DATA ANALYTICS AND APPLIED MATHEMATICS
E-ISSN: 2773-4854
VOLUME 5, ISSUE 1, 2024, 29 – 35
DOI: https://doi.org/10.15282/daam.v5i1.10970

RESEARCH ARTICLE

Finite cyclic *q*-group's automorphisms with q^r -generator

Fatin Hanani Hasan[1,2], Mohd Sham Mohamad[2,*], Yuhani Yusof[2], Nor Amirah Mohd Busul Aklan[3] , Siti Hasanah Jusoo[2] and Ekkasit Sangwisut[4]

[1]Tunku Abdul Rahman University of Management and Technology, Pahang Branch, Bandar Indera Mahkota, 25200 Kuantan, Pahang, Malaysia
[2]Centre for Mathematical Sciences, Universiti Malaysia Pahang Al-Sultan Abdullah, Lebuh Persiaran Tun Khalil Yaakob, 26300 Kuantan, Pahang, Malaysia
[3]Department of Computational and Theoretical Sciences, Kulliyah of Science, International Islamic University Malaysia, 25200 Kuantan, Pahang, Malaysia
[4]Department of Mathematics and Statistics, Faculty of Science and Digital Innovation, Thaksin University, Phattalung 93110, Thailand

ABSTRACT - The finite cyclic *q*-group, where *q* being odd prime, requires generators to validate the formation of automorphisms. A summary of cyclic groups, automorphisms, and characteristics is provided as a foundation for this research. By evaluating the automorphisms, the generators for the q^r -power cyclic group in their specific sequence have been uncovered and presented as the key finding.

ARTICLE HISTORY
Received : 15th Dec 2023
Revised : 25th Feb 2024
Accepted : 18th Mac 2024
Published : 31st Mac 2024

KEYWORDS
Cyclic group
Automorphism group
Generator
Compatible action
Number theory

1. INTRODUCTION

Understanding the generators is a prerequisite for producing automorphisms for finite cyclic q-groups. These are the nonabelian tensor product actions. These complex internal mechanisms for finite cyclic groups are easier to comprehend by looking at the generators of these automorphism groups.

Brown and Loday were pioneer researchers who propagated the theory of the group's nonabelian tensor product [1]. Then, Brown et. al released a list of unanswered concerns related to the nonabelian tensor square as well as the nonabelian tensor product, allowing colleague academics to evaluate and assess the group's theoretical properties [2]. An outstanding issue concerning the nonabelian tensor product of cyclic groups catalyzed this study.

In group theory, a group is considered cyclic if it is made up entirely of a single element, $g \in G$, namely the "group generator". As a result, the mapping $\rho : g \to g^x$ produces automorphism of the group G, where x is an integer and $\gcd(x, q^r) = 1$.

According to [3], the cyclic group's automorphisms shall be alternatively shown as $\mathrm{Aut}(G) \cong C_{q-1} \times C_{q^{r-1}} \cong C_{(q-1)q^{r-1}}$, where q is an odd prime and $r \in \mathbb{N}$ [3]. Additionally, a discovery has been made: the direct product of two finite cyclic groups is isomorphic to the automorphisms with q-power order. This suggests that finding the group generator is a prerequisite for figuring out the automorphisms' order of the q-group.

Clark has divided generators into four distinct categories: 2, 4, q^r, or $2q^r$ where q represents an odd prime and $r \in \mathbb{N}$ [4]. Broche et al. categorized finite cyclic groups of two generators by prime-power order. They created a procedure to generate every finite nonabelian cyclic group of 2-generators of prime power to confirm if such two groups are isomorphic [5].

Miech and Song grouped the odd cyclic q-groups for finite 2-generators. Nevertheless, they excluded the group theory approach when categorizing it into several groups depending on specifications [6,7]. Mohamad found the generators for automorphisms of order 2-power order [8]. As for the q-power order, Mohamad identified the automorphisms' generator with the order q^{r-1}, where q represents an odd prime and $r \in \mathbb{N}$. Subsequently, Shahoodh expanded on the generator's output for the q-power order that Mohamad had initially discovered [9].

