University of Chester

UNIVERSITY OF CHESTER

MA7190

RESEARCH DISSERTATION

# Group Algebras and Their Applications

*Student Number:*
J00267

*Supervisor:*
Dr. Joe Gildea

October 9, 2017

# Contents

**Abstract** **II**

**Acknowledgements** **III**

**Symbols** **IV**

**Introduction** **1**

**1 Introduction to Groups, Rings, Fields and Coding Theory** **2**
1.1 Groups . . . . . . . . . . 2
1.2 Rings & Fields . . . . . . . . . . 5
1.3 Group Rings . . . . . . . . . . 6
1.4 Coding Theory . . . . . . . . . . 10

**2 An Established Isomorphism** **16**

**3 Units of $\mathbb{F}_{2^k}D_8$** **21**
3.1 Constructing a Ring Homomorphism . . . . . . . . . . 21
3.2 Calculating the Exponent of the Kernel . . . . . . . . . . 23
3.3 Constructing a Subgroup $H$ and a Normal Subgroup $N$ . . . . . . . . . . 24
3.4 The Structure of $\mathcal{U}(\mathbb{F}_{2^k}D_8)$ . . . . . . . . . . 30

**4 Unitary Units of $\mathbb{F}_{2^k}D_8$** **33**

**5 Self-Dual Codes** **39**
5.1 Codes in $\mathbb{F}_2D_8$ . . . . . . . . . . 40
5.2 Codes in $\mathbb{F}_4D_8$ . . . . . . . . . . 43
5.3 Codes in $(\mathbb{F}_4 + u\mathbb{F}_4)D_8$ . . . . . . . . . . 47

**Appendix A Gap Code** **51**

**Appendix B Full Results for $(\mathbb{F}_4 + u\mathbb{F}_4)D_8$** **55**

# Abstract

Let $RG$ be the group ring of the group $G$ and the ring $R$. If $R$ is a field, we usually refer to $RG$ as a group algebra. We initially describe the unit group of the group algebra $\mathbb{F}_{2^k}D_8$ where $\mathbb{F}_{2^k}$ is a Galois Field of $2^k$ elements and $D_8$ is the dihedral group of order 8. We then describe the unitary unit group of $\mathbb{F}_{2^k}D_8$. Furthermore, we show the connection between unitary units in group rings and self-dual codes. Finally, we construct certain self-dual codes from the unitary units of the group algebra $\mathbb{F}_{2^k}D_8$.

# Acknowledgements

First I would like to thank my Research Supervisor Dr. Joe Gildea, whose encouragement and support during my Bachelor's degree led me to continue studying Mathematics at Master's level, something I would have not thought possible four years ago. His knowledge and previous research into Group Algebras, along with his excellent teaching style has given me a great insight into the field. I am also grateful to the rest of the Mathematics Department at the University of Chester, whose collective guidance has led me from a grade D in A Level Mathematics to a full PhD studentship.

Next I would like to thank my family, whose continued moral and financial support has inspired me to keep chasing the next academic qualification. I would also like to thank Hannah, my girlfriend of six years, who first encouraged me to apply to the University of Chester, and who has helped me through long periods of revision and difficult courseworks.

Finally I would like to express my gratitude to the Information Department at the Countess of Chester Hospital for supporting me throughout my time at University, and allowing me to be flexible with my work schedule so that I had sufficient time to study. I would also like to specifically thank my colleague Robert Cheetham who has helped and encouraged me to learn programming. Robert also introduced me to a number of useful programs and tools which have helped me throughout my dissertation, all of which I will continue to use in the future.

# Symbols

| | |
|---|---|
| $C_n$ | the cyclic group of order $n$. |
| $D_{2n}$ | the dihedral group of order $2n$. |
| $\|G\|$ | the order of the group $G$. |
| $H \cap K$ | the intersection of $H$ and $K$. |
| $H \times K$ | the external direct product $H$ and $K$. |
| $H \rtimes K$ | the semidirect product of $H$ and $K$. |
| $HK$ | the internal direct product of $H$ and $K$. |
| $N \lhd G$ | $N$ is a normal subgroup of $G$. |
| $\mathbb{F}_{p^k}$ | the Galois field of $p^k$ elements. |
| $RG$ | the group ring of $G$ over $R$. |
| $\mathcal{U}(RG)$ | the unit group of $RG$. |
| $\epsilon(RG)$ | the augmentation mapping of $RG$. |
| $V(RG)$ | the normalized unit group of $RG$. |
| $ZD(RG)$ | the zero divisors of $RG$. |
| $\ker(\theta)$ | the kernel of a group/ring homomorphism. |
| $\text{circ}(V)$ | the circulant matrix of the vector $V$. |
| $M_n(R)$ | the ring of $n \times n$ matrices over R. |
| $J_n$ | the $n \times n$ matrix of ones. |
| $I_n$ | the $n \times n$ identity matrix, sometimes denoted as just $I$. |

# Introduction

In this thesis, we describe the structure of the unit group and unitary unit group for certain group algebras. Additionally we detail the connection between unitary units of group rings and self-dual codes.

### Chapter Outlines

**Chapter 1:** First we study the fundamental terms and theorems related to groups, rings, fields, group-rings and coding theory which will be required to fully understand the material in the following chapters. This chapter will also introduce GAP, a system for computational discrete algebra. Examples will sometimes be verified using this package.

**Chapter 2:** Next, we introduce a ring isomorphism first shown by T. Hurley in [12]. This chapter is essential to chapters 2 and 3 where we examine the units and unitary units of group rings.

**Chapter 3:** This chapter follows the work of J. Gildea and L. Creedon [4], who have determined the structure of the unit group $\mathcal{U}(\mathbb{F}_{2^k}D_8)$. Alternative proofs to many of the results are provided, using the ring isomorphism from Chapter 2.

**Chapter 4:** Here we continue to follow the work of J. Gildea [6], this time studying the unitary units, $V_*(\mathbb{F}_{2^k}D_8)$. Again, alternative proofs with full details are provided.

**Chapter 5:** In this final chapter, we show how the unitary units from Chapter 4 relate to self-dual codes. We examine codes over $\mathbb{F}_2, \mathbb{F}_4$ and $\mathbb{F}_4 + u\mathbb{F}_4$, using a construction based on the isomophism given in Chapter 2.

# Chapter 1

# Introduction to Groups, Rings, Fields and Coding Theory

## 1.1 Groups

We start with the most basic of algebraic stuctures, namely, groups. Here we will cover basic definitions, see examples of different groups, and demonstrate how you can use `GAP` to create and manipulate them.

**Definition 1.1 ([17])** *A **group** $(G, *)$ is a set $G$ on which a binary operation $*$ has been defined such that the following axioms are satisfied:*

*i)* $x * y \in G \; \forall \; a, b \in G$

*ii)* $a * (b * c) = (a * b) * c \; \forall \; a, b, c \in G$

*iii) There exists a unique identity element* $e \in G$ *such that* $a * e = e * a = a \; \forall \; a \in G$

*iv) There exists an inverse element* $a^{-1} \in G$ *such that* $a * a^{-1} = a^{-1} * a = e \; \forall \; a \in G.$

*If the following extra condition is satisfied then $(G, *)$ is called an **abelian group**:*

*v)* $a * b = b * a \; \forall \; a, b \in G.$

**Definition 1.2 ([17])** *If the set $G$ has a finite number of elements, then the number of elements is called the **order** of the $G$ and is denoted $|G|$.*

**Example 1.3** *The set of integers modulo 4, $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. along with the addition operator form a group $(\mathbb{Z}_4, +)$. Therefore the order of $\mathbb{Z}_4$ is $|\mathbb{Z}_4| = 4$. since there are four elements in the set.*

**Definition 1.4 ([16])** *A group $G$ is said to be **cylic** if there exists $x \in G$ such that every element of $G$ can be written in the form $x^n$ for some $n \in \mathbb{Z}$. Such an element $x$ is said to be a generator of $G$*

**Example 1.5** *The cylic group generated by $x$ with order $n = 3$ has the following elements*

$$G = \{1, x, x^2\}.$$

Listing 1.1 shows how you can use `GAP` to display the elements of this group, and produce the cayley table. Note that `<id>` refers to the identity element which in this case is 1.

**Listing 1.1: Cyclic Group of Order 3**

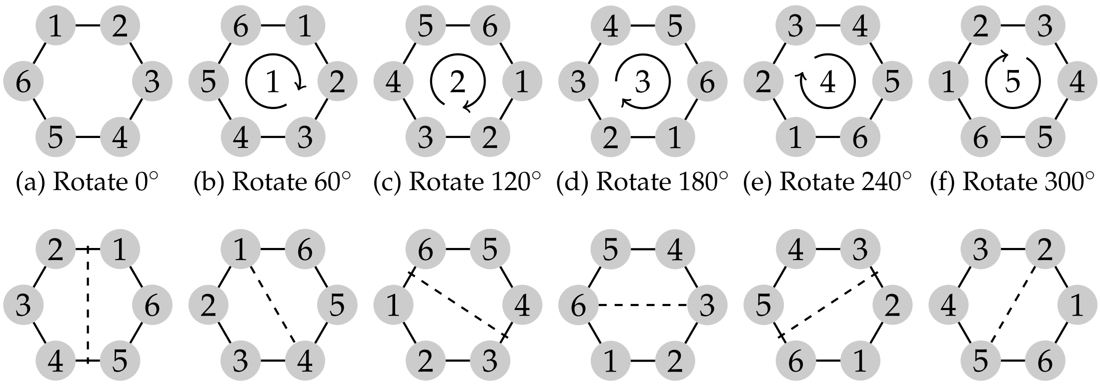
```
gap> G:=CyclicGroup(IsFpGroup,3); # defines the cyclic group of order 3
<fp group of size 3 on the generators [ a ]>
gap> Elements(G); # displays the elements of G
[ <identity ...>, a, a^2 ]
gap> ShowMultiplicationTable(G); # displays the cayley table
*     | <id>   a    a^2
------+----------------
<id>  | <id>   a    a^2
 a    |  a    a^2   <id>
a^2   | a^2   <id>   a
```

**Definition 1.6 ([16])** *The nth **dihedral group** of order $2n$ generated by $x$ and $y$ is defined to be*

$$D_{2n} = \langle x, y \mid x^n = y^2 = xyxy = 1 \rangle.$$

This particular type of group will feature throughout this thesis, therefore it will be useful to have an idea of how they can be represented.

**Example 1.7** *The dihedral group $D_{12}$ can be thought of as the number of different ways that you can rotate, or reflect a six-sided regular polygon.*



(a) Rotate 0° (b) Rotate 60° (c) Rotate 120° (d) Rotate 180° (e) Rotate 240° (f) Rotate 300°

(g) Reflect 1 (h) Reflect 2 (i) Reflect 3 (j) Reflect 4 (k) Reflect 5 (l) Reflect 6

Figure 1.1: Visual representation of $D_{12}$

It can be easily checked that six 60° rotations of any hexagon seen in Figure 1.1 will leave it unchanged i.e. $x^n$, similarly with two reflections along the same axis i.e. $y^2$. However, it is less obvious to see that the sequence: rotation, reflection, rotation, reflection i.e. $(xy)^2$ will also produce no change.

Next we look at subgroups and normal subgroups. We will use these definitions in order to identify the structures of $\mathcal{U}(\mathbb{F}_{2^k}D_8)$ and $V_*(\mathbb{F}_{2^k}D_8)$ in the later chapters.

**Definition 1.8 ([3])** *Let $G$ be a group, and let $H$ be a subset of $G$. Then $H$ is a **subgroup** of $G$ if and only if the following conditions hold:*

1. *$xy \in H$ for all $x, y \in H$*
2. *The identity element $e \in H$*
3. *$x^{-1} \in H$ for all $x \in H$.*

The following corollary provides a much shorter method for checking that a group is a subgroup.

**Corollary 1.9 ([3])** *Let $G$ be a group and let $H$ be a finite, nonempty subset of $G$. Then $H$ is a subgroup of $G$ if and only if $xy \in H$ for all $x, y \in H$.*

**Definition 1.10 ([17])** *Let $H$ be a subgroup of a group $G$. We say that $H$ is a **normal subgroup** of $G$, denoted $H \lhd G$, if for all $x \in G$ we have $x^{-1}Hx = H$.*

When describing the stucture of a group we are often required to break it down into products of subgroups. Let us define three different products of groups.

**Definition 1.11 ([3])** *Let $G$ be a group, and let $H$ and $K$ be subsets of $G$. Then*

$$HK = \{x \in G \mid x = hk \text{ for some } h \in H,\ k \in K\}.$$

*If $H$ and $K$ are subgroups of $G$ then we call $HK$ the **product** of $H$ and $K$.*

**Definition 1.12 ([17])** *Let $H$ and $K$ be two subgroups of a group $G$. We say that $G$ is the (internal) **direct product** of $H$ and $K$ if the following conditions hold:*

*i)* $G = HK$

*ii)* $H \cap K = \{1\}$

*iii)* *$H \lhd G$ and $K \lhd G$.*

*To denote this relation we write $G = H \times K$.*

**Definition 1.13 ([17])** *Let $H$ and $K$ be two subgroups of a group $G$. We say that $G$ is the (internal) **semidirect product** of $H$ and $K$, and write $G = H \rtimes K$ if we have the following:*

*i)* $G = HK$

*ii)* $H \cap K = \{1\}$

*iii)* $H \lhd G$.

The only difference being that a semidirect product is a weaker condition, since $K \lhd G$ is not required.

**Proposition 1.14 ([9])** *Let H and K be finite subgroups of a group G. Then*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

## 1.2 Rings & Fields

Next we look at Rings and Fields, an extension of Groups, the difference being that two operations are now considered. We also look briefly introduce the concept of a ring homomorphism, a function between two rings which respects the structure.

**Definition 1.15 ([17])** *A set R with two operations (usually addition and multiplication) denoted by $(R, +, \cdot)$ is called a ring if the following conditions hold:*

i) $(R, +)$ *is an abelian group*

ii) $a \cdot (b \cdot c) = (a \cdot b) \cdot c \; \forall \; a, b, c \in R$

iii) *There exists an identity element* $1$ *such that* $a \cdot 1 = 1 \cdot a = a \; \forall \; a \in R$

iv) $a \cdot (b + c) = a \cdot b + a \cdot c$ *and* $(a + b) \cdot c = a \cdot c + b \cdot c \; \forall \; a, b, c \in R$

*If the following additional property is satisfied then the ring is called commutative*

v) $a \cdot b = b \cdot a \; \forall \; a, b \in R.$

**Definition 1.16 ([17])** *An element a of a ring R is called invertible if there exists an inverse element, denoted $a^{-1} \in R$. such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$. The set of all invertible elements of R are known as the group units of R and are denoted by*

$$\mathcal{U}(R) = \{a \in R \, | a^{-1} \in R\}.$$

**Definition 1.17 ([8])** *An algebraic structure consisting of a set together with two operations (again, usually addition and multiplication) is called a field if $(F, +, \cdot)$ is a ring and $(F/\{0\}, \cdot)$ is an abelian group.*

**Definition 1.18 ([8])** *A finite field is a field which has a finite number of elements, this number is known as the order of the field. In general, we will denote a field with q elements by $\mathbb{F}_q$ or GF(q), a Galois Field with q elements.*

**Definition 1.19 ([17])** *Let R and S be two rings. Then, a map $\varphi : R \to S$ is called a ring homomorphism if for all $\alpha,\ \beta \in R$ we have*

*i)* $\varphi(\alpha+\beta) = \varphi(\alpha) + \varphi(\beta)$

*ii)* $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$.

**Example 1.20** *Consider the mapping $\varphi : \mathbb{F}_2 \to \mathbb{F}_2$ such that $\varphi(x) = x^2$. Let $x,\ y \in \mathbb{F}_2$ then we have*

$$\begin{aligned}\varphi(x+y) &= (x+y)^2\\ &= x^2+2xy+y^2\\ &= x^2+y^2\\ &= \varphi(x)+\varphi(y).\\ \varphi(xy) &= (xy)^2\\ &= x^2y^2\\ &= \varphi(x)\varphi(y).\end{aligned}$$

*Thus, $\varphi$ is a ring homomorphism.*

## 1.3 Group Rings

In this section we introduce group rings. We begin with a definition and accompanying examples, then we take a closer look at the invertible elements (units) of a group ring, $\mathcal{U}(RG)$. Next, we introduce the augmentation mapping $\epsilon$, which leads us to the normalized units, $V(RG)$. We then finish the section with a definition for $V_*(RG)$, a special subgroup of $V(RG)$.

**Definition 1.21 ([17])** *A group ring RG is the set of all linear combinations*

$$\alpha = \sum_{g\in G} a_g g,$$

*where $a_g \in R$.*

**Example 1.22** *Let $\mathbb{Z}_2 = \{0,1\}$ be a ring and $C_2$ be the cyclic group of order 2, i.e. $C_2 = \{x \mid x^2 = 1\} = \{1,x\}$. Then, the group ring $\mathbb{Z}_2C_2$ is defined as*

$$\begin{aligned}\mathbb{Z}_2C_2 &= \{a_1\cdot 1 + a_2\cdot x \mid a_i \in \mathbb{Z}_2\}\\ &= \{0,1,x,1+x\}.\end{aligned}$$

We can identify the units of a group ring by producing a multiplication table of all possible pairs of elements and see which ones give the identity. Such a table is often called a Cayley table.

We can construct the Cayley table for $\mathbb{Z}_2C_2$ as follows:

| $\times$ | $1$ | $x$ | $1+x$ |
|---|---|---|---|
| $1$ | $1$ | $x$ | $1+x$ |
| $x$ | $x$ | $1$ | $1+x$ |
| $1+x$ | $1+x$ | $1+x$ | $0$ |

Table 1.1: The Cayley Table for $\mathbb{Z}_2C_2$

From table 1.1, we can see that the units of this group ring are $\mathcal{U}(\mathbb{Z}_2C_2) = \{1, x\}$. We verify the units using `GAP` in Listing 1.2.

**Listing 1.2: Units of $\mathbb{Z}_2C_2$**

```
gap> Read("/home/harrison/.../CustomFunctions.g"); # import Tidy()
gap> RG := GroupRing(GF(2),CyclicGroup(IsFpGroup,2)); # defines F_2C_2
<algebra-with-one over GF(2), with 1 generators>
gap> Elements(Units(RG)); # prints the elements of RG
[ (Z(2)^0)*<identity ...>, (Z(2)^0)*a ]
gap> Print(Tidy(Elements(Units(RG)))); # prints reader friendly elements
[ 1, a ]
```

**Example 1.23** *Similarly to the previous example, let $\mathbb{Z}_2 = \{0, 1\}$ be a ring, but now combined with the cyclic group $C_3 = \{x \mid x^3 = 1\} = \{1, x, x^2\}$. Then, the group ring $\mathbb{Z}_2C_3$ is given as*

$$\begin{aligned}\mathbb{Z}_2C_3 &= \{a_1 \cdot 1 + a_2 \cdot x + a_3 \cdot x^2 \mid a_i \in \mathbb{Z}_2\} \\ &= \{0, 1, x, x^2, 1+x, 1+x^2, x+x^2, 1+x+x^2\}.\end{aligned}$$

| $\times$ | $1$ | $x$ | $x^2$ | $1+x$ | $1+x^2$ | $x+x^2$ | $1+x+x^2$ |
|---|---|---|---|---|---|---|---|
| $1$ | $1$ | $x$ | $x^2$ | $1+x$ | $1+x^2$ | $x+x^2$ | $1+x+x^2$ |
| $x$ | $x$ | $x^2$ | $1$ | $x+x^2$ | $1+x$ | $1+x^2$ | $1+x+x^2$ |
| $x^2$ | $x^2$ | $1$ | $x$ | $1+x^2$ | $x+x^2$ | $1+x$ | $1+x+x^2$ |
| $1+x$ | $1+x$ | $x+x^2$ | $1+x^2$ | $1+x^2$ | $x+x^2$ | $1+x$ | $0$ |
| $1+x^2$ | $1+x^2$ | $1+x$ | $x+x^2$ | $x+x^2$ | $1+x$ | $1+x^2$ | $0$ |
| $x+x^2$ | $x+x^2$ | $1+x^2$ | $1+x$ | $1+x$ | $1+x^2$ | $x+x^2$ | $0$ |
| $1+x+x^2$ | $1+x+x^2$ | $1+x+x^2$ | $1+x+x^2$ | $0$ | $0$ | $0$ | $1+x+x^2$ |

Table 1.2: The Cayley Table for $\mathbb{Z}_2C_3$

The units are the invertible elements from table 1.2 and are given as $\mathcal{U}(\mathbb{Z}_2C_3) = \{1, x, x^2\}$. Notice that $\mathcal{U}(\mathbb{Z}_2C2) = \{1, x, x^2\} \cong C_2$ and $\mathcal{U}(\mathbb{Z}_2C3) = \{1, x, x^2\} \cong C_3$. leading to our next definition.

**Definition 1.24 ([17])** *Let $RG$ be the group ring formed by the group $G$ over the ring $R$. The elements of $RG$ of the form $rg$, where $r \in \mathcal{U}(R)$ and $g \in G$ are called the trivial units.*

The units we've found in the examples so far are clearly trivial units. It is tempting to think that group rings only ever have trivial units, but we shall see now that this is not always the case.

**Definition 1.25 ([17])** *Let $G$ be an abelian group. Then, the subgroup*

$$T(G) = \{g \in G \mid o(g) < \infty\}$$

*is called the torsion subgroup of $G$. If $T(G) = \{1\}$ then we say that $G$ is a torsion-free group.*

**Proposition 1.26 ([18])** *Let $K$ be a field and let $G$ be a group that is not torsion-free. Then, with the exception of the following:*

*i)* $K = \mathbb{F}_2$. *with* $|G| = 2$ *or* $3$

*ii)* $K = \mathbb{F}_3$. *with* $|G| = 2$.

*the group ring contains non-trivial units.*

In Examples 1.22 and 1.23, the field was $\mathbb{F}_2$ and the order of the groups were 2 and 3 respectively.

**Definition 1.27 ([17])** *Let $R$ be a ring with $a,\ b \in R$, then if $a \cdot b = 0$ then $a$ and $b$ are **zero divisors**.*

**Example 1.28** *Consider the group ring $\mathbb{Z}_2C_3 = \{0, 1, x, x^2, 1+x, 1+x^2, x+x^2, 1+x+x^2\}$ from Example 1.23. The zero divisors can be seen from Table 1.2 and are denoted by $ZD(\mathbb{Z}_2C_3) = \{0, 1+x, 1+x^2, x+x^2, 1+x+x^2\}$.*

**Definition 1.29 ([17])** *The homomorphism $\epsilon : RG \to R$ given by*

$$\epsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g$$

*is called the augmentation mapping of $RG$*

This concept is best understood with an example.

