod_{i=1}^{n-1} (I - B^{C_i})(I - B^A) .$$

The following lemma completes the proof of Kostrikin's Theorem.

LEMMA 5. (a) *For $1 \geqq n \geqq (p-4)$, the last column of $P_n = (d_{i,j}^{(n)})$ has the following form:*

$$d_{p-2-n,p-2} \equiv \pm\omega^{p-1} \pmod{\Sigma}, \; d_{p-1-n,p-2} \equiv 0 \pmod{\Sigma},$$
$$d_{p-n,p-2} \equiv 0 \pmod{\Sigma^2}, \cdots, d_{p-3,p-2} \equiv 0 \pmod{\Sigma^{n-1}} ,$$

and

$$d_{p-2,p-2} = (1 - \omega^{p-2})^n \equiv 0 \pmod{\Sigma^n} .$$

(b) *For $(3p-7)/2 \geqq n \geqq (p-3)/2$, $d_{1,p-2}^{(n)} \equiv \pm\omega^{p-1}(1-\omega)^q \pmod{\Sigma^{q+1}}$ where $q = n - (p-3)/2$. In particular, the $(1, p-2)$ entry of $P_{(3p-7)/2}$ is $\equiv \pm\omega^{p-1}(1-\omega)^{p-2}$ which is not in Σ^{p-1} and hence is not the zero element of $Z_p[\omega]$.*

Proof. We represent $(I - B^{C_n})$ by

$$\begin{bmatrix} (1-\omega) & b_{12}^{(n)} & b_{13}^{(n)} & \cdot & \cdot & \cdot & b_{1,p-2}^{(n)} \\ & (1-\omega^2) & (-1+b_{23}^{(n)}) & b_{24}^{(n)} & \cdots & & \\ & & (1-\omega^3) & (-1+b_{34}^{(n)}) & \cdots & & \\ & & & (1-\omega^4) & \cdots & & \\ & 0 & & & \cdot & \cdot & (-1+b_{p-3,p-2}^{(n)}) \\ & & & & & & (1-\omega^{p-2}) \end{bmatrix}$$

where

$$b_{1,j}^{(n)} \equiv 0 \pmod{\Sigma^{n-j+3}}, \; 2 \leqq j \leqq n+2, \; b_{1,n+3}^{(n)} \equiv -1 \pmod{\Sigma},$$

and $b_{i,k}^{(n)} \equiv 0 \pmod{\Sigma^{n+1}}$ if $i > 1$ by Lemmas 2 and 4.

$P_1 = (I - B^A)$ satisfies property (a) of the lemma (B^A is exhibited in § 4). As our induction hypothesis, for $2 \leqq n < p-4$, suppose P_n satisfies (a) of the lemma. $P_{n+1} = (I - B^{C_n})P_n$. We may compute

modulo Σ^{n+1}, and thus modulo Σ^{n+1}, we have P_{n+1} equal to the following product.

$$P_{n+1} = \begin{bmatrix} (1-\omega) & b_{12}^{(n)} & b_{13}^{(n)} & \cdots & b_{1,p-2}^{(n)} \\ & (1-\omega^2) & -1 & & \\ & & (1-\omega^3) & -1 & \\ & & & \ddots & \\ & & 0 & & -1 \\ & & & & (1-\omega^{p-2}) \end{bmatrix} \cdot \begin{bmatrix} & & d_{1,p-2}^{(n)} \\ & & d_{2,p-2}^{(n)} \\ \text{Irrelevant} & & \vdots \\ & & d_{p-3,p-2}^{(n)} \\ & & (1-\omega^{p-2})^n \end{bmatrix}.$$

The $(p-2-n-1, p-2)$ entry of P_{n+1} is

$$(1-\omega^{p-2-n-1})d_{p-2-n-1,p-2} - d_{p-2-n,p-2} \equiv \pm\omega^{p-1} \pmod{\Sigma}$$

by the induction hypothesis. For $1 \leqq i \leqq n$, the $(p-3-n+i, p-2)$ entry of P_{n+1} is $(k = p-3-n+i)(1-\omega^k)d_{k,p-2} - d_{k+1,p-2} \equiv 0 \pmod{\Sigma^i}$ by the induction hypothesis on P_n. The $(p-2, p-2)$ entry of the right side is $(1-\omega^{p-2})^{n+1}$. Thus, by induction, we have prove (a) of Lemma 5.

