INSTITUTE OF TECHNOLOGY SLIGO

Coding Theory, Group Automorphisms and Units of Finite Group Algebras

Fergal Gallagher

This project is submitted in fulfilment of the
requirements for the Degree of
Master of Engineering

Supervisor: Dr. Leo Creedon

Submitted to the Institute of Technology, Sligo
July 2014

Declaration

I certify that the material which I submit for assessment leading to the award of MEng is entirely my own work and has not been taken from others, save the extent that such work has been cited and acknowledged within the text of the study.

.....

Fergal Gallagher

Contents

Abstract

Group Algebras can be used to construct Low Density Parity Check Codes (LDPC) and Convolution Codes. These codes have applications within digital communication and storage, such as to improve the performance of digital radio, digital video, mobile phones, satellite and deep space communications, as well as bluetooth implementations.

In this Masters Thesis, theoretical mathematical techniques are used to construct an atlas of finite group algebras. In particular, we find and list the automorphism group of abelian groups and the unit group of finite commutative group algebras. The aim of this atlas is to improve our understanding of group algebras and their applications to Coding Theory. Firstly, the basic concepts of coding theory are introduced.

The next section of this thesis (Chapter 2- Automorphisms of Finite Abelian Groups) deals with various techniques for finding the automorphism group of different categories of abelian groups. In particular, where the group is an abelian $p-group$ with 2 distinct direct factors, use is made of recent techniques by Bidwell and Curran (2010). Hillar and Rhea (2007) give a technique involving endomorphism rings which allows the calculation of the order of $Aut(G)$ where G is abelian. Using these techniques and others a table is presented giving the structure and order of the automorphism group for many abelian groups.

Chapter 3 (Automorphisms of Non-Abelian Groups) looks beyond abelian groups. Recent methods by Curran (2008) using crossed homomorphisms are used where G is a semidirect product. Dihedral groups and general linear groups are also examined. At the end of this section there are some conjectures relating to the automorphisms of groups in general and a table is presented showing the automorphism tower of small groups.

The next section of the thesis (Chapter 4 - Finite Commutative Group Algebras) introduces the concepts of group algebras and unit groups. This Chapter contains many specific example of group algebras. In these examples the structure and order of the unit groups are examined.

In Chapter 5 ($U(FG)$ where F has *char* p and G is a $p-group$), a technique is presented for finding the structure of the unit group for non-Maschke cases. This technique involves counting the number of elements in the normalised unit group which have order dividing a particular power of p for group algebras of the form FG where G is a $p-group$ and F is a field of characteristic p. This Chapter concludes with a Theorem which gives the unit group of all group algebras of the above form. There are also some examples illustrating this.

Chapter 6 (Idempotents and the decomposition of FG) then looks at ways of finding the Artin Wedderburn decomposition where applicable. Here, recent techniques by Broche and Del Rio (2007) are used to find the decomposition and also to find the primitive central idempotents.

Finally, in Chapter 7, The Perlis Walker Theorem (1950) is used and adapted to give more general results for all possible group algebras for abelian groups. This leads to a general table giving the decomposition and unit groups of the group algebras for all abelian groups of order up to 15. In doing this, we get a further insight into the isomorphism problem for group algebras. This includes the result that given two non-isomorphic abelian groups G and H each with order n, and a field F of order q such that $q \equiv 1(mod\ n)$, then $FG \simeq FH$. Thus there is a whole class of isomorphic group algebras of this type and in each of these instances the decomposition is the direct product of n copies of the field F. We show that the minimal isomorphic pair of group algebras FG and FH with G and H not isomorphic which is not of this type is $\mathbb{F}_5C_{12}$ and $\mathbb{F}_5(C_2 \times C_6)$. We also show that there is yet another class of isomorphic group algebras. Given two non-isomorphic abelian groups G and H each with order n and each containing m elements of order 2, and a field F of order q such that $q \equiv$ -1$(mod\ e)$ where e is the exponent of the group, then $FG \simeq FH$. In this case, $FG \simeq FH \simeq \bigoplus_{i=1}^{m} F_q \oplus \bigoplus_{i=1}^{[n-(m)]/2} F_{q^2}$. An example of this is $\mathbb{F}_7(C_2 \times C_4 \times C_8) \simeq \mathbb{F}_7(C_4^3)$.

Acknowledgements

First of all, thanks to my wonderful wife Shona Heffernan for supporting me while I studied. She must often have wondered when or if I would ever finish. Also to my parents, Joan and Lionel, and to Margaret and Padraic Heffernan I am very grateful for helping out in so many ways.

Second of all thanks to Grace Corcoran, who met me for coffee many moons ago and put me in touch with her colleague Leo Creedon who became my supervisor for this project.

Thanks to Leo for introducing me to linear and abstract algebra, a subject I knew nothing about and a subject that has fascinated me ever since. Thanks for listening to my questions and answering usually with another question. It has stood me in good stead. Apologies for scribbling in the margins of your *Topics in Algebra* book Leo!

Thanks to Ian McLoughlin and Faye Monaghan for their support and encouragement and for adding a new vibrancy to IT Sligo's mathematical research.

To my colleages in the research lab (some of whom have escaped already), thanks for helping me to do battle with printers, binders, computers and sandwichmakers and for providing lots of laughs along the way.

Thanks also to Aoife, Carmel, Catriona and Taraneh in the Engineering Office who are always happy to assist.

Finally thanks to John Bartlett and Mary McLoughlin in the research office for all of their work and to Sligo County Council for contributing to my college fees.

Frequently Used Notation

C	a code
c	a codeword
G	a generator matrix
H	a parity check matrix
$w(c)$	the minimum weight of c
d_{min}	the minimum distance of a code
(n, k) code	a k dimensional subspace of $\mathbb{F}_q^n$
(n, k, d) code	an (n, k) code with minimum distance d
p	a prime integer
n	a positive integer
$\mathbb{Z}$	the set of integers
$\mathbb{N}$	the set of positive integers
$a(mod\ n)$	the remainder when a is divided by n
(a, b)	the greatest common divisor of a, b
$\phi(n)$	Euler's totient function - the number of $a \leq n$ such that $(a, n) = 1$
G	a group
$\|G\|$	the order of the group G
$\langle x \rangle$	the group generated by x
x^y	yxy^{-1}, the conjugate of x by y
$\|x\|$	$o(x)$, the order of the group element x
$H < G$	H is a subgroup of G
$H \lhd G$	H is a normal subgroup of G
G/H	the group of cosets of the normal subgroup H
$G \times H$	the direct product of groups G and H
$N \rtimes H$	the semidirect product of groups N and H with N a normal subgroup
C_n	the cyclic group of order n
C_n^k	the direct product of k copies of the cyclic group of order n

	$1 \leq i \leq n$
D_n	the dihedral group of order n
S_n	the symmetric group on n objects
$Z(G)$	the centre of G
G'	the commutator subgroup of G
$Inn(G)$	the group of inner automorphisms of G
$Aut(G)$	the group of automorphisms of G
$Aut(G:H)$	the group of automorphisms of G which fix the subgroup H
Aut^0G	G
Aut^nG	$Aut(Aut^{n-1}G)$
χ	an irreducible character of a group
G^*	the group of irreducible characters of G
R	a ring
F	a field
$\mathbb{F}_n$	the finite field with n elements
$\mathbb{Z}/n\mathbb{Z}$	the ring of integers $mod\ n$
$(\mathbb{Z}/n\mathbb{Z})^\times$	the multiplicative group of units of the ring $\mathbb{Z}/n\mathbb{Z}$
$F[x]$	the algebra of polynomials in x with coefficients in F
$GL_n(F)$	the general linear group of degree n over the field F
$GL_n(\mathbb{Z}/m\mathbb{Z})$	the general linear group of degree n over $\mathbb{Z}/m\mathbb{Z}$
FG	the group algebra of G over F
α	an element of FG
$\epsilon(\alpha)$	the augmentation map on α
$\triangle(G)$	the augmentation ideal (the kernel of the augmentation map on FG)
$\triangle(G,H)$	the left ideal of FG generated by the set $\{h-1 : h \in H\}$
$F^\times$	the multiplicative group of units of the field F
V, $V(FG)$	the normalised units of FG (the units of augmentation 1)
U, $U(FG)$	the unit group of the group algebra FG
$\hat{X}$	$\sum_{x \in X} x$
$char(F)$	the characteristic of the field F

$Aut(K/F)$	the group of automorphisms of K which fix F
$Gal(K/F)$	the Galois group of K/F
A^T	the transpose of the matrix A
$tr(A)$	the trace of the matrix A
σ	an automorphism of the field K/F
$tr_{K/F}(\alpha)$	$\sum_\alpha \sigma(\alpha)$ (the sum of Galois conjugates of α)
ζ_k	a primitive k^{th} root of unity
$F(\zeta_k)$	the field extension formed by adjoining ζ_k to the field F
$\epsilon_C(G, N)$	the idempotent associated to G, N and cyclotomic class C
$R \oplus R'$	the direct sum of R and R'
$\bigoplus_{i=1}^{n} R$	the direct sum of n copies of the ring R

1 Introduction

Error control codes are used in the manufacture of digital communications devices and digital storage devices. We can think of both communication and storage devices as communication devices. When digital data is communicated, there is a possibility that errors can occur, for example due to noise or interference. The fundamental problem in coding theory is to determine what message was sent on the basis of what is received [27].

What happens when an error control code is used? Firstly, a $k-bit$ message (effectively a $k-tuple$ vector) is encoded. This can be thought of as a $k \times n$ matrix (with $n > k$ and rank $= k$) acting on the $k-tuple$ vector. The result is an $n-bit$ codeword. The matrix is effectively the code, and it adds redundancy to the $k-bit$ message. These extra $n-k$ bits are known as a parity check and they make it possible to detect errors and if the code (i.e. the matrix) is designed well enough then the errors can be corrected. We call the $k \times n$ matrix a *generator matrix* or G for short.

For example, let G be the matrix of a linear map from $\mathbb{F}_2^k$ to $\mathbb{F}_2^n$. The image of the map consists of the 2^k codewords in the larger vector space $\mathbb{F}_2^n$. In fact the code is a k-dimensional subspace of $\mathbb{F}_2^n$. A basis of the subspace is the rows of G. This type of code is called a *linear block code* or just a *linear code*. If we label a vector in $\mathbb{F}_2^k$ as $\underline{m}$, then $\underline{m} = [m_1, m_2, ..., m_k]$. Label the rows of G as $g_1, g_2, ..g_k$ where $g_i = [g_{i1}, g_{i2}, ..., g_{in}]$. Then $\underline{c} = m_1 g_1 + m_2 g_2 + ...m_k g_k$. Note that $m_i g_j = [m_i g_{j1}, m_i g_{j2}, ..., m_i g_{jn}]$. This is how a generator matrix is applied to a message $\underline{m}$. All multiplication and addition here is done modulo 2.

By row operations we can write G as $[I_k|P]$ where I_k is the $k \times k$ identity matrix and P is the $k \times (n-k)$ *parity* matrix. Thus the first k components of each codeword will be the same as the k components of the message. The remaining $n-k$ components will be the parity part of the codeword and will be the result of $\underline{m}P$. This parity part is the added redundancy. Thus we see that $\underline{c} = \underline{m}G = [\underline{m}\ \underline{m}P]$. When G is in this format then we say that G is a *systematic encoder*. Note that the code (the set of codewords) is the

rowspace of G. If G is a $k \times n$ matrix with rank k, then we say that G describes a (n, k) code with rate $\frac{k}{n}$.

Example 1.1. *Let G be the matrix of a linear map from $\mathbb{F}_2^3$ to $\mathbb{F}_2^6$ given by*

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

We say that G is a $(6, 3)$ code. Note that G is a systematic encoder.
Label $\underline{m} = [m_1, m_2, m_3]$.
Then each codeword $\underline{c} = [c_1, c_2, c_3, c_4, c_5, c_6] = [m_1, m_2, m_3, m_1 + m_2, m_2 + m_3, m_1 + m_3]$.
Thus we get equations matching the parity part of the codeword as follows

$$\begin{aligned} c_4 = c_1 + c_2 \quad &\Rightarrow c_1 + c_2 + c_4 = 0 \\ c_5 = c_2 + c_3 \quad &\Rightarrow c_2 + c_3 + c_5 = 0 \\ c_6 = c_1 + c_3 \quad &\Rightarrow c_1 + c_3 + c_6 = 0. \end{aligned}$$

$$\Leftrightarrow \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} c_1 & c_2 & c_3 & c_4 & c_5 & c_6 \end{bmatrix}^T = \underline{0}.$$

This 3×6 matrix is called a parity check matrix. When it is applied to any codeword, the result is the zero vector. So the nullspace of this new matrix is the code generated by the rowspace of G.

Definition The matrix whose nullspace consists of all of the codewords of G is called the *parity check matrix* of the code. We call it H for short.

Lemma 1.2. *[25] If $G = [I_k|P]$, then $H = [-P^T|I_{n-k}]$.*

Proof. $\underline{c} = \underline{m}G = [c_1, c_2, ..., c_k, c_{k+1}, ..., c_n] = [m_1, m_2, ...m_k, \underline{m}P]$.
$\Rightarrow$[$c_{k+1}, ..., c_n$] = $\underline{m}.P$
$\Rightarrow$[$c_{k+1}, ..., c_n$] = $[c_1, c_2, ..., c_k][P]$
$\Rightarrow$[$c_{k+1}, ..., c_n$]^T = $[P]^T[c_1, c_2, ..., c_k]^T$
$\Rightarrow$[-P]$^T[c_1, c_2, ..., c_k]^T$ + $[c_{k+1}, ..., c_n]^T = [0_1, 0_2, ..., 0_{n-k}]^T$

$\Rightarrow$[-P]$^T[c_1, c_2, ..., c_k]^T + [I_{n-k}][c_{k+1}, ..., c_n]^T = [0_1, 0_2, ..., 0_{n-k}]^T$
$\Rightarrow$[-P$^T|I_{n-k}][c_1, c_2, ..., c_k, c_{k+1}, ..., c_n]^T = [0_1, 0_2, ..., 0_{n-k}]^T$.

Thus we have that $H = [-P^T|I_{n-k}]$.

Note that in $\mathbb{F}_2$ we get $-P^T = P^T$ so we can usually write $H = [P^T|I_{n-k}]$. The rows of H are linearly independent, so H acts as a generator for a $(n, n-k)$ code. This code is called the *dual* code of the (n, k) code defined by G and vice versa. The dual code of G is defined as the rowspace of H and can be thought of as the *orthogonal complement* of the code defined as the rowspace of G. All of the vectors in the former are orthogonal to all of the vectors in the latter (i.e. their inner product is zero).
However, although these subspaces are orthogonal they are not necessarily mutually exclusive, especially over finite fields. Sometimes, in fact they can even be the same subspace.

Example 1.3. *Let G be the matrix of a linear map from $\mathbb{F}_2^2$ to $\mathbb{F}_2^4$ given by*

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}.$$

Then the parity check matrix is $H = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$.
Clearly, the code and the dual code are the same subspace in this example.

A very important feature of a code is the distance between the codewords, as it is this distance which enables us to correct errors.

Definition [4] The *Hamming distance* between two codewords is the number of components in which they differ.

Example 1.4. *The Hamming distance between the codewords [1 0 0 1 0 1] and [0 1 0 1 0 1] is 2 since they differ only in the first and second components.*

Definition [4] The *Hamming weight* $w(c)$ of a codeword c is the number of its non-zero components. The *minimum Hamming weight* w_{min} of a code is the smallest *Hamming weight* of its non zero codewords.

Thus to find the distance between two codewords, we can subtract one from the other and count the number of non-zero components in the result (i.e. calculate the Hamming weight). However, as the code is a subspace, the difference between two codewords is also a codeword, and so to find the minimum distance between all codewords, we simply calculate the minimum Hamming weight of all non-zero codewords.

Example 1.5. *Let c_1 = [1 0 0 1 0 1] and c_2 = [0 1 0 1 0 1].*
Then $c_1 - c_2$ = [1 1 0 0 0 0]. This is also a codeword and it has weight 2. This corresponds to the Hamming Distance between c_1 and c_2.

Definition [4] For a linear code C, the *minimum distance* $d_{min} = min_{c \in C, c \neq 0} w(c)$. If the minimum distance of a (n, k) code is d, then we say it is a (n, k, d) code.

Lemma 1.6. *Let H be the parity check matrix of a code. Then the minimum distance of the code is d if and only if the minimum number of linearly dependent columns of H is d.*

Proof. Let $\underline{c}$ be an arbitrary codeword with weight w (i.e. w non-zero terms). We can write $\underline{c} = [..., 1_1, .., 1_2, ..., 1_w, ..]$ where w of the entries are 1 and $n-w$ of the entries are 0.
Then, for a parity check matrix H we have that $H.\underline{c}^T = 0$.
We show this by writing $H.\underline{c}^T = 0$ as follows:

$$\begin{bmatrix} h_1 & h_2 & .... & h_n \end{bmatrix} \begin{bmatrix} \vdots \\ 1_{j1} \\ \vdots \\ 1_{j2} \\ \vdots \\ 1_{jw} \\ \vdots \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ 0 \end{bmatrix}$$ where h_i is a column of H.

(Note that we use $j1$ as the index to make clear that it is not the first component of the codeword, but the first 1 of the codeword)

Then $h_{j1} + h_{j2} + ... + h_{jw} = \underline{0}$.
That is, the columns of H corresponding to the 1's in the codeword add to zero. In other words there is a linear combination of w columns of H that add to 0 and so there are w columns of H that are linearly dependent.
Now if the minimum distance of a code is d then there exists a codeword with d 1's and so there exist d linearly dependent columns in H.
Conversely, suppose the minimum number of linearly dependent columns of H is d. Then the minimum distance of the code cannot be less that d. However, because the nullspace of H consists of the set of all codewords, we know that there must exist a codeword with 1's in the positions of these linearly dependent columns, and zeros elsewhere. Thus the minimum distance of the code is equal to d.

Now we show how to construct a code with minimum distance equal to 3.

Example 1.7. *Let the columns of H consist of all possible distinct non-zero $r-$bit vectors, where r is a natural number greater than 1.*
Then, because the zero vector is excluded, the number of linearly dependent columns is not equal to 1.
Next, because all of the columns are distinct, then the number of linearly dependent columns is not equal to 2.
Finally, because we have included all possible non-zero $r-$bit vectors, we will have that one of the vectors is the sum of two other vectors, and so there are 3 linearly dependent columns. By Lemma 1.6, the minimum distance of the code is equal to 3.

Example 1.8. *Let $n-k = 3$. We let the columns of H consist of all possible non-zero $3-$bit vectors.*

$$\textit{That is } H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Now $n = 7 \Rightarrow k = 4$, and as in the previous example the minimum distance is 3, so we have constructed a $(7, 4, 3)$ code.

This code is called the Hamming $(7, 4, 3)$ *code and is a famous code.[4] In systematic form* $[P^T|I]$*, such a check matrix is*

$$H' = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Note that in the previous example H was rearranged to form H'. This can be achieved by a series of elementary row operations and column swaps.
Generator matrices G can also be rearranged to be in systematic form $G' = [I|P]$ by elementary row operations and column swaps.
If G' (or H') can be reached by elementary row operations only, then it defines the same subspace as G (or H) and so the codes are equal. If column swaps are needed then the two codes are *equivalent* (though they are usually considered to be the same code). If two codes are equivalent, they are the same except for a permutation of components.

