ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 1, Number 3, Summer 1971

p-SUBGROUPS OF CORE-FREE QUASINORMAL SUBGROUPS

FLETCHER GROSS[1]

1. **Introduction.** The main object of this paper is to obtain bounds on the nilpotence class and derived length of a core-free quasinormal subgroup. Here the subgroup H of G is quasinormal in G if $HK = KH$ for each subgroup K of G; H is core-free if H contains no nonidentity normal subgroup of G. Since Itô and Szép [3] proved that a core-free quasinormal subgroup of a finite group is nilpotent, the problem of determining the class and derived length of the core-free quasinormal subgroup H of the finite group G is equivalent to the problem of determining the class and derived length of the p-subgroups of H. The principal result of the present paper is that if H is a core-free quasinormal subgroup of the (possibly infinite) group G and P is a subgroup of H generated by elements of order dividing p^n where p is a prime, then $x^{p^n} = 1$ for all x in P, P is nilpotent of class $\leqq$ Max $\{1, p^{n-1} - 1\}$, and $d(P)$, the derived length of P, is $\leqq [(n+1)/2]$ if $p = 2$, and $d(P) \leqq n$ if $p > 2$.

Bradway, Gross, and Scott [1] proved that if p is a prime and n is a positive integer $< p$, then there is a finite p-group which contains a core-free quasinormal subgroup of class n and exponent p^2. Thus the upper bound on the class given above is best-possible when $n \leqq 2$. In Theorem 5.2 of this paper it is shown that if p is a prime and n is a positive integer, then there is a finite p-group which contains a core-free quasinormal subgroup of class n and exponent $< np^3$. This theorem not only shows that for any fixed prime p the class of a core-free quasinormal p-subgroup can be arbitrarily large (previously, I do not believe it even was known if a core-free quasinormal 2-subgroup could be nonabelian), but also implies that for $n > 2$ there is a finite p-group which contains a core-free quasinormal subgroup of exponent p^n and class p^{n-2}. Hence if our upper bound on the class is too big, it is too big by less than a factor of p.

2. **Notation and assumed results.** If S is a subset of the group G, then $\langle S \rangle$ is the subgroup of G generated by the elements of S. If H is a

Received by the editors January 14, 1970 and, in revised form, March 24, 1970.
AMS 1970 *subject classifications.* Primary 20D15; Secondary 20F30, 20D40.
Key words and phrases. Quasinormal subgroup, p-group, nilpotence class, derived length.
[1]Research supported in part by NSF Grant GP-12028.

subgroup of G, then $N_H(S)$ and $C_H(S)$ are the normalizer and centralizer, respectively, of S in H. $|H|$ and $|G:H|$ denote the order of H and the index of H in G, respectively. H_G, the core of H in G, equals $\bigcap H^x$ where $H^x = x^{-1}Hx$ and the intersection is taken over all $x \in G$. H is core-free in G if, and only if, $H_G = 1$. If G is a p-group, then $\Omega_r(G)$ is the subgroup of G generated by all elements of order at most p^r and $\mho^r(G)$ is the subgroup generated by all p^rth powers of elements of G. $Z(G)$ is the center of G.

Commutators are defined inductively by $[x, y] = x^{-1}y^{-1}xy$ and $[x_1, \cdots, x_{n+1}] = [[x_1, \cdots, x_n], x_{n+1}]$. If A and B are subgroups of G, then $[A, B] = \langle [x, y] \mid x \in A, y \in B \rangle$. The subgroups $G^{(n)}$ and $L_n(G)$ of G are defined inductively by $G = G^{(0)} = L_1(G)$, $G^{(n+1)} = [G^{(n)}, G^{(n)}]$, and $L_{n+1}(G) = [L_n(G), G]$. If G is solvable, $d(G)$, the derived length of G, is the smallest integer d such that $G^{(d)} = 1$. If G is nilpotent, $\mathrm{cl}(G)$, the class of G, is the smallest integer c such that $L_{c+1}(G) = 1$.

The following results are known and so we state them without proof.

