A STUDY ON UNITS IN GROUP RINGS

A Thesis submitted
in fulfilment of the requirements
for the Degree of

Doctor of Philosophy

by

HIMANSHU SETIA
(2017MAZ0010)

Under the Guidance of

Dr. Manju Khan

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY ROPAR
OCTOBER 26, 2023

With boundless gratitude, I dedicate,
This thesis to those who helped create,
My family, friends, and mentors dear,
Whose support and love I hold so near.

Declaration of Originality

I hereby declare that the work which is being presented in the thesis entitled **A study on units in group rings** has been solely authored by me. It presents the result of my own independent investigation/research conducted during the time period from January 10, 2018 to February 22, 2022 under the supervision of **Dr. Manju Khan**, Associate Professor, Department of Mathematics, Indian Institute of Technology Ropar. To the best of my knowledge, it is an original work, both in terms of research content and narrative, and has not been submitted or accepted elsewhere, in part or in full, for the award of any degree, diploma, fellowship, associateship, or similar title of any university or institution. Further, due credit has been attributed to the relevant state-of-the-art and collaborations (if any) with appropriate citations and acknowledgments, in line with established ethical norms and practices. I also declare that any idea/data/fact/source stated in my thesis has not been fabricated/ falsified/ misrepresented. All the principles of academic honesty and integrity have been followed. I fully understand that if the thesis is found to be unoriginal, fabricated, or plagiarized, the Institute reserves the right to withdraw the thesis from its archive and revoke the associated Degree conferred. Additionally, the Institute also reserves the right to appraise all concerned sections of society of the matter for their information and necessary action (if any). If accepted, I hereby consent for my thesis to be available online in the Institute's Open Access repository, inter-library loan, and the title & abstract to be made available to outside organizations.

Signature

Name: Himanshu Setia

Entry Number: 2017MAZ0010

Department: Mathematics

Indian Institute of Technology Ropar

Rupnagar, Punjab 140001

Date: October 26, 2023

Acknowledgement

I wish to express my heartfelt gratitude to the individuals who have made this thesis possible. First and foremost, I would like to thank my supervisor, Dr. Manju Khan, for her support and encouragement throughout the journey. Her constant guidance and constructive feedback have been crucial in shaping the direction of this thesis. She has taught me to rise above roadblocks and to put my all into every effort. Her words, "Life is really hard and competitive," have been a constant reminder to strive for excellence. I extend my appreciation to the members of my doctoral committee, Dr. S. C. Martha, Dr. Arti Pandey, Dr. Apurva Mudgal, and Dr. Tapas Chatterjee, for their invaluable guidance, support, and feedback throughout the research process.

With gratitude, I recall Hita Ambrish ji and Acharya Prashant,
Whose wisdom and guidance left me with an enduring enchant.
Hita Ambrish ji showed me the path of devotion with his grace,
Acharya Prashant ji taught me the Vedantic truth with his embrace.
Their teachings led me to find inner peace and divine love so pure,
Forever grateful for the blessings of these spiritual mentors so sure.

I am deeply grateful for the support and guidance provided by my senior and collaborator, Dr. Surinder Kaur, during my doctorate. I would also like to express my appreciation to Dr. Leo Margolis for the informal discussions related to the beauty of concrete mathematics that enriched my understanding of the subject.

I extend my heartfelt gratitude to my colleague Ankita Gupta for her assistance in writing a GAP code and for her helping nature in general. I was fortunate to have her support and encouragement during the course of my research. In addition, I would like to acknowledge Sahil Joshi for the late night philosophical discussions related to mathematics that were a constant source of interest during my doctorate. I am grateful for his insightful perspectives and thought-provoking conversations. Moreover, I am thankful to all the research scholars in the department for creating a healthy research environment and providing me with the support and resources

necessary to continue my research in a creative way. Their encouragement and support were crucial to my academic growth and success. I would like to acknowledge Dr. Rahul Kaushik and Jyoti Garg for their invaluable contributions in clearing my doubts and for enlarging my vision.

I am grateful to the Department of Mathematics at IIT Ropar provided me with a welcoming and supportive environment and the necessary lab facilities and resources to carry out my research. I would also like to express my gratitude to Mr. Neeraj for his technical expertise and prompt resolution of every issue related to my PC, and to Ms. Jaspreet for her assistance with department facilities. I express my sincere gratitude to the MHRD for their financial support that has allowed me to conduct my research. Furthermore, the FIST program of the Department of Science and Technology, Government of India, Reference No. SR/FST/MS-I/2018/22(C) has also provided partial support for this work.

Lastly, I would like to thank my family for their constant love and support during my doctoral journey. I am grateful to my Mom for her unwavering love and motivation in all ups and downs during my research. Her encouragement helped me stay focused and motivated during difficult times. I would like to thank my Dad for providing me with every kind of help I needed. His support and guidance were crucial to my success. I am thankful for my younger brother Parth Setia's cheerful attitude and his willingness to sacrifice his sleep so I could study late at night during the Corona pandemic when we shared a room at home.

To each of you, I offer
my deepest thanks for your
contributions to this work.

Certificate

This is to certify that the thesis entitled **A study on units in group rings**, submitted by **Himanshu Setia** for the award of the degree of **Doctor of Philosophy** of Indian Institute of Technology Ropar, is a record of bonafide research work carried out under my guidance and supervision. To the best of my knowledge and belief, the work presented in this thesis is original and has not been submitted, either in part or full, for the award of any other degree, diploma, fellowship, associateship or similar title of any university or institution.

In my opinion, the thesis has reached the standard fulfilling the requirements of the regulations relating to the Degree.

Signature of the Supervisor

Name: Dr. Manju Khan

Department: Mathematics

Indian Institute of Technology Ropar

Rupnagar, Punjab 140001

Date: October 26, 2023

Lay Summary

The thesis investigates the structure of the unit group of group rings, which are formed by combining a group and a ring. The normal complement problem in group rings is also studied, which involves understanding the structure of the unit group of a group ring and determining if there exists a certain type of subgroup called a normal complement.

The thesis begins by studying unit groups of group algebras of the alternating group on 4 symbols, a class of dihedral groups and the symmetric group on 4 symbols, when taken over a field of characterstic 2. The thesis explores the group rings of the groups of exponent 2 and 4 over the ring of integers modulo n. The unit groups of these group rings are studied and their structure and generators are determined. Furthermore, the normal complement problem is solved for some of these group rings. Additionally, the unit group of the group ring of the elementary abelian 3-group over the ring of integers modulo n is investigated, and its structure and generators are determined.

List of Notations

Notation	Description
$\|X\|$	The cardinality of the set X
$o(g)$	The order of the group element g
$\hat{H}$	The sum of elements of H as an additive group
C_n	A cyclic group of order n
$\mathrm{char}(F)$	The characteristic of the field F
$G \simeq H$	The group isomorphism between G and H
$R \cong S$	The ring isomorphism between R and S
$C_H(g)$	The centralizer of g in a group H
RG	The group ring of a group G over a ring R
$\omega(RG)$	The augmentation ideal of a group ring RG
$Z(G)$	The center of a group G
$Z(RG)$	The center of a group ring RG
$\mathbb{U}(R)$	The unit group of a ring R
$\mathbb{V}(RG)$	The normalized unit group of a group ring RG
$R_1 \oplus R_2$	The direct sum of rings R_1 and R_2
$M_n(R)$	The ring of $n \times n$ matrices over R
$GL(n, R)$	The general linear group of degree n over R
$SL(n, R)$	The special linear group of degree n over R
$\varphi(m)$	The Euler-phi function of m
$H \times K$	The direct product of groups H and K
$H \rtimes K$	The internal semidirect product of groups H and K
$\exp(G)$	The exponent of the group G
$G^{(n)}$	The direct product of n-copies of G

Abstract

The primary objective of this thesis is to investigate the unit group of group rings and address the normal complement problem in the unit group.

Firstly, we assume that F is finite field of characteristic 2 and investigate the existence of normal complements for the dihedral group D_{4m} of order $4m$ and the alternating group A_4, where m is an odd integer greater than or equal to 3. A normal complement for S_4 in $\mathbb{V}(FS_4)$ over a field F containing exactly two elements has been found.

Further, let $\mathbb{Z}_n$ be the ring of integers modulo n. We use C_t, E_m, and $F_{r,s}$ to respectively denote the cyclic group of order t, the elementary abelian 2-group of order 2^m, and an abelian group of exponent 4 with order 2^r4^s. We find the generators of the normalized unit group $\mathbb{V}(\mathbb{Z}_nC_2)$ and solve the normal complement problem in $\mathbb{V}(\mathbb{Z}_nC_2)$. We also provide a normal complement of E_m in $\mathbb{V}(\mathbb{Z}_{2^n}E_m)$. Furthermore, we determine the structure of $\mathbb{V}(\mathbb{Z}_{p^n}F_{r,s})$ for an odd prime p and establish that $F_{r,s}$ does not have a normal complement in $\mathbb{V}(\mathbb{Z}_{p^n}F_{r,s})$.

Moreover, we give the structure and generators of the unit group $\mathbb{U}(\mathbb{Z}_nC_3)$. Lastly, we provide the structure of $\mathbb{U}(\mathbb{Z}_nT_m)$, where T_m is the elementary abelian 3-group of order 3^m and $\gcd(n, 3) = 1$.

Contents

Chapter 1

Introduction

In 1843, Cayley [1] introduced the abstract group, and also introduced group rings as the basic units of a hypercomplex system in the same article. However, group rings remained unnoticed until T. Molien used his semi-simple criteria to study these structures. Notably, F.G. Frobenius, R. Brauer, and E. Noether recognized the importance of group rings in the development of representation theory. The publication of Irving Kaplansky's books [2] and [3], in 1957 and 1970 generated significant interest in group rings among ring theorists, leading to increased exploration in this area. Ian G. Connell's [4] article in 1962 highlighted various ring-theoretic properties of group rings.

Group rings are a fundamental algebraic concept that integrates the study of groups, rings, and modules. They are a powerful tool for understanding algebraic structures in mathematics and physics. Specifically, they are essential in the study of representations of finite groups, which play a crucial role in algebraic number theory and algebraic geometry. Additionally, group rings have applications in topology, where they define higher K-theory groups. In cryptography, they are used to construct secure encryption algorithms. The broad range of applications and versatility of group rings make them a subject of significant importance in modern mathematics and its applications. Several books on the subject have been published in recent years (see [5], [6], [7], [8], [9]).

1.1 Preliminaries

In this section, we first provide some basic definitions from group theory and ring theory that will be used throughout this thesis. These definitions can be found in [10], [7], and [11].

Firstly, let us fix some notations. Suppose G is a group with identity element

e. Then, the exponent of group G is defined as the smallest positive integer l such that $g^l = e$ for all $g \in G$. We denote the exponent of G by $\exp(G)$. Furthermore, let $Z(G)$ denote the center of group G, and let $o(g)$ denote the order of an element $g \in G$. For any $n, m \in \mathbb{Z}$, we say that $n^i || m$ if n^i divides m but n^{i+1} does not.

Now, we recall some group-theoretic definitions that will be needed in later chapters of this thesis. These definitions can be found in [7].

Let H and K be subgroups of a group G. We say that G is an internal semidirect product of H by K, denoted by $G = H \rtimes K$, if:

1. $G = HK = KH$.
2. $H \cap K = \{e\}$.
3. H is a normal subgroup of G.

Consider the sequence of groups G, K, and H with homomorphisms ϕ and ψ:

$$\{e\} \to H \xrightarrow{\phi} G \xrightarrow{\psi} K \to \{e\}.$$

This sequence is called a short exact sequence if ϕ is injective, ψ is surjective, and the image of ϕ is equal to the kernel of ψ, i.e., $\operatorname{Im}\phi = \ker\psi$. If there exists a homomorphism $\delta : K \to G$ such that $\psi \circ \delta$ is the identity map on K, then the sequence is called a split exact sequence, and we have $G \cong H \rtimes K$.

A matrix representation of G over R of degree n is by definition a group homomorphism $T : G \to \mathrm{GL}(n, R)$. If the homomorphism T associates to every element of G with the identity of $GL(n, R)$, then it is said to be the trivial representation of G over R of degree n. The representations $T, T' : G \to GL(n, R)$ of the group G are said to be equivalent if there exists an invertible matrix $M \in GL(n, R)$ such that $T(g) = M^{-1}T'(g)M$ for all $g \in G$.

Let's review some definitions and standard results from ring theory. The characteristic of a ring R is defined to be the smallest number of times one must add the ring's multiplicative identity to get the additive identity. An element $x \in R$ is called a nilpotent element if there exists a positive integer k such that $x^k = 0$. If x is a nilpotent element of a ring R, then the element $(1 + x) \in \mathbb{U}(R)$. Thus, for a nil

ideal I of a ring R, $(1+I)$ is a normal subgroup of $\mathbb{U}(R)$. Hence, if I be a nil ideal of a ring R, then the natural epimorphism $R \to R/I$ induces an epimorphism from $\mathbb{U}(R)$ onto $\mathbb{U}(R/I)$ with kernel $1+I$. Thus,

$$\frac{\mathbb{U}(R)}{1+I} \simeq \mathbb{U}\left(\frac{R}{I}\right). \tag{1.1}$$

A ring A with unity (denoted by 1_A) is said to be an R-algebra, for a commutative ring R with unity (denoted by 1_R), if there is a ring homomorphism $\phi : R \to A$ such that $\phi(1_R) = 1_A$ and $\phi(R) \subset Z(A)$, the center of A.

1.2 Group Ring

This section serves as an introduction to the topic of group rings, where we present fundamental definitions and facts. The definitions and results presented in this section are sourced from [13].

For a group G and a ring with unity R, the set of all R-valued functions on G that vanish except for finitely many points, form a ring and is called a group ring and is denoted by RG. On denoting the function δ_α that takes value 1 on $\alpha \in G$ and zero elsewhere by simply α, the function that takes values $b_\alpha \in R$ at the point $\alpha \in G$, can be expressed as $\sum b_\alpha \alpha$, where $b_\alpha = 0$ for all but finitely many $\alpha \in G$. Note that RG is a free R-module with G as its basis. If R is commutative, then RG is an R-algebra as R gets embedded naturally inside the center of RG. Moreover, when G is a finite group, RG becomes a finite-dimensional R-algebra, and its rank over R, denoted $\text{rank}_R(RG)$, is equal to the cardinality of G, i.e., $\text{rank}_R(RG) = |G|$.

Let R be a commutative ring with prime characteristic p, and suppose there exists an element of order p in the group G. Then, the group algebra RG is called a modular group algebra.

A group algebra FG of a finite group G over a finite field F is semisimple if and only if the characteristic of F does not divide $|G|$. By the Wedderburn-Artin's structure theorem [13, Section 3.4], FG is isomorphic to a direct sum of matrix rings

over division rings, i.e.,

$$FG \cong \bigoplus_{i=1}^{r} M_{n_i}(D_i),$$

where D_i is a division ring containing an isomorphic copy of F in its center, and the above isomorphism is an isomorphism of F-algebras.