**Example 1.30** *Consider group ring $RG$ created by the ring $\mathbb{F}_3$ and the cyclic group $C_2$*

$$\begin{aligned}\mathbb{F}_3C_2 &= \{\alpha_1 + \alpha_2 x \mid \alpha_i \in \mathbb{F}_3\}\\ &= \{0, 1, 2, x, 2x, 1+x, 1+2x, 2+x, 2+2x\}.\end{aligned}$$

*The augmentation map of $RG$ is as follows:*

$$\begin{array}{rrr} \epsilon(1) = 1+0 = 1 & \epsilon(2x) = 0+2 = 2 & \epsilon(2+x) = 2+1 = 0 \\ \epsilon(2) = 2+0 = 2 & \epsilon(1+x) = 1+1 = 2 & \epsilon(2+2x) = 2+2 = 1 \\ \epsilon(x) = 0+1 = 1 & \epsilon(1+2x) = 1+2 = 0 & \epsilon(0) = 0+0 = 0. \end{array}$$

Listing 1.3 shows a loop created in GAP to verify the above augmentation map, for the Tidy function see Appendix A.1.

**Listing 1.3: Augmentation of $\mathbb{Z}_3C_2$**

```
gap> Read("/home/harrison/.../CustomFunctions.g"); # import Tidy()
gap> RG:= GroupRing(GF(3),CyclicGroup(IsFpGroup,2));
<algebra-with-one over GF(3), with 1 generators>
gap> for i in [1..Size(RG)] do
> Print(Tidy(Elements(RG)[i]),"\t->\t",Tidy(Augmentation(Elements(RG)[i])),"\n");
> od;
0    -> 0
1    -> 1
1+a  -> 2
1+2a -> 0
2    -> 2
2+a  -> 0
2+2a -> 1
a    -> 1
2a   -> 2
```

There also exists $V(RG) \subseteq \mathcal{U}(RG)$ known as the normalized units, which we define below.

**Definition 1.31 ([17])** *Let RG be a group ring with units $\mathcal{U}(RG)$. Then*

$$V(RG) = \{u \in \mathcal{U}(RG) \mid \epsilon(u) = 1\}$$

*is called the normalized units of RG, or units of augmentation one.*

**Example 1.32** *Continuing from Example 1.30, it can be shown that $\mathcal{U}(\mathbb{F}_3C_2) = \{1, 2, x, 2x\}$. From these units, the two with augmentation one are $1$ and $x$, therefore*

$$V(\mathbb{F}_3C_2) = \{1, x\} \cong C_2.$$

**Definition 1.33 ([6])** *Consider the map $* : RG \to RG$, defined by $\left(\sum_{g\in G} a_g g\right)^* = \sum_{g\in G} a_g g^{-1}$. This map is an antiautomorphism of RG of order $2$. An element $v \in V(RG)$ satisfying $v^{-1} = v^*$ is called unitary. We denote the subgroup consisting of the unitary elements of $V(RG)$ by $V_*(RG)$.*

**Theorem 1.34 ([15])** *$V(RG)$ is a normal subgroup of $\mathcal{U}(RG)$ and*

$$\mathcal{U}(RG) \cong \mathcal{U}(R) \times V(RG).$$

**Proof.** The result $V(RG) \triangleleft \mathcal{U}(RG)$ comes from the fact that $\epsilon : RG \to R$ is a homomorphism. Now, note that the only common element in $V(RG)$ and $\mathcal{U}(RG)$ is the identity, and that for any $u \in \mathcal{U}(RG)$, we have that $r = \epsilon(u) \in \mathcal{U}(R)$ is a unit such that $\epsilon(r^{-1}u) = \epsilon(r^{-1})\epsilon(u) = 1$. Then, $u = r(r^{-1}u)$ shows that $\mathcal{U}(RG) = \mathcal{U}(R) \cdot V(RG)$, hence the result. ■

**Definition 1.35 ([17])** *A group $G$ is called an extension of a group $K$ by a group $H$ if there an exists an epimorphism $\varphi$ from $G$ onto $K$ with $H = \ker(\varphi)$. Furthermore, the extension is called a split extension if there exists a homomorphism $\psi : K \to G$ such that $\varphi \circ \psi$ is the identity map of $K$*

We finish this section with a definition of a circulant matrix. We will see how this type of matrix relates to group rings in Chapter 2.

**Definition 1.36 ([5])** *The following $n \times n$ matrix:*

$$M = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_n & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \cdots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & a_4 & \cdots & a_1 \end{pmatrix}$$

*is called a circulant matrix.*

Since circulant matrices appear frequently within the later chapters, we will use the abbreviated form $M = \text{circ}[a_1, a_2, a_3, \cdots, a_n]$. For further reading on circulant matrices see [5].

## 1.4 Coding Theory

Error-correcting codes as the name suggests are used to correct errors in data transmitted through a noisy communication channel. In this section we will look at some basic definitions and important results from coding theory, including weight enumerators and minimum distance. We also look at what is meant by a self-dual code, which is the subject of chapter 5.

**Definition 1.37 ([7])** *An alphabet is a set of symbols, usually letters, characters or digits. The most commonly used alphabet is $\mathbb{F}_2 = \{0, 1\}$, the binary alphabet.*

**Example 1.38** $\mathbb{F}_2 = \{0, 1\}$ *has the following addition and multiplication tables*

| $+$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

| $\cdot$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

Alphabets are used to create codewords, which are the vectors which form code blocks.

**Definition 1.39 ([7])** *An error correcting code $C$ of length $n$ over a finite alphabet $\mathbb{F}_q$ is a subset of $\mathbb{F}_q^n$. The elements of $C$ are called codewords. A codeword of $C$ takes the form $(c_1, c_2, ..., c_n)$, where each $c_i \in \mathbb{F}_q$.*

If $C$ is a code over $\mathbb{F}_q$ then we say that $C$ is a $q$-ary code.

**Example 1.40** *Consider the following binary code over $\mathbb{F}_2$:*

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

*The rows of C produce 4 codewords: $c_1 = (1,1,1,1)$, $c_2 = (0,1,0,1)$, $c_3 = (1,0,1,0)$, $c_4 = (0,0,0,0)$.*

Two properties of codes which we are concerned with are the weight and the distance of codewords.

**Definition 1.41 ([7])** *Let $x, y \in \mathbb{F}_2^n$ be two codewords of length n, then the distance $d(x,y)$ of x and y is given by*

$$d(x,y) = |\{i \,|\, 1 \leq i \leq n,\ x_i \neq y_i\}|.$$

*The weight of a codeword is defined as*

$$w(x) = d(x, \mathbf{0}),$$

*where $\mathbf{0} = (0,0,...,0)$ is the zero vector.*

Definition 1.41 describes the Hamming-distance, named after Richard Hamming. You can think of the Hamming-distance as the number of places in which two codewords differ, and weight as the number of ones. In `GAP`, the Hamming-distance can be calculated with the command `DistanceCodeword(x,y)`, and the weight can be calculated using `WeightCodeword(x)`.

**Proposition 1.42 ([8])** *The Hamming-distance $d(x,y)$ satisfies the required conditions to be a metric:*

*a) $d(x,y) \geq 0$ and $d(x,y) = 0$ if and only if $x = y$*

*b) $d(x,y) = d(y,x)$*

*c) $d(x,z) \leq d(x,y) + d(y,z)$ for any $x,y,z \in \mathbb{F}_2^n$*

**Definition 1.43 ([7])** *The minimum distance of a code C is defined as*

$$d = min\{d(x,y) \,|\, x, y \in C, x \neq y\}.$$

The minimum distance is important in determining the error-correcting capability of a code. Codes with larger minimum distance can correct more errors. The command for finding the minimum distance of a code C in `GAP` is `MinimumDistance(C)`.

**Example 1.44** *Let $C = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ with codewords $c_1 = (1,1,1,1)$, $c_2 = (0,1,0,1)$, $c_3 = (1,0,1,0)$ and $c_4 = (0,0,0,0)$. The weights of the individual codewords are: $w(c_1) = 4$, $w(c_2) = 2$, $w(c_3) = 4$ and $w(c_4) = 0$.*

*The Hamming-distances for each pair of codewords are:*

- $d(c_1, c_2) = 2$
- $d(c_1, c_3) = 2$
- $d(c_1, c_4) = 4$
- $d(c_2, c_3) = 4$
- $d(c_2, c_4) = 2$
- $d(c_3, c_4) = 2$

*Therefore the minimum distance $d$ of $C$ is the smallest Hamming-distance which is* 2*.*

**Lemma 1.45 ([7])** *For $x, y \in \mathbb{F}_q^n$ (the finite field of $q-$elements)*

$$d(x, y) = w(x - y).$$

Note that in $\mathbb{F}_2^n$, $d(x, y) = w(x + y)$ also holds since the elements are modulo 2 (see example 1.38).

**Theorem 1.46 ([8])** *For a linear code $C$, the minimum distance is equal to the minimum weight.*

**Definition 1.47 ([7])** *The number of vectors in the basis of the subspace is called the dimension of $C$ and is denoted by $dim(C)$.*

**Definition 1.48 ([7])** *A q-ary linear code $C$ (binary if $q = 2$, ternary if $q = 3$) is a linear subspace of $\mathbb{F}_q^n$. If $C$ has dimension $k$ then $C$ is called an $[n, k]$ code.*

A $k-$dimensional linear code of length $n$ and minimum distance $d$ is often referred to as an $[n, k, d]$ code.

**Definition 1.49 ([7])** *Let $C$ be a linear $[n, k]$ code, then its' **weight enumerator** is defined to be the polynomial*

$$\begin{aligned} W_C(y) &= \sum_{i=0}^{n} A_i y_i \\ &= A_0 + A_1 y + \cdots + A_n y^n, \end{aligned}$$

*where each $A_i$ denotes the numbers of codewords in $C$ of weight $i$.*

**Definition 1.50 ([7])** *A generator matrix $G$ of a linear code $C$ is a $k \times n$ matrix for which the rows form a basis of $C$.*

We say that $G$ is in standard (or reduced echelon) form if $G = (I_k|A)$, where $I_k$ is the $k \times k$ identity matrix.

**Example 1.51** *Consider the code* $C = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$. *$C$ is not in standard form since the rows of $C$ are not linearly independent. Since $c_1$ and $c_4$ can be written in terms of $c_2$ and $c_3$ then* $C' = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ *is the $[4, 2, 2]$ generator matrix for $C$.*

There are inbuilt functions in `GAP` for finding the standard form of a given code:

**Listing 1.4: Standard form function in GAP**

```
gap> C1 := [[1,1,1,1],[1,0,1,0],[0,1,0,1],[0,0,0,0]];
[ [ 1, 1, 1, 1 ], [ 1, 0, 1, 0 ], [ 0, 1, 0, 1 ], [ 0, 0, 0, 0 ] ]
gap> C2 := GeneratorMatCode(C1,GF(2));
a linear [4,2,1..2]1..2 code defined by generator matrix over GF(2)
gap> G := MutableCopyMat(GeneratorMat(C2));;
gap> Display(G);
 1 1 1 1
 . 1 . 1
gap> PutStandardForm(G);;
gap> Display(G);
 1 . 1 .
 . 1 . 1
```

**Definition 1.52 ([7])** *Two linear codes over $\mathbb{F}_q$ are called equivalent if one can be obtained from another by the following operations:*

1. *permutations of the positions of the code*
2. *multiplication of symbols in a fixed position by a non-zero scalar in $\mathbb{F}_q$.*

**Theorem 1.53 ([7])** *Two $k \times n$ matrices are equivalent if one can be obtained from the other by a sequence of operations of the following types:*

*(R1) Exchanging of rows*

*(R2) Multiplication of a row by a non-zero element of $\mathbb{F}_q$*

*(R3) Adding a scalar multiple of one row to another*

*(C1) Exchanging of columns*

*(C2) Multiplication of a fixed column by a non-zero element of $\mathbb{F}_q$*

**Theorem 1.54 ([7])** *Let $G$ be a generator matrix of an $[n, k]$-code. Then by applying the operations described in theorem 1.53, $G$ can be transformed into an equivalent matrix of the form $(I_k|A)$ where $I_k$ is the $k \times k$ identity matrix and $A$ is a $k \times (n - k)$ matrix.*

**Example 1.55** *Consider the generator matrix*

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

*We can give $C$ in standard form $G = [I_k|A]$ by the following operations of type R3:*

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \begin{array}{l} \\ r_2 + r_1 \\ r_3 + r_1 \\ r_4 + r_1 \end{array}$$

$$\sim \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \begin{array}{l} r_1 + r_2 \\ \\ \\ \\ \end{array} \sim \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \begin{array}{l} \\ r_2 + r_3 \\ \\ \\ \end{array}$$

$$\sim \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \begin{array}{l} \\ \\ r_3 + r_4 \\ \\ \end{array}$$

We can confirm this result in GAP using the following code:

**Listing 1.5: Confirming Example 1.55 in GAP**

```
gap> C1:= [[1,1,1,1,1,1,1],[1,0,0,0,1,0,1],[1,1,0,0,0,1,0],[1,1,1,0,0,0,1]];;
gap> C2 := GeneratorMatCode(C1,GF(2));;
gap> G:=MutableCopyMat(GeneratorMat(C2));;
gap> Display(G);
 1 1 1 1 1 1 1
 . 1 1 1 . 1 .
 . . 1 1 1 . 1
 . . . 1 1 1 .
gap> PutStandardForm(G);;
gap> Display(G);
 1 . . . 1 . 1
 . 1 . . 1 1 1
 . . 1 . . 1 1
 . . . 1 1 1 .
```

This is the well known $[7, 4, 3]$ hamming code.

**Definition 1.56 ([7])** *The dual of a linear code $C \subset \mathbb{F}_q^n$ is another linear code defined to be*

$$C^{\perp} = \{x \in \mathbb{F}_q^n \mid \langle x, c \rangle = 0 \, \forall \, c \in C\},$$

*where $\langle x, c \rangle$ is the euclidean inner product given by*

$$\langle x, c \rangle = \sum_{i=1}^{n} x_i c_i.$$

In linear algebra this is actually the definition of a null space of $C$. There is a theorem known as the Rank Nullity theorem which tells us the dimension of the null space, or in this case $C^{\perp}$.

**Theorem 1.57 ([7])** *Let $C$ be a linear $[n,k]-$code over $\mathbb{F}_q$. Then, $C^{\perp}$ is a linear $[n, n-k]-$code.*

**Lemma 1.58** *Let $C$ be a linear code in $\mathbb{F}_q^n$ with generator matrix $G$. Then $x \in C^{\perp}$ if and only if $xG^T = 0$.*

**Definition 1.59 ([8])** *A linear code $C$ is said to be self-dual if it is equal to its own dual i.e. $C = C^{\perp}$.*

**Theorem 1.60 ([8])** *Let $C$ be a self-dual code of length $n$. Then $C$ is an $[n, \frac{n}{2}]$-code.*

**Proof.**
Since C is self-dual code then $C = C^{\perp}$ and by the rank nullity theorem we have

$$dim(C) + dim(C^{\perp}) = 2dim(C) = n$$

Therefore $dim(C) = \frac{n}{2}$.

■

**Theorem 1.61** *Let $C$ be a self-dual $[n, \frac{n}{2}]$-code with generator matrix $G = [I|A]$ then $AA^T = -I$, where $I$ is the $\frac{n}{2} \times \frac{n}{2}$ identity matrix.*

**Proof.** By Lemma 1.58, since $G$ consists of codewords which are orthogonal to every codeword in $G$ then we have

$$GG^T = 0 \Rightarrow \begin{pmatrix} I & A \end{pmatrix} \begin{pmatrix} I \\ A^T \end{pmatrix} = I^2 + AA^T = 0$$

Rearranging gives $AA^T = -I$ and when the elements are in $\mathbb{F}_2$, we have $AA^T = I$. ■

**Theorem 1.62 ([8])** *Let $C$ be an $[n, \frac{n}{2}, d]$ self-dual binary code. Then*

- $d \leq 4\lfloor \frac{n}{24} \rfloor + 4$, *if C is of Type II or C is Type I and* $n \not\equiv 22 \mod 24$
- $d \leq 4\lfloor \frac{n}{24} \rfloor + 6$, *if C is Type I and* $n \equiv 22 \mod 24$

Codes that achieve distance $d$ are called **extremal self-dual codes**.

# Chapter 2

# An Established Isomorphism

Let $R$ be a ring, $G$ be a group of order $n$, $RG$ be the group ring of $R$ over $G$ and $M_n(R)$ the ring of $n \times n$ matrices over $R$. In this second chapter we introduce a ring isomorphism from $RG$ to a subring of $M_n(R)$, first constructed by T. Hurley in [12]. This isomorphism is used to convert elements of group rings into matrix form which will be useful in Chapters 3 and 4.

**Definition 2.1 ([12])** *Let $\{g_1, g_2, ..., g_n\}$ be a fixed listing of the elements of the group $G$. Then the matrix*

$$M(G) = \begin{pmatrix} g_1^{-1}g_1 & g_1^{-1}g_2 & \cdots & g_1^{-1}g_n \\ g_2^{-1}g_1 & g_2^{-1}g_2 & \cdots & g_2^{-1}g_n \\ g_3^{-1}g_1 & g_3^{-1}g_2 & \cdots & g_3^{-1}g_n \\ \vdots & \vdots & \ddots & \vdots \\ g_n^{-1}g_1 & g_n^{-1}g_2 & \cdots & g_n^{-1}g_n \end{pmatrix}$$

*is called the matrix of $G$.*

**Example 2.2** *Consider the cyclic group of order 3, i.e. $C_3 = \{1, x, x^2\}$. Then, the matrix of $C_3$ is computed as follows:*

$$M(C_3) = \begin{pmatrix} 1 \cdot 1 & 1 \cdot x & 1 \cdot x^2 \\ x^2 \cdot 1 & x^2 \cdot x & x^2 \cdot x^2 \\ x \cdot 1 & x \cdot x & x \cdot x^2 \end{pmatrix} = \begin{pmatrix} 1 & x & x^2 \\ x^2 & 1 & x \\ x & x^2 & 1 \end{pmatrix}.$$

**Definition 2.3 ([12])** *Let $w = \sum_{i=1}^{n} a_{g_i} g_i \in RG$. Then, the following is called the RG-matrix of $w$:*

$$M(RG, w) = \begin{pmatrix} a_{g_1^{-1}g_1} & a_{g_1^{-1}g_2} & \cdots & a_{g_1^{-1}g_n} \\ a_{g_2^{-1}g_1} & a_{g_2^{-1}g_2} & \cdots & a_{g_2^{-1}g_n} \\ a_{g_3^{-1}g_1} & a_{g_3^{-1}g_2} & \cdots & a_{g_3^{-1}g_n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{g_n^{-1}g_1} & a_{g_n^{-1}g_2} & \cdots & a_{g_n^{-1}g_n} \end{pmatrix}.$$

**Example 2.4** *Let $RG$ be the group ring $\mathbb{F}_2C_3 = \{a_1 + a_2x + a_3x^2 \mid a_i \in \mathbb{F}_2\}$. Then,*

$$M(\mathbb{F}_2C_3, w) = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_3 & a_1 & a_2 \\ a_2 & a_3 & a_1 \end{pmatrix} = circ(a_1, a_2, a_3).$$

*Labelling the elements of $\mathbb{F}_2C_3$, calculated in Example 1.23, we have*

$$\mathbb{F}_2C_3 = \{\underset{w_1}{0}, \underset{w_2}{1}, \underset{w_3}{x}, \underset{w_4}{x^2}, \underset{w_5}{1+x}, \underset{w_6}{1+x^2}, \underset{w_7}{x+x^2}, \underset{w_8}{1+x+x^2}\}.$$

*So,*

| $w$ | $M(RG,w)$ | $w$ | $M(RG,w)$ |
|---|---|---|---|
| $0$ | $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ | $1+x$ | $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$ |
| $1$ | $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ | $1+x^2$ | $\begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ |
| $x$ | $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ | $x+x^2$ | $\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ |
| $x^2$ | $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ | $1+x+x^2$ | $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ |

Table 2.1: $RG$-matrix for $\mathbb{F}_2C_3$.

**Theorem 2.5 ([12])** *Given a listing of the elements of a group $G$ of order $n$ there is a bijective ring homomorphism between $RG$ and the $n \times n$ $G-$matrices over $R$. This bijective ring homomorphism is given by $\sigma : w \mapsto M(RG, w)$.*

**Proof.** Let $G = \{g_1, g_2, ..., g_n\}$ be the listing of the elements of $G$ and let $M$ denote the set of $G-$matrices relative to this listing. Now define the mapping $\sigma : RG \to M$ as follows. Suppose $w = \sum_{i=1}^{n} \alpha_{g_i} g_i$. Then

$$\sigma(w) = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \alpha_{g_1^{-1}g_3} & \cdots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \alpha_{g_2^{-1}g_3} & \cdots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \alpha_{g_n^{-1}g_3} & \cdots & \alpha_{g_n^{-1}g_n} \end{pmatrix}$$

This mapping is additive, surjective and injective. Therefore it is sufficient to show that $\sigma$ is multiplicative. So, consider $t = \sum_{i=1}^{n} \beta_{g_i} g_i$ and

$$\sigma(t) = \begin{pmatrix} \beta_{g_1^{-1}g_1} & \beta_{g_1^{-1}g_2} & \beta_{g_1^{-1}g_3} & \cdots & \beta_{g_1^{-1}g_n} \\ \beta_{g_2^{-1}g_1} & \beta_{g_2^{-1}g_2} & \beta_{g_2^{-1}g_3} & \cdots & \beta_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \beta_{g_n^{-1}g_1} & \beta_{g_n^{-1}g_2} & \beta_{g_n^{-1}g_3} & \cdots & \beta_{g_n^{-1}g_n} \end{pmatrix}.$$

Suppose $t * w = c$, where $c = \sum_{i=1}^{n} \gamma_{g_i} g_i$. Then

$$\sigma(t) * \sigma(w) = \begin{pmatrix} \gamma_{g_1^{-1}g_1} & \gamma_{g_1^{-1}g_2} & \gamma_{g_1^{-1}g_3} & \cdots & \gamma_{g_1^{-1}g_n} \\ \gamma_{g_2^{-1}g_1} & \gamma_{g_2^{-1}g_2} & \gamma_{g_2^{-1}g_3} & \cdots & \gamma_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \gamma_{g_n^{-1}g_1} & \gamma_{g_n^{-1}g_2} & \gamma_{g_n^{-1}g_3} & \cdots & \gamma_{g_n^{-1}g_n} \end{pmatrix},$$

which is of course $M(RG, c) = \sigma(t * w)$ as required. ■

The following results are extremely useful in identifying units and zero divisors of group rings. Checking matrix invertibility using a computer is quick and easy, since most computer software is designed to work with matrices.