2.1. LEMMA. *If H is a quasinormal subgroup of G and σ is a homomorphism of G, then H^σ is a quasinormal subgroup of G^σ.*

2.2. LEMMA. *Let H be a subgroup of G and N a normal subgroup of G contained in H. Then H is quasinormal in G if, and only if, H/N is quasinormal in G/N.*

2.3. LEMMA. *If H is a quasinormal subgroup of G and K is a subgroup of G, then $H \cap K$ is a quasinormal subgroup of K.*

2.4. LEMMA. *Let p be a prime, $t = p + 2 + (-1)^p$, and $p^e = t - 1$. (Thus $e = 1$ if p is odd and $e = 2$ if $p = 2$.) Then for $r \geqq 0$, $t^{p^r} - 1 \equiv p^{r+e} \pmod{p^{r+e+1}}$. If p^r is the highest power of p dividing the positive integer a, then the highest power of p dividing $(t^a - 1)$ is p^{r+e}.*

2.5. LEMMA. *Let G be a cyclic group of order p^n where p is a prime and $p^n > 2$. Let $t = p + 2 + (-1)^p$ and $p^e = t - 1$. Then the automorphism of G defined by $x \to x^t$ for all x in G has order p^{n-e}.*

2.6. LEMMA ([1]). *If H is a quasinormal subgroup of G, $x \in G$, and $|\langle x \rangle : H \cap \langle x \rangle|$ is infinite, then $x \in N_G(H)$.*

2.7. THEOREM ([3]). *Assume H is a core-free quasinormal subgroup of the finite group G. Then H is nilpotent and a Sylow p-subgroup of H is a core-free quasinormal subgroup of a Sylow p-subgroup of G.*

3. Upper bounds on the class and derived length.

3.1. LEMMA. *Assume $G = \langle x \rangle H$ is a finite p-group where H is a core-free quasinormal subgroup of G. Then*

(a) *$\Omega_1(G)$ is elementary abelian.*

(b) $\Omega_r(G) = \Omega_r(H)\Omega_r(\langle x \rangle)$, $\mho^r(\Omega_r(G)) = 1$, *and* $H\Omega_r(G)/\Omega_r(G)$ *is core-free in* $G/\Omega_r(G)$ *for any positive integer r.*

(c) $\mathrm{cl}(\Omega_2(G)) \leqq p - 1$.

(d) *If x has order p^n and $n \geqq 2$, then* $\log_p(|\Omega_1(G)|) \leqq p^{n-2}(p-1)$.

PROOF. If $x^p = 1$, then H must be normal in G. Since $H_G = 1$, this implies that $G = \langle x \rangle$ and so the lemma is trivial. We now assume that the order of x is at least p^2. Since $H_G = 1$, $C_H(x) = 1$. It follows from this that $C_G(x) = \langle x \rangle$. Since $Z(G) \neq 1$, we must have $\Omega_1(\langle x \rangle) \subseteq Z(G)$.

If y is an element of order p in G, then, since $G = H\langle x \rangle$ and since $|H\langle y \rangle : H| \leqq p$, it follows that $H\langle y \rangle \subseteq H\Omega_1(\langle x \rangle)$. Thus $\Omega_1(G)$ is contained in $H\Omega_1(\langle x \rangle) = H \times \Omega_1(\langle x \rangle)$. Using the fact that $\Omega_1(\Omega_1(G)) = \Omega_1(G)$, we obtain $\Omega_1(G) = \Omega_1(\langle x \rangle) \times \Omega_1(H)$. Since $\Omega_1(G)$ is normal in G and $\Omega_1(H)$ is core-free in G, $\Omega_1(G)$ is the subdirect product of the groups $\{\Omega_1(G)/(\Omega_1(H))^g \mid g \in G\}$. This implies that $\Omega_1(G)$ is elementary abelian.

Now let $M/\Omega_1(G)$ be the core of $H\Omega_1(G)/\Omega_1(G)$ in $G/\Omega_1(G)$. Then $M = \Omega_1(G)(H \cap M) = \Omega_1(\langle x \rangle) \times (H \cap M)$. Since M is normal in G, $H \cap M$ is normal in M, and $H \cap M$ is core-free in G, the same argument as above yields that M is elementary abelian. Thus M is contained in $\Omega_1(G)$ and so $H\Omega_1(G)/\Omega_1(G)$ is core-free in $G/\Omega_1(G)$.

