Rend. Sem. Mat. Univ. Padova 1xx (201x)

Rendiconti del Seminario Matematico della Università di Padova

Twisted Cyclic Groups

Neil Flowers – Thomas Wakefield*

Abstract – A finite group G is said to be *twisted cyclic* if there exist $\phi \in \mathrm{Aut}(G)$ and $x \in G$ such that $G = \{(x^i)\phi^j : i, j \in \mathbb{Z}\}$. In this note, we classify all groups satisfying this property and determine that, if a finite group G is twisted cyclic, then G is isomorphic to $\mathbb{Z}_{p^n}$, $\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$, Q_8, $\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^n}$ or direct products of these groups for some prime p and some $n \in \mathbb{Z}^+$.

Mathematics Subject Classification (2010). 20D45; 20E34

Keywords. cyclic groups, automorphisms, twisted cyclic.

1. Introduction

In this paper, all groups are finite. Exercise 6 in Chapter 10 of [1] asks the reader to consider a group G such that every element of G is of the form $(x^i)\alpha^j$ for suitable i, j, where α is a fixed-point-free automorphism of G and x is a fixed element of G. The exercise prompts the reader to prove that G is nilpotent, the Sylow subgroups of G are abelian, and thus allowing the reader to conclude that G is abelian. Motivated by this exercise, we remove the condition that the automorphism is fixed-point-free and propose the following definition.

Definition 1.1. A group G is **twisted cyclic** if there exist $\phi \in \mathrm{Aut}(G)$ and $x \in G$ such that $G = \{(x^i)\phi^j : i, j \in \mathbb{Z}\}$. In this case, we also say G is **twisted cyclic by** ϕ.

For example, the group $\mathbb{Z}_2 \times \mathbb{Z}_2$ is twisted cyclic by the automorphism $\phi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ defined by $(1)\phi = 1$, $(x)\phi = y$, $(y)\phi = xy$, and $(xy)\phi = x$. The quaternion group Q_8 is another example of a twisted cyclic group. In this case, the automorphism $\phi : Q_8 \to Q_8$ defined by $(i)\phi = j$, $(j)\phi = k$, $(k)\phi = i$, $(1)\phi = 1$, and $(-1)\phi = -1$ will establish the result. We aim to characterize all finite groups G satisfying this property. In particular, we prove Theorem 1.1.

Neil Flowers, Department of Mathematics and Statistics, Youngstown State University, One University Plaza, Youngstown, OH, United States

E-mail: nflowers@ysu.edu

Thomas Wakefield, Department of Mathematics and Statistics, Youngstown State University, One University Plaza, Youngstown, OH, United States

E-mail: tpwakefield@ysu.edu

THEOREM 1.1. *Let G be a twisted cyclic group. Then G is isomorphic to $\mathbb{Z}_{p^n}$, $\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$, Q_8, $\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^n}$ or direct products of these groups for some prime p and some $n \in \mathbb{Z}^+$.*

We begin by establishing several results concerning twisted cyclic groups.

2. Preliminary Results

In this section we establish some properties of twisted cyclic groups. Many will be used to establish Theorem 1.1. In Chapter 2, Theorem 1.1 of [1], we find the following result.

LEMMA 2.1. *Let G be a group, $\phi \in Aut(G)$ and $N \trianglelefteq G$ be ϕ-invariant and define $\phi \in Aut(G/N) = Aut(\overline{G})$ by $(\overline{g})\phi = \overline{(g)\phi}$ for all $\overline{g} \in \overline{G}$. Then $\phi \in Aut(\overline{G})$ and is called the automorphism induced by ϕ.*

Note that we denote ϕ and the automorphism induced by ϕ with the same symbol when context is clear and $\overline{G} = G/N$. We leave the proof of the next lemma as an exercise.

LEMMA 2.2. *Let G be a group and $\phi \in Aut(G)$. Then $C_G(\phi) = \{g \in G \mid (g)\phi = g\} \leq G$.*

PROPOSITION 2.1. *Let G be a cyclic group. Then G is twisted cyclic.*

PROOF. Since G is cyclic, there is $x \in G$ such that $G = \langle x \rangle$. Let $\phi : G \to G$ be defined by $(g)\phi = g$ for all $g \in G$. Then $G = \{x^i \ : \ i \in \mathbb{Z}\} = \{(x^i)\phi^j \ : \ i, j \in \mathbb{Z}\}$. Thus G is twisted cyclic by ϕ, the identity map. □

PROPOSITION 2.2. *Let G be a group, $\phi \in Aut(G)$ such that G is twisted cyclic by ϕ. If $N \trianglelefteq G$ is ϕ-invariant, then G/N is twisted cyclic by the induced map ϕ.*

PROOF. Since G is twisted cyclic by ϕ, there exists $x \in G$ such that $G = \{(x^i)\phi^j \ : \ i, j \in \mathbb{Z}\}$. Let $\overline{G} = G/N$. Consider the automorphism induced by ϕ given in Lemma 2.1. Let $\overline{g} \in \overline{G}$. Then $g \in G$ and so there exist $i, j \in \mathbb{Z}$ such that $g = (x^i)\phi^j$. Hence

$$\overline{g} = \overline{(x^i)\phi^j} = (\overline{x^i})\phi^j = (\overline{x}^i)\phi^j.$$

Thus $\overline{G} = \{(\overline{x}^i)\phi^j \ : \ i, j \in \mathbb{Z}\}$ and so $\overline{G}$ is twisted cyclic by the induced map ϕ. □

PROPOSITION 2.3. *Let G be a group, $\phi \in Aut(G)$ such that G is twisted cyclic by ϕ. If $H \leq G$ is ϕ-invariant, then H is twisted cyclic by ϕ^n for some $n \in \mathbb{Z}$.*