**Theorem 2.6 ([12])** *Let $R$ be a ring containing an identity element. Then, $w \in RG$ is a unit in $RG$ if and only if $\sigma(w)$ is a unit in $R^{n\times n}$.*

**Proof.** Suppose $w$ is a unit in $RG$ and that $u$ is its inverse. Then $u * w = 1$ and hence $\sigma(w) * \sigma(u) = I_n$, the $n \times n$ identity matrix. Thus $\sigma(u) * \sigma(w) = I_n$. Similarly, $\sigma(w) * \sigma(u) = I_n$, and so $\sigma(w)$ is invertible in $\mathbb{R}^{n\times n}$.

Suppose now that $\sigma(w)$ is a unit in $\mathbb{R}^{n\times n}$ and let $B$ denote its inverse. Let $w = \alpha_{g_1}g_1 + \alpha_{g_2}g_2 + \cdots + \alpha_{g_n}g_n$. Then

$$\sigma(w) = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \alpha_{g_1^{-1}g_3} & \cdots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \alpha_{g_2^{-1}g_3} & \cdots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \alpha_{g_n^{-1}g_3} & \cdots & \alpha_{g_n^{-1}g_n} \end{pmatrix}.$$

We do not yet know that $B$ is an $RG-$matrix. Let $b = (\beta_1, \beta_2, ..., \beta_n)$ be the first row of $B$. Then

$$\begin{aligned} \beta_1\alpha_{g_1^{-1}g_1} + \beta_1\alpha_{g_2^{-1}g_1} + \beta_1\alpha_{g_3^{-1}g_1} + \cdots + \beta_1\alpha_{g_n^{-1}g_1} &= 1 \\ \beta_1\alpha_{g_1^{-1}g_2} + \beta_1\alpha_{g_2^{-1}g_2} + \beta_1\alpha_{g_3^{-1}g_2} + \cdots + \beta_1\alpha_{g_n^{-1}g_2} &= 0 \\ \vdots \quad + \quad \vdots \quad + \quad \vdots \quad + \vdots + \quad \vdots \quad &= \vdots \\ \beta_1\alpha_{g_1^{-1}g_n} + \beta_1\alpha_{g_2^{-1}g_n} + \beta_1\alpha_{g_3^{-1}g_n} + \cdots + \beta_1\alpha_{g_n^{-1}g_n} &= 0 \end{aligned}$$

Now, $w = \alpha_{g_1}g_1 + \alpha_{g_2}g_2 + \cdots + \alpha_{g_n}g_n = \alpha_{g_i^{-1}g_1}g_i^{-1}g_1 + \alpha_{g_i^{-1}g_2}g_i^{-2}g_2 + \cdots + \alpha_{g_i^{-1}g_n}g_i^{-n}g_n$ for each $i, 1 \leq i \leq n$.

Define $u = \beta_1 g_1 + \beta_2 g_2 + \cdots \beta_n g_n$. Then:

$$\begin{aligned} \beta_i g_i(\alpha_{g_1}g_1 + \alpha_{g_2}g_2 + \cdots + \alpha_{g_n}g_n) &= \beta_i g_i \alpha_{g_i^{-1}g_1}g_i^{-1}g_1 + \beta_i g_i \alpha_{g_i^{-1}g_2}g_i^{-1}g_2 + \cdots + \beta_i g_i \alpha_{g_i^{-1}g_n}g_i^{-1}g_n \\ &= \beta_i \alpha_{g_i^{-1}g_1}g_1 + \beta_i \alpha_{g_i^{-1}g_2}g_2 + \cdots + \beta_i \alpha_{g_i^{-1}g_n}g_n. \end{aligned}$$

Hence:

$$\begin{aligned} u * w &= (\beta_1 g_1 + \beta_2 g_2 + ... + \beta_n g_n)(\alpha_{g_1}g_1 + \alpha_{g_2}g_2 + ... + \alpha_{g_n}g_n) \\ &= \beta_1 g_1 \alpha_{g_1^{-1}g_1}g_1^{-1}g_1 + \beta_2 g_2 \alpha_{g_2^{-1}g_1}g_2^{-1}g_1 + \cdots + \beta_n g_n \alpha_{g_n^{-1}g_1}g_n^{-1}g_1 + \\ &\quad + \beta_1 g_1 \alpha_{g_1^{-1}g_2}g_1^{-1}g_2 + \beta_2 g_2 \alpha_{g_2^{-1}g_2}g_2^{-1}g_2 + \cdots + \beta_n g_n \alpha_{g_n^{-1}g_2}g_n^{-1}g_2 + \\ &\quad + \cdots + \beta_1 g_1 \alpha_{g_1^{-1}g_n}g_1^{-1}g_n + \beta_2 g_2 \alpha_{g_2^{-1}g_n}g_2^{-1}g_n + \cdots + \beta_n g_n \alpha_{g_n^{-1}g_n}g_n^{-1}g_n \\ &= \beta_1 \alpha_{g_1^{-1}g_1}g_1 + \beta_2 \alpha_{g_2^{-1}g_1}g_1 + \cdots + \beta_n \alpha_{g_n^{-1}g_1}g_1 + \\ &\quad + \beta_1 \alpha_{g_1^{-1}g_2}g_2 + \beta_2 \alpha_{g_2^{-1}g_2}g_2 + \cdots + \beta_n \alpha_{g_n^{-1}g_2}g_2 + \\ &\quad + \cdots + \beta_1 \alpha_{g_1^{-1}g_n}g_n + \beta_2 \alpha_{g_2^{-1}g_n}g_n + \cdots + \beta_n \alpha_{g_n^{-1}g_n}g_n \end{aligned}$$

which is $g_1$ from the above. Thus $g_1^{-1} * u$ is the inverse of $w$ and $w$ is a unit in $RG$. ■

**Corollary 2.7 ([12])** *When $R$ is commutative, $w$ is a unit in $RG$ if and only if $\sigma(w)$ is a unit in $R^{n \times n}$ if and only if* $\det(\sigma(w))$ *is a unit in $R$.*

**Corollary 2.8 ([12])** *An element $w \in RG$ is a zero divisor if and only if $\sigma(w)$ is a zero divisor in $R^{n \times n}$.*

**Theorem 2.9 ([12])** *When $R$ is a field, $w \neq 0$ in $RG$ is either a unit or a zero divisor, depending on whether* $\det(\sigma(w)) \neq 0$ *or* $\det(\sigma(w)) = 0$.

We will now use some of the previous results to find the units and zero divisors of $\mathbb{F}_2 C_4$.

**Example 2.10** *Let $w = \sum_{i=0}^{3} a_i x^i \in \mathbb{F}_2C_4$, where $a_i \in \mathbb{F}_2$. Using Corollary's 2.7 and 2.8, we can determine the units and zero divisors in $\mathbb{F}_2C_4$ by checking the determinant of $\sigma(w)$ mod 2.*

| $w$ | $\sigma(w)$ | $\lvert\sigma(w)\rvert$ | Unit/ZD | $w$ | $\sigma(w)$ | $\lvert\sigma(w)\rvert$ | Unit/ZD |
|---|---|---|---|---|---|---|---|
| $0$ | circ$[0,0,0,0]$ | 0 | ZD | $x^3$ | circ$[0,0,0,1]$ | 1 | Unit |
| $x^2$ | circ$[0,0,1,0]$ | 1 | Unit | $x^2+x^3$ | circ$[0,0,1,1]$ | 0 | ZD |
| $x$ | circ$[0,1,0,0]$ | 1 | Unit | $x+x^3$ | circ$[0,1,0,1]$ | 0 | ZD |
| $x+x^2$ | circ$[0,1,1,0]$ | 0 | ZD | $x+x^2+x^3$ | circ$[0,1,1,1]$ | 1 | Unit |
| $1$ | circ$[1,0,0,0]$ | 1 | Unit | $1+x^3$ | circ$[1,0,0,1]$ | 0 | ZD |
| $1+x^2$ | circ$[1,0,1,0]$ | 0 | ZD | $1+x^2+x^3$ | circ$[1,0,1,1]$ | 1 | Unit |
| $1+x$ | circ$[1,1,0,0]$ | 0 | ZD | $1+x^2+x^3$ | circ$[1,1,0,1]$ | 1 | Unit |
| $1+x+x^2$ | circ$[1,1,1,0]$ | 1 | Unit | $1+x+x^2+x^3$ | circ$[1,1,1,1]$ | 0 | ZD |

Table 2.2: Units and zero divisors for $\mathbb{F}_2C_4$.

*This is verified in* `GAP`*, using a custom function* `UnitOrZDTable(n)` *where n denotes the order of the cyclic group. The source code can be found in Appendices A.1 and A.3.*

**Listing 2.1: Units and Zero Divisors for $\mathbb{F}_2C_4$.**

```
gap> Read("/home/harrison/.../MatrixFunctions.g"); # import Circulant() & Tidy()
gap> Read("/home/harrison/.../ZeroDivisorTable.g"); # import UnitOrZDTable()
gap> UnitOrZDTable(4);
Circ()              Det()       Unit/ZeroDivisor
[ 0, 0, 0, 0 ]          0           Zero Divisor
[ 0, 0, 0, 1 ]          1           Unit
[ 0, 0, 1, 0 ]          1           Unit
[ 0, 0, 1, 1 ]          0           Zero Divisor
[ 0, 1, 0, 0 ]          1           Unit
[ 0, 1, 0, 1 ]          0           Zero Divisor
[ 0, 1, 1, 0 ]          0           Zero Divisor
[ 0, 1, 1, 1 ]          1           Unit
[ 1, 0, 0, 0 ]          1           Unit
[ 1, 0, 0, 1 ]          0           Zero Divisor
[ 1, 0, 1, 0 ]          0           Zero Divisor
[ 1, 0, 1, 1 ]          1           Unit
[ 1, 1, 0, 0 ]          0           Zero Divisor
[ 1, 1, 0, 1 ]          1           Unit
[ 1, 1, 1, 0 ]          1           Unit
[ 1, 1, 1, 1 ]          0           Zero Divisor
```

# Chapter 3

# Units of $\mathbb{F}_{2^k}D_8$

In this chapter we will study the units of $\mathbb{F}_{2^k}D_8$, first constructed by Creedon and Gildea [4]. The original paper omits the details of the proofs, we aim to fill these gaps by proving the majority of results using an alternative, matrix-based approach.

## 3.1 Constructing a Ring Homomorphism

Let $D_8 = \langle x, y \mid x^4 = y^2 = (xy)^2 = 1\rangle$ be the dihedral group of order 8 and $\alpha = \sum_{i=0}^{3} x^i(a_i + a_{i+4}y)$, $a_i \in \mathbb{F}_{2^k}$ be an element of the group algebra $\mathbb{F}_{2^k}D_8$. We shall begin by constructing a ring homomorphism $\mathbb{F}_{2^k}D_8 \to \mathbb{F}_{2^k}C_2$, which we will then restrict to the group homomorphism $\mathcal{U}(\mathbb{F}_{2^k}D_8) \to \mathcal{U}(\mathbb{F}_{2^k}C_2)$. Later we will see that this can be used to construct a certain split extension.

**Proposition 3.1 ([4])** *There exists a mapping $\theta : \mathbb{F}_{2^k}D_8 \to \mathbb{F}_{2^k}C_2$ such that for $\alpha \in \mathbb{F}_{2^k}D_8$, we have*

$$\theta(\alpha) = \theta\left(\sum_{i=0}^{3} x^i(a_i + a_{i+4}y)\right) = \sum_{i=0}^{3} a_i + a_{i+4}\bar{y} \in \mathbb{F}_{2^k}C_2,$$

*where $\bar{y}$ is the generator of $C_2$. This mapping satisfies the two conditions for being a ring homomorphism.*

**Proof.** Let $\alpha = \sum_{i=0}^{3} x^i(a_i + a_{i+4}y) \in \mathbb{F}_{2^k}D_8$, $\beta = \sum_{i=0}^{3} x^i(b_i + b_{i+4}y) \in \mathbb{F}_{2^k}D_8$. Then,

$$\begin{aligned}\theta(\alpha+\beta) &= \theta\left(\sum_{i=0}^{3} x^i\left((a_i+b_i) + (a_{i+4}+b_{i+4})y\right)\right)\\ &= \sum_{i=0}^{3}(a_i+b_i) + (a_{i+4}+b_{i+4})\bar{y}\\ &= \sum_{i=0}^{3} a_i + a_{i+4}\bar{y} + \sum_{i=0}^{3} b_i + b_{i+4}\bar{y}\\ &= \theta(\alpha) + \theta(\beta).\end{aligned}$$

$$\begin{aligned}
\theta(\alpha\beta) = \theta\big(&a_0b_0 + a_0b_4y + a_4b_0y + a_4b_4 + a_0b_1x + a_0b_5xy + a_4b_1x^3y + a_4b_5x^3 \\
&+ a_0b_2x^2 + a_0b_6x^2y + a_4b_2x^2y + a_4b_6x^2 + a_0b_3x^3 + a_0b_7x^3y + a_4b_3xy + a_4b_7x \\
&+ a_1b_0x + a_1b_4xy + a_5b_0xy + a_5b_4x + a_1b_1x^2 + a_1b_5x^2y + a_5b_1y + a_5b_5 \\
&+ a_1b_2x^3 + a_1b_6x^3y + a_5b_2x^3y + a_5b_6x^3 + a_1b_3 + a_1b_7y + a_5b_3x^2y + a_5b_7x^2 \\
&+ a_2b_0x^2 + a_2b_4x^2y + a_6b_0x^2y + a_6b_4x^2 + a_2b_1x^3 + a_2b_5x^3y + a_6b_1xy + a_6b_5x \\
&+ a_2b_2 + a_2b_6y + a_6b_2y + a_6b_6 + a_2b_3x + a_2b_7xy + a_6b_3x^3y + a_6b_7x^3 \\
&+ a_3b_0x^3 + a_3b_4x^3y + a_7b_0x^3y + a_7b_4x^3 + a_3b_1 + a_3b_5y + a_7b_1x^2y + a_7b_5x^2 \\
&+ a_3b_2x + a_3b_6xy + a_7b_2xy + a_7b_6x + a_3b_3x^2 + a_3b_7x^2y + a_7b_3y + a_7b_7\big) \\
= \big(&a_0b_0 + a_0b_1 + a_0b_2 + a_0b_3 + a_1b_0 + a_1b_1 + a_1b_2 + a_1b_3 + a_2b_0 + a_2b_1 + a_2b_2 + a_2b_3 \\
&+ a_3b_0 + a_3b_1 + a_3b_2 + a_3b_3 + a_4b_4 + a_4b_5 + a_4b_6 + a_4b_7 + a_5b_4 + a_5b_5 + a_5b_6 + a_5b_7 \\
&+ a_6b_4 + a_6b_5 + a_6b_6 + a_6b_7 + a_7b_4 + a_7b_5 + a_7b_6 + a_7b_7\big) \cdot 1 \\
&+ \big(a_0b_4 + a_0b_5 + a_0b_6 + a_0b_7 + a_1b_4 + a_1b_5 + a_1b_6 + a_1b_7 + a_2b_4 + a_2b_5 + a_2b_6 + a_2b_7 \\
&+ a_3b_4 + a_3b_5 + a_3b_6 + a_3b_7 + a_4b_0 + a_4b_1 + a_4b_2 + a_4b_3 + a_5b_0 + a_5b_1 + a_5b_2 + a_5b_3 \\
&+ a_6b_0 + a_6b_1 + a_6b_2 + a_6b_3 + a_7b_0 + a_7b_1 + a_7b_2 + a_7b_3\big) \cdot \bar{y} \\
= &\sum_{i=0}^{3}\sum_{j=0}^{3}\left(a_ib_j + a_{i+4}b_{j+4}\right) + \bar{y}\sum_{i=0}^{3}\sum_{j=0}^{3}\left(a_ib_{j+4} + a_{i+4}b_j\right) \\
= &\left(\sum_{i=0}^{3} a_i + a_{i+4}\bar{y}\right)\left(\sum_{j=0}^{3} b_j + b_{j+4}\bar{y}\right) \\
= &\theta(\alpha)\theta(\beta).
\end{aligned}$$

Therefore, $\theta$ is a ring homomorphism. ■

**Proposition 3.2 ([4])** *Let the restricted mapping $\theta' : \mathcal{U}(\mathbb{F}_{2^k}D_8) \to \mathcal{U}(\mathbb{F}_{2^k}C_2)$ be a group homomorphism. Then $\mathcal{U}(\mathbb{F}_{2^k}D_8)$ is a split extension of $\mathcal{U}(\mathbb{F}_{2^k}C_2)$ by $K = \ker(\theta')$ i.e. $\mathcal{U}(\mathbb{F}_{2^k}D_8) \cong K \rtimes \mathcal{U}(\mathbb{F}_{2^k}C_2)$.*

**Proof.** Define the group homomorphism $\varphi : \mathcal{U}(\mathbb{F}_{2^k}C_2) \to \mathcal{U}(\mathbb{F}_{2^k}D_8)$, where $a + b\bar{y} \mapsto a + by$. Then, for $\alpha = a + b\bar{y}$ we have

$$\begin{aligned}
\theta' \circ \varphi(\alpha) &= \theta' \circ \varphi(a + b\bar{y}) \\
&= \theta'(a + by) \\
&= a + b\bar{y} \\
&= \alpha.
\end{aligned}$$

Thus, $\theta' \circ \varphi$ is the identity mapping and by Definition 1.35 we find that $\mathcal{U}(\mathbb{F}_{2^k}D_8)$ is a split extension of $\mathcal{U}(\mathbb{F}_{2^k}C_2)$ by $K$. ■

## 3.2 Calculating the Exponent of the Kernel

At this point, we will show that $K$ has exponent 4 and define an abelian subgroup of $K$, which we will call $H$.

**Proposition 3.3 ([4])** *The kernel of the group homomorphism $\theta'$ has exponent* 4.

**Proof.**
Let $\alpha = 1 + \sum_{i=1}^{3}\left(a_i(1+x^i) + b_i(1+x^i)y\right) \in K$. Then

$$\sigma(\alpha) = \begin{pmatrix} I+A & B \\ B^T & (I+A)^T \end{pmatrix},$$

where $A = \text{circ}[a_1+a_2+a_3, a_1, a_2, a_3]$ and $B = \text{circ}[b_1+b_2+b_3, b_1, b_2, b_3]$. Now,

$$\begin{aligned}
(\sigma(\alpha))^2 &= \begin{pmatrix} I+A & B \\ B^T & (I+A)^T \end{pmatrix}^2 \\
&= \begin{pmatrix} (I+A)(I+A)+BB^T & (I+A)B+B(I+A^T) \\ B^T(I+A)+(I+A^T)B^T & BB^T+(I+A^T)(I+A^T) \end{pmatrix} \\
&= \begin{pmatrix} I+A^2+BB^T & AB+BA^T \\ B^TA+A^TB^T & BB^T+I+(A^T)^2 \end{pmatrix} \\
&= \begin{pmatrix} I+X & Y \\ Y & I+X \end{pmatrix},
\end{aligned}$$

where

$$\begin{aligned}
X &= \text{circ}[a_1^2+a_3^2,\ b_1^2+b_3^2,\ a_1^2+a_3^2,\ b_1^2+b_3^2] \\
&= \text{circ}[\gamma_1,\ \gamma_2,\ \gamma_1,\ \gamma_2], \\
Y &= \text{circ}[(b_1+b_3)(a_1+a_3),\ (b_1+b_3)(a_1+a_3),\ (b_1+b_3)(a_1+a_3),\ (b_1+b_3)(a_1+a_3)] \\
&= \text{circ}[\gamma_3,\ \gamma_3,\ \gamma_3,\ \gamma_3].
\end{aligned}$$

We can immediately see that the exponent of $K$ is not 2. Squaring once more we have

$$\begin{aligned}
(\sigma(\alpha))^4 &= \begin{pmatrix} I+X & Y \\ Y & I+X \end{pmatrix}^2 \\
&= \begin{pmatrix} (I+X)^2+Y^2 & (I+X)Y+Y(I+X) \\ Y(I+X)+(I+X)Y & Y^2+(I+X)^2 \end{pmatrix} \\
&= \begin{pmatrix} I^2+X^2+Y^2 & Y+XY+Y+YX \\ Y+YX+Y+XY & I^2+X^2+Y^2 \end{pmatrix} \\
&= \begin{pmatrix} I+X^2+Y^2 & 0 \\ 0 & I+X^2+Y^2 \end{pmatrix} \quad (\text{since } XY=YX)
\end{aligned}$$

Let $J_4$ be the $4 \times 4$ matrix of ones, then notice that the $Y^2$ terms disappear since $Y^2 = (\gamma_3 J_4)^2 = 4\gamma_3^2 J = 0$. Then, letting $X = \begin{pmatrix} \beta & \beta \\ \beta & \beta \end{pmatrix}$ with $\beta = \text{circ}[\gamma_1, \gamma_2]$ gives

$$X^2 = \begin{pmatrix} 2\beta^2 & 2\beta^2 \\ 2\beta^2 & 2\beta^2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Therefore,

$$\begin{aligned}(\sigma(\alpha))^4 &= \begin{pmatrix} I + X^2 + Y^2 & 0 \\ 0 & I + X^2 + Y^2 \end{pmatrix} \\ &= \begin{pmatrix} I + 0 + 0 & 0 \\ 0 & I + 0 + 0 \end{pmatrix} \\ &= \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix}.\end{aligned}$$

Thus, $K$ has exponent 4. ■

## 3.3 Constructing a Subgroup $H$ and a Normal Subgroup $N$

**Proposition 3.4 ([4])** *Let $H = \{1 + \sum_{i=1}^{3} a_i(1 + x^i)(1 + y) \mid a_i \in \mathbb{F}_{2^k}\}$ be a subset of $K$. Then $H$ is an abelian subgroup of $K$.*

**Proof.** To show that $H$ is a subgroup, it is sufficient to check that $H$ is closed with respect to multiplication. So, let $h_1 = 1 + \sum_{i=1}^{3} a_i(1 + x^i)(1 + y)$, $h_2 = 1 + \sum_{i=1}^{3} b_i(1 + x^i)(1 + y) \in H$. Then

$$\sigma(h_1) = \begin{pmatrix} I + B & B \\ B^T & (I + B)^T \end{pmatrix}, \quad \sigma(h_2) = \begin{pmatrix} I + D & D \\ D^T & (I + D)^T \end{pmatrix},$$

where $B = \text{circ}[a_1 + a_2 + a_3,\ a_1,\ a_2,\ a_3]$, $D = \text{circ}[b_1 + b_2 + b_3,\ b_1,\ b_2,\ b_3]$. Now,

$$\begin{aligned}\sigma(h_1)\sigma(h_2) &= \begin{pmatrix} I + B & B \\ B^T & (I + B)^T \end{pmatrix} \begin{pmatrix} I + D & D \\ D^T & (I + D)^T \end{pmatrix} \\ &= \begin{pmatrix} (I + B)(I + D) + BD^T & (I + B)D + B(I + D^T) \\ B^T(I + D) + (I + B^T)D^T & B^T D + (I + B^T)(I + D^T) \end{pmatrix} \\ &= \begin{pmatrix} I + D + B + BD + BD^T & D + B + BD + BD^T \\ D^T + B^T + B^T D + B^T D^T & I + D^T + B^T + B^T D + B^T D^T \end{pmatrix} \\ &= \begin{pmatrix} I + D + B + BD + BD^T & D + B + BD + BD^T \\ D^T + B^T + DB^T + D^T B^T & I + D^T + B^T + DB^T + D^T B^T \end{pmatrix} \\ &= \begin{pmatrix} I + D + B + BD + BD^T & D + B + BD + BD^T \\ (D + B + BD + BD^T)^T & (I + D + B + BD + BD^T)^T \end{pmatrix} \in H.\end{aligned}$$

Therefore $H$ is closed, and a subgroup of $K$. Next, we need to show that $\sigma(h_1)\sigma(h_2) = \sigma(h_2)\sigma(h_1)$.