We now have proved (b) for $r = 1$. Assume now that $r > 1$ and use induction on r. Let σ be the natural homomorphism of G onto $G/\Omega_1(G)$. Then $(\Omega_r(G))^\sigma = \Omega_{r-1}(G^\sigma)$, $(\Omega_r(H))^\sigma = \Omega_{r-1}(H^\sigma)$, and $(\Omega_r(\langle x \rangle))^\sigma = \Omega_{r-1}(\langle x^\sigma \rangle)$. By induction, $\mho^{r-1}(\Omega_{r-1}(G^\sigma)) = 1, \Omega_{r-1}(G^\sigma) = \Omega_{r-1}(H^\sigma)\Omega_{r-1}(\langle x^\sigma \rangle)$, and $H^\sigma\Omega_{r-1}(G^\sigma)/\Omega_{r-1}(G^\sigma)$ is core-free in $G^\sigma/\Omega_{r-1}(G^\sigma)$. This immediately implies $\mho^r(\Omega_r(G)) = 1$, $\Omega_r(G) = \Omega_r(H)\Omega_r(\langle x \rangle)\Omega_1(G) = \Omega_r(H)\Omega_r(\langle x \rangle)$, and $H\Omega_r(G)/\Omega_r(G)$ is core-free in $G/\Omega_r(G)$. Thus (b) is proved.

To prove (c), let N be the core of $\Omega_2(H)$ in $\Omega_2(G)$. Now $\Omega_2(G)$ is the subdirect product of the groups $\{\Omega_2(G)/N^g \mid g \in G\}$. It follows from this that $\mathrm{cl}(\Omega_2(G)) = \mathrm{cl}(\Omega_2(G)/N)$. Suppose this class is $\geqq p$. Then we must have $|\Omega_2(G)/N| \geqq p^{p+1}$. But N is the kernel of the representation of $\Omega_2(G)$ as a permutation group on the cosets of $\Omega_2(H)$. Since $|\Omega_2(G) : \Omega_2(H)| = p^2$, we find that $\Omega_2(G)/N$ is isomorphic to a Sylow p-subgroup of the symmetric group on p^2 letters. This implies that $\Omega_2(G)/N$ is generated by its elements of order p. This is impossible, however, since by (a) applied to $\Omega_2(G)/N$ we have that $\Omega_1(\Omega_2(G)/N)$ is elementary abelian. This contradiction proves that $\mathrm{cl}(\Omega_2(G)) \leqq p - 1$.

If x has order p^n, $n \geqq 2$, and $y \in \Omega_1(G)$, then (c) implies

$$[y, x^{p^{n-2}}, \cdots, x^{p^{n-2}}] = 1$$

where $x^{p^{n-2}}$ occurs $p - 1$ times. If $\Omega_1(G)$ is written additively and X is the automorphism of $\Omega_1(G)$ induced by x, then the commutator relation above becomes $(X^{p^{n-2}} - 1)^{p-1} = 0$. Thus $(X - 1)^{p^{n-2}(p-1)} = 0$. But since $|C_{\Omega_1(G)}(x)| = p$, the Jordan normal form of X has only one block. This implies that the minimal polynomial of X is $(X - 1)^m$ where $p^m = |\Omega_1(G)|$. Then $m \leqq p^{n-2}(p - 1)$ which proves (d).

3.2. Lemma. *Suppose $G = \langle x \rangle H$ is a finite p-group where H is a core-free quasinormal subgroup of G. Assume G has exponent p^n. Then*

(a) $\mathrm{cl}(G) \leqq \mathrm{Max}\,\{1, p^{n-1} - 1\}$.

(b) $d(G) \leqq [(n + 1)/2]$ *if* $p = 2$ *and* $d(G) \leqq n$ *if* $p > 2$.

Proof. We use induction on n. (a) follows from Lemma 3.1 if $n \leqq 2$. Thus we assume $n > 2$. Let $t = p^{n-2}$, $N = \Omega_1(G)$, and $|N| = p^m$. Now G/N satisfies the hypothesis of the lemma with n replaced by $n - 1$. Hence by induction $\mathrm{cl}(G/N) \leqq t - 1$. Therefore $L_t(G) \subseteq N$. But certainly $[N, G, \cdots, G] = 1$ where G occurs m times. From this follows $L_{t+m}(G) = 1$ and so $\mathrm{cl}(G) \leqq t + m - 1$. Since $m \leqq p^{n-2}(p - 1)$ from the previous lemma, (a) follows at once.

(b) is proved in [1] when p is odd. Thus assume $p = 2$. Then (b) follows from (a) if $n \leqq 2$. Hence we also assume $n > 2$. $G/\Omega_2(G)$ satisfies the hypothesis of the lemma with n replaced by $n - 2$. By induction, therefore, $d(G/\Omega_2(G)) \leqq [(n - 1)/2]$. Since $\Omega_2(G)$ is abelian from Lemma 3.1, we obtain $d(G) \leqq [(n - 1)/2] + 1 = [(n + 1)/2]$.