PROOF. Since G is twisted cyclic by ϕ, there exists $x \in G$ such that $G = \{(x^i)\phi^j \ : \ i, j \in \mathbb{Z}\}$. If $H = 1$, then H is cyclic and therefore H is twisted cyclic by Proposition 2.1. Assume $H \neq 1$. Let $(x^i)\phi^j \in H$ so that $i + j$ is minimal and i, j both nonnegative. We claim that $H = \{(x^{ik})\phi^{j\ell} \ : \ k, \ell \in \mathbb{Z}\}$. Since H is ϕ-invariant and $(x^i)\phi^j \in H$, we have $x^i = ((x^i)\phi^j)\phi^{-j} \in H$. Therefore $H \supseteq \{(x^{ik})\phi^{j\ell} \ : \ k, \ell \in \mathbb{Z}\}$. Now let $(x^r)\phi^s \in H$. Then there exist q_i, r_i such that $r = iq_1 + r_1$ and $s = jq_2 + r_2$, $0 \leq r_1 < i$ and $0 \leq r_2 < j$. Thus

$$\begin{aligned}(x^r)\phi^s &= (x^{iq_1 + r_1})\phi^{jq_2 + r_2} \\ &= (x^{iq_1}x^{r_1})\phi^{jq_2}\phi^{r_2} \\ &= ((x^{iq_1})\phi^{r_2}(x^{r_1})\phi^{r_2})\phi^{jq_2} \in H.\end{aligned}$$

Since H is ϕ-invariant, we get $(x^{iq_1})\phi^{r_2}(x^{r_1})\phi^{r_2} \in H$. As $(x^i)\phi^j \in H$ and H is ϕ-invariant, we conclude $(x^{iq_1})\phi^j = ((x^i)\phi^j)^{q_1} \in H$ and therefore $(x^{iq_1})\phi^{-q_2 j} \in H$. Thus $(x^{iq_1})\phi^{r_2}(x^{r_1})\phi^{r_2} \in H$ and $(x^{iq_1})\phi^{r_2} \in H$. Since $H \leq G$, we conclude $(x^{r_1})\phi^{r_2} \in H$. Now $0 \leq r_1 + r_2 < i + j$. Thus, by the minimality of $i + j$, $r_1 + r_2 = 0$ implying $r_1 = r_2 = 0$. Hence $(x^r)\phi^s = (x^{iq_1})\phi^{jq_2}$. Therefore $H = \{(x^{ik})\phi^{j\ell} \mid k, \ell \in \mathbb{Z}\}$ and so H is twisted cyclic by ϕ^j. □

PROPOSITION 2.4. *Let G be twisted cyclic by ϕ. Then $\langle\phi\rangle$ acts transitively on the cyclic subgroups of G of order n for all $n \in \mathbb{Z}^+$.*

PROOF. Let $y_1, y_2 \in G$ such that $|y_1| = |y_2| = n$. Since G is twisted cyclic by ϕ, there exists $x \in G$ such that $G = \{(x^i)\phi^j \ : \ i, j \in \mathbb{Z}\}$. Thus there exist $i, j, k, \ell \in \mathbb{Z}$ such that $y_1 = (x^i)\phi^j$ and $y_2 = (x^k)\phi^\ell$. Then $n = |y_1| = |(x^i)\phi^j| = |x^i|$ and $n = |y_2| = |(x^k)\phi^\ell| = |x^k|$. Hence $|x^k| = |x^i|$. Since $\langle x\rangle$ is cyclic, we get $\langle x^k\rangle = \langle x^i\rangle$. Now

$$\begin{aligned}
(\langle y_1\rangle)\phi^{\ell-j} &= (\langle(x^i)\phi^j\rangle)\phi^{\ell-j} \\
&= \langle(x^i)\phi^j\phi^{\ell-j}\rangle \\
&= \langle(x^i)\phi^\ell\rangle \\
&= (\langle x^i\rangle)\phi^\ell \\
&= (\langle x^k\rangle)\phi^\ell \\
&= \langle(x^k)\phi^\ell\rangle \\
&= \langle y_2\rangle.
\end{aligned}$$

Therefore $\langle\phi\rangle$ acts transitively on the cyclic subgroups of G of order n. □

PROPOSITION 2.5. *Let G be a group and $\phi \in Aut(G)$ such that G is twisted cyclic by ϕ and $H \leq G$ be ϕ-invariant. If $n \in \mathbb{Z}^+$ and $h \in H$ such that $|h| = n$, then H contains all the elements of order n in G.*

PROOF. Let $g \in G$ such that $|g| = n$. Then $|\langle h\rangle| = |\langle g\rangle| = n$. By Proposition 2.4, there exists $i \in \mathbb{Z}$ such that $\langle g\rangle = (\langle h\rangle)\phi^i \leq (H)\phi^i = H$ since H is ϕ-invariant. Thus $g \in H$. □

PROPOSITION 2.6. *Let G be a twisted cyclic group. Then G is nilpotent.*

PROOF. Let G be a counterexample such that $|G|$ is minimal. Since G is twisted cyclic, there exist $\phi \in \mathrm{Aut}(G)$ and $x \in G$ such that $G = \{(x^i)\phi^j \ : \ i, j \in \mathbb{Z}\}$. Suppose first that $C_G(\phi) = 1$. Let $p \in \pi(G)$. By Theorem 10.1.2 of [1], there exists a unique Sylow p-subgroup P of G such that P is ϕ-invariant. Let $Q \in \mathrm{Syl}_p(G)$ and $q \in Q$. Then q is a p-element and, as P is ϕ-invariant and is a p-group, by Proposition 2.5, we get $q \in P$. Hence $Q \leq P$ and therefore $P = Q$. Since G has only one Sylow p-subgroup, we get $P \trianglelefteq G$ and therefore G is nilpotent, a contradiction.