Note $DB^T = (DB^T)^T = BD^T$, $D^TB = (D^TB)^T = B^TD = DB^T$ and that circulant matrices commute, then we have

$$\begin{aligned}\sigma(h_2)\sigma(h_1) &= \begin{pmatrix} I+D & D \\ D^T & (I+D)^T \end{pmatrix}\begin{pmatrix} I+B & B \\ B^T & (I+B)^T \end{pmatrix}\\ &= \begin{pmatrix} (I+D)(I+B)+DB^T & (I+D)B+D(I+B)^T \\ D^T(I+B)+(I+D)^TB^T & D^TB+(I+D)^T(I+B)^T \end{pmatrix}\\ &= \begin{pmatrix} I+D+B+DB+DB^T & D+B+DB+DB^T \\ B^T+D^T+D^TB+D^TB^T & I+B^T+D^T+D^TB+D^TB^T \end{pmatrix}\\ &= \begin{pmatrix} I+D+B+BD+BD^T & D+B+BD+BD^T \\ B^T+D^T+DB^T+D^TB^T & I+B^T+D^T+DB^T+D^TB^T \end{pmatrix}\\ &= \begin{pmatrix} I+D+B+BD+BD^T & D+B+BD+BD^T \\ (B+D+BD^T+BD)^T & (I+B+D+BD^T+BD)^T \end{pmatrix}\\ &= \sigma(h_1)\sigma(h_2).\end{aligned}$$

Thus, $H$ is an abelian subgroup. ■

**Proposition 3.5 ([4])** *Let $N$ be the set of elements of $K$ of the form*

$$1+p(x+x^3)+q(1+x^3)y+r(x+x^2)y$$

*where $p,q,r\in\mathbb{F}_{2^k}$. Then $N$ is an abelian subgroup of $K$.*

**Proof.**
Let $n_1 = 1+p_1(x+x^3)+q_1(1+x^3)y+r_1(x+x^3)y \in N$ and $n_2 = 1+p_2(x+x^3)+q_2(1+x^3)y+r_2(x+x^3)y \in N$. Then

$$\begin{aligned}\sigma(n_1)\sigma(n_2) &= \begin{pmatrix} A & B \\ B^T & A \end{pmatrix}\begin{pmatrix} C & D \\ D^T & C \end{pmatrix}\\ &= \begin{pmatrix} AC+BD^T & AD+BC \\ B^TC+AD^T & B^TD+AC \end{pmatrix},\end{aligned}$$

where $A=\text{circ}[1,p_1,0,p_1], B=\text{circ}[q_1,r_1,r_1,q_1], C=\text{circ}[1,p_2,0,p_2]$ and $D=\text{circ}[q_2,r_2,r_2,q_2]$.

Note that the product of two circulant matrices is itself circulant. Then, considering $AC, BD^T, AD$ and $BC$ separately, we need only find the first row of each result.

$$\begin{aligned}AC &= \text{circ}[(1,p_1,0,p_1)\cdot\text{circ}[1,p_2,0,p_2]]\\ &= \text{circ}[1+p_1p_2+p_1p_2, p_1+p_2, p_1p_2+p_1p_2, p_1+p_2]\\ &= \text{circ}[1,p_1+p_2,0,p_1+p_2]\\ &= \text{circ}[1,\alpha,0,\alpha].\end{aligned}$$

Let $x = \text{circ}[x_1, x_2, x_3, ..., x_n]$ be a circulant matrix, then its' transpose is $x^T = \text{circ}[x_1, x_n, ..., x_3, x_2]$. That is, with the exception of the first element, the order is reversed. So, $D^T = (\text{circ}[q_2, r_2, r_2, q_2])^T = \text{circ}[q_2, q_2, r_2, r_2]$ and we have

$$\begin{aligned} BD^T &= \text{circ}[(q_1, r_1, r_1, q_1) \cdot \text{circ}[q_2, q_2, r_2, r_2]] \\ &= \text{circ}[q_1q_2 + r_1r_2 + r_1r_2 + q_1q_2, q_1q_2 + r_1q_2 + r_1r_2 + q_1r_2, \\ &\qquad\qquad q_1r_2 + r_1q_2 + r_1q_2 + q_1r_2, q_1r_2 + r_1r_2 + r_1q_2 + q_1q_2] \\ &= \text{circ}[0, (q_1 + r_1)(q_2 + r_2), 0, (q_1 + r_1)(q_2 + r_2)] \\ &= \text{circ}[0, \beta, 0, \beta]. \end{aligned}$$

Therefore, $AC + BD^T = \text{circ}[1, \alpha, 0, \alpha] + \text{circ}[0, \beta, 0, \beta] = \text{circ}[1, \alpha + \beta, 0, \alpha + \beta]$, which is of the correct form, i.e. the first element is 1, the third is 0 and the second and fourth are identical. Now,

$$\begin{aligned} AD &= \text{circ}[(1, p_1, 0, p_1) \cdot \text{circ}[q_2, r_2, r_2, q_2]] \\ &= \text{circ}[q_2 + p_1q_2 + p_1r_2, r_2 + p_1q_2 + p_1r_2, r_2 + p_1r_2 + p_1q_2, q_2 + p_1r_2 + p_1q_2] \\ &= \text{circ}[\gamma, \delta, \delta, \gamma]. \end{aligned}$$

$$\begin{aligned} BC &= \text{circ}[(q_1, r_1, r_1, q_1) \cdot \text{circ}[1, p_2, 0, p_2]] \\ &= \text{circ}[q_1 + r_1p_1 + q_1p_1, q_1p_1 + r_1 + r_1p_1, r_1p_1 + r_1 + q_1p_1, q_1p_1 + r_1p_1 + q_1] \\ &= \text{circ}[\lambda, \mu, \mu, \lambda]. \end{aligned}$$

Therefore $AD + BC = \text{circ}[\gamma, \delta, \delta, \gamma] + \text{circ}[\lambda, \mu, \mu, \lambda] = \text{circ}[\gamma + \lambda, \delta + \mu, \delta + \mu, \gamma + \lambda]$, which is also of the desired form, since the first and last entries are equal, along with the second and third.

Observe that $BD^T$ is equal to its own transpose, so

$$AC + BD^T = AC + (BD^T)^T = AC + DB^T = AC + B^TD.$$

Also,

$$(AC + BC)^T = D^TA^T + C^TB^T = D^TA + CB^T = AD^T + B^TC.$$

Therefore,

$$\sigma(n_1)\sigma(n_2) = \begin{pmatrix} AC + BD^T & AD + BC \\ (AD + BC)^T & AC + BD^T \end{pmatrix} \in N.$$

In order to prove that $N$ is abelian we must show that $\sigma(n_1)\sigma(n_2) = \sigma(n_2)\sigma(n_1)$. Note again that circulant matrices commute and that $BD^T = \text{circ}[0, \beta, 0, \beta] = (BD^T)^T = B^TD$. Then,

$$\begin{aligned}
\sigma(n_2)\sigma(n_1) &= \begin{pmatrix} C & D \\ D^T & C \end{pmatrix}\begin{pmatrix} A & B \\ B^T & A \end{pmatrix} \\
&= \begin{pmatrix} CA + DB^T & CB + DA \\ D^TA + CB^T & D^TB + CA \end{pmatrix} \\
&= \begin{pmatrix} AC + BD^T & AD + BC \\ B^TC + AD^T & B^TD + AC \end{pmatrix} \\
&= \sigma(n_1)\sigma(n_2).
\end{aligned}$$

Thus, $N$ is an abelian subgroup. ■

**Proposition 3.6 ([4])** *$N$ is a normal subgroup of $K$.*

**Proof.** In order to be a normal subgroup, $n^k = k^{-1}nk \in N$ for all $n \in N, k \in K$. We have already seen that $K = NH$, so our problem can be considered as $n^{nh} \in N$ for all $n \in N, h \in H$. Now, since $N$ is a subgroup, $n^n \in N$, so it remains to show that $n^h \in N$.

Let $h = 1 + \sum_{i=1}^{3} a_i(1 + x^i)(1 + y) \in H$. Then,

$$\sigma(h) = \begin{pmatrix} I + A & A \\ A^T & (I + A)^T \end{pmatrix}, \quad A = \mathrm{circ}[a_1 + a_2 + a_3, a_1, a_2, a_3].$$

We have shown in Proposition 3.3 that the exponent of $K$ is 4, which means that $H \subseteq K$ also has exponent 4, i.e. for any $h \in H$, $h^{-1} = h^3$. So, our next step is to calculate $(\sigma(h))^3$.

Recall from the proof of Proposition 3.3, that for $\alpha = 1 + \sum_{i=1}^{3} \left(a_i(1 + x^i) + b_i(1 + x^i)y\right) \in K$ we had

$$(\sigma(\alpha))^2 = \begin{pmatrix} I + X & Y \\ Y & I + X \end{pmatrix},$$

where $X = \mathrm{circ}[a_1^2 + a_3^2, b_1^2 + b_3^2, a_1^2 + a_3^2, b_1^2 + b_3^2]$ and $Y = (b_1 + b_3)(a_1 + a_3)J_4$.

Now, $H$ is a subset of $K$ such that $a_i = b_i$. Therefore, replacing $b_i$ with $a_i$ in $X$ and $Y$ we get

$$(\sigma(h))^2 = \begin{pmatrix} I + B & C \\ C & I + B \end{pmatrix}$$

with

$$\begin{aligned}
B &= (a_1^2 + a_3^2)J_4, \\
C &= (a_1 + a_3)^2 J_4 = (a_1^2 + a_3^2)J_4.
\end{aligned}$$

As you can see, $B$ and $C$ are identical, so

$$\begin{aligned}(\sigma(h))^3 &= \begin{pmatrix} I+B & B \\ B & I+B \end{pmatrix}\begin{pmatrix} I+A & A \\ A^T & (I+A)^T \end{pmatrix} \\ &= \begin{pmatrix} (I+B)(I+A)+BA^T & (I+B)A+B(I+A)^T \\ B(I+A)+(I+B)A^T & BA+(I+B)(I+A)^T \end{pmatrix} \\ &= \begin{pmatrix} I+A+B+BA+BA^T & A+B+BA+BA^T \\ A^T+B+BA+BA^T & I+A^T+B+BA+BA^T \end{pmatrix}.\end{aligned}$$

Multiplying any matrix by $B=(a_1^2+a_3^2)J_4$ will give zero, therefore we have

$$(\sigma(h))^3 = \begin{pmatrix} I+A+B & A+B \\ A^T+B & I+A^T+B \end{pmatrix}.$$

Now,

$$\begin{aligned}(\sigma(h))^3\sigma(n)\sigma(h) &= \begin{pmatrix} I+A+B & A+B \\ A^T+B & I+A^T+B \end{pmatrix}\begin{pmatrix} N_1 & N_2 \\ N_2^T & N_1 \end{pmatrix}\begin{pmatrix} I+A & A \\ A^T & (I+A)^T \end{pmatrix} \\ &= \left[\begin{pmatrix} B & B \\ B & B \end{pmatrix} + \begin{pmatrix} I+A & A \\ A^T & (I+A)^T \end{pmatrix}\right]\begin{pmatrix} N_1 & N_2 \\ N_2^T & N_1 \end{pmatrix}\begin{pmatrix} I+A & A \\ A^T & (I+A)^T \end{pmatrix} \\ &= \left[\begin{pmatrix} B & B \\ B & B \end{pmatrix} + \begin{pmatrix} I+A & A \\ A^T & (I+A)^T \end{pmatrix}\right]\begin{pmatrix} N_1+N_1A+N_2A^T & N_2+N_1A+N_2A^T \\ N_2^T+N_1A^T+N_2^TA & N_1+N_1A^T+N_2^TA \end{pmatrix}\end{aligned} \tag{3.1}$$

Matrices are associative, so we can split Equation (3.1) into two parts. First we get

$$\begin{pmatrix} B & B \\ B & B \end{pmatrix}\begin{pmatrix} N_1+N_1A+N_2A^T & N_2+N_1A+N_2A^T \\ N_2^T+N_1A^T+N_2^TA & N_1+N_1A^T+N_2^TA \end{pmatrix} = \begin{pmatrix} B & B \\ B & B \end{pmatrix}, \tag{3.2}$$

since

$$\begin{aligned} BN_1(I+A+A^T) &= B\cdot \mathrm{circ}[1,p,0,p]\cdot \mathrm{circ}[1,a_1+a_3,0,a_1+a_3] \\ &= B\cdot \mathrm{circ}[1,a_1+a_3+p,0,a_1+a_3+p] \\ &= \mathrm{circ}[a_1^2+a_3^2,a_1^2+a_3^2,a_1^2+a_3^2,a_1^2+a_3^2] \\ &= B \\ BN_2^T(I+A) &= B\cdot \mathrm{circ}[q,q,r,r]\cdot \mathrm{circ}[1+a_1+a_2+a_3,a_1,a_2,a_3] \\ &= B\cdot \mathrm{circ}[\alpha+q,\beta+q,\alpha+r,\beta+r], \quad \alpha=(a_1+a_2)(q+r), \beta=(a_2+a_3)(q+r) \\ &= 0 \\ BN_2(I+A^T) &= B\cdot \mathrm{circ}[q,r,r,q]\cdot \mathrm{circ}[1+a_1+a_2+a_3,a_3,a_2,a_1] \\ &= B\cdot \mathrm{circ}[\alpha+q,\beta+r,\alpha+r,\beta+q], \quad \alpha=(a_1+a_2)(q+r), \beta=(a_2+a_3)(q+r) \\ &= 0 \end{aligned}$$

$$\begin{aligned}
BN_2A^T &= BN_2^TA = B\cdot \mathrm{circ}[q,r,r,q]\cdot \mathrm{circ}[a_1+a_2+a_3,a_1,a_2,a_3]\\
&= B\cdot \mathrm{circ}[\alpha,\beta,\alpha,\beta], \quad \alpha=(a_1+a_2)(q+r), \beta=(a_2+a_3)(q+r)\\
&= 0.
\end{aligned}$$

Next, we have

$$\begin{pmatrix} I+A & A\\ A^T & (I+A)^T\end{pmatrix}\begin{pmatrix} N_1+N_1A+N_2A^T & N_2+N_1A+N_2A^T\\ N_2^T+N_1A^T+N_2^TA & N_1+N_1A^T+N_2^TA\end{pmatrix} = \begin{pmatrix} D_1 & D_2\\ D_3 & D_4\end{pmatrix}, \tag{3.3}$$

where

$$\begin{aligned}
D_1 &= N_1+N_1A+N_2A^T+N_1A+N_1A^2+N_2AA^T+N_2^TA+N_1AA^T+N_2^TA^2\\
D_2 &= N_2+N_1A+N_2A^T+N_2A+N_1A^2+N_2AA^T+N_1A+N_1AA^T+N_2^TA^2\\
D_3 &= N_2^T+N_1A^T+N_1AA^T+N_2(A^T)^2+N_1A^T+N_2^TA+N_2^TA^T+N_1(A^T)^2+N_2^TAA^T\\
D_4 &= N_1+N_2A^T+N_1AA^T+N_2(A^T)^2+N_1A^T+N_2^TA+N_1A^T+N_1(A^T)^2+N_2^TAA^T.
\end{aligned}$$

Note the following:

$$\begin{aligned}
N_2A = N_2^TA^2 &= (q+r)\cdot \mathrm{circ}[a_2+a_3,a_1+a_2,a_2+a_3,a_1+a_2]\\
N_1A^2 = N_1(A^T)^2 &= (a_1^2+a_3^2)\cdot \mathrm{circ}[1,0,1,0]\\
N_2A^T = N_2^TA &= (q+r)\,\mathrm{circ}[a_1+a_2,a_2+a_3,a_1+a_2,a_2+a_3]\\
N_2^TA^2 = N_2AA^T = N_2(A^T)^2 = N_2AA^T &= (q+r)(a_1^2+a_3^2)\cdot J_4\\
N_1AA^T &= (a_1^2+a_3^2)\cdot \mathrm{circ}[0,1,0,1].
\end{aligned}$$

Using the above we find that

$$\begin{aligned}
D_1 &= N_1+N_1A^2+N_1AA^T\\
&= \mathrm{circ}[1,p,0,p]\\
D_2 &= N_2+N_2A^T+N_2A+N_1A^2+N_1AA^T\\
&= \mathrm{circ}[q,r,r,q]+(q+r)\left(\mathrm{circ}[\alpha,\beta,\alpha,\beta]+\mathrm{circ}[\beta,\alpha,\beta,\alpha]\right)+(a_1^2+a_3^2)\left(\mathrm{circ}[1,0,1,0]+\mathrm{circ}[0,1,0,1]\right)\\
&= \mathrm{circ}[q,r,r,q]+(q+r)(a_1+a_3)J_4\\
D_3 &= N_2^T+N_1AA^T+N_2^TA+N_2^TA^T+N_1(A^T)^2\\
&= \mathrm{circ}[q,q,r,r]+(q+r)\left(\mathrm{circ}[\alpha,\beta,\alpha,\beta]+\mathrm{circ}[\beta,\alpha,\beta,\alpha]\right)+(a_1^2+a_3^2)\left(\mathrm{circ}[1,0,1,0]+\mathrm{circ}[0,1,0,1]\right)\\
&= \mathrm{circ}[q,q,r,r]+(q+r)(a_1+a_3)J_4\\
D_4 &= N_1+N_1AA^T+A_1(A^T)^2\\
&= \mathrm{circ}[1,p,0,p].
\end{aligned}$$

Notice that $B=(a_1^2+a_3^2)J_4$ is present in each case, and will cancel when we add (3.2) to (3.3).

So finally, (3.1) reduces to

$$\begin{aligned}(\sigma(h))^3\sigma(n)\sigma(h) &= \begin{pmatrix} B & B \\ B & B \end{pmatrix} + \begin{pmatrix} D_1 & D_2 \\ D_3 & D_4 \end{pmatrix} \\ &= \begin{pmatrix} E_1 & E_2 \\ E_2^T & E_1 \end{pmatrix},\end{aligned}$$

with $E_1 = \text{circ}[1, p, 0, p]$ and $E_2 = \text{circ}[q, r, r, q] + (q + r)(a_1 + a_3)J_4$. Thus, $(\sigma(h))^3\sigma(n)\sigma(h) \in N$, and $N$ is a normal subgroup of $K$. ∎

## 3.4 The Structure of $\mathcal{U}(\mathbb{F}_{2^k}D_8)$

We now have all of the necessary information to determine the structure of $\mathcal{U}(\mathbb{F}_{2^k}D_8)$. First we write each subgroup as a product of cyclic groups, then finally we determine the structure of the unit group.

**Corollary 3.7 ([4])** $H \cong C_2^k \times C_4^k$.

**Proof.** We know that $H$ has exponent 4, and that $|H| = 2^{3k}$. Therefore $H \cong C_2^l \times C_4^m$ for some $l, m \in \mathbb{Z}^+$, meaning that all elements in $H$ have order either $1, 2$ or 4. The number of elements of order 1 or 2 in $C_2^l$ is $2^l$, and for $C_4^m$ is $2^m$. The total number of elements of order 1 or 2 in $C_2^l \times C_4^m$ is therefore $2^l \cdot 2^m = 2^{l+m}$.

So, the number of elements of order 4 in $C_2^l \times C_4^m$ is the total number of elements minus the number of elements of order 1 or 2, i.e. $2^l \cdot 4^m - 2^{l+m} \Leftrightarrow 2^l \cdot 2^m \cdot 2^m - 2^{l+m} \Leftrightarrow 2^{l+m}(2^m - 1)$.

Now, recall from Proposition 3.6 that

$$(\sigma(h))^2 = \begin{pmatrix} I + B & B \\ B & I + B \end{pmatrix}$$

where $B = (a_1^2 + a_3^2)J_4$.