3.3. Theorem. *Assume H is a core-free quasinormal subgroup of G. If x and y are elements of H such that $x^m = y^m = 1$ where m is a positive integer, then $(xy)^m = 1$.*

Proof. Suppose $(xy)^m \neq 1$. Since $H_G = 1$, there is an element z in G such that $(xy)^m \notin H^z$. It follows from Lemma 2.6 that $|\langle z \rangle H : H|$ is finite. If K is the core of H in $H\langle z \rangle$, then $H\langle z \rangle/K$ is a finite group satisfying the hypothesis but not the conclusion of the theorem. Thus it suffices to prove the theorem in the special case $G = \langle z \rangle H$ and $|G|$ finite. From Theorem 2.7, H is nilpotent. Therefore it is sufficient to prove the theorem when $m = p^n$ and p is a prime.

Now let P be a Sylow p-subgroup of H and S a Sylow p-subgroup of G. By Theorem 2.7, P is a core-free quasinormal subgroup of S. x and y belong to P since $x^{p^n} = y^{p^n} = 1$. From $G = \langle z\rangle H$ we conclude that $S = P\langle w\rangle$ for some element w. Thus the hypothesis of Lemma 3.1 is satisfied and so $\mho^n(\Omega_n(S)) = 1$. This implies that $(xy)^{p^n} = 1$.

3.4. THEOREM. *Assume H is a core-free quasinormal subgroup of G. Suppose A is a nonempty subset of H such that $x^{p^n} = 1$ for all $x \in A$ where p is a prime and n a positive integer. Then with $P = \langle A\rangle$ we have*

(a) *P is a p-group of exponent $\leqq p^n$.*

(b) *P is nilpotent of class $\leqq$ Max $\{1, p^{n-1} - 1\}$.*

(c) *$d(P) \leqq [(n+1)/2]$ if $p = 2$ and $d(P) \leqq n$ if $p > 2$.*

PROOF. (a) follows directly from the preceding theorem. If $x \in G$, let N_x be the core of H in $H\langle x\rangle$. Then P is the subdirect product of the groups $\{P/(N_x \cap P) \mid x \in G\}$. Thus in proving (b) and (c) it suffices to assume that $G = H\langle x\rangle$. If $|G : H|$ is infinite, then $H = H_G = 1$ from Lemma 2.6. Thus we may assume that $|G : H|$ is finite. This immediately implies that $|G| = |G : H_G|$ is finite.

Then H is nilpotent and a Sylow p-subgroup of H is a core-free quasinormal subgroup of a Sylow p-subgroup of G. Thus in proving (b) and (c) there is no loss of generality in assuming that G is a finite p-group and $G = H\langle x\rangle$.

Now let K be the core of $\Omega_n(H)$ in $\Omega_n(G)$. Then by Lemma 3.1(b) $\Omega_n(G)/K$ satisfies the hypothesis of Lemma 3.2. Since $\Omega_n(G)$ is the subdirect product of the groups $\{\Omega_n(G)/K^g \mid g \in G\}$, $\mathrm{cl}(\Omega_n(G)) = \mathrm{cl}(\Omega_n(G)/K)$ and $d(\Omega_n(G)) = d(\Omega_n(G)/K)$. From Lemma 3.2 and the fact that $P \subseteq \Omega_n(G)$, the theorem now follows.

It is shown in [1] that there is a finite p-group G which contains a core-free quasinormal subgroup H such that H has exponent p^2 and $\mathrm{cl}(H) = p - 1$. Thus the upper bound in Theorem 3.4 (b) is attainable when $n = 2$. Also the inequality $d(P) \leqq [(n+1)/2]$ is false for $n = 2$ and $p > 2$. For $n > 2$ I do not know whether the upper bound in Theorem 3.4(b) is best-possible or not. It will be shown in §5, however, that if $n > 2$, then there is a finite p-group which contains a core-free quasinormal subgroup of exponent p^n and class p^{n-2}.

4. **A sufficient condition for quasinormality.** The biggest problem in constructing an example of a core-free quasinormal subgroup is proving that the subgroup in question is quasinormal. In this section we prove a theorem which will imply that we indeed do have quasinormal subgroups in the examples constructed in §5. We begin with a lemma.