A fourth-degree equation in complex homogeneous coordinates is known as the Klein Quartic, which Lachaud formulated as an algebraic curve and a cyclic group generator [10]. Sander and Sander describe atoms as the set of all elements that produce $\langle a \rangle$ for the cyclic group, G, and eventually examined the sum of a pair of atoms. They counted the number of characterizations of every component in the disjoint union of atoms, namely sumset [11].

***CORRESPONDING AUTHOR** | **Mohd Sham Mohamad** ✉ mohdsham@umpsa.edu.my

Gopalakrishnan and Kumari associated cyclic groups using K_3 graphs relation by the generator for their study [12]. Villeta et al. determined the likelihood of obtaining a generator for a cyclic group up to 3000, however, focusing on prime numbers only [13]. Tanaka discovered that the standard likelihood of a cyclic group element is a generator [14].

A distinct connection established by Mohammed states that order is one of the important requirements for a pair of actions to act compatibly [8]. Sommer-Simpson determined the orders of $\mathrm{Aut}(\mathbb{Z}_n \times \mathbb{Z}_2)$ and $\mathrm{Aut}(\mathbb{Z}_q \times \mathbb{Z}_q \times \ldots \times \mathbb{Z}_q)$, given that *q* is prime [15]. Alperin observed that a definite established group is a cyclic group's core augmentation and has a finite automorphism group [16]. He also presented a clearer demonstration of Baer's prior theorem [17], which suggests that if a group processes only finitely many automorphisms, it is deemed finite.

Ahmad discovered the automorphism's cycle structure for a single, unidentified finite cyclic group of order [18]. Shahoodh's research focuses on the subsequent section of the instantaneous product of automorphisms [9]. Furthermore, the total number of automorphisms in these groups has been found and it was discovered that any automorphism group of this type contains a single element of order two.

Sommer-Simpson presented detailed conclusions regarding the structure of automorphism groups for semi-direct products where *M* and *N* are cyclic groups [15]. His work also included a general formulation of automorphisms and automorphism groups in dihedral groups. Additionally, he identified the automorphism group of the semi-direct product of $\mathbb{Z}_8 \rtimes \mathbb{Z}_2$. Meanwhile, Emery explored the automorphism groups of finite groups with small orders and provided broader insights into the automorphisms of cyclic groups [19].

Over time, only a limited number of generators have been identified for automorphisms of specific orders. This study aims to introduce generators for other orders, particularly focusing on the 2-power groups within finite cyclic groups. By utilizing the Groups, Algorithms, and Programming (GAP) software [20], the study determines the number of generators within these groups based on their respective orders.

2. METHODOLOGY

The subsequent theorem shows that one may express the automorphisms as an instantaneous multiplication of two finite cyclic groups with *q*-power order.

Theorem 2.1 [3]
Let *q* be an odd prime and $\alpha \in \mathbb{N}$. Assume *G*, a cyclic group of order q^r, where *q* is an odd prime and $r \in \mathbb{N}$. Therefore, $\mathrm{Aut}(G) \cong C_{q-1} \times C_{q^{\alpha-1}} \cong C_{(q-1)q^{\alpha-1}}$ and its order, $|\mathrm{Aut}(G)| = (q-1)q^{r-1}$.

Next, the interpretation of Euler's Phi-function is given.

Definition 2.1 Euler's φ-function [21]

Given that $x \geq 1$, Euler Phi-function, $\varphi(x)$ is a non-negative integer that is mutually prime to *x* and smaller than *x*.

The subsequent theorem clarified the order of every given number, *a*.

Theorem 2.2 [21]

Considering that the integer *z* modulo *m* with order *l* and $h > 0$, z^h has order $\left(\dfrac{l}{\gcd(h,l)}\right)$ modulo *m*.

The next theorem defines a generator, which provides the order of the automorphisms.

Theorem 2.3 [4]
Given U_n is cyclic where $n \geq 2$ if and only if it is in any of the following structures: 2, 4, q^r, or $2q^r$ with *q* being an odd prime and $r \in \mathbb{N}$.

The following proposition demonstrates that the automorphisms of a finite cyclic *q*-group include only a single element of order two.

Proposition 2.1 [9]

Every automorphism of finite cyclic *q*-group has a particular element with order two.