To prove (b) of Lemma 5, we first note that for $m = (p-5)/2$, $b_{1,p+1/2}^{(m)} \equiv -1 \pmod{\Sigma}$ and $d_{p+1/2,p-2}^{(m)} \equiv \pm\omega^{p-1} \pmod{\Sigma}$. Then $d_{1,p-2}^{(m+1)} \equiv \pm\omega^{p-1} \pmod{\Sigma}$ since all entries in the first row of $(I - B^{C_n})$ to the left of $b_{1,p+1/2}^{(m)}$ are in Σ and all entries in the last column of P_n below $d_{p+1/2,p-2}^{(m)}$ are also in Σ. Thus, $P_{(p-3)/2}$ satisfies part (b) of the lemma. For $n+1 > (p-3)/2$, we note that

$$\begin{aligned} d_{1,p-2}^{(n+1)} = (1-\omega)d_{1,p-2}^{(n)} &+ b_{12}^{(n)}d_{2,p-2}^{(n)} + \cdots + b_{1,p+1/2}^{(n)}d_{p+1/2,p-2}^{(n)} \\ &+ \cdots + b_{1,p-3}^{(n)}d_{p-3,p-2}^{(n)} + b_{1,p-2}^{(n)}(1-\omega^{p-2})^n . \end{aligned} \tag{5.1}$$

If $(n+1) = (p-1)/2$, then $b_{1j}^{(n)}$, $2 \leqq j \leqq (p-1)/2$, are in Σ, $b_{1,(p+1)/2,p-2}^{(n)}$ and $d_{(p+1)/2,p-2}^{(n)}$ are each in Σ, and $d_{i,p-2}^{(n)}$, $(p+3)/2 \leqq i \leqq (p-3)$, and $(1-\omega^{p-2})^n$ are in Σ^2. Thus $d_{1,p-2}^{((p-1)/2)} \equiv \pm\omega^{p-1}(1-\omega) \bmod \Sigma^2$.

For $(n+1) > (p-1)/2$, it is now clear that all other terms in (5.1) will be in one higher power of Σ than the term $(1-\omega)d_{1,p-2}^{(n)}$ since either the first factor of the second factor lies in a higher power of Σ for each increase in n. By induction we may assume that $d_{1,p-2}^{(n)} \equiv \pm\omega^{p-1}(1-\omega)^q \pmod{\Sigma^{q+1}}$ where $q = n-(p-3)/2$. Thus, in forming $d_{1,p-2}^{(n+1)}$, all the terms after the first in (5.1) are $\equiv 0$ modulo Σ^{q+1},

and hence $d_{1,p-2}^{(n+1)} \equiv \pm\omega^{p-1}(1-\omega)^{q+1} \pmod{\Sigma^{q+2}}$. This completes the proof of part (b) of Lemma 5.

6. **Concluding remarks.** The question naturally arises as to how far the number $n_p = (3p-5)/2$ is from the largest possible. That n_p is probably not the Engel length of the restricted Burnside group $B(p)$ of exponent p has also been demonstrated by Kostrikin [2] who showed that for $p = 5$, the Engel length of $B(5)$ is 6 while n_p is 5. Our proof has yielded the additional information that the group $G(p)$ whose Engel length is n_p has solubility class $k+1$ where k is the least integer satisfying $2^k > p-1$. In [1] Theorem D, it has been shown that the Engel length of groups of exponents p and solubility class $k+1$ is at most $k(p-1)+1$. The actual number for these groups is therefore between $(3p-5)/2$ and $k(p-1)+1$.

