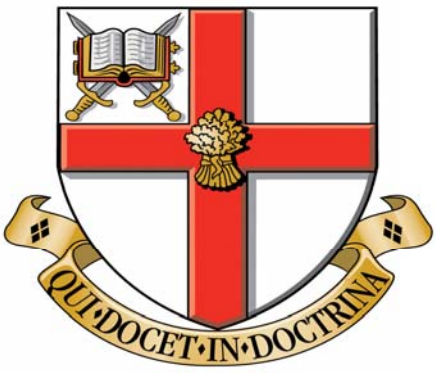


University of Chester

Units of Modular Group Algebras

by

Hilary C. Okoh

A thesis submitted to the School of Computer Science and Mathematics
Faculty of Science and Engineering
in partial fulfillment of the requirement for the degree of
Masters of Science in Mathematics

UNIVERSITY OF CHESTER

Supervised by.....

Dr. Joe Gildea
Faculty of Science and Engineering

September, 2014

To my uncle Engr. Tony Okoh, my parents Mr and Mrs P.N. Okoh and my siblings.

Acknowledgments

The success of this study depended on the support and encouragement of many. I take this opportunity to express my sincere gratitude to everyone who played instrumental in the successful completion of this thesis.

My deepest appreciation goes **to my thesis supervisor**: Dr. Joe Gildea, whose constant guidance helped me during the course of this study-from the thesis proposal up to the thesis manuscript. Without his guidance, timely criticisms and persistent help, this study would not have been possible.

I am very much thankful **to all Staff** in the Mathematics Department-University of Chester; for the privilege given to study under their tutelage. It was indeed a humbling experience to be taught by and more so learn from experienced and qualified academia.

Words cannot express how much indebted I am **to my very supportive uncle, Engr. Tony Okoh**: Thank you very much Sir for the opportunity you provided me to study overseas and most importantly in a recognised university in North-west England. I pray the source of your generousity stays kindled and never run 'dry'.

To all my friends and course mates in the university: Christian, Andy, Fiona, Jamie, Hasna, Julie, Kolawole, Temitope and especially Paul Useni. Even though you are not directly involved in this study, I thank you all for the moral support, encouragements and bondings that I will forever treasure. It really was an amazing time getting to know all of you and the fact that you all had a good work ethic challenged me to work harder as well.

To my present and former house mates: Thank you all for ensuring a condusive and homely atmosphere for study and rest. In a very special way, I thank Theethanat, Luke, Gemma, Ceri, Isobelle, Cheryl, Vicky, Jessica and Holly for their care and concern all through my academic year.

To the Catholic Society of St.Werburghs: The success of my academic year is not exclusive to study alone as you all played a significant role in my success by being good friends and brethren as well. It was a pleasure knowing all of you and I pray you grow and stay in the faith. A very big appreciation goes to the Chaplain of St Werburghs-Father Paul Shaw, for his tremendous assistance in my academic year and for being a source of motivation thus far.

To my beloved family: Thanks very much for being my 'backbone' and for being there for me through 'thick and thin'. Words are never enough to describe the delight and joy I feel to have you all. Thanks for the prayers as well, and I pray we continue to grow cohesively.

Last but not the least, **I would like to thank Jesus Christ** for the grace conferred on me to see this study to a successful end. All I am and all I have achieved today are testimonies to Christ's unequaled and abundant love for me. Thank you Lord, for blessing me much more than I deserve, cause without you I am nothing.

Contents

Abstract

Let RG denote the group ring of the group G over the ring R and $\mathcal{U}(RG)$ denote the unit group of RG. The objective of this thesis is to become familiar with the techniques used to establish $\mathcal{U}(RG)$ in a recently published article.

We begin with an introduction to groups, rings and fields. Group rings are then discussed and in particular, the decomposition of RG. We conclude with the structure of $\mathcal{U}(\mathbb{F}_{3^k} D_6)$.

Chapter 1

Introduction to Groups

We begin this investigation by defining some basic terminology associated with group theory and cite some examples as well. A good understanding of groups would enhance the comprehension of subsequent chapters. We establish what groups and subgroups are and go further to consider some types of groups and subgroups like dihedral group, quotient group, normal subgroup, commutator subgroup etcetera.

1.1 Groups

Definition 1.1 [9] *Let $(G, *)$ denote a nonempty set G together with a binary operation $*$ on G. That is, the following condition must be satisfied.*

(i) Closure: For all $a, b \in G$, the element $a * b$ is a well-defined element of G.
Then G is called a group if the following properties hold.

(a) Associativity: For all $a, b, c \in G$, we have $a * (b * c) = (a * b) * c$.

(b) Identity: There exists an identity element $e \in G$, that is, an element $e \in G$ such that $e * a = a$ and $a * e = a$ for all $a \in G$.

(c) Inverses: For each $a \in G$ there exists an inverse element $a^{-1} \in G$, that is, an element $a^{-1} \in G$ such that $a * a^{-1} = e$ and $a^{-1} * a = e$.

Definition 1.2 [9] *A group G is abelian if $a * b = b * a$ for all a, $b \in G$.*

Example 1.3 [9] *($M_n(R)$ under addition)*
The set of all $n \times n$ with entries in R forms a group under matrix additon. Since addition is defined componentwise, the zero matrix is the identity of $M_n(R)$, and the additive inverse of a matrix is it's negative.

Definition 1.4 [9] *A group G is said to be a finite group if the set G has a finite number of elements. In this case, the number of elements is called the order of G, denoted by $|G|$. If G is not finite, it is said to be an infinite group.*

We have different types of groups which we will discuss much later in the chapter but we need to introduce what a subgroup is to understand them better.

1.2 Subgroups

A very important extension of groups is a what we call a subgroup, these are formed from subsets of groups. Here we consider a type of subgroup called normal subgroups and commutator subgroups citing examples and proofs where necessary.

Definition 1.5 [9] *Let G be a group, and let H be a subset of G. Then H is called a subgroup of G if H is itself a group, under the operation induced by G.*

Example 1.6 [9] *We know Z,Q,R, and C to be groups under ordinary addition. Furthermore, as sets we have*
$Z \subseteq Q \subseteq R \subseteq C$
and each group is a subgroup of the next since the given operations are consistent.
If we consider multiplicative groups of nonzero elements, we also have the subgroups $Q^x \subseteq R^x \subseteq C^x$

Example 1.7 [9] *$(SL_2(R) \subseteq GL_2(R))$.*

Let $GL_2(R)$ be the set of all 2×2 invertible matrices over the real numbers R. The set of 2×2 with determinant equal to 1 is a subgroup of $GL_2(R)$, which can be seen easily as follows: if $A, B \in GL_2(R)$ with $det(A) = 1$ and $det(B) = 1$, then we have $det(AB) = det(A)det(B) = 1$. The associative law holds for all 2×2 matrices. The identity matrix certainly has determinant equal to 1, and if $det(A) = 1$ then $det(A^{-1}) = 1$.
The set of all $n \times n$ matrices over R with determinant equal to 1 is called the special linear group over R, denoted by $SL_n(R)$. Thus we have shown that $SL_2(R)$ is a subgroup of $GL_2(R)$.

Example 1.8 [9] *In the group $GL_2(R)$ of all invertible 2×2 matrices with real entries, let H be the following set of matrices:*

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

This set of matrices form the direct product of the ring of order two $C_2 \times C_2$ because the elements in the set of matrices are of order two, hence cannot be C_4. It is easy to see that the product of any two of these matrices is a diagonal matrix with entries ± 1, which again will be in the set. Since the set is finite and closed under matrix multiplication

Proposition 1.9 [9] *Let G be a group with identity element, and let H be a subset of G. Then H is a subgroup of G if and only if the following conditions hold:*

(i) $ab \in G$ *for all* $a, b \in H$;

(ii) $e \in h$;

(iii) $a^{-1} \in H$ *for all* $a \in H$.

Proof. First, assume that H is a subgroup of G. Since H is a group under the operation of G, the closure axiom guarantees that ab must belong to H whenever a, b belong to H. There must be identity element, say $e^{'}$, for H. Then considering the product in H, we have $e^{'}e^{'} = e^{'}$. Now consider the same product as an element of G. Then we can write $e^{'}e^{'} = e^{'}e$, and the cancellation law yields $e^{'} = e$. Finally, if $a \in H$, then a must have an inverse b in H, with $ab = e$. But then in G we have $ab = e = aa^{-1}$, and the cancellation law implies that $a^{-1} = b$ is an element of H.
Conversely, suppose that H is a subset of G that satisfies the given conditions. Condition **i** shows that the operation of G defines a binary operation on H, and so the closure axioms hold. If $a, b, c \in H$, then in G we have the equation $a(bc) = (ab)c$, and so by considering this as an equation in H we see that H inherits the associative law. Conditions **(ii)** and **(iii)** assure that H has an identity element, and that every element of H has an inverse in H, since these elements have the same properties in H as they do when viewed as elements of G.
Using the previous proposition, it is easy to see that for any group G, the entire set G is certainly a subgroup. At the other extreme, the set e consisting of only the identity element is always a subgroup of G, called the trivial subgroup.

The next corollary shortens the subgroup conditions. In applying these conditions, it is crucial to show that the subset H is nonempty. Often the easiest way to do this is to show that H contains the identity element e. ■

Corollary 1.10 [9] *Let G be a group and let H be a subset of G. Then H is a subgroup of G if and only if H is a nonempty and $ab^{-1} \in H$ for all $a, b \in H$.*

Proof. First assume that H is a subgroup of G. Using condition **(ii)** of the previous proposition, we see that H is nonempty since $e \in H$. If $a, b \in H$, the $b^{-1} \in H$ by condition **(iii)** of the proposition, and so condition **(i)** implies that a $b^{-1} \in H$.
Conversely, suppose that H is a nonempty subset of G such that $ab^{1} \in H$ for all $a, b \in H$. Since H is nonempty, there is at least one element a that belongs to H. Then $e \in H$ since $e = aa^{-1}$, and this product belongs to H by assumption. Next, if $a \in H$, then a^{-1} can be expressed in the form $a^{-1} = ea^{-1}$, and this product must belong to H since e and a belong to H. Finally, we must show that H is closed under products: if $a, b \in H$, then we have already shown that $b^{-1} \in H$. We can express ab in the form $a(b^{-1})^{-1}$, and then the given conditions show that ab must belong to H.

If the subset in question known to be finite(and nonempty), then it is only necessary to check the closure axiom. This is a bit surprising, but very useful. The crucial step in the proof of the next corollary is to show that in this case the inverse of each element in the set can be expressed as a positive power of the element. ■

Corollary 1.11 [9] *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 $ab \in H$ for all $a, b \in H$.*

Proof. If H is a subgroup of G, then Proposition **??** implies that $ab \in H$ for all $a, b \in H$. Conversely, assume that H is closed under the operation of G. We can use the previous corollary, provided we can show that $b^{-1} \in H$ whenever $b \in H$. Given $b \in H$, consider the powers $b, b^2, b^3, ...$ of b. These must all belong to H, by assumption, but since H is a finite set, they cannot all be distinct. There must be some repetition, say $b^n = b^m$ for positive integers $n > m$. The cancellation law then implies that $b^{n-m} = e$. Either $b = e$ or $n - m > 1$, and in the second case we then have $bb^{n-m-1} = e$, which shows that $b^{-1} = b^{n-m-1}$. Thus b^{-1} can be expressed as a positive power of b, which must belong to H. ■

Proposition 1.12 [9] *Let G be a group, and let $a \in G$.*

(a) The set $< a >$ is a subgroup of G.

(b) If K is any subgroup of G such that $a \in K$, then $< a > \subseteq K$.

Proof.

(a) The set $< a >$ is closed under multiplication since if a^m, $a^n \in < a >$, then $a^m\, a^n = a^{m+n} \in < a >$. Furthermore, $< a >$ includes the identity element and includes inverses, since by definition $a^0 = e$ and $(a^n)^{-1} = a^{-n}$.

(b) If K is any subgroup that contains a, then it must contain all positive powers of a since it is closed under multiplication. It also contains $a^0 = e$, and if $n < 0$, then $a^n \in K$ since $a^n = (a^n)^{-1}$. Thus $< a > \subseteq K$.

Thus the intersection of any collection of subgroups is again a subgroup. Given any subset S of a group G, the intersection of all subgroups of G that contains S is in fact the smallest subgroup that contains S. In the cases $S = a$, by the previous proposition we obtain $< a >$. In the cases of two elements a, b of a nonabelian group G, it becomes much more complicated to describe the smallest subgroup of G that contains a and b. The general problem of listing all subgroups of a given group becomes difficult very quickly as the order of the group increases. ■

Corollary 1.13 [9] *Let G be a finite group of order n.*

(a) For any $a \in G$, $\circ(a)$ is a divisor of n.

(b) For any $a \in G$, $a^n = e$.

Proof.

(a) The order of a is the same as the order of $< a >$, which by langrange's theorem is a divisor of the order of G.

(b) If a has order m, then by part (a) we have $n = mq$ for some integer q. Thus $a^n = a^{mq} = (a^m)^q = e$. ■

Corollary 1.14 [9] *Any group of prime order is cyclic.*

Proof. Let G be a group of order p, where p is a prime number . Let a be an element of G different from e. Then the order of $< a >$ is not 1, and so it must be p since it is a divisor of p. This implies that $< a >= G$, and thus G is cyclic. ■

1.3 Normal Subgroups

Definition 1.15 [2] *Let H be a subgroup of the group G. We say that H is a normal subgroup if $gH = Hg$, for all $g \in G$. If H is a normal subgroup, we can safely talk about it's cosets. We denote the set of all these cosets by G/H.*

Theorem 1.16 [2] *Let H be a subgroup of the group G. Then H is normal in G if and only if $g^{-1}Hg = H$,for all $g \in G$. Infact, this is true if and only if $g^{-1}Hg \subseteq H$, for all $g \in G$.*

Proof. Suppose that H is normal in G and $g \in G$; then $Hg = gH$. So for any $h \in H$, there exists $h_1 \in H$ such that $hg = gh_1$. But then $g^{-1}hg = h_1 \in H$. Thus, $g^{-1}Hg \subseteq H$.

Conversely, suppose that $g^{-1}Hg = H$ for all $g \in G$. Given any element $h \in H$, this means that $h = g^{-1}h_1g$, for some $h_1 \in H$. But then $gh = h_1g$; that is, $gH \subseteq Hg$. ■

Example 1.17 *Suppose a dihedral group $G = D_6 = \{1, x, x^2, y, xy, x^2y\}$ and $N = \{1, x, x^2\}$ is a subgroup, then $yN = \{y, yx, yx^{'}\} = \{y, x^2y, xy\} = \{y, xy, x^2y\} = Ny$. Hence a normal subgroup.*

Theorem 1.18 [2] *Let H be a normal subgroup of G. Then the set G/H of cosets of H in G is a group, under the operation $(Ha)(Hb) = Hab$.*

Proof. We must first check that the operation specified in the statement of the theorem is well defined; that is, it should be independent of coset representatives. This verification is the crucial part of the proof, and will depend in an essential way on the fact that H is normal.

Suppose then that $Ha = Hc$ and $Hb = Hd$. We claim that $Hab = Hcd$, this amounts to checking

that $ab(cd)^{-1} \in H$. Because $Hb = Hd$, we know that $bd^{-1} \in H$. Now H is a normal subgroup, and so $aH = Ha$. This means that $a(bd^{-1}) = ha$ for some $h \in H$.

Thus, $ab(cd)^{-1} = abd^{-1} = hac^{-1}$

But $Ha = Hc$ means exactly that $ac^{-1} \in H$, and so therefore $hac^{-1} \in H$ too. This completes the proof that the operation is well defined.

The operation is clearly associative:

$(HaHb)(Hc) = HabHc = H(ab)c = Ha(bc) = HaHbc = Ha(HbHc)$.

The element $H1$ serves as the identity for G/H: $H1Ha = H1a = Ha = Ha1 = HaH1$.