Note that if C is a binary (n, k, d) code with d odd, it can be extended to an $(n + 1, k, d + 1)$ code by adding a check symbol to the end of all codewords. For example, adding a 1 if the weight is odd, or a zero if the weight is even. In this way all of the codewords will have even weight, and those that had weight d, will now have weight $d + 1$.

Example 1.9. *Let* H *be the check matrix of a binary code given by*

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

This $(7, 4, 3)$ *Hamming Code can be extended to a* $(8, 4, 4)$ *code by adding a check symbol as metioned above. The new check matrix* H_e *can be formed by adding a column of zeros and then a row of 1s.*

$$H_e = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

For the new matrix H_e, there is no zero column and so the number of linearly dependent columns of H_e is not 1. The extra column is non-zero and different from all of the others and so the number of linearly dependent columns of H_e is not 2. Also, if we add any 3 columns, we will get 1+1+1 = 1 for the 4th component. Thus we will have to add at least 4 columns to get the zero vector, and the minimum number of linearly dependent columns is at least 4. By adding the 1^{st}, 2^{nd}, 6^{th} and 8^{th} columns we get 0, and so the minimum number of linearly dependent columns is equal to 4. By Lemma 1.6, the minimum distance of the code is 4. This code is called the extended Hamming $(8, 4, 4)$ code [27].

1.1 Cyclic Codes

Definition [27] A nonconstant polynomial $f(x) \in \mathbb{F}_q[x]$ is *irreducible over* $\mathbb{F}_q$, provided it does not factor into a product of two polynomials in $\mathbb{F}_q[x]$ of smaller degree.

Definition [4] A *monic* polynomial is a polynomial with leading coefficient equal to one.

Definition [4] A monic irreducible polynomial of degree at least one is called a *prime polynomial*.

Linear codes can be described more compactly by working in an extension field $\mathbb{F}_{q^n}$.
For example, consider the $(7, 4, 3)$ binary Hamming code given by

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix},$$

We can identify the columns of H with elements of $\mathbb{F}_{2^3}$ where the components of the column represent the coefficients of the three basis elements in the extended field $\mathbb{F}_{2^3}$. First let us define $\mathbb{F}_{2^3}$.
The elements of $\mathbb{F}_{2^3}$ are $0, 1, a, a^2, 1+a, 1+a^2, a+a^2, 1+a+a^2$.
This field extension can be considered as a 3-dimensional vector space over $\mathbb{F}_2$ with basis elements 1, a, a^2.
A prime polynomial of degree 3 over the field $\mathbb{F}_2$ is $p(x) = x^3 + x + 1$.
Taking a to be a root of this polynomial we see that a basis of the extension field containing this root is $\{a^0, a^1, a^2\}$ which is $\{1, a, a^2\}$. Because a is a root of $p(x)$ we also get that $a^3 = a + 1$. Also because a is a multiplicative generator of $(\mathbb{F}_{2^3})^\times$, we can write all of the non-zero elements of $\mathbb{F}_{2^3}$ as powers of a as follows.

non-zero element of $\mathbb{F}_{2^3}$	1	a	a^2	1+a	a+a^2	1+a+a^2	1+a^2
element as a power of a	a^0	a^1	a^2	a^3	a^4	a^5	a^6

Thus we can write $H = [a^0 a^1 a^2 a^3 a^4 a^5 a^6]$.

Recall that the null space of the check matrix H is the set of all codewords, so we have that $H\underline{c}^T = 0$. In this case we can write $\underline{c}H^T = 0$.
Note that $\underline{c} = [c_0, c_1, c_2, c_3, c_4, c_5, c_6]$ is a vector with entries in $\mathbb{F}_2$ while H^T is a vector with entries in $\mathbb{F}_{2^3}$. Multiplication and addition is performed in the extension field $\mathbb{F}_{2^3}$.
Now we can rewrite $\underline{c}H^T = 0$ as

$$\sum_{i=0}^{6} c_i a^i = 0.$$

This means that the codeword c can be represented by a *codeword polynomial* $c(x) = \sum_{i=0}^{6} c_i x^i$, where the operation of multiplying the codeword by the check matrix is done by evaluating the codeword polynomial at $x = a$.
Then $c(x)$ is a codeword if $c(a) = 0$ (i.e. if $\sum_{i=0}^{6} c_i a^i = 0$).
Thus a binary polynomial $c(x)$ is a codeword if and only if a is a zero of the polynomial. Thus the $(7, 4, 3)$ Hamming code is the set of all polynomials $c(x)$ over $\mathbb{F}_2$ of degree at most 6 that have a as a zero in $\mathbb{F}_{2^3}$.

1.2 Group Ring Matrices

Let RG be a group ring with $|G| = n$. Then for each element of the group ring there is a unique $n \times n$ matrix with coefficients from R according to a particular listing of the group elements. A listing of the group elements is a permutation of the n group elements. For example, consider the group ring $\mathbb{F}_2C_4$ with group listing $1, x, x^2, x^3$. We can form a group matrix as follows.

	1	x	x^2	x^3
1	1	x	x^2	x^3
x^3	x^3	1	x	x^2
x^2	x^2	x^3	1	x
x	x	x^2	x^3	1

.

The column headings are the group elements according to the group listing, and the row headings are the inverses of the group elements in the listing. The entries of the matrix consist of the product of the row and column headings. Thus we get the 4×4 group matrix

$$\begin{bmatrix} 1 & x & x^2 & x^3 \\ x^3 & 1 & x & x^2 \\ x^2 & x^3 & 1 & x \\ x & x^2 & x^3 & 1 \end{bmatrix}.$$

This matrix is circulant (each row is the same as the row above but shifted one place to the right). Some group listings give circulant group matrices and some do not. With this group matrix, we can form a group ring matrix for each group ring element. For example consider the group ring element $x^2 + x^3$ in $\mathbb{F}_2C_4$. Then the group ring matrix according to the group listing $1, x, x^2, x^3$ is the coefficients of the group elements x^2 and x^3 in the positions where these group elements appear in the group matrix.
So the group ring matrix of $x^2 + x^3$ is

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

There is a bijective ring homomorphism between the ring of group ring matrices according to a group listing and the group ring itself [18].

Lemma 1.10. *[18] In a group algebra FG, a non-zero element u is a zero divisor if the corresponding group ring matrix does not have full rank, and is a unit otherwise.*

Definition [18] The *rank* of a group ring element is the rank of the corresponding group ring matrix.

Example 1.11. *Let $RG \simeq \mathbb{F}_2 C_7$. For the listing $1, x, x^2, x^3, x^4, x^5, x^6$ we get the group matrix*

$$\begin{bmatrix} 1 & x & x^2 & x^3 & x^4 & x^5 & x^6 \\ x^6 & 1 & x & x^2 & x^3 & x^4 & x^5 \\ x^5 & x^6 & 1 & x & x^2 & x^3 & x^4 \\ x^4 & x^5 & x^6 & 1 & x & x^2 & x^3 \\ x^3 & x^4 & x^5 & x^6 & 1 & x & x^2 \\ x^2 & x^3 & x^4 & x^5 & x^6 & 1 & x \\ x & x^2 & x^3 & x^4 & x^5 & x^6 & 1 \end{bmatrix}.$$

The group ring matrix of the element $1 + x + x^3$ according to this listing is

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

By row reduction, this group ring matrix becomes

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

Thus the group ring element $1 + x + x^3$ *has rank 4.*

1.3 Zero Divisor Codes

Another way of constructing a code is to use zero divisors in group rings. To construct a code we need a group ring, a submodule of the group ring and a zero divisor in the group ring.

Example 1.12. *Take the group ring* $\mathbb{F}_2C_7$*. This can be considered as a group ring or as a vector space over* $\mathbb{F}_2$ *with group elements* $1, x, x^2, x^3, x^4, x^5, x^6$ *as a basis. Let* W *be a submodule of* $\mathbb{F}_2C_7$ *with basis* $S = \{1, x, x^2, x^3\}$*. That is* W *consists of all linear combinations of these 4 group elements with coefficients from* $\mathbb{F}_2$*. Clearly* $|W| = 16$*.*
Let $u = 1 + x + x^3 \in \mathbb{F}_2C_7$*. Now* $1 + x + x^3$ *is a zero divisor in* $\mathbb{F}_2C_7$ *because* $(1 + x + x^3)(x + x^4 + x^5 + x^6) = 0$*. We also saw that* $1 + x + x^3$ *has rank 4 in Example 1.11 and so by Lemma 1.10 it is a zero divisor.*
Multiplying u *by the 4 basis elements of* W *we get*

$$\begin{aligned} 1u &= 1 + x + x^3 \\ xu &= x + x^2 + x^4 \\ x^2u &= x^2 + x^3 + x^5 \\ x^3u &= x^3 + x^4 + x^6 \end{aligned}$$

These 4 group ring elements form a basis Su *of the code* Wu*.*
Writing these elements as vectors over $\mathbb{F}_2$ *we can form a matrix*

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

The rowspace of this matrix will be the set of vectors in the code Wu. Now we apply a series of elementary row reduction steps.
Firstly, $R1 \to R1 - R4$ and $R3 \to R3 - R4$ gives us

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

Then, $R2 \to R2 - R3$ gives

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

And finally $R1 \to R1 - R2$ gives

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} = G.$$

Note that this matrix is the same as the row reduced version of the group ring matrix of $1 + x + x^3$ with the zero rows deleted. We found this in Example 1.11 by using row reduction techniques. In this way, we say that the element $1+x+x^3$ generates the code. It is in fact the Hamming (7,4,3) code that we encountered earlier [21]. The length of the code is the number of elements in the group G, in this case 7. Note that the rank of the group ring matrix of $1 + x + x^3$ equals the size of the basis S of the sub-module W. Now, with this generator matrix G, we can form the 16 elements of the code Wu as the rowspace of G. They are:

[0000000], [0001101], [0010111], [0011010],
[0100011], [0101110], [0110100], [0111001],
[1000110], [1001011], [1010001], [1011100],
[1100101], [1101000], [1110010], [1111111].

Since our generator matrix is in standard form ($[I|P]$) we can easily form the parity check matrix $H = [P^T|I]$.

We get the matrix

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} = H.$$

The rowspace of this matrix H is the dual code of the Hamming (7,4,3) code G above. The rowspace of H is a (7,3) code and it consists of the following 8 vectors:

[1011100], [1110010], [0111001], [0101110]
[1100101], [1001011], [0010111], [0000000].

Note first of all that all of the non-zero codewords in this dual code have weight 4 and so the minimum distance is 4. Thus we have a (7,3,4) code. Secondly, all 8 vectors in the dual code are also in the Hamming (7,4,3) code, so we have another example where a subspace and its orthogonal complement (i.e. dual code) are not mutually exclusive. Indeed here the Hamming (7,4,3) code contains its dual code.

The Hamming (7,4,3) code generated in the above example is revisited later on in this thesis in Example 6.21 where it is shown how this code arises as a subspace of the group algebra $\mathbb{F}_2 C_7$.

2 Automorphisms of Finite Abelian Groups

The next section of the thesis explores group theory and in particular the automorphisms of abelian groups. The following result will be used throughout this Chapter.

Lemma 2.1. *[17] Let $G = H \times K$ be a direct product of groups where $|H|$ and $|K|$ are coprime. Then $Aut(G) \simeq Aut(H) \times Aut(K)$.*

This is a very useful result, because by the fundamental theorem of abelian groups all finite abelian groups can be written as a direct product of groups of the form: $H_p = C_{p^{e_1}} \times C_{p^{e_2}} \times .....\times C_{p^{e_n}}$ in which p is a prime number and $1 \leq e_1 \leq .... \leq e_n$ are positive integers.
That is, if G is a finite abelian group, then $G = H_{p_1} \times H_{p_2} \times .... \times H_{p_m}$.

Example 2.2. *Let $G = C_8 \times C_{16} \times C_{32} \times C_3 \times C_{27} \times C_{27}$*
This can be broken down into two factor groups $H_2 = C_{2^3} \times C_{2^4} \times C_{2^5}$ and $H_3 = C_{3^1} \times C_{3^3} \times C_{3^3}$ where $|H_2|$ and $|H_3|$ are coprime. So $G = H_2 \times H_3$. Hence $Aut(G) \simeq Aut(H_2) \times Aut(H_3)$.

Thus in order to find the order and structure of $Aut(G)$ for all finite abelian groups G, it is only necessary to look at $Aut(H_p)$. In this section, all possible groups of the form H_p are examined, starting with basic examples and finishing with more complex ones.

The most basic example is C_1. For this group there is only one possible automorphism, the identity map which maps each element to itself. Thus $Aut(C_1) \simeq C_1$. The next smallest group is C_2 which contains two elements, a generator of order 2 and the identity. Now an automorphism being an isomorphism must send elements of order n to elements of order n, and so the generator of this group can only be mapped to itself, and thus $Aut(C_2)$ $\simeq C_1$ also.

Before looking at whole classes of abelian groups, it is useful to look in detail at a specific group to show how an automorphism group can be found step by step.

Example 2.3. *Finding the automorphisms of* $C_4 \times C_2$. *Writing* $C_4 \times C_2$ *as* $\langle x \rangle \times \langle y \rangle$, *the elements are* $1, x, x^2, x^3, y, xy, x^2y, x^3y$.
The orders of the elements are as follows:

element	*1*	x	x^2	x^3	y	xy	x^2y	x^3y
order	*1*	*4*	*2*	*4*	*2*	*4*	*2*	*4*

The generator x *can be mapped to any of the elements of order 4:* x, x^3, xy *or* x^3y. *This gives 4 automorphisms. In each case the image of* x *when squared gives* x^2, *so* x^2 *will also be mapped to* x^2 *as these mappings are homomorphisms. Thus the generator* y *cannot go to* x^2, *and can only go to* y *or to* x^2y. *Thus there are a further 2 automorphisms for each of the earlier 4. Thus there are a possible* $4 \times 2 = 8$ *automorphisms.*

These automorphisms are as follows:

$$\begin{array}{llll} \psi_1(x) = x & \psi_2(x) = x^3 & \psi_3(x) = xy & \psi_4(x) = x^3y \\ \psi_1(y) = y & \psi_2(y) = y & \psi_3(y) = y & \psi_4(y) = y \end{array}$$

$$\begin{array}{llll} \psi_5(x) = x & \psi_6(x) = x^3 & \psi_7(x) = xy & \psi_8(x) = x^3y \\ \psi_5(y) = x^2y & \psi_6(y) = x^2y & \psi_7(y) = x^2y & \psi_8(y) = x^2y \end{array}$$

By labelling the 8 elements of $C_4 \times C_2$ *from* 1 *to* 8, *it is possible to describe the mapping of each automorphism by the cycle decomposition on these 8 elements.*

Element	*Cycle Decomposition*	*Order*
ψ_1	(1)	*1*
ψ_2	(24)(68)	*2*
ψ_3	(26)(48)	*2*
ψ_4	(28)(46)	*2*
ψ_5	(57)(68)	*2*
ψ_6	(24)(57)	*2*
ψ_7	(2648)(57)	*4*
ψ_8	(2846)(57)	*4*

Each of these cycle decompositions is distinct, and so $|Aut(G)| = 8$. *Clearly there are 5 elements of order* 2 *in* $Aut(G)$ *and the only group of order* 8 *with exactly 5 elements of order* 2 *is* D_8. *Thus* $Aut(C_4 \times C_2) \simeq D_8 \simeq C_4 \rtimes C_2 \simeq \langle \psi_7 \rangle \rtimes \langle \psi_6 \rangle$ *with the action being conjugation by inversion.*

2.1 Automorphisms of Cyclic Groups C_p and C_{p^n}

Definition For $n \in \mathbb{N}$ let $\phi(n)$ be the number of positive integers $a \leq n$ with a relatively prime to n. This is Euler's totient function.
For example $\phi(10) = 4$ as there are 4 numbers less than 10 which are coprime to 10. These are $\{1, 3, 7, 9\}$.

Note that when a group is cyclic, all elements can be written in terms of the generator and therefore when an automorphism on a generator is defined, it defines the automorphism for the whole group. Thus the number of distinct automorphisms is equal to the number of generators of the group.

Lemma 2.4. *For cyclic groups C_n, $Aut(C_n) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$, an abelian group of order $\phi(n)$ where ϕ is Euler's totient function.*

Proof. [13, p. 135] Let x be a generator of C_n and let $\psi_a(x) = x^a \in Aut(C_n)$ for some $a \in Z$.
Since $|x| = n$, a is only defined *mod* n. Since ψ is an automorphism, $|x| = |x^a|$, hence $(a, n) = 1$. For every a relatively prime to n, ψ_a is an automorphism of C_n.
Hence there is a surjective map Ψ from $Aut(C_n)$ to $(Z/nZ)^\times$ defined by $\psi_a \mapsto a \ (mod\ n)$. That is $\Psi : Aut(C_n) \to (Z/nZ)^\times$ where $\Psi(\psi_a) = a \ (mod\ n)$.

The map Ψ is a homomorphism because $\psi_a\psi_b(x) = \psi_a(x^b) = (x^b)^a = x^{ab} = \psi_{ab}(x)$ for all ψ_a, $\psi_b \in Aut(C_n)$ so that $\Psi(\psi_a\psi_b)$=$\Psi(\psi_{ab}) = ab \ (mod\ n) = a \ (mod\ n)b \ (mod\ n)$= $\Psi(\psi_a)\Psi(\psi_b)$.
Ψ is clearly injective, hence it is an isomorphism.

We show that the automorphism group is abelian by multiplying two such automorphisms ψ_a and ψ_b and considering the effect on x.
$\psi_a\psi_b(x) = \psi_a(x^b) = (x^b)^a = x^{ba}$
$\psi_b\psi_a(x) = \psi_b(x^a) = (x^a)^b = x^{ab}$
But $ba = ab$ because $a, b \in \mathbb{Z}$ so $\psi_a\psi_b(x) = \psi_b\psi_a(x)$

Corollary 2.5. $Aut(C_p) \simeq C_{p-1}$.

Proof. This is a result of $(\mathbb{Z}/p\mathbb{Z})^\times$ being the multiplicative group of the finite field $\mathbb{F}_p$ which is cyclic of order $p-1$.

Example 2.6. *$Aut(C_3) \simeq C_2$ by Corollary 2.5.*

Example 2.7. *$Aut(C_{17}) \simeq C_{16}$ by Corollary 2.5*

It is worth noting that cyclic groups of composite order such as C_6 can be decomposed into $C_2 \times C_3$, so that $Aut(C_6) \simeq Aut(C_2) \times Aut(C_3)$ by Lemma 2.1. As a result we need only look at cyclic groups C_p and C_{p^n}. The case for cyclic groups C_p has been described above. The case for cyclic groups C_{p^n} follows.