Suppose now $C_G(\phi) \neq 1$. Let $1 \neq z \in C_G(\phi)$ and $g \in G$. Then there exist $i, j, k, \ell \in \mathbb{Z}$ such that $z = (x^i)\phi^j$ and

$g = (x^k)\phi^\ell$. Now, since $z \in C_G(\phi)$,

$$\begin{aligned} zg = z(x^k)\phi^\ell &= (z)\phi^{\ell-j}(x^k)\phi^\ell \\ &= ((x^i)\phi^j)\phi^{\ell-j}(x^k)\phi^\ell \\ &= (x^i)\phi^\ell(x^k)\phi^\ell \\ &= (x^i x^k)\phi^\ell \\ &= (x^k x^i)\phi^\ell \\ &= (x^k)\phi^\ell(x^i)\phi^\ell \\ &= g(x^i)\phi^\ell \\ &= g(x^i)\phi^j\phi^{\ell-j} \\ &= g(z)\phi^{\ell-j} \\ &= gz. \end{aligned}$$

Hence $1 \neq z \in Z(G)$. Since $Z(G)$ char G, we have $Z(G) \trianglelefteq G$ and $Z(G)$ is ϕ-invariant. Let $\overline{G} = G/Z(G)$. By Proposition 2.2, $\overline{G}$ is twisted cyclic. Thus, by the minimality of $|G|$, $\overline{G} = G/Z(G)$ is nilpotent. Therefore G is nilpotent. □

As twisted cyclic groups are nilpotent, to know their structure, it is enough to know the structure of their Sylow subgroups. We are ready to prove Theorem 1.1.

3. Proof of Theorem 1.1

Before proceeding with the proof of Theorem 1.1, we state some useful lemmas. The first result can be found in Theorem 1.3 of Chapter 5 of [1] and Lemmas 3.2 and 3.3 appear as Results 5.2.13 and 5.3.2 in [2].

LEMMA 3.1. *Let P be a p-group. Then the factor group $P/\Phi(P)$ is elementary abelian. Furthermore, P is an elementary abelian p-group if and only if $\Phi(P) = 1$.*

LEMMA 3.2. *Let G be a group and $N \trianglelefteq G$ such that $N \leq \Phi(G)$. Then $\Phi(G/N) = \Phi(G)/N$.*

LEMMA 3.3. *Let P be a p-group. Then $\Phi(P) = \langle x^p, P' \mid x \in P \rangle$.*

We are now ready to establish Theorem 1.1.

THEOREM 1.1. *Let G be a twisted cyclic group. Then G is isomorphic to $\mathbb{Z}_{p^n}$, $\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$, Q_8, $\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^n}$ or direct products of these groups for some prime p and some $n \in \mathbb{Z}^+$.*

PROOF. To prove Theorem 1.1, we proceed by cases, again examining when $C_G(\phi) \neq 1$ and $C_G(\phi) = 1$ separately.

Case 1: First suppose $C_G(\phi) \neq 1$. Let p be a prime divisor of $|C_G(\phi)|$. By Cauchy's Theorem, there exists $1 \neq z \in C_G(\phi)$ such that $z^p = 1$. Let $P \in \mathrm{Syl}_p(G)$. Since G is nilpotent, $P \trianglelefteq G$ and, by Sylow's Theorem, $\langle z \rangle \leq P$. Since $P \in \mathrm{Syl}_p(G)$ and $P \trianglelefteq G$, we have that P char G. Thus P is ϕ-invariant and P is twisted cyclic by

ϕ^i for some $i \in \mathbb{Z}$ by Proposition 2.3. Since $z \in C_G(\phi)$, $\langle z \rangle$ is a ϕ-invariant cyclic subgroup of P of order p. By Proposition 2.4, $\langle \phi^i \rangle$ acts transitively on the cyclic subgroups of P of order p. Therefore, P has a unique cyclic subgroup of order p. Hence $P \cong \mathbb{Z}_{p^n}$ or $P \cong Q_{2^n} = \langle x, y \mid x^{2^{n-1}} = y^4 = 1, x^{2^{n-2}} = y^2, x^y = x^{-1} \rangle$ with $n \geq 3$ by Result 9.7.3 of [3]. If $P \cong Q_{2^n}$ and $n = 3$, we get $P \cong Q_8$. If $n > 3$, then P has a normal cyclic subgroup of order 4 and a non-normal cyclic subgroup of order 4, namely $\langle x^{2^{n-3}} \rangle$ and $\langle y \rangle$. This is a contradiction since $\phi^i \in \mathrm{Aut}(P)$ and $\langle \phi^i \rangle$ acts transitively on the cyclic subgroups of P of order 4.

Case 2: Now suppose $C_G(\phi) = 1$. Let $p \in \pi(G)$. Since G is nilpotent, there exists $P \in \mathrm{Syl}_p(G)$ such that P is ϕ-invariant. By Proposition 2.3, there exists $k \in \mathbb{Z}$ such that P is twisted cyclic by ϕ^k. Let $\exp(P) = p^e$ and $P_i = \Omega_i(P) = \langle x \in P \mid x^{p^i} = 1 \rangle$, for all $0 \leq i \leq e$. Then $P = P_e \trianglerighteq P_{e-1} \trianglerighteq \cdots \trianglerighteq P_1 \trianglerighteq P_0 = 1$. Let $\overline{P_i} = P_i/P_{i-1}$ for all $1 \leq i \leq e$.

