On Cyclotomic Cosets as Orbit Structures under the Action of Cyclic Subgroups of $GL(d, q)$

Original Research Article

Abstract

Cyclotomic cosets are classical algebraic objects that arise naturally in modular arithmetic, finite field theory, and coding theory, especially in the study of polynomial factorization and cyclic codes. Traditionally, they are defined arithmetically through the formation of sets of the form $C_i = \{i \cdot p^j \bmod n \mid j \geq 0\}$, and their study has largely remained within that framework. However, this approach does not fully capture the group-action structure inherent in their formation. In particular, the interpretation of cyclotomic cosets as orbits under subgroup actions has not been formally developed in a way that extends to general linear groups over finite fields. This creates a theoretical gap between classical cyclotomy and the broader framework of orbit theory and linear group actions. This paper uses methods of mathematical proofs to addresses this gap by reinterpreting cyclotomic cosets as orbit structures. This idea is further extended to the natural action of subgroups of $GL(d, q)$ on the vector space $\mathbb{F}_q^d$, thereby defining a generalized cyclotomic orbit structure in higher dimensions. It is established that

$$\mathrm{Orb}_{\langle p \rangle}(i) = \{p^j \cdot i \mid j \geq 0\} = \{i \cdot p^j \bmod n \mid j \geq 0\}, \implies C_i = \mathrm{Orb}_{\langle p \rangle}(i),$$

showing that classical cyclotomic cosets are precisely orbit structures arising from cyclic subgroup actions. The findings further reveal that for the action of a subgroup $H \leq GL(d, q)$ on $\mathbb{F}_q^d$, the cyclotomic orbit $C_H(v) = \{h \cdot v \mid h \in H\}$ satisfies $|C_H(v)| = [H : \mathrm{Stab}_H(v)]$, showing that the size of each cyclotomic orbit is determined by the index of its stabilizer. This establishes a direct connection between cyclotomic structures and the Orbit–Stabilizer Theorem.This formulation places classical cyclotomic cosets within a wider orbit-theoretic setting and provides a new perspective for studying cyclotomic behavior through linear actions, contributing to the further study of orbit structures, invariants, and their advanced applications in finite fields, and group theory.

Keywords: *Cyclotomic orbit structuress; Cyclotomic cosets; group actions; orbits, general linear groups,$GL(d, q)$; finite fields; Orbit–Stabilizer Theorem.*

1 Introduction

Cyclotomic cosets are fundamental algebraic structures that arise in finite field theory and coding theory, particularly in the factorization of polynomials of the form $x^n - 1$ over $\mathbb{F}_q$ and in the construction of cyclic and constacyclic codes [4, 7, 8, 15, 12, 3, 1]. According to Ongili et al.[16], for a prime p with $\gcd(p, n) = 1$, a cyclotomic coset modulo n is defined as

$$C_i = \{i \cdot p^j \bmod n \mid j \geq 0\}, \quad i \in \mathbb{Z}_n.$$

These cosets form a partition of $\mathbb{Z}_n$, are finite, and exhibit periodicity determined by the smallest integer m such that $p^m \equiv 1 \pmod{n}$ [16]. Their structural properties have been widely applied in the enumeration and construction of cyclic codes over finite fields, particularly for specific prime fields $\mathrm{GF}(p)$ [16, 23, 24], where the number of cyclotomic cosets directly determines the number of irreducible factors of $x^n - 1$ and hence the number of cyclic codes [15, 16, 9, 10, 11, 18, 19, 13, 14, 20]. From the perspective of group theory [17, 5, 6, 2, 21, 22], let G be a group acting on a set X. The orbit of an element $x \in X$ under the action of G is defined by

$$\mathrm{Orb}_G(x) = \{g \cdot x \mid g \in G\},$$

which partitions X into disjoint equivalence classes and satisfies the orbit-stabilizer relation