So, $(\sigma(h))^2 = 1$ when $a_1 = a_3$, so the number of elements in $H$ with order 1 or 2 is $2^{2k}$. Therefore the number of elements with order 4 is $2^{3k} - 2^{2k} = 2^{2k}(2^k - 1)$. So, $2k = l + m \Rightarrow l = m = k$ and thus $H \cong C_2^k \times C_4^k$. ∎

**Corollary 3.8 ([4])** $N \cong C_2^k \times C_4^k$.

**Proof.** Let $n = 1 + p(x + x^3) + q(1 + x^3)y + r(x + x^2)y \in N$ then

$$\sigma(n) = \begin{pmatrix} A & B \\ B^T & A \end{pmatrix}$$

and

$$\begin{aligned}(\sigma(n))^2 &= \begin{pmatrix} A^2 + BB^T & AB + BA \\ B^TA + AB^T & B^TB + A^2 \end{pmatrix} \\ &= \begin{pmatrix} A^2 + BB^T & 0 \\ 0 & A^2 + BB^T \end{pmatrix}\end{aligned}$$

where $A = \text{circ}[1, p, 0, p]$ and $B = \text{circ}[q, r, r, q]$. Now,

$$\begin{aligned} A^2 &= \text{circ}[1, p, 0, p] \cdot \text{circ}[1, p, 0, p] \\ &= \text{circ}[1 + p^2 + p^2, p + p, p^2 + p^2, p + p] \\ &= \text{circ}[1, 0, 0, 0] \\ &= I_4 \\ BB^T &= \text{circ}[q, r, r, q] \cdot \text{circ}[q, q, r, r] \\ &= \text{circ}[2q^2 + 2r^2, q^2 + r^2 + 2qr, 4qr, q^2 + r^2 + 2qr] \\ &= \text{circ}[0, q^2 + r^2, 0, q^2 + r^2]. \end{aligned}$$

Therefore, $(\sigma(n))^2 = 1$ if $A^2 + BB^T = I_4$, which is only true if $q = r$. Elements of order 1 or 2 are of the form $n' = 1 + p(x + x^3) + q(1 + x + x^2 + x^3)y$, which gives $2^k$ possibilities. Thus, by following the same argument as in Corollary 3.8 we find that $N \cong C_2^k \times C_4^k$.

■

**Proposition 3.9 ([4])** $\mathcal{U}(\mathbb{F}_{2^k}C_2) \cong C_2^k \times C_{2^k-1}$.

**Proof.** First, we know that $\mathcal{U}(RG) \cong V(RG) \times \mathcal{U}(R)$. Therefore, $\mathcal{U}(\mathbb{F}_{2^k}C_2) \cong V(\mathbb{F}_{2^k}C_2) \times \mathcal{U}(\mathbb{F}_{2^k})$. It is known that, for a Galois Field $\mathbb{F}_{p^k}$, $\mathcal{U}(\mathbb{F}_{p^k}) \cong C_{p^k-1}$. So, $\mathcal{U}(\mathbb{F}_{2^k}) \cong C_{2^k-1}$.

Now, let $\alpha = a_1 + a_2x \in \mathbb{F}_{2^k}C_2$ and $u \in \mathcal{U}(\mathbb{F}_{2^k}C_2)$. Recall from definition blah that $u \in V(\mathbb{F}_{2^k}C_2)$ if $\epsilon(u) = 1$, where $\epsilon$ is the augmentation mapping. $\epsilon(u) = 1 \Leftrightarrow a_1 + a_2 = 1 \Leftrightarrow a_2 = 1 + a_1$. Then

$$\begin{aligned}\sigma(u) &= \begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix} \\ &= \begin{pmatrix} 1 + a_1 & a_1 \\ a_1 & 1 + a_1 \end{pmatrix}\end{aligned}$$

Therefore,

$$(\sigma(u))^2 = \begin{pmatrix} 1 + a_1 & a_1 \\ a_1 & 1 + a_1 \end{pmatrix} \begin{pmatrix} 1 + a_1 & a_1 \\ a_1 & 1 + a_1 \end{pmatrix}$$

$$= \begin{pmatrix} (1+a_1)^2 + a_1^2 & (1+a_1)a_1 + a_1(1+a_1) \\ a_1(1+a_1) + (1+a_1)a_1 & a_1^2 + (1+a_1)^2 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

So the exponent of $V(\mathbb{F}_{2^k}C_2)$ is 2, meaning $V(\mathbb{F}_{2^k}C_2) \cong C_2^k$. Thus, $\mathcal{U}(\mathbb{F}_{2^k}C_2) \cong C_2^k \times C_{2^k-1}$. ■

**Theorem 3.10 ([4])** $\mathcal{U}(\mathbb{F}_{2^k}D_8) \cong \left[\, (((C_2^k \times C_4^k) \rtimes C_4^k) \times C_2^k) \rtimes C_2^k \,\right] \times C_{2^k-1}$.

**Proof.** Recall from Proposition 3.2 that $\mathcal{U}(\mathbb{F}_{2^k}D_8) \cong K \rtimes \mathcal{U}(\mathbb{F}_{2^k}C_2)$. Then, since $H \cap N = 1$ we have that

$$K \cong N \rtimes H \cong (C_2^k \times C_4^k) \rtimes (C_2^k \times C_4^k) \cong ((C_2^k \times C_4^k) \rtimes C_4^k) \times C_2^k.$$

Thus,

$$\mathcal{U}(\mathbb{F}_{2^k}D_8) \cong \left[\, (((C_2^k \times C_4^k) \rtimes C_4^k) \times C_2^k) \rtimes C_2^k \,\right] \times C_{2^k-1}.$$

■

# Chapter 4

# Unitary Units of $\mathbb{F}_{2^k}D_8$

In this chapter, we descibe a special subgroup of the unit group of a group algebra called the unitary units, specifically for $\mathbb{F}_{2^k}D_8$. Recall from Definition 1.33 that $V_*(\mathbb{F}_{2^k}D_8) = \{v \in V(RG) | v^* = v^{-1}\}$. We describe the structure as a semidirect product of a normal subgroup $N$ with a subgroup $H$. We begin by constructing $N$, followed by $H$, then show that $N \cong C_2^{5k}$, $H \cong C_2^k$. Then finally we show that $V_*(\mathbb{F}_{2^k}D_8) \cong C_2^{5k} \rtimes C_2^k$. These results were first shown in [6], however many of the details are omitted. Here, not only do we provide alternative methods of proof, but full details of each proof are also included.

**Proposition 4.1 ([6])** *Let $N$ be the set of elements of $V_*(\mathbb{F}_{2^k}D_8)$ of the form $1 + a_2 + a_3 + a_5 + a_1(x + x^3) + a_2x^2 + a_3y + a_4(xy + x^3y) + a_5x^2y$ where $a_i \in \mathbb{F}_{2^k}$. Then, $N$ is an abelian subgroup of $V_*(\mathbb{F}_{2^k}D_8)$ and $N \cong C_2^{5k}$.*

**Proof.** Let $n_1 = 1 + a_2 + a_3 + a_5 + a_1(x + x^3) + a_2x^2 + a_3y + a_4(xy + x^3y) + a_5x^2y$ and $n_2 = 1 + b_2 + b_3 + b_5 + b_1(x + x^3) + b_2x^2 + b_3y + b_4(xy + x^3y) + b_5x^2y$. Then,

$$\begin{aligned}\sigma(n_1)\sigma(n_2) &= \begin{pmatrix} I+A & B \\ B & I+A \end{pmatrix}\begin{pmatrix} I+C & D \\ D & I+C \end{pmatrix} \\ &= \begin{pmatrix} (I+A)(I+C)+BD & (I+A)D+B(I+C) \\ B(I+C)+(I+A)D & BD+(I+A)(I+C) \end{pmatrix} \\ &= \begin{pmatrix} I+A+C & B+D \\ B+D & I+A+C \end{pmatrix} + \begin{pmatrix} AC+BD & AD+BC \\ AD+BC & AC+BD \end{pmatrix}.\end{aligned}$$

where

$$\begin{aligned} A &= \mathrm{circ}[a_2+a_3+a_5, a_1, a_2, a_1], & B &= \mathrm{circ}[a_3, a_4, a_5, a_4], \\ C &= \mathrm{circ}[b_2+b_3+b_5, b_1, b_2, b_1], & D &= \mathrm{circ}[b_3, b_4, b_5, b_4]. \end{aligned}$$

By splitting the matrix in two, we can immediately see that $\begin{pmatrix} I+A+C & B+D \\ B+D & I+A+C \end{pmatrix} \in N$. Therefore we only need to consider the second matrix, i.e. we need to show that $AC + BD = \mathrm{circ}[x_2 + x_3 + x_5, x_1, x_2, x_1]$ and $AD + BC = \mathrm{circ}[x_3, x_4, x_5, x_4]$.

$$\begin{aligned}
AC &= \operatorname{circ}[a_2+a_3+a_5, a_1, a_2, a_1]\cdot\operatorname{circ}[b_2+b_3+b_5, b_1, b_2, b_1]\\
&= \operatorname{circ}[a_2(b_3+b_5)+a_3(b_2+b_5)+a_5(b_2+b_3)+a_3b_3+a_5b_5, a_1(b_3+b_5)+b_1(a_3+a_5),\\
&\qquad a_2(b_3+b_5)+b_2(a_3+a_5), a_1(b_3+b_5)+b_1(a_3+a_5)]\\
BD &= \operatorname{circ}[a_3, a_4, a_5, a_4]\cdot\operatorname{circ}[b_3, b_4, b_5, b_4]\\
&= \operatorname{circ}[a_3b_3+a_5b_5, a_4(b_3+b_5)+b_4(a_3+a_5), a_3b_5+a_5b_3, a_4(b_3+b_5)+b_4(a_3+a_5)]
\end{aligned}$$

$$\begin{aligned}
AD &= \operatorname{circ}[a_2+a_3+a_5, a_1, a_2, a_1]\cdot\operatorname{circ}[b_3, b_4, b_5, b_4]\\
&= \operatorname{circ}[a_2(b_3+b_5)+b_3(a_3+a_5), a_1(b_3+b_5)+b_4(a_3+a_5), a_2(b_3+b_5)+b_5(a_3+a_5),\\
&\qquad a_1(b_3+b_5)+b_4(a_3+a_5)]\\
BC &= \operatorname{circ}[a_3, a_4, a_5, a_4]\cdot\operatorname{circ}[b_2+b_3+b_5, b_1, b_2, b_1]\\
&= \operatorname{circ}[a_3(b_2+b_3)+a_2b_5+a_5b_2, a_4(b_3+b_5)+b_1(a_3+a_5), b_2(a_3+a_5)+a_5(b_3+b_5),\\
&\qquad a_4(b_3+b_5)+b_1(a_2+a_5)]
\end{aligned}$$

So,

$$\begin{aligned}
AC+BD &= \operatorname{circ}[x_2+x_3+x_5, x_1, x_2, x_1]\\
AD+BC &= \operatorname{circ}[x_3, x_4, x_5, x_4]
\end{aligned}$$

where

$$\begin{aligned}
x_1 &= (a_1+a_4)(b_3+b_5)+(b_1+b_4)(a_3+a_5)\\
x_2 &= a_2(b_3+b_5)+b_2(a_3+a_5)+a_3b_5+a_5b_3\\
&= a_2(b_3+b_5)+a_3(b_2+b_5)+a_5(b_2+b_3)\\
x_3 &= a_2(b_3+b_5)+b_3(a_3+a_5)+a_3(b_2+b_3)+a_3b_5+a_5b_2\\
&= a_2(b_3+b_5)+a_3(b_2+b_5)+a_5(b_2+b_3)\\
x_4 &= (a_1+a_4)(b_3+b_5)+(b_1+b_4)(a_3+a_5)\\
x_5 &= a_2(b_3+b_5)+b_5(a_3+a_5)+b_2(a_3+a_5)+a_5(b_3+b_5)\\
&= a_2(b_3+b_5)+a_3(b_2+b_5)+a_5(b_2+b_3).
\end{aligned}$$

Therefore $N$ is closed and is a subgroup of $V_*(\mathbb{F}_{2^k}D_8)$. Now, since $I, A, B, C, D$ are all circulant matrices, we have that

$$\begin{aligned}
\sigma(n_2)\sigma(n_1) &= \begin{pmatrix} I+C & D\\ D & I+C\end{pmatrix}\begin{pmatrix} I+A & B\\ B & I+A\end{pmatrix}\\
&= \begin{pmatrix} (I+C)(I+A)+DB & (I+C)B+D(I+A)\\ D(I+A)+(I+C)B & DB+(I+C)(I+A)\end{pmatrix}\\
&= \begin{pmatrix} (I+A)(I+C)+BD & (I+A)D+B(I+C)\\ B(I+C)+(I+A)D & BD+(I+A)(I+C)\end{pmatrix}
\end{aligned}$$

$$\begin{aligned}&= \begin{pmatrix} I+A & B \\ B & I+A \end{pmatrix} \begin{pmatrix} I+C & D \\ D & I+C \end{pmatrix} \\ &= \sigma(n_1)\sigma(n_2),\end{aligned}$$

which shows that $N$ is abelian. Now, $n \in V_*(\mathbb{F}_{2^k}D_8)$ if and only if $n^{-1} = n^* \forall n \in N$. So,

$$\begin{aligned}\sigma(n^{-1}) = \sigma(n^*) &\Leftrightarrow \sigma(n)^{-1} = \sigma(n^*) \\ &\Leftrightarrow \sigma(n)^{-1} = \sigma(n)^T \\ &\Leftrightarrow \sigma(n)\sigma(n)^T = I.\end{aligned}$$

Let $n = 1 + a_2 + a_3 + a_5 + a_1(x + x^3) + a_2x^2 + a_3y + a_4(xy + x^3y) + a_5x^2y \in N$. Then

$$\sigma(n) = \sigma(n)^T = \begin{pmatrix} I+A & B \\ B & I+A \end{pmatrix},$$

with $A = \text{circ}[a_2 + a_3 + a_5, a_1, a_2, a_1]$ and $B = \text{circ}[a_3, a_4, a_5, a_4]$. Therefore,

$$\begin{aligned}\sigma(n)\sigma(n)^T &= \begin{pmatrix} I+A & B \\ B & I+A \end{pmatrix}^2 \\ &= \begin{pmatrix} I+A^2+B^2 & 0 \\ 0 & I+A^2+B^2 \end{pmatrix} \\ &= \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix},\end{aligned}$$

since $A^2 = B^2 = \text{circ}[a_3^2 + a_5^2, 0, 0, 0]$. Thus, $N \cong C_2^{5k} < V_*(\mathbb{F}_{2^k}D_8)$. ■

**Proposition 4.2 ([6])** *Let $H$ be the set of elements of $V_*(\mathbb{F}_{2^k}D_8)$ of the form $1 + \alpha\sum_{i=1}^{3} x^i + \alpha\sum_{j=0}^{2} x^jy$ where $\alpha \in \mathbb{F}_{2^k}$. Then $H$ is an abelian subgroup of $V_*(\mathbb{F}_{2^k}D_8)$ and $H \cong C_2^k$.*

**Proof.** Let $h_1 = 1 + \alpha\sum_{i=1}^{3} x^i + \alpha\sum_{j=0}^{2} x^jy$ and $h_2 = 1 + \beta\sum_{i=1}^{3} x^i + \beta\sum_{j=0}^{2} x^jy$. Then,

$$\begin{aligned}\sigma(h_1)\sigma(h_2) &= \begin{pmatrix} A & B \\ B^T & A \end{pmatrix} \begin{pmatrix} C & D \\ D^T & C \end{pmatrix} \\ &= \begin{pmatrix} AC + BD^T & AD + BC \\ B^TC + AD^T & B^TD + AC \end{pmatrix} \\ &= \begin{pmatrix} AC + BD^T & AD + BC \\ (AD + BC)^T & AC + B^TD \end{pmatrix}\end{aligned}$$

with $A = \text{circ}[1, \alpha, \alpha, \alpha], B = \text{circ}[\alpha, \alpha, \alpha, 0], C = \text{circ}[1, \beta, \beta, \beta]$ and $D = \text{circ}[\beta, \beta, \beta, 0]$. Considering each multiplication separately we have

$$\begin{aligned}
AC &= \text{circ}[1,\alpha,\alpha,\alpha]\cdot\text{circ}[1,\beta,\beta,\beta]\\
&= \text{circ}[1+\alpha\beta,\alpha+\beta,\alpha+\beta,\alpha+\beta]\\
BD^T &= \text{circ}[\alpha,\alpha,\alpha,0]\cdot\text{circ}[\beta,0,\beta,\beta]\\
&= \text{circ}[\alpha\beta,0,0,0]\\
&= (BD^T)^T = DB^T = B^TD\\
AD &= \text{circ}[1,\alpha,\alpha,\alpha]\cdot\text{circ}[\beta,\beta,\beta,0]\\
&= \text{circ}[\beta,\beta,\beta,\alpha\beta]\\
BC &= \text{circ}[\alpha,\alpha,\alpha,0]\cdot\text{circ}[1,\beta,\beta,\beta]\\
&= \text{circ}[\alpha,\alpha,\alpha,\alpha\beta].
\end{aligned}$$

Therefore,

$$\begin{aligned}
AC+BD^T &= \text{circ}[1+\alpha\beta,\alpha+\beta,\alpha+\beta,\alpha+\beta]+\text{circ}[\alpha\beta,0,0,0]\\
&= \text{circ}[1,\alpha+\beta,\alpha+\beta,\alpha+\beta]\\
AD+BC &= \text{circ}[\beta,\beta,\beta,\alpha\beta]+\text{circ}[\alpha,\alpha,\alpha,\alpha\beta]\\
&= \text{circ}[\alpha+\beta,\alpha+\beta,\alpha+\beta,0].
\end{aligned}$$

Thus, $H$ is closed. Now,

$$\begin{aligned}
\sigma(h_2)\sigma(h_1) &= \begin{pmatrix} C & D\\ D^T & C\end{pmatrix}\begin{pmatrix} A & B\\ B^T & A\end{pmatrix}\\
&= \begin{pmatrix} CA+DB^T & CB+DA\\ D^TA+CB^T & D^TB+CA\end{pmatrix}\\
&= \begin{pmatrix} AC+B^TD & AD+BC\\ (AD+BC)^T & AC+BD^T\end{pmatrix}\\
&= \sigma(h_1)\sigma(h_2),
\end{aligned}$$

which shows that $H$ is also abelian. Now consider $h = 1+\alpha\sum_{i=1}^{3}x^i+\alpha\sum_{j=0}^{2}x^jy \in H$. Then, in order to be an element of $V_*(\mathbb{F}_{2^k}D_8)$, $h^{-1}=h^* \Leftrightarrow \sigma(h)\sigma(h)^T = I$, So,

$$\begin{aligned}
\sigma(h)\sigma(h)^T &= \begin{pmatrix} A & B\\ B^T & A\end{pmatrix}\begin{pmatrix} A & B\\ B^T & A\end{pmatrix}\\
&= \begin{pmatrix} A^2+BB^T & 0\\ 0 & B^TB+A^2\end{pmatrix}\\
&= \begin{pmatrix} I & 0\\ 0 & I\end{pmatrix},
\end{aligned}$$

since $A^2+BB^T = \text{circ}[1+\alpha^2,0,0,0]+\text{circ}[\alpha^2,0,0,0] = I_4$. Thus, $H \cong C_2^k < V_*(\mathbb{F}_{2^k}D_8)$. ■

**Proposition 4.3 ([6])** *$N$ is a normal subgroup of $V_*(\mathbb{F}_{2^k}D_8)$.*

**Proof.** $N = \{1 + a_2 + a_3 + a_5 + a_1(x + x^3) + a_2x^2 + a_3y + a_4(xy + x^3y) + a_5x^2y | a_i \in \mathbb{F}_{2^k}\}$ and $H = \{1 + \alpha \sum_{i=1}^{3} x^i + \alpha \sum_{j=0}^{2} x^j y | \alpha \in \mathbb{F}_{2^k}\}$. Clearly $N \cap H = 1$.

Let $n = 1 + a_2 + a_3 + a_5 + a_1(x + x^3) + a_2x^2 + a_3y + a_4(xy + x^3y) + a_5x^2y \in N$ and $h = 1 + \alpha \sum_{i=1}^{3} x^i + \alpha \sum_{j=0}^{2} x^j y \in H$, where $a_i, \alpha \in \mathbb{F}_{2^k}$. Then,

$$\begin{aligned}
\sigma(h)^{-1}\sigma(n)\sigma(h) &= \sigma(h)\sigma(n)\sigma(h)\\
&= \begin{pmatrix} H_1 & H_2 \\ H_2^T & H_1 \end{pmatrix} \begin{pmatrix} I + N_1 & N_2 \\ N_2 & I + N_1 \end{pmatrix} \begin{pmatrix} H_1 & H_2 \\ H_2^T & H_1 \end{pmatrix}\\
&= \begin{pmatrix} H_1 & H_2 \\ H_2^T & H_1 \end{pmatrix} \left[ \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix} + \begin{pmatrix} N_1 & N_2 \\ N_2 & N_1 \end{pmatrix} \right] \begin{pmatrix} H_1 & H_2 \\ H_2^T & H_1 \end{pmatrix}\\
&= \left[ \begin{pmatrix} H_1 & H_2 \\ H_2^T & H_1 \end{pmatrix} + \begin{pmatrix} H_1N_1 + H_2N_2 & H_1N_2 + H_2N_1 \\ H_2^TN_1 + H_1N_2 & H_2^TN_2 + H_1N_1 \end{pmatrix} \right] \begin{pmatrix} H_1 & H_2 \\ H_2^T & H_1 \end{pmatrix}\\
&= \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix} + \begin{pmatrix} H_1N_1 + H_2N_2 & H_1N_2 + H_2N_1 \\ H_2^TN_1 + H_1N_2 & H_2^TN_2 + H_1N_1 \end{pmatrix} \begin{pmatrix} H_1 & H_2 \\ H_2^T & H_1 \end{pmatrix}\\
&= \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix} + \begin{pmatrix} X & Y \\ Y & X \end{pmatrix}.
\end{aligned}$$

where $H_1 = \text{circ}[1, \alpha, \alpha, \alpha]$, $H_2 = \text{circ}[\alpha, \alpha, \alpha, 0]$, $N_1 = \text{circ}[a_2 + a_3 + a_5, a_1, a_2, a_1]$, $N_2 = \text{circ}[a_3, a_4, a_5, a_4]$, $X = H_1^2N_1 + H_1H_2N_2 + H_1H_2^TN_2 + H_2H_2^TN_1$ and $Y = H_2^2 + H_1^2N_2$. Now,

$$\begin{aligned}
H_1^2N_1 &= \text{circ}[(\alpha^2 + 1)(a_2 + a_3 + a_5), (\alpha^2 + 1)a_1, (\alpha^2 + 1)a_2, (\alpha^2 + 1)a_1]\\
&= (\alpha^2 + 1)\,\text{circ}[a_2 + a_3 + a_5, a_1, a_2, a_1]\\
&= (\alpha^2 + 1)N_1\\
H_1H_2N_2 &= \alpha \cdot \text{circ}[\alpha a_4 + a_3 + a_4 + a_5, \alpha a_5 + a_3, \alpha a_4 + a_3 + a_4 + a_5, \alpha a_3 + a_5]\\
H_1H_2^TN_2 &= \alpha \cdot \text{circ}[\alpha a_4 + a_3 + a_4 + a_5, \alpha a_3 + a_5, \alpha a_4 + a_3 + a_4 + a_5, \alpha a_5 + a_3]
\end{aligned}$$

$$\begin{aligned}
H_2H_2^TN_1 &= \text{circ}[\alpha^2(a_2 + a_3 + a_5), \alpha^2a_1, \alpha^2a_2, \alpha^2a_1]\\
&= \alpha^2\,\text{circ}[a_2 + a_3 + a_5, a_1, a_2, a_1]\\
&= \alpha^2N_1\\
H_1^2N_2 &= \text{circ}[(\alpha^2 + 1)a_3, (\alpha^2 + 1)a_4, (\alpha^2 + 1)a_5, (\alpha^2 + 1)a_4]\\
&= (\alpha^2 + 1)\,\text{circ}[a_3, a_4, a_5, a_4]\\
&= (\alpha^2 + 1)N_2\\
(H_2^T)^2N_2 &= \text{circ}[\alpha^2a_5, \alpha^2a_4, \alpha^2a_3, \alpha^2a_4]\\
&= \alpha^2\,\text{circ}[a_5, a_4, a_3, a_4]\\
&= H_2^2N_2.
\end{aligned}$$

Therefore,

$$\begin{aligned}
X &= H_1^2N_1 + H_1H_2N_2 + H_1H_2^TN_2 + H_2H_2^TN_1 \\
&= (\alpha^2+1)N_1 + \alpha^2N_1 + \alpha \cdot \operatorname{circ}[0,(\alpha+1)(a_3+a_5),0,(\alpha+1)(a_3+a_5)] \\
&= N_1 + (\alpha+1)(a_3+a_5)\operatorname{circ}[0,1,0,1] \\
&= \operatorname{circ}[a_2+a_3+a_5, a_1+\alpha(\alpha+1)(a_3+a_5), a_2, a_1+\alpha(\alpha+1)(a_3+a_5)] \\
Y &= H_2^2 + H_1^2N_2 \\
&= \alpha^2 \cdot \operatorname{circ}[a_5,a_4,a_3,a_4] + (1+\alpha^2)\operatorname{circ}[a_3,a_4,a_5,a_4] \\
&= \operatorname{circ}[a_3+\alpha^2(a_3+a_5), a_4, a_5+\alpha^2(a_3+a_5), a_4].
\end{aligned}$$

We can see that $X$ and $Y$ are of the same form as $N_1$ and $N_2$, therefore $\sigma(h)^{-1}\sigma(n)\sigma(h) \in N$. Thus $N$ is a normal subgroup of $V_*(\mathbb{F}_{2^k}D_8)$. ■

We are now in a position to fully describe the structure of $V_*(\mathbb{F}_{2^k}D_8)$.