Next, we introduce the augmentation map and the augmentation ideal, which play a key role in our study in this thesis. We define the map $\epsilon : RG \to R$ by the rule $\epsilon(\sum_{g\in G} \alpha_g g) = \sum_{g\in G} \alpha_g$, which is known as the augmentation map. It is easy to see that ϵ is a surjective homomorphism. The kernel of ϵ is called the augmentation ideal of RG, denoted by $\omega(RG)$. Explicitly, we have

$$\omega(RG) = \left\{ \sum_{g\in G} \alpha_g g \in RG \mid \sum_{g\in G} \alpha_g = 0 \right\}.$$

Note that any element $w = \sum_{g\in G} \alpha_g g \in \omega(RG)$ can be written as $w = \sum_{g\in G} \alpha_g(g-1)$. It follows that the set $\{g-1 \mid g \in G, g \neq 1\}$ forms a basis of $\omega(RG)$ as an R-module.

Let H be a subgroup of G, and let $T_l\left(\frac{G}{H}\right) = \{t_\alpha \mid \alpha \in I\}$ denote a left transversal of H in G. Thus, any element g of G can be written as $t_\alpha h$, where $t_\alpha \in T_l\left(\frac{G}{H}\right)$ and $h \in H$. Therefore, any element $\alpha = \sum_{g\in G} \alpha_g g \in RG$ can be expressed uniquely as $\alpha = \sum_{i=1}^{m} t_{\alpha_i} x_i$, where $x_i \in RH$. Thus, RG is a free right RH-module with $T_l\left(\frac{G}{H}\right)$ as a free RH-basis. Moreover, RG is also a free left RH-module with a right transversal of H in G as a free RH-basis.

For a subgroup H of G, we define $\Gamma_l(H)$ to be the left ideal of RG generated by elements $\{h-1, h \in H\}$. Then it is evident that the elements in the set

$$L = \left\{ t_\alpha(h-1) \mid t_\alpha \in T_l\left(\frac{G}{H}\right), 1 \neq h \in H \right\}$$

form a basis of $\Gamma_l(H)$ as a left R-module. In a similar way one can define the right ideal $\Gamma_r(H)$ of RG. Note that $\Gamma_l(H)$ or $\Gamma_r(H)$ is a two-sided ideal of RG if and only if H is a normal subgroup of G and in this case, we denote this two sided ideal by $\Gamma(H)$. Therefore, $\Gamma(H) = \omega(RH) \cdot RG = RG \cdot \omega(RH)$. In particular, when $H = G$, we have $\Gamma(G) = \omega(RG)$.

Let F be a finite field. Suppose H is a normal subgroup of the group G. Consider the canonical group homomorphism $\psi : G \to G/H$ defined by the rule $g \mapsto gH$. Then ψ can be extended to an F-algebra homomorphism from FG onto $F(G/H)$ with $\Gamma(H)$ as its kernel. Thus

$$\frac{FG}{\Gamma(H)} \cong F(G/H).$$

If $H = G$, then

$$\frac{FG}{\omega(FG)} \cong F$$

and so in this case $\omega(FG)$ is a maximal ideal of FG. Further, it follows from [6, Lemma 1.6] that the augmentation ideal of a group algebra FG is a nilpotent ideal if and only if $\mathrm{char}(F) = p > 0$ and G is a finite p-group.

For a fixed element $a \in G$, define $C_a = \{g^{-1}ag : g \in G\}$, a set of all conjugates of the element a in G. It is called the conjugacy class of the group G containing a. Note that the class sum $\widehat{C_a} \in Z(FG)$. It is well known that the set of all finite class sums forms a basis of $Z(FG)$ over F.

Let R be a ring with unity and H be a subgroup of G. If $|H|$ is invertible in R, then $e_H = \frac{\hat{H}}{|H|}$ is idempotent in RG. Moreover, if $H \trianglelefteq G$, then e_H is central and

$$RG \cong RGe_H \oplus RG(1 - e_H).$$

Further, let $R_1, R_2, \ldots, R_t$ be unital rings. Then for any finite group G, we have

$$\left(\prod_{i=1}^{t} R_i\right) G \cong \prod_{i=1}^{t} R_i G.$$

For details, see [14, Lemma 1].

1.3 Unit Group

The study of units, nilpotent elements, idempotent elements, and zero divisors plays a crucial role in the theory of group rings. However, the study of units has

received significant research attention in the last few decades. This section will define some terms and explain the fundamental concepts related to the unit group of a group algebra. We also provide a literature review of the unit group in the end. We begin with defining the normalized unit group of group algebra FG, which is the collection of all invertible elements of FG that have an augmentation equal to 1. This set is denoted by $\mathbb{V}(FG)$. Thus

$$\mathbb{V}(FG) = \left\{ \sum_{g\in G} \alpha_g g \in \mathbb{U}(FG) : \sum_{g\in G} \alpha_g = 1 \right\}.$$

It is clear that $\mathbb{V}(FG)$ forms a subgroup of the unit group $\mathbb{U}(FG)$ and that

$$\mathbb{U}(FG) = \mathbb{V}(FG) \times F^{\times}.$$

Further, note that for a normal subgroup H of a finite p-group G and a field F of characteristic p, the F-algebra isomorphism $\frac{FG}{\Gamma(H)} \cong F(G/H)$ induces a group epimorphism from $\mathbb{V}(FG)$ to $\mathbb{V}(F(G/H))$ whose kernel is $(1+\Gamma(H))$ and so

$$\frac{\mathbb{V}(FG)}{1+\Gamma(H)} \simeq \mathbb{V}(F(G/H)).$$

In particular, when $H = G$, we get that $(1+\omega(FG)) \subseteq \mathbb{V}(FG)$ and therefore, $\mathbb{V}(FG) = 1+\omega(FG)$ is a p-group.

In his paper [15], G. Higman investigated the units in integral group rings of finite abelian groups and provided a characterization of the finite groups that have only trivial units. A. Bovdi's survey article [16] discussed various results and open problems related to the group of units of the group algebra FG, where F is a finite field of characteristic p and G is a finite p-group. R. Sandling [17] determined the generators and invariants of the unit group of FG when G is a finite abelian p-group and F has p elements. This line of investigation was continued in [18] by V. Bovdi and M. Salim, who provided the invariants for the unit group of the group algebra $\mathbb{Z}_{p^e}G$. For more articles in this direction, see [19], [20], and [21].

Several authors have explicitly determined the structure of the unit group of some group algebras of non-abelian groups. The structures of $\mathbb{U}(FS_4)$, $\mathbb{U}(FD_{10})$,

$\mathbb{U}(FA_4)$, and $\mathbb{U}(FS_3)$ over any finite field F are obtained in [22], [23], [24], and [25], respectively. For an odd prime p, the descriptions of $\mathbb{U}(FD_{2p})$ over the field F with 2 elements and over a finite field F such that $\mathrm{char}(F) = p$ are provided in [26] and [27], respectively. The structure of $\mathbb{U}(F(C_3 \times D_6))$ over a finite field F of characteristic 3 is established in [28]. For a detailed study of the structure of the unit group in various integral group rings, one can refer to [5] and [8].

1.4 Normal Complement

In this section, we introduce the normal complement problem in group rings and provide an overview of its current status.

R. Keith Dennis in 1977 posed a problem which asks,“ For which group G and ring R, there exists a homomorphism $\phi : \mathbb{U}(RG) \to G$ such that it is split by the natural inclusion $i : G \to \mathbb{U}(RG)$.” If it splits, then we have

$$\mathbb{U}(RG) = N \rtimes G,$$

where $N = \ker \phi$. Even, if it is known that G has a normal complement in $\mathbb{U}(RG)$, finding N is also an interesting problem. This problem has connections with other intriguing problems of group algebras, such as Fuchs' problem and Isomorphism problem.

It is known that if $G = H \times K$ is a group and F is a field, then G has a normal complement in $\mathbb{V}(FG)$ if and only if H and K have a normal complement in $\mathbb{V}(FH)$ and $\mathbb{V}(FK)$, respectively (see [29]). Further, note that for any group $G = H \rtimes K$, if G has a normal complement in $\mathbb{V}(FG)$, then K also has a normal complement in $\mathbb{V}(FK)$. Indeed, if $\phi : \mathbb{V}(FG) \to G$ is a map fixing elements of G, then for the natural projection $p : G \to K$ and the natural inclusion $i : \mathbb{V}(FK) \to \mathbb{V}(FG)$, $p \circ \phi \circ i : \mathbb{V}(FK) \to K$ is an epimorphism fixing elements of K.

In this direction, several results have been obtained for modular group algebras over finite p-groups. Let L_p denote the class of p-groups which have a normal

complement in the normalized unit group of group algebra FG, over the field F with p elements. Moran and Tench proved in 1977 that any finite abelian p-group lies in L_p (see [30]). They also obtained that for an odd prime p, any finite p-group of exponent p and nilpotency class 2 lies in L_p. Moreover, D_8 and $Q_8 \in L_2$, whereas D_{16} does not. In the next year, D.L. Johnson [31] gave some more results in favor of the normal complement problem.

In 1980, L. R. Ivory proved in [32] that dihedral, semi-dihedral and quaternion groups of order 16 and greater do not lie in L_2, hence proving that out of 14 groups of order 16, only 11 lie in L_2.

The existence of torsion-free normal complement of A_4 in $\mathbb{V}(\mathbb{Z}A_4)$ was shown in [33]. Further, in [34], it was established that a normal complement to A_4 in $\mathbb{V}(\mathbb{Z}A_4)$ must be torsion-free. A normal complement of S_4 in $\mathbb{V}(\mathbb{Z}S_4)$ was studied in [35]. In [36], the normal complement problem for central elementary-by-abelian p-groups over the field F_p was discussed.

Many results on the normal complement problem for modular group algebras of finite groups which are not p-groups can be found in [38, 39].

There are infinite examples of abelian semisimple group algebras in which the normal complement problem has an affirmative answer, see [29, Example 1]. In the same article, it was shown that normal complement does not exist in the case of semisimple group algebras of metacyclic groups of order $p_1 \cdot p_2$, where p_1 and p_2 are odd primes. Recently, the problem for semisimple group algebras of symmetric and alternating groups was also discussed in [37].

1.5 Organization of the Thesis

In this section, we give a brief outline of the present thesis. The research work has been divided into the following three chapters.

In Chapter 2, we examine the problem for modular group algebras of A_4, S_4, and D_{4m} over a field of characteristic 2. The existence of normal complement

is shown in case of A_4, S_4 and D_{12} in their respective unit groups of group algebra when the underlying field contains 2 elements. Further, we prove that A_4 does not have a normal complement in $\mathbb{U}(FA_4)$, when $|F| > 4$. It is also proved that D_{4m} does not have a normal complement in $\mathbb{U}(FD_{4m})$ for $m > 3$. Also, we have explicitly found a normal complement of the symmetric group S_4 in $\mathbb{V}(FS_4)$ over the field F containing 2 elements.

In Chapter 3, we find the generators of the unit group $\mathbb{V}(\mathbb{Z}_nC_2)$ and solve the normal complement problem in $\mathbb{V}(\mathbb{Z}_{p^k}C_2)$, where p is a prime number. We also provide a normal complement of E_m in $\mathbb{V}(\mathbb{Z}_{2^n}E_m)$. Further, we determine the structure of $\mathbb{V}(\mathbb{Z}_{p^n}F_{r,s})$ for an odd prime p.

In Chapter 4, we give the structure and generators of the unit group $\mathbb{U}(\mathbb{Z}_nC_3)$, where $\gcd(n, 3) = 1$. Also, we give structure of $\mathbb{U}(\mathbb{Z}_nT_m)$.

Chapter 2

Normal complement problem over a finite field of characteristic 2

Let F be a finite field of characteristic 2. In this chapter, we look into the existence of normal complement of G in $\mathbb{V}(FG)$, where G is either the alternating group A_4 or the dihedral group D_{4m} of order $4m$, for an odd integer $m \geq 3$. Also, we explicitly provide a normal complement of the symmetric group S_4 in $\mathbb{V}(FS_4)$ over the field F containing 2 elements.

Let A be a finite normal 2-group contained in G and F a finite field of characteristic 2. Then $\Gamma(A)$ is a nilpotent ideal of FG. Let $G = A \rtimes B$. In this case, the group homomorphism $a \mapsto 1,\ b \mapsto b,\ a \in A,\ b \in B$ from G to B induces an epimorphism ψ from the normalized unit group $\mathbb{V}(FG)$ to the normalized unit group $\mathbb{V}(FB)$ with kernel $1 + \Gamma(A)$.

$$\frac{\mathbb{V}(FG)}{(1+\Gamma(A))} \overset{\psi}{\cong} \mathbb{V}(FB).$$

If $i : \mathbb{V}(FB) \to \mathbb{V}(FG)$ denotes the natural inclusion, then $\psi \circ i$ is the identity map on $\mathbb{V}(FB)$ and hence the short exact sequence

$$\{1\} \to (1+\Gamma(A)) \to \mathbb{V}(FG) \to \mathbb{V}(FB) \to \{1\}$$

splits. Thus,

$$\mathbb{V}(FG) = (1+\Gamma(A)) \rtimes \mathbb{V}(FB).$$

Firstly, we investigate the existence of normal complement of A_4 in $\mathbb{V}(FA_4)$ over a finite field F of characteristic 2. Subsequently, we show that if F is a finite field of characteristic 2, then for any odd integer $m \geq 3$, D_{4m} does not have a normal complement in $\mathbb{V}(FD_{4m})$, except for $m = 3$ and $|F| = 2$. At the end, we explicitly give a normal complement of S_4 in $\mathbb{V}(FS_4)$ over the field F containing 2 elements.

2.1 Normal complement in $\mathbb{V}(FA_4)$

In this section, we study the existence of normal complement of A_4 in $\mathbb{V}(FA_4)$, over a finite field F of characteristic 2. We use the presentation $A_4 = \langle a, b : a^2 = b^3 = 1,\ (ab)^3 = 1\rangle$. Therefore, we can write $A_4 = \langle bab^2, b^2ab\rangle \rtimes \langle b\rangle \cong K_4 \rtimes C_3$, where K_4 is the Klein-4 group and C_3 is the cyclic group of order 3. We can observe that $\Gamma(K_4)^2$ is contained in the center of FA_4, which implies that $\Gamma(K_4)^3 = 0$ and the exponent of $1 + \Gamma(K_4)$ is 4. For $|F| = 2$, we have $\mathbb{V}(FC_3) = C_3$. Further, if $3 \mid (|F| - 1)$, then by [43], we have $FC_3 \cong F \oplus F \oplus F$ and hence $\mathbb{V}(FC_3) \cong F^\times \times F^\times$. The main theorem of this section is as follows:

Theorem 2.1.1. *Let F be a finite field of characteristic 2.*

(i) If $|F| = 2$ elements, then $1 + \omega(FA_4)\omega(FK_4)$ is a normal complement to A_4 in $\mathbb{V}(FA_4)$.

(ii) If $|F| = 2^t$ with $t > 2$ a multiple of 2 or 3, then A_4 does not have a normal complement in $\mathbb{V}(FA_4)$.