$$|\,\mathrm{Orb}_G(x)| = [G : \mathrm{Stab}_G(x)].$$

A comparison of these constructions reveals a strong structural similarity that both cyclotomic cosets and orbits are generated through repeated application of a transformation, both partition the underlying set, and both exhibit periodic behavior. In particular, the mapping $x \mapsto px \bmod n$ induces a cyclic subgroup $\langle p \rangle$, under which each cyclotomic coset can be expressed as

$$C_i = \{p^j \cdot i \mid j \geq 0\} = \mathrm{Orb}_{\langle p \rangle}(i),$$

establishing cyclotomic cosets as special cases of orbits under cyclic subgroup actions. This correspondence motivates the extension of cyclotomic structures beyond the classical one-dimensional setting. In particular, by considering the natural action of subgroups $H \leq GL(d, q)$ on the vector space $\mathbb{F}_q^d$, cyclotomic cosets admit a natural generalization to higher-dimensional orbit structures, forming the basis for cyclotomic actions in linear groups. For $\gcd(p, n) = 1$, multiplication by p modulo n defines an element of $(\mathbb{Z}/n\mathbb{Z})^\times$, and $\langle p \rangle$ denotes the cyclic subgroup generated by this element.

1.1 Definitions

This section presents the fundamental concepts and structures that form the basis of the results developed in this paper.

1. **Finite Field.** A finite field $\mathbb{F}_q$ is a field consisting of a finite number of elements, where $q = p^m$ for some prime p and positive integer m. The operations of addition and multiplication are defined such that $\mathbb{F}_q$ forms a commutative field with identity.

2. **General Linear Group.** The general linear group of degree d over $\mathbb{F}_q$, denoted by $GL(d, q)$, is the group of all invertible $d \times d$ matrices with entries in $\mathbb{F}_q$, under matrix multiplication:
$$GL(d, q) = \{A \in M_{d\times d}(\mathbb{F}_q) \mid \det(A) \neq 0\}.$$

3. **Group Action.** Let G be a group and X a non-empty set. A (left) group action of G on X is a function
$$G \times X \to X, \quad (g, x) \mapsto g \cdot x,$$
satisfying the following properties for all $g, h \in G$ and $x \in X$:
$$e \cdot x = x, \quad (gh) \cdot x = g \cdot (h \cdot x),$$
where e is the identity element of G.

4. **Orbit.** Let G act on a set X. The orbit of an element $x \in X$ under G is defined as
$$\mathrm{Orb}_G(x) = \{g \cdot x \mid g \in G\}.$$
The set X is partitioned into disjoint orbits under this action.

5. **Stabilizer.** Let G act on X. The stabilizer of an element $x \in X$ is defined as
$$\mathrm{Stab}_G(x) = \{g \in G \mid g \cdot x = x\}.$$
It is a subgroup of G.

6. **Orbit-Stabilizer Theorem.** If G is a finite group acting on a set X, then for any $x \in X$,
$$|\mathrm{Orb}_G(x)| = [G : \mathrm{Stab}_G(x)] = \frac{|G|}{|\mathrm{Stab}_G(x)|}.$$

7. **Lagrange's Theorem.** Let G be a finite group and let $H \leq G$ be a subgroup. Then
$$|H| \mid |G|.$$
In particular, for any element $g \in G$, the order of g, denoted $\mathrm{ord}_n(g)$, divides $|G|$, and hence is finite.

8. **Cyclotomic Coset.** Let n be a positive integer and p a prime such that $\gcd(p, n) = 1$. The cyclotomic coset modulo n containing $i \in \mathbb{Z}_n$ is defined as
$$C_i = \{i \cdot p^j \bmod n \mid j \geq 0\}.$$
Each cyclotomic coset is finite and the collection of all such cosets forms a partition of $\mathbb{Z}_n$.

9. **Order of an Element Modulo n.** Let p be relatively prime to n. The order of p modulo n, denoted by $\mathrm{ord}_n(p)$, is the smallest positive integer m such that
$$p^m \equiv 1 \pmod{n}.$$
This value determines the size of cyclotomic cosets.