Claim 1: $P_i \backslash P_{i-1} = \{g \in P \mid |g| = p^i\}$, ϕ acts irreducibly on $\overline{P_i} = P_i/P_{i-1}$ and $\overline{P_i}$ is an elementary abelian p-group for all $1 \leq i \leq e$.
Let $g \in P_i \backslash P_{i-1}$. Then $g^{p^i} = 1$. Suppose there exists $k \in \mathbb{Z}^+ \cup \{0\}$ such that $g^{p^k} = 1$ and $k < i$. Then $k \leq i-1$ and $g^{p^{i-1}} = 1$. Hence, we get $g \in P_{i-1}$, a contradiction. Therefore $|g| = p^i$ and so $P_i \backslash P_{i-1} \subseteq \{g \in P \mid |g| = p^i\}$. Now $P_i \backslash P_{i-1} \supseteq \{g \in P \mid |g| = p^i\}$ and we have $P_i \backslash P_{i-1} = \{g \in P \mid |g| = p^i\}$. Let $1 \neq \overline{A} = A/P_{i-1} \leq \overline{P_i}$ such that $\overline{A}$ is ϕ-invariant and $1 \neq \overline{a} \in \overline{A}$. Then $P_{i-1} \leq A \leq P_i$ and $a \in A \backslash P_{i-1}$. Thus $|a| = p^i$. Since $\overline{A}$ is ϕ-invariant, A is ϕ-invariant and therefore A is ϕ^i-invariant. By Proposition 2.5, A contains all the elements of P of order p^i. Thus $A \supseteq P_i \backslash P_{i-1}$ and so $A = P_i$. But then $\overline{A} = \overline{P_i}$. Now $\Phi(\overline{P_i})$ char $\overline{P_i}$ and so $\Phi(\overline{P_i})$ is ϕ-invariant. Since ϕ acts irreducibly on $\overline{P_i}$, $\Phi(\overline{P_i}) = 1$. Hence, by Lemma 3.1, $\overline{P_i}$ is an elementary abelian p-group.

Claim 2: If $|\overline{P_i}| = p$, then P_i is cyclic for all $1 \leq i \leq e$.
To establish this result, we proceed by induction on i. Suppose $|\overline{P_1}| = p$. Then $P_1 \cong P_1/\langle 1 \rangle = P_1/P_0 = \overline{P_1} \cong \mathbb{Z}_p$, and so P_1 is cyclic.

Let $i \geq 2$ and suppose $|\overline{P_i}| = p$. Let $\widetilde{P} = P/P_{i-2}$, $a \in P_i \backslash P_{i-1}$ and $1 \neq \widetilde{b} \in \Omega_1(Z(\widetilde{P_i}))$. Then $1 = \widetilde{b}^p = \widetilde{b^p}$ and so $b^p \in P_{i-2}$. Hence $1 = (b^p)^{p^{i-2}} = b^{p^{i-1}}$ and so $b \in P_{i-1}$. But then $\widetilde{b} \in \widetilde{P_{i-1}}$ and so $\Omega_1(Z(\widetilde{P_i})) \leq \widetilde{P_{i-1}}$. But $\Omega_1(Z(\widetilde{P_i}))$ char $\widetilde{P_i}$ and so $\Omega_1(Z(\widetilde{P_i}))$ is ϕ-invariant. Since ϕ acts irreducibly on $\widetilde{P_{i-1}} = \overline{P_{i-1}}$, we obtain $\widetilde{P_{i-1}} = \Omega_1(Z(\widetilde{P_i}))$. As $|\overline{P_i}| = p$ and $\overline{a} \neq 1$, we get $\overline{P_i} = \langle \overline{a} \rangle$. But then $P_i = \langle a, P_{i-1} \rangle = \langle a \rangle P_{i-1}$ and therefore $\widetilde{P_i} = \langle \widetilde{a} \rangle \widetilde{P_{i-1}}$.

We next show $\Phi(\widetilde{P_i}) = \langle \widetilde{a}^p \rangle$. Since $\langle \widetilde{a} \rangle$ is abelian, we know $\langle \widetilde{a}^p \rangle \trianglelefteq \langle \widetilde{a} \rangle$. Also, $\widetilde{P_{i-1}} = \Omega_1(Z(\widetilde{P_i})) \leq Z(\widetilde{P_i}) \leq N_{\widetilde{P_i}}(\langle \widetilde{a}^p \rangle)$. Thus $\langle \widetilde{a}^p \rangle \trianglelefteq \langle \widetilde{a} \rangle \widetilde{P_{i-1}} = \widetilde{P_i}$. Since $\widetilde{P_i}$ is a p-group and $\langle \widetilde{a}^p \rangle \neq 1$, we get $1 \neq \langle \widetilde{a}^p \rangle \cap Z(\widetilde{P_i}) \leq \langle \widetilde{a}^p \rangle$. But $|\langle \widetilde{a}^p \rangle| = p$ and therefore $\langle \widetilde{a}^p \rangle = \langle \widetilde{a}^p \rangle \cap Z(\widetilde{P_i})$. Hence $\langle \widetilde{a}^p \rangle \leq Z(\widetilde{P_i})$ but then $\langle \widetilde{a}^p \rangle \widetilde{P_{i-1}} \leq Z(\widetilde{P_i})$. Now

$$\frac{\widetilde{P_i}}{\langle \widetilde{a}^p \rangle \widetilde{P_{i-1}}} = \frac{\langle \widetilde{a} \rangle \widetilde{P_{i-1}}}{\langle \widetilde{a}^p \rangle \widetilde{P_{i-1}}} \cong \frac{\frac{\langle \widetilde{a} \rangle \widetilde{P_{i-1}}}{\widetilde{P_{i-1}}}}{\frac{\langle \widetilde{a}^p \rangle \widetilde{P_{i-1}}}{\widetilde{P_{i-1}}}}$$

is a quotient of $\frac{\langle \widetilde{a} \rangle \widetilde{P_{i-1}}}{\widetilde{P_{i-1}}}$. But $\frac{\langle \widetilde{a} \rangle \widetilde{P_{i-1}}}{\widetilde{P_{i-1}}} \cong \frac{\langle \widetilde{a} \rangle}{\langle \widetilde{a} \rangle \cap \widetilde{P_{i-1}}}$ is cyclic. Hence $\frac{\widetilde{P_i}}{\langle \widetilde{a}^p \rangle \widetilde{P_{i-1}}}$ is cyclic. Since $\langle \widetilde{a}^p \rangle \widetilde{P_{i-1}} \leq Z(\widetilde{P_i})$, we get $\widetilde{P_i}$ is abelian and so $\widetilde{P_i}' = 1$. Since $\widetilde{P_i}$ is a p-group, $\widetilde{P_i} = \langle \widetilde{a} \rangle \widetilde{P_{i-1}}$, $\widetilde{P_{i-1}} \leq Z(\widetilde{P_i})$, and $\widetilde{P_{i-1}}$ is an elementary abelian p-group, we obtain $\Phi(\widetilde{P_i}) = \langle \widetilde{a}^p \rangle$ from Lemma 3.3.