And the element Ha has an inverse; namely, $Ha^{-1}Ha$.
Thus, G/H is a group, as we claim. ■

Example 1.19 [2] *Consider the subgroup $H = \{\iota, (12)\}$ of a symmetric group S_3. We obtain three distinct right cosets, as follows:*

$H\iota = H(12) = \{\iota, (12)\} = H$,

$H(123) = H(23) = \{(123), (23)\}$,

and,

$H(132) = H(13) = \{(132), (13)\}$.
The subgroup H is obviously a coset of itself; we obtained this by choosing the two elements in H itself. The other two cosets also have two elements each.

Example 1.20 [2] *Consider the group*

$\mathcal{U}(\mathbb{Z}_{21}) = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$.

Let's compute the right cosets of the subgroup $H = \{1, 4, 16\}$:

We obtain:
$H1 = H4 = H16 = 1, 4, 16$,

$H2 = H8 = H11 = 2, 8, 11$,

$H10 = H13 = H19 = 10, 13, 19$,

and $H5 = H20 = H17 = 5, 20, 17$.

Theorem 1.21 [2] ***(The Coset Theorem)***
Let H be a subgroup of a group G, and $a, b \in G$. Then

(a) If $Ha \subseteq Hb$, then $Ha = Hb$.

(b) If $Ha \cap Hb \neq= \emptyset$, then $Ha = Hb$.

(c) $Ha = Hb$, if and only if $ab^{-1} \in H$.

(d) There exists a one-to-one and onto function between any two right cosets Ha and Hb. Thus, if H has finitely many elements, every right coset has the that same number of elements.

Proof.

(a) Suppose that H is a subgroup of the group G, and a and b are elements of the group for which $Ha \subseteq Hb$. Then

$a = 1a \in Ha \subseteq Hb$,

and so there exists $h \in H$ such that $a = hb$. But then $b = h^{-1}a \in Ha$. Now, if $k \in H, kb = kh^{-1}a \in Ha$, and so $Hb \subseteq Ha$. That is, $Ha = Hb$.

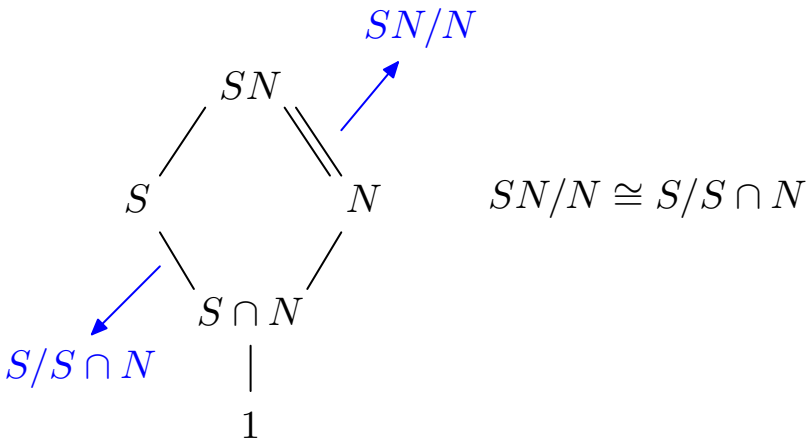
(b) Suppose that $Ha \cap Hb \neq \emptyset$. Choose c in this intersection. Then $c \in Ha$, and so $Hc \subseteq Ha$. But then by apart (a), $Hc = Ha$. But similarly, $Hc = Hb$, and so $Ha = Hb$.

(c) If $Ha = Hb$, then $a = 1a \in Ha = Hb$, and so there exists $h \in H$ such that $a = hb$. But then $ab^{-1} = h \in H$, as required. Conversely, if $ab^{-1} \in H$, then $a = ab^{-1}b \in Hb$. But then $a \in Ha \cap Hb$, and so by part (b) $Ha = Hb$.

(d) Define the function $\varphi : Ha \to Hb$ by $\varphi(x) = xa^{-1}b$. First, note that if $x \in Ha$, then $x = ha$, for $h \in H$. But then $\varphi(x) = \varphi(ha) = (ha)(a^{-1}b) = hb \in Hb$. Thus, our function is well defined. It is one-to-one, because if $\varphi(x) = \varphi(y)$, then $xa^{-1}b = ya^{-1}b$, and multiplying on the right by b^{-1} a gives us that $x = y$. It is onto, because if we choose the arbitrary element $hb \in Hb$, then $\varphi(ha) = ha(a^{-1}b) = hb$. ■

Theorem 1.22 [2] *Let G be a group, S be a subgroup of G and N be a normal subgroup of G. Then*

1. *The product SN is a subgroup of G,*
2. *The intersection $S \cap N$ is a normal subgroup of S, and*
3. *The quotient groups SN/N and $S/(S \cap N)$ are isomorphic.*



Theorem 1.23 [2] *Let G be a group and H a normal subgroup of G. Then the operation $*$ given by (Q) is well defined.*

Proof. We need to show that if $g_1, g_2, k_1, k_2 \in G$ are such that $g_1H = g_2H$ and $k_1H = k_2H$, then $g_1k_1H = g_2k_2H$.
If ${g_1}^{-1}g_2 \in H$ and ${k_1}^{-1}k_2 \in H$, then $(g_1k_1)^{-1}g_2k_2 \in H$.

So, assume that ${g_1}^{-1}g_2 \in H$ and ${k_1}^{k_2} \in h$. Then there exist $h, h^{'} \in H$ such that ${g_1}^{-1}g_2 = h$ and ${k_1}^{-1}k_2 = h^{'}$, and thus $k_2 = k_1h^{'}$.

Hence, $(g_1k_1)^{-1}g_2k_2 = {k_1}^{-1}{g_1}^{-1}g_2k_2 = {k_1}^{-1}hk_1h^{'} = (k_1^{-1}hk_1)h^{'}$.

Since H is normal, ${k_1}^{-1}hk_1 \in H$, and so $(k_1^{-1}hk_1)h^{'} \in H$.
Thus, theorem is proved. ■

Example 1.24 [2] *Let $G = \mathcal{Z}$ and $H = n\mathcal{Z}$. H is a subgroup and, since G is abelian, it is normal. The right cosets of $H \in G$ are: $H, H+1, \ldots, H+(n-1)$. It should be clear at this point that these cosets coincide with the congruence classes mod n:*

$H = [0] \qquad H + 1 = [1] \quad \therefore \quad H + (n-1) = [n-1].$

Moreover, the binary operation is given by: $H + a * H + b = H + (a + b)$, which is better written as

$(H + a) + (H + b) = H + (a + b) \quad i.e \quad [a] + [b] = [a + b],$

which is the usual addition mod n. Hence,

$\mathcal{Z}/n\mathcal{Z} = \mathcal{Z}_n.$

That is, the definition of addition modn is exactly the binary operation that $\mathcal{Z}_\backslash$ inherits as the quotient group of $\mathcal{Z}$ over $n\mathcal{Z}$.

Definition 1.25 [14] *Let G be a group. An element $g \in G$ is called a commutator if*

$$g = xyx^{-1}y^{-1}$$

for elements $x, y \in G$. The commutator subgroup (also called a derived group) of a group G denoted by $G^{'}$ or $[G, G]$ is the subgroup generated by the commutators of its elements. It is the unique smallest normal subgroup of G such that $G/[G, G]$ is Abelian.

For better understanding of the examples below, see Example 1.32 and 1.33 for the structure of D_6 and D_{10} respectively.

Example 1.26 [10] *The commutator subgroup of D_6; $D_6^{'} = \{1, x^2, x^4\}$ The set $D_6/D_6^{'}$ of all the left cosets of $D_6^{'}$ is given by*

$$1\,D_6^{'} = \{1, x^2, x^4\},\ x\,D_6^{'} = \{x, x^3, x^5\}$$
$$y\,D_6^{'} = \{y, y\,x^2, y\,x^4\},\ y\,x\,D_6^{'} = \{y\,x, y\,x^3, y\,x^5\}$$

Thus we have two generators for this group, namely $x\,D_6^{'}$ and $y\,D_6^{'}$. Therefore, $D_6^{'}$ is Abelian given by $D_6/D_6^{'} \cong C_2 \times C_2$.

Example 1.27 [10] *The commutator subgroup of D_{10} ; $D_{10}^{'} = \{1,\ x,\ x^2,\ x^3,\ x^4\} \cong C_5$*

1.4 Quotient Group

Definition 1.28 [11] *Given a group G and a normal subgroup H, the group $(G/H, *)$, or simply G/H, is known as the quotient (factor) group of G over H.*

Let G be a group and H a subgroup of G. Denote by G/H the set of distinct(left) cosets with respect to H. In other words, we will list all the cosets of the form gH(with $g \in G$) without repetitions and consider each coset as a single element of the newly formed set G/H. The set G/H (pronounced G *mod* H) is called the quotient set.
Next we would like to define a binary operation $*$ on G/H such that $(G/H, *)$ is a group.It is natural to try to define the operation $*$ by the formula
$gH * kH = gkH$ for all $g, k \in G$.

1.5 Dihedral Group

Dihedral groups form an important part of this study as the dihedral group of order six D_6 is used in most calculations and proofs in the group ring and unit algebra chapters. For the sake of this study, the dihedral group of order 8 is considered in detail and a cayley table is constructed alike.

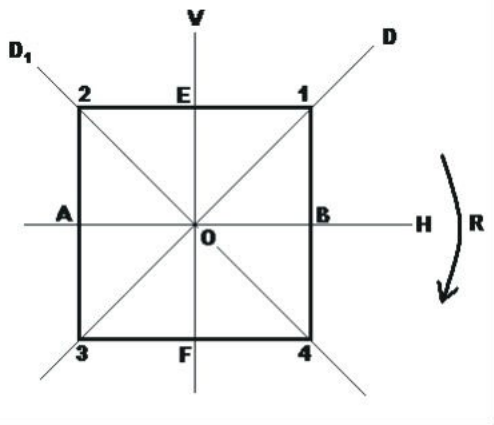
Definition 1.29 *The dihedral group D_n is the symmetry group of an n-sided regular polygon for $n > 1$. The group order of D_n is $2n$. Dihedral groups D_n are non-Abelian permutation groups for $n > 2$* [10].

This means that a regular polygon with n sides has $2n$ different symmetries: n rotational symmetries and n reflection symmetries. The associated rotations and reflections make up the dihedral group

D_n. If n is odd each axis of symmetry connects the midpoint of one side to the opposite vertex. If n is even there are $\frac{n}{2}$ axes of symmetry connecting the midpoints of opposite sides and $\frac{n}{2}$ axes of symmetry connecting opposite vertices. In either case, there are n axes of symmetry altogether and $2n$ elements in the symmetry group.

Definition 1.30 *Group Structure* $\{D_8\}$
Consider a square:
There are eight motions of this square which, when performed one after the other, form a group called the Dihedral Group of order 8. *They are:*

(i) R_1 $0°$ *rotation (clockwise)*
(ii) R_2 $90°$ *rotation (clockwise)*
(iii) R_3 $180°$ *rotation (clockwise)*
(iv) R_4 $270°$ *rotation (clockwise)*
(v) S_1 *reflection about horizontal axis* AB
(vi) S_2 *reflection about vertical axis* EF
(vii) S_3 *reflection about diagonal 1-O-3*
(viii) S_4 *reflection about diagonal 2-O-4*



The Dihedral Group of the Square then is given by $G = [R_1, R_2, R_3, R_4, S_1, S_2, S_3, S_4]$.

Multiplication in G consists of performing two of these motions in succession. Thus the product S_3R_2 corresponds to first performing operation S_3, then operation R_2. A multiplication table for G is shown in Figure. Entries in the table contain the product ab where a corresponds to the row and b corresponds to the column. Thus in the table $S_3R_2 = S_2$.

The eight motions R_1, R_2, R_3, R_4, S_1, S_2, S_3, S_4 can be represented as permutations of the numbers 1, 2, 3, and 4 where these numbers correspond to the four vertices of the square as shown in Figure [1.1]The permutation representation of G is:

$G = [(1), (1432), (13)(42), (1234), (14)(23), (12)(43), (42), (13)]$

Where,

$$R_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = (1)(2)(3)(4) = 1$$

$$R_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1\ 2\ 3\ 4)$$

$$R_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1\ 3)(2\ 4)$$

$$R_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = (1\ 4\ 3\ 2)$$

$$S_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1\ 2)(3\ 4)$$

$$S_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = (1\ 3)(2)(4) = (13)$$

$$S_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (1\ 4)(2\ 3)$$

$$S_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (1)(2\ 4)(4) = (24)$$

The table below corresponds to the multiplication of permutations in G. See [12] for clarity.

	R_1	R_2	R_3	R_4	S_1	S_2	S_3	S_4
R_1	R_1	R_2	R_3	R_4	S_1	S_2	S_3	S_4
R_2	R_2	R_3	R_4	R_1	S_4	S_1	S_2	S_3
R_3	R_3	R_4	R_1	R_2	S_2	S_1	S_4	S_3
R_4	R_4	R_1	R_2	R_3	S_3	S_4	S_2	S_1
S_1	S_1	S_3	S_2	S_4	R_1	R_3	R_2	R_4
S_2	S_2	S_4	S_1	S_3	R_3	R_1	R_4	R_2
S_3	S_3	S_2	S_4	S_1	R_4	R_2	R_1	R_3
S_4	S_4	S_1	S_3	S_2	R_2	R_4	R_3	R_1

Table 1.1: Cayley table for G

Example 1.31 *Let* $D_8 = \langle x, y |\ x^4 = 1, y^2 = 1, \quad xy = yx^{-1} \rangle$ *such that* $D_8 = \{y^i x^i |\ 0 \leq i \leq 3,\ 0 \leq j \leq 1\}$ *where* x *denotes rotation and* y *reflection. We prepared a Cayley table showing the direct product of* D_8

Example 1.32 [10] $D_6 = \langle x, y :\ x^2 = y^2 = (xy)^3 = 1, \rangle$.

The group elements can be listed as $D_6 = \{x^i,\ yx^i :\ 0 \leq i \leq 5\}$.

Example 1.33 [10] $D_{10} = \langle x, y :\ x^5 = y^2 = 1,\ xy = yx^{-1} \rangle$. *The group elements can be listed as* $x,\ x^2,\ x^3,\ x^4,\ y,\ xy,\ x^2y,\ x^3y,$ *and* x^4y

	1	x	x^2	x^3	y	yx	yx^2	yx^3
1	1	x	x^2	x^3	x	yx	yx^2	yx^3
x	x	x^2	x^3	1	yx	yx^2	yx^3	y
x^2	x^2	x^3	1	x	yx^2	yx^3	y	yx
x^3	x^3	1	x	x^2	yx^3	y	yx	yx^2
y	x	yx^3	yx^2	yx	1	x^3	x^2	x
yx	yx	y	yx^3	yx^2	x	1	x^3	x^2
x^2	yx^2	yx	y	yx^3	x^2	x	1	x^3
yx^3	yx^3	yx^2	yx	y	x^3	x^2	x	1

Table 1.2: Cayley table for D_8

Definition 1.34 [6] *Given any subset a of a group G, the centralizer of $\{a\}$ denoted as $C_G(a)$, is defined as the subgroup of G comprising all x such that $xg = gx$ for all $g \in a$. For any S, the centralizer $C_G(a)$ is a subgroup of the group G.*

Theorem 1.35 *Let $(G, \circ)$ be a group and let $a \in G$. Then $C_G(a)$, the centralizer of a in G, is a subgroup of G.*

Proof.[15] Let $(G, \circ)$ be a group.

We have that: $\forall a \in G$: $e \circ a = a \circ e \implies e \in C_G(a)$
Thus $C_G(a) \neq \varnothing$.

Let x, $y \in C_G(a)$. Then:

$x \circ a = a \circ x$
$y \circ a = a \circ y$
$\implies x \circ y \circ a = x \circ a \circ y$
$= a \circ x \circ y$
$\implies x \circ y \in C_G(a)$

Thus $C_G(a)$ is closed under $\circ$.