Lemma 2.8. *For all $n \geq 3$, $Aut(C_{2^n}) \simeq C_2 \times C_{2^{n-2}}$.*

Proof. $\phi(2^n) = 2^{n-1}$ and so by Lemma 2.4 we have $Aut(C_{2^n}) \simeq (\mathbb{Z}/2^n\mathbb{Z})^\times$, an abelian group of order 2^{n-1}. The next step is to describe the structure of $(\mathbb{Z}/2^n\mathbb{Z})^\times$.
First we show that $(1+2^2)$ has order dividing 2^{n-2} in $(\mathbb{Z}/2^n\mathbb{Z})^\times$.

By the binomial theorem $(1+2^2)^{2^{n-2}}$

$= 1+2^{n-2}(2^2)+\frac{(2^{n-2})(2^{n-2}-1)}{2}(2^2)^2+\frac{(2^{n-2})(2^{n-2}-1)(2^{n-2}-2)}{(3)(2)}(2^2)^3+...+(2^2)^{2^{n-2}}$

$= 1 + 2^n + (2^{n+1})(2^{n-2}-1) + (2^{n+3})\frac{(2^{n-2}-1)(2^{n-2}-2)}{3} +...+ 2^{2^{n-1}}$

$= 1 + 0 + 0 +... + 0 \equiv 1 \ (mod\ 2^n)$.

Now, we show that $(1+2^2)$ cannot have order less than 2^{n-2} in $(\mathbb{Z}/2^n\mathbb{Z})^\times$.

Again using the binomial theorem $(1+2^2)^{2^{n-3}}$

$= 1+2^{n-3}(2^2)+\frac{(2^{n-3})(2^{n-3}-1)}{2}(2^2)^2+\frac{(2^{n-3})(2^{n-3}-1)(2^{n-3}-2)}{(3)(2)}(2^2)^3+...+(2^2)^{2^{n-3}}$

$= 1 + 2^{n-1} + (2^n)(2^{n-3}-1) + (2^{n+2})\frac{(2^{n-3}-1)(2^{n-3}-2)}{3} +...+ 2^{2^{n-2}}$

$= 1 + 2^{n-1} + 0 +... + 0 \not\equiv 1 \ (mod\ 2^n)$

Thus $(1+2^2)$ generates a cyclic subgroup of order 2^{n-2} which is necessarily of index 2 in $(\mathbb{Z}/2^n\mathbb{Z})^\times$ by the order of $(\mathbb{Z}/2^n\mathbb{Z})^\times$ given above.

Now we show that the structure of the group is not cyclic by exhibiting two distinct elements of order 2.

$[(1+2^{n-1})]^2 = 1 + 2^n + 2^{2n-2} \equiv 1 \ (mod\ 2^n)$.

Also $[-1]^2 = 1 \equiv 1 \ (mod\ 2^n)$.

Clearly these elements have order 2. If they are the same element then their product $\equiv 1 \ (mod\ 2^n)$.

By multiplying them, we get $(-1)(1+2^{n-1}) = (-1-2^{n-1}) \not\equiv 1 \ (mod\ 2^n)$.

To see that this more clearly, suppose $(-1-2^{n-1}) \equiv 1 \ (mod\ 2^n)$.

Then $-2^{n-1} \equiv 2 \ (mod\ 2^n)$

$\Rightarrow 2^{n-1} \equiv -2 \ (mod\ 2^n)$

$\Rightarrow 2(2^{n-1}) \equiv 2(-2) \ (mod\ 2^n)$

$\Rightarrow 2^n \equiv -4 \ (mod\ 2^n)$, a contradiction as $n \geq 3$.

So $(-1-2^{n-1}) \not\equiv 1 \ (mod\ 2^n)$ as supposed.

Now because the product of the two elements $(-1-2^{n-1}) \not\equiv 1 \ (mod\ 2^n)$ this means that the two elements are distinct.

Thus, the structure of $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is abelian but not cyclic, and has a cyclic subgroup of index 2, so it is $C_2 \times C_{2^{n-2}}$.

Example 2.9. *$Aut(C_4) \simeq C_2$ by Lemma 2.4*

Example 2.10. *$Aut(C_8) \simeq C_2 \times C_2$ by Lemma 2.8.*

Example 2.11. *$Aut(C_{16}) \simeq C_2 \times C_4$ by Lemma 2.8.*

Example 2.12. *$Aut(C_{32}) \simeq C_2 \times C_8$ by Lemma 2.8.*

Lemma 2.13. $\phi(p^n) = p^{n-1}(p-1)$

Proof. Let $A = \{a|(a,p) \neq 1, a \leq p^n\}$. Then $\phi(p^n) = p^n$ - $|A|$.

Thus $A = \{a|$ a is a multiple of $p\}$, $a \leq p^n$.

Thus $A = \{1p, 2p, ..., p^{n-1}p\} \Rightarrow |A| = p^{n-1}$.

Thus $\phi(p^n) = p^n$ - $p^{n-1} = p^{n-1}(p-1)$.

Lemma 2.14. *For p an odd prime and for $n \geq 3$, then $p^{n-2} \geq n$.*

Proof. We proceed by induction. Let $n = 3$. Then $p \geq n$ because p is an odd prime.
Assume true for $n = k$. That is $p^{k-2} \geq k$.
Now test for $n = k+1$. $p^{k+1-2} = p^{k-2}p \geq kp$ by our induction hypothesis.
Clearly $kp \geq k+1$ for all p odd prime and $k \geq 3$. Thus $p^{k+1-2} \geq k+1$.

Lemma 2.15. *For all p odd, $n \in \mathbb{N}$, $n \geq 1$, $Aut(C_{p^n}) \simeq C_{p^{n-1}} \times C_{p-1}$.*

Proof. By Lemma 2.13, $Aut(C_{p^n}) \simeq (\mathbb{Z}/p^n\mathbb{Z})^\times$, an abelian group of order $p^{n-1}(p-1)$. Now we describe the structure of $(\mathbb{Z}/p^n\mathbb{Z})^\times$.
First we show that $(1+p)$ has order dividing p^{n-1} in $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

By the binomial theorem $(1+p)^{p^{n-1}}$

$= 1+p^{n-1}(p) + \frac{(p^{n-1})(p^{n-1}-1)}{2}p^2 + \frac{(p^{n-1})(p^{n-1}-1)(p^{n-1}-2)}{(3)(2)}p^3 + ... + (p)^{p^{n-1}}$

$= 1 + p^n + (p^{n+1})\frac{(p^{n-1}-1)}{2} + (p^{n+2})\frac{(p^{n-1}-1)(p^{n-1}-2)}{(3)(2)} + ... + p^{p^{n-1}}$

$= 1 + 0 + 0 + 0 ... + 0 \equiv 1 \ (mod\ p^n)$.

Now, we show that $(1+p)$ cannot have order less than p^{n-1} in $(\mathbb{Z}/p^n\mathbb{Z})^\times$.
First consider the case where $n = 1$. Clearly $(1+p)$ cannot have order less than $p^{1-1} = p^0 = 1$.
Now consider the case where $n \geq 2$. If $(1+p)$ has order less than p^{n-1} then $(1+p)^{p^{n-2}} \equiv 1 \ (mod\ p^n)$.
Again using the binomial theorem $(1+p)^{p^{n-2}}$

$= 1+p^{n-2}(p)+\frac{(p^{n-2})(p^{n-2}-1)}{2}p^2+\frac{(p^{n-2})(p^{n-2}-1)(p^{n-2}-2)}{(3)(2)}p^3+...+p^{p^{n-2}}$

$= 1 + p^{n-1} + (p^n)\frac{(p^{n-2}-1)}{2} + (p^{n+1})\frac{(p^{n-2}-1)(p^{n-2}-2)}{(3)(2)} +...+ p^{p^{n-2}}$

$= 1 + p^{n-1} + 0 + 0 +... + 0 + p^{p^{n-2}}$.

Now if n = 2, then the last term doesn't arise as there are only two terms in

the expansion, so the expansion is $1 + p^{n-1}$.
If $n \geq 3$, then by Lemma 2.14, we have that $p^{p^{n-2}} \geq p^n$ and so we get that
$(1+p)^{p^{n-2}} = 1 + p^{n-1} + 0 + 0 + ... + 0 \not\equiv 1 \ (mod\ p^n)$.

Thus $(1+p)$ generates a cyclic subgroup of index $p-1$ in $(\mathbb{Z}/p^n\mathbb{Z})^\times$.
The following part of the proof is outlined in [13, p. 314].
The map $(\mathbb{Z}/p^n\mathbb{Z}) \to (\mathbb{Z}/p\mathbb{Z})$ defined by $a + p^n\mathbb{Z} \mapsto a + p\mathbb{Z}$ is a ring homomorphism which gives a surjective group homomorphism $f : (\mathbb{Z}/p^n\mathbb{Z})^\times$ onto $(\mathbb{Z}/p\mathbb{Z})^\times$. The latter group is cyclic of order $p-1$ by Corollary 2.5. Thus the kernel of f has order p^{n-1}.

Now $|\mathbb{Z}/p^n\mathbb{Z})^\times| = p^{n-1}(p-1)$. Clearly $p \not| (p-1)$, so let $Aut(C_{p^n}) \simeq C_{p^{n-1}}$ $\times A$ where $|A| = p-1$ which is co-prime to p.
Since the kernel of f has order p^{n-1}, none of the non-identity elements of A are in the kernel of f by considering their order. Thus A maps isomorphically into the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times$ and so A is cyclic and $A \simeq C_{p-1}$ and $Aut(C_{p^n})$ $\simeq C_{p^{n-1}} \times C_{p-1}$.

Example 2.16. $C_{25} \simeq C_{5^2} \Rightarrow Aut(C_{25}) \simeq C_{5^{2-1}} \times C_{5-1} \simeq C_5 \times C_4$ *by Lemma 2.15.*

Example 2.17. $C_{27} \simeq C_{3^3} \Rightarrow Aut(C_{27}) \simeq C_{3^{3-1}} \times C_{3-1} \simeq C_9 \times C_2$ *by Lemma 2.15.*

2.2 Automorphisms of Elementary Abelian groups

Lemma 2.18. *[29] If G is the elementary abelian group C_p^n then $Aut(G) \simeq GL_n(\mathbb{F}_p)$.*

Proof. The group C_p^n can be viewed as the vector space of dimension n over the field $\mathbb{F}_p$ with group elements as $1 \times n$ column vectors.
The automorphisms of the group are the invertible linear transformations from the group to itself. These are the matrices with entries from the field $\mathbb{F}_p$ which form the group $GL_n(\mathbb{F}_p)$.

Lemma 2.19. *[5]* $|GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p)(p^n - p^2)....(p^n - p^{n-1})$.

Proof. There are p^n possibilities for each row. However an invertible $n \times n$ matrix must have n linearly independent rows so restrictions apply.

The first row cannot be the zero vector, so there are $p^n - 1$ choices.
The second row cannot be a scalar multiple of the first row so there are $p^n - p$ choices.
The third row must not be in the subspace spanned by the first two rows so there are $p^n - p^2$ choices.
This process is continued until the nth row which must not be in the subspace spanned by the first $n - 1$ rows so there are $p^n - p^{n-1}$ choices.

Hence $|GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p)(p^n - p^2)....(p^n - p^{n-1})$.

Example 2.20. $Aut(C_2^3) \simeq GL_3(\mathbb{F}_2)$.

$|GL_3(\mathbb{F}_2)| = (2^3 - 1)(2^3 - 2)(2^3 - 2^2) = (7)(6)(4) = 168.$

Example 2.21. $Aut(C_7^2) \simeq GL_2(\mathbb{F}_7)$.

$|GL_2(\mathbb{F}_7)| = (7^2 - 1)(7^2 - 7) = (48)(42) = 2016.$

Example 2.22. $Aut(C_7^4) \simeq GL_4(\mathbb{F}_7)$.

$|GL_4(\mathbb{F}_7)| = (7^4 - 1)(7^4 - 7)(7^4 - 7^2)(7^4 - 7^3) = (2400)(2394)(2352)(2058) = 27,811,094,169,600.$

In order to better illustrate these automorphisms as linear transformations of a vector space, here is a detailed look at the automorphisms of the group C_2^2.

Let $C_2^2 = \langle x \rangle \times \langle y \rangle = \{1, x, y, xy\}$. There are 2 generators and 3 elements of order 2.
The first generator can be mapped to 3 elements and the other generator has 2 remaining choices. Hence there are $3 \times 2 = 6$ automorphisms.
These 6 automorphisms are: ψ_1, ψ_2, ψ_3, ψ_4, ψ_5, ψ_6 where:

$$\begin{array}{lll} \psi_1(x) = x & \psi_2(x) = x & \psi_3(x) = y \\ \psi_1(y) = y & \psi_2(y) = xy & \psi_3(y) = x \end{array}$$

$$\begin{array}{lll} \psi_4(x) = y & \psi_5(x) = xy & \psi_6(x) = xy \\ \psi_4(y) = xy & \psi_5(y) = y & \psi_6(y) = x \end{array}$$

These automorphisms correspond to the 6 invertible 2×2 matrices over $\mathbb{F}_2$:

$$\psi_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \psi_2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \qquad \psi_3 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\psi_4 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \qquad \psi_5 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \qquad \psi_6 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

These 6 matrices with the usual matrix multiplication form the group $GL_2(\mathbb{F}_2)$.
The group $GL_2(\mathbb{F}_2)$ is also isomorphic to D_6. It can be written as $\langle \psi_4 \rangle \rtimes \langle \psi_2 \rangle$ where the action is conjugation by inverting.
By Lemma 2.18 $Aut(C_2^2) \simeq GL_2(\mathbb{F}_2)$ and $|GL_2(\mathbb{F}_2)| = (2^2 - 1)(2^2 - 2) = (3)(2) = 6$.

2.3 Automorphisms of $C_{p^\alpha}^n$

Lemma 2.23. *$Aut(C_{p^\alpha}^n) \simeq GL_n(\mathbb{Z}/p^\alpha\mathbb{Z})$.*

Proof. The group $C_{p^\alpha}^n$ can be viewed as an *R-module* over the commutative ring $\mathbb{Z}/p^\alpha\mathbb{Z}$. The automorphisms of the group are then the invertible *R-module* homomorphisms from G to itself. These are the invertible $n \times n$ matrices with entries from $\mathbb{Z}/p^\alpha\mathbb{Z}$ which form the group $GL_n(\mathbb{Z}/p^\alpha\mathbb{Z})$.

The order of this group is found using a corollary to the following theorem.

Theorem 2.24. *[5] Let m be a positive integer and let $p_1^{\alpha_1}p_2^{\alpha_2}.....p_k^{\alpha_k}$ be the prime factorisation of m. Then for each positive integer n,*

$$|GL_n(\mathbb{Z}/m\mathbb{Z})| = m^{n^2} \prod_{i=1}^{k}\prod_{j=1}^{n}(1 - p_i^{-j}).$$

Corollary 2.25. $|GL_n(\mathbb{Z}/p^\alpha\mathbb{Z})| = \prod_{j=1}^{n}(p^{\alpha n} - p^{\alpha n - j})$

Proof. Let $m = p^\alpha$

$$\text{Then } |GL_n(\mathbb{Z}/p^\alpha\mathbb{Z})| = (p^\alpha)^{n^2} \prod_{j=1}^{n}(1 - p^{-j}) = p^{\alpha n^2} \prod_{j=1}^{n}(1 - p^{-j})$$

$$= \prod_{j=1}^{n} p^{\alpha n}(1 - p^{-j}) = \prod_{j=1}^{n}(p^{\alpha n} - p^{\alpha n - j}).$$

Example 2.26. *$Aut(C_4^2) \simeq GL_2(\mathbb{Z}/4\mathbb{Z})$ by Lemma 2.23.*

$|GL_2(\mathbb{Z}/4\mathbb{Z})| = (2^{2(2)} - 2^{2(2)-1})(2^{2(2)} - 2^{2(2)-2})$

$= (2^4 - 2^3)(2^4 - 2^2) = (8)(12) = 96$ *by Corollary 2.25.*

Example 2.27. *$Aut(C_4^3) \simeq GL_3(\mathbb{Z}/4\mathbb{Z})$ by Lemma 2.23.*

$|GL_3(\mathbb{Z}/4\mathbb{Z})| = (2^{2(3)} - 2^{2(3)-1})(2^{2(3)} - 2^{2(3)-2})(2^{2(3)} - 2^{2(3)-3})$

$= (2^6 - 2^5)(2^6 - 2^4)(2^6 - 2^3) = (32)(48)(56) = 86,016$ *by Corollary 2.25.*

2.4 Automorphisms of $C_{p^m} \times C_{p^n}$

This section looks at $Aut(G)$ where G is an abelian $p-group$ with 2 distinct direct factors. Because m, n are distinct positive integers the results from the previous section do not apply. The theorems here are taken from a 2010 paper by Bidwell and Curran where there are extensive proofs given. The theorems are given here with examples. First, the case where p is odd.

Definition [13] A generator of the cyclic group of all n^{th} roots of unity is called a *primitive n^{th} root of unity.*

Definition [7] An integer s is a *primitive root modulo n* if every integer coprime to n is congruent to a power of s modulo n. In other words, s is a generator of the multiplicative group of integers modulo n.

Note that not all integers n have primitive roots mod n. However, n has primitive roots mod n if n is of the form 2,4, p^a or $2p^a$, where p is an odd prime [7]. When n has primitive roots mod n, then there are $\phi(\phi(n))$ of them where ϕ is Euler's totient function[32].

Theorem 2.28. *[3] Let $G = C_{p^m} \times C_{p^n}$, where $m > n \geq 1$. Let $u = p^{m-n}$.*

Let s be a primitive root mod p^m, so also a primitive root mod p^n and let t be its multiplicative inverse (mod p^n).

Choose w such that $s^w \equiv 1 + u \ (mod\ p^m)$.