One possibility of enlarging the number $(3p-5)/2$ which comes immediately to mind is to replace the entries of the matrices by elements of a "larger" ring. That is, instead of taking entries from $Z_p[\omega]$, use entries from the group ring of an abelian group of exponent p; e.g., if C_p is the cyclic group of order p, use entries from $Z_p[C_p \times C_p]$ modulo a suitable ideal. The suitable ideal would have to be the cyclotomic ideal (see [1] for definitions) so that the propositions in §3 remain valid. But the results in [1] (specifically Theorem B) indicate that there would be no change in the first result. In fact, for a prime p, the results in [1] indicate that going to any finite number of variables would make no difference and one may as well use one variable as we have done.

Finally, we conclude with the observation, based upon computer calculations for small primes, that it should be possible to give an even more elementary proof of Kostrikin's Theorem. Namely, instead of using $(p-2) \times (p-2)$ matrices, enlarge the matrices to $p \times p$. Specifically, let

$$A = \begin{bmatrix} 1 & 1 & & & & \\ & \omega & & & & \\ & & \omega^2 & & 0 & \\ & & & \cdot & & \\ & 0 & & & \cdot & \\ & & & & & \omega^{p-1} \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 & & & & & \\ & \omega & 1 & & & & \\ & & \omega^2 & 1 & & & \\ & & & \cdot & \cdot & & \\ & & & & \cdot & \cdot & \\ & & & & & \cdot & 1 \\ & & & & & & \cdot \\ & & & & & & \omega^{p-1} \end{bmatrix}$$

and let as before $C_1 = [A, B]$, $C_n = [A, B; n]$. The group generated by A, B is a group of exponent p, and the idea now is to show directly that $C_{(3p-5)/2} \neq 1$. Conceptually this is simpler than the proof given in

this paper, since it avoids the trick of using the Magnus representation, and furthermore one now has a concrete matrix group which is amenable to computer calculations (for small primes) to aid in discovering other properties of these groups. Computer calculations for $p = 5, 7, 11$ have shown that indeed for these primes, the $(1, p)$ entry of $C_{(3p-7)/2}$ is not in Σ^{p-1} and hence is nonzero. In fact, the pattern shown makes it quite clear what happens for arbitrary p. Namely, the $(1, p)$ entry is a unit for each C_n, $n < p - 1$, and finally the $(1, p)$ entry of C_{p-1} falls into Σ. But, unfortunately this entry, in fact, falls into Σ^2 and thereafter the $(1, p)$ entry of C_p falls into Σ^4, the $(1, p)$ entry of C_{p+1} falls into Σ^6, etc.; until finally the $(1, p)$ entry of $C_{(3p-7)/2}$ lies in Σ^{p-3} and the $(1, p)$ entry of $C_{(3p-5)/2}$ lies in Σ^{p-1}; i.e. $C_{(3p-7)/2} \neq 1$. Because of the jumps in the highest power of Σ in which the $(1, p)$ entry lies at these later stages, one must have exact knowledge of the terms in the matrices used to compute C_n in order to demonstrate that the entries do not fall into even higher powers of Σ. The bookkeeping involved here is rather horrendous, and because of the difficult technical problems involved we have abandoned such a direct proof of Kostrikin's Theorem. The method we used enabled us at each stage to calculate modulo Σ^i if the entries involved were in Σ^{i-1}. Much more precise information is required in a direct proof.

Appendix.

THEOREM. *Let $p \geqq 3$ be a prime and $e \geqq 1$ any integer. Then there exists a group $\mathfrak{G}$ which has exponent p^e and Engel length $e(p^e - p^{e-1}) + (p - 3)/2$. Furthermore, $\mathfrak{G}$ has solubility class at most $k + 1$, where k is the least integer for which $2^{k-1} \geqq (p - 2)$.*