Proof. Let $A_4 = K_4 \rtimes C_3$. Since F is a finite field of characteristic 2, we have $\mathbb{V}(FA_4) = (1 + \Gamma(K_4)) \rtimes \mathbb{V}(FC_3)$.
(i) Suppose that $|F| = 2$. Let T denote a transversal of K_4 in A_4. Define a map $\theta : 1 + \Gamma(K_4) \to K_4$ by

$$x \mapsto \prod_{k \in K_4 \setminus \{1\}} k^{\epsilon(\alpha_k)},$$

where $x = 1 + \sum_{k \in K_4 \setminus \{1\}} \alpha_k(k-1)$ such that the support of α_k belongs to T. Note that for $t \in T$, we can write $t(k-1) = (k-1) + (t-1)(k-1)$ and therefore x can be written as $x = 1 + x_1 + x_2$, where $x_1 = \sum_{k \in K_4 \setminus \{1\}} \beta_k(k-1)$, $\beta_k \in F$ and x_2 is a F-linear combination of $(t-1)(k-1)$, where $t \in T$ and $k \in K_4$. It is clear that $\theta(x) = \prod_{k \in K_4 \setminus \{1\}} k^{\beta_k}$. If $y = 1 + y_1 + y_2$, where $y_1 \in \omega(FK_4)$ and $y_2 \in \omega(FA_4)\omega(FK_4)$, is another element of $1 + \Gamma(K_4)$, then $xy = 1 + x_1 + y_1 + z$, for some $z \in \omega(FA_4)\omega(FK_4)$. This implies that $\theta(xy) = \theta(x)\theta(y)$ and so θ is a group homomorphism. Now, if $x \in \ker\theta$, then $\theta(x) = \prod_{k \in K_4 \setminus \{1\}} k^{\beta_k} = 1$, and therefore $x \in 1 + \omega(FA_4)\omega(FK_4)$. Now, consider an element $1 + (h-1)(k_1 - 1) \in 1 + \omega(FA_4)\omega(FK_4)$, where $h = tk$, for

some $k \in K_4$ and $t \in T$. Then $1 + (tk-1)(k_1-1) = 1 + (t(k-1)+(t-1))(k_1-1)$ and hence $\theta(1+(h-1)(k_1-1)) = 1$. Hence, $\ker\theta = 1+\omega(FA_4)\omega(FK_4)$ and we can construct an exact sequence

$$\{1\} \to 1+\omega(FA_4)\omega(FK_4) \to 1+\Gamma(K_4) \to K_4 \to \{1\}.$$

If i denotes the natural embedding of K_4 into $1+\Gamma(K_4)$, then $\theta \circ i$ is an identity map on K_4. Therefore, $1+\Gamma(K_4) = (1+\omega(FA_4)\omega(FK_4)) \rtimes K_4$. Since the ideal $\omega(FA_4)\omega(FK_4)$ is contained in $\Gamma(K_4)$ and $\Gamma(K_4)$ is a nilpotent ideal of FA_4, it follows that $1+\omega(FA_4)\omega(FK_4)$ is a normal subgroup of $\mathbb{V}(FA_4)$. Hence, $\mathbb{V}(FA_4) = (1+\omega(FA_4)\omega(FK_4)) \rtimes A_4$.

(ii) Case (I). $|F| = 2^{2k},\ k > 1$. Assume that N is a normal complement of A_4 in $\mathbb{V}(FA_4)$. Let $\phi : \mathbb{V}(FA_4) \to A_4$ be an epimorphism fixing A_4 element-wise, such that $\ker\phi = N$. The exponent of $1+\Gamma(K_4)$ and $\mathbb{V}(FC_3)$ are 4 and $|F|-1$ respectively, which are coprime, so restriction of ϕ on $1+\Gamma(K_4)$ and $\mathbb{V}(FC_3)$ map to K_4 and C_3 respectively. Therefore, $|N \cap (1+\Gamma(K_4))| = \frac{|1+\Gamma(K_4)|}{4}$ and so

$$\begin{aligned} |N\backslash 1+\Gamma(K_4)| &= |N| - |N \cap (1+\Gamma(K_4))| \\ &= \frac{|1+\Gamma(K_4)|}{4}\left(\frac{(|F|-1)^2}{3} - 1\right). \end{aligned}$$

Further, $|N \cap \mathbb{V}(FC_3)| = \dfrac{(|F|-1)^2}{3}$.

One can compute that $C_{1+\Gamma(K_4)}(b) = \{1+\alpha(1+a+bab^2+b^2ab),\ \alpha \in FC_3\}$. Since $\{1,\ a+bab^2+b^2ab,\ b(1+a+bab^2+b^2ab),\ b^2(1+a+bab^2+b^2ab)\}$ is a set of class sums of A_4, we have that $C_{1+\Gamma(K_4)}(b)$ is contained in the center of FA_4.

Define

$$S = \{v \in \mathbb{V}(FC_3) \mid C_{1+\Gamma(K_4)}(b) = C_{1+\Gamma(K_4)}(v)\}.$$

Now, if $z \in C_{1+\Gamma(K_4)}(b)$, then $\phi(z) \in C_{K_4}(b) = \{1\}$, which implies that central subgroup $C_{1+\Gamma(K_4)}(b) \leq N$. Consider the set

$$W = \{s \cdot z \mid s \in S \cap N,\ z \in C_{1+\Gamma(K_4)}(b)\}.$$

We claim that the elements of W are disjoint conjugacy class representatives of $N\backslash 1+\Gamma(K_4)$ in $\mathbb{V}(FA_4)$. Indeed, if s_1z_1 and s_2z_2 are in the same conjugacy class, then the equation $v^{-1}s_1z_1v = s_2z_2$ can be written as $z_1(s_1z_1, v)z_2^{-1} = s_1^{-1}s_2$. It implies that $s_1 = s_2$, as $(1+\Gamma(K_4)) \cap \mathbb{V}(FC_3) = \{1\}$. Since the exponent of $1+\Gamma(K_4)$ is 4 and the exponent of $\mathbb{V}(FC_3)$ is $|F|-1$, it follows that

$$v^{-1}(s_1z_1)^{(|F|-1)}v = (s_2z_2)^{(|F|-1)}$$

implies $v^{-1}{z_1}^{-1}v = {z_2}^{-1}$ and therefore $z_1 = z_2$ as z_1 is a central element.

Next, choose $w \in \mathbb{V}(FC_3)$. Since w is an element of augmentation 1, we can write $w = 1+\alpha_1(b-1)+\alpha_2(b^2-1)$, where $\alpha_1, \alpha_2 \in F$. If either $\alpha_1 = 0$ or $\alpha_2 = 0$ (excluding the case when both $\alpha_1 = \alpha_2 = 0$), then $C_{1+\Gamma(K_4)}(w) = C_{1+\Gamma(K_4)}(b)$. Let us suppose that both α_1 and α_2 are non-zero. Then we can write $w = 1+\alpha_1((b-1)+i(b^2-1))$, where $i = {\alpha_1}^{-1}\alpha_2$. Since $3 \mid (2^{2k}-1)$, we have $I \subset F^\times$, where I denotes the set of cube roots of unity.

- We claim that there are exactly $3(|F|-2)$ invertible elements corresponding to the set I. It is enough to show that for each $i \in I$ there is a unique $\alpha_1 \in F^\times$ such that $w = 1+\alpha_1(b-1)+i(b^2-1)$ is not a unit. Observe that w is a unit if and only if $\phi_i(w) \neq 0$ for every $i \in I$, where ϕ_i is the representation of $\langle b\rangle$ mapping b to i. Since $\phi_1(w) = 1$, if ξ denotes a primitive 3^{rd} root of unity then w is a unit if and only if $\phi_\xi(w)\phi_{\xi^2}(w) \neq 0$. If $i = 1$ then $\phi_\xi(w)\phi_{\xi^2}(w) = (1+\alpha_1(\xi-1)+(\xi^2-1))(1+\alpha_1(\xi^2-1)+(\xi-1)) = (1+\alpha_1)^2$ and hence w is a unit if and only if $\alpha_1 \neq 1$. If $i = \xi$ then $\phi_\xi(w)\phi_{\xi^2}(w) = (1+\alpha_1(\xi-1)+\xi(\xi^2-1))(1+\ \alpha_1(\xi^2-1)+\xi(\xi-1)) = 1-\alpha_1\xi^2$ and hence w is a unit if and only if $\alpha_1 \neq \xi$. Finally, if $i = \xi^2$ then $\phi_\xi(w)\phi_{\xi^2}(w) = (1+\alpha_1(\xi-1)+\xi^2(\xi^2-1))(1+\alpha_1(\xi^2-1)+\xi^2(\xi-1)) = 1+\alpha_1\xi$ and hence w is a unit if and only if $\alpha_1 \neq \xi^2$.

- If $i \in F^\times\backslash I$, we can define

$$v = 1+\frac{i}{1+i+i^2}((b-1)+i(b^2-1))$$

Since $i \neq 1$, it implies that $v \in \mathbb{V}(FC_3)$. We can observe that $C_{1+\Gamma(K_4)}(v) = C_{1+\Gamma(K_4)}(vb)$ and therefore $C_{1+\Gamma(K_4)}(v) \leq C_{1+\Gamma(K_4)}(b)$, which further implies that $C_{1+\Gamma(K_4)}(v) = C_{1+\Gamma(K_4)}(b)$. Note that $C_{1+\Gamma(K_4)}(w) = C_{1+\Gamma(K_4)}(v)$, and hence $C_{1+\Gamma(K_4)}(w) = C_{1+\Gamma(K_4)}(b)$.

We can deduce that the cardinality of the set

$$\{y \in \mathbb{V}(FC_3) \mid C_{1+\Gamma(K_4)}(y) \neq C_{1+\Gamma(K_4)}(b)\}$$

is at most $3(|F| - 2)$. As $N \cap S = X^c$, where

$$X = \{x \in N \cap \mathbb{V}(FC_3) \mid C_{1+\Gamma(K_4)}(x) \neq C_{1+\Gamma(K_4)}(b)\}$$

and X^c is the complement of X in $N \cap \mathbb{V}(FC_3)$, we get

$$\begin{aligned} |N \cap S| &= |N \cap \mathbb{V}(FC_3)| - |X| \\ &\geq \frac{(|F|-1)^2}{3} - 3(|F| - 2). \end{aligned}$$

Note that the identity element does not belong to $N \cap S$. It follows that there are at least $\left(\frac{(|F|-1)^2}{3} - (3(|F| - 2) + 1)\right)$ elements in $S \cap N$. Thus,

$$|W| \geq \left(\frac{(|F|-1)^2}{3} - (3(|F| - 2) + 1)\right) |C_{1+\Gamma(K_4)}(b)|.$$

Since $z \in C_{1+\Gamma(K_4)}(b)$ is a central element, we have that $C_{\mathbb{V}(FA_4)}(sz) = C_{\mathbb{V}(FA_4)}(s)$ and $|Cl(s.z)| = |Cl(s)|$, where $s \in S$. Further, as $C_{\mathbb{V}(FA_4)}(s) = C_{1+\Gamma(K_4)}(s) \rtimes \mathbb{V}(FC_3)$, we have $|Cl(s)| = \frac{|1+\Gamma(K_4)|}{|C_{1+\Gamma(K_4)}(b)|}$. Therefore,

$$|N \backslash 1 + \Gamma(K_4)| \geq \left(\frac{(|F|-1)^2}{3} - (3(|F| - 2) + 1)\right) |1 + \Gamma(K_4)|.$$

Since $|F|^2 - 14|F| + 22 > 0$ for $|F| \geq 16$, we have that

$$|1 + \Gamma(K_4)| \left(\frac{(|F|-1)^2}{3} - (3(|F| - 2) + 1)\right) > \frac{|1 + \Gamma(K_4)|}{4} \left(\frac{(|F|-1)^2}{3} - 1\right).$$

This leads to a contradiction. Therefore, A_4 does not have a normal complement in

$\mathbb{V}(FA_4)$.

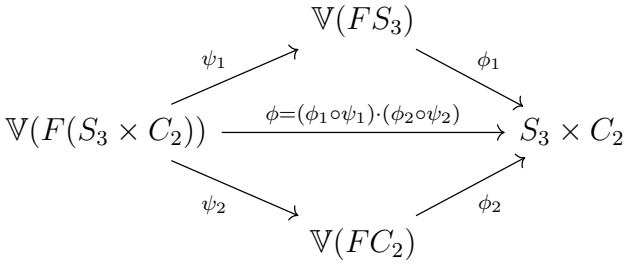
Case (II). $|F| = 2^{3r}, r \in \mathbb{N}$. By [29, Proposition 1], if A_4 has a normal complement in $\mathbb{V}(FA_4)$, then C_3 has a normal complement in $\mathbb{V}(FC_3)$. Further, it is known [29, Theorem 2] that C_3 has a normal complement in $\mathbb{V}(FC_3)$ if and only if $3 \parallel 2^{3rO_3} - 1$, where O_3 denotes the order of 2^{3r} modulo 3 and for $n, m \in \mathbb{Z}$, $n^i \parallel m$ means $n^i \mid m$, but $n^{i+1} \nmid m$. If $3r$ is even, then $O_3 = 1$ and $3^2 \mid (2^{3r} - 1)$. Further, when $3r$ is odd, $O_3 = 2$ and $3^2 \mid (2^{2(3r)} - 1)$. Therefore, A_4 does not have a normal complement in $\mathbb{V}(FA_4)$. □

2.2 Normal complement in $\mathbb{V}(FD_{4m})$

In this section, we study the existence of normal complement of D_{4m} in $\mathbb{V}(FD_{4m})$, for any odd integer $m \geq 3$. Consider $D_{12} = S_3 \times C_2$, where $S_3 = \langle a, b \mid a^3 = b^2 = 1,\ b^{-1}ab = a^{-1} \rangle$ and $C_2 = \{1, c\}$. The main result of this section is as follows:

Theorem 2.2.1. *Let F be a finite field of characteristic 2 and D_{4m} be the dihedral group of order $4m$, where m is an odd integer. Then, D_{4m} does not have a normal complement in $\mathbb{V}(FD_{4m})$, except for $m = 3$ and $|F| = 2$.*

Proof. Assume that $m = 3$ and F has 2 elements. It is known [29] that $\mathbb{V}(FS_3) = \langle bu \rangle \rtimes S_3$, where $u = 1 + (1 + b)a(1 + b)$. Also, we have $\mathbb{V}(FC_2) = C_2$. Let $\phi_1 : \mathbb{V}(FS_3) \to S_3$ and $\phi_2 : \mathbb{V}(FC_2) \to C_2$ be epimorphisms, fixing S_3 and C_2 and having kernels $\langle bu \rangle$ and $\{1\}$ respectively. Define ϕ as shown in the following diagram:



Here, ψ_1 is the canonical epimorphism, defined as $\psi_1\left(\sum_{s \in S_3} \sum_{x \in C_2} \alpha_{s \cdot x}(s \cdot x)\right) = \sum_{s \in S_3} \sum_{x \in C_2} \alpha_{s \cdot x} s$, where $\alpha_{s \cdot x} \in F$. Clearly, ψ_1 fixes S_3 element-wise. Similarly, we

can define $\psi_2\left(\sum_{s\in S_3}\sum_{x\in C_2}\alpha_{s\cdot x}(s\cdot x)\right)=\sum_{s\in S_3}\sum_{x\in C_2}\alpha_{s\cdot x}x$, fixing C_2. Hence, ϕ is an epimorphism, fixing $S_3\times C_2$ and the kernel of ϕ is the required normal complement, say N. Observe that

$$T=\langle u_i=s_ic+s_i+c \mid 1\leq i\leq 5,\ s_i \text{ is non-identity element of } S_3\rangle$$

is a subgroup of N. Further, observe that

$$\begin{aligned}
u_1 &= s_1c+s_1+c\\
u_1\cdot u_2 &= 1+s_1+s_2+s_1c+s_2c\\
u_1\cdot u_2\cdot u_3 &= s_1+s_2+s_3+s_1c+s_2c+s_3c+c\\
u_1\cdot u_2\cdot u_3\cdot u_4 &= 1+s_1+s_2+s_3+s_4++s_1c+s_2c+s_3c+s_4c\\
u_1\cdot u_2\cdot u_3\cdot u_4\cdot u_5 &= s_1+s_2+s_3+s_4+s_5+s_1c+s_2c+s_3c+s_4c+s_5c+c.
\end{aligned}$$

Since order of u_i is 2 and $u_i\cdot u_j=u_j\cdot u_i$, we have that $T=\langle u_1\rangle\times\langle u_2\rangle\times\langle u_3\rangle\times\langle u_4\rangle\times\langle u_5\rangle$. Note that $u=ac+a^2c+b+ab+a^2b\in N$ and the order of u is 2. As 1 or c does not belong to the support of u, it implies that $u\notin T$. Also, we have that $u\cdot u_i=u_i\cdot u$ for $1\leq i\leq 5$. Therefore, we can conclude that $T\times\langle u\rangle$ is an elemantary abelian 2-group of order 2^6. Further, we can deduce from [45, Theorem 1] that the order of N is 2^6. Therefore, $N=T\times\langle u\rangle$. If $|F|>2$, then S_3 does not have a normal complement in $\mathbb{V}(FS_3)$, which implies that D_{12} does not have a normal complement in $\mathbb{V}(FD_{12})$.

Next, assume that $m>3$. Since $D_{4m}\cong C_2\times D_{2m}$ and D_{2m} does not have a normal complement in $\mathbb{V}(FD_{2m})$ over any finite field of characteristic 2 [29], it implies that D_{4m} does not have a normal complement in $\mathbb{V}(FD_{4m})$. □

2.3 Normal complement in $\mathbb{V}(FS_4)$

In the last section, we construct a normal complement of S_4 in $\mathbb{V}(FS_4)$. We use the presentation $S_4=\langle x,y,a,b \mid x^2=y^2=a^3=b^2=1,\ a^{-1}xa=b^{-1}xb=xy,\ a^{-1}ya=x,\ b^{-1}yb=y,\ b^{-1}ab=a^{-1}\rangle$. Therefore, we can write $S_4=\langle x,y\rangle\rtimes\langle a,b\rangle\cong K_4\rtimes S_3$.

Proposition 2.3.1. *Let F be the field with 2 elements and let $S_3 = \langle a, b\rangle$ with $|a| = 3$ and $|b| = 2$. Let $u = 1 + (1 + b)a(1 + b)$. Then $(1 + \omega(FS_4)\,\omega(FK_4)) \rtimes \langle bu\rangle$ is a normal complement of S_4 in $\mathbb{V}(FS_4)$.*

Proof. We already know that $\mathbb{V}(FS_4) = (1 + \Gamma(K_4)) \rtimes \mathbb{V}(FS_3)$. Proceeding along the same line as Theorem 3.1.1(i), we get that $1 + \Gamma(K_4)$ is a split extension of K_4 by $1 + \omega(FS_4)\omega(FK_4)$. Therefore, $\mathbb{V}(FS_4) = (1 + \omega(FS_4)\omega(FK_4) \rtimes K_4) \rtimes (\langle bu\rangle \rtimes S_3)$. Since $\omega(FS_4)\omega(FK_4)$ is a nilpotent ideal, we have that $(1 + \omega(FS_4)\omega(FK_4))$ is a normal subgroup of $\mathbb{V}(FS_4)$. It follows that $\langle bu\rangle$ normalizes $(1 + \omega(FS_4)\omega(FK_4))$. Furthermore, since

$$x^{-1}(bu)x = bu(1 + (bu)^{-1}(a + b)(y - 1) + (bu)^{-1}(a^2 + ba)(xy - 1)) \text{ and}$$
$$y^{-1}(bu)y = bu(1 + (bu)^{-1}(ab + a^2)(x - 1) + (bu)^{-1}(a + ba)(xy - 1))$$

are in $(1+\omega(FS_4)\omega(FK_4)) \rtimes \langle bu\rangle$, it implies that K_4 normalizes $(1+\omega(FS_4)\omega(FK_4)) \rtimes \langle bu\rangle$. Hence, the result follows. □

Chapter 3

Unit group of group rings of groups of exponent 2 and 4 over $\mathbb{Z}_n$

Let C_t, E_m, and $F_{r,s}$ respectively denote the cyclic group of order t, the elementary abelian 2-group of order 2^m, and an abelian group of exponent 4 with order $2^r 4^s$. In this chapter, we find the generators of the unit group $\mathbb{V}(\mathbb{Z}_n C_2)$ and solve the normal complement problem in $\mathbb{V}(\mathbb{Z}_{p^k} C_2)$, where p is a prime number. We also provide a normal complement of E_m in $\mathbb{V}(\mathbb{Z}_{2^n} E_m)$. Further, we determine the structure of $\mathbb{V}(\mathbb{Z}_{p^n} F_{r,s})$ for an odd prime p.

This chapter is organized as follows: In section 1, we find the generators of $\mathbb{V}(\mathbb{Z}_n C_2)$ and solve the normal complement problem for this unit group in the case when $n = p^k$. In section 2, we find a normal complement of E_m in $\mathbb{V}(\mathbb{Z}_{2^n} E_m)$. Also, we give the necessary and sufficient conditions on prime p such that E_m has a normal complement in $\mathbb{V}(\mathbb{Z}_{p^n} E_m)$. In section 3, we compute the structure of $\mathbb{V}(\mathbb{Z}_{p^n} F_{r,s})$ for an odd prime p.

3.1 The structure of $\mathbb{V}(\mathbb{Z}_n C_2)$

In this section, we discuss the structure of the normalized unit group $\mathbb{V}(\mathbb{Z}_n C_2)$. For $n = p^k$, where p is an odd prime, it is known that $\mathbb{Z}_{p^k} C_2 \cong \mathbb{Z}_{p^k} \oplus \mathbb{Z}_{p^k}$ and so $\mathbb{V}(\mathbb{Z}_{p^k} C_2) \simeq \mathbb{U}(\mathbb{Z}_{p^k})$, which is cyclic. Here, we find a generator of this cyclic group. Further, we obtain the structure and provide the generators of $\mathbb{V}(\mathbb{Z}_n C_2)$ for any positive integer n. Finally, we solve the normal complement problem in $\mathbb{V}(\mathbb{Z}_{p^k} C_2)$ for a prime number p.

The following lemma plays a crucial role in proving this theorem.

Lemma 3.1.1. *Let p be an odd prime and $n > 1$. Then $\mathbb{Z}_{p^n}$ contains a primitive root of the form $2a - 1$ for some $a \in \mathbb{Z}_{p^n} \backslash \{0\}$.*

Proof. Let g be a primitive root modulo p. Then from [49, Theorem 2.39], we have $g+tp$ is a primitive root modulo p^n for $0 \leq t \leq p-1$ except for $t = \frac{1-g^{p-1}}{p}\left((p-1)g^{p-2}\right)^{-1}$, which can be understood to be reduced modulo p. Here $\left((p-1)g^{p-2}\right)^{-1}$ is the inverse of $(p-1)g^{p-2}$ modulo p.

Note that for $p=3$, 2 is a primitive root modulo 3 and $2+3t$ is a primitive root modulo 3^n for $t=0,1$. Thus, the primitive root $2+3(1)$ is of the form $2a-1$. Further, for $p \geq 5$, there exist two consecutive values of t, $0 \leq t \leq p-2$ such that $g+tp$ is a primitive root modulo p^n. Out of which, one of the primitive roots is of the form $2a-1$. □

The main theorem of this section is as follows:

Theorem 3.1.1. *Let $n = 2^k {p_1}^{m_1} {p_2}^{m_2} \dots {p_s}^{m_s}$, where $p_i's$ are distinct odd primes and $m_i > 1$ for $1 \leq i \leq s$. Then*

$$\mathbb{V}(\mathbb{Z}_n C_2) \simeq \begin{cases} \prod_{i=1}^{s} C_{\varphi({p_i}^{m_i})}; & k=0 \\ C_2 \times C_{2^{k-1}} \times \prod_{i=1}^{s} C_{\varphi({p_i}^{m_i})}; & k \geq 1 \end{cases}.$$

Proof. Suppose $C_2 = \langle x \rangle$. Note that $a+(1-a)x$, $a \in \mathbb{Z}_n$ is an element of $\mathbb{V}(\mathbb{Z}_n C_2)$ if and only if there exist $c+dx \in \mathbb{Z}_n C_2$ such that

$$\begin{bmatrix} a & 1-a \\ 1-a & a \end{bmatrix} \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

has a non-zero solution, i.e. if $a^2-(1-a)^2 = 2a-1 \in \mathbb{U}(\mathbb{Z}_n)$.
Case 1. Let $n = 2^k$. If $k=1$, then

$$\mathbb{V}(\mathbb{Z}_2 C_2) = \langle x \rangle \simeq C_2.$$

Next, assume that $k > 1$. For every $z \in \mathbb{Z}_{2^k}$, $2z-1 \in \mathbb{U}(\mathbb{Z}_{2^k})$, which implies that $|\mathbb{V}(\mathbb{Z}_{2^k} C_2)| = 2^k$. Since $3 \in \mathbb{U}(\mathbb{Z}_{2^k})$, we get that $2-x \in \mathbb{V}(\mathbb{Z}_{2^k} C_2)$. It can be easily

observed that $(2-x)^{2^{k-1}} = 1$ and

$$(2-x)^{2^{k-2}} = \begin{cases} 2-x; & k=2 \\ 1+2^{k-1}(2^{k-2}-1)-2^{k-1}(2^{k-2}-1)x; & k>2 \end{cases}$$

which is neither 1 nor x. Hence $2-x$ is an element of order 2^{k-1} and therefore

$$\mathbb{V}(\mathbb{Z}_{2^k}C_2) = \langle x \rangle \times \langle 2-x \rangle \simeq C_2 \times C_{2^{k-1}}. \tag{3.1}$$

Case 2. Let $n = {p_i}^{m_i}$, where p_i is an odd prime and $m_i > 1$. By Lemma 5.1.1, $\mathbb{Z}_{{p_i}^{m_i}}$ always has a primitive root of the form $2a_i - 1$ for some $a_i \in \mathbb{Z}_{{p_i}^{m_i}} \backslash \{0\}$. Therefore, the element $\alpha_i = a_i + (1-a_i)x$ belongs to $\mathbb{V}(\mathbb{Z}_{p_i^{m_i}}C_2)$. For any divisor d of $\varphi({p_i}^{m_i})$, $\alpha^d = A + Bx$, where $A = \frac{1+(2a_i-1)^d}{2}$. Note that $A = 1$ if and only if $d = \varphi({p_i}^{m_i})$. Therefore, $\mathbb{V}(\mathbb{Z}_{{p_i}^{m_i}}C_2) = \langle \alpha_i \rangle$.
Case 3. Let $n = 2^k {p_1}^{m_1} {p_2}^{m_2} \dots {p_s}^{m_s}$. Then

$$\mathbb{Z}_n \cong \mathbb{Z}_{2^k} \times \mathbb{Z}_{{p_1}^{m_1}} \times \cdots \times \mathbb{Z}_{{p_s}^{m_s}}$$

and therefore

$$\mathbb{Z}_n C_2 \cong \mathbb{Z}_{2^k}C_2 \times \mathbb{Z}_{{p_1}^{m_1}}C_2 \times \cdots \times \mathbb{Z}_{{p_s}^{m_s}}C_2.$$

Hence

$$\mathbb{V}(\mathbb{Z}_n C_2) \simeq \begin{cases} \prod_{i=1}^{s} \langle a_i + (1-a_i)x \rangle; & k=0 \\ \langle x \rangle \times \prod_{i=1}^{s} \langle a_i + (1-a_i)x \rangle; & k=1 \\ (\langle x \rangle \times \langle 2-x \rangle) \times \prod_{i=1}^{s} \langle a_i + (1-a_i)x \rangle; & k>1. \end{cases}$$

□

For $n = 2^k$, the existence of a normal complement can be seen from equation (5.1). Now, we will discuss the problem for $n = p^k$, where p is an odd prime. The following theorem proves the result:

Theorem 3.1.2. *Let p be an odd prime. Then C_2 has a normal complement in $\mathbb{V}(\mathbb{Z}_{p^m}C_2)$ if and only if $p \equiv 3 \mod 4$.*

Proof. Suppose C_2 has a normal complement N in $\mathbb{V}(\mathbb{Z}_{p^m}C_2)$. Therefore

$$|N| = \frac{p^{m-1}(p-1)}{2}.$$

Since $\mathbb{V}(\mathbb{Z}_{p^m}C_2)$ is cyclic, it follows that the cardinality of N must be odd and it is possible if and only if $p \equiv 3 \mod 4$. □

3.2 Normal complement in $\mathbb{V}(\mathbb{Z}_{p^n}E_m)$

In this section, we discuss the normal complement problem for the unit group $\mathbb{V}(\mathbb{Z}_{p^n}E_m)$, where E_m is the elementary abelian 2-group of order 2^m and $p \geq 2$. At first, we obtain the structure of the unit group of $\mathbb{V}(\mathbb{Z}_{2^n}E_m)$ and provide a normal complement of E_m. Later, a necessary and sufficient condition has been given for the existence of a normal complement in $\mathbb{V}(\mathbb{Z}_{p^n}E_m)$ for an odd prime p.

Theorem 3.2.1. *Let $E_m = \langle a_1\rangle \times \langle a_2\rangle \times \cdots \times \langle a_m\rangle$ be the elementary abelian 2-group of order 2^m. Then*

$$\mathbb{V}(\mathbb{Z}_{2^n}E_m) = E_m \times (\langle 2 - a_1\rangle \times \ker\phi_2 \times \cdots \times \ker\phi_m),$$

where $\phi_i : 1 + \Gamma(\langle a_i\rangle) \to \langle a_i\rangle$ is a group homomorphism.