Since $a \in P_i$, we get $a^p \in P_{i-1}$ and therefore $\widetilde{a}^p \in \widetilde{P_{i-1}}$. Hence $\Phi(\widetilde{P}_i) = \langle \widetilde{a}^p \rangle \leq \widetilde{P_{i-1}} = \overline{P_{i-1}}$. But $\Phi(\widetilde{P}_i)$ char $\widetilde{P}_i$ and $\widetilde{P}_i$ is ϕ-invariant implies $\Phi(\widetilde{P}_i)$ is ϕ-invariant. Since ϕ acts irreducibly on $\widetilde{P_{i-1}}$, $\Phi(\widetilde{P}_i) = \widetilde{P_{i-1}}$. Hence $\widetilde{P_{i-1}} = \Omega_1(Z(\widetilde{P}_i)) = \Phi(\widetilde{P}_i) = \langle \widetilde{a}^p \rangle$. We have $(a^p)^p = a^{p^2} \in P_{i-2}$. Hence $\widetilde{a}^{p^2} = 1$, and so $|\widetilde{P_{i-1}}| = p$. Therefore by induction, P_{i-1} is cyclic. Let $g \in P_{i-1}$. Then $g^{p^{i-1}} = 1$ and so $|g| \leq p^{i-1}$. Since $a \in P_i \backslash P_{i-1}$, we have $|a| = p^i$ and therefore $|a^p| = p^{i-1}$. Thus $|a^p| \geq |g|$, $a^p \in P_{i-1}$ and P_{i-1} is cyclic. Hence $P_{i-1} = \langle a^p \rangle$ and $P_i = \langle a, P_{i-1} \rangle = \langle a \rangle P_{i-1} = \langle a \rangle \langle a^p \rangle = \langle a \rangle$ is cyclic.

Claim 3: If there exists $1 \leq i \leq e$ such that $|\overline{P_i}| = p$, then P is cyclic.
Let i be maximal such that $|\overline{P_i}| = p$. If $i = e$, then $|\overline{P_e}| = p$ and so by Claim 2, P_e is cyclic. But then $P = P_e$ is cyclic. Therefore, we may assume $i \neq e$. Let $\widetilde{P} = P/P_{i-1}$ and $a \in P_{i+1} \backslash P_i$. If $\widetilde{a}^p = 1$, then $a^p \in P_{i-1}$. Hence $1 = (a^p)^{p^{i-1}} = a^{p^i}$ and so we get $a \in P_i$, a contradiction. Thus $\widetilde{a}^p \neq 1$ and so $\Phi(\widetilde{P_{i+1}}) \neq 1$ by Lemma 3.3. If $\widetilde{P_{i+1}}$ is abelian, let $\widetilde{x} \in \widetilde{P_{i+1}}$. Then $x^p \in P_i$ and so $x^{p^2} \in P_{i-1}$. Thus $\widetilde{x}^{p^2} = 1$ and so $\exp(\widetilde{P_{i+1}}) \leq p^2$. If $\exp(\widetilde{P_{i+1}}) = p$, then $\widetilde{x}^p = 1$ and therefore $x^p \in P_{i-1}$ for every $x \in P_{i+1}$. Hence $1 = (x^p)^{p^{i-1}} = x^{p^i}$ and so $x \in P_i$ for all $x \in P_{i+1}$. Thus $P_{i+1} \leq P_i$ and therefore $P_{i+1} = P_i$. But then we get $i = e$, which is a contradiction. Thus $\exp(\widetilde{P_{i+1}}) \neq p$ forcing $\exp(\widetilde{P_{i+1}}) = p^2$.

As shown in Claim 2, $1 \neq \Phi(\widetilde{P_{i+1}}) \leq \widetilde{P}_i$ and $\Phi(\widetilde{P_{i+1}})$ is ϕ-invariant. Since ϕ acts irreducibly on $\widetilde{P}_i = \overline{P_i}$, we get $\Phi(\widetilde{P_{i+1}}) = \widetilde{P}_i \cong \mathbb{Z}_p$. As $\widetilde{P_{i+1}}$ is twisted cyclic and $\Phi(\widetilde{P_{i+1}})$ is ϕ-invariant, $\widetilde{P_{i+1}}$ has a unique subgroup of order p. Hence $\widetilde{P_{i+1}} \cong \mathbb{Z}_{p^n}$ or $\widetilde{P_{i+1}} \cong Q_{2^n}$. Since $\widetilde{P_{i+1}}$ is abelian, we get $\widetilde{P_{i+1}} \cong \mathbb{Z}_{p^n}$ is cyclic and has exponent p^2. Therefore, since $\exp(\widetilde{P_{i+1}}) = p^2$, we have $\widetilde{P_{i+1}} \cong \mathbb{Z}_{p^2}$. Then

$$p^2 = \frac{|P_{i+1}|}{|P_{i-1}|} = \frac{|P_{i+1}|}{|P_i|} \frac{|P_i|}{|P_{i-1}|} = \frac{|P_{i+1}|}{|P_i|} \cdot p.$$

Hence $\frac{|P_{i+1}|}{|P_i|} = p$ and so $|\overline{P_{i+1}}| = p$. This contradicts the maximality of i.

Thus $\widetilde{P_{i+1}}$ is not abelian. Repeating the argument from above, we conclude $\widetilde{P_{i+1}} \cong Q_{2^n}$. Since $\widetilde{P_{i+1}}$ is twisted cyclic, we get $\widetilde{P_{i+1}} \cong Q_8$. Now $C_P(\phi) \leq C_G(\phi) = 1$ and so $C_P(\phi) = 1$. Thus $C_{\widetilde{P}}(\phi) = 1$. Now $|\Omega_1(\widetilde{P_{i+1}})| = |\Omega_1(Q_8)| = 2$ and $\Omega_1(\widetilde{P_{i+1}})$ is ϕ-invariant. Hence, we get $\Omega_1(\widetilde{P_{i+1}}) \leq C_{\widetilde{P}}(\phi) = 1$, a contradiction as $|\Omega_1(\widetilde{P_{i+1}})| = 2$.