4.1. LEMMA. *Let G be a finite p-group generated by two elements x and y. Assume that $\langle x\rangle \cap \langle y\rangle = 1$ and $x^{-1}yx = y^t$ where $t = p + 2 + (-1)^p$. Then the following are true*:

(a) *If A is a subgroup of $\langle x\rangle$, and B is a subgroup of $\langle y\rangle$, then $\Omega_r(AB) = \Omega_r(A)\Omega_r(B)$ and $\mho^r(AB) = \mho^r(A)\mho^r(B)$ for all nonnegative integers r.*

(b) *$\langle x\rangle$ is quasinormal in G.*

PROOF. Since $\langle y\rangle$ is normal in G and B is characteristic in $\langle y\rangle$, AB is a subgroup of G. Now if i and j are any positive integers, then a straightforward calculation yields $(x^iy^j)^p = x^{ip}y^{jn}$ where $n = (t^{ip} - 1)/(t^i - 1)$. From Lemma 2.4, n is divisible by p but not by p^2. By induction on r, it follows that $(x^iy^j)^{p^r} = x^{ip^r}y^{jm}$ where m is divisible by p^r but not by p^{r+1}. Since $\langle x\rangle \cap \langle y\rangle = 1$, $x^iy^j = 1$ if, and only if, $x^i = y^j = 1$. From this we obtain that the order of (x^iy^j) is the maximum of the orders of x^i and y^j. This implies that $\Omega_r(AB) = \Omega_r(A)\Omega_r(B)$ for all r. That $\mho^r(AB) = \mho^r(A)\mho^r(B)$ follows from the fact that $(x^iy^j)^{p^r} \in \mho^r(\langle x^i\rangle)\mho^r(\langle y^j\rangle)$. Thus (a) is proved.

To prove (b) let N be the core of $\langle x\rangle$ in G. Then G/N satisfies the hypothesis of the lemma. Hence, if $N \neq 1$, $\langle x\rangle/N$ is quasinormal in G/N by induction on G. By Lemma 2.2 this would imply that $\langle x\rangle$ is quasinormal in G. Thus we may assume that $N = 1$.

Now suppose y has order p^n. Since $\langle x\rangle$ is core-free in G, $n \geqq 2$. Thus $n \geqq e$ where $p^e = t - 1$. Lemma 2.5 implies that x has order p^{n-e}. Suppose K is a subgroup of G such that $K\langle x\rangle \neq \langle x\rangle K$. Since $\langle x, y^p\rangle$ satisfies the hypothesis of the lemma, we may assume by induction that $\langle x\rangle$ is quasinormal in $\langle x, y^p\rangle$. Hence $K \not\subseteq \langle x, y^p\rangle$. But by (a), $\langle x, y^p\rangle = \Omega_{n-1}(G)$. This implies that $K \cap \mho^{n-1}(G) \neq 1$. Since $\mho^{n-1}(G) = \mho^{n-1}(\langle y\rangle) = \Omega_1(\langle y\rangle)$, we obtain $\Omega_1(\langle y\rangle) \subseteq K$.

Now $G/\Omega_1(\langle y\rangle)$ satisfies the hypothesis of the lemma. By induction, therefore, $\langle x\rangle\Omega_1(\langle y\rangle)$ is quasinormal in G. Hence $\langle x\rangle\Omega_1(\langle y\rangle)K = \langle x\rangle K$ is a subgroup of G. This contradicts $K\langle x\rangle \neq \langle x\rangle K$ and so the lemma is proved.

4.2. THEOREM. *Assume that G is a finite p-group containing subgroups H and V and elements x and y such that*

(a) $G = \langle y\rangle H$,

(b) *V is a normal elementary abelian subgroup of G,*

(c) $V = (V \cap \langle y\rangle) \times (V \cap H)$,

(d) $H = (V \cap H)\langle x\rangle$,

(e) *$x^{-1}yx = y^t$ where $t = p + 2 + (-1)^p$,*

(f) $\mathrm{cl}(\Omega_2(\langle y\rangle)V) \leqq p - 1$.

Then H is quasinormal in G.

PROOF. To prove this theorem, which generalizes Theorem 3.2 of [1], we assume that G is a minimal counterexample. Then G has a subgroup K such that $HK \neq KH$.

Let $U = V \cap H$. If $U = 1$, then H is quasinormal in G because of Lemma 4.1. Hence $U \neq 1$. Lemma 4.1 also implies that HV/V is quasinormal in G/V. Therefore HV is quasinormal in G which implies that $V \not\subseteq H$. This immediately implies that $V \cap \langle y \rangle = \Omega_1(\langle y \rangle) \neq 1$. Since H is not normal in G, y must have order p^r where $r \geqq 2$.