10. **Cyclic Subgroup.** Let G be a group and $p \in G$. The cyclic subgroup generated by p is defined as
$$\langle p \rangle = \{p^k \mid k \in \mathbb{Z}\}.$$

11. **Natural Action of $GL(d, q)$.** The group $GL(d, q)$ acts naturally on the vector space $\mathbb{F}_q^d$ by matrix multiplication:
$$A \cdot v = Av, \quad \forall A \in GL(d, q),\ v \in \mathbb{F}_q^d.$$

2 Results and Discussions

This section uses mathematical proofs, and examples to establish that classical cyclotomic cosets can be reinterpreted as orbits under cyclic subgroup actions, and that this extends naturally to subgroup actions in $GL(d, q)$.

2.1 Cyclotomic Cosets as Orbits under Cyclic Subgroup Actions

Lemma 2.1. *Let n be a positive integer and let p be a prime such that $\gcd(p, n) = 1$. Then multiplication by p modulo n defines a group action of the cyclic subgroup $\langle p \rangle$ on $\mathbb{Z}_n$.*

Proof. :
Since $\gcd(p, n) = 1$, the residue class of p modulo n is invertible in $\mathbb{Z}_n$. Hence p belongs to the multiplicative group of units modulo n, and so the set

$$\langle p \rangle = \{p^j \bmod n \mid j \geq 0\}$$

forms a cyclic subgroup under multiplication modulo n.

Define a map

$$\langle p \rangle \times \mathbb{Z}_n \to \mathbb{Z}_n$$

by

$$(p^j, i) \mapsto p^j \cdot i := ip^j \bmod n,$$

for all $i \in \mathbb{Z}_n$ and all $p^j \in \langle p \rangle$.

It remains to show that this map satisfies the axioms of a group action;

Identity property: Let $1 \in \langle p \rangle$ be the identity element. Then for every $i \in \mathbb{Z}_n$,

$$1 \cdot i = i \cdot 1 \bmod n = i \bmod n = i.$$

Thus the identity element fixes every element of $\mathbb{Z}_n$.

Compatibility property: Let $p^a, p^b \in \langle p \rangle$. Then for every $i \in \mathbb{Z}_n$,

$$p^a \cdot (p^b \cdot i) = p^a \cdot (ip^b \bmod n) = (ip^b)p^a \bmod n = ip^{a+b} \bmod n.$$

On the other hand,

$$(p^a p^b) \cdot i = p^{a+b} \cdot i = ip^{a+b} \bmod n.$$

Hence

$$p^a \cdot (p^b \cdot i) = (p^a p^b) \cdot i.$$

Therefore both axioms of a group action are satisfied. It follows that multiplication by p modulo n defines a group action of $\langle p \rangle$ on $\mathbb{Z}_n$. □

Theorem 2.1. *Let n be a positive integer and let p be a prime such that $\gcd(p, n) = 1$. Let $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, and let $\langle p \rangle$ denote the cyclic subgroup generated by p under multiplication modulo n. Then the cyclotomic coset $C_i = \{ip^j \bmod n \mid j \geq 0\}$ containing $i \in \mathbb{Z}_n$ is precisely the orbit of i under the action of $\langle p \rangle$ on $\mathbb{Z}_n$. That is,*

$$C_i = \mathrm{Orb}_{\langle p \rangle}(i).$$

Proof. :
Since $\gcd(p, n) = 1$, the residue class of p modulo n is a unit in $\mathbb{Z}_n$. Hence multiplication by p modulo n defines a permutation of $\mathbb{Z}_n$, and the set

$$\langle p \rangle = \{p^j \bmod n \mid j \in \mathbb{Z}_{\geq 0}\}$$

forms a cyclic subgroup of the multiplicative group of units modulo n.