Let $x \in C_G(a)$. Then:

$x \circ a = a \circ x$
$\implies x^{-1} \circ x \circ a \circ x^{-1} = x^{-1} \circ a \circ x \circ x^{-1}$
$\implies a \circ x^{-1} = x^{-1} \circ a$

So: $x \in C_G(a) \implies x^{-1} \in C_G(a)$ ■

Definition 1.36 [4] *Given a group G, we define the exponent of G as $exp(G) = min\{n \geq 1 : g^n = 1, \forall g \in G\}$ We use the convention that $exp(G) = \infty$ if the set that we are minimizing over is empty.*

It is the least common multiple of the orders of all elements of the group. If there is no least common multiple, the exponent is taken to be infinity (or sometimes zero, depending on the convention).

1.6 Group Homomorphism

This is an important function in groups theory that maps groups together. It is a crucial subject to consider to fully comprehend the final two chapters. Here, we define and cite some examples of group homomorphism and go further to describe other terminologies in group theory like; the centraliser of a group, direct and indirect semiproducts etcetera.

Definition 1.37 *Let G together with the operation $\circ$, and H together with operation $*$, be groups. A function $\varphi : G \to H$ such that*

$\varphi(g \circ k) = \varphi(g) * \varphi(k)$,

for all g,k $\in G$ is a group homomorphism.

Speaking more coloquially, a group homomorphism is a function between groups that preserves the group operation.Note that because g and k are elements of G, we are combining them via the operation $\circ$ in G. But $\varphi(g)$ and $\varphi(k)$ are elements of H, and so we are combining them via the operation $* \in H$.

Example 1.38 *:*

(1) Consider the groups $\mathbb{R}$ under addition, and $\mathbb{R}^+$ of positive real numbers, under multiplication. Recall the function $log : \mathbb{R}^+ \to \mathbb{R}$, the natural logarithm function. (That is, $log(r)$ is the exponent needed on the irrational number e so that $e^{log(r)} = r$.)
Recall first of all that this function is only defined for positive real numbers. The most important and useful property of the logarithmic function is:

$log(ab) = log(a) + log(b)$.

That is, the logarithm turns multiplication into addition. And this equation is exactly what is required to assert that log is a homomorphism! This example shows us that the group operations in two groups connected by a homomorphism can be quite different.

(2) Consider another famous function, this time between the groups $\mathcal{U}(M_2(mathbbR))$, the group of units of the 2×2 real-valued matrices, and R^*, the multiplicative group of non-zero reals. Recall that $\mathcal{U}(M_2(\mathbb{R}))$ are precisely those matrices in $M_2(\mathbb{R})$ with non-zero determinant . Here, the operation in the first group is matrix multiplication, while in the second it is ordinary real number multiplication. The function is the determinant function det:

$$det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = ad - bc$$

Let's show that this is homomorphism. For that purpose, we need to choose two arbitrary matrices,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ and } \begin{bmatrix} r & s \\ t & u \end{bmatrix},$$

where the entries are all real numbers. The product of these two matrices is

$\begin{bmatrix} ar+bt & as+bu \\ cr+dt & cs+du \end{bmatrix}$, *and the determinant of this matrix is* $ardu + btcs - bucr - asdt$.

But the product of the determinants is $(ad-bc)(ru-ts)$,
which is the same. Thus, the determinant function preserves multiplication. To paraphrase, the determinant of a product is the product of the determinants.

(3) Consider the group

$D_3 = \{\iota, \rho, \rho^2, \varphi, \rho\varphi, \varphi\rho\}$ *of symmetries of the equilateral triangle, whose operation is functional composition. Consider also the multiplicative subgroup* $\{1, -1\}$ *of the integers. Define the function The pattern of* F *and* R *we observed there shows us that a rotation times a rotation is a rotation, flip times a flip is a rotation, and a rotation times a flip (in either order) is a flip. Now replace 'rotation' by* 1 *and 'flip' by* -1 *in the previous sentence. This is just the way multiplication in the group* $\{1, -1\}$ *works.*

Definition 1.39 [7] *A group* G *is called an extension of a group* K *by a group* H *if there exists an epimorphism* φ *from* G *onto* K *with kernel* H. *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.

Proposition 1.40 [7] *Let* H *and* K *be subgroups of a group* G. *Then* G *is a split extension of* K *by* $H \iff G \cong H \rtimes K'$, *where* $K' \cong K$.

Definition 1.41 [7] *Let* H, K *be subgroups of a group* G. *We say that* G *is the internal direct product of* H *and* K *and write* $G = H \rtimes K$, *if the following holds:*

(i) $G = HK$,

(ii) $H \cap K = \{1\}$,

(iii) $H \triangleleft G$ *and* $K \triangleleft G$.

Definition 1.42 [1] *Let* G *be a group,* N *a normal subgroup of* G *and* H *a subgroup of* G. *If* $\big[G = NH \ \text{ and } \ N \cap H = \{1\}\big]$, *we say that* G *is a semi-direct product of* N *and* H, *written* $G = N \rtimes H$.

Definition 1.43 [1] *A group* G *is the internal semidirect product of* N *by* A, *which we denote by* $G = N \rtimes A$, *when* G *contains subgroups* N *and* A *such that* $NA = G$, $N \cap A = \{1\}$, *and* $N \triangleleft G$.

Definition 1.44 [1] *Let* X *and* A *be groups, and let* θ *be a given action of* A *on* X; *that is, a homomorphism* $\theta : A \mapsto Aut(X)$, *where* $Aut(X)$ *denotes the group of automorphisms of* X. *Then , for* $c \in A$, $\theta(c) : X \mapsto X$, *and if* $b \in X$, *we denote its image under this automorphism by* $\theta(c)(b)$. *The external semidirect product* $X \rtimes_\theta A$ *of the group* X *and the group* A *relative to* θ *is, as a set, simply* $X \rtimes A$. *We make this into a group by defining* $(d, c)(b, a) = \big(d\theta(c)(b), ca\big)$. *When* θ *is clear, we write* $X \times A$.

Chapter 2

Ring Theory

This is another aspect that forms the foundation of our study. In this chapter we treat rings and subsets of rings called subrings. A special type of ring(division ring) is discussed; the zero divisors, integral domain and units of ring are considered as it relates to fields. We also consider a special behaviour of rings in 'ring homomorphism' as well. Some examples are given to make clear our points throughout the chapter.

2.1 Rings

Definition 2.1 [2] *A ring R is a set together with two binary operations $+$ and $\times$ (called addition and multiplication) satisfying the following axioms:*

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

(ii) Associative on multiplication: $(a \times b) \times c = a \times (b \times c)$ *for all a,b,c* $\in R$,

(iii) The distributive laws hold in R: *for all* $a, b, c \in R$
$(a + b) \times c = (a \times b) + (b \times c)$ *and* $a \times (b + c) = (a \times b) + (a \times c)$.

The ring is commutative if multiplication is commutative, and said to have an identity (or contain a 1) if there is an element $1 \in R$ *with* $1 \times a = a = a$ *for all* $a \in R$.

Example 2.2 [6]

(1) The simplest examples of rings are the trivial rings obtained by taking R to be any commutative group (denoting the group operation by $+$ and defining the multiplication $\times$ on R by: $a \times b = 0$ *for all a,b* $\in R$. *It is easy to see that this multiplication defines a commutative ring. In particular, if* $R = 0$ *is the trivial group, the resulting ring R is called the zero ring, denoted* $R = 0$. *Except for the zero ring, a trivial ring does not contain an identity (*$R = 0$ *is the only ring where* $1 = 0$*; we shall often exclude this ring by imposing the condition* $1 \neq 0$*). Although trivial rings have two binary operations, multiplication adds no new structure to the additive group and the theory of rings gives no information which could not already be obtained from (abelian) group theory.*

(2) The quotient group $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with identity (the element 1) under the operations of addition and multiplication of residue classes (frequently referred to as 'modular arithmetic'). We saw that the additive abelian group axioms followed from the general principals of the theory of quotient groups (indeed this was the prototypical quotient group). We shall shortly prove that the remaining ring axioms (in particular, the fact that multiplication of residue classes is well defined) follow analogously from the general theory of quotient rings. In all of the examples so far, the rings have been commutative. Historically, one of the first non-commutative rings was discovered in 1843 by Sir William Rowell Hamilton (1805-1865). This ring, which is a division ring , was extremely influential in the subsequent development of mathematics and it continues to play an important role in certain areas of mathematics and physics.

2.2 Subrings

Definition 2.3 [17] *A subring of a ring R is any subset $S \subseteq R$ which forms a ring with respect to the operations of R.*

To show that a subset of a ring is a subring it suffices to check that it is nonempty and closed under subtraction and under multiplication.

Theorem 2.4 [6] ***(The Subring Theorem)***
A non-empty subset of a ring is a subring under the same operations if and only if it is closed under multiplication and subtraction.

Proof. It is obvious that a subring is closed under multiplication and subtraction. For the converse, suppose that R is a ring and S a non-empty subset, which is closed under multiplication and subtraction. We wish to show that S is a ring. Now, because S is non-empty, we can then choose an element of it, which we call s. First note that because S is closed under subtraction, then $s-s = 0 \in S$. That is, the additive identity belongs to S. Next, suppose that $a \in S$. Because S is closed under subtraction, $-a = 0 - a \in S$. This means that S is closed under taking additive inverses. Now suppose that $a, b \in S$. Then we have just seen that $-b \in S$. But then $a + b = a - (-b) \in S$, and so S is closed under addition as well.
To show that S is a ring, it remains to show that additive is commutative, that addition and multiplication are associative, and that multiplication distributes over addition. But all these properties hold in R, and so are automatically inherited for S.
Commutativity is automatically inherited by a subset, it follows that a subring of a commutative ring is also commutative. Note that a subring of a non-commutative ring may be commutative, because the zero ring is a commutative subring of any ring. ■

We now consider examples of subrings:

Example 2.5 [3] *Let $m\mathbb{Z} = \{mn : n \in \mathbb{Z}\}$, where m is an integer greater than 1. That is, mZ is the set of integer multiples of m. We claim that $m\mathbb{Z}$ is a subring of $\mathbb{Z}$. For $ma, mb \in m\mathbb{Z}$, then*

• $ma - mb = m(a - b) \in \mathbb{Z}$

and so $m\mathbb{Z}$ is closed under subtraction. Similarly,

- $(ma)mb = m(mab) \in m\mathbb{Z}$,

and so $m\mathbb{Z}$ is closed under multiplication.

2.3 Division Ring

Now we know what rings and subrings are, we now discuss a type of ring called division ring. We must comprehend this section especially as it is a prelude to the next chapter 'Fields'.

Definition 2.6 [7] *A ring R is called a division ring if all its non-zero elements R are invertible (i.e., if $R\ \{0\} = \mathcal{U}$).*

$\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}$, and $M_n(\mathbb{R})$ are examples of division rings which we look consider in detail under examples of division rings.

Definition 2.7 [18] *A commutative ring with unity is a commutative ring with an element such that $a \times 1 = 1 \times a = a$ for all $a \in R$.*

Definition 2.8 [18] *A commutative ring is a ring such that for all $a, b \in R$, $a \times b = b \times a$.*

Definition 2.9 [2] *A division ring R is called a field if R is a commutative ring.*

See next Chapter for clarity.

There are some basic definitions we need to note to fully understand in detail the division ring defined above. We define:

Definition 2.10 [2] *In a ring R, if $a\dot{b} = 0$ but $a \neq 0$ and $b \neq 0$ then a and b are called zero divisors.*

See Section 2.5 for clear examples.

Definition 2.11 [2] *If a ring has no zero-divisors, then R is called an integral domain.*

See Section 2.6 for example.

Definition 2.12 [7] *Let R be a ring. An element $a \in R$ is invertible in R if there exists $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$. The set*

$$\mathcal{U}(R) = \{a \in R :\ a \text{ is invertible}\}$$

is called the group of units of R.

We now consider examples of division rings we stated earlier on. There exists commutative and non-commutative division rings. Common commutative rings are:

Definition 2.13 [18] *The ring of integers modulo n is $(Z_n, +, \cdot)$ (where $n \in \mathbb{Z}, n > 0$). In fact this is a commutative ring.*

Example 2.14 [18] *Consider $(\mathbb{Z}_5, +, \cdot)$:*

$\mathcal{Z}_5$ has elements $0, 1, 2, 3,$ and 4. This ring has an identity $1 \in \mathbb{Z}_5$ since $[1] \times [a] = [1 \times a] = [a]$. Also, $\mathcal{Z}_5$ is a commutative ring since $[a] \times [b] = [a \times b] = [b \times a] = [b] \times a$, where $a \times b = b \times a$. This ring does not have zero divisors since if $[a] \times [b] = [a \times b] = [0]$, then 5 divides $a \times b$. Since 5 is prime, it must either divide a or b, in the first case $[a] = [0]$ and in the second case $[b] = [0]$. Therefore, if a product of elements is $[0]$, then one of them must be $[0]$. Hence, $\mathbb{Z}_5$ is an integral domain.
Finally, this ring has inverses since $[1] \times [1] = [1]$, $[2] \times [3] = [6] = [1]$, $[3] \times [2] = [6] = [1]$, and $[4] \times [4] = [16] = [1]$. Therefore $\mathbb{Z}_5$ is a division ring and hence a field.

Example 2.15 [18] *Consider $(\mathbb{Z}_6, +, \cdot)$:*

This ring has an identity 1 since $[1] \times [a] = [1 \times a] = [a]$. Similarly as shown in $\mathbb{Z}_5$, $\mathbb{Z}_5$ is a commutative ring. However, this ring has zero divisors since $[2] \times [3] = [2 \times 3] = [6] = [0]$ hence $\mathbb{Z}_6$ is not an integral domain. There exist no inverses in this ring which we can see by inspection. $[1] \times [2] = [2]$, $[2] \times [2] = [4]$, $[3] \times [2] = [0]$, $[4] \times [2] = [2]$, and $[5] \times [2] = [4]$, none of which are equal to $[1]$. Therefore, $\mathbb{Z}_6$ is a commutative ring with unity.

There also exist non-commutative division rings and one common example of such is the $M(2, \mathbb{R}, +, \times)$ ring.

Example 2.16 [18] *$M(2, \mathbb{R}, +, \times)$: is the set of all 2×2 matrices*

This ring has an identity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ *because for any* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2, \mathbb{R})$,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

This ring has zero divisors since

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

but neither $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ *or* $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ *are zero matrices.*

It is not commutative since

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

Then, if we multiply the expression for zero divisors on the left by A, we would have

$$A \times \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = A \times \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

but $A \times \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ *and so the original expression is also*

$$A \times \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

This means $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ *cannot have an inverse. Therefore* $M(2, \mathbb{R})$ *is a division ring.*

2.4 The Multiplicative Identity

It is an important part of the definition of a ring that it has an additive identity or 0. We make no such assumption about a multiplicative identity; many rings do possess a multiplicative identity however.

Definition 2.17 [6] *We call an element u of a ring R a 'unity' or 'multiplicative identity' if* $ua = au = a$ *for all elements* $a \in R$.

Example 2.18 *Obviously, the integer* 1 *is the unity of* $\mathbb{Z}$. *Similarly,* 1 *is the unity for the rings* $\mathbb{Q}$, $\mathbb{R}$, *and* $\mathbb{C}$. *In* $\mathbb{Q}[x]$, *the constant polynomial* 1 *is the unity. In the ring* $M_2(\mathbb{Q})$, *the unity is* $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

The residue class [1] plays the role of multiplicative identity in $\mathbb{Z}_m$. On the other hand, the ring $2\mathbb{Z}$ has no unity, because in the integers $2a = 2$ holds exactly when $a = 1$, an element which $2\mathbb{Z}$ lacks. More generally, $m\mathbb{Z}$ lacks unity for all $m > 1$.

2.5 Zero Divisors

Definition 2.19 [6] *Let R be a commutative ring. An element* $a \neq 0$ *is a zero divisor if there exists an element* $b \in R$ *such that* $b \neq 0$ *and* $ab = 0$. *Of course, then b is a zero divisor also.*

Example 2.20 [6] *As shown clearly in Example 2.15, the elements* 2 *and* 3 *in* $\mathbb{Z}_6$ *are zero divisors because* $2.3 = 0$. *Another example is found in the ring of complex numbers* $(\mathbb{C}, +, \cdot)$ [18]. *This ring does not have zero divisors because for any complex number a and b,* $a \times b = 0$, *then* $a = 0$ *or* $b = 0$. *Hence* $\mathbb{C}$ *is an integral domain. This ring is also commutative since for complexes,* $a \times b = b \times a$ *hence a commutative ring with unity since* $1 = 1 + 0i \in \mathbb{C}$.