3. RESULTS AND DISCUSSION

Assuming $n \geq 2$ and U_n is a unitary group and it takes any of the specified structures 2, 4, q^r, or $2q^r$ with *q* being an odd prime and $r \in \mathbb{N}$. This paper primarily concentrates on the case of the q^r generator. Next, consider an integer *z* modulo *m* with order *l* and $h > 0$, z^h has order $\left(\frac{l}{\gcd(h,l)}\right)$ modulo *m*. Hence, the order-specific generator is as follows with *o* as an odd prime where $o < q$.

Table 1. Overview of the generators of the automorphism group based on their orders

Result	Generator	Order
Proposition 3.1	$\rho : g \rightarrow g^{q^r - 1}$	2
Theorem 3.1	$\rho : g \rightarrow g^{q-1}$	$2q^{r-1}$
Theorem 3.2	$\rho : g \rightarrow g^{o^{q^{r-1}}}$	$q-1$
Proposition 3.2	$\rho : g \rightarrow g^{o}$	$(q-1)(q^{r-1})$
Proposition 3.3	$\rho : g \rightarrow g^{-o^{q^{r-1}}}$	o
Proposition 3.4	$\rho : g \rightarrow g^{2}$	oq

A discussion on several lemmas, corollary, and theorems were given to support the previous claim.

Proposition 3.1
Let $G = \langle g \rangle \cong C_{q^r} = \langle q^r \rangle$, where *q* denotes an odd prime for some $r \geq 2$. Hence, $\rho : g \rightarrow g^{q^r - 1}$ in $\text{Aut}(C_{q^r})$ having an order of two.

Proof
Let $g^{q^r - 1}$ be an element for $G = \langle g \rangle \cong C_{q^r}$, where *q* denotes an odd prime for some $r \geq 2$. To prove $g^{(q^r - 1)^2} = g^1$, consider

$$\begin{aligned}(q^r - 1)^2 &= q^{2r} - 2q^r + 1 \\ &\equiv 1 \ (\text{mod}\, q^r)\end{aligned}$$

which gives $g^{q^r - 1}$ as the automorphism with order two. □

Lemma 3.1
Let *q* represents an odd prime, hence

$$(q-1)^{2q^{n-2}} \equiv m_n q^n + 1 - 2q^{n-1}$$

for some integer, m_n where $n \geq 2$.

Proof
The assertion is true through induction by letting $m_2 = 1$ when $n = 2$.

$$\begin{aligned}(q-1)^{2p^{2-2}} &\equiv m_2 q^2 + 1 - 2q^{2-1} \\ (q-1)^2 &\equiv m_2 q^2 + 1 - 2q \\ q^2 - 2q + 1 &\equiv q^2 - 2q + 1.\end{aligned}$$

Assume the statement holds for a specific $n > 2$. In light of Fermat's theorem and through the use of the binomial theorem,

$$
\begin{aligned}
(q-1)^{2q^{n-2+1}} &\equiv ((q-1)^{2q^{n-2}})^q \\
&\equiv (m_n q^n + 1 - 2q^{n-1})^q \\
&\equiv ((m_n q - 2)q^{n-1} + 1)^q \\
&\equiv ((m_n q - 2)q^{n-1})^q + \binom{q}{1}((m_n q - 2)q^{n-1})^{q-1} + \ldots + \binom{q}{q-1}(m_n q - 2)q^{n-1} + 1 \\
&\equiv Hq^{n+1} + m_n q^{n+1} + 1 - 2q^{n-1} \\
&\equiv m_{n+1} q^{n+1} + 1 - 2q^{n-1}
\end{aligned}
$$

where $m_{n+1} = H + m_n$ and H for some integers. In case of $n+1 > 2$, The statement is thus proven to be true. Consequently, by relying on the principle of mathematical induction, the assertion is valid for all $n \geq 2$. □

Lemma 3.2
Let q acts as an odd prime number, hence

$$(q-1)^{q^{n-2}} \equiv m_n q^n + q^{n-1} - 1$$

for some integers, m_n where $n \geq 2$.