Now suppose H contains a nontrivial normal subgroup N of G. Then G/N satisfies the hypothesis of the theorem. Due to the minimality of G, we must have that H/N is quasinormal in G/N. But this is impossible since H is not quasinormal in G. Thus $H_G = 1$. From $G = \langle y \rangle H$, we obtain $H_G = \bigcap_i H^{y^i}$. This implies $C_H(y) = 1$. We conclude from this and from Lemma 2.5 that x has order p^{r-e} where $p^e = t - 1$. If $p \neq 2$, then $r \geqq 2 > 1 = e$. If $p = 2$ and $r = 2$, then $H = U$ and $\langle y \rangle = \Omega_2(\langle y \rangle)$ which, because of (f), implies that G is abelian, an impossibility. Thus in all cases, $r > e$.

I now assert that $\Omega_1(\langle x \rangle) \subseteq U$. For suppose $z = x^{p^{r-e-1}}$. Then $\langle z \rangle = \Omega_1(\langle x \rangle)$ and $[y, z] = y^{s-1}$ where $s - 1 = t^{p^{r-e-1}} \equiv p^{r-1} \pmod{p^r}$ by Lemma 2.4. Thus $\langle y^{s-1} \rangle = \Omega_1(\langle y \rangle) = \langle y \rangle \cap V$. On the other hand, $\langle y \rangle$ is properly contained in $\langle y \rangle V = \langle y \rangle U$. Thus U has a nonidentity element u which normalizes $\langle y \rangle$. Then $1 \neq [y, u] \subseteq \langle y \rangle \cap V$. Clearly $\langle y, u \rangle$ has class 2 and so $[y, u^k] = [y, u]^k$ for all k. Since $\langle y \rangle \cap V$ is cyclic of order p, $[y, u^k] = [y, z]$ for some k. Then $zu^{-k} \in C_H(y) = 1$. Hence $z = u^k \in U$.

$\langle y^p \rangle V/V$ is a normal subgroup of G/V. Then it follows that $\langle y^p \rangle V \langle x \rangle$ is a subgroup of G. It is easily seen that $\langle y^p \rangle V \langle x \rangle = \langle y^p \rangle H$. $\langle y^p \rangle H$ satisfies the hypothesis of the theorem with y replaced by y^p. Therefore H is quasinormal in $\langle y^p \rangle H$. This implies that $K \not\subseteq \langle y^p \rangle H$. From Lemma 4.1, $\langle y^p \rangle H/V = \Omega_{r-2}(G/V)$. Thus $KV/V \cap \mho^{r-2}(G/V) \neq 1$. Lemma 4.1 also yields that $\mho^{r-2}(G/V) = \langle y^{p^{r-2}} \rangle V/V = \Omega_2(\langle y \rangle)V/V$ which has order p. Hence $\Omega_2(\langle y \rangle) \subseteq KV$.

This implies that K has an element of the form $y^{p^{r-2}} v$ where $v \in V$. Since $\mathrm{cl}(\Omega_2(\langle y \rangle)V) \leqq p - 1$, $\Omega_2(\langle y \rangle)V$ is a regular p-group in the sense of P. Hall [2]. Clearly the derived group of $\Omega_2(\langle y \rangle)V$ is contained in V. It now follows that $(y^{p^{r-2}} v)^p = y^{p^{r-1}}$. Thus we have shown that $\Omega_1(\langle y \rangle) \subseteq K$. Then $HVK = HU\Omega_1(\langle y \rangle)K = HK$. HVK is a subgroup of G because HV is quasinormal in G. Hence HK is a subgroup of G which contradicts $HK \neq KH$.

5. **Examples.** The method used to construct our examples is similar to that employed in [1] and, earlier, by Thompson in [4] and depends upon the following lemma.

5.1. LEMMA. *Assume p is a prime and $t = p + 2 + (-1)^p$.*

(a) *Let V be a vector space of finite dimension m over* GF(p) *with basis $v_1, \cdots, v_m$, let U be the subspace spanned by $v_2, \cdots, v_m$, and let Y be the linear transformation of V determined by $v_1Y = v_1$ and $v_kY = v_k + v_{k-1}$ for $2 \leqq k \leqq m$. Then there is a unique p-element X in* GL(V) *such that $X^{-1}YX = Y^t$, $v_1X = v_1$, and $UX = U$.*

(b) *If n is a positive integer, then it is possible in* (a) *to choose m such that the minimal polynomial of X is $(X - 1)^n$.*

PROOF. Set $V_0 = 0$ and for $1 \leqq k \leqq m$ let V_k be the subspace of V spanned by $v_1, \cdots, v_k$. The minimal polynomial of Y is $(Y - 1)^m$ and so Y is a p-element of $G = \mathrm{GL}(V)$. Then $\langle Y \rangle = \langle Y^t \rangle$. Since $|C_V(Y)| = p$, we must have $|C_V(Y^t)| = p$. Thus the Jordan normal form of Y^t has only one block. Hence Y and Y^t have the same Jordan normal form. Since GF(p) contains the eigenvalues of Y, Y and Y^t must be conjugate in G.