$Aut(G)$ is given by the presentation:

$$Aut(G) \simeq \langle a, b, c, d : a^{\phi(p^m)} = b^{p^n} = c^{p^n} = d^{\phi(p^n)} = 1, b^a = b^t, b^d = b^s,$$
$$c^a = c^s, c^d = c^t, a^d = a, cb = a^{-w}bcd^w \ \rangle.$$

Theorem 2.29. *[3] For $m > n \geq 1$, $|Aut(C_{p^m} \times C_{p^n})| = (p-1)^2 p^{m+3n-2}$.*

Example 2.30. *$C_9 \times C_3 = C_{3^2} \times C_{3^1}$. $m = 2$, $n = 1$, $u = 3$.*
$s^w \equiv 1 + u \ (mod\ p^m)$ so choosing $s = 2$, we have $w = 2$ because $2^2 \equiv 1 + 3$ $(mod\ 3^2)$. The multiplicative inverse $(mod\ p^n)$ of $s = 2$ is $t = 2$, because $(2)(2) = 4 \equiv 1(mod\ 3)$. Thus we have $m = 2$, $n = 1$, $u = 3$, $s = 2$, $w = 2$ and $t = 2$.

$$Aut(G) \simeq \langle a, b, c, d : a^{\phi(3^2)} = b^{3^1} = c^{3^1} = d^{\phi(3^1)} = 1, b^a = b^2, b^d = b^2,$$
$$c^a = c^2, c^d = c^2, a^d = a, cb = a^{-2}bcd^2\rangle.$$
$$\Rightarrow Aug(G) \simeq \langle a, b, c, d : a^6 = b^3 = c^3 = d^2 = 1, b^a = b^2, b^d = b^2,$$
$$c^a = c^2, c^d = c^2, a^d = a, cb = a^{-2}bcd^2\rangle.$$
$$|Aut(C_9 \times C_3)| = (3-1)^2(3)^{2+3(1)-2} = (4)(27) = 108.$$

Example 2.31. *$C_{27} \times C_3 = C_{3^3} \times C_{3^1}$. $m = 3$, $n = 1$, $u = 9$, so choosing $s = 2$, we have $w = 6$ because $2^6 = 64 \equiv 1 + 9$ $(mod\ 3^3)$. The multiplicative inverse $(mod\ p^n)$ of $s = 2$ is $t = 2$, because $(2)(2) = 4 \equiv 1(mod\ 3)$. Thus we have $m = 3$, $n = 1$, $u = 9$, $s = 2$, $w = 6$ and $t = 2$.*

$$Aut(G) \simeq \langle a, b, c, d : a^{\phi(3^3)} = b^{3^1} = c^{3^1} = d^{\phi(3^1)} = 1, b^a = b^2, b^d = b^2,$$
$$c^a = c^2, c^d = c^2, a^d = a, cb = a^{-6}bcd^6\rangle.$$
$$\Rightarrow Aut(G) \simeq \langle a, b, c, d : a^{18} = b^3 = c^3 = d^2 = 1, b^a = b^2, b^d = b^2,$$
$$c^a = c^2, c^d = c^2, a^d = a, cb = a^{-6}bcd^6\rangle.$$
$$|Aut(C_{27} \times C_3)| = (3-1)^2(3)^{3+3(1)-2} = (4)(81) = 324.$$

Next, the automorphisms of $C_{p^m} \times C_{p^n}$, in the case where $p = 2$.

Theorem 2.32. *[3] Let $G = C_{2^m} \times C_{2^n}$, where $m > n \geq 2$. Let $u = 2^{m-n}$.*
If $u \geq 4$, choose w such that $5^w \equiv 1 + u(mod\ 2^m)$.
For $u = 2$, choose w such that $-5^w \equiv 3(mod\ 2^m)$.

$Aut(G)$ is given by the presentation:

$Aut(G) \simeq \langle\ a_1, a_2, b, c, d_1, d_2 : a_1^2 = a_2^{2^{m-2}} = b^{2^n} = c^{2^n} = d_1^2 = d_2^{2^{n-2}} = 1,$

$b^{a_1} = b^{-1}, b^{a_2} = b^{5^{-1}}, b^{d_1} = b^{-1}, c^{a_1} = c^{-1}, c^{a_2} = c^5, c^{d_1} = c^{-1},$

$c^{d_2} = c^{5^{-1}}, cb = a_2^{-w}bcd_2^w, \langle a_1, a_2, d_1, d_2\ \rangle$ *is abelian* $\rangle$

If $u = 2$, *the relation* $cb = a_2^{-w}bcd_2^w$ *must be replaced by* $cb = a_1a_2^{-w}bcd_1d_2^w$ *and an additional relation* $c^2b = a_2^{-1}bc^2d_2$ *must be included.*

Theorem 2.33. *[3] For* $m > n \geq 2$, $|Aut(C_{2^m} \times C_{2^n})| = 2^{m+3n-2}$.

Example 2.34. $C_8 \times C_4 = C_{2^3} \times C_{2^2}$. $m = 3$, $n = 2$. *Now* $u = 2$, *so choosing* $w = 1$, *we have* $-5^1 = -5 \equiv 3\ (mod\ 2^3)$. *Thus we have* $m = 3$, $n = 2$, $u = 2$, *and* $w = 1$.
Then by Theorem 2.32,
$Aut(C_8 \times C_4) \simeq \langle a_1, a_2, b, c, d_1, d_2 : a_1^2 = a_2^2 = b^4 = c^4 = d_1^2 = d_2 = 1,$

$b^{a_1} = b^{-1}, b^{a_2} = b^{5^{-1}}, b^{d_1} = b^{-1}, c^{a_1} = c^{-1}, c^{a_2} = c^5, c^{d_1} = c^{-1},$

$c^{d_2} = c^{5^{-1}}, cb = a_1a_2^{-1}bcd_1d_2,\ c^2b = a_2^{-1}bc^2d_2,\ \langle a_1, a_2, d_1, d_2\rangle$ *is abelian*$\rangle$

$|Aut(C_8 \times C_4)| = 2^{3+3(2)-2} = 2^7 = 128$ *by Theorem 2.33.*

Theorem 2.35. *[3] Let* $G = C_{2^m} \times C_2$, $m \geq 3$.

$$Aut(G) \simeq \langle\ a, b, c, d : a^{m-2} = b^2 = c^2 = d^2 = 1, b^c = a^{2^{m-3}}b,\ others\ commute\rangle$$
$$\simeq ((\langle a\rangle \times \langle b\rangle) \rtimes \langle c\rangle) \times \langle d\rangle \simeq ((C_{2^{m-2}} \times C_2) \rtimes C_2) \times C_2$$

Finally, the case where $n = 1$ and $m = 2$ is not dealt with above. There is only one group of this type, $C_4 \times C_2$. As shown in Example 2.3, $Aut(C_4 \times C_2) \simeq D_8$.

Example 2.36. $Aut(C_8 \times C_2) \simeq ((C_2 \times C_2) \rtimes C_2) \times C_2$ *by Theorem 2.35. A presentation is* $\langle\ a, b, c, d : a = b^2 = c^2 = d^2 = 1, b^c = ab,\ others\ commute\rangle$

We show that this group is isomorphic to $D_8 \times C_2$.
Label the 4 generators of $((C_2 \times C_2) \rtimes C_2) \times C_2$ *as a, b, c and d respectively. Theorem 2.35 states that all generators commute, except for b and c.*

$b^c = a^{2^{3-3}}b = ab.$

The 16 elements are $1, a, b, ab, c, ac, bc, abc, d, ad, bd, cd, abd, acd, bcd, abcd$. *From the presentation we know that all of the 4 generators have order 2. The products of commuting generators also have order 2 because*

$(ab)^2 = abab = aabb = 1$

$(abd)^2 = abdabd = aabbdd = 1$.

The elements ad, bd, cd, acd *can be shown to have order 2 in the same way.*

Thus the following 11 elements all have order 2: $a, b, ab, c, ac, d, ad, bd, cd, abd, acd$. *We show that the four remaining non-identity elements* $bc, abc, bcd, abcd$ *have order 4.*

$(bc)^2 = bcbc = bcbc^{-1} = bb^c = bab = abb = a$
$(bc)^3 = (a)(bc) = abc$
$(bc)^4 = (abc)(bc) = (a)(bcbc) = aa = 1$, *so* $|bc| = 4$.

$(abc)^2 = abcabc = aabcbc = a$
$(abc)^3 = (a)(abc) = bc$
$(abc)^4 = (bc)(abc) = (a)(bcbc) = aa = 1$, *so* $|abc| = 4$.

$(abc)^2 = abcabc = aabcbc = a$
$(abc)^3 = (a)(abc) = bc$
$(abc)^4 = (bc)(abc) = (a)(bcbc) = aa = 1$, *so* $|abc| = 4$.

$(bcd)^2 = bcdbcd = ddbcbc = a$
$(bcd)^3 = (a)(bcd) = adbc$
$(bcd)^4 = (adbc)(bcd) = (add)(bcbc) = aa = 1$, *so* $|bcd| = 4$.

Thus the automorphism group comprises exactly 11 elements of order 2, 4 elements of order 4 plus the identity, and the only group of order 16 with this property is $D_8 \times C_2$.

Example 2.37. *Aut*$(C_{16} \times C_2) \simeq ((C_4 \times C_2) \rtimes C_2) \times C_2$ *by Theorem 2.35. The presentation is* $\langle\ a, b, c, d : a^2 = b^2 = c^2 = d^2 = 1, b^c = a^2 b,$ *others commute*$\rangle$.

Lemma 2.38. *For all* $G = C_{2^m} \times C_2$, $m \geq 2$, $|Aut(G)| = |G|$.

Proof. The order of G is $(2^m)(2) = 2^{m+1}$. By Theorem 2.35 for all $m \geq 3$, $Aut(G) \simeq ((C_{2^{m-2}} \times C_2) \rtimes C_2) \times C_2$ which has order $(2^{m-2})(2)(2)(2) = 2^{m+1}$.

Also, when $m = 2$, $G = C_4 \times C_2$, and $Aut(G) \simeq D_8$ as shown in Example 2.3 with $|Aut(G)| = |G|$, completing the proof.

2.5 Automorphisms of abelian $p-groups$ with repeating factors

The method we used for finding a presentation for the automorphism group of $C_{p^m} \times C_{p^n}$ in the previous section can be extended to cover all direct products $C_{p^{m_1}} \times C_{p^{m_2}} \times ..... \times C_{p^{m_n}}$ where $m_1 > m_2 > ..... > m_n$. This method is described in Bidwell and Curran's 2010 paper [3] and gives a presentation for $Aut(G)$ for all such groups. However, it is limited to groups where each m_i $(1 \leq i \leq n)$ is distinct. That is, it is limited to abelian $p-group$ with no repeating factors.

Thus the last remaining class of abelian groups without a method for finding the stucture of $Aut(G)$ is the direct product of $p-groups$ with repeating factors which are not of the form $C^n_{p^\alpha}$.
The smallest such abelian group is $C_2 \times C_2 \times C_4$.

Example 2.39. $|Aut(C_2 \times C_2 \times C_4)|$. *Writing* $C_2 \times C_2 \times C_4$ *as* $\langle x \rangle \times \langle y \rangle \times \langle a \rangle$, *the elements are:*

$\{1, x, y, xy, a, a^2, a^3, xa, xa^2, xa^3, ya, ya^2, ya^3, xya, xya^2, xya^3\}$.

The orders of the elements are as follows:

1	x	y	xy	a	a^2	a^3	xa	xa^2	xa^3	ya	ya^2	ya^3	xya	xya^2	xya^3
1	2	2	2	4	2	4	4	2	4	4	2	4	4	2	4

The generator a can be mapped to either a, a^3, xa, xa^3, ya, ya^3, xya *or* xya^3. *This gives a maximum of 8 automorphisms. In each case the image*

of a when squared gives a^2, so a^2 will be mapped to a^2 as these mappings are homomorphisms.

Thus the generator x (which has order 2) cannot go to a^2, but can be mapped to either x, y, xy, xa^2, ya^2, or to xya^2. Thus there are a further 6 automorphisms for each of the earlier 8. This gives $8 \times 6 = 48$ possible automorphisms of the group.

Now because it has been determined where the generators x and a are mapped to, so it is determined where the element xa^2 is mapped to. Thus there are only 4 remaining elements of order 2 to which the the generator y can be mapped to (i.e. not to the image of x or to the image of xa^2). This gives a further 4 different automorphisms for each of the earlier 48, giving a total of 192 possible automorphisms for the group. There may be some further restrictions but we have an upper bound for the order of the automorphism group. In the next section it is shown that $|Aut(C_2 \times C_2 \times C_4)| = 192$.

2.6 Finding $|Aut(H_p)|$ using Endomorphism Rings

Now we look at another method for finding the order of $Aut(H_p)$. This approach is outlined in a paper by Hillar and Rhea[17] in 2007 .
Again define $H_p = C_{p^{e_1}} \times C_{p^{e_2}} \times .....\times C_{p^{e_n}}$ in which p is a prime number and $1 \leq e_1 \leq .... \leq e_n$ are positive integers.

Definition [17] Let $E_p = End(H_p)$ be the endomorphism ring of H_p.
Elements of E_p are endomorphisms from H_p into itself (i.e. homomorphisms from H_p to H_p) with ring multiplication given by composition and ring addition given by $(A+B)h = A(h) + B(h)$ for $A, B \in E_p$ and $h \in H_p$. Elements of E_p are written as matrices much like linear operators on vector spaces. Elements h are written as column vectors $(\bar{h_1}, \bar{h_2}, ..., \bar{h_n})^T$ with each $\bar{h_i} \in \mathbb{Z}/p^{e_i}\mathbb{Z}$, being an integer reduced *mod* p^{e_i}.

Definition [17] Let $R_p = \{(a_{ij}) \in \mathbb{Z}^{n\times n} : p^{e_i - e_j} | a_{ij} \ \forall\ i, j$ such that $1 \leq j \leq i \leq n\}$.
As an example take n = 3 with $e_1 = 1$, $e_2 = 2$ and $e_3 = 5$. Then

$$R_p = \left\{ \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ pb_{21} & b_{22} & b_{23} \\ p^4 b_{31} & p^3 b_{32} & b_{33} \end{bmatrix} : b_{ij} \in \mathbb{Z} \right\}.$$

Lemma 2.40. *[17] R_p forms a ring under the usual matrix addition and multiplication.*

Proof. Let A, $B \in R_p$. Clearly, $A + B \in R_p$. Now we check that it is closed under multiplication.
Let $(ab)_{ij}$ be the ij^{th} entry of the matrix AB. We only need to check the entries $(ab)_{ij}$ with $j < i$ as when $j = i$ then $p^{e_i - e_j} = p^0 = 1$ which divides all $(ab)_{ij} \in \mathbb{Z}$. Also when $j > i$ there is no restriction.

For all i, j such that $1 \leq j < i \leq n$, the ij^{th} entry of the matrix AB is given by

$\sum_{k=1}^{n} a_{ik} b_{kj}$.

We can rewrite this summation by separating it into three parts.
If $k \leq j$, then $k < i$, and the entry a_{ik} from the matrix A must be divisible by $p^{e_i - e_k}$ (because $A \in R_p$) so we write it as $a_{ik}p^{e_i-e_k}$. There is no restriction on the entry from the matrix B as $k \leq j$.

If $j < k \leq i$, then the entry a_{ik} from the matrix A is divisible by $p^{e_i-e_k}$ and we write it as $a_{ik}p^{e_i-e_k}$. For the entry b_{kj} from the matrix B, we have that $j < k$ and this is divisible by $p^{e_k-e_j}$ (because $B \in R_p$) so we write it as $b_{kj}p^{e_k-e_j}$.

If $k > i$, there are no restrictions on the entry a_{ik} from A. For the entry b_{kj} from the matrix B, we again have that $j < k$ (because $k > i > j$) and again this entry is divisible by $p^{e_k-e_j}$ so we write is as $b_{kj}p^{e_k-e_j}$.

Thus $\sum_{k=1}^{n} a_{ik}b_{kj}$
$= \sum_{k=1}^{j} a_{ik}p^{e_i-e_k}b_{kj} + \sum_{k=j+1}^{i} a_{ik}p^{e_i-e_k}b_{kj}p^{e_k-e_j} + \sum_{k=i+1}^{n} a_{ik}b_{kj}p^{e_k-e_j}$.

This then is the ij^{th} entry of the matrix AB and for it to be $\in R_p$ we must have that $p^{e_i-e_j}$ divides all three summands.

In the first summand $p^{e_i-e_k}$ is a factor of the entry and $p^{e_i-e_j} \mid p^{e_i-e_k}$ because $k \leq j$.
In the second summand $p^{e_i-e_k}p^{e_k-e_j}$ is a factor and this factor is equal to $p^{e_i-e_j}$ so clearly $p^{e_i-e_j} \mid p^{e_i-e_j}$.
Finally, in the third summand $p^{e_k-e_j}$ is a factor of the entry and $p^{e_i-e_j} \mid p^{e_k-e_j}$ because $k > i$. This completes the proof.

Definition [17] Let $\pi_i : \mathbb{Z} \to \mathbb{Z}/p^{e_i}\mathbb{Z}$ be the usual quotient mapping $\pi_i(h) = \bar{h}$ and let $\pi : \mathbb{Z}^n \to H_p$ be the homomorphism given by $\pi(h_1, h_2, ...h_n)^T = (\pi_1(h_1), \pi_2(h_2), ..., \pi_n(h_n))^T = (\bar{h_1}, \bar{h_2}, ..., \bar{h_n})^T$.

Theorem 2.41. *[17] Let $A \in R_p$ and let $(\bar{h_1}, \bar{h_2}, ..., \bar{h_n}) \in H_p$.*
The map $\psi : R_p \to End(H_p)$ given by $\psi(A)(\bar{h_1}, \bar{h_2}, ..., \bar{h_n})^T = \pi(A(h_1, h_2, ..., h_n)^T)$ is a surjective ring homomorphism.

The map ψ describes $E_p = End(H_p)$ as a quotient of the matrix ring R_p.

Lemma 2.42. *[17] The kernel of ψ is the set of matrices $A = (a_{ij}) \in R_p$ such that $p^{e_i} \mid a_{ij}\ \forall\ i, j$.*

Proof. Let $w_j = (0, ..., g_j, ..., 0)^T \in H_p$ be the vector with g_j in the jth position and zeroes everywhere else. If $A = (a_{ij})$ has the property that $p^{e_i} \mid a_{ij}\ \forall\ i, j$, then

$\psi(A)w_j = (\pi_1(a_{1j}), ..., \pi_n(a_{nj})) = 0.$

In particular, since each $h \in H_p$ is a $\mathbb{Z}$-linear combination of the w_j it follows that $\psi(A)h = 0\ \forall\ h \in H_p$. This proves that $A \in ker(\psi)$.

Conversely, suppose that $A = (a_{ij}) \in ker(\psi)$, so that $\psi(A)w_j = 0$ for each w_j. Then from the above calculation, each a_{ij} is divisible by p^{e_i}.

Theorem 2.43. *[17] An endomorphism $M = \psi(A)$ is an automorphism if and only if $A(mod\ p) \in GL_n(\mathbb{F}_p)$.*

Thus in order to form an automorphism of H_p, is is necessary to first form a matrix $A = (a_{ij}) \in R_p$. Then we quotient out each row $mod\ p^{e_i}$ to get an element of E_p. Finally this element of E_p is an automorphism of H_p if and only if we get an element of $GL_n(\mathbb{F}_p)$ when we quotient out $p\mathbb{Z}$ from each entry.

For example, consider the group $C_2 \times C_4$. Here $p = 2$, $e_1 = 1$, $e_2 = 2$.
An element A of R_2 must be of the form: $\begin{bmatrix} a_{11} & a_{12} \\ 2a_{21} & a_{22} \end{bmatrix}$

The matrix $\begin{bmatrix} 7 & 8 \\ 14 & 11 \end{bmatrix}$ is one such matrix.

When we quotient out each row $mod\ p^{e_i}$, we get: $\begin{bmatrix} 1 & 0 \\ 2 & 3 \end{bmatrix}$. This is an element of E_p.

Is it an automorphism of H_p? Well, when we quotient out $2\mathbb{Z}$, we get $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ which is an element of $GL_2(\mathbb{F}_2)$. In fact it is the identity matrix which fixes all elements of $C_2 \times C_4$.

In this way, all of the automorphisms of H_p can be formed.

In practice, it is easier to work backwards, and start with the elements of $GL_n(\mathbb{F}_p)$ that can be extended to form an element of R_p. Then we calculate the number of ways this element can be extended to form an element of E_p.