Proof
The assertion is true through induction by letting $m_2 = 0$ when $n = 2$.

$$
\begin{aligned}
(q-1)^{p^{2-2}} &\equiv m_2 q^2 + q^{2-1} - 1 \\
(q-1) &\equiv m_2 q^2 + q - 1 \\
q - 1 &\equiv q - 1.
\end{aligned}
$$

Now, let us assume the statement holds for a certain $n > 2$. By referencing Fermat's theorem and utilizing the binomial theorem,

$$
\begin{aligned}
(q-1)^{q^{n-1+1}} &\equiv (m_n q^n + q^{n-1} - 1)^q \\
&\equiv ((m_n q + 1)q^{n-1} - 1)^q \\
&\equiv ((m_n q + 1)q^{n-1})^q + \binom{q}{1}((m_n q + 1)q^{n-1})^{q-1} + \ldots + \binom{q}{q-1}(m_n q + 1)q^{n-1} - 1 \\
&\equiv Hq^{n+1} + m_n q^{n+1} + q^{n-1} - 1 \\
&\equiv m_{n+1} q^{n+1} + q^{n-1} - 1
\end{aligned}
$$

where $m_{n+1} = H + m_n$ and H for some integers. In case of, the statement is therefore true. For the case of $n+1 > 2$, the statement is confirmed to be true. Thus, by the principle of mathematical induction, the assertion holds for all *n*. □

Theorem 3.1
Let $G = \langle g \rangle \cong C_{q^r} = \langle q^r \rangle$, where q denotes an odd prime for some $r \geq 2$. Next, the automorphism with order $2q^{r-1}$ is $\rho : g \to g^{q-1}$.

Proof
Referring to Theorem 2.1, *G* is a cyclic group with order q^r, which q represents odd prime and $r \in \mathbb{N}$. Hence, the $\mathrm{Aut}(G)$ represented as the instantaneous multiplication of two finite cyclic groups, and its order is $(q-1)q^{r-1}$. In order to validate the claim where ρ is an automorphism of order $2q^{r-1}$, it can be shown as follows:

(i) $(q-1)^{2q^{r-1}} \equiv 1 \bmod q^r$
(ii) $(q-1)^{2q^{r-2}} \equiv 1 - 2q^{r-1} \bmod q^r$.

By referring to Lemma 3.1, if raising the power of q to the equation, thus

$$(q-1)^{2q^{r-2}} \equiv 1-2q^{r-1} \bmod q^r$$

holds for all $r \geq 2$. Hence, (ii) follows by (i). This implies $\rho^{2q^{r-1}}(g) = g$ and $\rho^{2q^{r-2}}(g) \neq g$, which proves that ρ is an element of order $2q^{r-1}$. □

Theorem 3.2
Let $G = \langle g \rangle \cong C_{q^r} = \langle q^r \rangle$, where q denotes an odd prime for some $r \geq 2$. Next, $\rho : g \to g^{o^{q^{r-1}}}$ is an automorphism with order $q-1$, where o represents odd prime number, and $o < q$.

Proof
According to Theorem 2.1, G is a cyclic group with order q^r, which p represents odd prime and $r \in \mathbb{N}$. Hence, the $\operatorname{Aut}(G)$ represented as the instantaneous multiplication between two finite cyclic groups, and its order is $(q-1)q^{r-1}$. In pursuance of validating the claim, where ρ is an automorphism of order $q-1$, it can be stated as follows:

(i) $(o^{q^{r-1}})^{q-1} \equiv 1 \bmod q^r$
(ii) $(o^{q^{r-1}-1})^{q-1} \not\equiv 1 \bmod q^r$.

Given that any order with power of the highest order for the group will produce 1 as follows,

$$(o^{q^{r-1}})^{q-1} \equiv o^{(q^{r-1})(q-1)} \equiv 1 \bmod q^r$$

which holds for all $r \geq 2$. Hence, (ii) follows by (i).

$$\begin{aligned}(o^{q^{r-1}-1})^{q-1} &\equiv o^{(q^{r-1}-1)(q-1)} \\ &\equiv o^{(q^{r-1}q-q-q^{r-1}+1)} \\ &\equiv o^{(q^r-q-q^{r-1}+1)} \\ &\equiv o^{1-q(1-q^{r-1}+q^{r-2})} \\ &\not\equiv 1 \bmod q^r\end{aligned}$$

This implies $\rho^{q-1}(g) = g$, which validates that ρ is an element with order $q-1$. □

Proposition 3.2
Let $G = \langle g \rangle \cong C_{q^r} = \langle q^r \rangle$, where q denotes an odd prime for some $r \geq 2$. Hence, $\rho : g \to g^o$ is an automorphism with order $(q-1)q^{r-1}$, where o is an odd prime and $o < q$.