Define an action of $\langle p \rangle$ on $\mathbb{Z}_n$ by

$$(p^j, i) \longmapsto p^j \cdot i := ip^j \bmod n,$$

for all $i \in \mathbb{Z}_n$ and all $p^j \in \langle p \rangle$.

It follows from Lemma 2.1 that $\langle p \rangle$ acts on $\mathbb{Z}_n$.

Now, by definition, the orbit of $i \in \mathbb{Z}_n$ under this action is

$$\mathrm{Orb}_{\langle p \rangle}(i) = \{g \cdot i \mid g \in \langle p \rangle\}.$$

Since every element $g \in \langle p \rangle$ has the form $p^j \bmod n$ for some $j \geq 0$, it follows that

$$\mathrm{Orb}_{\langle p \rangle}(i) = \{p^j \cdot i \mid j \geq 0\} = \{ip^j \bmod n \mid j \geq 0\}.$$

But the right-hand side is exactly the definition of the cyclotomic coset C_i. Therefore

$$C_i = \mathrm{Orb}_{\langle p \rangle}(i).$$

Hence every classical cyclotomic coset is an orbit under the cyclic subgroup generated by multiplication by p modulo n. □

2.2 Consequences of Orbit Interpretation and Derived Properties

Remark 2.2. *The reinterpretation is achieved by replacing the usual arithmetic description,*

$$C_i = \{ip^j \bmod n \mid j \geq 0\},$$

with a group-action description. In the arithmetic viewpoint, successive powers of p are repeatedly multiplied by i modulo n. In the orbit-theoretic viewpoint, the same process is regarded as the action of the cyclic subgroup $\langle p \rangle$ on the element i. Thus no new set is created; rather, the same object is viewed through a different structural framework.

Corollary 2.3. *The cyclotomic cosets modulo n form a partition of $\mathbb{Z}_n$.*

Proof. By Theorem 2.1,

$$C_i = \mathrm{Orb}_{\langle p \rangle}(i), \quad i \in \mathbb{Z}_n.$$

Since orbits of a group action partition the underlying set, it follows immediately that the family $\{C_i \mid i \in \mathbb{Z}_n\}$ forms a partition of $\mathbb{Z}_n$ (see [17, 5, 6]). □

Corollary 2.4. *If $\mathrm{Stab}_{\langle p \rangle}(i)$ denotes the stabilizer of i, then*

$$|C_i| = \left[\langle p \rangle : \mathrm{Stab}_{\langle p \rangle}(i)\right].$$

Proof. By Theorem 2.1,

$$C_i = \mathrm{Orb}_{\langle p \rangle}(i).$$

By the Orbit–Stabilizer Theorem,

$$|C_i| = \big[\langle p \rangle : \mathrm{Stab}_{\langle p \rangle}(i)\big] = \frac{|\langle p \rangle|}{|\mathrm{Stab}_{\langle p \rangle}(i)|}.$$

Here, the stabilizer is given by

$$\mathrm{Stab}_{\langle p \rangle}(i) = \{p^k \in \langle p \rangle \mid ip^k \equiv i \pmod{n}\}.$$

Thus, $\mathrm{Stab}_{\langle p \rangle}(i)$ consists of all powers of p that fix i, and its size determines the length of the cyclotomic coset C_i. □

Example 2.5. *Consider $n = 7$ and $p = 2$. Since $\gcd(2, 7) = 1$, the action is valid. The subgroup generated by 2 modulo 7 is*

$$\langle 2 \rangle = \{1, 2, 4\},$$

because

$$2^1 \equiv 2 \pmod{7}, \qquad 2^2 \equiv 4 \pmod{7}, \qquad 2^3 \equiv 8 \equiv 1 \pmod{7}.$$

Take $i = 1$. Then the cyclotomic coset containing 1 is

$$C_1 = \{1 \cdot 2^j \bmod 7 \mid j \geq 0\} = \{1, 2, 4\}.$$

Now compute the orbit of 1 under $\langle 2 \rangle$:

$$\mathrm{Orb}_{\langle 2 \rangle}(1) = \{1 \cdot 1, 1 \cdot 2, 1 \cdot 4\} \bmod 7 = \{1, 2, 4\}.$$