By doing this, it is possible to determine $|Aut(H_p)|$ for any H_p.

We now use $C_2 \times C_4$ as an example of how Hillar and Rhea's method for counting the automorphisms is applied. Also, in doing this, we can view the 8 elements of $\mathrm{Aut}(C_2 \times C_4)$ as matrices.

Example 2.44. *Let $H_p \simeq C_2 \times C_4$. That is $H_p \simeq C_{2^1} \times C_{2^2}$ and so $p = 2$, $e_1 = 1$ and $e_2 = 2$.*
We need to find all the elements of $GL_2(\mathbb{F}_2)$ that can be extended to a matrix $A \in R_2$, and then calculate all of the distinct ways of extending such an element to an endomorphism.

The 6 elements of $GL_2(\mathbb{F}_2)$ are:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

Of these only $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ can be extended to a matrix $A \in R_2$ because they are the only ones with zero in a_{21} position.

The next step is to calculate all of the distinct ways of extending each of the two matrices to an endomorphism. We first look at the necessary zeros of which there is just one. There are 2 ways to extend this entry as we can add any element of $p\mathbb{Z}/p^{e_i}\mathbb{Z}$. That is we can add any element of $2\mathbb{Z}/4\mathbb{Z}$ (i.e. $\{0, 2\}$). So there are 2 ways of extending this element.
At the not necessarily zero entries we can add any element of $p\mathbb{Z}/p^{e_i}\mathbb{Z}$ to the entries on the i^{th} row.
That is we can add any element of $2\mathbb{Z}/2^1\mathbb{Z}$ (i.e. $\{0\}$) to the 2 entries on the 1st row and we can add any element of $2\mathbb{Z}/4\mathbb{Z}$ (i.e. $\{0, 2\}$)to a_{22}. So a_{22} becomes either 1 or 3. This gives a total of 2 ways for all of the not

necessarily zero elements of the two matrices.
Thus the total number of distinct automorphisms is equal to the product of the number of matrices in $GL_2(\mathbb{F}_2)$ *which we can extend (2) by the number of possiblitites for the zeros (2) by the number of possiblilties for the not necessarily zero entries (2). That is* $2 \times 2 \times 2 = 8$ *automorphisms. By Example 2.3 it was established that the automorphism group of* $C_2 \times C_4$ *is* D_8*. We can now write the* 8 *automorphisms as* 2×2 *matrices thus:*

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 2 & 3 \end{bmatrix}.$$

Next we look again at $Aut(C_2 \times C_2 \times C_4)$.

Example 2.45. *Let* $H_p \simeq C_2 \times C_2 \times C_4$*. That is* $H_p \simeq C_{2^1} \times C_{2^1} \times C_{2^2}$ *and so* $p = 2$*,* $e_1 = 1$*,* $e_2 = 1$*,* $e_3 = 2$ *and* $n = 3$*.*
First we find all the elements of $GL_3(\mathbb{F}_2)$ *that can be extended to a matrix* $A \in R_2$*.*
Each matrix $A \in R_2$ *will be of the form:* $\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ 2a_{31} & 2a_{32} & a_{33} \end{bmatrix}$*, where* $a_{ij} \in \mathbb{Z}$*.*
Then $(b_{ij}) \in GL_3(\mathbb{F}_2)$ *will be of the form:* $\begin{bmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ 0 & 0 & b_{33} \end{bmatrix}$*, where* $b_{ij} \in \mathbb{F}_2$*.*

To count the number of ways of forming an invertible matrix (b_{ij})*, we need to count the number of ways it can have linearly independent rows.*
For the third row, there are already two zeros in the first two entries. The third entry cannot be zero and so it must be a 1, so there is only one choice for the third row.
For the first row there are $2^3 - 2 = 6$ *choices (all except a scalar multiple of the third row).*
For the second row there are $2^3 - 2^2 = 4$ *choices, that is all except a linear*

combination of the first and third rows (not in the span of the first and third rows).
Thus there are $6 \times 4 = 24$ *different matrices in* $GL_3(\mathbb{F}_2)$ *that can be extended to a matrix* $A \in R_2$.

Next we count the number of ways of extending each of these 24 matrices to an endomorphism.
First we count the number of choices for the necessary zeros. Because they are in the third row, they must be elements of $\mathbb{Z}/4\mathbb{Z}$ *that will be reduced to 0* $(mod\ 2)$ *and so can be either 0 or 2. That is two choices for each of the two which gives 4 different possibilities for the necessary zeros.*
Finally we count the number of choices for the not necessarily zero entries. We can add any element of $2\mathbb{Z}/2\mathbb{Z}$ *(i.e.* $\{0\}$*) to the entries on the 1st and second rows (so only one choice here) and we can add any element of* $2\mathbb{Z}/4\mathbb{Z}$ *to* b_{33}*. So we can add either 0 or 2. This gives a total of 2 ways for all of the not necessarily zero elements of the 24 matrices.*
Thus the total number of distinct automorphisms is equal to the product of the number of matrices in $GL_3(\mathbb{F}_2)$ *which we can extend (24) by the number of possiblitites for the zeros (4) by the number of possiblilties for the not necessarily zero entries (2). That is* $24 \times 4 \times 2 = 192$ *automorphisms.*

Example 2.46. *Let* $H_p \simeq C_2 \times C_4 \times C_4$ *and so* $p = 2$, $e_1 = 1$, $e_2 = 2$, $e_3 = 2$ *and* $n = 3$.
First we find all the elements of $GL_3(\mathbb{F}_2)$ *that can be extended to a matrix* $A \in R_2$.

Each matrix $A \in R_2$ *will be of the form:* $\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ 2a_{21} & a_{22} & a_{23} \\ 2a_{31} & a_{32} & a_{33} \end{bmatrix}$, *where* $a_{ij} \in \mathbb{Z}$

Then $(b_{ij}) \in GL_3(\mathbb{F}_2)$ *will be of the form:* $\begin{bmatrix} b_{11} & b_{12} & b_{13} \\ 0 & b_{22} & b_{23} \\ 0 & b_{32} & b_{33} \end{bmatrix}$, *where* $b_{ij} \in \mathbb{F}_2$.

This time, we can count the number of ways (b_{ij}) can have linearly independent columns. Because of the two zeros in the first column, the situation is identical to the previous example, and we have 24 different matrices in $GL_3(\mathbb{F}_2)$ that can be extended to a matrix $A \in R_2$.

Next we count the number of ways of extending each of these 24 matrices to an endomorphism.
First we count the number of choices for the necessary zeros. Because they are in the second and third row, we can add any element of $2\mathbb{Z}/4\mathbb{Z}$ and the entry can be either 0 or 2. That is two choices for each of the two, which gives 4 different possibilities for the necessary zeros.
Finally we count the number of choices for the not necessarily zero entries. We can add any element of $2\mathbb{Z}/2\mathbb{Z}$ (i.e. $\{0\}$) to the entries on the 1st row (so only one choice here) and we can add any element of $2\mathbb{Z}/4\mathbb{Z}$ to the four remaining entries on the second and third rows. This gives a total of $2^4 = 16$ ways for all of the not necessarily zero elements of the 24 matrices.
Thus the total number of distinct automorphisms is equal to the product of the number of matrices in $GL_3(\mathbb{F}_2)$ which we can extend (24) by the number of possiblitites for the zeros (4) by the number of possiblilties for the not necessarily zero entries (16). That is $24 \times 4 \times 16 = 1536$ automorphisms.

The slightly ad-hoc method for calculating $|Aut(H_p)|$ used in the previous three examples is stated more systematically in the following theorem from Hillar and Rhea. It is useful to take a more systematic approach for calculating $|Aut(H_p)|$ as H_p becomes larger.

Theorem 2.47. *[17] The abelian group $H_p = \mathbb{Z}/p^{e_1}\mathbb{Z} \times .... \times \mathbb{Z}/p^{e_n}\mathbb{Z}$ has*
$|Aut(H_p)| = \prod_{k=1}^{n}(p^{d_k} - p^{k-1}) \prod_{j=1}^{n}(p^{e_j})^{n-d_j} \prod_{i=1}^{n}(p^{e_i})^{n-c_i+1}$
where $d_k = max\{l : e_l = e_k\}$ and $c_k = min\{l : e_l = e_k\}$.

In words the formula states that the total number of distinct automorphisms is equal to the number of matrices in $GL_n(\mathbb{F}_p)$ which we can extend

multiplied by the number of possiblitites for the zeros multiplied by the number of possiblilties for the not necessarily zero entries.

Example 2.48. *Let* $H_p \simeq C_2^2 \times C_4 \times C_8^2 \times C_{128}$. *Then* $p = 2$, $e_1 = 1$, $e_2 = 1$, $e_3 = 2$, $e_4 = 3$, $e_5 = 3$, $e_6 = 7$ *and* $n = 6$.
First we find all the elements of $GL_6(\mathbb{F}_2)$ *that can be extended to a matrix* $A \in R_2$. *Each matrix* $A \in R_2$ *will be of the form:*

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} & a_{16} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} & a_{26} \\ 2a_{31} & 2a_{32} & a_{33} & a_{34} & a_{35} & a_{36} \\ 2^2a_{41} & 2^2a_{42} & 2a_{43} & a_{44} & a_{45} & a_{46} \\ 2^2a_{51} & 2^2a_{52} & 2a_{53} & a_{54} & a_{55} & a_{56} \\ 2^6a_{61} & 2^6a_{62} & 2^5a_{63} & 2^4a_{64} & 2^4a_{65} & a_{66} \end{bmatrix}, \text{ where } a_{ij} \in \mathbb{Z}.$$

Then $(b_{ij}) \in GL_6(\mathbb{F}_2)$ *will be of the form:*

$$\begin{bmatrix} b_{11} & b_{12} & b_{13} & b_{14} & b_{15} & b_{16} \\ b_{21} & b_{22} & b_{23} & b_{24} & b_{25} & b_{26} \\ 0 & 0 & b_{33} & b_{34} & b_{35} & b_{36} \\ 0 & 0 & 0 & b_{44} & b_{45} & b_{46} \\ 0 & 0 & 0 & b_{54} & b_{55} & b_{56} \\ 0 & 0 & 0 & 0 & 0 & b_{66} \end{bmatrix}, \text{ where } b_{ij} \in \mathbb{F}_2.$$

To count the number of ways of forming such a matrix (b_{ij}), *we need to count the number of ways it can have linearly independent columns.*
For the 1st column, there are $2^2 - 1 = 3$ *choices (all except two more zeros).*
For the 2nd column, there are $2^2 - 2 = 2$ *choices (all except a scalar multiple of the first column).*
For the 3rd column, there are $2^3 - 2^2 = 4$ *choices (all except a linear combination of the first two columns).*
For the 4th column, there are $2^5 - 2^3 = 24$ *choices (all except a linear combination of the first three columns).*
For the 5th column, there are $2^5 - 2^4 = 16$ *choices (all except a linear combination of the first four columns).*

For the 6th column, there are $2^6 - 2^5 = 32$ *choices (all except a linear combination of the first five columns).*

This is a total of $3.2.4.24.16.32 = 2^{15}.3^2$ *different matrices in* $GL_6(\mathbb{F}_2)$ *that can be extended to a matrix* $A \in R_2$.

Next we count the number of ways of extending each of these $2^{15}.3^2$ *matrices to an endomorphism.*
In each column, the necessary zeros can be extended by adding any element of $(2)^{e_i - e_j}\mathbb{Z}/(2)^{e_i}\mathbb{Z}$. *Thus for each necessary zero in a particular column* j, *there are* p^{e_j} *ways that it can be extended.*
Thus in the 1st column, there are 2^1 *ways for each of the four entries, that is* $2^4 = 16$ *choices. In the 2nd column, there are also* $2^4 = 16$ *choices. In the 3rd column there are* $4^3 = 64$ *choices. In the 4th column, there are* $8^1 = 8$ *choices and in the 5th column there are also* $8^1 = 8$ *choices.*
Altogether that is $16.16.64.8.8 = 2^{20}$ *choices for the necessarily zero entries.*

Next, we count the choices for the not necessarily zero entries. We do this one row at a time.
In each row, we can add any element of $2\mathbb{Z}/(2)^{e_i}\mathbb{Z}$ *to the not necessarily zero entries. Thus for each entry in a particular row* i, *there are* $p^{e_i - 1}$ *ways that it can be extended.*
Thus in the 1st row, there are 2^0 *ways for each of the six entries, that is* $1^6 = 1$ *choice. In the 2nd row, there are also* $1^6 = 1$ *choice. In the 3rd row there are* $2^4 = 16$ *choices. In the 4th row, there are* $4^3 = 64$ *choices. In the 5th row there are also* $4^3 = 64$ *choices. Finally, in the 6th row, there are* 64^1 *choices.*
Altogether that is $1.1.16.64.64.64 = 2^{22}$ *choices for the not necessarily zero entries.*

This means that $|Aut(C_2^2 \times C_4 \times C_8^2 \times C_{128})| = (2^{15}.3^2)(2^{20})(2^{22}) = 2^{57}.3^2$.

The results of this Chapter can be summarised in the following table.

2.7 Table of $Aut(G)$ for Small Abelian Groups

|G|	**G**	**Decomposition**	**|Aut(G)|**	**Aut(G)**
1	C_1		1	C_1
2	C_2		1	C_1
3	C_3		2	C_2
4	C_4		2	C_2
4	C_2^2		6	$GL_2(\mathbb{F}_2) \simeq D_6$
5	C_5		4	C_4
6	C_6	$C_2 \times C_3$	2	C_2
7	C_7		6	C_6
8	C_8		4	C_2^2
8	$C_2 \times C_4$		6	D_8
8	C_2^3		168	$GL_3(\mathbb{F}_2)$
9	C_9		6	C_6
9	C_3^2		48	$GL_2(\mathbb{F}_3)$
10	C_{10}	$C_2 \times C_5$	4	C_4
11	C_{11}		10	C_{10}
12	C_{12}	$C_3 \times C_4$	4	C_2^2
12	$C_2 \times C_6$	$C_2^2 \times C_3$	12	D_{12}
13	C_{13}		12	C_{12}
14	C_{14}	$C_2 \times C_7$	6	C_6
15	C_{15}	$C_3 \times C_5$	8	$C_2 \times C_4$
16	C_{16}		8	$C_2 \times C_4$
16	$C_2 \times C_8$		16	$C_2 \times D_8 \simeq D_{16}$
16	C_4^2		96	$GL_2(\mathbb{Z}/4\mathbb{Z})$
16	$C_2^2 \times C_4$		192	
16	C_2^4		20160	$GL_4(\mathbb{F}_2)$
17	C_{17}		16	C_{16}
18	C_{18}	$C_2 \times C_9$	6	C_6

Continued on next page

Table 2 – continued from previous page

|G|	G	Decomposition	|Aut(G)|	Aut(G)
18	$C_3 \times C_6$	$C_2 \times C_3^2$	48	$GL_2(\mathbb{F}_3)$
19	C_{19}		18	C_{18}
20	C_{20}	$C_4 \times C_5$	8	$C_2 \times C_4$
20	$C_2 \times C_{10}$	$C_2^2 \times C_5$	24	$C_4 \times GL_2(\mathbb{F}_2) \simeq C_4 \times D_6$
21	C_{21}	$C_3 \times C_7$	12	$C_2 \times C_6$
22	C_{22}	$C_2 \times C_{11}$	10	C_{10}
23	C_{23}		22	C_{22}
24	C_{24}	$C_3 \times C_8$	8	C_2^3
24	$C_2 \times C_{12}$	$C_2 \times C_3 \times C_4$	16	$C_2 \times D_8 \simeq D_{16}$
24	$C_2^2 \times C_6$	$C_2^3 \times C_3$	336	$C_2 \times GL_3(\mathbb{F}_2)$
25	C_{25}		20	C_{20}
25	C_5^2		480	$GL_2(\mathbb{F}_5)$
26	C_{26}	$C_2 \times C_{13}$	12	C_{12}
27	C_{27}		18	C_{18}
27	$C_3 \times C_9$		108	$\langle a, b, c, d : a^6 = b^3 = c^3 = d^2 = 1, b^a = b^2, b^d = b^2, c^a = c^2, c^d = c^2, a^d = a, cb = a^{-2}bcd^2 \rangle$
27	C_3^3		11232	$GL_3(\mathbb{F}_3)$
28	C_{28}	$C_4 \times C_7$	12	$C_2 \times C_6$
28	$C_2 \times C_{14}$	$C_2 \times C_2 \times C_7$	36	$C_6 \times D_6$
29	C_{29}		28	C_{28}
30	C_{30}	$C_2 \times C_3 \times C_5$	8	$C_2 \times C_4$
31	C_{31}		30	C_{30}
32	C_{32}		16	$C_2 \times C_8$
32	$C_2 \times C_{16}$		32	$((C_4 \times C_2) \rtimes C_2) \times C_2$

Continued on next page

Table 2 – continued from previous page

|G|	G	Decomposition	|Aut(G)|	Aut(G)
32	$C_4 \times C_8$		128	$\langle a_1, a_2, b, c, d_1, d_2$: $a_1^2 = a_2^2 = b^4 = c^4 = d_1^2 = d_2 = 1, b^{a_1} = b^{-1}, b^{a_2} = b^{5^{-1}}, b^{d_1} = b^{-1}, c^{a_1} = c^{-1}, c^{a_2} = c^5, c^{d_1} = c^{-1}, c^{d_2} = c^{5^{-1}}, cb = a_1 a_2^{-1} b c d_1 d_2, c^2 b = a_2^{-1} b c^2 d_2,$ $\langle a_1, a_2, d_1, d_2 \rangle$ is abelian$\rangle$
32	$C_2^2 \times C_8$		384	
32	$C_2 \times C_4^2$		1536	
32	$C_2^3 \times C_4$		21504	
32	C_2^5		9999360	$GL_5(\mathbb{F}_2)$
33	C_{33}	$C_3 \times C_{11}$	32	C_{32}
34	C_{34}	$C_2 \times C_{17}$	16	C_{16}
35	C_{35}	$C_5 \times C_7$	24	$C_4 \times C_6$
36	C_{36}	$C_4 \times C_9$	12	$C_2 \times C_6$
36	$C_2 \times C_{18}$	$C_2^2 \times C_9$	36	$D_6 \times C_6$

Continued on next page

Table 2 – continued from previous page

|G|	**G**	**Decomposition**	**|Aut(G)|**	**Aut(G)**
36	C_6^2	$C_2^2 \times C_3^3$	288	$D_6 \times GL_2(\mathbb{F}_3)$
37	C_{37}		36	C_{36}
38	C_{38}	$C_2 \times C_{19}$	18	C_{18}
39	C_{39}	$C_3 \times C_{13}$	24	$C_2 \times C_{12}$
40	C_{40}	$C_5 \times C_8$	16	$C_2^2 \times C_4$
40	$C_2 \times C_{20}$	$C_2 \times C_4 \times C_5$	32	$C_4 \times D_8$
40	$C_2^2 \times C_4$	$C_2^3 \times C_5$	672	$GL_3(\mathbb{F}_2) \times C_4$
41	C_{41}		40	C_{40}
42	C_{42}	$C_2 \times C_3 \times C_7$	12	$C_2 \times C_6$
43	C_{43}		42	C_{42}
44	C_{44}	$C_4 \times C_{11}$	20	$C_2 \times C_{10}$
44	$C_2 \times C_{22}$	$C_2^2 \times C_{11}$	60	$D_6 \times C_{10}$
45	C_{45}	$C_5 \times C_9$	24	$C_4 \times C_6$
45	$C_5 \times C_3^2$		192	$C_4 \times GL_2(\mathbb{F}_3)$
46	C_{46}	$C_2 \times C_{23}$	22	C_{22}
47	C_{47}		46	C_{46}
48	C_{48}	$C_3 \times C_{16}$	16	$C_2^2 \times C_4$
48	$C_2 \times C_{24}$	$C_2 \times C_3 \times C_8$	32	$C_2^2 \times D_8$
48	$C_4 \times C_{12}$	$C_2 \times C_3 \times C_8$	32	$C_2^2 \times D_8$

Table 2: Table of $Aut(G)$ for Small Abelian Groups

3 Automorphisms of Non-Abelian Groups

In this section we look at the automorphisms of some categories of non-abelian groups, including dihedral groups, semidirect products and general linear groups. Some basic techniques and more advanced and recent methods of M.J.Curran [11] (2008) are employed.