2.6 Integral Domain

Definition 2.21 [6] *A commutative ring with unity that has no zero divisors is called an integral domain, or simply a domain.*

Example 2.22 $(\mathbb{Z}_5, +, \cdot)$ *and* $(\mathbb{C}, +, \cdot)$ *are examples of an integral domain. See 2.14 for verification.*

Theorem 2.23 *(Multiplicative Cancellation)*
Suppose R is an integral domain and a,b,c are elements of R, with $a \neq 0$. *If ab=ac, then b=c*

Proof. Suppose that R is a domain, $a \neq 0$, and $ab = ac$. Then $ab - ac = 0$. But then $a(b-c) = 0$, and because R is a domain with $a \neq 0$, we must have $b - c = 0$, or $b = c$, as required.

2.7 Units

Definition 2.24 [6] *Suppose R is a ring with unity 1. Let a be any non-zero element of R. We say a is a 'unit' if there is an element b of R such that* $ab = ba = a$. *In this case, b is a (multiplicative) inverse of a. b is also a unit with inverse a.*

First note that the unity 1 is always a unit, because $1.1 = 1$. What other elements are units? In $\mathbb{Z}$, the units are just 1 and -1, because the only integer solutions of $ab = 1$ are ± 1. In $\mathbb{Q}$ and $\mathbb{R}$, all non-zero elements are units. In $\mathbb{Z}_6$ we have $5.5 = 1$, and so 5 is a unit, as well as 1. Furthermore, there are no elements a and b for which $ab = 1$ is true.
Note that the concept of multiplicative inverses makes good sense in non-commutative rings. For example, in the (non-commutative) ring of matrices $M_2\mathbb{R}$, the elements

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \text{ and } \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{3}{2} \end{pmatrix}$$

are units, because their product in either order is the multiplicative identity. We now claim that multiplicative inverses, if they exist, are unique. To show this, suppose that a has multiplicative inverses b and c; then $1 = ba = ca$. Multiply through the right hand equations by b; W e then have $b = bab = cab = c$ (where the last equation holds because $ab = 1$ also). But $b = c$, as required. Consequently, we will denote the (unique) inverse of an element a (if it exists) by a^{-1}. This is of course consistent with the ordinary notation for multiplicative inverses which we use in $\mathbb{R}$.
We denote the set of units of a ring $\mathbb{R}$ by $\mathcal{U}(R)$. Thus, $\mathcal{U}(\mathbb{Z}) = \{1, -1\}$, $\mathcal{U}(\mathbb{Q}) = \mathbb{Q}\ \{0\}$, and $\mathcal{U}(\mathbb{Z}_6) = \{1, 5\}$.

Example 2.25 $\mathcal{U}(\mathbb{Z}) = \{+1, -1\}$, *the cyclic group of order* 2 *(written* C_2*).*

Example 2.26 $\mathcal{U}(M_n(\mathbb{R})) = \{A \in M_n(\mathbb{R}) |\ detA \neq 0\} = GL_n(\mathbb{R})$

Example 2.27 $\mathcal{U}(Q) = Q\ \{0\}$.
$\left\{(\frac{a}{b})\right\}^{-1} = \frac{b}{a}$ *where* $a \neq 0$, $b \neq 0$

2.8 Ring Homomorphism

This is an important behaviour of rings that is vital in our study of ′group rings′. Here, we are given a handy knowledge of the subject ′Ring Homomorphism′. It is expected that the reader must have understood what the term ′homomorphism′ means in the first place.

Definition 2.28 [7] *Let R and S be rings. $f : R \longrightarrow S$ is a ring homomorphism if*

- $f(a+b) = f(a) + f(b) \quad \forall\, a, b \in R.$
- $f(ab) = f(a)f(b) \quad \forall\, a, b \in R.$

Definition 2.29 *A ring homomorphism that is one-to-one and onto is called a ring isomorphism* [?BnB].

Example 2.30 [2] *Consider $\phi : \mathbb{Z} \to M_2(\mathbb{Z})$ defined by ϕ defined by $\phi(a) = \begin{bmatrix} 0 & 0 \\ a & a \end{bmatrix}$ for all $a \in \mathbb{Z}$. Then for all $a, b \in \mathbb{Z}$*

- $\phi(a) + \phi(b) = \begin{bmatrix} 0 & 0 \\ a & a \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ b & b \end{bmatrix} = \begin{pmatrix} 0 & 0 \\ a+b & a+b \end{pmatrix} = \phi(a+b)$
- $\phi(a)\phi(b) = \begin{bmatrix} 0 & 0 \\ a & a \end{bmatrix} \begin{bmatrix} 0 & 0 \\ b & b \end{bmatrix} = \begin{pmatrix} 0 & 0 \\ ab & ab \end{pmatrix} = \phi(ab).$

It is easy to see that $\phi(R) = \left\{ \begin{bmatrix} 0 & 0 \\ a & a \end{bmatrix} | a \in \mathbb{Z} \right\}$. Also, $Ker(\phi) = \{0\}$.

Note that ϕ is one-to-one, but not onto.

Example 2.31 [2] *Consider $\phi : \mathbb{Z} \to \mathbb{Z}_6$ defined by $\phi(a) = a mod 6$ for all $a \in \mathbb{Z}$. Then for $a, b \in \mathbb{Z}$:*

- $\phi(a) + \phi(b) = (a \bmod 6) + (b \bmod 6) = (a+b) \bmod 6 = \phi(a+b)$
- $\phi(a)\phi(b) = (a \bmod 6)\,(b \bmod 6) = (ab) \bmod 6 = \phi(ab).$

It is easy to see that $\phi(R) = \mathbb{Z}_6$. also, $Ker(\theta) = 6\mathbb{Z}$.

Note that $\phi(0) = 0 = \phi(6)$, so ϕ is not one-to-one but is onto.

Theorem 2.32 [7] *Let $\theta : R \to S$ be a ring homomorphism. Units in R get mapped to units in S.*

Proof. Let $r_1, r_2 \in R$, where $r_1 r_2 = 1_R$. Clearly

$$\theta(r_1\, r_2) = \theta(1_R)$$
$$\theta(r_1)\, \theta(r_2) = 1_S$$

Therefore $\theta(r_1)$ and $\theta(r_2)$ are invertible in S. Thus units in R get mapped to units in S. ■

Definition 2.33 [7] *Let $f : R \to S$ be a ring homomorphism. Then, the image of f is the subring*

$$Im(f) = \{y \in S : (\exists x \in R) f(x) = y\}$$

The kernel of f is the ideal

$$Ker(f) = \{x \in R : f(x) = 0\}).$$

Now, we shall show that every two-sided ideal of a ring R is the kernel of a homomorphism defined on R. Let I be an ideal of a ring R. Then the additive factor group R/I can be made into a ring by defining multiplication in a natural way $\bar{r}\bar{s} = \bar{r}\bar{s}$.

Definition 2.34 [7] *A ring homomorphism $f : R \to S$ is called an epimorphism if it is surjective; i.e., if $Im(f) = S$ and it is called a monomorphism if it is injective; i.e., if $f(x) = f(y) \implies x = y$, for $x, y \in R$. It is easy to see that f is a monomorphism if and only if $Ker(f) = (0)$*
Finally, f is called an isomorphism if it is both surjective and injective. In this case, we say that R and S are isomorphic and write $R \simeq S$.

A homomorphism of a ring R to itself is called an endomorphism and, if it is also an isomorphism, then it is called automorphism of R.

Chapter 3

Field Theory

The definition of division ring was necessary for introducing what is called a 'field'. Here, we discuss fields, subfields using examples. We go further to explain the order and characteristics of a field and consider a finite field otherwise known as the Galois field-we then construct fields $\mathbb{F}_2$ and $\mathbb{F}_{2^2}$.

3.1 Field

Definition 3.1 *A field is a commutative ring in which all nonzero elements are invertible. It is a set of elements F for which addition, multiplication, subtraction and division operations performed with its elements result in another element of the same set.For addition and multiplication operations, the following conditions define a field:*

- F^+ *is a commutative group with respect to the addition operation. The identity element for the addition is called* $'0'$.
- F^* *is a commutative group for the multiplication operation. The identity element for multiplication is called* $'1'$.
- *Multiplication is distributive with respect to addition:* $a(b+c) = ab + ac$

Example 3.2 $(\mathbb{Q}, +, \times)$:

This is a ring of rational numbers. The ring has an identity since $1 \in \mathbb{Q}$ *and* $1 \times a = a == a \times 1$ *for any real number a and in particular it holds for rational numbers. Also, this ring has inverses, for a non zero element of this ring is of the form* p/q *where neither* p *nor* q *is* 0. *The inverse of* p/q *is* q/p, *we only must show that this is in* $\mathbb{Q}$. q/p *is in* $\mathbb{Q}$ *since* $p \neq 0$. *This ring does not have zero divisors since for real numbers, if* $a \times b = 0$, *then either* $a = 0$ *or* $b = 0$, *thus for rationals, this also holds. Finally, it is a commutative since for real numbers* $a \times b = b \times a$, *which holds for rationals in particular. Therefore Q is a field.*

Example 3.3 $(\mathbb{Z}_5, +, \cdot)$ *is also an example of a field. See Example 2.14 for* $(\mathbb{Z}_5, +, \cdot)$.

Definition 3.4 *The number of element of a field is called the order of that field.*

Definition 3.5 [16] *The characteristics of a field M denoted by char$(M) = k$ is the smallest positive integer such that*

$$k.1 = \underbrace{1+1+ \ ... \ +1}_{k \text{ times}} = 0.$$

If no such k exists then the field is said to have characteristic 0-which implies char(M)=0.

The following lemma gives useful properties of the characteristic.

Lemma 3.6 [16] *Let M be a field.*

1. If the characteristic of M is positive, char (K) is prime.

2. Finite fields have char $(M) > 0$. By the first part of this lemma we even have that a finite field has a prime characteristic.

Proof. 1. Assume on the contrary that there exists a nontrivial factorization $\text{char}(M) = n = p.q$. Then

$0 = n.1 = (p.q).1 = p.(q.1) = (p.1).(q.1) = (1+1+...+1).(1+1+...+1)$

We encountered earlier that fields have no zero divisors, that means that one of the terms in the product must be zero which contradicts the minimality of the characteristic.

2. In a finite field, not all of $1, 2 \cdot 1, 3 \cdot 1, ...$ can be distinct, for example, $r \cdot 1 = s \cdot 1$ for some $s > r$. Then $\implies (s-r) \cdot 1 = 0$ and so char $(K) \mid s - r > 0$. ■

Lemma 3.7 [16] *k must be a positive number ≥ 2.*

Proof. Since $1 \neq 0$ we have $k \geq 2$. Suppose $k = k_1 \cdot k_2$ where $k_1 > 1$, $k_2 > 1$.

Then, $1+1+...+1 = (1+1+...+1).(1+1...+1)$. But L.H.S equals 0 which implies that at least one of the R.H.S terms equals 0, which is a contradiction. Hence k must be a prime number. This is called the characteristics of the field. If F is a finite field of characteristic p, then the order of F is a prime power $q = p^r$ for some positive integer r, and we write $F = \mathbb{F}_{p^r}$ or $F = \mathbb{F}_p$. If F and F' are two fields of order q, then F and F' are isomorphic. Thus we can talk about the finite field $\mathbb{F}_q$. ■

3.2 Galois Fields

Definition 3.8 [16] *A finite field is a field with a finite number of elements; the number of elements is the order of the field. $GF(q)$ is used to represent a finite field. However, the notation $\mathbb{F}_q$ is preferred for the purpose of this study. Finite fields are often called Galois fields(in honour of evariste Galois).*

Definition 3.9 [19] *If F is a finite field of characteristic k, then the order of F is a prime power $q = p^r$ for some positive integer r, and we write $F = \mathbb{F}_{p^r}$ or $F = \mathbb{F}_q$.*

Definition 3.10 [19] *A subfield of a field* $\mathbb{F}$ *is a subset* $K \subset \mathbb{F}$ *containing* 0 *and* 1*, and closed under the arithmetic operations-addition, subtraction, multiplication and division (by non-zero elements).*

Proposition 3.11 [19] *Suppose* $\mathbb{F}$ *is a field. Then* $\mathbb{F}$ *contains a smallest subfield* P*.*

Proof. Any intersection of subfields is evidently a subfield. In particular, the intersection of all subfields of $\mathbb{F}$ is a subfield P contained in every other subfield. ■

Definition 3.12 [19] *We call the smallest subfield* P *of a field* F *the prime (or rational) subfield of* F*.*

If F and F' are two fields of order q, then we F and F' are isomorphic i.e $\phi : F \to F'$. Thus we can talk about the

Definition 3.13 [16] *If* F *is any field, then* $F[x]$ *denotes the ring of polynomials in the variable* x *with coefficients in* F*, i.e., expressions of the form* $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ *with the* $a_i \in F$*.*

Definition 3.14 [16] *The integer* d *is the degree of* f*. A polynomial* f *of degree* d *is monic if* $a_d = 1$*. A polynomial* $f(x)$ *of degree* d *is irreducible if there is no way to write* $f(x) = g(x)h(x)$ *with deg* $g <$ *deg* f *and deg* $h <$ *deg* f*. Any polynomial* $f \in F[x]$ *can be written uniquely as a product of a scalar* $a \in F$ *and monic irreducible polynomials* $f_1, \ldots, f_l \in F[x]$*.*

Definition 3.15 [16] *If* $f \in F[x]$ *is a polynomial, a root of* f *is an element* $\alpha \in F$ *with* $f = 0$*. Any polynomial* $f \in F[x]$ *of degree* d *has at most* d *roots in* F*.*

Definition 3.16 *A field* $\mathbb{F}$ *is algebraically closed if it contains all of the roots of the polynomials in* $\mathbb{F}[x]$*.*

Example 3.17 $\mathbb{C}$ *is algebraically closed.*

3.3 Characterizing Finite Fields.

Lemma 3.18 [16] *Let* F *be a finite field containing a subfield* K *with* q *elements. Then* F *has* q^m *elements, where* $m = [F : K]$*.*

Proof. F is a vector space over K, finite-dimensional since F is finite. Denote this dimension by m; then F has a basis over K consisting of m elements, say $b_1, \ldots, b_m$. Every element of F can be uniquely represented in the form $k_1 b_1 + \ldots k_m b_m$ (where $k_1, \ldots, k_m \in K$). Since each $k_i \in K$ can take q values, F must have exactly q^m elements. ■

Theorem 3.19 [16] *Let* F *be a finite field. Then* F *has* p^n *elements, where the prime* p *is the characteristic of* F *and* n *is the degree of* F *over it's prime subfield.*

Proof. Since F is finite, it must have characteristics p for some prime p. Thus the prime subfield K of F is isomorphic to $\mathbb{F}_p$, and so contains p elements. ■

Lemma 3.20 [16] *If F is a finite field with q elements, then every $a \in F$ satisfies $a^q = a$.*

Proof. Clearly $a^q = a$ is satisfied for $a = 0$. The non-zero elements form a group of order $q - 1$ under multiplication. Using the fact that $a^{|G|} = 1_G$ for any element a of a finite group G, we have that all $0 \neq a \in F$ satisfy $a^{q-1} = 1$, i.e $a^q = a$ ■

Lemma 3.21 [16] *If F is a finite field with q-elements and K is a subfield of F, then the polynomial $x^q - x$ in $K[x]$ factors in $F[x]$ as*

$$x^q - x = \prod_{a \in F} (x - a)$$

and F is a splitting field of $x^q - x$ over K.

Proof. Since the polynomial $x^q - x$ has degree q, it has at most q roots in F. By Lemma 3.20, all the elements of F are roots of the polynomial, and there are q of them. Thus the polynomial splits in F as claimed, and cannot split in any smaller field. ■

We go on to prove the 'main characterization theorem' for finite fields.