Hence

$$C_1 = \mathrm{Orb}_{\langle 2 \rangle}(1).$$

Similarly, for $i = 3$,

$$C_3 = \{3 \cdot 2^j \bmod 7 \mid j \geq 0\} = \{3, 6, 5\}.$$

Also,

$$\mathrm{Orb}_{\langle 2 \rangle}(3) = \{3 \cdot 1, 3 \cdot 2, 3 \cdot 4\} \bmod 7 = \{3, 6, 5\}.$$

Thus the reinterpretation holds concretely in this case.

Example 2.6. *Consider $n = 15$ and $p = 2$. Since $\gcd(2, 15) = 1$, multiplication by powers of 2 modulo 15 defines an action. The powers of 2 modulo 15 are*

$$2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 8, \quad 2^4 \equiv 16 \equiv 1 \pmod{15}.$$

Hence

$$\langle 2 \rangle = \{1, 2, 4, 8\}.$$

Take $i = 1$. Then

$$C_1 = \{1, 2, 4, 8\}.$$

The orbit is

$$\mathrm{Orb}_{\langle 2\rangle}(1) = \{1 \cdot 1, 1 \cdot 2, 1 \cdot 4, 1 \cdot 8\} \bmod 15 = \{1, 2, 4, 8\}.$$

Take $i = 3$. Then

$$C_3 = \{3 \cdot 2^j \bmod 15 \mid j \geq 0\} = \{3, 6, 12, 9\}.$$

The corresponding orbit is

$$\mathrm{Orb}_{\langle 2\rangle}(3) = \{3 \cdot 1, 3 \cdot 2, 3 \cdot 4, 3 \cdot 8\} \bmod 15 = \{3, 6, 12, 9\}.$$

Again,

$$C_3 = \mathrm{Orb}_{\langle 2\rangle}(3).$$

2.3 Orbit Structures under Subgroups of $GL(d, q)$

This section extends the idea from the one-dimensional setting $\mathbb{Z}_n$ to higher-dimensional vector spaces over finite fields.

Definition 2.7. *Let $H \leq GL(d, q)$ act naturally on $\mathbb{F}_q^d$ by*

$$h \cdot v = hv, \qquad h \in H,\ v \in \mathbb{F}_q^d.$$

For any $v \in \mathbb{F}_q^d$, define

$$C_H(v) = \{h \cdot v \mid h \in H\}.$$

So that $C_H(v)$ is the orbit of v under H. This formulation extends the interpretation of cyclotomic cosets as orbits under cyclic subgroup actions to higher-dimensional linear group actions.

Theorem 2.8. *Let $H \leq GL(d, q)$. Then the family of sets*

$$\{C_H(v) \mid v \in \mathbb{F}_q^d\}$$

forms a partition of $\mathbb{F}_q^d$. Moreover, each $C_H(v)$ is finite and

$$|C_H(v)| = [H : \mathrm{Stab}_H(v)].$$

Proof. :
Since $H \leq GL(d, q)$, each $h \in H$ is an invertible linear transformation on $\mathbb{F}_q^d$. Hence the rule

$$h \cdot v = hv$$

defines a group action of H on $\mathbb{F}_q^d$. Indeed, if I is the identity matrix, then

$$I \cdot v = Iv = v$$

for all $v \in \mathbb{F}_q^d$, and if $h_1, h_2 \in H$, then

$$h_1 \cdot (h_2 \cdot v) = h_1(h_2 v) = (h_1 h_2)v = (h_1 h_2) \cdot v.$$

Therefore H acts on $\mathbb{F}_q^d$.