Proof. Let

$$A = \begin{bmatrix} \omega & 1 & & & \\ & \omega^2 & & & \\ & & \cdot & & 0 \\ & & & \cdot & \\ & 0 & & \cdot & \\ & & & & \omega^{p-2} \end{bmatrix} \quad B = \begin{bmatrix} \omega & 0 & & & & \\ & \omega^2 & 1 & & & \\ & & \omega^3 & \cdot & & 0 \\ & & & \cdot & \cdot & \\ & & & & \cdot & \cdot \\ & 0 & & & \cdot & 1 \\ & & & & & \omega^{p-2} \end{bmatrix}$$

where ω is a primitive p^{eth} root of unity. We first observe that any element H in the group $\mathfrak{H}$ generated by A and B satisfies the cyclotomic identity $1 + H + H^2 + \cdots + H^{p^e-1} = 0$. To see this, we note that either H has the form

$$H_1 = \begin{bmatrix} \gamma & & & & \\ & \gamma^2 & & * & \\ & & \ddots & & \\ & 0 & & \ddots & \\ & & & & \gamma^{p-2} \end{bmatrix}$$

where γ is a primitive $p^{j\text{th}}$ root of unity, $1 \leqq j \leqq e$, or H has the form

$$H_2 = \begin{bmatrix} 1 & & & & \\ & 1 & & * & \\ & & \ddots & & \\ & 0 & & \ddots & \\ & & & & 1 \end{bmatrix} = I + N$$

where $N^{p-2} = 0$.

We have $1 + H_1 + \cdots + H_1^{p^e-1} = 0$, since the characteristic polynomial of H_1, $\prod_{i=1}^{p-2}(Z - \gamma^i)$, divides $1 + Z + Z^2 + \cdots + Z^{p^e-1}$. To show that

$$\begin{aligned} 1 + H_2 + H_2^2 + \cdots + H_2^{p^e-1} &= I + (I + N) + (I + N)^2 + \cdots + (I + N)^{p^e-1} \\ &= 0 , \end{aligned}$$

we shall show that the coefficient of N^i, $1 \leqq i \leqq (p - 2)$, is congruent to zero modulo p^e. The coefficient of N^i is

$$\sum_{j=0}^{p^e-1-i} \binom{i + j}{i} = \binom{i + p^e - i}{i + 1} = \binom{p^e}{i + 1} .$$

Since $(i + 1) \leqq (p - 1)$, we have $\binom{p^e}{i + 1} \equiv 0 \pmod{p^e}$.

It thus follows that $\mathfrak{H}$ is a group with exponent p^e and as before we let $\mathfrak{G}$ be the group of 2×2 matrices over $Z(\mathfrak{H})[t_1, t_2]$ generated by

$$R = \begin{bmatrix} A & t_1 \\ 0 & 1 \end{bmatrix} \text{ and } S = \begin{bmatrix} B & t_2 \\ 0 & 1 \end{bmatrix} .$$

The proof that $\mathfrak{G}$ satisfies all the conditions of the theorem now proceeds exactly as in the prime case by replacing p by p^e where appropriate. The only remark necessary to make is that the augmentation ideal Σ of $Z_{p^e}[\omega]$ now satisfies $\Sigma^{e(p^e-p^{e-1})} = 0$, but $\Sigma^{e(p^e-p^{e-1})-1} \neq 0$, (see [1]).

We would like to mention here the authors' conviction that this

work could not have been possible without the aid of a computer. The computer calculations for small primes not only showed us that the result is possible but also enabled us to discover the method of proof. It is a pleasure for us to acknowledge the generous assistance of Professor Glen Culler, who placed the computing facilities of the University of California at Santa Barbara at our disposal, and to Miss Helen Smith, who did outstanding programming work for us.

REFERENCES

[1] S. Bachmuth, H. Heilbronn, H. Y. Mochizuki, *Metabelian Burnside groups*, (submitted for publication).

[2] A. I. Kostrikin, *On Engel properties of groups with the identical relation* $x^{p^a} = 1$, Dokl. Akad. Nauk SSSR **135** (1960), 524-526 (Russian); translated as Soviet Math. Dokl. **1** (1961), 1282-1284.

[3] ———, *On the connection between periodic groups and Lie rings*, Izv. Akad. Nauk SSSR Ser. Mat. **21** (1957), 289-310 (Russian).

[4] W. Magnus, *On a Theorem of Marshall Hall*, Ann. of Math. (2) **40** (1939), 764-768.

Received March 14, 1967. This work was supported by the U.S. Navy, Grant No. NONR-4222 (09).

UNIVERSITY OF CALIFORNIA
SANTA BARBARA