Theorem 3.22 ***(Existence and Uniqueness of finite fields)*** [`?fFFF`] *For every prime p and every positive positive integer n, there exists a finite field with p^n elements. Any finite field with $q = p^n$ elements is isomorphic to the splitting f of $x^q - x$ over $\mathbb{F}_p$.*

Proof. (Existence) For $q = p^n$, consider $x^q - x$ in $\mathbb{F}_p[x]$, and let F be its splitting field over V. Since its derivatives is $q\, x^{q-1} - 1 = -1$ in $\mathbb{F}_p[x]$, it can have no common root with $x^q - x$ and so, $x^q - x$ has distinct roots in F. Let $S = \{a \in F : a^q - a = 0\}$. Then S is a subfield of F since

- S contains 0;
- $a, b \in S$ (by Freshmen's Exponentiation) that $(a - b)^q = a^q - b^q = a - b$, so $a - b \in S$;
- for $a, b \in S$ and $b \neq 0$ we have $(a^q b^{-q})^q = a^q b^{-q} = ab^{-1}$, so $ab^{-1} \in S$.

On the other hand, $x^q - x$ must split in S since S contains all its roots, i.e it's splitting field F is a subfield of S. Thus $F = S$ and, since S has q elements, F is s finite field with $q = p^n$ elements. Then F has characteristic p by Theorem 3.19, and so contains $\mathbb{F}_p$ as a subfield. So by Lemma 3.21, F is a splitting field of $x^q - x$. The result now follows that the uniqueness (up to isomorphism) of splitting fields.

As a result of the uniqueness part of Theorem 3.22, we may speak of the finite field (or the Galois field) of q elements. We shall denote this field by $\mathbb{F}_q$, where q denotes a power of the prime characteristic p of $\mathbb{F}_q$. ■

Example 3.23 [16] *The field* $L = \{\alpha_i + b_j\theta | \, \alpha_i, \beta_j \in \mathbb{F}_3\}$ *of* 9 *elements, where* θ *is a root of the polynomial* $x^2 + x + 2 \in \mathbb{F}_3[x]$. *By Theorem [], L is the field of* 9 *elements, i.e* $\mathbb{F}_9$.

Example 3.24 [16] *The field* $L = \{\alpha_i + b_j\theta | \, \alpha_i, \beta_j \in \mathbb{F}_2\}$ *of* 4 *elements, where* θ *is a root of the polynomial* $x^2 + x + 1 \in \mathbb{F}_2[x]$. *By Theorem [], L is the field of* 4 *elements, i.e* $\mathbb{F}_4$.

Theorem 3.25 [16] *For every finite field* $\mathbb{F}_q$, *the multiplicative group* $\mathbb{F}_q^*$ *of nonzero elements of* $\mathbb{F}_q$ *is cyclic.*

Proof. We may assume $q \geq 3$. Set $h = q - 1$, the order of $\mathbb{F}_{q^*}$, and let $h = {p_1}^{r_1}{p_2}^{r_2}...{p_m}^{r^m}$ be its prime factor decomposition. For each i, $1 \leq i \leq m$, the polynomial $x^{h/p^i} - 1$ has at most h/p_i roots in $\mathbb{F}_q$. Since $h/p_i < h$, it follows that there are nonzero elements of $\mathbb{F}_q$ which are not roots of this polynomial. Let a_i be such an element, and $b_i = {a_i}^{h/{p_i}^{r_i}}$. Now, ${b_i}^{{p_i}^{r_i}} = 1$, so the order of b_i divides ${p_i}^{r_i}$ and so has the form ${p_i}^{s_i}$ for some $0 \leq s_i \leq r_i$. On the other hand,

$$ {b_i}^{{p_i}^{r_i - 1}} = {a_i}^{h/{p_i}^{r_i}} \neq 1, $$

so the order of b_i is precisely $p_i^{r_i}$.
Let $b = b_1 b_2 \, ... \, b_m$. We claim: b has order $h(equalssq - 1)$, i.e. is a generator for the group. Suppose, on the contrary, that the order of b is a proper divisor of h. It is therefore a divisor of at last one of the m integers h/p_i, $1 \leq i \leq m$; *wlog*, say of h/p_1. Then

$1 = b^{h/p_1} = {b_1}^{h/p_1}{b_2}^{h/p_1}...{b_m}^{h/p_1}$.

Now, if $2 \leq i \leq m$, then $p_i^{r_i}$ divides h/p_1, and so ${b_i}^{h/p_1} = 1$. This forces ${b_i}^{h/p_1} = 1$. Thus the order of b_1 must divide h/p_1, which is impossible since the order of b_1 is ${p_1}^{r_1}$. Thus $\mathbb{F}_q^*$ is a cyclic group with generator b. ■

3.4 Constructing finite field $\mathbb{F}_{2^2}$

To construct $\mathbb{F}_{2^2}$; we first need to construct $\mathbb{F}_2$ and then extend it to $\mathbb{F}_{2^2}$

Example 3.26 $\mathbb{F}_2$:

Since this $\mathbb{F}_2$ *is a field of characteristics* 2, *then we must have* $|F| = 2^m$ *where* m *in this case is* 1. *For* $m = 1$, *a field exists, namely* $\mathbb{F}_2 = \{0, 1\}$. *Note however* $2 = 0$ *in* $\mathbb{F}_2$. *We construct the smallest example possible using addition and multiplication in* $\mathbb{F}_2$.

+	0	1
0	0	1
1	1	0

Table 3.1: $\mathbb{F}_2$: Addition

•	0	1
0	0	0
1	0	0

Table 3.2: $\mathbb{F}_2$: Multiplication

Example 3.27 $\mathbb{F}_{2^2}$:

Let us now construct the finite field $\mathbb{F}_{2^2}$ *where* $[2^2 = 4]$ *using the prime degree-2 polynomial* $g(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$. *There are four remainder polynomials mod*(x^2+x+1), *namely* $\{0, 1, x, 1 + x\}$. *Addition is componentwise mod*2. *For multiplication, note that* $x*x = x+1$ *since* x^2 *mod* $(x^2 + x + 1) = x + 1$. *Also* $x * x * x = x * (x * 1) = 1$ *since* x^3 *mod* $(x^2 + x + 1) = 1$. *The three nonzero elements* $\{1, x, x+1\}$ *thus forms a cyclic group under mod* $- g(x)$ *multiplication.*

The complete mod $- g(x)$ *addition and multiplication cayley table for* $\mathbb{F}_{2^2}$ *which is constructed below clearly validates this:*

•	1	x	$1 + x$
1	0	$1 + x$	x
x	$1 + x$	0	1
$1 + x$	x	1	0

Table 3.3: Cayley table showing addition in $\mathbb{F}_{2^2}$

•	1	x	$1 + x$
1	1	x	$1 + x$
x	x	1	$1 + x$
$1 + x$	$1 + x$	1	x

Table 3.4: Cayley table showing multiplication in $\mathbb{F}_{2^2}$

Chapter 4

Group Ring

We learned about groups and rings in the first and second chapter respectively. A group ring is basically a ring and a group functioning as a set of linear combinations. But the question is 'how does this set behave?'. Is it likely to behave more like a group or conversely, like a ring? With the help of few examples in this chapter, we have been able to establish the behaviour of a 'group ring'. This chapter summarily introduces the definition of group rings, and it's structure. We study the structure of group rings such as $\mathbb{F}_2C_2$, $\mathbb{F}_2C_3$ and $\mathbb{F}_2C_4$, we establish the units and zero divisors in each case and use a little bit of software to validate our findings.

4.1 Definition

Definition 4.1 [7] *Given a group G and a ring R, define the Group Ring RG to be the set of all linear combinations*

$$\sum_{g\in G} a_g g$$

where $a_g \in R$ and where only finitely many of the a_g's are non-zero.

4.2 Order of a Group Ring

Theorem 4.2 [7] *Let R be the a ring of order m and G be a group of order n. Then RG is a finite group ring of order $|R|^{|G|} = m^n$.*

Proof. $RG = \left\{ \sum_{g\in G} a_g g |\ a_g \in R \right\}$. For each g, there are m choices for a_g.
So there are $m \cdot m \cdots m$-elements in RG.
Hence $m^n = |R|^{|G|}$ ■

Definition 4.3 *Let RG be the group ring of the group G over the ring R. An element of the form rg where $r \in \mathcal{U}(R)$ and $g \in G$, has an inverse $r^{-1}g^{-1}$. Elements of this form are called trivial units of RG.*

4.3 Structure of some Group Rings

Example 4.4 *Let $R = \mathbb{F}_2$ and $G = C_2$. Writing down the elements: $\mathbb{F}_2 = \{0, 1\}$ and $C_2 = \langle a | a^2 = 1 \rangle = \{1, a\}$. Clearly $|RG| = |R|^{|G|} = 2^2 = 4$.*

$$\begin{aligned}
\mathbb{F}_2C_2 &= \left\{ \sum_{g \in C_2} a_g g | a_g \in \mathbb{F}_2 \right\} \\
&= \{a_g.g_1 + a_g.g_2 | a_g \in \mathbb{F}_2\} \\
&= \{a_g.1 + a_g.a | a_g \in \mathbb{F}_2\} \\
&= \{0.1 + 0.a,\ 1.1 + 0.a,\ 0.1 + 1.a,\ 1.1 + 1.a\} \\
&= \{\mathbf{0},\ \mathbf{1},\ \mathbf{a},\ \mathbf{1 + a}\}.
\end{aligned}$$

We shall now construct a Cayley table (multiplication) for $\mathbb{F}_2C_2$:

$\bullet$	$\mathbf{1}$	$\mathbf{a}$	$\mathbf{1+a}$
$\mathbf{1}$	1	a	$1+a$
$\mathbf{a}$	a	1	$1+a$
$\mathbf{1+a}$	$1+a$	$1+a$	0

Table 4.1: Cayley table for $\mathbb{F}_2C_2$

Therefore $\mathcal{U}(\mathbb{F}_2C_2) = \{1, a\} \cong C_2$ and $ZD(\mathbb{F}_2C_2) = \{1 + a\}$.

Here the units are clearly the trivial units, since $\mathcal{U}(\mathbb{F}_2C_2) \cong C_2$. A program was written in GAP to validate the above calculation. See Appendix A.1 for further details. Another example of group rings whose units are trivial units is $\mathbb{F}_2C_3$. We consider this in the next example.

Example 4.5 *Let $R = \mathbb{F}_2$ and $G = C_3$. Like the previous example, we write down the elements: $\mathbb{F}_2 = \{0, 1\}$ and $C_3 = \langle a | a^3 = 1 \rangle = \{1, a, a^2\}$. Here $|RG| = |R|^{|G|} = 2^3 = 8$.*

$$\begin{aligned}
\mathbb{F}_2C_3 &= \left\{ \sum_{g \in C_3} a_g g |\ a_g \in \mathbb{F}_2 \right\} \\
&= \left\{\mathbf{0},\ \mathbf{1},\ \mathbf{a},\ \mathbf{1 + a},\ \mathbf{a^2},\ \mathbf{a + a^2},\ \mathbf{1 + a^2},\ \mathbf{1 + a + a^2}\right\}
\end{aligned}$$

We now construct a Cayley table (multiplication) for $\mathbb{F}_2C_3$:

$\bullet$	$\mathbf{1}$	$\mathbf{a}$	$\mathbf{a^2}$	$\mathbf{1+a}$	$\mathbf{a+a^2}$	$\mathbf{1+a^2}$	$\mathbf{1+a+a^2}$
$\mathbf{1}$	1	a	a^2	$1+a$	$a+a^2$	$1+a^2$	$1+a+a^2$
$\mathbf{a}$	a	a^2	1	$a+a^2$	$1+a^2$	$1+a$	$1+a+a^2$
$\mathbf{a^2}$	a^2	1	a	$1+a^2$	$1+a$	$a+a^2$	$1+a+a^2$
$\mathbf{1+a}$	$1+a$	$a+a^2$	$1+a^2$	$1+a^2$	$1+a$	$a+a^2$	0
$\mathbf{a+a^2}$	$a+a^2$	$1+a^2$	$1+a$	$1+a$	$a+a^2$	$1+a^2$	0
$\mathbf{1+a^2}$	$1+a^2$	$1+a$	$a+a^2$	$a+a^2$	$1+a^2$	$1+a$	0
$\mathbf{1+a+a^2}$	$1+a+a^2$	$1+a+a^2$	$1+a+a^2$	0	0	0	$1+a+a^2$

Table 4.2: Cayley table for $\mathbb{F}_2C_3$

Therefore $\mathcal{U}(\mathbb{F}_2C_3) = \{1, a, a^2\} \cong C_3$ *and* $ZD(\mathbb{F}_2C_2) = \{1+a, 1+a^2, a+a^2, 1+a+a^2\}$.

As seen here, the unit elements of $\mathbb{F}_2C_3$ are trivial units as well. We used GAP to verify these calculations, see Appendix A.1 for further details. The next example studies $\mathbb{F}_3C_2$ whose units are not the trivial units.

Example 4.6 *Let* $R = \mathbb{F}_3$ *and* $G = C_2$. $\mathbb{F}_3$ *is a group of order three. This time the elements are:* $\mathbb{F}_2 = \{0, 1, 2\}$ *and* $C_2 = \langle a | a^2 = 1\rangle = \{1, a, \}$. *Here* $|RG| = |R|^{|G|} = 3^2 = 9$.

$$\mathbb{F}_3C_2 = \left\{ \sum_{g \in C_2} a_g g |\ a_g \in \mathbb{F}_3 \right\}$$

$$= \{\mathbf{0},\ \mathbf{a},\ \mathbf{1},\ \mathbf{2a},\ \mathbf{1+a},\ \mathbf{1+2a},\ \mathbf{2},\ \mathbf{2+a},\ \mathbf{2+2a}\}$$

We now construct a Cayley table (multiplication) for $\mathbb{F}_3C_2$*:*

$\bullet$	$\mathbf{1}$	$\mathbf{2}$	$\mathbf{a}$	$\mathbf{1+a}$	$\mathbf{1+2a}$	$\mathbf{2a}$	$\mathbf{2+a}$	$\mathbf{2+2a}$
$\mathbf{1}$	1	2	a	$1+a$	$1+2a$	$2a$	$2+a$	$2+2a$
$\mathbf{2}$	2	1	$2a$	$2+2a$	$2+a$	a	$1+a$	$1+a$
$\mathbf{a}$	a	$2a$	1	$1+a$	$2+a$	2	$1+2a$	$2+2a$
$\mathbf{1+a}$	$1+a$	$2+2a$	$1+a$	$2+2a$	0	$2a+2$	0	$1+a$
$\mathbf{1+2a}$	$1+2a$	$2+a$	$2+a$	0	$2+a$	$1+2a$	$1+2a$	0
$\mathbf{2a}$	$2a$	a	2	$2a+2$	$1+2a$	1	$2+a$	$1+a$
$\mathbf{2+a}$	$2+a$	$1+2a$	$1+2a$	0	$1+2a$	$2+a$	$2+a$	0
$\mathbf{2+2a}$	$2+2a$	$1+a$	$2+2a$	$1+a$	0	$1+a$	0	$2+2a$

Table 4.3: Cayley table for $\mathbb{F}_3C_2$

Therefore $\mathcal{U}(\mathbb{F}_3C_2) = \{1, 2, a, 2a\} \cong C_2 \times C_2$ *and* $ZD(\mathbb{F}_3C_2) = \{1+a, 1+2a, 2+a, 2+2a\}$. *We used GAP to verify these calculations, see Appendix A.1 for further details.*

Example 4.7 *Let* $R = \mathbb{F}_2$ *and* $G = C_4$. *The elements are:* $\mathbb{F}_2 = \{0, 1, 2\}$ *and* $C_4 = \langle a | a^4 = 1\rangle = \{1, a, a^2, a^3\}$. *Here* $|RG| = |R|^{|G|} = 2^4 = 16$.

$$\mathbb{F}_2C_4 = \left\{ \sum_{g\in C_2} a_g g |\, a_g \in \mathbb{F}_2 \right\}$$
$$= \left\{ \mathbf{0},\ \mathbf{1},\ \mathbf{a},\ \mathbf{a^2},\ \mathbf{a^3},\ \mathbf{1+a},\ \mathbf{1+a^2},\ \mathbf{1+a^3},\ \mathbf{a+a^2},\ \mathbf{a+a^3},\ \mathbf{a^2+a^3},\ \mathbf{a^3+\hat{a}},\ \mathbf{a^2+\hat{a}},\ \mathbf{a+\hat{a}},\ \mathbf{1+\hat{a}},\ \mathbf{\hat{a}} \right\}$$

Clearly $\{1, a, a^2, a^3\} \in \mathcal{U}(\mathbb{F}_2C_4)$. *Now*

- $(1+\hat{a})^2 = (a+a^2+a^3)^2 = a^2+a^4+a^6 = 2a^2+1 = 1$. *Similarly* $(a^2+\hat{a})^2 = 1$.
- $(a+\hat{a})^2 = (1+a^2+a^3)^2 = 1+1+a^2 = a^2$, *therefore* $(a+\hat{a})$ *has order* 4. *Similarly* $(a^3+\hat{a})$ *has order* 4.