By definition, $C_H(v)$ is the orbit of v under this action. Since orbits of a group action partition the underlying set, the family

$$\{C_H(v) \mid v \in \mathbb{F}_q^d\}$$

partitions $\mathbb{F}_q^d$.

Because $\mathbb{F}_q^d$ is finite and H is a finite subgroup of $GL(d, q)$, every orbit $C_H(v)$ is finite. Finally, by the Orbit-Stabilizer Theorem,

$$|C_H(v)| = |\operatorname{Orb}_H(v)| = [H : \operatorname{Stab}_H(v)].$$

□

Remark 2.9. *The term generalization is used here in a structural sense. Classical cyclotomic cosets are generated by repeated application of a single multiplicative transformation modulo n, forming finite partitions whose sizes are determined by the order of the acting element. The identification*

$$C_i = \operatorname{Orb}_{\langle p \rangle}(i)$$

shows that these cosets are precisely orbits under cyclic subgroup actions.

The extension to subgroups $H \leq GL(d, q)$ preserves this orbit-generating mechanism: sets are formed through group actions, they partition the underlying space, and their sizes are governed by stabilizers. Thus, the generalization lies in extending the underlying orbit structure from a one-dimensional modular setting to higher-dimensional linear actions, rather than in preserving specific number-theoretic properties.

The comparison between classical cyclotomic cosets and orbit structures under linear group actions is presented below.

Example 2.10. *Let $q = 3$, $d = 2$, and let*

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL(2, 3).$$

Let $H = \langle A \rangle \leq GL(2, 3)$. Consider the vector

$$v = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Then

$$Av = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = v.$$

Hence

$$C_H(v) = \{v\}.$$

Now take

$$w = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Then

$$Aw = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \qquad A^2 w = \begin{pmatrix} 2 \\ 1 \end{pmatrix},$$

Table 1: Classical Cyclotomic Cosets vs Orbit Structures under $GL(d, q)$

Property	**Classical Cyclotomic Cosets**	**Orbits under** $GL(d, q)$
Underlying Set	$\mathbb{Z}_n$	$\mathbb{F}_q^d$
Generating Mechanism	Repeated multiplication by p modulo n	Repeated application of linear transformations $h \in H$
Defining Structure	$C_i = \{ip^j \bmod n \mid j \geq 0\}$	$C_H(v) = \{h \cdot v \mid h \in H\}$
Group-Theoretic Interpretation	Orbit under cyclic subgroup $\langle p \rangle \subset (\mathbb{Z}/n\mathbb{Z})^\times$	Orbit under subgroup $H \leq GL(d, q)$
Partition Property	Cosets partition $\mathbb{Z}_n$	Orbits partition $\mathbb{F}_q^d$
Finiteness	Finite due to finite order $\mathrm{ord}_n(p)$	Finite since H is finite
Size Formula	$\lvert C_i \rvert = [\langle p \rangle : \mathrm{Stab}(i)]$	$\lvert C_H(v) \rvert = [H : \mathrm{Stab}_H(v)]$
Underlying Principle	Cyclic group action in one dimension	General group action in higher dimensions
Nature of Generalization	Number-theoretic and modular	Structural and group-theoretic

For A^3,

$$A^3 = A^2 \cdot A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}.$$

Now, since computations are carried out in $\mathbb{F}_3$*, we have*

$$3 \equiv 0 \pmod 3.$$

Thus,

$$\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I.$$

Hence,

$$A^3 = I.$$

Thus

$$C_H(w) = \left\{ \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \end{pmatrix} \right\}.$$

This shows how the higher-dimensional analogue of a cyclotomic coset arises as an orbit under a subgroup of $GL(d, q)$*.*

Remark 2.11. *The classical cyclotomic coset is therefore recovered when the acting subgroup is cyclic and the action is given by repeated multiplication in a one-dimensional setting. The extension to* $GL(d, q)$ *replaces scalar multiplication by linear transformation, while preserving the essential orbit structure.*

Limitations

This study is developed within a strictly algebraic framework and is subject to the following limitations:

(i) The extension to subgroups of $GL(d, q)$ is introduced to establish a higher-dimensional generalization of cyclotomic structures; however, a detailed classification and analysis of these orbit systems is beyond the scope of this work and is reserved for future research.