Proof. Define a group homomorphism

$$\theta : E_m \to E_{m-1}$$

such that $\theta(a_i) = a_i$ for $1 \leq i \leq m-1$ and $\theta(a_m) = 1$. The above map can be extended linearly to an algebra homomorphism $\mathbb{Z}_{2^n}E_m \to \mathbb{Z}_{2^n}E_{m-1}$. Since the kernel of this map is a nil ideal, it implies that there exists an epimorphism $\theta' : \mathbb{V}(\mathbb{Z}_{2^n}E_m) \to \mathbb{V}(\mathbb{Z}_{2^n}E_{m-1})$ with kernel $1+\Gamma(\langle a_m\rangle)$. If $i : \mathbb{V}(\mathbb{Z}_{2^n}E_{m-1}) \to \mathbb{V}(\mathbb{Z}_{2^n}E_m)$ is the inclusion map, then $\theta \circ i = 1_{\mathbb{V}(\mathbb{Z}_{2^n}E_{m-1})}$. Therefore, $\mathbb{V}(\mathbb{Z}_{2^n}E_m) = (1 + \Gamma(\langle a_m\rangle)) \times \mathbb{V}(\mathbb{Z}_{2^n}E_{m-1})$.

Thus from equation (5.1), we have

$$\mathbb{V}(\mathbb{Z}_{2^n}E_m) = \prod_{i=2}^{m}(1+\Gamma(\langle a_i\rangle)) \times \langle a_1\rangle \times \langle 2-a_1\rangle.$$

Next, define a group homomorphism

$$\phi_i : 1+\Gamma(\langle a_i\rangle) \to \langle a_i\rangle$$

such that $\phi_i(1+\alpha(a_i-1)) = {a_i}^{\epsilon(\alpha)}$, where the support of α belongs to a transversal of $\langle a_i\rangle$ in E_m. If $\psi_i : \langle a_i\rangle \to 1+\Gamma(\langle a_i\rangle)$ is the inclusion map, then $\phi_i \circ \psi_i$ is the identity map on $\langle a_i\rangle$. Therefore, $1+\Gamma(\langle a_i\rangle) = \ker\phi_i \times \langle a_i\rangle$ and hence

$$\mathbb{V}(\mathbb{Z}_{2^n}E_m) = \prod_{i=2}^{m}(\ker\phi_i \times \langle a_i\rangle) \times \langle a_1\rangle \times \langle 2-a_1\rangle.$$

□

Theorem 3.2.2. *Let p be an odd prime. Then E_m has a normal complement in $\mathbb{V}(\mathbb{Z}_{p^n}E_m)$ if and only if $p \equiv 3 \mod 4$.*

Proof. It follows by Theorem 3.1.2 and [29, Theorem 1]. □

3.3 The structure of $\mathbb{V}(\mathbb{Z}_{p^n}F_{r,s})$

Let $F_{r,s}$ be the direct product of r cyclic groups of order 2 and s cyclic groups of order 4 with $s \geq 1$. In this section, we compute the structure of $\mathbb{V}(\mathbb{Z}_{p^n}F_{r,s})$ for an odd prime p.

Theorem 3.3.1. *For an odd prime p, we have*

$$\mathbb{V}(\mathbb{Z}_{p^n}F_{r,s}) \simeq \begin{cases} \left(C_{p^{n-1}} \times C_{p-1}\right)^{2^r 4^s}; & p \equiv 1 \mod 4 \\ \left(C_{p^{n-1}} \times C_{p-1}\right)^{2^{r+s}} \times \left(C^2_{p^{n-1}} \times C_{p^2-1}\right)^{2^{r+s-1}(2^s-1)}; & p \equiv 3 \mod 4 \end{cases}.$$

Proof. Suppose $F_{r,s} = \underbrace{C_2 \times C_2 \times \ldots \times C_2}_{r \text{ copies}} \times \underbrace{C_4 \times C_4 \times \ldots \times C_4}_{s \text{ copies}}$, where $C_4 = \langle g\rangle$.

Then $e = \frac{1+g^2}{2}$ is a central idempotent and therefore

$$\mathbb{Z}_{p^n}C_4 = \mathbb{Z}_{p^n}C_4(e) \oplus \mathbb{Z}_{p^n}C_4(1-e).$$

Note that

$$\mathbb{Z}_{p^n}C_4(e) = \{\, ae + bge \mid a, b \in \mathbb{Z}_{p^n} \,\}$$

and

$$\mathbb{Z}_{p^n}C_4(1-e) = \{\, a(1-e) + bg(1-e) \mid a, b \in \mathbb{Z}_{p^n} \,\}.$$

The mapping

$$\mathbb{Z}_{p^n}C_4(e) \to \frac{\mathbb{Z}_{p^n}[x]}{\langle x^2 - 1\rangle}$$

given by $ae + bge \mapsto a + b\bar{x}$ is a ring isomorphism. Similarly, the mapping

$$\mathbb{Z}_{p^n}C_4(1-e) \to \frac{\mathbb{Z}_{p^n}[x]}{\langle x^2 + 1\rangle}$$

given by $a(1-e) + bg(1-e) \mapsto a + b\bar{x}$ is also a ring isomorphism. Moreover,

$$\frac{\mathbb{Z}_{p^n}[x]}{\langle x^2 - 1\rangle} \cong \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^n}$$

and

$$\frac{\mathbb{Z}_{p^n}[x]}{\langle x^2 + 1\rangle} \cong \begin{cases} \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^n}; & p \equiv 1 \mod 4 \\ \mathbb{Z}_{p^n}[i]; & p \equiv 3 \mod 4 \end{cases},$$

where $i^2 = -1$. Therefore, we get that

$$\mathbb{Z}_{p^n}C_4 \cong \begin{cases} \mathbb{Z}_{p^n}^4; & p \equiv 1 \mod 4 \\ \mathbb{Z}_{p^n}^2 \times \mathbb{Z}_{p^n}[i]; & p \equiv 3 \mod 4 \end{cases}.$$

By following the same steps, we can prove that

$$\mathbb{Z}_{p^n}[i]C_4 \cong (\mathbb{Z}_{p^n}[i])^4.$$

The isomorphism $\mathbb{Z}_{p^n}(C_4 \times C_4) \cong (\mathbb{Z}_{p^n}C_4)C_4$ implies

$$\mathbb{Z}_{p^n}C_4^s \cong \begin{cases} \mathbb{Z}_{p^n}^{4^s}; & p \equiv 1 \mod 4 \\ \mathbb{Z}_{p^n}^{2^s} \times \mathbb{Z}_{p^n}[i]^{2^{s-1}(2^s-1)}; & p \equiv 3 \mod 4 \end{cases}.$$

Since $2^{-1} \in \mathbb{Z}_{p^n}C_4^s$, we have $\mathbb{Z}_{p^n}(C_4^s \times C_2) \cong (\mathbb{Z}_{p^n}C_4^s)C_2 \cong \mathbb{Z}_{p^n}C_4^s \times \mathbb{Z}_{p^n}C_4^s$. Thus, we get

$$\mathbb{Z}_{p^n}(C_2^r \times C_4^s) \cong \begin{cases} \mathbb{Z}_{p^n}^{2^r4^s}; & p \equiv 1 \mod 4 \\ \mathbb{Z}_{p^n}^{2^{r+s}} \times \mathbb{Z}_{p^n}[i]^{2^{r+s-1}(2^s-1)}; & p \equiv 3 \mod 4 \end{cases}.$$

It is known [50, Theorem 7] that $\mathbb{U}(\mathbb{Z}_{p^n}[i]) \simeq C_{p^{n-1}}^2 \times C_{p^2-1}$ and hence the result follows. □

Chapter 4

Unit group of group rings of groups of exponent 3 over $\mathbb{Z}_n$

In this chapter, we give the structure and generators of the unit group $\mathbb{U}(\mathbb{Z}_nC_3)$. Further, we provide the structure of $\mathbb{U}(\mathbb{Z}_nT_m)$, where T_m is the elementary abelian 3-group of order 3^m and $\gcd(n, 3) = 1$.

For a prime p, let F_p denote the field with p elements. Let $n \geq 2$ be an integer and $f(x)$ be a monic polynomial of degree m over $\mathbb{Z}_{p^n}$, which is irreducible modulo p. Then the quotient ring $\frac{\mathbb{Z}_{p^n}[x]}{\langle f(x)\rangle}$ is known as the Galois ring. If we take $\zeta = x + \langle f(x)\rangle$, then we have

$$\frac{\mathbb{Z}_{p^n}[x]}{\langle f(x)\rangle} = \mathbb{Z}_{p^n}[\zeta].$$

Any element of this ring is written as $(a_0 + a_1\zeta + \ldots + a_{m-1}\zeta^{m-1})$, for some $a_0, a_1, \ldots, a_{m-1} \in \mathbb{Z}_{p^n}$. For more details regarding Galois rings, one can refer to [51].

Now we discuss the criteria for the reducibility of polynomials in the ring $\mathbb{Z}_{p^n}[x]$, which is crucial to obtain the results in last section. In this direction, we first recall what a Hensel's lift is and then mention Hensel's lemma.

Let $g(x)$ be a monic polynomail over F_p. A monic polynomial $f(x)$ over $\mathbb{Z}_{p^n}[x]$ is called a Hensel lift of $g(x)$ if $\tilde{f}(x) = g(x)$, where $\tilde{f}(x)$ denotes the polynomial obtained by reducing the coefficients of the polynomial $f(x)$ modulo p, and there is a positive integer s not divisible by p such that $f(x) \mid (x^s - 1)$.

Hensel lemma [51, Lemma 13.7] states that if $f(x)$ is monic polynomial over $\mathbb{Z}_{p^n}$ and $\tilde{f}(x) = g_1(x)g_2(x)\ldots g_r(x)$, where $g_i(x)$ are pairwise coprime monic polynomials over F_p, then there exist pairwise co-prime monic polynomials over $\mathbb{Z}_{p^n}$ such that $f(x) = f_1(x)f_2(x)\ldots f_r(x)$ in $\mathbb{Z}_{p^n}[x]$ and $\tilde{f}_i = g_i,\ \forall\ 1 \leq i \leq r$. Thus if $f(x)$ is a Hensel lift of a polynomial $g(x)$ over F_p, which is reducible, then $f(x)$ is also

reducible in $\mathbb{Z}_{p^n}[x]$.

Let $n = 2^k \prod_{i=1}^{t} {p_i}^{r_i}$, where p_i, for any $1 \leq i \leq m$, is an odd prime except 3. Then $\mathbb{Z}_n \cong \mathbb{Z}_{2^k} \times \prod_{i=1}^{t} \mathbb{Z}_{{p_i}^{r_i}}$, and $\mathbb{Z}_n C_3 \cong \mathbb{Z}_{2^k} C_3 \times \prod_{i=1}^{t} \mathbb{Z}_{{p_i}^{r_i}} C_3$. The restriction to the unit groups yields

$$\mathbb{U}(\mathbb{Z}_n C_3) \cong \mathbb{U}(\mathbb{Z}_{2^k} C_3) \times \prod_{i=1}^{t} \mathbb{U}(\mathbb{Z}_{{p_i}^{r_i}} C_3).$$

Therefore, it is sufficient to study the unit group $\mathbb{U}(\mathbb{Z}_{p^n} C_3)$, where p is a prime.

This chapter is organized as follows: In the first and second sections, we discuss the generators of $\mathbb{U}(\mathbb{Z}_{p^n} C_3)$, when p is the even and an odd prime, respectively. In the last section, we provide the structure of $\mathbb{U}(\mathbb{Z}_{p^n} T_m)$, where $T_m = \underbrace{C_3 \times C_3 \times \ldots \times C_3}_{m \text{ copies}}$.

4.1 The structure of $\mathbb{U}(\mathbb{Z}_{2^n} C_3)$

In this section, we study the structure and generators of the unit group of $\mathbb{Z}_{2^n} C_3$. In this direction, the following theorem determines the structure of the unit group.

Theorem 4.1.1. $\mathbb{U}(\mathbb{Z}_{2^n} C_3) \simeq \begin{cases} {C_2}^{(3)} \times C_3, & n = 2 \\ {C_2}^{(2)} \times {C_{2^{n-2}}}^{(2)} \times C_{2^{n-1}} \times C_3, & n > 2. \end{cases}$

Proof. Assume that $C_3 = \langle g \rangle$. Then $e = \frac{(1+g+g^2)}{3}$ is a central idempotent of $\mathbb{Z}_{2^n} C_3$ and therefore,

$$\mathbb{Z}_{2^n} C_3 \cong \mathbb{Z}_{2^n} C_3 e \oplus \mathbb{Z}_{2^n} C_3 (1 - e), \tag{4.1}$$

where

$$\mathbb{Z}_{2^n} C_3 e = \{\alpha e \mid \alpha \in \mathbb{Z}_{2^n}\}$$

and

$$\mathbb{Z}_{2^n} C_3 (1 - e) = \{\alpha_0 (1 - e) + \alpha_1 g (1 - e) \mid \alpha_0, \alpha_1 \in \mathbb{Z}_{2^n}\}.$$

The mapping

$$\mathbb{Z}_{2^n}C_3e \to \mathbb{Z}_{2^n}$$

given by $\alpha e \mapsto \alpha$ is a ring isomorphism. Similarly, the mapping

$$\mathbb{Z}_{2^n}C_3(1-e) \to \frac{\mathbb{Z}_{2^n}[x]}{\langle 1+x+x^2\rangle}$$

given by $\alpha_0(1-e)+\alpha_1 g(1-e) \mapsto \alpha_0+\alpha_1 x+\left\langle 1+x+x^2\right\rangle$ is also a ring isomorphism. If ω denotes the element $x+\left\langle 1+x+x^2\right\rangle$, then $\dfrac{\mathbb{Z}_{2^n}[x]}{\langle 1+x+x^2\rangle} = \mathbb{Z}_{2^n}[\omega]$. Let φ denote the ring isomorphism obtained by the linear extension of map $g \mapsto (1,\omega)$. Then the isomorphism (6.1) becomes

$$\mathbb{Z}_{2^n}C_3 \overset{\varphi}{\cong} \mathbb{Z}_{2^n} \oplus \mathbb{Z}_{2^n}[\omega], \tag{4.2}$$

Thus $\varphi(\alpha_0+\alpha_1 g+\alpha_2 g^2) = (\alpha_0+\alpha_1+\alpha_2, \alpha_0+\alpha_1\omega+\alpha_2\omega^2)$. Now the following two lemmas provide the order and structure of $\mathbb{U}(\mathbb{Z}_{2^n}[\omega])$.