Definition [13] $Z(G) = \{g \in G | gx = xg \ \forall x \in G\}$. $Z(G)$ is called the centre of G and is a normal subgroup of G.

Definition [13] Let G be a group and let $g \in G$. Conjugation by g is called an *inner automorphism* of G and the subgroup of $Aut(G)$ consisting of all inner automorphisms is denoted by $Inn(G)$. Also $Inn(G) \simeq G/Z(G)$.

Example 3.1. *The inner automorphism group of Q_8. C_2^2 is a subgroup of $Aut(Q_8)$. Q_8 is generated by the elements -1, i, j and k. Of these elements only -1 commutes with all of the others and so the centre of Q_8 is $< -1 >$ $= \{1, -1\} \simeq C_2$. The inner automorphism group is found by quotienting out the centre of the group. $Q_8/C_2 \simeq C_2^2$. The inner automorphism group of Q_8 $\simeq C_2^2$. $Inn(G)$ is a normal subgroup of $Aut(G)$ and so C_2^2 is a subgroup of $Aut(Q_8)$.*

Example 3.2. *The automorphism group of D_8. Writing D_8 as $\langle x \rangle \times \langle y \rangle$, the elements are $1, x, x^2, x^3, y, xy, x^2y, x^3y$.*
The orders of the elements are as follows:

element	*1*	x	x^2	x^3	y	xy	x^2y	x^3y
order	*1*	*4*	*2*	*4*	*2*	*2*	*2*	*2*

The generator x can be mapped to any of the elements of order 4: x or x^3. This gives 2 automorphisms. In each case the image of x when squared gives x^2, so x^2 will also be mapped to x^2 as these mappings are homomorphisms. Thus the generator y cannot go to x^2, but can only go to the other elements of other 2 which are y, xy, x^2y or x^3y. Thus there are a further 4 automorphisms for each of the earlier 2 giving a possible $2 \times 4 = 8$ automorphisms.

These automorphisms are as follows:

$$\begin{array}{llll} \psi_1(x) = x & \psi_2(x) = x^3 & \psi_3(x) = x & \psi_4(x) = x^3 \\ \psi_1(y) = y & \psi_2(y) = y & \psi_3(y) = xy & \psi_4(y) = xy \end{array}$$

$$\begin{array}{llll} \psi_5(x) = x & \psi_6(x) = x^3 & \psi_7(x) = x & \psi_8(x) = x^3 \\ \psi_5(y) = x^2y & \psi_6(y) = x^2y & \psi_7(y) = x^3y & \psi_8(y) = x^3y \end{array}$$

By labelling the 8 elements of D_8 from 1 to 8, it is possible to describe the mapping of each automorphism by the cycle decomposition on these 8 elements.

Element	*Cycle Decomposition*	*Order*
ψ_1	(1)	*1*
ψ_2	(24)	*2*
ψ_3	(5678)	*4*
ψ_4	(24)(56)(78)	*2*
ψ_5	(57)(68)	*2*
ψ_6	(24)(57)	*2*
ψ_7	(5876)	*4*
ψ_8	(24)(58)(67)	*2*

Each of these cycle decompositions is distinct, and so $|Aut(G)| = 8$. Clearly there are 5 elements of order 2 in $Aut(G)$ and the only group of order 8 with exactly 5 elements of order 2 is D_8. Thus $Aut(D_8) \simeq D_8$.

Example 3.3. *$C_3 \rtimes C_4 = \langle x, y \rangle$ with presentation $\langle x, y | x^3 = y^4 = 1, x^y = x^{-1} \rangle$.*

The elements are: $1, x, x^2, y, y^2, y^3, xy, x^2y, xy^2, x^2y^2, xy^3, x^2y^3$.

The orders of the elements are as follows:

element	*1*	x	x^2	y	y^2	y^3	xy	x^2y	xy^2	x^2y^2	xy^3	x^2y^3
order	*1*	*3*	*3*	*4*	*2*	*4*	*4*	*4*	*6*	*6*	*4*	*4*
label	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*

The generator x can be mapped to any of the elements of order 3: x or x^2. This gives 2 automorphisms. The generator y can be mapped to any of the six elements of order 4. Thus there are a further 6 automorphisms for each of the earlier 2 giving a possible $2 \times 6 = 12$ automorphisms.

These automorphisms are as follows:

$$\begin{array}{llll} \psi_1(x) = x & \psi_2(x) = x & \psi_3(x) = x & \psi_4(x) = x \\ \psi_1(y) = y^3 & \psi_2(y) = x^2y & \psi_3(y) = xy & \psi_4(y) = xy^3 \end{array}$$

$$\begin{array}{llll} \psi_5(x) = x & \psi_6(x) = x & \psi_7(x) = x^2 & \psi_8(x) = x^2 \\ \psi_5(y) = x^2y^3 & \psi_6(y) = y & \psi_7(y) = y^3 & \psi_8(y) = x^2y \end{array}$$

$$\begin{array}{llll} \psi_9(x) = x^2 & \psi_{10}(x) = x^2 & \psi_{11}(x) = x^2 & \psi_{12}(x) = x^2 \\ \psi_9(y) = xy & \psi_{10}(y) = xy^3 & \psi_{11}(y) = x^2y^3 & \psi_{12}(y) = y \end{array}$$

Each of these automorphisms is distinct, and so $|Aut(C_3 \rtimes C_4)| = 12$.

By labelling the 12 elements of $C_3 \rtimes C_4$ from 1 to 12, we can write automorphisms as a cycle decomposition on these 12 elements. Six such automorphisms are as follows:

Element	*Cycle Decomposition*	*Order*
ψ_1	(46)(7.11)(8.12)	*2*
ψ_2	(487)(6.12.11)	*3*
ψ_3	(478)(6.11.12)	*3*
ψ_4	(4.11.8.6.7.12)	*6*
ψ_6	(1)	*1*
ψ_7	(23)(46)(7.12)(8.11)	*2*

The centre of $C_3 \rtimes C_4$ *is the group generated by* y^2 *and so the inner automorphism group is found by quotienting out the centre. This quotient group is* D_6*. Because this is a subgroup of the group of automorphisms,* $Aut(C_3 \rtimes C_4)$ *must be non-abelian.*
Now by process of elimination, we can determine the automorphism group. Since at least one of the elements above has order 6 *the group cannot be* A_4 *(*A_4 *has no subgroup of order 6 [13]).*
Since at least two of the elements above have order 2, it cannot be $C_3 \rtimes C_4$*. This leaves only one non-abelian group of order 12, so* $Aut(C_3 \rtimes C_4) \simeq D_{12}$*.*

Lemma 3.4. *[13] For all* $n \neq 2$*,* $n \neq 6$*, we have* $Aut(S_n) \simeq S_n$*.*

Example 3.5. $D_6 \simeq S_3$*, and so by Lemma 3.4* $Aut(D_6) \simeq D_6$*.*

Lemma 3.6. *[23] For all* $n \neq 2$*,* $n \neq 6$*, we have* $Aut(S_n \times C_2) \simeq S_n \times C_2$*.*

Lemma 3.7. *For* $m < n$*,* $GL_m(\mathbb{F}_q)$ *is isomorphic to a subgroup of* $GL_n(\mathbb{F}_q)$*.*

Proof. Let $A \in GL_m(\mathbb{F}_q)$ and consider the following homomorphism from $GL_m(\mathbb{F}_q)$ into $GL_n(\mathbb{F}_q)$.

$$\Psi(A) = \begin{bmatrix} I_{n-m} & 0 \\ 0 & A \end{bmatrix} \text{ where } I_{n-m} \text{ is the } (n-m)\times(n-m) \text{ identity matrix.}$$

Conjecture 1: If $H < G$, then $Aut(H) < Aut(G)$.

This conjecture is false. The minimum counterexamples are of order 8. They are $C_4 \times C_2$ and D_8.
Here we list the smaller groups and check that the conjecture holds for them:

Note that $H = C_1 < G \ \forall \ G$ and $Aut(C_1) \simeq C_1$ so clearly $Aut(H) < Aut(G)$. Also for $H = C_2$, we have $Aut(C_2) \simeq C_1$ so clearly $Aut(H) < Aut(G)$. Thus we need only look at subgroups bigger than C_2. Similarly, $H = G < G$ and again clearly $Aut(H) < Aut(G)$. Thus we need only look at proper subgroups H where $|H| > 2$ to test the conjecture.

C_4: No proper subgroups of order > 2.

C_2^2: No proper subgroups of order > 2.

C_5 has only trivial subgroups.

C_6: $C_3 < C_6$, and $Aut(C_3) \simeq C_2 < Aut(C_6) \simeq C_2$.

D_6: $C_3 < D_6$, and $Aut(C_3) \simeq C_2 < Aut(D_6) \simeq D_6$.

C_7 has only trivial subgroups.

C_8: $C_4 < C_8$, and $Aut(C_4) \simeq C_2 < Aut(C_8) \simeq C_2^2$.

Q_8: $C_4 < Q_8$, and $Aut(C_4) \simeq C_2 < C_2^2 < Aut(Q_8)$ by Example 3.1.

C_2^3: $C_2^2 < C_2^3$, and $Aut(C_2^2) \simeq GL_2(\mathbb{F}_2) < Aut(C_2^3) \simeq GL_3(\mathbb{F}_2)$ by Lemma 3.7.

Therefore the conjecture holds for all of the above groups. There are two other groups of order 8, and for them we find that:

$Aut(\mathrm{C}_4 \times C_2) \simeq D_8$ by Example 2.3.

$Aut(D_8) \simeq D_8$ by Example 3.2.

Thus both of the groups $C_4 \times C_2$ and D_8 have the same automorphism group (D_8) and both also have C_2^2 as a subgroup. But $Aut(C_2^2) \simeq GL_2(\mathbb{F}_2)$ by Lemma 2.18 and $GL_2(\mathbb{F}_2) \not\simeq D_8$ by Lagrange's Theorem. Therefore the conjecture is false and these are minimum counterexamples.

In his 1943 paper *Possible Groups of Automorphisms* [23], G.A.Miller lists some interesting properties of automorphism groups.

Lemma 3.8. *[23] Let G be a group with no proper subgroup of index 2. Then $Aut(G \times C_2) \simeq Aut(G)$.*

Example 3.9. *A_4 contains no subgroup of order 6 [13]. (In fact, it can be shown that A_4 is the group of smallest possible order not having subgroups of all orders dividing the group order). Thus by 3.8, $Aut(A_4 \times C_2) \simeq Aut(A_4)$.*

Lemma 3.10. *[23] No group has a cyclic group of odd prime power order as its automorphism group. The minimum group which is not the automorphism group of any group is C_3.*

3.1 Semidirect products

Definition *[13] Let p be a prime. If G is a group of order $p^\alpha m$ where $p \nmid m$, then a subgroup of order p^α is called a Sylow $p-$subgroup of G.*

Theorem 3.11. *[13] (Sylow's Theorem) Let G be a group of order $p^\alpha m$ where $p \nmid m$. Then Sylow p-subgroups of G exist. The number of Sylow p-subgroups (n_p) is of the form $1 + kp$, i.e.*

$$n_p \equiv 1 (\mathrm{mod}\ p)$$

Furthermore n_p is the index of the normaliser $N_G(P)$ for any Sylow p-subgroup P, hence

$$n_p \mid m.$$

Definition *[13] A subgroup H of a group G is called characteristic if every automorphism of G maps H to itself.*

Note that one particularly useful property of characteristic subgroups which we make use of here is that if H is the unique subgroup of G of a given order, then H is characteristic in G [13].

Example 3.12. *Taking* $D_{14} = \langle x, y | x^7 = y^2, x^y = x^{-1} \rangle$, *the elements and their orders are as follows:*

1	x	x^2	x^3	x^4	x^5	x^6	y	xy	x^2y	x^3y	x^4y	x^5y	x^6y
1	7	7	7	7	7	7	2	2	2	2	2	2	2

The generator x *can be mapped to any of the 6 elements of order 7, while the generator* y *can be mapped to any of the 7 elements of order 2. This gives 6* $\times$ *7 = 42 automorphisms. What about the structure of* $Aut(D_{14})$*?*

42 has prime decomposition 2.3.7. By Theorem 3.11 there are Sylow 7-subgroups in $Aut(D_{14})$*. The number of them must divide the index of the group which is 6. That is* $n_7|6$ *where* n_7 *is the number of Sylow-7-subgroups. Also* $n_7 \equiv 1(mod\ 7)$*, and so* $n_7 = 1$*.*

C_7 *is normal in* D_{14} *and is the unique subgroup of order 7, so it is characteristic. This means that every automorphism of* D_{14} *maps* C_7 *to itself.*

Theorem 3 in Curran's paper Automorphisms of Semidirect Products [11], deals with groups $G = H \rtimes K$ *(with* H *abelian), and gives a method for finding the group of automorphisms that fix* H*. Because* $H = C_7$ *is characteristic in* D_{14}*, then this method can be applied here and will reveal the structure of* $Aut(D_{14})$*.*

The Theorem says that these automorphisms form a group $B \rtimes E$ *where* $B = \{\begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} : \beta \in CHom(K, Z(H))\}$ *and* $CHom(K, Z(H))$ *are the crossed homomorphisms from* K *into the centre of* H *such that* $\beta(kk') = \beta(k)\beta(k')^k$ *and* $E = \{\begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} : (\alpha, \delta) \in R\}$ *where* $R = \{(\alpha, \delta) \in Aut(H) \times Aut(K) : \alpha(h^k) = \alpha(h)^{\delta(k)}\}$.

Now $\alpha \in Aut(C_7) \Rightarrow \alpha \in C_6$. $\delta \in Aut(C_2) \Rightarrow \delta \in C_1 \Rightarrow \delta = 1$. *Thus* $R = C_6 = E$.

What are the crossed homomorphisms from C_2 *into the centre of* C_7*?*

There are 7 possible mappings for the generator y into C_7. Labelling each map as $f_i : y \mapsto x^i$, we can check whether each map is a crossed homomorphism according to the definition above.

$f_i(y.y) = f_i(y)f_i(y)^{\delta(y)} = f_i(y)f_i(y)^y = x^i.(x^i)^y = x^i.x^{-i} = 1\ \forall i.$ *Thus* $f_i(1) = 1\ \forall i.$

$f_i(y.1) = f_i(y)f_i(1)^{\delta(y)} = f_i(y) = x^i\ \forall i.$

$f_i(1.y) = f_i(y) = x^i.\ f_i(1)f_i(y)^{\delta(1)} = f_i(y) = x^i\ \forall i.$

Thus all 7 maps are crossed homomorphisms according to the definition set out above. That is $|B| = 7 \Rightarrow B{=}C_7 \Rightarrow Aut(D_{14}) \simeq C_7 \rtimes C_6$. *The next step is to define the group action.*

Let $C_7 = \langle a \rangle$ *and let* $C_6 = \langle b \rangle$. *We now find automorphisms of order 7 and 6 (which will serve as generators for the two groups* C_7 *and* C_6 *respectively) and check how the latter conjugates the former.*
We can write each automorphism as a permutation of the elements of D_{14} *using its cycle decomposition. First we number the 14 elements of* D_{14}*:*

1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*
1	x	x^2	x^3	x^4	x^5	x^6	y	xy	x^2y	x^3y	x^4y	x^5y	x^6y

The automorphism which fixes x but sends y to xy has cycle decomposition (8 9 10 11 12 13 14) *and order 7 so we label it a.*
The automorphism which sends x to x^3 *and which sends y to xy has cycle decomposition* (2 4 3 7 5 6)(8 9 12 14 13 10) *and order 6. We label it b.*

$b^{-1} = (6\ 5\ 7\ 3\ 4\ 2)(10\ 13\ 14\ 12\ 9\ 8)$. *Thus* $a^b = bab^{-1} = (8\ 13\ 11\ 9\ 14\ 12\ 10)$.

We can now find the power of a that matches this cycle decomposition.
$a^2 = (8\ 10\ 12\ 14\ 9\ 11\ 13)$
$a^3 = (8\ 11\ 14\ 10\ 13\ 9\ 12)$
$a^4 = (8\ 12\ 9\ 13\ 10\ 14\ 11)$
$a^5 = (8\ 13\ 11\ 9\ 14\ 12\ 10) = a^b$.

So $Aut(D_{14}) \simeq C_7 \rtimes C_6 \simeq \langle a \rangle \rtimes \langle b \rangle$ *with* $a^b = a^5$.

3.2 Automorphisms of Dihedral Groups

The order of the automorphism group of a dihedral group D_{2n} is well known. $|Aut(D_{2n})| = n(\phi(n))$ [13] where $\phi(n)$ is the Euler totient function giving the number of positive integers less than n which are coprime with n.
A dihedral group, when viewed as a group of symmetries of an n-gon, has two generators, a rotation (x) of $2\pi/n$ radians and any reflection (y) through a line joining a vertex and the centre of the n-gon. The rotation x has order n, and altogether there are $\phi(n)$ rotations which have order n and so there are $\phi(n)$ possible images for x under an automorphism. The reflection y has order 2 as do all of the n reflections. The reflection y can be mapped to any of these n reflections. Thus there are $n(\phi(n))$ automorphisms.

Example 3.13. *For* D_{10}*, we have* $n = 5$*.* $\phi(5) = 4$*, and so* $|Aut(D_{10})| = 5(4) = 20$*.*

The structure of the automorphism group of a dihedral group D_{2n} is also well known to be the holomorph of C_n [22].

Definition [1] The *holomorph* of a group G, denoted $Hol\ G$ is the semidirect product $G \rtimes Aut(G)$, with multiplication defined as $(x_1, \sigma_1)(x_2, \sigma_2) = (x_1\sigma_1(x_2), \sigma_1\sigma_2)$ for $x_i \in G$ and $\sigma_i \in Aut(G)$.

Theorem 3.14. *[22]* $Aut(D_{2n}) \simeq Hol\ C_n \simeq C_n \rtimes Aut(C_n)$.

Example 3.15. $Aut(D_6) \simeq C_3 \rtimes Aut(C_3) \simeq C_3 \rtimes C_2 \simeq D_6$.