(ii) The results rely on the condition $\gcd(p, n) = 1$, which ensures that multiplication by p modulo n defines a valid group action through invertibility. This restriction is essential for the correspondence between cyclotomic cosets and orbit structures.

(iii) The study is confined to finite fields $\mathbb{F}_q$, where the finiteness of the underlying sets guarantees well-defined orbit and stabilizer structures. Extensions to infinite fields or more general algebraic settings are not considered in this work.

3 Conclusion and Recommendations

3.1 Conclusion

This study establishes a structural reinterpretation of classical cyclotomic cosets within the framework of group actions. It showns that for a prime p with $\gcd(p, n) = 1$, each cyclotomic coset

$$C_i = \{ip^j \bmod n \mid j \geq 0\}$$

is precisely the orbit of the element $i \in \mathbb{Z}_n$ under the action of the cyclic subgroup $\langle p \rangle$. This result demonstrates that cyclotomic cosets are not merely analogous to orbits, but are exactly orbit structures arising from a well-defined group action. Building on this observation, the concept of cyclotomic actions of subgroups of $GL(d, q)$ is introduced. Under this framework, classical cyclotomic cosets appear as special cases of orbit structures, while their higher-dimensional analogues arise through the natural action of subgroups $H \leq GL(d, q)$ on the vector space $\mathbb{F}_q^d$. This establishes a direct and rigorous connection between cyclotomy and orbit theory, thereby providing a unified perspective that links modular arithmetic, group actions, and linear algebra over finite fields. The results presented form a foundational basis for the study of cyclotomic orbit structures in linear groups.

Table 2: Summary of Key Findings

Concept	**Key Finding**
Cyclotomic Cosets	Cyclotomic cosets defined by $$C_i = \{ip^j \bmod n \mid j \geq 0\}$$ are shown to be equivalent to orbit structures under group actions.
Group Action	Multiplication by p modulo n defines a valid group action of the cyclic subgroup $\langle p \rangle$ on $\mathbb{Z}_n$.
Main Result	Cyclotomic cosets are precisely orbits: $$C_i = \mathrm{Orb}_{\langle p \rangle}(i).$$
Partition Property	Cyclotomic cosets form a partition of $\mathbb{Z}_n$ as a direct consequence of orbit decomposition under group actions.
Finiteness	Each cyclotomic coset is finite since it corresponds to an orbit under a finite cyclic subgroup.
Orbit-Stabilizer Connection	The size of each cyclotomic coset satisfies $$\lvert C_i \rvert = [\langle p \rangle : \mathrm{Stab}_{\langle p \rangle}(i)],$$ linking cyclotomic structure to the Orbit–Stabilizer Theorem.
Higher-Dimensional Extension	The concept extends to subgroups $H \leq GL(d, q)$, where $$C_H(v) = \{hv \mid h \in H\}$$ defines cyclotomic orbits in $\mathbb{F}_q^d$.
General Insight	Cyclotomic cosets are reinterpreted as intrinsic orbit structures, unifying classical algebraic constructions with group action theory.

3.2 Recommendations

The framework developed in this study opens several directions for further investigation;

(i) A detailed classification of cyclotomic orbits under various subgroups of $GL(d, q)$, including cyclic, diagonal, and more general matrix groups, would provide deeper insight into their structure and distribution.

(ii) The exploration of connections between cyclotomic orbit structures and cycle index theory, particularly in relation to permutation representations of linear subgroups.

(iii) Potential applications in coding theory, especially in the construction of new classes of linear and cyclic codes.

Competing Interests
Author has declared no competing interest.

References

[1] Almazrouei, K., & Alnajjar, K. A. (2024). Error-correcting Codes in Communication Systems. IWCMC Proceedings.