Lemma 4.1.1. *Let $n \in \mathbb{N}$. Then, $|\mathbb{U}(\mathbb{Z}_{2^n}[\omega])| = 3\cdot 4^{n-1}$.*

Proof. Let $(a+b\omega) \in \mathbb{U}(\mathbb{Z}_{2^n}[\omega])$. It implies that there exists a unique $(c+d\omega) \in \mathbb{Z}_{2^n}[\omega]$ such that $(a+b\omega)(c+d\omega) = 1$. Now the system of equations $ac-bd = 1$ and $bc+(a-b)d = 0$ have a unique solution if and only if $(a^2-ab+b^2) \in \mathbb{U}(\mathbb{Z}_{2^n})$. Since $\mathbb{U}(\mathbb{Z}_{2^n}) = \{\bar{1}, \bar{3}, \ldots, \overline{(2^n-1)}\}$, $(a^2-ab+b^2) \in \mathbb{U}(\mathbb{Z}_{2^n})$ if and only if at least one of a and b is of the form $\overline{(2k+1)}$ for some $0 \le k \le (2^{n-1}-1)$. The number of possible $(a,b) \in \mathbb{Z}_{2^n}^2$ such that $a+b\omega$ is a unit, is $3(2^{n-1})(2^{n-1}) = 3\cdot 4^{n-1}$. □

Lemma 4.1.2. $\mathbb{U}(\mathbb{Z}_{2^n}[\omega]) \simeq C_2 \times C_{2^{n-2}} \times C_{2^{n-1}} \times C_3$.

Proof. When $n = 2$, $\mathbb{U}(\mathbb{Z}_4[\omega]) = \langle 3\rangle \times \langle (1+2\omega)\rangle \times \langle \omega\rangle \simeq C_2 \times C_2 \times C_3$. Further, when $n > 2$, we consider the subgroups $H_1 = \langle (2^{n-1}-1)\rangle$, $H_2 = \langle (1+4\omega)\rangle$ and $H_3 = \langle (1+2\omega)\rangle$ of $\mathbb{U}(\mathbb{Z}_{2^n}[\omega])$. We claim that the product of the groups H_1, H_2 and H_3 is direct and is of order 4^{n-1}.

In order to prove the claim, we first note that $(1+4\omega)^{2^{n-2}} = 1$ and $(1+4\omega)^{2^{n-3}} = (1+2^{n-1}\omega)$. Therefore, $H_2 \cong C_{2^{n-2}}$. Similarly, $(1+2\omega)^{2^{n-1}} = 1$ and

$(1+2\omega)^{2^{n-2}} = (1+2^{n-1})$ imply that $H_3 \cong C_{2^{n-1}}$. Further, since $(2^{n-1}-1)$ is of order 2, $H_1 \cong C_2$.

Now we prove that $H_i \cap H_j = \{1\}$ for distinct $i, j \in \{1,2,3\}$. Since the element of order 2 in H_2 and H_3 is $(1+2^{n-1}\omega)$ and $(1+2^{n-1})$, respectively; H_1 intersects H_2 and H_3 trivially.

Finally, we consider $H_2 \cap H_3$. Since $(1+2\omega)^2 = -3$, the unique subgroup of H_3 of order 2^{n-2} is generated by -3. Note that if i is such that $\gcd(i, 2^{n-2}) = 1$, then $(1+4\omega)^i \notin H_3$. Otherwise, for the integer j such that $ji \equiv 1 \mod (2^{n-2})$, $(1+4\omega)^{ij} = (1+4w) \in H_3$. Therefore, $(1+4\omega) = 3^b$, for some $1 \leq b \leq 2^{n-2}$, which is not possible.

Further, since the element $(1+2^{n-1}\omega)$ of order 2 in H_2 is not the same as the element $(-3)^{2^{n-3}}$ of order 2 in H_3, it follows that $(1+4w)^t \notin H_3$, for any $t = 2^r$ with $1 \leq r \leq n-3$. Now if $(1+4\omega)^{2^r i} \in H_3$ for some i and r as defined above, then since $(1+4\omega)^i$ is a generator of H_2, the above argument supplies a contradiction. Thus H_2 and H_3 are disjoint.

We denote $H_i \times H_j$ by $H_{i,j}$ and prove our claim as follows:

- Assume that $H_1 \cap H_{2,3} \neq \{1\}$. Then $(2^{n-1}-1) \in H_1 \cap H_{2,3}$. Since the only elements of order 2 in $H_{2,3}$ are $(1+2^{n-1})$, $(1+2^{n-1}\omega)$ and $(1+2^{n-1}+2^{n-1}\omega)$, it is not possible.

- If $y \in H_3 \cap H_{1,2}$, then $y^2 \in H_3 \cap H_2 = \{1\}$. If $y \neq 1$, then $y = (1+2^{n-1}\omega) \in H_3$. But it is not possible as y is different from $(2^{n-1}-1), (2^{n-1}+1)$ and -1, which are the only elements of order 2 in $H_{1,2}$.

- Similarly, if $z \in H_2 \cap H_{1,3}$, then $z^2 \in H_2 \cap H_3 = \{1\}$. Now if we assume that $z = (1+2^{n-1}) \in H_2$, then since it is different from the elements $(2^{n-1}-1), (2^{n-1}\omega+1)$ and $(2^{n-1}-2^{n-1}\omega-1)$ of order 2 in $H_{1,3}$, we arrive at a contradiction. Thus $z = 1$.

Hence $|H_1 \times H_2 \times H_3| = 4^{n-1}$ and $\mathbb{U}(\mathbb{Z}_{2^n}[\omega]) \simeq C_2 \times C_{2^{n-2}} \times C_{2^{n-1}} \times C_3$, where $C_3 \simeq \langle \omega \rangle$. □

By restricting the isomorphism in (6.2) to the unit groups, we obtain

$$\mathbb{U}(\mathbb{Z}_{2^n}C_3) \simeq \mathbb{U}(\mathbb{Z}_{2^n}) \times \mathbb{U}(\mathbb{Z}_{2^n}[\omega]). \tag{4.3}$$

Since $\mathbb{U}(\mathbb{Z}_{2^n}) = C_2 \times C_{2^{n-2}}$, the result now follows from Lemma 4.1.2. □

Our next aim is to describe a set of generators of the unit group of $\mathbb{Z}_{2^n}C_3$. Since $\mathbb{U}(\mathbb{Z}_{2^n}C_3) = \mathbb{U}(\mathbb{Z}_{2^n}) \times \mathbb{V}(\mathbb{Z}_{2^n}C_3)$ and

$$\mathbb{U}(\mathbb{Z}_{2^n}) = \begin{cases} \langle 3 \rangle \simeq C_2, & n = 2 \\ \langle -1 \rangle \times \langle 5 \rangle \cong C_2 \times C_{2^{n-2}}, & n > 2, \end{cases}$$

it follows from (6.3) that $\mathbb{V}(\mathbb{Z}_{2^n}C_3) \simeq \mathbb{U}(\mathbb{Z}_{2^n}[w])$ and hence $|\mathbb{V}(\mathbb{Z}_{2^n}C_3)| = 3 \cdot 4^{n-1}$. Now in the following theorem, we give the generators for $\mathbb{V}(\mathbb{Z}_{2^n}C_3)$.

Theorem 4.1.2. *Let $C_3 = \langle g \rangle$. Then*

(i) $\mathbb{V}(\mathbb{Z}_4C_3) = \langle 1 + 2g \rangle \times \langle 3 + 2g \rangle \times \langle g \rangle$.

(ii) For $n > 2$, we have $\mathbb{V}(\mathbb{Z}_{2^n}C_3) = \langle s_1 \rangle \times \langle s_2 \rangle \times \langle s_3 \rangle \times \langle g \rangle$, where $s_1 = 1 + 2 \cdot 3^{-1}(g + g^2 - 2)$, $s_2 = 3^{-1}(1 + 2g)$, and $s_3 = 5^{-1}(1 + 4g)$.

Proof. Since *(i)* is trivial, we prove *(ii)*. We have $\varphi(s_2) = (1, 3^{-1}(1 + 2\omega))$ and $\varphi(s_3) = (1, 5^{-1}(1 + 4\omega))$. Here $\langle (1, 3^{-1}(1 + 2\omega)) \rangle \simeq C_{2^{n-1}}$ and $\langle (1, 5^{-1}(1 + 4\omega)) \rangle \simeq C_{2^{n-2}}$. Similarly, since $\varphi(s_1) = (1, -1)$, s_1 is of order 2. Now, to prove that these subgroups have trivial intersection, we proceed as in Lemma 4.1.2. □

4.2 The structure of $\mathbb{U}(\mathbb{Z}_{p^n}C_3)$

In this section, we study the unit group $\mathbb{U}(\mathbb{Z}_{p^n}C_3)$, when $p > 3$ is a prime. In the following, we give the structure and generators of the unit group.

Theorem 4.2.1. *Let p be a prime such that $p \equiv 1 \mod 3$. Then*

$$\mathbb{U}(\mathbb{Z}_{p^n}C_3) \simeq {C_{p^{n-1}}}^{(3)} \times {C_{p-1}}^{(3)}.$$

Proof. Recall that

$$\mathbb{Z}_{p^n}C_3 \cong \mathbb{Z}_{p^n} \oplus \frac{\mathbb{Z}_{p^n}[x]}{\langle(1+x+x^2)\rangle}.$$

Since $\gcd(3,p) = 1$ and $(1+x+x^2) \mid (x^3-1)$, it follows that the polynomial $(1+x+x^2)$ in $\mathbb{Z}_{p^n}[x]$ is the Hensel's lift of the polynomial $(1+x+x^2) \in F_p[x]$. Since $3 \mid (p-1)$, all the roots of $(1+x+x^2)$ lie in F_p. Therefore, Hensel's Lemma implies that $(1+x+x^2)$ is reducible over $\mathbb{Z}_{p^n}$ also. Thus

$$(1+x+x^2) = (x-\alpha)(x-\alpha^2) \in \mathbb{Z}_{p^n}[x],$$

where $1+\alpha+\alpha^2 = 0$. Now observe that $\langle(x-\alpha)\rangle$ and $\langle(x-\alpha^2)\rangle$ are comaximal. Indeed, since $(1+2\alpha)(3^{-1}(1+2\alpha^2)) = 1$, $(1+2\alpha)$ is a unit in $\mathbb{Z}_{p^n}$ and hence we have

$$1 = (1+2\alpha)^{-1}(x-\alpha^2) - (1+2\alpha)^{-1}(x-\alpha).$$

Therefore,

$$\frac{\mathbb{Z}_{p^n}[x]}{\langle(1+x+x^2)\rangle} = \frac{\mathbb{Z}_{p^n}[x]}{\langle(x-\alpha)\rangle} \oplus \frac{\mathbb{Z}_{p^n}[x]}{\langle(x-\alpha^2)\rangle}$$

and so

$$\mathbb{Z}_{p^n}C_3 \overset{\rho}{\cong} \mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}. \tag{4.4}$$

Now the restriction to the unit group gives the structure. □

Since $\mathbb{U}(\mathbb{Z}_{p^n}C_3) = \mathbb{U}(\mathbb{Z}_{p^n}) \times \mathbb{V}(\mathbb{Z}_{p^n}C_3)$, we now obtain generators of the normalized unit group $\mathbb{V}(\mathbb{Z}_{p^n}C_3)$. In this direction, we first give the following lemma:

Lemma 4.2.1. *Let R be a ring with units $\{r_i \mid 1 \le i \le m\}$ of finite order. Let n be an integer such that $char(R) \nmid n$. If $G = \langle g\rangle$ is the cyclic group of order n, then for any $1 \le i \le m$, the symmetric elements $x_i = r_i + \Big(\frac{1-r_i}{n}\Big)\hat{g}$ of RG, where $\hat{g} = \sum_{i=1}^{n} g^i$, are of order $o(r_i)$. Further, if $(o(r_i), o(r_j)) = 1 \ \forall\ 1 \le i \ne j \le m$, then $\prod_{i=1}^{m}\langle x_i\rangle$ is a subgroup of order $\prod_{i=1}^{m} o(r_i)$ of $\mathbb{U}(RG)$.*

Proof. Consider the element $y_{\alpha_i} = 1 + \alpha_i(\hat{g} - n) \in RG$, where $\alpha_i \in R$. Since $\rho(\hat{g}) = (n, 0, 0 \ldots, 0)$, $\rho(y_{\alpha_i}) = \Big(1, (1-n\alpha_i), \ldots, (1-n\alpha_i)\Big)$ and so $o(y_{\alpha_i}) = o(1-n\alpha_i)$.

Therefore, if $\alpha_i = \dfrac{(1-r_i)}{n}$, then the element $y_{\alpha_i} = \left(r_i + \dfrac{(1-r_i)}{n}\hat{g}\right)$ is a symmetric unit of order $o(r_i)$. □

Now since $\mathbb{U}(\mathbb{Z}_{p^n}) \simeq C_{p^{n-1}} \times C_{p-1}$, assume that $\mathbb{U}(\mathbb{Z}_{p^n}) = \langle 1+p \rangle \times \langle \eta \rangle$, where $o(\eta) = (p-1)$. Then we have:

Proposition 4.2.1. *Let $C_3 = \langle g \rangle$. Then the elements $t_1 = \left(1 + \frac{p}{3} + \left(\frac{p\alpha}{3}\right)g + \left(\frac{p\alpha^2}{3}\right)g^2\right)$ and $t_2 = \left(1+p-\frac{p\hat{g}}{3}\right)$ of $\mathbb{Z}_{p^n}C_3$ are of order p^{n-1}. Further, the elements $t_3 = \left(\eta+\frac{1-\eta}{3}\hat{g}\right)$ and $t_4 = \big(1 + a(g-1) + b(g^2-1)\big)$, where $a = \frac{(1-\eta)(1-\eta\alpha)}{3}$ and $b = \frac{(1-\eta)(1-\eta\alpha^2)}{3}$, are of order $(p-1)$ and*

$$\mathbb{V}\left(\mathbb{Z}_{p^n}C_3\right) = \langle t_1 \rangle \times \langle t_2 \rangle \times \langle t_3 \rangle \times \langle t_4 \rangle .$$

Proof. It follows from the last lemma that the order of t_2 and t_3 is p^{n-1} and $p-1$, respectively. Further, note that the isomorphism in (4.1) gives $g \overset{\rho}{\mapsto} (1, \alpha, \alpha^2)$. Since $\rho(t_1) = (1, 1, 1+p)$, $\rho(t_2) = (1, 1+p, 1+p)$, $\rho(t_3) = (1, \eta, \eta)$, and $\rho(t_4) = (1, \eta, \eta^2)$, the result follows. □

Next, we discuss the case for the remaining primes.

Theorem 4.2.2. *Let p be an odd prime such that $p \equiv 2 \mod 3$. Then we have the following:*

(i) Let $k_1 = (1+p)^{-1}(1+pg)$ and $k_2 = (1-2p)^{-1}(1-p(g+g^2))$. Then the subgroups $K_1 = \langle k_1 \rangle$ and $K_2 = \langle k_2 \rangle$ of $\mathbb{V}(\mathbb{Z}_{p^n}C_3)$ are of order p^{n-1} and are disjoint.