Proof
Let $G = \langle g \rangle \cong C_{q^r} = \langle q^r \rangle$, where q denotes an odd prime for some $r \geq 2$. Suppose that q, odd prime divisor for o. Consider $o = q^r s$, where s is a non-divisible integer by q. Since s is odd, $s^{\phi(q^r)} \equiv 1 (\bmod q^r)$ by Euler's theorem. By considering $t = \phi(q^r)$, $s^t \equiv 1(\bmod q^r)$. Since s is odd, $s^2 \equiv 1(\bmod 2)$. Hence $s^{2t} \equiv 1(\bmod 2)$. Therefore, $s^{2t} \equiv 1(\bmod 2q^r)$ and $o^{2t} \equiv 1(\bmod 2q^r)$. Consider, $o = q^r$, then $o^{2t} = q^{2rt} \equiv 1(\bmod 2q^r)$ since $2rt \geq r+1$ for $r \geq 1$ and q^{r+1} divides $2q^r$. Therefore, g^o is the generator with order $(q-1)q^{r-1}$ of automorphism group. □

Proposition 3.3
Let $G = \langle g \rangle \cong C_{q^r} = \langle q^r \rangle$, where q denotes an odd prime for some $r \geq 2$. Next, the automorphism of order o is $\rho : g \to g^{-o^{q^{r-1}}}$, where o as an odd prime and $o < q$.

Proof

Referring to Theorem 2.1, G is a cyclic group with order q^r, which q represents odd prime, and $r \in \mathbb{N}$. Hence, the $\mathrm{Aut}(G)$ represented as the instantaneous multiplication for a pair of finite cyclic groups, and its order is $(q-1)q^{r-1}$. In the interest of proving the claim, where ρ is an automorphism of order o, it can be stated as follows:

(i) $(-o^{q^{r-1}})^o \equiv 1 \bmod q^r$

(ii) $(-o^{q^{r-1}-1})^o \not\equiv 1 \bmod q^r$.

Given that any order with power of the highest order for the group will produce 1 as follows,

$$(-o^{q^{r-1}})^o \equiv -o^{(q^{r-1})(o)} \equiv 1 \bmod q^r$$

which holds for all $r \geq 2$. Hence, (ii) follows by (i).

$$\begin{aligned}(-o^{q^{r-1}-1})^o &\equiv -o^{(q^{r-1}-1)(o)} \\ &\equiv -o^{(q^{r-1}o-o)} \\ &\not\equiv 1 \bmod q^r\end{aligned}$$

This proves $\rho^o(g) = g$, which proves that ρ is an automorphism of order o. □

Proposition 3.4

Let $G = \langle g \rangle \cong C_{q^r} = \langle q^r \rangle$, where q denotes an odd prime for some $r \geq 2$. Thus, $\rho : g \to g^2$ is an automorphism of order oq, where o represents an odd prime and $o < q$.

Proof

Let $G = \langle g \rangle \cong C_{q^r} = \langle q^r \rangle$, where q denotes an odd prime for some $r \geq 2$. Given that o has an odd prime divisor, q. Consider $o = q^r s$, where s is an odd prime that cannot be divided by q, and $o < q$. Since o is odd, thus $o^{\phi(q^r)} \equiv 1(\bmod q^r)$ by Euler's theorem. Assuming $t = \phi(q^r)$, then $o^t \equiv 1(\bmod q^r)$. Since o is odd, $o^2 \equiv 1(\bmod 2)$. Hence, $o^{2t} \equiv 1(\bmod 2)$ and $s^{2t} \equiv 1(\bmod 2q^r)$. By letting $o = 2$, $o^{2t} = 2^{2t} \equiv 1(\bmod 2q^r)$ since $2^{2t} \equiv 1(\bmod 2)$ and $2^{2t} \equiv 1(\bmod q^r)$ by Euler's theorem. Hence, g^2 is the generator with the order oq for automorphism group, where o is an odd prime and $o < q$. □

4. CONCLUSIONS

This study extensively examined the generators of the q^r-power group's automorphism groups based on their precise order. The results presented here demonstrate how crucial the generator is in determining the automorphisms and, ultimately, the compatibility conditions of these groupings. This paper establishes a framework for future research exploring the formation and utilization of finite cyclic groups in diverse disciplines, contributing to the current discipline regarding the issue.