[2] Adsul, B., Sohoni, M., & Subrahmanyam, K. V. (2023). Orbit closures, stabilizer limits and intermediate G-varieties. arXiv preprint arXiv:2309.15816.

[3] Ball, S. (2020). Finite Fields: A Course in Algebraic Error-Correcting Codes.

[4] Childs, L. N., Childs, L. N. *Rings and Fields. Cryptology and Error Correction: An Algebraic Introduction and Real-World Applications*, 65-82.(2019).

[5] Dixon, J. D. (1985). The orbit-stabilizer problem for linear groups. Canadian Journal of Mathematics, 37(2), 238-259.

[6] Giudici, M., Liebeck, M., Praeger, C., Saxl, J., & Tiep, P. (2016). Arithmetic results on orbits of linear groups. Transactions of the American Mathematical Society, 368(4), 2415-2467.

[7] Koroglu, M. E., & Siap, I. *Quantum codes from a class of constacyclic codes over group algebras. Malaysian Journal of Mathematical Sciences*, 11(2), 289-301.(2017).

[8] La Guardia, G. G., & Alves, M. M. *On cyclotomic cosets and code constructions. Linear Algebra and its Applications*, 488, 302-319. (2016).

[9] Lao, H., Kivunge, B., Kimani, P., Muthoka, G. *On the Number of Cyclotomic Cosets and Cyclic Codes over Z_{13}*. (2015)

[10] Lao, H., Kivunge, B., Muthoka, G., Mwangi, P. *Enumeration of cyclic codes over GF (17)*.(2017)

[11] Maganga, B. M. and Joash, M. N. *Enumeration of cyclic codes over GF (19). Kenyatta University*.(2017).

[12] Mesnager, S. (2021). Linear Codes from Functions. In Concise Encyclopedia of Coding Theory.

[13] Ondiany, J. J. O., Obogi, R., Mude, L. H., & Monari, F. (2024). On the Number of Cyclic Codes Over Z_{31}. Journal of Advances in Mathematics and Computer Science.

[14] Ondiany, J. J. O., & Mude, L. H. (2025). On the Zeros of Linear Factors of Cyclotomic Polynomials Over Galois Fields. Journal of Advances in Mathematics and Computer Science.

[15] Ongili, P., Mude, L. H., & Ndung'u, K. J. (2024). On the generalization of the number of cyclic codes over the prime field GF (37).

[16] Ongili, P. O., Mude, L. H., Kaunda, Z. K., & Kibe, K. K. (2025). On Counting the Number of Cyclic Codes of Length n Over Prime Fields. Earthline Journal of Mathematical Sciences, 15(3), 419-435.

[17] Pyone, A. (2018). Orbit-Stabilizer Theorem and Consequences. J. Myanmar Acad. Arts Sci, 16(3), 1.

[18] Runji, Flora Mati. *Enumeration of cyclic codes over GF (5)*.4(4):3241-3302.(2014).

[19] Simatwo, K. B., Mati, R. F., Karieko, O. R. *Enumeration of Cyclic Codes Over GF (23).Journal of Advances in Mathematics and Computer Science*, 38(9), 194-206. (2023).

[20] Singh, M., & Deepak. (2024). Explicit factorization of $x^n - 1$ over finite fields. Journal of Algebra and Its Applications.

[21] van Zanten, A. J. (2019). Primitive idempotents of cyclic codes. Designs, Codes and Cryptography.

[22] Vega, G. (2021). Explicit factorization of period polynomials. Arithmetic of Finite Fields.

[23] Zhu, L., Liu, J., & Wu, H. (2024). Explicit Representatives and Sizes of Cyclotomic Cosets and their Application to Cyclic Codes over Finite Fields. arXiv:2410.12122.

[24] Zhu, L., Liu, J., & Wu, H. (2024). Cyclotomic Systems and their Arithmetic. arXiv:2412.12455.