**Theorem 4.4 ([6])** $V_*(\mathbb{F}_{2^k}D_8) \cong C_2^{5k} \rtimes C_2^k$.

**Proof.** Recall from Definition 1.13 that for a semidirect product we require $V_*(\mathbb{F}_{2^k}D_8) = NH$, $N \cap H = \{1\}$ and $N \lhd V_*(\mathbb{F}_{2^k}D_8)$. We have already shown these to be true in the previous Lemmas, therefore since $N \cong C_2^{5k}$ and $H \cong C_2^k$ the result is proven. ■

# Chapter 5

# Self-Dual Codes

It is well known in the literature that there is a connection between group rings and Coding Theory [10, 11, 13, 19]. In particular, ideals in group rings correspond to certain codes. In this chapter, we describe the connection between unitary units in group rings and self-dual codes. This was first established by Gildea et al. in [13]. Further into the chapter we will constuct certain self-dual codes and detail the units that correspond to each code. In addition, we will prove that these elements are unitary.

First, we shall describe the connection between unitary units and self-dual codes. Recall from Chapter 1 that a generator matrix $G$ is said to be self-dual if $GG^T = 0$. So, note that $\sigma(v^*) = \sigma(v)^T$, then for generators of the form $G = (I \mid \sigma(v))$ we have

$$\begin{aligned} GG^T &= \begin{pmatrix} I & \sigma(v) \end{pmatrix} \begin{pmatrix} I \\ \sigma(v)^T \end{pmatrix} \\ &= I + \sigma(v)\sigma(v)^T \\ &= I + \sigma(v)\sigma(v^*) \\ &= I + \sigma(vv^*). \end{aligned}$$

Therefore $GG^T = 0$ implies that

$$\begin{aligned} I + \sigma(vv^*) &= 0 \\ \sigma(vv^*) &= I \\ vv^* &= 1 \\ v^{-1} &= v^*. \end{aligned}$$

Definition 1.33 tells us that $v^* = v^{-1}$ corresponds to an element of $V_*(RG)$, and thus the connection is shown.

Now, let $\alpha = \sum_{i=0}^{3} x^i(a_i + a_{i+4}y) \in RD_8$, then $\sigma(\alpha) = \left(\begin{smallmatrix} A & B \\ B^T & A^T \end{smallmatrix}\right)$ where $A = \text{circ}[a_0, a_1, a_2, a_3]$ and $B = \text{circ}[a_4, a_5, a_6, a_7]$.

Consequently, we will consider codes over $\mathbb{F}_2, \mathbb{F}_4$ and $\mathbb{F}_4 + u\mathbb{F}_4$ of the following from

$$G = \left( \begin{array}{cc|cc} I & 0 & A & B \\ 0 & I & B^T & A^T \end{array} \right),$$

where $I$ is the identity matrix.

## 5.1 Codes in $\mathbb{F}_2 D_8$

Let us begin by studying the codes generated by the group algebra $\mathbb{F}_2 D_8$. There are $2^8$ possible codes of this structure, using code written in `GAP` we will construct each one. We begin by creating a set $G$ containing all possible generator matrices of the form described above. To do this we use the `DihedralGeneratorMatrix()` function which can be found in Appendix A.2.

**Listing 5.1: Creating generator matrices for $\mathbb{F}_2 D_8$**

```
gap> Read("/home/harrison/.../CodingFunctions.g");;
gap> G:=DihedralGeneratorMatrix(4);; # 4 refers to dimensions of A and B
gap> Size(G); # number of generator matrices (2^8)
256
gap> Display(G[10]); # print 10th element (arbitrary)
 1 . . . . . . . . . . . 1 . . 1
 . 1 . . . . . . . . . . 1 1 . .
 . . 1 . . . . . . . . . . 1 1 .
 . . . 1 . . . . . . . . . . 1 1
 . . . . 1 . . . 1 1 . . . . . .
 . . . . . 1 . . . 1 1 . . . . .
 . . . . . . 1 . . . 1 1 . . . .
 . . . . . . . 1 1 . . 1 . . . .
```

Next we check for self-duality using the $GG^T = 0$ condition from Theorem 1.61, this is done using another custom function `GetSelfDual()`, also found in Appendix A.2.

**Listing 5.2: Self-dual generator matrices for $\mathbb{F}_2 D_8$**

```
gap> S:= GetSelfDual(G);; # extracts only self-dual codes from G
gap> Size(S); # number of self-dual codes
64
gap> Display(S[1]*TransposedMatS[1]);
 . . . . . . . .
 . . . . . . . .
 . . . . . . . .
 . . . . . . . .
 . . . . . . . .
 . . . . . . . .
 . . . . . . . .
 . . . . . . . .
```

As explained in Definition 1.52, we can have codes which are equivalent under certain row operations. The `guava` package in `GAP` contains the function `IsEquivalent()`, which checks whether two codes are equivalent over $\mathbb{F}_2$. The custom function `UniqueGenerators()` utilises this function to compare each of the self-dual codes in $S$ and returns only the unique ones with minimum distance atleast 4. The reason for only selecting those with minimum distance 4 is because those are the extremal codes, this value is obtained from Theorem 1.62.

**Listing 5.3: Unique self-dual generator matrices for $\mathbb{F}_2 D_8$**

```
gap> U:= UniqueGenerators(S,4);; # unique generators in S with min distance >= 4
 1 . . . . . . . . . . . . 1 1 1
 . 1 . . . . . . . . . . 1 . 1 1
 . . 1 . . . . . . . . . 1 1 . 1
 . . . 1 . . . . . . . . 1 1 1 .
 . . . . 1 . . . . 1 1 1 . . . .
 . . . . . 1 . . 1 . 1 1 . . . .
 . . . . . . 1 . 1 1 . 1 . . . .
 . . . . . . . 1 1 1 1 . . . . .
Type II self-dual code with MinimumDistance = 4
 1 . . . . . . . . . . 1 1 1 1 1
 . 1 . . . . . . 1 . . . 1 1 1 1
 . . 1 . . . . . . 1 . . 1 1 1 1
 . . . 1 . . . . . . 1 . 1 1 1 1
 . . . . 1 . . . 1 1 1 1 . 1 . .
 . . . . . 1 . . 1 1 1 1 . . 1 .
 . . . . . . 1 . 1 1 1 1 . . . 1
 . . . . . . . 1 1 1 1 1 1 . . .
Type I self-dual code with MinimumDistance = 4
 1 . . . . . . . . 1 1 1 1 1 1 1
 . 1 . . . . . . 1 . 1 1 1 1 1 1
 . . 1 . . . . . 1 1 . 1 1 1 1 1
 . . . 1 . . . . 1 1 1 . 1 1 1 1
 . . . . 1 . . . 1 1 1 1 . 1 1 1
 . . . . . 1 . . 1 1 1 1 1 . 1 1
 . . . . . . 1 . 1 1 1 1 1 1 . 1
 . . . . . . . 1 1 1 1 1 1 1 1 .
Type II self-dual code with MinimumDistance = 4
```

For each of the three codes above, the last 8 elements of the first row i.e. `. . . . . 1 1 1` correspond to the coefficients of 1, $x$, ..., $x^3y$. From this we obtain the following table:

| $\alpha$ | $1$ | $x$ | $x^2$ | $x^3$ | $y$ | $xy$ | $x^2y$ | $x^3y$ | $d$ |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 4 |
| 2 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 4 |
| 3 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 4 |

Table 5.1: Table of coefficients for $\mathbb{F}_2 D_8$, obtained using GAP.

We will now check that each element is unitary by computing $\alpha_i \alpha_i^*$, in each case the result should be 1.

First, we have

$$\begin{aligned}
\alpha_1 &= xy + x^2y + x^3y \\
&= y + \hat{x}y \\
\alpha_1^* &= (xy)^{-1} + (x^2y)^{-1} + (x^3y)^{-1} \\
&= xy + x^2y + x^3y \\
&= y + \hat{x}y \\
\alpha_1\alpha_1^* &= (y + \hat{x}y)(y + \hat{x}y) \\
&= y^2 + y\hat{x}y + \hat{x}y^2 + \hat{x}y\hat{x}y \\
&= 1 + 2\hat{x} + 0 \\
&= 1.
\end{aligned}$$

Secondly,

$$\begin{aligned}
\alpha_2 &= x^3 + y + xy + x^2y + x^3y \\
&= x^3 + \hat{x}y \\
\alpha_2^* &= (x^3)^{-1} + (y)^{-1} + (xy)^{-1} + (x^2y)^{-1} + (x^3y)^{-1} \\
&= x + y + xy + x^2y + x^3y \\
&= x + \hat{x}y \\
\alpha_2\alpha_2^* &= (x^3 + \hat{x}y)(x + \hat{x}y) \\
&= x^4 + x^3\hat{x}y + \hat{x}yx + \hat{x}y\hat{x}y \\
&= 1 + \hat{x}y + \hat{x}y + (\hat{x})^2 \\
&= 1 + 2\hat{x}y + 0 \\
&= 1.
\end{aligned}$$

Finally,

$$\begin{aligned}
\alpha_3 &= x + x^2 + x^3 + y + xy + x^2y + x^3y \\
&= 1 + \hat{x} + \hat{x}y \\
\alpha_3^* &= (x)^{-1} + (x^2)^{-1} + (x^3)^{-1} + (y)^{-1} + (xy)^{-1} + (x^2y)^{-1} + (x^3y)^{-1} \\
&= x^3 + x^2 + x + y + xy + x^2y + x^3y \\
&= 1 + \hat{x} + \hat{x}y \\
\alpha_3\alpha_3^* &= (1 + \hat{x} + \hat{x}y)(1 + \hat{x} + \hat{x}y) \\
&= 1 + \hat{x} + \hat{x}y + \hat{x} + (\hat{x})^2 + (\hat{x})^2y + \hat{x}y + \hat{x}y\hat{x} + (\hat{x}y)^2 \\
&= 1 + \hat{x} + 2\hat{x} + 2\hat{x}y \\
&= 1.
\end{aligned}$$

## 5.2 Codes in $\mathbb{F}_4 D_8$

Due to memory restrictions and the fact that `GAP` can only check equivalency over $\mathbb{F}_2$, the following codes are obtained using `MAGMA`. We find four unique codes with minimum distance 8 and five with minimum distance 6, which we must check are unitary.

| $\beta$ | $1$ | $x$ | $x^2$ | $x^3$ | $y$ | $xy$ | $x^2y$ | $x^3y$ | $d$ |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | $w$ | 0 | 1 | $w+1$ | 1 | 6 |
| 2 | 0 | 0 | 0 | $w$ | 1 | 1 | 1 | $w$ | 6 |
| 3 | 0 | 0 | 0 | $w$ | 1 | $w+1$ | $w$ | $w+1$ | 8 |
| 4 | 0 | 0 | 1 | 1 | 0 | 1 | $w$ | $w$ | 6 |
| 5 | 0 | 0 | 1 | 1 | 1 | 1 | $w$ | $w+1$ | 8 |
| 6 | 0 | 0 | $w$ | $w+1$ | 0 | $w$ | 1 | $w+1$ | 8 |
| 7 | 0 | 1 | $w$ | $w$ | 0 | $w$ | 1 | $w+1$ | 6 |
| 8 | 0 | 1 | $w$ | $w$ | $w$ | $w$ | $w+1$ | $w+1$ | 8 |
| 9 | 0 | $w$ | 1 | $w+1$ | 1 | 1 | $w$ | $w+1$ | 6 |

Table 5.2: Unique codes over $\mathbb{F}_4$, obtained using MAGMA.

First, we have

$$\begin{aligned}\beta_1 &= wx^3 + xy + (w+1)x^2y + x^3y\\ \beta_1^* &= w(x^3)^{-1} + (xy)^{-1} + (w+1)(x^2y)^{-1} + (x^3y)^{-1}\\ &= wx + xy + (w+1)x^2y + x^3y\end{aligned}$$

Multiplying gives

$$\begin{aligned}\beta_1\beta_1^* &= w^2x^4 + wx^4y + w(w+1)x^5y + wx^6y + wxyx + xyxy + (w+1)xyx^2y + xyx^3y\\ &\quad + w(w+1)x^2yx + (w+1)x^2yxy + (w+1)^2x^2yx^2y + (w+1)x^2yx^3y\\ &\quad + wx^3yx + x^3yxy + (w+1)x^3yx^2y + x^3yx^3y\\ &= \big(2 + w + (1+w)\big) + 2(w+1)x + 2x^2 + 2(w+1)x^3 + 2wy + 2xy + 2wx^2y\\ &= 1.\end{aligned}$$

Secondly,

$$\begin{aligned}\beta_2 &= wx^3 + y + xy + x^2y + wx^3y\\ \beta_2^* &= w(x^3)^{-1} + (y)^{-1} + (xy)^{-1} + (x^2y)^{-1} + w(x^3y)^{-1}\\ &= wx + y + xy + x^2y + wx^3y.\end{aligned}$$

Multiplying,

$$\begin{aligned}
\beta_2\beta_2^* &= w^2x^4 + wx^3y + wx^4y + wx^5y + w^2x^6y + wyx + y^2 + yxy + yx^2y + wyx^3y \\
&\quad + wxyx + xy^2 + xyxy + xyx^2y + wxyx^2y + wx^2yx + x^2y^2 + x^2yxy \\
&\quad + x^2yx^2y + wx^2yx^3y + w^2x^3yx + wx^3y^2 + wx^3yxy + wx^3yx^2y + w^2x^3yx^3y \\
&= \big(3 + 2(w+1)\big) + \big(2 + 2w\big)x + \big(2 + 2w\big)x^2 + \big(2 + 2w\big)x^3 \\
&\quad + 2wy + 2wxy + 2(w+1)x^2y + 2wx^3y \\
&= 1.
\end{aligned}$$

Next,

$$\begin{aligned}
\beta_3 &= wx^3 + y + (w+1)xy + wx^2y + (w+1)x^3y \\
\beta_3^* &= w(x^3)^{-1} + y + (w+1)(xy)^{-1} + wx^2(y)^{-1} + (w+1)(x^3y)^{-1} \\
&= wx + y + (w+1)xy + wx^2y + (w+1)x^3y
\end{aligned}$$

Multiplying gives

$$\begin{aligned}
\beta_3\beta_3^* = {} & w^2x^4 + wx^3y + w(w+1)x^4y + w^2x^5y + w(w+1)x^6y + wyx + y^2 + (w+1)yxy + wyx^2y + \\
& (w+1)yx^3y + w(w+1)xyx + (w+1)xy^2 + (w+1)^2xyxy + w(w+1)xyx^2y + \\
& (w+1)^2xyx^3y + w^2x^2yx + wx^2y^2 + w(w+1)x^2yxy + w^2x^2yx^2y + w(w+1)x^2yx^3y + \\
& w(w+1)x^3yx + (w+1)x^3y^2 + (w+1)^2x^3yxy + w(w+1)x^3yx^2y + (w+1)^2x^3yx^3y \\
= {} & \big(1 + 2w + 2(w+1)\big) + \big(2 + 2(w+1)\big)x + \big(4w + 2(w+1)\big)x^2 + \big(2 + 2(w+1)\big)x^3 + \\
& 2y + 2(w+1)xy + 2x^2y + 2x^3y \\
= {} & 1.
\end{aligned}$$

Next,

$$\begin{aligned}
\beta_4 &= x^2 + x^3 + xy + wx^2y + wx^3y \\
\beta_4^* &= x^2 + x + xy + wx^2y + wx^3y.
\end{aligned}$$

Multiplying,

$$\begin{aligned}
\beta_4\beta_4^* &= x^4 + x^3 + x^3y + wx^4y + wx^5y + x^5 + x^4 + x^4y + wx^5y + wx^6y \\
&\quad + xyx^2 + xyx + xyxy + wxyx^2y + wxyx^3y + wx^2yx^2 + wx^2yx + wx^2yxy \\
&\quad + w^2x^2yx^2y + w^2x^2yx^3y + wx^3yx^2 + wx^3yx + wx^3yxy + w^2x^3yx^2y + w^2x^3yx^3y \\
&= \big(3 + 2(w+1)\big) + \big(1 + w + (w+1)\big)x + 2wx^2 + \big(1 + w + (w+1)\big)x^3 \\
&\quad + \big(2 + 2w\big)y + 4wxy + 2wx^2y + 2x^3y \\
&= 1.
\end{aligned}$$

For the fifth element we have

$$\begin{aligned}
\beta_5 &= x^2 + x^3 + y + xy + wx^2y + (1+w)x^3y \\
\beta_5^* &= x + x^2 + y + xy + wx^2y + (1+w)x^3y.
\end{aligned}$$

Multiplying gives

$$\begin{aligned}
\beta_5\beta_5^* = {} & x^3 + 1 + x^2y + x^3y + wy + (1+w)xy + 1 + x + x^3y + y + wxy + (1+w)x^2y + yx + yx^2 + \\
& y^2 + yxy + wyx^2y + (1+w)yx^3y + xyx + xyx^2 + xy^2 + xyxy + wxyx^2 + (1+w)xyx^3y + \\
& wx^2yx + wx^2yx^2 + wx^2y^2 + wx^2yxy + w^2x^2yx^2y + w(1+w)x^2yx^3y + (1+w)x^3yx + \\
& (1+w)x^3yx^2 + (1+w)x^3y^2 + (1+w)x^3yxyx + w(1+w)x^3yx^2y + (1+w)^2x^3yx^3y \\
= {} & \big(5 + w + (1+w)\big) + \big(3 + w + (1+w)\big)x + \big(2w + 2(1+w)\big)x^2 + \big(3 + w + (1+w)\big)x^3 + \\
& \big(2 + 2w\big)y + \big(2w + 2(1+w)\big)xy + \big(2 + 2(1+w)\big)x^2y + 4x^3y \\
= {} & 1.
\end{aligned}$$

Next,

$$\begin{aligned}
\beta_6 &= wx^2 + (1+w)x^3 + wxy + x^2y + (1+w)x^3y \\
\beta_6^* &= wx^2 + (1+w)x + wxy + x^2y + (1+w)x^3y.
\end{aligned}$$

Therefore,

$$\begin{aligned}
\beta_6\beta_6^* = {} & w(1+w)x^3 + w^2 + w^2x^3y + wy + w(1+w)xy + (1+w)^2 + w(1+w)x + w(1+w)y + \\
& (1+w)xy + (1+w)^2x^2y + w(1+w)xyx + w^2xyx^2 + w^2xyxy + wxyx^2y + \\
& w(1+w)xyx^3y + (1+w)x^2yx + wx^2yx^2 + wx^2yxy + x^2yx^2y + (1+w)x^2yx^3y + \\
& (1+w)^2x^3yx + w(1+w)x^3yx^2 + w(1+w)x^3yxy + (1+w)x^3yx^2y + (1+w)^2x^3yx^3y \\
= {} & \big(1 + 2w + 2(1+w)\big) + \big(1 + w + (1+w)\big)x + 2x^2 + \big(1 + w + (1+w)\big)x^3 \\
& \big(2 + 2w\big)y + \big(2 + 2(1+w)\big)xy + 2wx^2y + 2\big(1+w\big)x^3y \\
= {} & 1.
\end{aligned}$$

For the seventh element we have

$$\begin{aligned}
\beta_7 &= x + wx^2 + wx^3 + wxy + x^2y + (w+1)x^3y \\
\beta_7^* &= x^3 + wx^2 + wx + wxy + x^2y + (w+1)x^3y.
\end{aligned}$$