Also

- $(\hat{a})^2 = (1+a+a^2+a^3)^2 = 1+a^2+a^4+a^6 = 2a^2+2 = 0$.
- $\hat{a}(1+a) = \hat{a}+\hat{a}.a = \hat{a}+\hat{a} = 2\hat{a} = 0$. *Similarly* $\hat{a}(1+a^2) = \hat{a}(1+a^3) = \hat{a}(a+a^2) = \hat{a}(a+a^3) = \hat{a}(a^2+a^3) = \hat{a}(1+a)$.

A Cayley table can be constructed in this case if desired just like in previous examples.
Now $|\mathcal{U}(\mathbb{F}_2C_4)| = 8$ *since* $\mathcal{U}(\mathbb{F}_2C_4) = \{1,\ a,\ a^2,\ a^3,\ 1+\hat{a},\ a+\hat{a},\ a^2+\hat{a},\ a^3+\hat{a}\}$. *Now every element in* $\mathcal{U}(\mathbb{F}_2C_4)$ *has order* 4 *or* 2. *Therefore* $\mathcal{U}(\mathbb{F}_2C_4) \cong C_2 \times C_4$. *We used GAP to verify these calculations, see Appendix A.1 for further details.*

4.4 Decomposition of Group Ring RG

This is a very vital part of our discuss as it shows how a group ring can be split into a direct sum of finitely many parts. What form do these decomposed parts take? Are likely questions this chapter would help to answer. We consider the decomposition of group algebra like $\mathbb{F}_7D_6$ and $\mathbb{F}_{3k}D_6$.

Definition 4.8 [7] *Let* RG *be the group ring of the group* G *over the ring* R. *Let* $\alpha \in \sum_{g\in G} a_g g \in RG$, *then the support of* α *(denoted by* $supp(\alpha)$*) is:*

$$supp(\alpha) = \{g \in G \,|\, a_g \neq 0\}.$$

Example 4.9 *Let* $\alpha = 1+a+a^3 \in \mathbb{F}_2C_4$. *then* $supp(\alpha) = 3$.

Theorem 4.10 ***(Wedderburn-Artin Theorem)*** [7] R *is a semisimple ring if and only if* R *can be decomposed as a direct sum of finitely many matrix rings over division rings.*

$$i.e.\ R \cong M_{n_1}(D_1) \oplus M_{n_2}(D_2) \oplus \cdots M_{n_s}(D_s)$$

where D_i *is a division ring and* $M_{n_i}(D_i)$ *is the ring of* $n_i \times n_i$ *matrices over* D_i.

Theorem 4.11 [7] *Let R be a semisimple ring. Then the wedderburn-artin decomposition above is unique.*

Theorem 4.12 [7] *Let G be a group and R a ring. Then RG is semisimple if the following conditions hold:*

(i) R is semisimple

(ii) G is finite

(iii) $|G|$ is invertible in R.

Corollary 4.13 [7] *Let G be a group and K a field. Then KG is semisimple if and only if G is finite and the characteristics $K \dagger |G|$*

Proof. First note that any field K is semisimple ($K = M_1(K)$ and use a previous lemma).
($\Leftarrow$) Let $|G| < \infty$ and $charK \dagger |G|$. So $|G| \in K\ \{0\}$.
($\Rightarrow$) $|G|$ is invertible in K. Now apply Maschke's Theorem $\implies$ let KG be semisimple. G is finite by Maschke's and also $|G|$ is invertible in K so semisimple. $G :\in: K : \{0\}$. So $|G|$ is not a multiple of $charK \in K$. Therefore, $K \dagger |G|$. ■

Theorem 4.14 [7] *Let G be a finite group and K a finite field such that $char(K) \dagger |G|$. Then $KG \cong \oplus_{i=1}^{s} M_{ni}(D_i)$ where D_i is a division ring containing K in it's center and*

$$|G| = \sum_{i=1}^{s} ({n_i}^2 \cdot dim_k(D_i))$$

Corollary 4.15 [7] *Let G be a finite group and K an algebraically closed field, where $char(K) \dagger |G|$. Then*

$$VKG \cong \oplus_{i=1}^{s}(K) \text{ and } |G| = \sum_{i=1}^{s} {n_i}^2$$

Example 4.16 [7] $\mathbb{C}C_3 \cong \oplus_{i=1}^{s} M_{n_i}(D_i) = \oplus_{i=1}^{s} M_{n_i}(\mathbb{C})$ *by the corollary above*

Counting dimensions we see that $3 = \sum_{i=1}^{s} {n_i}^2 = \sum_{i=1}^{2}$. *Therefore,* $D_i = \mathbb{C}$, $n_i = 1\ \forall\, i$ *and* $s = 3$. *Therefore,* $\mathbb{C}C_3 \cong \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}$. *Therefore* $\mathcal{U}(\mathbb{C}C_3) \cong \mathcal{U}(\mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}) = \mathcal{U}(\mathbb{C}) \times \mathcal{U}(\mathbb{C}) \times \mathcal{U}(\mathbb{C})$.

Example 4.17 [7] $\mathbb{C}S_3$. S_3 *is finite and* $\mathbb{C} = 0 \dagger 6$ *so Maschke's Theorem does apply and*

$$\mathbb{C}S_3 \cong \oplus_{i=1}^{s} M_{n_i}(D_i) = \oplus_{i=1}^{s} M_{n_i}(\mathbb{C})$$

$6 = 1^2 + 1^2 + 1^2$ *or* $6 = \sum_{i=1}^{6} 1^2$. *So* $\mathbb{C} \cong \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C})$ *or* $\mathbb{C}S_3 \cong \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}$.
But $\oplus_{i=1}^{6}$ *is a commutative ring so* $\mathbb{C}S_3 \ncong \oplus_{i=1}^{6}\mathbb{C}$. *Therefore,* $\mathbb{C}S_3 \cong \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C})$ *and* $\mathcal{U}(\mathbb{C}S_3) \cong \mathcal{U}(\mathbb{C}) \times \mathcal{U}(\mathbb{C}) \times GL_2(\mathbb{C})$.

Theorem 4.18 [7] *Let* G *be a finite group and* K *a field such that char* $K \dagger |G|$.
Then

$$KG \cong \oplus_{i=1}^{s} M_{n_i}(D_i) \cong K \oplus \oplus_{i=1}^{s-1} M_{n_i}(D_i)$$

(i.e. the field itself appears at least once as a direct summand in the Wedderburn-Artin decomposition).

Lemma 4.19 [7] *Let* K *be a finite field. Then if char* $K \dagger |G| < \infty$, *then*

$$KG \cong \oplus_{i=1}^{s} M_{n_i}(K_i)$$

where the K_i *are fields (i.e. all the division rings appearing are fields).*

Proof. Clearly $KG \cong \oplus_{i=1}^{s} M_{n_i}(D_i)$ where the D_i are division rings. But D_i is a division ring that $dim_K D_i < \infty$ (since G is finite). Now Wedder-burn's theorems implies that D_i must be a field. ■

Lemma 4.20 [7] *Let* R *be a commutative ring and* I *an ideal of* RG. *Then* RG/I *is commutative if and only if* $\Delta(G, G') \subset I$

Proposition 4.21 [7] *Let* G *be a finite. Let* RG *be semisimple (i.e.* $RG \cong \oplus_{i=1}^{s} M_{n_i}(D_i)$*).*

Here $R(G/G'')$ is the direct sum of all the commutative summands of the decomposition of RG and $\delta(G, G'')$ is the direct sum of all the non-commutative summands of the decomposition of RG.

Proof. Clearly $RG \cong R(G/G'') \oplus \Delta(G, G')$. Now it is also clear that $R(G/G'') \cong \oplus$ sum of the commutative summands of RG. It suffices to show that $\Delta(G, G')$ contains no commutative summands.
Assume $\Delta(G, G') \cong A \oplus B$ where A is commutative (and $\neq \{0\}$). Thus $RG \cong R(G/G') \oplus A \oplus B$. Now $RG/B \cong R(G/G') \oplus A$ (check). (In general, $R \cong C \oplus D \implies R/C \cong D$). So RG/B is commutative, so by the previous lemma, $\delta(G, G'') \subset B$. Thus $\Delta(G, G'') \cong A \oplus B \subset B$ which is a contradiction. ■

Example 4.22 $\mathbb{F}_7 D_6$. *Note that Maschke applies so* $\mathbb{F}_7 D_6 \cong \oplus_{i=1}^{s} M_{n_i}(D_i) \cong \oplus_{i=1}^{s} M_{n_i}(K_i)$ *(where* K_i *are finite fields containing* $\mathbb{F}_7$*)* $\mathbb{F}_7 \oplus \oplus_{i=1}^{t} M_{n_i}(K_i)$

Note: $D_6 = \langle x, y : x^2 = y^2 = (xy)^3 = 1, \rangle$ *from Example 1.32: hence* $D_6 \cong S_3$, *where* S_3 *is the symmetric group of degree three.*

Therefore, $\mathbb{F}_7 D_6 \cong \mathbb{F}_3(D_6/D_6') \oplus \Delta(G, G') \cong \mathbb{F}_7 C_2 \oplus$ *non-commutative part,*
where,

$$\mathbb{F}_7 C_2 = \mathbb{F}_7 \oplus \mathbb{F}_7 \oplus M_2(\mathbb{F}_{7^2}).$$

The units group $\mathcal{U}(\mathbb{F}_7 C_2) \cong \mathcal{U}(\mathbb{F}_7) \times \mathcal{U}(\mathbb{F}_7) \times GL_2(\mathbb{F}_{7^2})$

We used GAP to verify the decomposition of $\mathbb{F}_7 D_6$. *See Appendix A.3.*

Theorem 4.23 $\mathcal{U}(\mathbb{F}_{3k} C_2) \cong C_{3^k-1} \times C_{3^k-1}$

Proof. Consider $\mathbb{F}_{3k} C_2$, clearly $3 \nmid 2$ as Maschke Theorem/ Wedderburn Decomposition applies.

Now by Theorem 4.18,

$$\mathbb{F}_{3k} C_2 \cong \mathbb{F}_{3k} \oplus ?$$

$\mathbb{F}_{3k} C_2$ is abelian and implies $\mathbb{F}_{3k} C_2 \cong \mathbb{F}_{3k} \oplus \mathbb{F}_{3k}$.

The unit group $\mathcal{U}\mathbb{F}_{3k} C_2 \cong \mathcal{U}\mathbb{F}_{3k} \oplus \mathcal{U}\mathbb{F}_{3k}$.
Hence $\mathcal{U}\mathbb{F}_{3k} C_2 \cong C_{3^k-1} \times C_{3^k-1}$ by Theorem 3.25 ■

Chapter 5

The Unit Group of the Group Algebra $\mathbb{F}_{3^k}D_6$

The group algebra $\mathbb{F}_{3^k}D_6$ forms the focus of this thesis. In the previous chapter we talked about groups and rings functioning cohesively as a group ring. In this case however, it is more about a group and a field hence the term $'$group algebra$'$. The reference used in this chapter is Gildea and Creedon's research paper [5]. We seek to explain in detail the calculations done in that paper as it seemed quite implicitly conclusive and I predict a huge reliance on software was employed in the course of that paper to validate results. What is contained in this chapter is an alternative approach to verify calculations in the referenced paper.
We start by explaining a ring homomorphism θ which is a mapping from $\mathbb{F}_{3^k}D_6$ to $\mathbb{F}_{3^k}C_2$ and justify it using proofs. We then restrict θ to the unit group of $\mathbb{F}_{3^k}D_6$, a group epimorphism $\theta^{'}$is constructed by mapping unit group $\mathcal{U}(\mathbb{F}_{3^k}D_6)$ and $\mathcal{U}(\mathbb{F}_{3^k}C_2)$. A kernel of $\theta^{'}$ (i.e $ker(\theta^{'})$) with an exponent 3 is established, it attains congruence with $\mathcal{U}(\mathbb{F}_{3^k}D_6)$ by forming a semiproduct with $\mathcal{U}(\mathbb{F}_{3^k}C_2)$. We go further to prove the centraliser of h (where $H = ker(\theta^{'}),\ h \in H$) exists, is commutative and hence abelian. The consequence of this implies any subset $T \in H$ forms a subgroup in H and becomes congruent to $'{C_3}^{k}{}'$, hence H can be written as the multiplication T and $C_H(x)$ (where $x \in H$). This opens up on how a group algebra-in this case $\mathbb{F}_{3^k}D_6$ can be written as a multiplication of abelian and non-abelian parts.

Theorem 5.1 *Define the mapping* $\theta : \mathbb{F}_{3^k}D_6 \longrightarrow \mathbb{F}_{3^k}C_2$ *given by*

$$\sum_{i=0}^{2} a_i x^i + \sum_{j=0}^{2} b_j x^j y \mapsto \sum_{i=0}^{2} a_i + \sum_{j=0}^{2} b_j \bar{x}.$$

Then θ *is a ring homomorphism.*

Proof. Let $\alpha = \sum_{i=0}^{2} a_i x^i + \sum_{j=0}^{2} b_j x^j y \in \mathbb{F}_{3^k} D_6$ and $\beta = \sum_{i=0}^{2} c_i x^i + \sum_{j=0}^{2} d_j x^j y \in \mathbb{F}_{3^k} D_6$ where $a_i, b_j, c_k, d_m \in \mathbb{F}_{3^k}$. Then

$$\begin{aligned}
\theta(\alpha+\beta) &= \theta\left(\sum_{i=0}^{2} a_i x^i + \sum_{j=0}^{2} b_j x^j y + \sum_{i=0}^{2} c_i x^i + \sum_{j=0}^{2} d_j x^j y\right) \\
&= \theta\left(\sum_{i=0}^{2} (a_i + c_i) x^i + \sum_{j=0}^{2} (b_j + d_j) x^j y\right) \\
&= \sum_{i=0}^{2} (a_i + c_i) + \sum_{j=0}^{2} (b_j + d_j)\bar{x} \\
&= \left(\sum_{i=0}^{2} a_i + \sum_{j=0}^{2} b_j \bar{x}\right) + \left(\sum_{i=0}^{2} c_i + \sum_{j=0}^{2} d_j \bar{x}\right) \\
&= \theta(\alpha) + \theta(\beta).
\end{aligned}$$

Now

$$\begin{aligned}
\alpha\beta = {} & a_0c_0 + a_0c_1x + a_0c_2x^2 + a_0d_0y + a_0d_1xy + a_0d_2x^2y \\
& + a_1c_2 + a_1c_0x + a_1c_1x^2 + a_1d_2y + a_1d_0xy + a_1d_1x^2y \\
& + a_2c_1 + a_2c_2x + a_2c_0x^2 + a_2d_1y + a_2d_2xy + a_2d_0x^2y \\
& + b_0d_0 + b_0d_2x + b_0d_1x^2 + b_0c_0y + b_0c_2xy + b_0c_1x^2y \\
& + b_1d_1 + b_1d_0x + b_1d_2x^2 + b_1c_1y + b_1c_0xy + b_1c_2x^2y \\
& + b_2d_2 + b_2d_1x + b_2d_0x^2 + b_2c_2y + b_2c_1xy + b_2c_0x^2y
\end{aligned}$$

and

$$\begin{aligned}
\theta(\alpha\beta) = {} & \left(c_0 \sum_{i=0}^{2} a_i + c_1 \sum_{i=0}^{2} a_i + c_2 \sum_{i=0}^{2} a_i + d_0 \sum_{j=0}^{2} b_j + d_1 \sum_{j=0}^{2} b_j + d_2 \sum_{j=0}^{2} b_j\right).1 \\
& + \left(d_0 \sum_{i=0}^{2} a_i + d_1 \sum_{i=0}^{2} a_i + d_2 \sum_{i=0}^{2} a_i + c_0 \sum_{j=0}^{2} b_j + c_1 \sum_{j=0}^{2} b_j + c_2 \sum_{j=0}^{2} b_j\right)\bar{x} \\
= {} & \left[\left(\sum_{i=0}^{2} a_i\right)\left(\sum_{i=0}^{2} c_i\right) + \left(\sum_{j=0}^{2} b_j\right)\left(\sum_{j=0}^{2} d_j\right)\right].1 + \left[\left(\sum_{i=0}^{2} a_i\right)\left(\sum_{j=0}^{2} d_j\right) + \left(\sum_{j=0}^{2} b_j\right)\left(\sum_{i=0}^{2} c_i\right)\right]\bar{x} \\
= {} & \theta(\alpha)\theta(\beta).
\end{aligned}$$

Finally, $\theta\left(1_{\mathbb{F}_{3^k} D_6}\right) = (1+0+0).1 + (0+0+0)\bar{x} = 1 = 1_{\mathbb{F}_{3^k} C_2}$. ■

Now if we restrict θ to $\mathcal{U}(\mathbb{F}_{3^k} D_6)$, by Theorem 2.32, we can construct a group epimorphism $\theta' : \mathcal{U}(\mathbb{F}_{3^k} D_6) \to \mathcal{U}(\mathbb{F}_{3^k} C_2)$.