ACKNOWLEDGEMENTS

Institution(s)

All the authors would like to express their gratitude to Universiti Malaysia Pahang Al-Sultan Abdullah, Tunku Abdul Rahman University of Management and Technology (Pahang Branch), International Islamic University Malaysia, and Thaksin University for the support.

Fund

The authors would like to thank the Telkom University and Universiti Malaysia Pahang Al-Sultan Abdullah for the financial support under International Matching Grant, UIC221520: Deep Learning via Long Short-Term Memory (LSTM) Model in Predicting Stock Price (University reference RDU222707).

Individual Assistant

NA

DECLARATION OF ORIGINALITY

The authors declare no conflict of interest to report regarding this study conducted.

REFERENCES

[1] Brown R, Loday JL. Excision homotopique en basse dimension. Comptes Rendus de l'Académie des Sciences - Series I - Mathematics. 1984;298(15):353-56.

[2] Brown R, Johnson DL, Roberson EF. Some computations of non-abelian tensor products of groups. Journal of Algebra. 1987;11(1):177-202.

[3] Dummit DS, Foote RM. Abstract Algebra. 3rd ed. Hoboken, NJ: Wiley; 2003.

[4] Clark WE. Elementary Abstract Algebra. Retrieved from https://math.libretexts.org/Bookshelves/Abstract_and_Geometric_Algebra/Elementary_Abstract Algebra_(Clark); 2021.

[5] Broche O, García-Lucas D, Del Rio A. A classification of the finite 2-generator cyclic-by-abelian groups of prime-power order. International Journal of Algebra and Computation. 2023;33(04):641-86.

[6] Miech RJ. On *p*-groups with a cyclic commutator subgroup. Journal of the Australian Mathematical Society. 1975;20(2):178-98.

[7] Song Q. Finite two-generator *p*-groups with cyclic derived group. Communications in Algebra. 2013;41(4):1499-513.

[8] Mohamad MS. Compatibility conditions and nonabelian tensor products of finite cyclic groups of *p*-power order. PhD Thesis. Malaysia: Universiti Teknologi Malaysia, 2012.

[9] Shahoodh MK. Compatible Pair of Actions for Finite Cyclic Groups of *p*-Power Order. PhD Thesis. Malaysia: Universiti Malaysia Pahang, 2018.

[10] Lachaud G. The Klein quartic as a cyclic group generator. Moscow Mathematical Journal. 2005;5:857-68.

[11] Sander JW, Sander T. The Klein quartic as a cyclic group generator. Moscow Mathematical Journal. 2013;133(2):705-18.

[12] Gopalakrishnan M, Kumari NNM. Generator graphs for cyclic groups. AIP Conference Proceedings. 2019 June; 2112(1):020119.

[13] Villeta RB, Castillano EC, Padua RN. On the generators of the group of units modulo a prime and its analytic and probabilistic view. Recoletos Multidisciplinary Research Journal. 2021;9(2):115-21.

[14] Tanaka Y. Average probability of an element being a generator in the cyclic group. American Journal of Computational Mathematics. 2023;13(2):230-235.

[15] Sommer-Simpson J. Automorphism Groups for Semidirect Products of Cyclic Groups. arXiv preprint. 2019; arXiv:1906.05901.

[16] Alperin J. Groups with finitely many automorphisms. Pacific Journal of Mathematics. 1962;12(1):1-5.

[17] Baer R. Finite extensions of abelian groups with minimum condition. Transactions of the American Mathematical Society. 1955;79(2):521-40.

[18] Ahmad S. Cycle structure of automorphisms of finite cyclic groups. Journal of Combinatorial Theory. 1969;6(4):370-74.

[19] Emery S. About Automorphisms of Some Finite Groups. Master Thesis. United States: West Chester University, 2021.

[20] Groups, Algorithm, and Programming (GAP) Software. Retrieved from https://www.gap-system.org/; 2024.

[21] Burton D. Elementary Number Theory. 6th ed. USA: McGraw Hill; 2005.