Multiplying gives

$$\begin{aligned}
\beta_7\beta_7^* &= x^4 + wx^3 + wx^2 + wx^2y + x^3y + (w+1)x^4y + wx^5 + w^2x^4 + w^2x^3 + w^2x^3y \\
&\quad + wx^4y + w(w+1)x^5y + wx^6 + w^2x^5 + w^2x^4 + w^2x^4y + wx^5y + w(w+1)x^6y \\
&\quad + wxyx^3 + w^2xyx^2 + w^2xyx + w^2xyxy + wxyx^2y + w(w+1)xyx^3y + x^2yx^3 \\
&\quad + wx^2yx^2 + wx^2yx + wx^2yxy + x^2yx^2y + (w+1)x^2yx^3y + (w+1)x^3yx^3 \\
&\quad + w(w+1)x^3yx^2 + w(w+1)x^3yx + w(w+1)x^3yxy + (w+1)x^3yx^2y + (w+1)^2x^3yx^3y \\
&= \big(2 + w + 3(w+1)\big) + \big(2w + 2(w+1)\big)x + \big(2+2w\big)x^2 + \big(2w + 2(w+1)\big)x^3 \\
&\quad \big(2w + 4(w+1)\big)y + \big(2+2w\big)xy + \big(2+2w\big)x^2y + \big(2 + 2(w+1)\big)x^3y \\
&= 1.
\end{aligned}$$

Now,

$$\begin{aligned}
\beta_8 &= x + wx^2 + wx^3 + wy + wxy + (1+w)x^2y + (1+w)x^3y \\
\beta_8^* &= (x)^{-1} + w(x^2)^{-1} + w(x^3)^{-1} + w(y)^{-1} + w(xy)^{-1} + (1+w)(x^2y)^{-1} + (1+w)(x^3y)^{-1} \\
&= x^3 + wx^2 + wx + wy + wxy + (1+w)x^2y + (1+w)x^3y.
\end{aligned}$$

Therefore,

$$\begin{aligned}
\beta_8\beta_8^* &= 1 + wx^3 + wx^2 + wxy + wx^2y + (1+w)x^3y + (1+w)y + wx + w^2 + w^2x^3 + w^2x^3y + \\
&\quad w(1+w)y + w(1+w)xy + wx^2 + w^2x + w^2 + w^2x^3y + w^2y + w(1+w)xy + \\
&\quad w(1+w)x^2y + wyx^3 + w^2yx^2 + w^2y^2 + w^2yxy + w(1+w)yx^2y + w(1+w)yx^3y + \\
&\quad wxyx^3 + w^2xyx^2w^2xyx + w^2xy^2 + w^2xyxy + w(1+w)xyx^2y + w(1+w)xyx^3y + \\
&\quad (1+w)x^2yx^3 + w(1+w)x^2yx^2w(1+w)x^2yx + w(1+w)x^2y^2 + w(1+w)x^2yxy + \\
&\quad (1+w)^2x^2yx^2y + (1+w)^2x^2yx^3 + (1+w)x^3yx^3 + w(1+w)x^3yx^2 + w(1+w)x^3yx + \\
&\quad w(1+w)x^3y^2 + w(1+w)x^3yxy + (w+1)^2x^3yx^2y + (1+w)^2x^3yx^3y \\
&= \big(1 + 2w + 4(1+w)\big) + \big(2 + 2w + 2(1+w)\big)x + \big(4+2w\big)x^2 + \big(2 + 2w + 2(1+w)\big)x^3 + \\
&\quad \big(2 + 4(1+w)\big)y + \big(4+2w\big)xy + \big(2 + 2w + 2(1+w)\big)x^2y + 6(1+w)x^3y \\
&= 1.
\end{aligned}$$

Finally, we have

$$\begin{aligned}
\beta_9 &= wx + x^2 + (w+1)x^3 + y + xy + wx^2y + (w+1)x^3y \\
\beta_9^* &= wx^3 + x^2 + (w+1)x + y + xy + wx^2y + (w+1)x^3y
\end{aligned}$$

Thus,

$$\begin{aligned}
\beta_9\beta_9^* &= w^2x^4 + wx^3 + w(w+1)x^2 + wxy + wx^2y + w^2x^3y + w(w+1)x^4y + wx^5 + x^4 + (w+1)x^3 \\
&\quad + x^2y + x^3y + wx^4y + (w+1)x^5y + w(w+1)x^6 + (w+1)x^5 + (w+1)^2x^4 + \\
&\quad + wyx^2y + (w+1)yx^3y + wxyx^3 + xyx^2 + (w+1)xyx + xy^2 + xyxy + wxyx^2y \\
&\quad + (w+1)xyx^3y + w^2x^2yx^3 + wx^2yx^2 + w(w+1)x^2yx + wx^2y^2 + wx^2yxy + w^2x^2yx^2y \\
&\quad + w(w+1)x^2yx^3y + w(w+1)x^3yx^3 + (w+1)x^3yx^2 + (w+1)^2x^3yx + (w+1)x^3y^2 \\
&\quad + (w+1)x^3yxy + w(w+1)x^3yx^2y + (w+1)^2x^3yx^3y \\
&= \big(3 + 2w + (w+1)\big) + \big(2 + 2w + 2(w+1)\big)x + \big(2 + 2w + 2(w+1)\big)x^2 + \big(2 + 2w + 2(w+1)\big)x^3 \\
&\quad + \big(2 + 2w + 2(w+1)\big)y + \big(2 + 2w + 2(w+1)\big)xy + \big(2 + 4w\big)x^2y + \big(2 + 4(w+1)\big)x^3y \\
&= 1.
\end{aligned}$$

As expected, each of the codes produced are unitary. Next we will use these nine codes to create codes in $(\mathbb{F}_4 + u\mathbb{F}_4)D_8$.

## 5.3 Codes in $(\mathbb{F}_4 + u\mathbb{F}_4)D_8$

The ring $\mathbb{F}_4 + u\mathbb{F}_4$ defined by $\{a + bu \mid a,\ b \in \mathbb{F}_4,\ u^2 = 0\}$ can be viewed as an extension of $\mathbb{F}_4$. The following Gray maps are used to lift the codes in Section 5.2 to generate codes over $\mathbb{F}_4 + u\mathbb{F}_4$:

$$\begin{array}{l|l}
\varphi : (\mathbb{F}_4 + u\mathbb{F}_4)^n \to (\mathbb{F}_2 + u\mathbb{F}_2)^{2n} & \phi : (\mathbb{F}_2 + u\mathbb{F}_2)^n \to \mathbb{F}_2^{2n} \\
aw + b\bar{w} \mapsto (a,b),\ a,b \in (\mathbb{F}_2 + u\mathbb{F}_2)^n & a + bu \mapsto (b, a+b),\ a,\ b \in \mathbb{F}_2^n
\end{array}$$

Using this method we are able to produce the 114 $[64, 32, 12]$ codes found in Appendix B.

J. H. Conway and N. J. A. Sloane [14] provide three possible weight enumerators for codes of length 64. For Type I codes we have

$$\begin{aligned}
W_1(y) &= 1 + (1312 + 16\beta)y^{12} + (22016 - 64\beta)y^{14} + (239148 - 32\beta)y^{16} + \cdots \\
W_2(y) &= 1 + (1312 + 16\beta)y^{12} + (23040 - 64\beta)y^{14} + (228908 - 32\beta)y^{16} + \cdots,
\end{aligned}$$

and for Type II codes:

$$W_3(y) = 1 + 2976y^{12} + 454956y^{16} + 18275616y^{20} + 233419584y^{24} + \cdots.$$

Now, the maps used preserve orthogonality, so self-dual codes should map to self-dual codes. As we have done previously, we will still verify that they are unitary, however we will only do this for those with unique $\beta$ values[1].

[1] Not to be confused with $\beta_i$ from Section 5.2

In the first case, where $\beta = 104$, we have

$$\begin{aligned}
\gamma_1 &= ux^2 + wx^3 + uwy + xy + (w+u+1)x^2y + (uw+u+1)x^3y \\
\gamma_1 &= ux^2 + wx + uwy + xy + (w+u+1)x^2y + (uw+u+1)x^3y.
\end{aligned}$$

Multiplying gives

$$\begin{aligned}
\gamma_1\gamma_1^* = {}& u^2x^4 + uwx^3 + u^2wx^2y + ux^3y + (uw+u^2+u)x^4y + (u^2w+u^2+u)x^5y \\
&+ uwx^5 + w^2x^4 + uw^2x^3y + wx^4y + (w^2+uw+w)x^5y + (uw^2+uw+w)x^6y \\
&+ u^2wyx^2 + uw^2yx + u^2w^2y^2 + uwyxy + (uw^2+u^2w+uw)yx^2y + (u^2w^2+u^2w+uw)yx^3y \\
&+ uxyx^2 + wxyx + uwxy^2 + xyxy + (w+u+1)xyx^2y + (uw+u+1)xyx^3y \\
&+ (uw+u^2+u)x^2yx^2 + (w^2+uw+w)x^2yx + (uw^2+u^2w+uw)x^2y^2 \\
&+ (w+u+1)x^2yxy + (w+u+1)^2x^2yx^2y + (w+u+1)(uw+u+1)x^2yx^3y \\
&+ (u^2w+u^2+u)x^3yx^2 + (uw^2+uw+w)x^3yx + (u^2w^2+u^2w+uw)x^3y^2 \\
&+ (uw+u+1)x^3yxy + (uw+u+1)(w+u+1)x^3yx^2y + (uw+u+1)^2x^3yx^3y \\
= {}& \big(3+2w^2\big) + \big(3uw + (w+u+1) + w^2(u+1)\big)x + \big(2(uw+u+1) + 2(uw^2+uw)\big)x^2 \\
&+ \big(3uw + (w+u+1) + w^2(u+1)\big)x^3 + \big(2w + 2u(w+1)\big)y \\
&+ \big(2uxy + 2(w^2+uw+w)\big)xy + 2\big(uw^2+uw+w\big)x^2y + \big(2u+2uw^2\big)x^3y \\
= {}& 1.
\end{aligned}$$

For the second code, which has $\beta = 8$, we have

$$\begin{aligned}
\gamma_2 &= ux^2 + (w+u)x^3 + uwy + xy + (w+u+1)x^2y + (uw+u+1)x^3y \\
\gamma_2^* &= ux^2 + (w+u)x + uwy + xy + (w+u+1)x^2y + (uw+u+1)x^3y.
\end{aligned}$$

Multiplying gives

$$\begin{aligned}
\gamma_2\gamma_2^* = {}& u^2x^4 + u(w+u)x^3 + u^2wx^2y + ux^3y + (uw+u^2+u)x^4y + (u^2w+u^2+u)x^5y \\
&+ u(w+u)x^5 + (w+u)^2x^4 + uw(w+u)x^3y + (w+u)x^4y + (w+u)(w+u+1)x^5y \\
&+ (w+u)(uw+u+1)x^6y + u^2wyx^2 + uw(w+u)yx + u^2w^2y^2 + uwyxy \\
&+ uw(w+u+1)yx^2y + uw(uw+u+1)yx^3y + uxyx^2 + (w+u)xyx + uwxy^2 \\
&+ xyxy + (w+u+1)xyx^2y + (uw+w+1)xyx^3y + u(w+u+1)x^2yx^2 \\
&+ (w+u)(w+u+1)x^2yx + uw(w+u+1)x^2y^2 + (w+u+1)x^2yxy \\
&+ (w+u+1)^2x^2yx^2y + (w+u+1)(uw+u+1)x^2yx^3y + u(uw+u+1)x^3yx^2 \\
&+ (w+u)(uw+u+1)x^3yx + uw(uw+u+1)x^3y^2 + (uw+u+1)x^3yxy \\
&+ (w+u+1)(uw+u+1)x^3yx^2y + (uw+u+1)^2x^3yx^3y
\end{aligned}$$

$$\begin{aligned}
&= \big(2+w+w^2\big) + \big(3uw + (w+u+1) + w^2(u+1)\big)x + \big(2u + 2(1+u)\big)x^2 \\
&\qquad + \big(3uw + (w+u+1) + w^2(u+1)\big)x^3 + \big(2(u+w) + 2(w+1)\big)y + \big(2u + 2(1+u)\big)xy \\
&\qquad + 2wx^2y + \big(2u + 2uw^2\big)x^3y \\
&= 1.
\end{aligned}$$

The next code with unique $\beta$ is the fifth one in our list, with a $\beta$ value of 24:

$$\begin{aligned}
\gamma_3 &= uwx^2 + wx^3 + (uw+u)y + xy + (w+u+1)x^2y + (u+1)x^3y \\
\gamma_3^* &= uwx^2 + wx + (uw+u)y + xy + (w+u+1)x^2y + (u+1)x^3y.
\end{aligned}$$

Multiplying gives

$$\begin{aligned}
\gamma_3\gamma_3^* &= u^2w^2x^4 + uw^2x^3 + uw(uw+u)x^2y + uwx^3y + uw(w+u+1)x^4y \\
&\quad + uw(u+1)x^5y + uw^2x^5 + w^2x^4 + w(uw+u)x^3y + wx^4y + w(w+u+1)x^5y \\
&\quad + w(u+1)x^6y + uw(uw+u)yx^2 + w(uw+u)yx + (uw+u)^2y^2 \\
&\quad + (uw+u)yxy + (uw+u)(w+u+1)yx^2y + (uw+u)(u+1)yx^3y + uwxyx^2 \\
&\quad + wxyx + (uw+u)xy^2 + xyxy + (w+u+1)xyx^2y + (u+1)xyx^3y \\
&\quad + uw(w+u+1)x^2yx^2 + w(w+u+1)x^2yx + (uw+u)(w+u+1)x^2y^2 \\
&\quad + (w+u+1)x^2yxy + (w+u+1)^2x^2yx^2y + (u+1)(w+u+1)x^2yx^3y \\
&\quad + uw(u+1)x^3yx^2 + w(u+1)x^3yx + (u+1)(uw+u)x^3y^2 \\
&\quad + (u+1)x^3yxy + (u+1)(w+u+1)x^3yx^2y + (u+1)^2x^3yx^3y \\
&= \big(2+w+w^2\big) + \big(uw^2 + 2(uw+u) + (w+u+1) + (uw+w+1)\big)x \\
&\quad + \big(2uw + 2(u+1)\big)x^2 + \big(uw^2 + 2(uw+u) + (w+u+1) + (uw+w+1)\big)x^3 \\
&\quad + \big(2u+2w\big)y\big(2uw + 2w(w+u+1)\big)xy + 2w(u+1)x^2y + \big(2uw + 2w(uw+u)\big)x^3y \\
&= 1.
\end{aligned}$$

Skipping ahead now to the 23rd code in our list which has a $\beta$ value of 40:

$$\begin{aligned}
\gamma_4 &= ux + uwx^2 + wx^3 + uwy + xy + (w+u+1)x^2y + (u+1)x^3y \\
\gamma_4^* &= ux^3 + uwx^2 + wx + uwy + xy + (w+u+1)x^2y + (u+1)x^3y.
\end{aligned}$$

Multiplying gives

$$\begin{aligned}
\gamma_4\gamma_4^* &= u^2x^4 + u^2wx^3 + uwx^2 + u^2wxy + ux^2y + u(w+u+1)x^3y + u(u+1)x^4y \\
&\quad + u^2wx^5 + u^2w^2x^4 + uw^2x^3 + u^2w^2x^2y + uwx^3y + uw(w+u+1)x^4y + uw(u+1)x^5y \\
&\quad + uwx^6 + uw^2x^3 + w^2x^4 + uw^2x^3y + wx^4y + w(w+u+1)x^5y + w(u+1)x^6y \\
&\quad + u^2wyx^3 + u^2w^2yx^2 + uw^2yx + u^2w^2y^2 + uwyxy + uw(w+u+1)yx^2y + uw(u+1)yx^3y
\end{aligned}$$

$$
\begin{aligned}
&\quad + uxyx^3 + uwxyx^2 + wxyx + uwxy^2 + xyxy + (w+u+1)xyx^2y + (u+1)xyx^3y \\
&\quad + u(w+u+1)x^2yx^3 + uw(w+u+1)x^2yx^2 + w(w+u+1)x^2yx + uw(w+u+1)x^2y^2 \\
&\quad + (w+u+1)x^2yxy + (w+u+1)^2x^2yx^2y + (u+1)(w+u+1)x^2yx^3y \\
&\quad + u(u+1)x^3yx^3 + uw(u+1)x^3yx^2 + w(u+1)x^3yx + uw(u+1)x^3y^2 + (u+1)x^3yxy \\
&\quad + (u+1)x^3yxy + (u+1)(w+u+1)x^3yx^2y + (u+1)^2x^3yx^3y \\
&= \big(2 + w + w^2\big) + \big(2uw + uw^2 + (w+u+1) + (uw+w+1)\big)x \\
&\quad + \big(2u + 2uw + 2(u+1)\big)x^2 + \big(2uw + uw^2 + (w+u+1) + (uw+w+1)\big)x^3 \\
&\quad + \big(4u + 2w\big)y + \big(2uw + 2w(w+u+1)\big)xy \\
&\quad + \big(2u + 2w(u+1)\big)x^2y + \big(2uw + 2uw^2 + 2u(w+1)\big)x^3y \\
&= 1.
\end{aligned}
$$

Finally, the 37th code in our list gives us our last unique $\beta$ value of 16:

$$
\begin{aligned}
\gamma_5 &= (uw+u)x + ux^2 + (w+u)x^3 + uwy + xy + (w+1)x^2y + (uw+u+1)x^3y \\
\gamma_5^* &= (uw+u)x^3 + ux^2 + (w+u)x + uwy + xy + (w+1)x^2y + (uw+u+1)x^3y.
\end{aligned}
$$

Multiplying gives

$$
\begin{aligned}
\gamma_5\gamma_5^* &= (uw+u)^2x^4 + u(uw+u)x^3 + (uw+u)(w+u)x^2 + uw(uw+u)xy + (uw+u)x^2y \\
&\quad + (uw+u)(w+1)x^3y + (uw+u)(uw+u+1)x^4y + u(uw+u)x^5 + u^2x^4 + u(w+u)x^3 \\
&\quad + u^2wx^2y + ux^3y + u(w+1)x^4y + u(uw+u+1)x^5y + (w+u)(uw+u)x^6 + u(w+u)x^5 \\
&\quad + (w+u)^2x^4 + uw(w+u)x^3y + (w+u)x^4y + (w+u)(w+1)x^5y + (w+u)(uw+u+1)x^6y \\
&\quad + uw(uw+u)yx^3 + u^2wyx^2 + uw(w+u)yx + u^2w^2y^2 + uwyxy + uw(w+1)yx^2y \\
&\quad + uw(uw+u+1)yx^3y + (uw+u)xyx^3 + uxyx^2 + (w+u)xyx + uwxy^2 + xyxy \\
&\quad + (w+1)xyx^2y + (uw+u+1)xyx^3y + (w+1)(uw+u)x^2yx^3 + u(w+1)x^2yx^2 \\
&\quad + (w+1)(w+u)x^2yx + uw(w+1)x^2y^2 + (w+1)x^2yxy + (w+1)^2x^2yx^2y \\
&\quad + (w+1)(uw+u+1)x^2yx^3y + (uw+u+1)(uw+u)x^3yx^3 + u(uw+u+1)x^3yx^2 \\
&\quad + (w+u)(uw+u+1)x^3yx + uw(uw+u+1)x^3y^2 + (uw+u+1)x^3yxy \\
&\quad + (uw+u+1)(w+1)x^3yx^2y + (uw+u+1)^2x^3yx^3y \\
&= \big(2 + w + w^2\big) + \big(3uw + (w+1) + (uw+w+1)\big)x + \big(3u + 2(uw+u+1) + w(uw+u)\big)x^2 \\
&\quad + \big(3uw + (w+1) + (uw+w+1)\big)x^3 + \big(4u(w+1) + 2(w+u)\big)y \\
&\quad + \big(2u + 2(w^2+uw+u+w)\big)xy + \big(2w + 2(uw+u)\big)x^2y + \big(2u + 2uw + 2uw^2\big)x^3y \\
&= 1.
\end{aligned}
$$

# Appendix A

# Gap Code

For more information on GAP and the Guava package, see [1, 2].