Proposition 5.2 *Let $\psi : \mathcal{U}(\mathbb{F}_{3^k}C_2) \to \mathcal{U}(\mathbb{F}_{3^k}D_6)$ be the mapping given by $a + b\bar{x} \mapsto a + by$. ψ is a group homomorphism.*

Proof. Let $\alpha = a + b\bar{x} \in \mathcal{U}(\mathbb{F}_{3^k}C_2)$ and $\beta = c + d\bar{x} \in \mathcal{U}(\mathbb{F}_{3^k}C_2)$ where $a, b, c, c \in \mathbb{F}_{3^k}$, then

$$\psi(\alpha\beta) = \theta\left((a + b\bar{x})(c + d\bar{x})\right) = \psi((ac + bd) + (bc + ad)\bar{x}) = (ac + bd) + (bc + ad)y = \psi(\alpha)\psi(\beta).$$

Now let $\alpha = \bar{x} \in \mathcal{U}(\mathbb{F}_{3^k}C_2)$,

$$\begin{aligned}\theta' \circ \psi(\alpha) &= \theta'(a + by)\\ &= (a + 0 + 0).1 + (b + 0 + 0)\bar{x}\\ &= a + b\bar{x}\\ &= \alpha.\end{aligned}$$

By Proposition 1.40, $\mathcal{U}(\mathbb{F}_{3^k}D_6) \cong H \rtimes \mathcal{U}(\mathbb{F}_{3^k}C_2)$ where $H = ker(\theta)$. ■

Theorem 5.3 *$H = ker(\theta')$ has exponent 3.*

Proof. Let $\alpha = \sum_{i=0}^{2} a_i x^i + \sum_{j=0}^{2} b_j x^j y \in \mathcal{U}(\mathbb{F}_{3^k}D_6)$ where $a_i, b_j \in \mathbb{F}_{3^k}$. Then $\alpha \in H$ iff $\sum_{i=0}^{2} a_i = 1$ and $\sum_{j=0}^{2} b_j = 0$. Thus every element of H takes the form

$$1 + \sum_{i=1}^{2}(a_i x^i - a_i) + \sum_{j=1}^{2}(b_j x^j y - b_j y)$$

where $a_i, b_j \in \mathbb{F}_{3^k}$. Now

$$\begin{aligned}1 + \sum_{i=1}^{2}(a_i x^i - a_i) + \sum_{j=1}^{2}(b_j x^j y - b_j y) &= 1 + a_1 x - a_1 + a_2 x^2 - a_2 + b_1 xy - b_1 y + b_2 x^2 y - b_2 y\\ &= 1 + a_1(x - 1) + a_2(x^2 - 1) + b_1(x - 1)y + b_2(x^2 - 1)y\\ &= 1 + (x - 1)(a_1 + b_1 y) + (x^2 - 1)(a_2 + b_2 y)\\ &= 1 + \mathbb{B}_1 + \mathbb{B}_2\end{aligned}$$

where $\mathbb{B}_1 = (x - 1)(a_1 + b_1 y)$ and $\mathbb{B}_2 = (x^2 - 1)(a_2 + b_2 y)$.

Now Let $\kappa = 1 + \mathbb{B}_1 + \mathbb{B}_2 \in H$ where $\mathbb{B}_1 = (x - 1)(a_1 + b_1 y)$ and $\mathbb{B}_2 = (x^2 - 1)(a_2 + b_2 y)$, then

$$\begin{aligned}\kappa^2 &= (1 + \mathbb{B}_1 + \mathbb{B}_2)^2\\ &= 1 + 2\mathbb{B}_1 + 2\mathbb{B}_2 + (\mathbb{B}_1^2 + \mathbb{B}_1\mathbb{B}_2 + \mathbb{B}_2\mathbb{B}_1 + \mathbb{B}_2^2).\end{aligned}$$

Now

- $$\begin{aligned}\mathbb{B}_1^2 &= [(x-1)(a_1+b_1y)]^2\\ &= a_1^2x^2 + a_1b_1x^2y - a_1^2x - a_1b_1xy + a_1b_1y + b_1^2 - a_1b_1xy - b_1^2x\\ &- a_1^2 - a_1b_1xy + a_1^2 + a_1b_1y - a_1b_1x^2y - b_1^2x^2 + a_1b_1y + b_1^2\\ &= (a_1^2+2b_1^2)\hat{x} + 3a_1b_1(1-x)y\\ &= (a_1^2+2b_1^2)\hat{x}.\end{aligned}$$

- $$\begin{aligned}\mathbb{B}_1\mathbb{B}_2 &= (x-1)(a_1+b_1y)(x^2-1)(a_2+b_2y)\\ &= a_1a_2 + a_1b_2y - a_1a_2x - a_1b_2xy + a_2b_1x^2y + b_1b_2x^2 - a_2b_1xy - b_1b_2x\\ &- a_1a_2x^2 - a_2b_1x^2y + a_1a_2 + a_1b_2y - a_2b_1xy - b_1b_2x + a_2b_1y + b_1b_2\\ &= (2a_1a_2+b_1b_2)\hat{x} + (2a_1b_2+a_2b_1)\hat{x}y.\end{aligned}$$

- $$\begin{aligned}\mathbb{B}_2\mathbb{B}_1 &= (x^2-1)(a_2+b_2y)(x-1)(a_1+b_1y)\\ &= a_1a_2 + a_2b_1y - a_1a_2x^2 - a_2b_1x^2y + a_1b_2xy + b_1b_2x - a_1b_2x^2y - b_1b_2x^2\\ &- a_1a_2x - a_2b_1xy + a_1a_2 + a_2b_1y - a_1b_2x^2y - b_1b_2x^2 + a_1b_2y + b_1b_2\\ &= (2a_1a_2+b_1b_2)\hat{x} + (a_1b_2+2a_2b_1)\hat{x}y.\end{aligned}$$

- $$\begin{aligned}\mathbb{B}_2^2 &= [(x^2-1)(a_2+b_2y)]^2\\ &= a_2^2x + a_2b_2xy - a_2^2x^2 - a_2b_2x^2y + a_2b_2y + b_2^2 - a_2b_2x^2y - b_2^2x^2\\ &- a_2^x2 - a_2b_2x^2y + a_2^2 + a_2b_2y - a_2b_2xy - b_2^2x + a_2b_2y + b_2^2\\ &= (a_2^2+2b_2^2)\hat{x} + 3a_2b_2(1-x^2)y\\ &= (a_2^2+2b_2^2)\hat{x}.\end{aligned}$$

Recall that $\mathbb{B}_1^2 = (a_1^2+2b_1^2)\hat{x}$, $\mathbb{B}_1\mathbb{B}_2 = (2a_1a_2+b_1b_2)\hat{x} + (2a_1b_2+a_2b_1)\hat{x}y$, $\mathbb{B}_2\mathbb{B}_1 = (2a_1a_2+b_1b_2)\hat{x} + (a_1b_2+2a_2b_1)\hat{x}y$ and $\mathbb{B}_2^2 = (a_2^2+2b_2^2)\hat{x}$. Therefore

$$\begin{aligned}\mathbb{B}_1^2 + \mathbb{B}_1\mathbb{B}_2 + \mathbb{B}_2\mathbb{B}_1 + \mathbb{B}_2^2 &= (a_1^2+2b_1^2+4a_1a_2+2b_1b_2+a_2^2+2b_2^2)\hat{x} + (3a_1b_2+3a_2b_1)\hat{x}y\\ &= (a_1^2+a_1a_2+a_2^2+2(b_1^2+b_1b_2+b_2^2))\hat{x}\\ &= ((a_1-a_2)^2+2(b_1-b_2)^2)\hat{x}\\ &= \gamma\hat{x}\end{aligned}$$

where $\gamma = (a_1-a_2)^2 + 2(b_1-b_2)^2$. Finally,

$$\begin{aligned}
\kappa^3 &= (1+\mathbb{B}_1+\mathbb{B}_2)^2(1+\mathbb{B}_1+\mathbb{B}_2)\\
&= (1+2\mathbb{B}_1+2\mathbb{B}_2+\gamma\hat{x})(1+\mathbb{B}_1+\mathbb{B}_2)\\
&= 1+3\mathbb{B}_1+3\mathbb{B}_2+2(\mathbb{B}_1^2+\mathbb{B}_1\mathbb{B}_2+\mathbb{B}_2\mathbb{B}_1+\mathbb{B}_2^2)+\gamma\hat{x}+\gamma\hat{x}\mathbb{B}_1+\gamma\hat{x}\mathbb{B}_2\\
&= 1+2\gamma\hat{x}+\gamma\hat{x}+\gamma\hat{x}(x-1)(a_1+b_1y)+\gamma\hat{x}(x^2-1)(a_2+b_2y)\\
&= 1+3\gamma\hat{x}+\gamma(\hat{x}-\hat{x})(a_1+b_1y)+\gamma(\hat{x}-\hat{x})(a_2+b_2y)\\
&= 1.
\end{aligned}$$

■

Theorem 5.4 *Let $C_H(x)=\{h\in H\mid hx=xh\}$, then $C_H(x)\cong C_3^{3k}$.*

Proof. Let $\alpha=\sum_{i=0}^{2}a_ix^i+\sum_{j=0}^{2}b_jx^jy\in H$ where $\sum_{i=0}^{2}a_i=1$, $\sum_{i=0}^{2}b_j=0$ and $a_i,b_j\in\mathbb{F}_{3^k}$. Then

$$\begin{aligned}
\alpha x-x\alpha &= \left(\sum_{i=0}^{2}a_ix^i+\sum_{j=0}^{2}b_jx^jy\right)x-x\left(\sum_{i=0}^{2}a_ix^i+\sum_{j=0}^{2}b_jx^jy\right)\\
&= \sum_{i=0}^{2}a_ix^{i+1}+\sum_{j=0}^{2}b_jx^jyx-\sum_{i=0}^{2}a_ix^{i+1}-\sum_{j=0}^{2}b_jx^{j+1}y\\
&= \sum_{j=0}^{2}b_jx^{j-1}y-\sum_{j=0}^{2}b_jx^{j+1}y\\
&= (b_1-b_2)y+(b_2-b_0)xy+(b_0-b_1)x^2y
\end{aligned}$$

Now $\alpha x-x\alpha=0$ iff $b_0=b_1=b_2$. Therefore every element of $C_H(x)$ takes the form

$$\sum_{i=0}^{2}a_ix^i+b\hat{x}y$$

where $\sum_{i=0}^{2}a_i=1$ and $a_i,b\in\mathbb{F}_{3^k}$. Let $\alpha=\sum_{i=0}^{2}a_ix^i+b\hat{x}y\in C_H(x)$ and $\beta=\sum_{i=0}^{2}c_ix^i+d\hat{x}y\in C_H(x)$ where $\sum_{i=0}^{2}a_i=1$, $\sum_{i=0}^{2}c_i=1$ and $a_i,c_j,b,d\in\mathbb{F}_{3^k}$. Then

$$\begin{aligned}\alpha\beta &= \left(\sum_{i=0}^{2} a_i x^i + b\hat{x}y\right)\left(\sum_{i=0}^{2} c_i x^i + d\hat{x}y\right)\\ &= \left(\sum_{i=0}^{2} a_i x^i\right)\left(\sum_{i=0}^{2} c_i x^i\right) + \left(\sum_{i=0}^{2} a_i x^i\right)(d\hat{x}y) + (b\hat{x}y)\left(\sum_{i=0}^{2} c_i x^i\right) + bd\,(\hat{x}y)^2\\ &= \left(\sum_{i=0}^{2} a_i x^i\right)\left(\sum_{i=0}^{2} c_i x^i\right) + d\left(\sum_{i=0}^{2} a_i \hat{x}y\right) + b\left(\sum_{i=0}^{2} c_i \hat{x}y\right)\end{aligned}$$

and

$$\begin{aligned}\beta\alpha &= \left(\sum_{i=0}^{2} c_i x^i + d\hat{x}y\right)\left(\sum_{i=0}^{2} a_i x^i + b\hat{x}y\right)\\ &= \left(\sum_{i=0}^{2} c_i x^i\right)\left(\sum_{i=0}^{2} a_i x^i\right) + \left(\sum_{i=0}^{2} c_i x^i\right)(b\hat{x}y) + (d\hat{x}y)\left(\sum_{i=0}^{2} a_i x^i\right) + bd\,(\hat{x}y)^2\\ &= \left(\sum_{i=0}^{2} c_i x^i\right)\left(\sum_{i=0}^{2} a_i x^i\right) + b\left(\sum_{i=0}^{2} c_i \hat{x}y\right) + d\left(\sum_{i=0}^{2} a_i \hat{x}y\right).\end{aligned}$$

Therefore $\alpha\beta = \beta\alpha$ and $C_H(x)$ is abelian. Clearly $|C_H(x)| = (3^k)^3 = 3^{3k}$, therefore $C_H(x) \cong C_3^{3k}$. ■

Theorem 5.5 *Let T be the subset of H consisting of elements of the form*

$$1 + r\sum_{i=0}^{2} ix^i(1+y)$$

where $r \in \mathbb{F}_{3^k}$, then $T \cong C_3^k$.