Example 3.16. $Aut(D_8) \simeq C_4 \rtimes Aut(C_4) \simeq C_4 \rtimes C_2 \simeq D_8$.

Example 3.17. $Aut(D_{10}) \simeq C_5 \rtimes Aut(C_5) \simeq C_5 \rtimes C_4$.
Note that this particular semidirect product is not isomorphic to D_{20}*. In fact it is called the Frobenius Group of order 20 or* F_{20} *and it has presentation* $\langle x, y | x^4 = y^5 = 1, xyx^{-1} = y^2 \rangle$ *[13].*

Definition [1] The group of affine transformations over $\mathbb{Z}/n\mathbb{Z}$ is denoted by $\text{Aff}(\mathbb{Z}/n\mathbb{Z})$ where $\text{Aff}(\mathbb{Z}/n\mathbb{Z}) = \{\theta : x \mapsto ax + b | a, b \in \mathbb{Z}/n\mathbb{Z}, (a, n) = 1\}$.

Another way to view $Aut(D_{2n})$ is as the group of affine transformations over $\mathbb{Z}/n\mathbb{Z}$. The group $Hol\ C_n$ (which is isomorphic to $Aut(D_{2n})$) is isomorphic to $\text{Aff}(\mathbb{Z}/n\mathbb{Z})$ [1].
The structure of $\text{Aff}(\mathbb{Z}/n\mathbb{Z})$ is described in a paper by S.S. Abhyankar [1].
To see that $G = \text{Aff}(\mathbb{Z}/n\mathbb{Z})$ is a group, first take two maps, $T_{a,b} : x \mapsto ax + b$ and $T_{c,d} : x \mapsto cx + d$ and compose them. We get $T_{a,b}T_{c,d} : x \mapsto cax + (cb + d)$, which is in G, since ca is the product of two units and is thus a unit also. Thus G is closed. Composition of maps is associative. Taking $a = 1$ and $b = 0$ gives the identity transformation. The inverse operation is $x \mapsto xa^{-1} - ba^{-1}$ which again is ok because a is a unit in $\mathbb{Z}/n\mathbb{Z}$. Thus G is a group.

The structure of $G = \text{Aff}(\mathbb{Z}/n\mathbb{Z})$ is shown as follows. Let $a, b \in \mathbb{Z}/n\mathbb{Z}$ such that $(a, n) = 1$.
$(\mathbb{Z}/n\mathbb{Z})^+$ is isomorphic to the subgroup $N = \{\omega : x \mapsto 1x + b\}$.
$(\mathbb{Z}/n\mathbb{Z})^\times$ is isomorphic to the subgroup $A = \{\kappa : x \mapsto ax + 0 | (a, n) = 1\}$.
The intersection of these two subgroups is the identity transformation.
The group of affine transformations $\text{Aff}(\mathbb{Z}/n\mathbb{Z})$ is the semidirect product of these two subgroups with N normal in G, that is $G \simeq N \rtimes A$ [1]. In other words, it is the semidirect product of the additive and multiplicative groups of C_n. So we have that $\text{Aff}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^+ \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$.
Note that $N \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ is an abelian group of order $\phi(n)$ and is the automorphism group of C_n by Lemma 2.4. This is the same structure as the holomorph of C_n given above.
Thus we have the following theorem.

Theorem 3.18. *$Aut(D_{2n}) \simeq Hol\ C_n \simeq C_n \rtimes Aut(C_n) \simeq (\mathbb{Z}/n\mathbb{Z})^+ \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$.*

Example 3.19. *Consider D_6. We have $n = 3$. Then $a \in \{1, 2\}$ (i.e. $a \in (\mathbb{Z}/n\mathbb{Z})^\times$) and $b \in \{0, 1, 2\}$ (i.e. $b \in (\mathbb{Z}/n\mathbb{Z})^+$). Then the elements of Aff$(\mathbb{Z}/n\mathbb{Z})$ are the following 6 maps:*

$g_1 : x \mapsto 1x + 0$

$g_2 : x \mapsto 2x + 0$

$g_3 : x \mapsto 1x + 1$

$g_4 : x \mapsto 2x + 1$

$g_5 : x \mapsto 1x + 2$

$g_6 : x \mapsto 2x + 2$

The group operation is composition. Thus $g_6 g_3$*:* $x \mapsto 2(1x + 1) + 2$ *which is* $x \mapsto 2x + 0$ *which is* g_2*.*

Example 3.20. *Consider* D_{12}*. Then Aff*$(\mathbb{Z}/6\mathbb{Z}) = \{x \mapsto ax + b\}$ *where* $a \in \{1, 5\}$ *and* $b \in \{0, 1, 2, 3, 4, 5\}$*. The subgroup N consists of the 6 elements:*

$n_1 : x \mapsto x + 0$

$n_2 : x \mapsto x + 1$

$n_3 : x \mapsto x + 2$

$n_4 : x \mapsto x + 3$

$n_5 : x \mapsto x + 4$

$n_4 : x \mapsto x + 5$

N is abelian and so $N \simeq C_6$*.*

The subgroup A consists of the 2 elements

$a_1 : x \mapsto x + 0$

$a_2 : x \mapsto 2x + 0$

Thus the structure of Aff$(\mathbb{Z}/6\mathbb{Z}) \simeq C_6 \rtimes C_2$*. There is only one semidirect product of these two groups and it is* $Aut(D_{12}) \simeq D_{12}$*.*

Example 3.21. *Consider* D_{10}*. Then Aff*$(\mathbb{Z}/5\mathbb{Z}) = \{x \mapsto ax + b\}$ *where* $a \in \{1, 2, 3, 4\}$ *and* $b \in \{0, 1, 2, 3, 4\}$*. The subgroup* $N \simeq C_5$*. The subgroup A* $\simeq Aut(C_5) \simeq C_4$*. Thus the structure of* $Aut(D_{10}) \simeq C_5 \rtimes C_4$*.*

3.3 Automorphisms of General Linear Groups

In 1951 Dieudonne [12] characterised the automorphisms of general linear groups $GL_n(R)$ where R is a commutative ring with unity. The automorphisms are composites of three types of *standard automorphisms* and are summarised in papers by W.C Waterhouse [31] and B.R. McDonald [20]. Before listing the three types of standard automorphisms, let us recall a couple of definitions from earlier in this Chapter.

Definition [13] $Z(G) = \{g \in G | gx = xg \ \forall x \in G\}$. $Z(G)$ is called the centre of G and is a normal subgroup of G.

Definition [13] Let G be a group and let $g \in G$. Conjugation by g is called an *inner automorphism* of G and the subgroup of $Aut(G)$ consisting of all inner automorphisms is denoted by $Inn(G)$. Also $Inn(G) \simeq G/Z(G)$.

Definition [13] An *outer automorphism* is an automorphism which is not inner. The outer automorphism group, defined $Out(G)$ is isomorphic to $Aut(G)/Inn(G)$. The elements of $Out(G)$ are cosets of $Inn(G)$ in $Aut(G)$.

For general linear groups $GL_n(R)$, the centre consists of the scalar matrices. These scalar matrices are found by multiplying the identity matrix by the units in R. Note that when R is a field $\mathbb{F}_p$ then the order of the centre $|Z(GL_n(\mathbb{F}_p))|$ is $p-1$ as there are $p-1$ invertible elements of the field $\mathbb{F}_p$.

Definition [8] The *projective general linear group* $PGL_n(\mathbb{F}_p)$ is the group obtained from $GL_n(\mathbb{F}_p)$ by factoring out the scalar matrices contained in that group.

In other words, the inner automorphism group of $GL_n(\mathbb{F}_p)$ is $PGL_n(\mathbb{F}_p)$ and $|PGL_n(\mathbb{F}_p)| = \frac{|GL_n(\mathbb{F}_p)|}{p-1}$.

Definition [19] The *special linear group* $SL_n(\mathbb{F}_p)$ is the group of $n \times n$ matrices over $\mathbb{F}_p$ with determinant equal to 1.

Definition Let $A \in GL_n(\mathbb{F}_p)$. The *inverse transpose* maps A to $(A^T)^{-1}$. Note that $(A^T)^{-1} = (A^{-1})^T$.

Now we can list the three types of standard automorphisms of general linear groups.
First there are the *algebraic* automorphisms. These are the inner automorphisms (conjugation by an element of $GL_n(R)$) as well as the inverse transpose.
Secondly, there are automorphisms of the ring R which are applied to the entries of the matrix.
Finally, there are the radial automorphisms which map a matrix A to $\lambda(A)A$ where $\lambda(A)$ is some scalar (depending on the matrix A). The existence of these radial automorphisms depends on the prime p. An example of a radial automorphism is $det(A)A$.

Lemma 3.22. *[24] The inverse transpose map is an inner automorphism on the special linear group $SL_2(\mathbb{F}_p)$ and equals conjugation by the matrix* $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$.
For $n \geq 3$, or for $n = 2$ and $p \geq 3$, the inverse transpose map is an outer automorphism of the general linear group $GL_n(\mathbb{F}_p)$.

Lemma 3.23. *[31] The inverse transpose is an involution (a function that is its own inverse) and has order 2. When the inverse transpose is an outer automorphism, the group of algebraic automorphisms of $GL_n(R)$ is the semidirect product of the inner automorphism group and the outer automorphism group of order 2 consisting of the inverse transpose. When the inverse transpose is an inner automorphism, the group of algebraic automorphisms of $GL_n(R)$ is simply $Inn(GL_n(R))$.*

Example 3.24. *Let $G \simeq GL_2(\mathbb{F}_2)$. We look at the three standard automorphism types in turn.*
Firstly, $Inn(G) \simeq GL_2(\mathbb{F}_2)$ as the center is trivial. Also $n = 2$ but $p = 2$, and so $GL_2(\mathbb{F}_2) \simeq SL_2(\mathbb{F}_2)$ and so by Lemma 3.22 the inverse transpose map

is an inner automorphism. Thus the algebraic automorphisms consists only of the inner automorphisms, so the group of algebraic automorphisms is isomorphic to $GL_2(\mathbb{F}_2)$.
Secondly, $\mathbb{F}_2$ *has only the trivial field automorphism so there is nothing extra here.*
Finally, radial automorphisms are multiples of the matrix by a scalar, and $\mathbb{F}_2$ *only admits one non-zero scalar multiple, which is the trivial automorphism. So there are no extra radial automorphisms.*
Note that $GL_2(\mathbb{F}_2) \simeq D_6 \simeq S_3$ *and we already established that* $Aut(S_3) \simeq S_3$ *in Example 3.5.*
In conclusion, $Aut(GL_2(\mathbb{F}_2)) \simeq GL_2(\mathbb{F}_2)$.

Example 3.25. *Let* $G \simeq GL_3(\mathbb{F}_2)$.
Firstly, $Inn(G) \simeq GL_3(\mathbb{F}_2)$ *as the center is trivial. Because* $n > 2$, *the inverse transpose gives an outer automorphism by Lemma 3.22. Thus the group of algebraic automorphisms is* $GL_3(\mathbb{F}_2) \rtimes C_2$ *by Lemma 3.23.*
Secondly, $\mathbb{F}_2$ *has only the trivial field automorphism.*
Thirdly, there are no extra radial outer automorphisms as in the previous example.
By GAP [14] we confirm that $Aut(GL_3(\mathbb{F}_2)) \simeq GL_3(\mathbb{F}_2) \rtimes C_2$.

Example 3.26. *Let* $G \simeq GL_2(\mathbb{F}_3)$. *Let the elements of* $\mathbb{F}_3$ *be* $0, 1, 2$ *where 2 = -1.*
Firstly, $Inn(G) \simeq PGL_2(\mathbb{F}_3) \simeq S_4$ *[14] which is a subgroup of* G *of index 2 as the centre of* G *consists of two elements (the scalar multiples of the identity matrix by 1 and 2). Because* $n = 2$ *and* $p = 3$, *the inverse transpose gives an outer automorphism by Lemma 3.22.*
$\mathbb{F}_3$ *has only the trivial field automorphism.*
There is a radial automorphism for this group and it is the automorphism which maps A to det(A)A.
By GAP [14] we note that $Aut(GL_2(\mathbb{F}_3)) \simeq S_4 \times C_2$. *It is a direct product because the action of the inverse transpose on* S_4 *is trivial. The radial outer automorphism sends each matrix either to itself or to its negative (so that it*

stays in the same coset of the center, and therefore induces the same map by conjugation). It fixes the subgroup $SL_2(\mathbb{F}_3)$ pointwise, and sends all the elements in the other coset of $SL_2(\mathbb{F}_3)$ to their negatives. This isn't the same as the transpose-inverse. But it is in the same outer automorphism class. It can be obtained by composing the transpose-inverse with the inner automorphism consisting of conjugation by the matrix

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

We now examine this composition in more detail.

Let f be the radial outer automorphism. So $f : A \mapsto det(A)A$.

Let t be the inverse transpose. That is $t : A \mapsto (A^T)^{-1}$.

Let g be conjugation by B. That is $g : A \mapsto BAB^{-1}$.

Now, let A be the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

Then $t(A) = (A^T)^{-1} = [det(A)]^{-1} \begin{bmatrix} d & -c \\ -b & a \end{bmatrix}$.

$$g(t(A)) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} [det(A)]^{-1} \begin{bmatrix} d & -c \\ -b & a \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

$$= [det(A)]^{-1} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} d & -c \\ -b & a \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

$$= [det(A)]^{-1} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} c & d \\ -a & -b \end{bmatrix}$$

$$= [det(A)]^{-1} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = f(A) \text{ as defined above.}$$

Note that $[det(A)]^{-1} = det(A)$ in $\mathbb{F}_3$.

Thus the outer radial automorphism $f : A \mapsto det(A)A$ is the composition of conjugation by B with the inverse transpose. The inverse transpose generates the outer automorphism group of order 2 which acts on the inner automorphism group as a direct product. By GAP [14] we note that $Aut(GL_2(\mathbb{F}_3)) \simeq S_4 \times C_2$.

3.4 Automorphism Groups of Automorphism Groups

It is natural to ask what is the automomorphism group of the automorphism group of a group G?

Definition $Aut^nG = Aut(Aut^{n-1}G)$ where $Aut^0G = G$. Listing Aut^2G, Aut^3G, and so on gives a sequence of automorphism groups, known as an *automorphism tower*.

Definition An automorphism tower is said to *terminate* when $Aut^kG = Aut^{k-1}G$ for some positive integer k. We will call the smallest such k the height of the automorphism tower.

Conjecture. Aut^nG terminates at C_1 for all cyclic groups. This conjecture is false. C_8 is the minimum counterexample. It converges to $GL_2(F_2)$.

Another natural question to ask is whether the automorphism tower terminates for all groups G?
H. Wielandt (1939) [33] proved that the automorphism tower of any centerless finite group terminates in finitely many steps. Simon Thomas (1985) [30] proved that the automorphism tower of any centerless group eventually terminates. In 1998, J.D.Hamkins [15] proved that every group has a terminating transfinite automorphism tower.

In the table which follows, we show the automorphism tower for a number of small abelian groups. In completing this table, we make use of some of the results from this Chapter as well as the computer algebra system GAP [14].
$Aut(D_6) \simeq D_6$ by Lemma 3.4.
$Aut(D_8) \simeq D_8$ by Example 3.2.
$Aut(Q_8) \simeq S_4$ [2].
$Aut(S_4) \simeq S_4$ by Lemma 3.4.
$Aut(D_{10}) \simeq F_{20}$ by Example 3.17.
$Aut(F_{20}) \simeq F_{20}$ by GAP [14].
$Aut(C_3 \rtimes C_4) \simeq D_{12}$ by Example 3.3.

$Aut(D_{12}) \simeq D_{12}$ by Example 3.20.
$Aut(A_4) \simeq S_4$ [2].
$Aut(GL_3(\mathbb{F}_2)) \simeq GL_3(\mathbb{F}_2) \rtimes C_2$ by Example 3.25.
$Aut(GL_3(\mathbb{F}_2) \rtimes C_2) \simeq GL_3(\mathbb{F}_2) \rtimes C_2$ by GAP [14].
$Aut(GL_2(\mathbb{F}_3)) \simeq S_4 \times C_2$ by Example 3.26.
$Aut(S_4 \times C_2) \simeq S_4 \times C_2$ by Lemma 3.6.
$Aut(D_{14}) \simeq C_7 \rtimes C_6$ by Example 3.12.
$Aut(C_7 \rtimes C_6) \simeq C_7 \rtimes C_6$ by GAP [14].

3.5 Automorphism Tower for Small Groups

G	AutG	$\mathbf{Aut^2G}$	$\mathbf{Aut^3G}$	$\mathbf{Aut^4G}$
C_1	C_1	C_1	C_1	C_1
C_2	C_1	C_1	C_1	C_1
C_3	C_2	C_1	C_1	C_1
C_4	C_2	C_1	C_1	C_1
C_2^2	$GL_2(\mathbb{F}_2) \simeq D_6$	D_6	D_6	D_6
C_5	C_4	C_2	C_1	C_1
C_6	C_2	C_1	C_1	C_1
D_6	D_6	D_6	D_6	D_6
C_7	C_6	C_2	C_1	C_1
C_8	C_2^2	$GL_2(\mathbb{F}_2) \simeq D_6$	D_6	D_6
$C_2 \times C_4$	D_8	D_8	D_8	D_8
D_8	D_8	D_8	D_8	D_8
Q_8	S_4	S_4	S_4	S_4
C_2^3	$GL_3(\mathbb{F}_2)$	$GL_3(\mathbb{F}_2) \rtimes C_2$	$GL_3(\mathbb{F}_2) \rtimes C_2$	$GL_3(\mathbb{F}_2) \rtimes C_2$
C_9	C_6	C_2	C_1	C_1
C_3^2	$GL_2(\mathbb{F}_3)$	$C_2 \times S_4$	$C_2 \times S_4$	$C_2 \times S_4$
C_{10}	C_4	C_2	C_1	C_1
D_{10}	F_{20}	F_{20}	F_{20}	F_{20}
C_{11}	C_{10}	C_4	C_2	C_1
C_{12}	C_2^2	$GL_2(\mathbb{F}_2) \simeq D_6$	D_6	D_6
$C_2 \times C_6$	D_{12}	D_{12}	D_{12}	D_{12}
D_{12}	D_{12}	D_{12}	D_{12}	D_{12}
$C_3 \rtimes C_4$	D_{12}	D_{12}	D_{12}	D_{12}
A_4	S_4	S_4	S_4	S_4
C_{13}	C_{12}	C_2^2	$GL_2(\mathbb{F}_2) \simeq D_6$	D_6
C_{14}	C_6	C_2	C_1	C_1
D_{14}	$C_7 \rtimes C_6$	$C_7 \rtimes C_6$	$C_7 \rtimes C_6$	$C_7 \rtimes C_6$

4 Finite Commutative Group Algebras

Definition Fix a field F and let $G = \{g_1, g_2, ..., g_n\}$ be any finite abelian group with group operation written multiplicatively. Then the *group algebra* FG is the set of all linear combinations of group elements with coefficients in F. FG can be considered as the vector space with basis G over the field F.