If $e = 1$, then $P \cong P/1 = P_e/P_0 = P_e/P_{e-1} = \overline{P_e}$ is an elementary abelian p-group. Also, if $|\overline{P_i}| = 1$, then $\overline{P_i}$ is cyclic and so P is cyclic. So, without loss of generality, $e \geq 2$ and $|\overline{P_i}| \geq 2$ for all $1 \leq i \leq e$. If there exists $1 \leq i \leq e$ such that $|\overline{P_i}| = p$, then P is cyclic.

Claim 4: Let $\langle \alpha \rangle \in \mathrm{Syl}_p(\langle \phi \rangle)$. We assert that $[P_i, \alpha^p] \leq P_{i-2}$ for $2 \leq i \leq e$.
Let $2 \leq i \leq e$ and $\widetilde{P} = P/P_{i-2}$. Then the p-group $\langle \alpha \rangle$ acts on the p-group $\overline{P_i}$. Hence $1 \neq C_{\overline{P_i}}(\langle \alpha \rangle) \leq \overline{P_i}$ and $C_{\overline{P_i}}(\langle \alpha \rangle)$ is ϕ-invariant. Since ϕ acts irreducibly on $\overline{P_i}$, we get $\overline{P_i} = C_{\overline{P_i}}(\langle \alpha \rangle)$. Hence, $[\overline{P_i}, \alpha] = 1$ and therefore $[P_i, \alpha] \leq P_{i-1}$. Let $x \in P_i$. Then $\widetilde{[x, \alpha]} \in \widetilde{P_{i-1}} = \Omega_1(Z(\widetilde{P}_i))$. Thus $\widetilde{[x, \alpha]} = [\widetilde{x}, \alpha]$ commutes with $\widetilde{x}$. Now $[x, \alpha, \alpha] \in [P_{i-1}, \alpha] \leq P_{i-2}$. Hence $\widetilde{[x, \alpha, \alpha]} = [\widetilde{x}, \alpha, \alpha] \in \widetilde{P_{i-2}} = 1$. Therefore $[\widetilde{x}, \alpha]$ commutes with α in the group $\widetilde{P}_i \ltimes \langle \alpha \rangle$. Since $[x, \alpha] \in P_{i-1}$, we get $\widetilde{[x, \alpha]}^p \in P_{i-2}$. This implies $\widetilde{[x, \alpha]}^p \in \widetilde{P_{i-2}} = 1$. But since $[\widetilde{x}, \alpha]$ commutes with $\widetilde{x}$ and α, we have $\widetilde{[x, \alpha]}^p = \widetilde{[x, \alpha]^p} = [\widetilde{x}, \alpha^p]$. Thus $[\widetilde{x}, \alpha^p] = 1$ and therefore $[\widetilde{P}_i, \alpha^p] = 1$. Hence $[P_i, \alpha^p] \leq P_{i-2}$.

Claim 5: $|\overline{P_i}| = p^2$ for all $1 \leq i \leq e$.
Let $i \geq 2$ and $\widetilde{P} = P/P_{i-2}$. By Proposition 2.2, since P is twisted cyclic, we have $\widetilde{P}$ is twisted cyclic. By

Proposition 2.3, $\widetilde{P}_i$ is twisted cyclic by ϕ^k for some $k \in \mathbb{Z}$. By Proposition 2.4, $\langle \phi^k \rangle$ acts transitively on the cyclic subgroups of $\widetilde{P}_i$ of order p^2. Thus so does $\langle \phi \rangle$. Now the number of cyclic subgroups of $\widetilde{P}_i$ of order p^2 is

$$\begin{aligned}\frac{|\widetilde{P}_i| - |\widetilde{P_{i-1}}|}{p^2 - p} &= \frac{|P_i|/|P_{i-2}| - |P_{i-1}|/|P_{i-2}|}{p(p-1)} \\ &= \frac{(|P_i|/|P_{i-1}|)(|P_{i-1}|/|P_{i-2}|) - |P_{i-1}|/|P_{i-2}|}{p(p-1)} \\ &= \frac{|\overline{P_{i-1}}|(|\overline{P_i}| - 1)}{p(p-1)}.\end{aligned}$$

On the other hand, the number of cyclic subgroups of $\widetilde{P}_i$ of order p^2 can be found by exploiting the transitivity of the action of $\langle \phi \rangle$ on $\widetilde{P}_i$ to be

$$\frac{|\langle \phi \rangle|}{|N_{\langle \phi \rangle}(\widetilde{H})|}$$

where $\widetilde{H} \leq \widetilde{P}_i$ such that $\widetilde{H} \cong \mathbb{Z}_{p^2}$. Therefore

$$\frac{|\langle \phi \rangle|}{|N_{\langle \phi \rangle}(\widetilde{H})|} = \frac{|\overline{P_{i-1}}|(|\overline{P_i}| - 1)}{p(p-1)}.$$

Since $[P_i, \alpha^p] \leq P_{i-2}$, we get $[\widetilde{P}_i, \alpha^p] = 1$. But then $[\widetilde{P}_i, \langle \alpha^p \rangle] = 1$. Hence $\langle \alpha^p \rangle \leq C_{\langle \phi \rangle}(\widetilde{P}_i) \leq N_{\langle \phi \rangle}(\widetilde{H})$ and so

$$\begin{aligned}\left| \frac{\langle \phi \rangle}{N_{\langle \phi \rangle}(\widetilde{H})} \right|_p &= \frac{|\langle \phi \rangle|_p}{|N_{\langle \phi \rangle}(\widetilde{H})|_p} \\ &= \frac{|\langle \alpha \rangle|_p}{|N_{\langle \phi \rangle}(\widetilde{H})|_p} \\ &\leq \frac{|\langle \alpha \rangle|}{|\langle \alpha^p \rangle|} \\ &= \frac{|\alpha|}{\left(\dfrac{|\alpha|}{\gcd(|\alpha|, p)} \right)} \\ &= \gcd(|\alpha|, p),\end{aligned}$$

which is equal to 1 or p. Thus

$$\left| \frac{|\overline{P_{i-1}}|(|\overline{P_i}| - 1)}{p(p-1)} \right|_p = 1 \text{ or } p.$$