(ii) If $p^2 \not\equiv 1 \mod 9$ and a satisfies $(-3)^{\frac{p^2-1}{12}}(x)^{\frac{p^2-1}{6}} \equiv -1 \mod p^n$, then $\mathbb{V}(\mathbb{Z}_{p^n}C_3) = K_1 \times K_2 \times K_3$, where K_3 is a cyclic group of order (p^2-1) generated by $k_3 g$, where

$$k_3 = (1 + (3^{-1}+a)(g-1) + (3^{-1}-a)(g^2-1)).$$

Proof. (i) If $p \equiv 2 \mod 3$, then 3 does not divide $\phi(p^n)$ and so, $\mathbb{Z}_{p^n}^{\times}$ does not contain a cube root of unity. It follows that $(1+x+x^2)$ is irreducible in $\mathbb{Z}_{p^n}[x]$ and hence $\frac{\mathbb{Z}_{p^n}[x]}{\langle(1+x+x^2)\rangle} = \mathbb{Z}_{p^n}[\omega]$, where $\omega = x + \langle(1+x+x^2)\rangle$. Therefore,

$$\mathbb{Z}_{p^n}C_3 \overset{\psi}{\cong} \mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}[\omega]. \tag{4.5}$$

Clearly, $\psi(k_1) = (1, (1+p)^{-1}(1+p\omega))$ and $\psi(k_2) = (1, (1-2p)^{-1}(1+p))$. Since the order of the elements $(1-2p)^{-1}(1+p)$ and $(1+p)^{-1}(1+p\omega)$ of $\mathbb{Z}_{p^n}[\omega]$ is p^{n-1}, it follows that $K_1 \cong K_2 \cong C_{p^{n-1}}$.

Now we prove that $K_1 \cap K_2 = \{1\}$. Clearly,

$$(1+p)^{-1}(1+p\omega) \notin \langle(1-2p)^{-1}(1+p)\rangle.$$

It implies that

$$\big((1+p)^{-1}(1+p\omega)\big)^i \notin \langle(1-2p)^{-1}(1+p)\rangle,$$

where $\gcd(i, p^{n-1}) = 1$. Observe that $\langle(1-2p^{n-1})^{-1}(1+p^{n-1})\rangle$ is the unique subgroup of order p in $\langle(1-2p)^{-1}(1+p)\rangle$. Since

$$\big((1+p)^{-1}(1+p\omega)\big)^{p^{n-2}} = ((1+p^{n-1})^{-1})(1+p^{n-1}\omega),$$

which is not in $\langle(1-2p^{n-1})^{-1}(1+p^{n-1})\rangle$, therefore

$$\big((1+p)^{-1}(1+p\omega)\big)^{p^k} \notin \langle(1-2p)^{-1}(1+p)\rangle$$

for $1 \leq k \leq n-2$. Further, assume that for any i with $\gcd(i, p^k) = 1$,

$$\big((1+p)^{-1}(1+p\omega)\big)^{p^k i} \in \langle(1-2p)^{-1}(1+p)\rangle.$$

Then since $\big((1+p)^{-1}(1+p\omega)\big)^i$ generates $\langle\big((1+p)^{-1}(1+p\omega)\big)\rangle$, we arrive at a contradiction. Now the result follows.

(ii) In order to prove this, we first give the following lemma which is crucial to the upcoming discussion as well

Lemma 4.2.2. *Let p be an odd prime such that $p \equiv 2 \mod (3)$. Then*

$$|\mathbb{V}(\mathbb{Z}_{p^n}C_3)| = p^{2n-2}(p^2-1). \tag{4.6}$$

Proof. We first observe that if $x = (a + b\omega) \in \mathbb{U}(\mathbb{Z}_{p^n}[\omega])$, then both a and b can not be divisible by p; because otherwise, $p^{n-1}x = 0$ implies $p^{n-1} = 0$, which is a contradiction. Therefore, at least one of a and b must not be divisible by p and so we have at most

$$p^{n-1}p^{n-1}(p-1) + p^{n-1}p^{n-1}(p-1) + p^{n-1}(p-1)p^{n-1}(p-1) = p^{2n-2}(p^2-1)$$

choices for x. Now we obtain the inverse of any such element. Clearly, when $a = b, x^{-1} = \dfrac{-\omega}{a}$. Further, when $a \neq b$, then proceeding as in Lemma 4.1.1, we obtain that $(a + b\omega) \in \mathbb{U}(\mathbb{Z}_{p^n}[\omega])$ if and only if $(a^2 + b^2 - ab) \in \mathbb{U}(\mathbb{Z}_{p^n})$. Here note that if $p \mid (a^2 + b^2 - ab)$ then $p \mid (a^3 + b^3)$; which is not possible as both a and b are not simultaneously divisible by p. Thus $(a^2 + b^2 - ab)$ is a unit in $\mathbb{Z}_{p^n}$ and hence x is invertible. Now since $|\mathbb{V}(\mathbb{Z}_{p^n}C_3)| = |\mathbb{Z}_{p^n}[\omega]|$, the claim is established. □

Now we proceed to prove the main result. If $(-3)^{\frac{p^2-1}{12}}(a)^{\frac{p^2-1}{6}} \equiv -1 \mod p^n$, then

$$(a(1+2\omega))^{\frac{p^2-1}{6}} \equiv -1 \mod p^n$$

and therefore $a(1 + 2\omega)$ is an element of order $\frac{(p^2-1)}{3}$ in $\mathbb{Z}_{p^n}[\omega]$. Since

$$\psi(k_3) = (1, a(1+2\omega))$$

and $\gcd\left(3, \frac{(p^2-1)}{3}\right) = 1$, we get that the order of $k_3 g$ is $(p^2 - 1)$. Using 4.2.2 and *(i)*, we get the desired structure. □

Next, we give the generators of the unit group when $p = 5$. For that, we make use of the following lemma.

Lemma 4.2.3. *The congruence $9x^4 \equiv -1 \mod 5^n$ has a solution.*

Proof. It is known that the congruence

$$9x^4 \equiv -1 \mod 5 \tag{4.7}$$

has 4 solutions. Thus using Hensel's lemma, we can lift these solutions modulo 5^n. □

Corollary 4.2.1. $\mathbb{U}(\mathbb{Z}_{5^n}C_3) = \langle 6^{-1}(1+5g)\rangle \times \langle (-9)^{-1}\langle 1-5(g+g^2)\rangle \times \langle 1+(3^{-1}+a)(g-1)+(3^{-1}-a)(g^2-1)\rangle \times \langle g\rangle$, *where* a *is a solution of the congruence* $9x^4 \equiv -1 \mod 5^n$.

Finally, in the following, we discuss the unit group of $\mathbb{Z}_{p^n}C_3$, when $p \equiv 2 \mod (3)$ and $p^2 \equiv 1 \mod (9)$. Clearly, any such prime is of form $(9l+8)$. It follows from Theorem 4.2.2 that the p-Sylow subgroup of $\mathbb{V}(\mathbb{Z}_{p^n}C_3)$, say A, which is of order $p^{2(n-1)}$ is generated by k_1 and k_2. Further, Lemma 4.2.2 implies that $\mathbb{V}(\mathbb{Z}_{p^n}C_3) = A \times B = \langle k_1\rangle \times \langle k_2\rangle \times B$, where B is an abelian group of order (p^2-1). Now we give a lemma which is crucial to determine the structure of the unit group in the upcoming cases:

Lemma 4.2.4. *Let* p *be a prime such that* $p \equiv 2 \mod (3)$. *Then the* 2- *and the* 3-*subgroup of* $\mathbb{V}(\mathbb{Z}_{p^n}C_3)$ *are cyclic.*

Proof. In order to establish the claim, we prove that $\mathbb{V}(\mathbb{Z}_{p^n}C_3)$ contains only one element of order 2. Recall that $\mathbb{V}(\mathbb{Z}_{p^n}C_3) \cong \mathbb{Z}_{p^n}[w]$. If $x = (a+bw)$ is an element of $\mathbb{Z}_{p^n}[w]$ of order 2, then $x^2 = 1$ gives $a^2 - b^2 = 1$ and $b(2a-b) = 0$; which in turn implies that $p^n \mid b(2a-b)$. If $p \nmid b$, then $p^n \mid (2a-b)$ and hence $b = 2a + p^n k$. Thus $a^2 - b^2 = -3a^2 = 1$ in $\mathbb{Z}_{p^n}[w]$. Since -3 is not a quadratic residue in $\mathbb{Z}_p$, the above situation can not arise.

Therefore, $p^i \mid b$, for some $i \geq 1$ and so $p^{n-i} \mid (2a-b)$. If $n-i > 0$, it further implies that $p \mid a$. Since it follows from Lemma 4.2.2 that if x is invertible, then both a and b can not be multiples of p; we get that $i = n$ and so $b = 0$. Further, $a^2 - b^2 = 1$ gives $a = -1 = x$.

Similar way, it can be checked that the only elements of $\mathbb{Z}_{p^n}[w]$ that are of

order 3 are ω and ω^2. Now the claim follows. □

Note that $(p^2-1) = (p-1)(p+1)$ and Lemma 4.2.1 and Proposition 4.2.1 provide a generator of $\mathbb{V}(\mathbb{Z}_{p^n}C_3)$ of order $(p-1)$. Further, based on the discussion in previous lemma, we are able to obtain the structure and generators in the following cases, where the only prime divisors of $(p+1)$ are 2 and 3:

Example 4.2.1. $\mathbb{V}(\mathbb{Z}_{17^n}C_3) \simeq C_{17^{n-1}} \times C_{17^{n-1}} \times C_9 \times C_{32}$.

Proof. It follows from Lemma 4.2.2 that $|\mathbb{V}(\mathbb{Z}_{17^n}C_3)| = 17^{2(n-1)}(17^2-1) = 17^{2(n-1)}(288)$. Now observe that if some element of $\mathbb{V}(\mathbb{Z}_{17^n}C_3)$ satisfies $u_1^3 = g$, then $o(u_1) = 9$. For instance, when $n = 1, F_{17}^* = \langle 3\rangle$ and $u_1 = 3^5 + 3^9 g + 3^8 g^2 = 5 + 14g + 16g^2$. Further, as per the discussion in Proposition 4.2.1, the element $\frac{1}{3}\left(-1 + \frac{4}{3}\hat{g}\right)$, say v, is t_3 with $\eta = \frac{-1}{3}$. Since $o\left(\frac{-1}{3}\right) = (17-1) = 16, v$ is of order 16. As $\left(\frac{1}{3}(1+2g)\right)^2 = v$, we obtain that $\frac{1}{3}(1+2g)$ is of order 32. □

Example 4.2.2. $\mathbb{V}(\mathbb{Z}_{53^n}C_3) \simeq C_{53^{n-1}} \times C_{53^{n-1}} \times C_{27} \times C_{104}$.

Proof. Here we have that $(53^2-1) = 52(54) = (13(2^3))(3^3)$. Now any solution of $u_1^9 = g$ is of order 27. Further, note that here the order of $\left(\frac{1}{3}(1+2g)\right)$ is $2(53-1) = 104$. □

When $p = 71, (p^2-1) = (70)(8)(9)$. Thus we have the following:

Example 4.2.3. $\mathbb{V}(\mathbb{Z}_{71^n}C_3) \simeq C_{71^{n-1}} \times C_{71^{n-1}} \times C_{560} \times C_9$.

Proof. In a similar manner, one can claim that a solution of $u_1^4 = \left(\frac{1}{3}(1+2g)\right)$ is of order 560 and any element satisfying $y^3 = g$ is of order 9. Now the result follows. □

4.3 The structure of $\mathbb{U}(\mathbb{Z}_{p^n}T_m)$

In this section, we provide the structure of $\mathbb{U}(\mathbb{Z}_{p^n}T_m)$. The main result of this section is as follows:

Theorem 4.3.1. $\mathbb{U}(\mathbb{Z}_{p^n}T_m) \simeq \mathbb{U}(\mathbb{Z}_{p^n}) \times (\mathbb{U}(\mathbb{Z}_{p^n}[\omega]))^{\frac{3^m-1}{2}}$.

Proof. It is known that

$$\mathbb{Z}_{p^n}(C_3 \times C_3) \cong (\mathbb{Z}_{p^n}C_3)C_3,$$

where $\mathbb{Z}_{p^n}C_3 \cong \mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}[\omega]$. Further, using $e = \frac{(1+g+g^2)}{3}$, we can write

$$\mathbb{Z}_{p^n}[\omega]C_3 \cong \mathbb{Z}_{p^n}[\omega] \oplus \frac{\mathbb{Z}_{p^n}[\omega][y]}{\langle 1+y+y^2\rangle},$$

where

$$\frac{\mathbb{Z}_{p^n}[\omega][y]}{\langle 1+y+y^2\rangle} \cong \frac{\mathbb{Z}_{p^n}[\omega][y]}{\langle (y-\omega)(y-\omega^2)\rangle}.$$

Since $\langle y-\omega\rangle$ and $\langle y-\omega^2\rangle$ are comaximal, we have

$$\frac{\mathbb{Z}_{p^n}[\omega][y]}{\langle 1+y+y^2\rangle} \cong \mathbb{Z}_{p^n}[\omega] \oplus \mathbb{Z}_{p^n}[\omega].$$

Therefore, $\mathbb{Z}_{p^n}[\omega]C_3 \cong \mathbb{Z}_{p^n}[\omega]^3$ and hence $\mathbb{Z}_{p^n}(C_3 \times C_3) \cong \mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}[\omega]^4$. Continuing this way, we obtain

$$\mathbb{Z}_{p^n}({C_3}^m) \cong \mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^n}[\omega]^{\frac{3^m-1}{2}}.$$

The restriction to the unit group proves the result. □

In the end, we give the structure of the unit group in the following corollaries.

Corollary 4.3.1. *For $p = 2$,*

$$\mathbb{U}(\mathbb{Z}_{2^n}T_m) \simeq \begin{cases} C_2 \times (C_2^2 \times C_3)^{\frac{3^m-1}{2}}, & n = 2 \\ C_2 \times C_{2^{n-2}} \times (C_2 \times C_{2^{n-2}} \times C_{2^{n-1}} \times C_3)^{\frac{3^m-1}{2}}, & n > 2 \end{cases}.$$

Corollary 4.3.2. *For an odd prime p,*

(i) If $p \equiv 1 \mod 3$ then

$$\mathbb{U}(\mathbb{Z}_{p^n}T_m) \simeq C_{p^n-1} \times C_{p-1} \times (C_{{p^{n-1}}^{(2)}} \times C_{{p-1}^{(2)}})^{\frac{3^m-1}{2}}.$$

(ii) Let $p \equiv 2 \mod 3$. *If* $p^2 \not\equiv 1 \mod 9$ *and* $(-3)^{\frac{p^2-1}{12}}(x)^{\frac{p^2-1}{6}} \equiv -1 \mod p^n$ *has a solution, then*

$$\mathbb{U}(\mathbb{Z}_{p^n}T_m) \simeq C_{p^n-1} \times C_{p-1} \times ({C_{p^{n-1}}}^{(2)} \times C_{p^2-1})^{\frac{3^m-1}{2}}.$$

References

[1] A. Cayley. On the theory of groups, as depending on the symbolic equation $\theta^n = 1$. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, 7(42):40–47, 1854.

[2] I. Kaplansky. *Problems in the theory of rings.* Report of a conference on linear algebras, National Academy of Sciences-National Research Council, Washington, Publ. 502, pp. 1-3. National Academy of Sciences-National Research Council, Washington, Publ. 502, 1957.