Proof. Let $\alpha = 1 + r\sum_{i=0}^{2} ix^i(1+y) \in T$ and $\beta = 1 + s\sum_{i=0}^{2} ix^i(1+y) \in T$ where $r, s \in \mathbb{F}_{3^k}$. Then

$$\begin{aligned}\alpha\beta &= \left(1 + r\sum_{i=0}^{2} ix^i(1+y)\right)\left(1 + s\sum_{i=0}^{2} ix^i(1+y)\right)\\ &= 1 + s\sum_{i=0}^{2} ix^i(1+y) + r\sum_{i=0}^{2} ix^i(1+y) + rs\left(\sum_{i=0}^{2} ix^i(1+y)\right)^2.\end{aligned}$$

Now

$$\begin{aligned}\left(\sum_{i=0}^{2} ix^i(1+y)\right)^2 &= \big((x+2x^2)(1+y)\big)^2 \\ &= (x+2x^2)(1+y)(x+2x^2)(1+y) \\ &= (x+2x^2)(x+2x^2)(1-y)(1+y) \\ &= (x+2x^2)^2(1-y^2) \\ &= 0.\end{aligned}$$

Therefore $\alpha\beta = 1 + (s+r)\sum_{i=0}^{2} ix^i(1+y) \in T$ and T is closed under multiplication. Additionally,

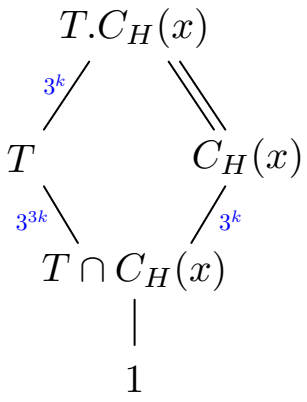
$$\begin{aligned}\beta\alpha &= \left(1 + s\sum_{i=0}^{2} ix^i(1+y)\right)\left(1 + r\sum_{i=0}^{2} ix^i(1+y)\right) \\ &= 1 + r\sum_{i=0}^{2} ix^i(1+y) + s\sum_{i=0}^{2} ix^i(1+y) + rs\left(\sum_{i=0}^{2} ix^i(1+y)\right)^2 \\ &= 1 + (r+s)\sum_{i=0}^{2} ix^i(1+y) \\ &= \alpha\beta.\end{aligned}$$

Now $|T| = 3^k$ and T is a subgroup of H by Corrollary 1.11. Therefore $T \cong C_3^k$. ■

We need to prove that the product of $C_H x$ and T equals H

Theorem 5.6 $H = T.C_H(x)$.

Proof. Let $c = 1 + a_1(x-1) + a_2(x^2-1) + b\hat{x}y \in C_H(x)$ and $t = 1 + r\sum_{i=0}^{2} ix^i(1+y) \in T$ where $a_i, b, r \in \mathbb{F}_{3^k}$. Consider $C_H(x) \cap T$. Clearly $b = 0 \Longrightarrow r = 0 \Longrightarrow C_H(x) \cap T = \{1\}$. By Theorem 1.22, $T.C_H(x)/C_H(x) \cong T/T \cap C_H(x) \Longrightarrow |T.C_H(x)/C_H(x)| = 3^k$. Therefore $|T.C_H(x)| = 3^{3k}.3^k = 3^{4k} = |H|$ and $H = C_H(x).T$.



■

Theorem 5.7 $C_H(x) \lhd H$.

Proof. Let $h \in H$, $c = 1 + a_1(x-1) + a_2(x^2-1) + b\hat{x}y \in C_H(x)$ and $t = 1 + r\sum_{i=0}^{2} ix^i(1+y) \in T$ where $a_i, b, r \in \mathbb{F}_{3^k}$. We need to show $c^h \in C_H(x)$, however it remains to show $c^t \in C_H(x)$ since $H = T.C_H(x)$.

$$\begin{aligned}
c^t &= t^{-1}ct \\
&= t^2ct \\
&= \left(1 + r\sum_{i=0}^{2} ix^i(1+y)\right)^2 \left(1 + a_1(x-1) + a_2(x^2-1) + b\hat{x}y\right) \left(1 + r\sum_{i=0}^{2} ix^i(1+y)\right) \\
&= \left(1 + 2r\sum_{i=0}^{2} ix^i(1+y)\right) \left(1 + a_1(x-1) + a_2(x^2-1) + b\hat{x}y\right) \left(1 + r\sum_{i=0}^{2} ix^i(1+y)\right) \\
&= \left(1 + 2r\sum_{i=0}^{2} ix^i(1+y)\right) \Big(1 + r\sum_{i=0}^{2} ix^i(1+y) + a_1(x-1) + ra_1(x-1)\sum_{i=0}^{2} ix^i(1+y) \\
&\quad + a_2(x^2-1) + ra_2(x^2-1)\sum_{i=0}^{2} ix^i(1+y) + b\hat{x}y + br\hat{x}y\sum_{i=0}^{2} ix^i(1+y) \Big).
\end{aligned}$$

- $br\hat{x}y\sum_{i=0}^{2} ix^i(1+y) = 0.$
- $ra_1(x-1)\sum_{i=0}^{2} ix^i(1+y) = 2a_1r\hat{x}(1+y).$
- $ra_2(x^2-1)\sum_{i=0}^{2} ix^i(1+y) = a_2r\hat{x}(1+y).$

Thus

$$c^t = \left(1 + 2r\sum_{i=0}^{2} ix^i(1+y)\right)\left(1 + a_1(x-1) + a_2(x^2-1) + b\hat{x}y + r\sum_{i=0}^{2} ix^i(1+y) + (2a_1r + a_2r)\hat{x}(1+y)\right)$$

$$= 1 + a_1(x-1) + a_2(x^2-1) + b\hat{x}y + r\sum_{i=0}^{2} ix^i(1+y) + (2a_1r + a_2r)\hat{x}(1+y) + 2r\sum_{i=0}^{2} ix^i(1+y)$$

$$+ 2a_1r\sum_{i=0}^{2} ix^i(1+y)(x-1) + 2a_2r\sum_{i=0}^{2} ix^i(1+y)(x^2-1) + 2br\sum_{i=0}^{2} ix^i(1+y)\hat{x}y$$

$$+ 2r^2\left(\sum_{i=0}^{2} ix^i(1+y)\right)^2 + 2r(2a_1r + a_2r)\sum_{i=0}^{2} ix^i(1+y)\hat{x}(1+y)$$

- $2a_1r\sum_{i=0}^{2} ix^i(1+y)(x-1) = a_1r\hat{x}(1+2y)$.
- $2a_2r\sum_{i=0}^{2} ix^i(1+y)(x^2-1) = a_2r\hat{x}(2+y)$.
- $2br\sum_{i=0}^{2} ix^i(1+y)\hat{x}y = 0$.
- $2r^2\left(\sum_{i=0}^{2} ix^i(1+y)\right)^2 = 0$.
- $2r(2a_1r + a_2r)\sum_{i=0}^{2} ix^i(1+y)\hat{x}(1+y) = 0$.

Thus

$$c^t = 1 + a_1(x-1) + a_2(x^2-1) + b\hat{x}y + (2a_1r + a_2r)\hat{x}(1+y) + a_1r\hat{x}(1+2y) + a_2r\hat{x}(2+y)$$
$$= 1 + a_1(x-1) + a_2(x^2-1) + b\hat{x}y + 2a_1r\hat{x} + 2a_1r\hat{x}y + a_2r\hat{x} + a_2r\hat{x}y + a_1r\hat{x} + 2a_1r\hat{x}y + 2a_2r\hat{x} + a_2r\hat{x}y$$
$$= 1 + a_1(x-1) + a_2(x^2-1) + (b + a_1r + 2a_2r)\hat{x}y \ \in C_H(x).$$

Therefore $C_H(x) \lhd H$. ■

Theorem 5.8 $H \cong C_H(x) \rtimes T$.

Proof. Clearly $H = C_H(x)T$, $C_H(x) \cap T = \{1\}$, $C_H(x) \lhd H$ and $T < H$. Therefore $H \cong C_H(x) \rtimes T$. ■

Theorem 5.9 $\mathcal{U}(\mathbb{F}_{3^k} D_6) \cong (C_{3^k}^{3k} \rtimes C_{3^k}^{k}) \rtimes (C_{3^k-1} \times C_{3^k-1})$

Proof. Recall that $\mathcal{U}(\mathbb{F}_{3^k} D_6) \cong H$. By Theorem 4.23 & 5.8 & 5.7,

$$\begin{aligned} \mathcal{U}\left(\mathbb{F}_{3^k} D_6\right) &\cong H \rtimes \mathcal{U}\left(\mathbb{F}_{3^k} C_2\right) \\ &\cong \left(C_3^{3k} \rtimes C_3^{k}\right) \rtimes \left(C_{3^k-1} \times C_{3^k-1}\right). \end{aligned}$$

■

With this established, we have been able to validate results in the referenced paper.

Appendices

Appendix A

Appendix

A.1 Verification of Calculations in Chapter 4

A program was written to output the units and zero divisors for any group ring RG. In this section we verify all the calculations performed at the beginning of Chapter 4. The code for the program can be found in Appendix A.2.

```
gap> f1(GF(2),CyclicGroup(2));
[R,G]=[ GF(2), "C2" ]
|RG|=4
#I  LAGUNA package: Computing the unit group ...
Unit Group: C2
Elements: [ (Z(2)^0)*<identity> of ..., (Z(2)^0)*f1 ]
Zero Divisors: 1
Elements: [ (Z(2)^0)*<identity> of ...+(Z(2)^0)*f1 ]

gap> f1(GF(2),CyclicGroup(3));
[R,G]=[ GF(2), "C3" ]
|RG|=8
Unit Group: C3
Elements: [ (Z(2)^0)*<identity> of ..., (Z(2)^0)*f1, (Z(2)^0)*f1^2 ]
Zero Divisors: 4
Elements: [ (Z(2)^0)*<identity> of ...+(Z(2)^0)*f1,
(Z(2)^0)*<identity> of ...+(Z(2)^0)*f1+(Z(2)^0)*f1^2,
(Z(2)^0)*<identity> of ...+(Z(2)^0)*f1^2, (Z(2)^0)*f1+(Z(2)^0)*f1^2 ]
\begin{verbatim}
\begin{verbatim}
gap> f1(GF(3),CyclicGroup(2));
[R,G]=[ GF(3), "C2" ]
|RG|=9
Unit Group: C2 x C2
```

```
Elements: [ (Z(3)^0)*<identity> of ..., (Z(3))*<identity> of ..., (Z(3)^0)*f1, (Z(3))*f1 ]
Zero Divisors: 4
Elements: [ (Z(3)^0)*<identity> of ...+(Z(3)^0)*f1,
(Z(3)^0)*<identity> of ...+(Z(3))*f1,
(Z(3))*<identity> of ...+(Z(3)^0)*f1, (Z(3))*<identity> of ...+(Z(3))*f1 ]
gap> f1(GF(2),CyclicGroup(4));
[R,G]=[ GF(2), "C4" ]
|RG|=16
#I  LAGUNA package: Computing the unit group ...
Unit Group: C4 x C2
Elements:
[(Z(2)^0)*<identity> of ..., (Z(2)^0)*<identity> of ...+(Z(2)^0)*f1+(Z(2)^0)*f2,
(Z(2)^0)*<identity> of ...+(Z(2)^0)*f1+(Z(2)^0)*f1*f2,
(Z(2)^0)*<identity> of ...+(Z(2)^0)*f2+(Z(2)^0)*f1*f2,
(Z(2)^0)*f1, (Z(2)^0)*f1+(Z(2)^0)*f2+(Z(2)^0)*f1*f2,
(Z(2)^0)*f2, (Z(2)^0)*f1*f2 ]
Zero Divisors: 7
Elements: [ (Z(2)^0)*<identity> of ...+(Z(2)^0)*f1,
(Z(2)^0)*<identity> of ...+(Z(2)^0)*f1+(Z(2)^0)*f2+(Z(2)^0)*f1*f2,
(Z(2)^0)*<identity> of ...+(Z(2)^0)*f2, (Z(2)^0)*<identity> of ...+(Z(2)^0)*f1*f2,
(Z(2)^0)*f1+(Z(2)^0)*f2, Z(2)^0)*f1+(Z(2)^0)*f1*f2, (Z(2)^0)*f2+(Z(2)^0)*f1*f2 ]
```

A.2 Code for Program

Here's a code for the program to output the units and zero divisors of a group ring.

```
f1:=function(ring,group)
local RG,U,M,N,K,i,j,ZD;
ZD:=[];
RG:=GroupRing(ring,group);
Print("[R,G]=",[ring,StructureDescription(group)],"\n","|RG|=",Size(RG),"\n");
U:=Units(RG);
Print("Unit Group: ",StructureDescription(U),"\n","Elements: ", Elements(U),"\n");
M:=Elements(RG);
N:=[Zero(RG)];
K:=Difference(M,N);
for i in [1..Size(K)] do
for j in [1..Size(K)] do
if K[i]*K[j]=Zero(RG) then Add(ZD,K[i]);
fi;od;od;
Print("Zero Divisors: ",Size(SSortedList(ZD)),"\n","Elements: ",SSortedList(ZD),"\n");
end;
```

A.3 Verification of the decomposition of $\mathbb{F}_7 D_{10}$

A program was written to validate the decomposition of $\mathbb{F}_7 D_{10}$ in chapter 4.

```
gap> FG:=GroupRing(GF(7),DihedralGroup(6));
<algebra-with-one over GF(7), with 2 generators>
gap> WedderburnDecomposition(FG);
[ ( GF(7)^[ 1, 1 ] ), ( GF(7)^[ 1, 1 ] ), ( GF(7)^[ 2, 2 ] ) ]
```

Conclusion

This study has been such an enjoyable experience so far. Although it seemed unrealisable at the early stages of this thesis, my drive and commitment towards unwinding the puzzle surrounding the conclusive solutions in Gildea and Creedon's paper never dwindled. That aim has been achieved and has become obvious that approaches to mathematical problems are very subjective due to varying perspectives. But a fascinating discovery will be to find out if and how this technique can be applied to group algebra ($\mathcal{U}\mathbb{F}_{3^k}D_{2,3^x}$). More alternatively, can a new technique be constructed to decompose the group algebra ($\mathcal{U}\mathbb{F}_{3^k}D_{2,3^x}$)? If the latter is achievable, can the technique be generalized so it can apply to most group algebras? These are some aspects of this study that can be ascertained through further research.

Bibliography

[1] S.S Abhyankar and C. Christensen, *Semidirect product: $x \mapsto ax+b$ as a First Example*, Mathematical Association of America (2002), 284-289.

[2] R. Allenby, *Rings, fields and groups: An Introduction to Abstract Algebra: First Edition*, Butterworth-Heinemann, 1991.

[3] M. Anderson and T. Feil, *A First Course in Abstract Algebra-rings, Groups and Fields: Second Edition*, Algebras and Applications, Chapman Hall/CRC Press, 2005.

[4] J. Pakianathan, *Exponents and the cohomology of finite groups*, Proceedings of the American Mathematical Society **128** (2000), 1893–1897.

[5] J. Gildea, *The Structure of the Unit Group of the Group Algebra of Pauli's Group over Any Field of Characteristic 2*, Internat. J. Algebra Comput. **20** (2010), 721–729.

[6] F.J Humphreys, *An Course in Group Theory: First Edition*, Algebras and Applications, Oxford University Press, USA, 1996.

[7] C.M. Polcino and S. Sehgal, *An Introduction to Group Rings: First Edition*, Algebras and Applications, Kluwer Academic Publishers, Dordrecht, 2002.

[8] D. Summit and R. Foote, *Abstract algebra: Third Edtion*, Wiley, 2003.

[9] Beachy A.J and D. Blair William, *Abstract algebra: Third Edition*, Waveland Press, 2006.

[10] G. Arfken, *Mathematical Methods for Physicists: Third Edition*, Orlando FL: Academic Press, 1985.

[11] J. Linda, *Elements of Modern Algebra: Eighth Edition*, Cengage Learning, 2005.

[12] B. A. Brown, *Generalized Dihedral Groups of Small Order*, Undergraduate thesis, Available in Simpson Library (2010).

[13] J. A. Beachy and W. D. Blair, *Abstract algebra: Second Edition*, Waveland Press, 1996.

[14] J. S. Rose, *A Course on Group Theory*, New York: Dover, 1994.

[15] S. Warner, *Modern Algebra*, Prentice-Hall Inc., 1965.

[16] R. Lidl and R. Niederreiter, *Introduction to Finite Fields and their Application*, Cambridge University Press, 1986.

[17] M.B Finan, *Introductory Notes in Linear Algebra for the Engineers*, Arkansas Tech University (2011).

[18] M. Burr, *Ring Examples*, New York University's Courant Institute of Mathematical Sciences (2008).

[19] T. Murphy, *Course 373-Finite Fields*, University of Dublin, Trinity College School of Mathematics http://www. maths. tcd. ie/pub/Maths/Courseware/FiniteFields/FiniteFields. pdf (2006).