A straightforward calculation yields that the transformation T determined by $v_iT = \sum_{j=1}^{m} a_{ij}v_j$ commutes with Y if, and only if, $a_{ij} = 0$ for $1 \leqq i < j \leqq m$ and $a_{ij} = a_{i+1,\ j+1}$ for $1 \leqq j \leqq i \leqq m - 1$. This implies that only the identity of $C_G(Y)$ leaves U invariant. Thus (a) is proved if $Y = Y^t$.

Now assume $Y^t \neq Y$. If $p^e = t - 1$ and p^r is the order of Y, then $r > e$. If $X \in G$ and $X^{-1}YX = Y^t$, then $X \in N_G(\langle Y \rangle)$ and, from Lemma 2.5, $X^{p^{r-e}} \in C_G(Y)$. It follows from this that Y and Y^t are conjugate in some Sylow p-subgroup of $N_G(\langle Y \rangle)$.

Since $V_k/V_{k-1} = C_{V/V_{k-1}}(\langle Y \rangle)$ for $1 \leqq k \leqq m$, an induction argument yields that V_k for $1 \leqq k \leqq m$ is invariant under $N_G(\langle Y \rangle)$. Let H be the subgroup of G consisting of those linear transformations which leave V_k invariant for all k, $1 \leqq k \leqq m$. Clearly $N_G(\langle Y \rangle) \subseteq H$. H has a normal Sylow p-subgroup P which consists of those elements of H which induce the identity transformation on V_k/V_{k-1} for $1 \leqq k \leqq m$. Thus Y and Y^t must be conjugate in P.

Next let $Q = N_P(U)$ and $C = C_P(Y)$. From our earlier determination of $C_G(Y)$, we readily conclude that $C \cap Q = 1$ and $|C| = p^{m-1}$. But it is easily verified that $|P : Q| = p^{m-1}$. Thus Q is a complement of C in P. Therefore there is one and only one X in Q such that $X^{-1}YX = Y^t$. This proves (a).

If in (b), $n = 1$, then $m = 1$ is a suitable choice. Thus we will assume that $n > 1$. We first show that m can be chosen so that $(X - 1)^{n-1} \neq 0$. For this let $m \geqq p^{e+1}(n - 1)$. Then $(Y - 1)^{p^e} \neq 0$. Thus $Y^t \neq Y$. Using the same notation as in the proof of (a), we have that X must have order p^{r-e}. This follows from Lemma 2.5 and the fact that $C \cap Q = 1$. Thus $(X - 1)^{p^{r-e-1}} \neq 0$. Since $(Y - 1)^{p^r}$

$= 0$ and $(Y-1)^m$ is the minimal polynomial of Y, $p^{r-e-1} \geqq mp^{-e-1} \geqq n-1$. Therefore $(X-1)^{n-1} \neq 0$.

Now let m be the smallest integer such that $(X-1)^{n-1} \neq 0$. Since $(X-1)^{n-1} \neq 0$ implies that X is not the identity, we must have $m > 1$. Now V_{m-1} is invariant under both X and Y. Due to the minimality of m, $V_{m-1}(X-1)^{n-1} = 0$. But X induces the identity transformation on V/V_{m-1}. Thus $V(X-1) \subseteq V_{m-1}$. It now follows that $(X-1)^n$ is the minimal polynomial of X.

5.2. THEOREM. *Let p be a prime and n a positive integer. Then there is a finite p-group G such that G contains a core-free quasinormal subgroup of class n and exponent $< np^3$.*

PROOF. If $n = 1$, then the theorem follows from Lemma 4.1. Thus we assume $n > 1$. Let $t = p + 2 + (-1)^p$ and $p^e = t - 1$. By the previous lemma, there is a vector space W of dimension m over GF(p) with basis $v_1, \cdots, v_m$ such that GL(W) contains two p-elements X and Y which satisfy:

(i) $v_1 Y = v_1$ and $v_k Y = v_k + v_{k-1}$ for $2 \leqq k \leqq m$,

(ii) $v_1 X = v_1$ and $W_1 X = W_1$ where W_1 is the subspace spanned by $v_2, \cdots, v_m$,

(iii) $X^{-1} Y X = Y^t$, and

(iv) the minimal polynomial of X is $(X-1)^n$.