If

$$\left| \frac{|\overline{P_{i-1}}|(|\overline{P_i}| - 1)}{p(p-1)} \right|_p = 1,$$

then, since p does not divide $(|\overline{P_i}| - 1)/(p-1)$, we get $||\overline{P_{i-1}}|/p|_p = 1$. But then $|\overline{P_{i-1}}| = p$ and so $P \cong \mathbb{Z}_{p^n}$ is cyclic. Hence, without loss of generality, we may assume that

$$\left| \frac{|\overline{P_{i-1}}|(|\overline{P_i}| - 1)}{p(p-1)} \right|_p = p.$$

Then we get $||\overline{P_{i-1}}|/p|_p = p$ and so $|\overline{P_{i-1}}| = p^2$. But then $\langle \alpha \rangle \nleq N_{\langle \phi \rangle}(\widetilde{H})$. Now $C_{\langle \phi \rangle}(\widetilde{P}_i) \leq N_{\langle \phi \rangle}(\widetilde{H})$ implies $\langle \alpha \rangle \nleq C_{\langle \phi \rangle}(\widetilde{P}_i)$. Thus $[\widetilde{P}_i, \langle \alpha \rangle] \neq 1$ and therefore $[\widetilde{P}_i, \alpha] \neq 1$. Now we have $1 \neq [\widetilde{P}_i, \alpha] \leq \widetilde{P_{i-1}}$ and $[\widetilde{P}_i, \alpha]$ is ϕ-invariant. Since ϕ acts irreducibly on the normal series $P = P_e \trianglerighteq P_{e-1} \trianglerighteq P_{e-2} \trianglerighteq \cdots \trianglerighteq P_1 \trianglerighteq P_0 = 1$, we know that ϕ acts irreducibly on the normal series $\widetilde{P} = \widetilde{P_e} \trianglerighteq \widetilde{P_{e-1}} \trianglerighteq \widetilde{P_{e-2}} \trianglerighteq \cdots \trianglerighteq \widetilde{P_1} \trianglerighteq \widetilde{P_0} = 1$. Hence $\widetilde{P_{i-1}} = [\widetilde{P}_i, \alpha]$.

Since $[\widetilde{P}_i, \alpha] \neq 1$, we get $\widetilde{P}_i > C_{\widetilde{P}_i}(\alpha) = \widetilde{P_{i-1}}$. Note that $1 \neq [\widetilde{P}_i, \alpha]$ implies that $1 \neq [P_i, \alpha] \leq P_{i-1}$. Thus $\widetilde{P_{i-1}} = C_{\widetilde{P_{i-1}}}(\alpha) = C_{\widetilde{P}_i}(\alpha)$. Define $\theta : \widetilde{P}_i \to \widetilde{P_{i-1}} = \overline{P_{i-1}}$ by $(\widetilde{x})\theta = [\widetilde{x}, \alpha]$ for all $\widetilde{x} \in \widetilde{P}_i$. Since $\widetilde{P_{i-1}} \leq Z(\widetilde{P}_i)$, the mapping θ is a homomorphism. Also $\widetilde{P_{i-1}} = [\widetilde{P}_i, \alpha]$ implies θ is onto. Moreover, $\ker\theta = C_{\widetilde{P}_i}(\alpha)$. Hence, by the First and Second Isomorphism Theorems,

$$\widetilde{P_{i-1}} = \frac{P_{i-1}}{P_{i-2}} \cong \frac{\widetilde{P}_i}{C_{\widetilde{P}_i}(\alpha)} = \frac{\widetilde{P}_i}{\widetilde{P_{i-1}}} \cong \frac{P_i}{P_{i-1}} = \overline{P_i}.$$

Thus $|\overline{P_i}| = |\widetilde{P_{i-1}}| = |\overline{P_{i-1}}| = p^2$.

Claim 6: P is abelian.

Suppose P is not abelian. Then there exists $1 \leq i \leq e$ such that i is minimal with respect to the property of P_i being not abelian. Now P_i/P_{i-1} is abelian and so $P_i' \leq P_{i-1}$. Now $P_{i-2} \leq P_i'P_{i-2} \leq P_{i-1}$ and $P_i'P_{i-2}$ is ϕ-invariant. Since ϕ acts irreducibly on P_{i-1}/P_{i-2}, we get $P_{i-2} = P_i'P_{i-2}$ or $P_{i-1} = P_i'P_{i-2}$. Thus $P_i' \leq P_{i-2}$ or $P_{i-1}/P_{i-2} = (P_i'P_{i-2})/P_{i-2}$. Since P_i is not abelian and $P_0 = 1$, there exists $1 \leq j \leq i-1$ such that $\overline{P_j} = P_j/P_{j-1} = [\overline{P_i}, \overline{P_i}] = \overline{P_i}'$. Since $\overline{P_i}$ is nilpotent, we get $j < i$. Let $1 \leq k \leq e$ be minimal such that $[\overline{P_i}, \overline{P_k}] = \overline{P_j}$. Since $\overline{P_j}$ is nilpotent, we have $j < k \leq i$. Now $[\overline{P_i}, \overline{P_{k-1}}] < [\overline{P_i}, \overline{P_k}] = \overline{P_j}$ by the minimality of k. But $[\overline{P_i}, \overline{P_{k-1}}]$ is ϕ-invariant, and so $[\overline{P_i}, \overline{P_{k-1}}] = 1$ since ϕ acts irreducibly on $\overline{P_j}$. If $k < i$, then $k \leq i-1$ and so $P_k \leq P_{i-1}$. But P_{i-1} is abelian by the minimality of i. Thus $[P_{i-1}, P_k] = 1$ and so $[\overline{P_{i-1}}, \overline{P_k}] = 1$. If $k = i$, then $[\overline{P_i}, \overline{P_{i-1}}] < [\overline{P_i}, \overline{P_k}] = \overline{P_j}$ and $[\overline{P_i}, \overline{P_{i-1}}]$ is ϕ-invariant. Therefore, since ϕ acts irreducibly on $\overline{P_j}$, we have $[\overline{P_i}, \overline{P_{i-1}}] = 1$.