**Listing A.1: Custom Functions**

```
Circulant := function(V)
    local i,C;

    # the first row of C is the input vector V
    C:=[];
    C[1]:=V;

    # each subsequent row places the last element of previous row in    first pos
    # the remaining positions are the first 1..(n-1) elements of previous row
    for i in [2..Size(V)] do
        C[i] := Flat([C[i-1][Size(V)],C[i-1]{[1..Size(V)-1]}]);
    od;
    return(C);
end;

# Notation in an easier to read format
Tidy := function(S)
    local O,R,i;
    O := String(S);
    R := [["<identity ...>","1"],["<identity> of ...","1"],["\<\>",""],["(Z(2)^0)
       *",""],["<zero> of ...","0"],
    ["0*Z(2)","0"],["Z(2)^0","1"]];

    for i in [1..Size(R)] do
        O := ReplacedString(O,R[i][1],R[i][2]);
    od;

    return(O);
end;
```

**Listing A.2: Coding Functions**

```
DihedralGeneratorMatrix := function(d)
    local R,L,C,F,G,V,i,x,y;
    LoadPackage("guava");;

    R:=GF(2);;
    L:=R^d;;
    C:=[];;
    F:=[];;
    G:=[];;
    V:=Elements(L);;

    # circulant function from CustomFunctions.g
    for i in [1..Size(V)] do
        C[i] := Circulant(V[i]);
    od;;

    # create the [A B | B^T A^T] block matrix
    for x in [1..Size(C)] do
        for y in [1..Size(C)] do
            Add(F,BlockMatrix([ [1,1,C[x]] , [1,2,C[y]] , [2,1,TransposedMat(C[y
               ])] , [2,2,TransposedMat(C[x])]],2,2));;
        od;;
    od;;

    # add the identity matrix to the LHS to create the generator matrix
    for i in [1..Size(F)] do
        Add(G,BlockMatrix([ [1,1,IdentityMat(Size(F[1]),GF(2))],[1,2,F[i]]],1,2))
           ;;
    od;;

    return(G);;
end;

GetSelfDual := function(G)
    local S,i;
    S:=[];

    # return only self-dual by checking GG^T = 0
    for i in [1..Size(G)] do
        if G[i]*TransposedMat(G[i]) = 0*IdentityMat(Size(G[i]*TransposedMat(G[i])
           ),GF(2)) then
            Add(S,G[i]);;
        fi;;
    od;;

    return(S);;
end;
```

**Listing A.2: Coding Functions (cont.)**

```
UniqueGenerators := function(S,d)
    local i,j,k,U,seen,D;;
    U:=[];;
    D:=[];;

    # add first element of S to unique list
    Add(U,S[1]);;

    # check each element in S against unique list using IsEquivalent,
    # if the element is not equiv then add it to the unique list
    for i in [2..Size(S)] do
        k := Size(U);;
        seen := 0;;
        for j in [1..k] do
            if IsEquivalent(GeneratorMatCode(S[i],GF(2)),GeneratorMatCode(U[j],GF
                (2))) = true then
                seen := 1;;
                break;;
            fi;
            if seen = 0  and j = k then
                Add(U,S[i]);;
            fi;
        od;
    od;

    # check the minimum distance against the user specified 'd'
    for i in [1..Size(U)] do
        if MinimumDistance(GeneratorMatCode(U[i],GF(2))) >= d then
            Add(D,U[i]);;
        fi;
    od;

    # check whether the codes are Type I or Type II
    # display the code along with type and minimum distance
    for i in D do
        if IsSinglyEvenCode(GeneratorMatCode(i,GF(2))) = true then
            Display(i);;
            Print("Type I self-dual code with MinimumDistance = ",MinimumDistance
                (GeneratorMatCode(i,GF(2))),"\n");;
        elif IsDoublyEvenCode(GeneratorMatCode(i,GF(2))) = true then
            Display(i);;
            Print("Type II self-dual code with MinimumDistance = ",
                MinimumDistance(GeneratorMatCode(i,GF(2))),"\n");;
        fi;
    od;

    return(D);;

end;
```

Listing A.3: Zero Divisor Table

```
## Verification for zero divisors of F_2C_n for any n in the form of a table

# Import Matrix Functions File (to get Circulant() and Tidy())
Read("/home/harrison/Dropbox/Mathematics/Level 7/MA7190 - Research Dissertation/
    GAP/MatrixFunctions.g");

UnitOrZDTable:=function(x)

# define variables etc
    local i,j,k,R,L,G,B,D,S,V,wspace;

    R:=GF(2);           # the set {0,1}
    L:=R^x;             # GF(2)^4
    B:=[];D:=[];G:=[];

# construct all possible vectors over (F_2)^4
    V:=Elements(L);

# convert each vector in V to a circulant matrix
# check the determinant of the matrix
# if |B| = 1 then Unit, if |B| = 0 then ZD
    for i in [1..Size(V)] do
        B[i] := Circulant(V[i]);
        D[i] := Determinant(B[i]);

        if D[i] = Elements(R)[1] then
            G[i] := "Zero Divisor";
        else
            G[i] := "Unit";
        fi;
    od;

# white space for table alignment (not necessary, just to tidy the table)
    S := [[","," "],["0"," "],["1"," "],["[",""],["]",""]];
    wspace := Tidy(V[1]);
    for j in [1..Size(S)] do
        wspace := ReplacedString(wspace,S[j][1],S[j][2]);
    od;

# finally, print the table Circ(v), Det(Circ(v)), Unit/ZD
    for k in [1..Size(B)] do
        if k = 1 then
            Print("\n");
            Print("Circ()",wspace,"\t","Det()","\t\t","Unit/ZeroDivisor","\n");
        fi;
        Print(Tidy(V[k]),"        \t",Tidy(D[k]),"        \t",G[k],"\n");
    od;

end;
```

# Appendix B

# Full Results for $(\mathbb{F}_4 + u\mathbb{F}_4)D_8$

| $\gamma$ | $1$ | $x$ | $x^2$ | $x^3$ | $y$ | $xy$ | $x^2y$ | $x^3y$ | $\beta$ | Weight Enumerator (excl. $y^0$) |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | $u$ | $w$ | $wu$ | 1 | $w+u+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 2 | 0 | 0 | $u$ | $w+u$ | $wu$ | 1 | $w+u+1$ | $wu+u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 3 | 0 | 0 | $wu$ | $w$ | 0 | $wu+1$ | $w+u+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 4 | 0 | 0 | $wu$ | $w$ | $wu+u$ | 1 | $w+1$ | $u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 5 | 0 | 0 | $wu$ | $w$ | $wu+u$ | 1 | $w+u+1$ | $u+1$ | 24 | $1696y^{12}+21504y^{14}+228140y^{16}$ |
| 6 | 0 | 0 | $wu$ | $w$ | $wu+u$ | $wu+1$ | $w+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 7 | 0 | 0 | $wu$ | $w$ | $wu$ | $wu+1$ | $w+1$ | $wu+u+1$ | 24 | $1696y^{12}+21504y^{14}+228140y^{16}$ |
| 8 | 0 | 0 | $wu$ | $w$ | $wu$ | $wu+1$ | $w+u+1$ | $wu+u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 9 | 0 | 0 | $wu$ | $w+u$ | $u$ | 1 | $w+1$ | $u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 10 | 0 | 0 | $wu$ | $w+u$ | $u$ | $wu+1$ | $w+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 11 | 0 | 0 | $wu$ | $w+u$ | $wu+u$ | $wu+1$ | $w+1$ | $wu+u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 12 | 0 | 0 | $wu$ | $w+u$ | $wu+u$ | $wu+1$ | $w+u+1$ | $wu+u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 13 | 0 | 0 | $wu$ | $w+u$ | $wu$ | 1 | $w+u+1$ | $u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 14 | 0 | 0 | $wu$ | $w+u$ | $wu$ | $wu+1$ | $w+1$ | $wu+u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 15 | 0 | 0 | $wu$ | $w+u$ | $wu$ | $wu+1$ | $w+u+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 16 | 0 | $u$ | $u$ | $w$ | $wu+u$ | 1 | $w+u+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 17 | 0 | $u$ | $u$ | $w+u$ | $u$ | 1 | $w+u+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 18 | 0 | $u$ | $u$ | $w+u$ | $wu$ | 1 | $w+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 19 | 0 | $u$ | $wu$ | $w$ | $u$ | 1 | $w+u+1$ | $u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 20 | 0 | $u$ | $wu$ | $w$ | $u$ | $wu+1$ | $w+u+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 21 | 0 | $u$ | $wu$ | $w$ | $wu+u$ | $wu+1$ | $w+1$ | $wu+u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 22 | 0 | $u$ | $wu$ | $w$ | $wu+u$ | $wu+1$ | $w+u+1$ | $wu+u+1$ | 24 | $1696y^{12}+21504y^{14}+228140y^{16}$ |
| 23 | 0 | $u$ | $wu$ | $w$ | $wu$ | 1 | $w+u+1$ | $u+1$ | 40 | $1952y^{12}+20480y^{14}+227628y^{16}$ |
| 24 | 0 | $u$ | $wu$ | $w$ | $wu$ | $wu+1$ | $w+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 25 | 0 | $u$ | $wu$ | $w+u$ | 0 | $wu+1$ | $w+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 26 | 0 | $u$ | $wu$ | $w+u$ | $u$ | 1 | $w+u+1$ | $u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 27 | 0 | $u$ | $wu$ | $w+u$ | $u$ | $wu+1$ | $w+1$ | $wu+u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 28 | 0 | $u$ | $wu$ | $w+u$ | $wu+u$ | 1 | $w+u+1$ | $u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 29 | 0 | $u$ | $wu$ | $w+u$ | $wu+u$ | $wu+1$ | $w+1$ | $wu+u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 30 | 0 | $u$ | $wu$ | $w+u$ | $wu+u$ | $wu+1$ | $w+u+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 31 | 0 | $u$ | $wu$ | $w+u$ | $wu$ | $wu+1$ | $w+1$ | $wu+u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 32 | 0 | $wu+u$ | $u$ | $w$ | $u$ | 1 | $w+u+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 33 | 0 | $wu+u$ | $u$ | $w$ | $wu$ | 1 | $w+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 34 | 0 | $wu+u$ | $u$ | $w$ | $wu$ | 1 | $w+u+1$ | $wu+u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 35 | 0 | $wu+u$ | $u$ | $w+u$ | 0 | 1 | $w+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 36 | 0 | $wu+u$ | $u$ | $w+u$ | $wu+u$ | 1 | $w+u+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 37 | 0 | $wu+u$ | $u$ | $w+u$ | $wu$ | 1 | $w+1$ | $wu+u+1$ | 16 | $1568y^{12}+22016y^{14}+228396y^{16}$ |
| 38 | 0 | $wu+u$ | $wu$ | $w$ | 0 | $wu+1$ | $w+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 39 | 0 | $wu+u$ | $wu$ | $w$ | $u$ | 1 | $w+u+1$ | $u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 40 | 0 | $wu+u$ | $wu$ | $w$ | $wu+u$ | 1 | $w+u+1$ | $u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 41 | 0 | $wu+u$ | $wu$ | $w$ | $wu+u$ | $wu+1$ | $w+u+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |

| No. | 1 | $x$ | $x^2$ | $x^3$ | $y$ | $xy$ | $x^2y$ | $x^3y$ | $\beta$ | Weight Enumerator |
|---|---|---|---|---|---|---|---|---|---|---|
| 42 | 0 | $wu+u$ | $wu$ | $w$ | $wu$ | 1 | $w+1$ | $u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 43 | 0 | $wu+u$ | $wu$ | $w$ | $wu$ | 1 | $w+u+1$ | $u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 44 | 0 | $wu+u$ | $wu$ | $w+u$ | $u$ | 1 | $w+u+1$ | $u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 45 | 0 | $wu+u$ | $wu$ | $w+u$ | $u$ | $wu+1$ | $w+1$ | $wu+u+1$ | 24 | $1696y^{12}+21504y^{14}+228140y^{16}$ |
| 46 | 0 | $wu+u$ | $wu$ | $w+u$ | $u$ | $wu+1$ | $w+u+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 47 | 0 | $wu+u$ | $wu$ | $w+u$ | $wu$ | 1 | $w+1$ | $u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 48 | 0 | $wu$ | $u$ | $w$ | $wu+u$ | 1 | $w+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 49 | 0 | $wu$ | $u$ | $w+u$ | $wu+u$ | 1 | $w+1$ | $wu+u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 50 | 0 | $wu$ | $u$ | $w+u$ | $wu$ | 1 | $w+u+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 51 | 0 | $wu$ | $wu$ | $w$ | $u$ | 1 | $w+1$ | $u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 52 | 0 | $wu$ | $wu$ | $w$ | $u$ | $wu+1$ | $w+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 53 | 0 | $wu$ | $wu$ | $w$ | $wu+u$ | $wu+1$ | $w+1$ | $wu+u+1$ | 40 | $1952y^{12}+20480y^{14}+227628y^{16}$ |
| 54 | 0 | $wu$ | $wu$ | $w$ | $wu+u$ | $wu+1$ | $w+u+1$ | $wu+u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 55 | 0 | $wu$ | $wu$ | $w$ | $wu$ | 1 | $w+1$ | $u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 56 | 0 | $wu$ | $wu$ | $w$ | $wu$ | $wu+1$ | $w+u+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 57 | 0 | $wu$ | $wu$ | $w+u$ | 0 | 1 | $w+u+1$ | $u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 58 | 0 | $wu$ | $wu$ | $w+u$ | 0 | $wu+1$ | $w+1$ | $wu+u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 59 | 0 | $wu$ | $wu$ | $w+u$ | $u$ | 1 | $w+1$ | $u+1$ | 24 | $1696y^{12}+21504y^{14}+228140y^{16}$ |
| 60 | 0 | $wu$ | $wu$ | $w+u$ | $wu+u$ | 1 | $w+1$ | $u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 61 | 0 | $wu$ | $wu$ | $w+u$ | $wu+u$ | $wu+1$ | $w+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 62 | 0 | $wu$ | $wu$ | $w+u$ | $wu$ | 1 | $w+1$ | $u+1$ | 24 | $1696y^{12}+21504y^{14}+228140y^{16}$ |
| 63 | 0 | $wu$ | $wu$ | $w+u$ | $wu$ | $wu+1$ | $w+u+1$ | $wu+u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 64 | $u$ | 0 | $wu+u$ | $w$ | 0 | 1 | $w+u+1$ | $u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 65 | $u$ | 0 | $wu+u$ | $w$ | 0 | $wu+1$ | $w+u+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 66 | $u$ | 0 | $wu+u$ | $w$ | $wu+u$ | $wu+1$ | $w+u+1$ | $wu+u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 67 | $u$ | 0 | $wu+u$ | $w+u$ | $u$ | $wu+1$ | $w+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 68 | $u$ | 0 | $wu+u$ | $w+u$ | $wu+u$ | 1 | $w+1$ | $u+1$ | 40 | $1952y^{12}+20480y^{14}+227628y^{16}$ |
| 69 | $u$ | 0 | $wu+u$ | $w+u$ | $wu+u$ | $wu+1$ | $w+1$ | $wu+u+1$ | 40 | $1952y^{12}+20480y^{14}+227628y^{16}$ |
| 70 | $u$ | 0 | $wu+u$ | $w+u$ | $wu+u$ | $wu+1$ | $w+u+1$ | $wu+u+1$ | 24 | $1696y^{12}+21504y^{14}+228140y^{16}$ |
| 71 | $u$ | 0 | $wu+u$ | $w+u$ | $wu$ | 1 | $w+u+1$ | $u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 72 | $u$ | 0 | $wu+u$ | $w+u$ | $wu$ | $wu+1$ | $w+1$ | $wu+u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 73 | $u$ | 0 | $wu+u$ | $w+u$ | $wu$ | $wu+1$ | $w+u+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 74 | $u$ | $u$ | $wu+u$ | $w$ | 0 | 1 | $w+u+1$ | $u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 75 | $u$ | $u$ | $wu+u$ | $w$ | $u$ | 1 | $w+u+1$ | $u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 76 | $u$ | $u$ | $wu+u$ | $w$ | $u$ | $wu+1$ | $w+u+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 77 | $u$ | $u$ | $wu+u$ | $w$ | $wu$ | 1 | $w+1$ | $u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 78 | $u$ | $u$ | $wu+u$ | $w$ | $wu$ | 1 | $w+u+1$ | $u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 79 | $u$ | $u$ | $wu+u$ | $w$ | $wu$ | $wu+1$ | $w+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 80 | $u$ | $u$ | $wu+u$ | $w+u$ | 0 | 1 | $w+u+1$ | $u+1$ | 24 | $1696y^{12}+21504y^{14}+228140y^{16}$ |
| 81 | $u$ | $u$ | $wu+u$ | $w+u$ | $wu+u$ | $wu+1$ | $w+u+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 82 | $u$ | $u$ | $wu+u$ | $w+u$ | $wu$ | 1 | $w+1$ | $u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 83 | $u$ | $wu+u$ | $wu+u$ | $w$ | 0 | 1 | $w+1$ | $u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 84 | $u$ | $wu+u$ | $wu+u$ | $w$ | 0 | $wu+1$ | $w+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 85 | $u$ | $wu+u$ | $wu+u$ | $w$ | 0 | $wu+1$ | $w+u+1$ | $wu+u+1$ | 24 | $1696y^{12}+21504y^{14}+228140y^{16}$ |
| 86 | $u$ | $wu+u$ | $wu+u$ | $w$ | $u$ | 1 | $w+1$ | $u+1$ | 24 | $1696y^{12}+21504y^{14}+228140y^{16}$ |
| 87 | $u$ | $wu+u$ | $wu+u$ | $w$ | $u$ | 1 | $w+u+1$ | $u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 88 | $u$ | $wu+u$ | $wu+u$ | $w$ | $wu+u$ | 1 | $w+u+1$ | $u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 89 | $u$ | $wu+u$ | $wu+u$ | $w$ | $wu+u$ | $wu+1$ | $w+1$ | $wu+u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 90 | $u$ | $wu+u$ | $wu+u$ | $w$ | $wu$ | $wu+1$ | $w+1$ | $wu+u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 91 | $u$ | $wu+u$ | $wu+u$ | $w+u$ | $u$ | 1 | $w+1$ | $u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 92 | $u$ | $wu+u$ | $wu+u$ | $w+u$ | $wu+u$ | 1 | $w+u+1$ | $u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 93 | $u$ | $wu+u$ | $wu+u$ | $w+u$ | $wu$ | 1 | $w+1$ | $u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 94 | $u$ | $wu+u$ | $wu+u$ | $w+u$ | $wu$ | $wu+1$ | $w+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 95 | $u$ | $wu$ | $wu+u$ | $w$ | $u$ | 1 | $w+1$ | $u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 96 | $u$ | $wu$ | $wu+u$ | $w$ | $wu$ | $wu+1$ | $w+1$ | $wu+u+1$ | 24 | $1696y^{12}+21504y^{14}+228140y^{16}$ |
| 97 | $u$ | $wu$ | $wu+u$ | $w+u$ | 0 | 1 | $w+u+1$ | $u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 98 | $u$ | $wu$ | $wu+u$ | $w+u$ | 0 | $wu+1$ | $w+u+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |

| No. | $1$ | $x$ | $x^2$ | $x^3$ | $y$ | $xy$ | $x^2y$ | $x^3y$ | $\beta$ | Weight Enumerator |
|---|---|---|---|---|---|---|---|---|---|---|
| 99 | $u$ | $wu$ | $wu+u$ | $w+u$ | $wu+u$ | $1$ | $w+1$ | $u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 100 | $u$ | $wu$ | $wu+u$ | $w+u$ | $wu+u$ | $wu+1$ | $w+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 101 | $wu+u$ | $0$ | $wu$ | $w$ | $u$ | $1$ | $w+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 102 | $wu+u$ | $0$ | $wu$ | $w$ | $wu$ | $1$ | $w+u+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 103 | $wu+u$ | $0$ | $wu$ | $w+u$ | $0$ | $1$ | $w+u+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 104 | $wu+u$ | $0$ | $wu$ | $w+u$ | $wu+u$ | $1$ | $w+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 105 | $wu+u$ | $u$ | $wu$ | $w$ | $0$ | $1$ | $w+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 106 | $wu+u$ | $u$ | $wu$ | $w+u$ | $u$ | $1$ | $w+u+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 107 | $wu+u$ | $wu+u$ | $wu$ | $w$ | $u$ | $1$ | $w+1$ | $wu+u+1$ | 8 | $1440y^{12}+22528y^{14}+228652y^{16}$ |
| 108 | $wu+u$ | $wu+u$ | $wu$ | $w$ | $u$ | $1$ | $w+u+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 109 | $wu+u$ | $wu+u$ | $wu$ | $w+u$ | $0$ | $1$ | $w+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 110 | $wu+u$ | $wu$ | $wu$ | $w$ | $0$ | $1$ | $w+u+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 111 | $wu+u$ | $wu$ | $wu$ | $w$ | $u$ | $1$ | $w+1$ | $wu+u+1$ | 16 | $1568y^{12}+22016y^{14}+228396y^{16}$ |
| 112 | $wu+u$ | $wu$ | $wu$ | $w$ | $wu+u$ | $1$ | $w+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 113 | $wu+u$ | $wu$ | $wu$ | $w+u$ | $u$ | $1$ | $w+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |
| 114 | $wu+u$ | $wu$ | $wu$ | $w+u$ | $wu$ | $1$ | $w+u+1$ | $wu+u+1$ | 104 | $2976y^{12}+454956y^{16}$ |

# Bibliography

[1] J. Cramwinckel et al. *A GAP4 Package for computing with error-correcting codes*. `https://www.gap-system.org/Manuals/pkg/guava-3.12/htm/chap0.html`. 2012.

[2] Multiple Authors. *GAP - Reference Manual*. `https://www.gap-system.org/Manuals/doc/ref/chap0.html`. 2016.

[3] J.A. Beachy and W.D. Blair. *Abstract Algebra*. Waveland Press, 2006. ISBN: 9781577664437.

[4] L. Creedon and J. Gildea. “The Structure of the Unit Group of the Group Algebra $\mathbb{F}_{2^k}D_8$”. In: *Canad. Math. Bull.* 54.2 (2011), pp. 237–243.

[5] Philip J. Davis. *Circulant Matrices*. 1st ed. Pure & Applied Mathematics. John Wiley & Sons Inc, 1979. ISBN: 0471057711,9780471057710.

[6] J. Gildea. “The Structure of the Unitary Units of the Group Algebra $\mathbb{F}_{2^k}D_8$”. In: *International Electronic Journal of Algebra* 9 (2011), pp. 171–176.

[7] R. Hill. *A First Course in Coding Theory*. Oxford applied mathematics and computing science series. Oxford, Oxfordshire: Clarendon Press New York, 1986. ISBN: 0-19-853804-9.

[8] W. Cary Huffman and Vera Pless. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2003. ISBN: 9780521782807.

[9] John F. Humphreys. *A Course in Group Theory*. Oxford science publications. Oxford University Press, 1996. ISBN: 9780198534594.

[10] B. Hurley and T. Hurley. “Systems of MDS Codes from Units and Idempotents”. In: *Discrete Mathematics* 355.11 (2014), pp. 81–91.

[11] P. Hurley and T. Hurley. “Codes from Zero-Divisors and units in group Rings”. In: *Int. J. Inf. Coding Theory* 1.1 (2009), pp. 57–87.

[12] T. Hurley. “Group Rings and Rings of Matrices”. In: *Int. J. Pure Appl. Math.* 31.3 (2006), pp. 319–335.

[13] R. Taylor J. Gildea A. Kaya and B. Yildiz. “Binary Generator Matrices for Some Extremal Binary Self-dual Codes of Length 64”. submitted.

[14] N. J. A. Sloane J. H. Conway. “A New Upper Bound on the Minimum Distance of Self-Dual Codes”. In: *IEEE Trans. Inform. Theory* 36 (1990), pp. 1319–1333.

[15] G. Karpilovsky. *Unit Groups of Group Rings*. Pitman Monographs and Surveys in Pure and Applied Mathematics. Longman Scientific & Technical, 1989. ISBN: 9780470213698.

[16] S. Lang. *Algebra (Graduate Texts in Mathematics)*. Springer, 2005. ISBN: 038795385X.

[17] C. Polcino Milies and S. Sehgal. *An Introduction to Group Rings*. Algebras and Applications. Kluwer Academic Publishers, Dordrecht, 2002. ISBN: 9781402002380.

[18] D.S. Passman. *The Algebraic Structure of Group Rings*. Dover Publications, 2011. ISBN: 9780486482064.

[19] R. Taylor S. Dougherty J. Gildea and A. Tylyschak. "Constructions of Self-Dual and Formally Self-Dual Codes from Group Rings". In: *CoRR* (2016). `https://arxiv.org/abs/1604.07863`.