Let Y have order p^r. Since $X \neq 1$, $r > e$. Then, as is shown in the proof of Lemma 5.1, X has order p^{r-e}. Let A be the group generated by two elements a and b subject only to the relations $b^{p^{r+2}} = a^{p^{r+2-e}} = 1$ and $a^{-1}ba = b^t$. Then $a \rightarrow X$, $b \rightarrow Y$ determines a homomorphism of A into GL(W). Let B be the semidirect product AW relative to the above homomorphism.

Since $b^{p^{r+1}}$ and v_1 both belong to $Z(B)$, $\langle b^{p^{r+1}} v_1^{-1} \rangle$ is a normal subgroup of order p in B. $[b, a^{p^{r-e+1}}] = b^{s-1}$ where $s = t^{p^{r-e+1}}$. Lemma 2.4 now implies that $[b, a^{p^{r-e+1}}] = b^{p^{r+1}}$. If $N = \langle b^{p^{r+1}} v_1^{-1} \rangle$, then $[b, v_2^{-1}] = v_1 \equiv [b, a^{p^{r-e+1}}] \pmod N$. Thus, if $M = \langle a^{p^{r-e+1}} v_2 \rangle$, $[b, M] \equiv 1 \pmod N$. Since $X^{p^{r-e+1}} = 1$, it now follows that MN is a normal elementary abelian subgroup of order p^2 in B.

Finally let $G = B/MN$, $V = WMN/MN$, $U = W_1MN/MN$, $x = MNa$, $y = MNb$, and $H = U\langle x \rangle$. Since $Y^{p^r} = 1$, $[y^{p^r}, V] = 1$. Thus $[\Omega_2(\langle y \rangle), V] = 1$. Hence the hypothesis of Theorem 4.2 is satisfied. Therefore H is quasinormal in G. From the fact that the minimal polynomial of X is $(X-1)^n$, it follows that cl$(H) = n$. H/U is cyclic of order p^{r-e+1}, U is elementary abelian, and H contains $\langle x \rangle$ which is cyclic of order p^{r-e+2}. Thus H has exponent p^{r-e+2}. Since $(X-1)^{p^{r-e-1}} \neq 0 = (X-1)^n$, $p^{r-e+2} < np^3$. It only remains to show that $H_G = 1$.

If $H_G \neq 1$, then there is an element z of order p in $H \cap Z(G)$. Since $C_{W_1}(Y) = 1$, z cannot belong to U. Since H/U is cyclic, it follows that $\langle z \rangle U = \langle x^{p^{r-e}} \rangle U$. This implies that $[y, x^{p^{r-e}}] \in V$. But $[y, x^{p^{r-e}}] = y^{q-1}$ where $q - 1 = t^{p^{r-e}} - 1 \equiv p^r \pmod{p^{r+1}}$. Thus $y^{q-1} \notin \langle y^{p^{r+1}} \rangle = \langle y \rangle \cap V$. This contradiction shows that $H_G = 1$.

5.3. Corollary. *If p is a prime and n is an integer > 2, then there is a finite p-group G which contains a core-free quasinormal subgroup of class p^{n-2} and exponent p^n.*

Proof. The theorem with n replaced by p^{n-2} implies that there is a p-group G which contains a core-free quasinormal subgroup H of class p^{n-2} and exponent $< p^{n+1}$. Thus H has exponent $\leqq p^n$. If H has exponent $\leqq p^{n-1}$, then $\mathrm{cl}(H) \leqq p^{n-2} - 1$ by Theorem 3.4. Therefore the exponent of H is precisely p^n.

References

1. R. H. Bradway, F. Gross and W. R. Scott, *The nilpotence class of core-free quasinormal subgroups*, Rocky Mt. J. Math. **1** (1971), 375–382.

2. P. Hall, *A contribution to the theory of groups of prime-power order*, Proc. London Math. Soc. (2) **36** (1933), 29–95.

3. N. Itô and J. Szép, *Über die quasinormalteiler von endlichen gruppen*, Acta Sci. Math. (Szeged) **23** (1962), 168–170. MR **25** #2119.

4. J. Thompson, *An example of core-free quasinormal subgroups of p-groups*, Math. Z. **96** (1967), 226–227. MR **34** #7658.

University of Utah, Salt Lake City, Utah 84112