[3] I. Kaplansky. Problems in the theory of rings revisited. *Amer. Math. Monthly*, 77:445–454, 1970.

[4] I. G. Connell. On the group ring. *Canad. J. Math.*, 15:650–685, 1963.

[5] E. Jespers and Á. del Río. *Group ring groups. Vol. 1. Orders and generic constructions of units.* De Gruyter, Berlin, 2016.

[6] D. S. Passman. *The algebraic structure of group rings.* Pure and Applied Mathematics, Wiley-Interscience [John Wiley & Sons], New York-London-Sydney. Wiley-Interscience [John Wiley & Sons], New York-London-Sydney, 1977.

[7] C. P. Milies and S. K. Sehgal. *An introduction to group rings*, volume 1 of *Algebras and Applications.* Kluwer Academic Publishers, Dordrecht, 2002.

[8] S. K. Sehgal. *Units in integral group rings*, volume 69 of *Pitman Monographs and Surveys in Pure and Applied Mathematics.* Longman Scientific & Technical, Harlow; copublished in the United States with John Wiley & Sons, Inc., New York, 1993.

[9] S. K. Sehgal. *Topics in group rings*, volume 50 of *Monographs and Textbooks in Pure and Applied Math.* Marcel Dekker, Inc., New York, 1978.

[10] D. S. Dummit and R. M. Foote. *Abstract algebra.* John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[11] J. J. Rotman. *An introduction to the theory of groups*, volume 148 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, fourth edition, 1995.

[12] E. Artin. *Geometric Algebra.* Wiley Classics Library. Wiley, 2011.

[13] C. Milies and S. Sehgal. *An Introduction to Group Rings.* 01 2002.

[14] M. Parmenter and S. Sehgal. Uniqueness of the coefficient ring in some group rings. *Canadian Mathematical Bulletin*, 16(4):551–555, 1973. doi: 10.4153/CMB-1973-090-5.

[15] G. Higman. The Units of Group-Rings. *Proceedings of the London Mathematical Society*, s2-46(1):231–248, 01 1940.

[16] A. Bovdi. The group of units of a group algebra of characteristic p. *Publ. Math. Debrecen*, 52(1-2):193–244, 1998.

[17] R. Sandling. Units in the modular group algebra of a finite abelian p-group. *J. Pure Appl. Algebra*, 33(3):337–346, 1984.

[18] V. Bovdi and M. Salim. On the unit group of a commutative group ring. *Acta Sci. Math. (Szeged)*, 80(3-4):433–445, 2014.

[19] K.R. Pearson. On the units of a modular group ring. *Bulletin of the Australian Mathematical Society*, 7(2):169–182, 1972.

[20] A. Herman, Y. Li, and M. M. Parmenter. Trivial units for group rings with g-adapted coefficient rings. *Canadian Mathematical Bulletin*, 48(1):80–89, 2005.

[21] A. Herman and Y. Li. Trivial units for group rings over rings of algebraic integers. *Proc. Amer. Math. Soc.*, 134(3):631–635, 2006.

[22] M. Khan, R. K. Sharma, and J. B. Srivastava. The unit group of FS_4. *Acta Math. Hungar.*, 118(1-2):105–113, 2008.

[23] M. Khan. Structure of the unit group of FD_{10}. *Serdica Math. J.*, 35(1):15–24, 2009.

[24] R. K. Sharma, J. B. Srivastava, and M. Khan. The unit group of FA_4. *Publ. Math. Debrecen*, 71(1-2):21–26, 2007.

[25] R. K. Sharma, J. B. Srivastava, and M. Khan. The unit group of FS_3. *Acta Math. Acad. Paedagog. Nyházi. (N.S.)*, 23(2):129–142, 2007.

[26] K. Kaur and M. Khan. Units in F_2D_{2p}. *J. Algebra Appl.*, 13(2):1350090, 9, 2014.

[27] K. Kaur and M. Khan. Units of FD_{2p}. *Publ. Math. Debrecen*, 86(3-4):275–283, 2015.

[28] J. Gildea. The structure of the unit group of the group algebra $\mathbb{F}_{3^k}(c_3 \times d_6)$. *Communications in Algebra*, 38(9):3311–3317, 2010.

[29] K. Kaur, M. Khan, and T. Chatterjee. A note on normal complement problem. *J. Algebra Appl.*, 16(1):1750011, 11, 2017.

[30] L. E. Moran and R. N. Tench. Normal complements in mod p-envelopes. *Israel J. Math.*, 27(3-4):331–338, 1977.

[31] D. L. Johnson. The modular group-ring of a finite p-group. *Proc. Amer. Math. Soc.*, 68(1):19–22, 1978.

[32] L. R. Ivory. A note on normal complements in mod p envelopes. *Proc. Amer. Math. Soc.*, 79(1):9–12, 1980.

[33] P. J. Allen and C. Hobby. A characterization of units in $V(ZA_4)$. *Journal of Algebra*, 66(2):534–543, 1980.

[34] P. J. Allen and C. Hobby. Elements of finite order in $V(ZA_4)$. *Pacific Journal of Mathematics*, 138(1):1 – 8, 1989.

[35] P. J. Allen and C. Hobby. A characterization of units in $\mathcal{V}(\mathbb{Z}S_4)$. *Communications in Algebra*, 16(7):1479–1505, 1988.

[36] R. Sandling. The modular group algebra of a central-elementary-by-abelianp-group. *Archiv der Mathematik*, 52(1): 22–27, 1989.

[37] S. Kaur. On the normal complement problem in modular and semisimple group algebras. *Communications in Algebra*, 0(0):1–7, 2022.

[38] H. Setia and M. Khan. Normal complement problem over a finite field of characteristic 2. *Communications in Algebra*, 51(3):977–982, 2023.

[39] S. Kaur and M. Khan. The normal complement problem and the structure of the unitary subgroup. *Communications in Algebra*, 48(8):3628–3636, 2020.

[40] H. Setia and M. Khan. The normal complement problem in group algebras. *Communications in Algebra*, 50(1):287–291, 2022.

[41] Bertram Huppert. *Endliche gruppen I*, volume 134. Springer-verlag, 2013.

[42] G. Tang, Y. Wei, and Y. Li. Unit groups of group algebras of some small groups. *Czechoslovak Mathematical Journal*, 64(1):149–157, 2014.

[43] L. Creedon. The unit group of small group algebras and the minimum counterexample to the isomorphism problem. *arXiv preprint arXiv:0905.4295*, 2009.

[44] A. Herman, Y. Li, and M. M. Parmenter. Trivial units for group rings with g-adapted coefficient rings. *Canadian Mathematical Bulletin*, 48(1):80–89, 2005.

[45] M. Sahai and S. F. Ansari. Unit groups of group algebras of certain dihedral groups-ii. *Asian-European Journal of Mathematics*, 12(04):1950066, 2019.

[46] R. K. Sharma and G. Mittal. On the unit group of a semisimple group algebra $\mathbb{F}_q\mathrm{SL}(2, \mathbb{Z}_5)$. *Mathematica Bohemica*, 147(1):1–10, 2022.

[47] G. Bakshi, S. Gupta, and I.B.S. Passi. The structure of finite semisimple metacyclic group algebras. *Journal of the Ramanujan Mathematical Society*, 28 (2):141–158, 2013.

[48] S. Gupta and S. Maheshwary. Finite semisimple group algebra of a normally monomial group. *International Journal of Algebra and Computation*, 29(01): 159–177, 2019.

[49] I. Niven, H. S. Zuckerman, and H. L. Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons, 1991.

[50] A. A. Allan, M. J. Dunne, J. R. Jack, J. C. Lynd, and H. W. Ellingsen. Classification of the group of units in the gaussian integers modulo n. *Pi Mu Epsilon Journal*, 12(9):513–519, 2008.

[51] Z.X. Wan. *Lectures on Finite Fields and Galois Rings*. World Scientific, 2003.

List of Publications

1. Himanshu Setia and Manju Khan. The normal complement problem in group algebras, Communications in Algebra, 50(1):287-291, 2022

2. Himanshu Setia and Manju Khan. Normal complement problem over a field of characteristic 2, Communications in Algebra, 51(3):977-982, 2023

3. Himanshu Setia and Manju Khan. A note on the normal complement problem in semisimple group algebras. (accepted in IJPAM)

4. Himanshu Setia and Manju Khan. Unit group of group ring over $\mathbb{Z}_n$. (under review)

5. Himanshu Setia, Surinder Kaur and Manju Khan. On the units in group ring over $\mathbb{Z}_n$. (under review)

GAP-code

1. Himanshu Setia. GAP-code for calculating conjugacy class length. GitHub repository (2022). https://github.com/HimanSetia/GAP-code-for-calculating-conjugacy-class-length.git.

Future plans

We outline several research plans related to this topic, including the study of group rings over $\mathbb{Z}_n$, the investigation of the normal complement problem and its connection to the isomorphism problem and the exploration of the Fuchs' problem. By pursuing these objectives, we aim to gain a deeper understanding of the properties and structures of group rings.

- **To study the unit groups of group rings over $\mathbb{Z}_n$**

  The study of group rings over $\mathbb{Z}_n$ is an under-explored area in the literature of group rings. We have investigated the unit group structure of $\mathbb{Z}_nG$, where G is a finite group of exponent at most 4. However, there is still much to be explored in terms of the unit group structure for groups with larger exponents.

- **To find an example of a non-abelian group such that normal complement exists in the unit group of corresponding semisimple group algebra**

  The question of whether supporting examples for the normal complement problem exist for semisimple group algebras of non-abelian groups is still unsolved.

- **To investigate the connection between isomorphism problem and normal complement problem**

  In integral group rings, the isomorphism and normal complement problems are linked. We might expect a similar connection in modular and semisimple group algebras.

- **To analyse the Fuchs' problem**

  In recent years, researchers have noted a connection between Fuchs' problem and the normal complement problem. By exploring this intersection, we may be able to gain new insights and find solutions to the Fuchs' problem.

Himanshu Setia

Department of Mathematics
Indian Institute of Technology
Nangal Road, Rupnagar
Punjab-140001, India

Phone: (+91) 9888589944
Email: himansetia@gmail.com

Education

† *Indicates expected*

2018–2023 †	Ph.D. Mathematics
	Indian Institute Of Technology, Ropar, Punjab, India
2015–2017	M.Sc. Mathematics
	Hindu College, University of Delhi, Delhi, India
2012–2015	B.Sc. Non Medical
	Multani Mal Modi College, Patiala, Punjab, India

Appointments

2020–2022	Senior research fellow (SRF), Department of Mathematics, Indian Institute of Technology, Ropar
2018–2019	Junior research fellow (JRF), Department of Mathematics, Indian Institute of Technology, Ropar
2017–2017	Guest assistant professor, Mathematics, Post Graduate Government College for Girls, Panjab University, Chandigarh

Publications

- Himanshu Setia and Manju Khan. The normal complement problem in group algebras, Communications in Algebra, 50(1):287-291, 2022
- Himanshu Setia and Manju Khan. Normal complement problem over a field of characteristic 2, Communications in Algebra, 51(3):977-982, 2023
- Himanshu Setia and Manju Khan. A note on the normal complement problem in semisimple group algebras. (accepted)
- Himanshu Setia and Manju Khan. Unit group of group ring over $\mathbb{Z}_n$. (submitted)
- Himanshu Setia, Surinder Kaur and Manju Khan. On the units of group ring over $\mathbb{Z}_n$. (submitted)

GAP-code

- Himanshu Setia. GAP-code for calculating conjugacy class length. GitHub repository (2022). https://github.com/HimanSetia/GAP-code-for-calculating-conjugacy-class-length.git.

Academic events attended

Workshops

[1] Participated (10th-29th Dec, 2018) in AIS on Lie Algebras held at HRI, Allahabad

[2] Participated (1st-27th July, 2019) in AFS-3 held at NISER, Bhubhaneshwar

Conferences/Symposiums

[1] Participated (14th-23rd Oct, 2019) in an international conference on Group Algebras, Representations and Computations held at ICTS, Bangalore

[2] Presented a paper entitled "A study of normal complements in $\mathcal{V}(FA_4)$" in the annual research day, Cynosure-2021 & National Symposium on Advances in Mathematics held on December 21-22, 2021 at IIT Ropar.

[3] Presented a poster entitled "Unit group of group ring over $\mathbb{Z}_n$" in the annual research day, Cynosure-2022 & National Symposium on Advances in Mathematics held on December 10, 2022 at IIT Ropar.

[4] Presented a paper entitled "The normal complement problem in group algebras of symmetric groups" in the conference on Group Theory and Related Topics held on 27 Feb.-4 March, 2023 at NISER Bhubaneswar.

[5] Presented a paper entitled "The normal complement problem in group algebras" in the conference on Groups, Rings and the Yang Baxter equation held on 19 June-23 June, 2023 at Corsendonk Duisine Podlers, Blankenberge, Belgium.

Teaching assistant

2018	MAL-412, Basic Linear Algebra	Indian Institute Of Technology, Ropar
2019	MA-102, Calculus	Indian Institute Of Technology, Ropar
2020	MA-614, Applied Linear Algebra	Indian Institute Of Technology, Ropar
2021	MAL-413, Abstract Algebra	Indian Institute Of Technology, Ropar
2022	MA-202, Probability and Statistics	Indian Institute Of Technology, Ropar

List of courses studied

Algebra:

Field Theory, Rings and Modules, Representation Theory of Finite Groups, Advanced Group Theory, Group Rings, Module Theory, Lie Algebras.

Topology:

Point Set Topology, Topological Dynamics.

Analysis:

Functional Analysis, Fourier Analysis, Complex Analysis, Operators on Hardy Hilbert Spaces.

Miscellaneous:

Optimization Techniques and Control Theory, Fluid Dynamics, Differential Equations, Basic Automata Theory (Foundations of Computer Science), Applied Cryptography, Graph Theory.

Awards and achievements

2018	Awarded Institute fellowship (IIT Ropar) 2018-2022
2017	Qualified IIT-GATE-2017 in MA (Mathematics)
2017	Qualified CSIR-UGC NET-JRF JUNE-2017 in Pure Mathematics
2016	Qualified CSIR-UGC NET-LS DEC-2016 in Pure Mathematics
2015	Qualified IIT-JAM-2015 in MA
2012	Qualified AIEEE-2012 with All India Rank-8487
2012	Received the DST INSPIRE SHE 2012-2017 for scoring in the top 1% of students nationwide in 12th grade in CBSE.
2010	Awarded full fee waiver for schooling 2010-2012 based on my 116th place in the state merit list for matriculation examination prepared by P.S.Ed.B. Mohali, Punjab.

Co-curricular activities

- Volunteered at the π-ictionary event held on Pi Day 2016 at the Department of Mathematics, University of Delhi, Delhi.
- Participated in several science fairs and quiz competitions during high school and undergraduate studies.
- Competent in sports such as badminton, table tennis, chess, and carrom.
- Proficient in playing the acoustic guitar at a beginner level.