Since $P_i/P_{i-1} \cong \mathbb{Z}_p \times \mathbb{Z}_p$, there exist $x, y \in P_i$ such that $x^p, y^p \in P_{i-1}$ and $P_i = \langle x, y\rangle P_{i-1}$. Let $q = p^{i-k}$. Then $x^q = x^{p^{i-k}} \in P_k$ and $y^q \in P_k$. Also $(x^q)^p = (x^{p^{i-k}})^p = x^{p^{i-k+1}} \in P_{k-1}$ and $(y^q)^p \in P_{k-1}$. Since $P_k/P_{k-1} \cong \mathbb{Z}_p \times \mathbb{Z}_p$, we get $P_k = \langle x^q, y^q\rangle P_{k-1}$. Since $j < k$, $j \leq k-1$. Thus $P_j \leq P_{k-1}$ and so $\overline{P_i}' = \overline{P_j} \leq \overline{P_{k-1}}$. Thus $\overline{P_i}/\overline{P_{k-1}}$ is abelian. Hence there exists $\overline{z} \in \overline{P_{k-1}}$ such that $(\overline{xy})^q\overline{z} = \overline{x}^q\overline{y}^q$. Now

$$\begin{aligned}[\overline{xy}, \overline{x}^q\overline{y}^q] &= [\overline{xy}, (\overline{xy})^q\overline{z}] \\ &= [\overline{xy}, \overline{z}][\overline{xy}, (\overline{xy})^q]^{\overline{z}} \\ &= [\overline{xy}, \overline{z}].\end{aligned}$$

But $[\overline{xy}, \overline{z}] \in [\overline{P_i}, \overline{P_{k-1}}] = 1$ and so $[\overline{xy}, \overline{x}^q\overline{y}^q] = 1$. On the other hand,

$$[\overline{xy}, \overline{x}^q\overline{y}^q] = [\overline{xy}, \overline{y}^q][\overline{xy}, \overline{x}^q]^{\overline{y}^q} = [\overline{x}, \overline{y}^q]^{\overline{y}}[\overline{y}, \overline{x}^q]^{\overline{y}^q}.$$

Now $[\overline{y}, \overline{x}^q]^{\overline{y}^q} \in [\overline{P_i}, \overline{P_i}] = \overline{P_i}' = \overline{P_j} \leq \overline{P_{i-1}}$ since $j \leq i-1$. Also, since $\overline{y}^q \in \overline{P_k}$ and $[\overline{P_{i-1}}, \overline{P_k}] = 1$, we get

$$[\overline{xy}, \overline{x}^q\overline{y}^q] = [\overline{x}, \overline{y}^q]^{\overline{y}}[\overline{y}, \overline{x}^q]^{\overline{y}^q} = [\overline{x}^{\overline{y}}, \overline{y}^q][\overline{y}, \overline{x}^q].$$

But since $j \leq i-1 < i$, $P_j \leq P_{i-1} \leq P_i$ and $\overline{P_i}' = \overline{P_j}$, the quotient $\overline{P_i}/\overline{P_{i-1}}$ is abelian. Therefore there exists $\overline{z_1} \in \overline{P_{i-1}}$ such that $\overline{x}^{\overline{y}} = \overline{z}_1\overline{x}$. Thus, since $[\overline{P_{i-1}}, \overline{P_k}] = 1$, we get

$$[\overline{xy}, \overline{x}^q\overline{y}^q] = [\overline{z}_1\overline{x}, \overline{y}^q][\overline{y}, \overline{x}^q] = [\overline{x}, \overline{y}^q][\overline{y}, \overline{x}^q].$$

Thus $[\overline{x}, \overline{y}^q][\overline{y}, \overline{x}^q] = 1$ or $[\overline{x}, \overline{y}^q] = [\overline{y}, \overline{x}^q]^{-1}$. Now

$$\overline{P_j} = [\overline{P_i}, \overline{P_k}] = [\langle\overline{x}, \overline{y}\rangle, \langle\overline{x}^q, \overline{y}^q\rangle] = \langle[\overline{x}, \overline{y}^q], [\overline{y}, \overline{x}^q]\rangle = \langle[\overline{x}, \overline{y}^q]\rangle$$

is cyclic. Hence we get P is cyclic, which is a contradiction. Therefore P is abelian.

But then if P is non-cyclic, non-elementary, and is not isomorphic to Q_8, since $P_i/P_{i-1} \cong \mathbb{Z}_p \times \mathbb{Z}_p$ for all $0 \leq i \leq e$, we get $P \cong \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^n}$ for some $n \in \mathbb{Z}^+$. Thus, since G is nilpotent, we get G is isomorphic to $\mathbb{Z}_{p^n}$, $\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$, Q_8, $\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^n}$ or direct products of these groups for some prime p and some $n \in \mathbb{Z}^+$.

□

Acknowledgements: The authors thank the referee for helpful suggestions that greatly improved the manuscript.

References

[1] D. Gorenstein, "Finite Groups," Harper & Row, New York, 1968.

[2] D.J.S. Robinson, "A Course in the Theory of Groups," Springer-Verlag, New York, 1996.

[3] W.R. Scott, "Group Theory," Prentice Hall, Englewood Cliffs, 1964.

Received 3 January 2018; revised 30 January 2018