Elements of FG are of the form: $a_1g_1 + a_2g_2 + ... + a_ng_n$, where $a_i \in F$, $1 \leq i \leq n$.

If g_1 is the identity of G, then a_1g_1 is sometimes written as a_1. Similarly, $1g$ is sometimes written as g.
Addition is performed componentwise. Multiplication is performed as follows: $(ag_i)(bg_j) = (ab)g_k$, where the product ab is taken in F, and the product $g_ig_j = g_k$ is taken in G.

These operations make FG a ring. This type of ring is called a group ring. Moreover, if F is a finite field, FG is called a finite group algebra.

Lemma 4.1. *Let R be a ring of order m and G a group of order n. Then RG is a group ring of order $|R|^{|G|}$.*

Proof. Let $RG = \{\sum_{g \in G} a_g | a_g \in R\}$.
For each g, there are m elements of R, so there are $\underbrace{m.m \ldots m}_{|G| = \text{n}}$ elements in RG. So $m^n = |R|^{|G|}$.

4.1 The Unit Group of FG

In this section, group algebras formed by a finite field and an abelian group are examined. For each group algebra, the Artin-Wedderburn decomposition is found where applicable. The unit group is also found.

At the end of this section a table is presented detailing these results. We start with a detailed look at some of the smaller group algebras to get an illustration of the method used to decompose and find the unit group.

Definition The units of a group algebra are the invertible elements. These units form a group called $U(FG)$ under multiplication.

Lemma 4.2. *For finite G and finite F, $|G| \leq |U(FG)| < |FG|$.*
Also $|G|$ divides $|U(FG)|$.

Proof. The elements of the group are all units so $|G| \leq |U(FG)|$ and by Lagrange's Theorem $|G|$ divides $|U(FG)|$. The units must be elements of FG, so $|U(FG)| \leq |FG|$. Also $0 \in FG$ but $0 \notin |U(FG)|$ so $|U(FG)| < |FG|$.

The task of finding $U(FG)$ is greatly simplified if FG can be decomposed as a direct sum of matrix rings over division rings. The following two theorems are used throughout this section. Note that FG is a ring, so both theorems apply to group algebras.

Definition [28] A ring R is *semisimple* if it can be decomposed as a direct sum of finitely many minimal left ideals, i.e. $R = L_1 \oplus L_2 \oplus ... \oplus L_t$ where L_i is a minimal left ideal. Note that L is a minimal left ideal of R if L is a left ideal of R and if J is any other left ideal of R contained in L, then either $J = \{0\}$ or $J = L$.

Theorem 4.3. *[28] (Artin-Wedderburn Theorem) 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. $R \simeq M_{n_1}(D_1) \oplus M_{n_2}(D_2) \oplus ..... \oplus M_{n_s}(D_s)$ 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.*

This decomposition is unique [28] and is known as the Artin-Wedderburn decomposition or the Wedderburn decomposition.

Definition [10] Let R be a ring. If n is the smallest positive integer such that $nr = 0 \; \forall \; r \in R$ then n is called the characteristic of R, and $char(R) = n$. If no such n exists, then $char(R) = 0$.

Theorem 4.4. *[28] (Maschke's Theorem) 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 4.5. *[10] Let G be a finite group and F a field. Then FG is semisimple if and only if $char(F) \nmid |G|$. Note that any field F is semisimple ($F = M_1(F)$) and if $|G|$ is not a multiple of $char(F)$ then $|G|$ is invertible in F.*

Definition [13] Let R be a ring. An element $e \in R$ is called an *idempotent* if $e^2 = e$.

Definition [26] For a ring containing an idempotent e, there exist left, right and two-sided *Peirce decompositions*, which are defined by $R = Re \oplus R(1-e)$, $R = eR \oplus (1-e)R$, and $R = eRe \oplus eR(1-e) \oplus (1-e)Re \oplus (1-e)R(1-e)$ respectively.

There is also a Peirce decomposition with respect to an orthogonal system of idempotents $\{e_1, e_2, ..., e_n\}$ where $e_1 + ... + e_n = 1$ and $e_i e_j = 0$ for $i \neq j$, which is defined by $R = \bigoplus_{i,j} e_i R e_j$ for $1 \leq i, j \leq n$.

Definition [28] Given a group ring RG and a finite subset X of the group G, $\hat{X}$ is defined as the following element in RG

$$\hat{X} = \sum_{x \in X} x.$$

Lemma 4.6. *[10] Let G be a finite group and R a commutative ring such that $char(R) \nmid |G|$. Then $e_G = |G|^{-1}\hat{G}$ is a central idempotent in RG.*

Proof. $e_G^2 = |G|^{-1}\hat{G}|G|^{-1}\hat{G}$
$= |G|^{-2}\sum_{i=1}^{n} g_i\hat{G}$ where $|G| = n$
$= |G|^{-2}\sum_{i=1}^{n} \hat{G} = |G|^{-2}n\hat{G} = |G|^{-2}|G|\hat{G} = |G|^{-1}\hat{G} = e_G$.

It can be shown that e_G is central in RG by showing that it commutes with all elements of G as elements of R are central in the group ring. We check how g conjugates e_G.

$e_G^g = ge_Gg^{-1} = g|G|^{-1}\hat{G}g^{-1} = |G|^{-1}g(g_1 + g_2 + ... + g_n)g^{-1}$
$= |G|^{-1}(g_1 + g_2 + ... + g_n) = e_G$.
Thus e_G commutes with all elements of G, and is central in RG.

Corollary 4.7. *Let G be a finite group with $H \lhd G$ and let R be a commutative ring such that char(R) does not divide $|H|$. Then $e_H = |H|^{-1}\hat{H}$ is a central idempotent in FG.*

Proof. By the previous lemma, $e_H^2 = e_H$. It can be shown that e_H is central in R by showing that it commutes with all elements of G as elements of R are central in the group ring. We check how g conjugates e_H. Note that because H is normal in G that ghg^{-1} is an element of H. The map ψ_g (where $\psi_g(h) = ghg^{-1}$) is an inner automorphism of H and so it permutes the elements of H. Thus we get the following:

$e_H^g = ge_Hg^{-1} = g|H|^{-1}\hat{H}g^{-1} = |H|^{-1}g(h_1 + h_2 + ... + h_n)g^{-1} = |H|^{-1}(h_1 + h_2 + ... + h_n) = e_H$.
Thus e_H commutes with all elements of G, and is central in RG.

Definition [28] The ring homomorphism ϵ:$RG \to R$ given by $\epsilon(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g$ is called the augmentation mapping of RG and its kernel, denoted by $\triangle(G)$ is called the augmentation ideal of RG.

Lemma 4.8. $|\triangle(G)| = |RG|/|R|$.

Proof. ϵ is a ring homomorphism from RG onto R
Then by the first isomorphism theorem for rings, $RG/ker(\epsilon) \simeq R$
$\Rightarrow |RG|/|ker(\epsilon)| = |R| \Rightarrow |RG|/|R| = |ker(\epsilon)| \Rightarrow |RG|/|R| = |\triangle(G)|$.

Definition [28] Let X be a subset of a group ring RG. The left annihilator of X is the set

$$Ann_l(X) = \{\alpha \in RG | \alpha x = 0, \forall x \in X\}.$$

Similarly, the right annihilator is defined as

$$Ann_r(X) = \{\alpha \in RG | x\alpha = 0, \forall x \in X\}.$$

Definition For a subgroup $H < G$, denote by $\triangle(G, H)$ the left ideal of RG generated by the set $\{h - 1 : h \in H\}$. That is,

$$\triangle(G, H) = \left\{ \sum_{h \in H} \alpha_h (h - 1) : \alpha_h \in RG \right\}.$$

Definition [28] Given an element $\alpha = \sum_{g \in G} a_g g$ we define the *support* of α to be $supp(\alpha) = \{g \in G : a_g \neq 0\}$.

Lemma 4.9. *[28] Let H be a subgroup of a group G and let R be a commutative ring. Then $Ann_l(\triangle(G, H)) \neq 0$ if and only if H is finite. In this case, we have*

$$Ann_l(\triangle(G, H)) = RG.\hat{H}.$$

Furthermore, if $H \triangleleft G$, then the element $\hat{H}$ is central in RG and we have

$$Ann_l(\triangle(G, H)) = Ann_r(\triangle(G, H)) = \hat{H}.RG$$

Proof. Assume that $Ann_l(\triangle(G, H)) \neq 0$ and choose $\alpha = \sum_{g \in G} a_g g \neq 0$ in $Ann_l(\triangle(G, H))$. For each element $h \in H$ we have that $\alpha(h - 1) = 0$, hence $\alpha h = \alpha$. That is,

$$\alpha = \sum_{g \in G} a_g g = \sum_{g \in G} a_g gh.$$

Take $g_0 \in supp(\alpha)$. Then $\alpha_{g_0} \neq 0$, so the equation above shows that $g_0 h \in supp(\alpha)$ for all $h \in H$. Since $supp(\alpha)$ is finite, then H must be finite.
Now for $g_0 \in supp(\alpha)$ then the coefficient of every element of the form $g_0 h$ is equal to the coefficient of g_0 and so we can write

$$\alpha = a_{g_0} g_0 \hat{H} + a_{g_1} g_1 \hat{H} + ... + a_{g_t} g_t \hat{H} = \beta \hat{H},\ \beta \in RG.$$

This shows that, if H is finite, then $Ann_l(\triangle(G,H)) \subseteq RG.\hat{H}$. The reverse inclusion follows trivially, since $\hat{H}h = \hat{H}$ implies that $\hat{H}(h-1) = 0$ for all $h \in H$. Thus $Ann_l(\triangle(G,H)) = RG.\hat{H}$.
If $H \lhd G$, then by Corollary 4.7, the element e_H is central in RG, and so $\hat{H}$ is central in RG and so $RG.\hat{H} = \hat{H}.RG$ and the result follows.

Corollary 4.10. *Let G be a finite group. Then*

$$Ann_l(\triangle(G)) = RG.\hat{G} = R\hat{G}.$$

Proof. This is a consequence of taking $H = G$ in the above Lemma.

Definition [28] Let R be a ring. An abelian group M (written additively) is called a (left) $R-module$ if for each element $a \in R$ and each $m \in M$ we have a product $am \in M$ such that:

(i) $(a+b)m = am + ab$,

(ii) $a(m_1 + m_2) = am_1 + am_2$,

(iii) $a(bm) = (ab)m$,

(iv) $1m = m$,

for all $a, b \in R$ and $m, m_1, m_2 \in M$.

Definition [28] Let M be an $R-module$. A nonempty subset $N \subset M$ is called a $R-submodule$ of M if the following conditions hold:

(i) For all $x, y \in N$ we have $x + y \in M$.

(ii) For all $r \in R$ and all $n \in N$, we have that $rn \in N$.

A nonzero module which contains no proper submodules is called *simple*.

Example 4.11. *Let L be a (left) ideal of a group algebra FG. Since the (left) product of elements of FG by elements of L is in L, it follows that L can be regarded as a (left) $FG-module$.*

Theorem 4.12. *[28] Let $R = L_1 \oplus L_2 \oplus ... \oplus L_t$ be a decomposition of a semisimple ring R as a direct sum of minimal left ideals. Then every simple $R-module$ is isomorphic to one of the ideals L_i in the given decomposition.*

Lemma 4.13. *[10] Let F be a field and let $H \lhd G$. If $|H|$ is invertible in F then we have $FG \simeq FGe_H \oplus FG(1-e_H)$ where $FGe_H \simeq F(G/H)$ and $FG(1-e_H) \simeq \triangle(G,H)$.*

Corollary 4.14. *Let G be a finite group and F a field such that $char(F)$ does not divide $|G|$. Then $FG \simeq F \oplus \triangle(G)$. Also, F appears at least once in the Wedderburn decomposition.*

Proof. By taking $H = G$ in the above Lemma, we get $FG \simeq F(G/G) \oplus \triangle(G,G)$ and so $FG \simeq F \oplus \triangle(G)$. Thus F appears at least once in a decomposition of FG where $char(F)$ does not divide $|G|$.
But we have seen that when $char(F)$ does not divide $|G|$, that there is an Artin-Wedderburn decomposition. Thus $FG \simeq F \oplus \triangle(G) \simeq L_1 \oplus L_2 \oplus ... \oplus L_t$ where L_i is a minimal left ideal.
By Theorem 4.12, every simple $FG-module$ is isomorphic to one of the ideals L_i in the given decomposition. We now show that F is a simple $FG-module$. First of all, $F \simeq FGe_G$ and so is the principal ideal generated by the element e_G. As in Example 4.11 each ideal of FG is an $FG-module$ and so F is an $FG-module$. We now show that it is simple.
Assume that $M \subset F$ and that M is an $FG-submodule$ of F and that $M \neq \{0\}$. All of the non-zero elements of F are invertible in F and so M contains an invertible element of F. Let $a \in M$ be such an invertible element. Then $1 = a^{-1}a \in M$. Then $x.1 \in M \; \forall \; x \in F$, and so $M = F$. Thus F has no proper $FG-submodules$ and so F is a simple $FG-module$ and is isomorphic to one of the ideals L_i in the decomposition $L_1 \oplus L_2 \oplus ... \oplus L_t$ by Theorem 4.12. That is, the field F appears at least once in the Wedderburn decomposition.

Example 4.15. $\mathbb{F}_2C_2 = \{0, 1, x, 1+x\}$. $|\mathbb{F}_2C_2| = 2^2 = 4$. $|C_2| = 2$.
By Lemma 4.2, 2 divides $|U|$ and $|U| < 4$, so $|U| = 2$. Thus $U = \{1, x\} \simeq C_2$.
There is no Artin-Wedderburn decomposition by Corollary 4.5.

Lemma 4.16. $\mathbb{F}_2C_3 \simeq \mathbb{F}_2 \oplus \mathbb{F}_{2^2}$.

Proof. G is finite. $char(F) = 2$, $|G| = 3$ and $2 \not| 3$ so Maschke's Theorem applies.
By Corollary 4.14, $\mathbb{F}_2$ appears at least once as a summand in the decomposition, so there are two possible decompositions, $\mathbb{F}_2 \oplus \mathbb{F}_2 \oplus \mathbb{F}_2$ and $\mathbb{F}_2 \oplus \mathbb{F}_{2^2}$.
If $\mathbb{F}_2C_3 \simeq \mathbb{F}_2 \oplus \mathbb{F}_2 \oplus \mathbb{F}_2$, then $U(\mathbb{F}_2 \oplus \mathbb{F}_2 \oplus \mathbb{F}_2) \simeq C_1 \times C_1 \times C_1 \simeq C_1$ which is not possible because C_3 must be a subgroup of the unit group.
Thus $\mathbb{F}_2C_3 \simeq \mathbb{F}_2 \oplus \mathbb{F}_{2^2}$. $U(\mathbb{F}_2 \oplus \mathbb{F}_{2^2}) \simeq C_1 \times C_3 \simeq C_3$.

Definition The subgroup of units of augmentation 1 in $U(RG)$ is called $V(RG)$ or just V.
That is $V(RG) = \{u \in U(RG) | \epsilon(u) = 1\}$.

Lemma 4.17. *[28]* $U(FG) = V \times F^{\times}$

Lemma 4.18. $U(\mathbb{F}_3C_3) = C_3^2 \times C_2$.

Proof. $|\mathbb{F}_3C_3| = 3^3 = 27$. $|C_3| = 3$.
By working out which of the elements of augmentation 1 are units, the order and structure of V and hence of U will be determined. The elements of augmentation 1 are $\{1, x, x^2, 2 + 2x, 2 + 2x^2, 2x + 2x^2, 1 + x + 2x^2, 1 + 2x + x^2, 2 + x + x^2\}$.
Clearly, $\{1, x, x^2\}$ are all units.
$(2 + 2x)^2 = (2 + 2x)(2 + 2x) = 4 + 4x + 4x + 4x^2 = 1 + 2x + x^2 \Rightarrow$
$(2+2x)^3 = (1 + 2x + x^2)(2 + 2x) = 2 + 2x + 4x + 4x^2 + 2x^2 + 2(1) = 1$.
Thus $(2 + 2x)$ is a unit of order 3 and its inverse $(1 + 2x + x^2)$ is also a unit.
$(2 + 2x^2)^2 = (2 + 2x^2)(2 + 2x^2) = 4 + 4x^2 + 4x^2 + 4x^4 = 1 + 2x^2 + x \Rightarrow$
$(2+2x^2)^3 = (1 + 2x^2 + x)(2 + 2x^2) = 2 + 2x^2 + 2x + 2(1) + 4x^2 + 4x = 1$.
Thus $(2 + 2x^2)$ is a unit of order 3 and its inverse $(1 + 2x^2 + x)$ is also a unit.
$(2x + 2x^2)^2 = (2x + 2x^2)(2x + 2x^2) = 4x^2 + 4(1) + 4(1) + 4x = x^2 + 2 + x \Rightarrow$
$(2x+2x^2)^3 = (x^2 + 2 + x)(2x + 2x^2) = 4x + 4x^2 + 2x^2 + 2(1) + 2(1) + 2x = 1$.
Thus $(2x + 2x^2)$ is a unit of order 3 and its inverse $(x^2 + 2 + x)$ is also a unit.
Thus all 9 elements of augmentation 1 are units and so $|V| = 9$. There are two possible abelian groups of order 9, C_9 and C_3^2.

C_9 has exactly two elements of order 3. However, we have shown that V has 8 elements of order 3, so $V \not\simeq C_9$ and thus $V \simeq C_3^2$.
So $U \simeq C_3^2 \times C_2$, $|U| = 18$ and $Aut(U) \simeq GL_2(\mathbb{F}_3)$ by Lemma 2.18.
Finally, $\mathbb{F}_3C_3$ does not decompose by Corollary 4.5.

Example 4.19. $\mathbb{F}_2C_5$. *$|FG| = 2^5 = 32$.*
$|G| = 5$, $char(F) = 2$ and $2 \not| 5$ so Maschke's Theorem applies.
By Corollary 4.14, $\mathbb{F}_2$ appears at least once as a summand in the decomposition.
Thus the possible decompositions are $\mathbb{F}_2 \oplus \mathbb{F}_{2^4}$, $\mathbb{F}_2 \oplus \mathbb{F}_2 \oplus \mathbb{F}_{2^3}$, $\mathbb{F}_2 \oplus \mathbb{F}_2 \oplus \mathbb{F}_2 \oplus \mathbb{F}_{2^2}$, $\mathbb{F}_2 \oplus \mathbb{F}_{2^2} \oplus \mathbb{F}_{2^2}$, $\mathbb{F}_2 \oplus \mathbb{F}_2 \oplus \mathbb{F}_2 \oplus \mathbb{F}_2 \oplus \mathbb{F}_2$, or $\mathbb{F}_2 \oplus M_2(\mathbb{F}_2)$.
The unit groups of these decompositions have orders 15, 7, 3, 9, 1 and 6 respectively, but since C_5 must be a subgroup of the unit group, the only possible decomposition is the first one, $\mathbb{F}_2 \oplus \mathbb{F}_{2^4}$.
Thus $U(F_2C_5) \simeq C_{15} \simeq C_3 \times C_5$. $Aut(U) \simeq C_2 \times C_4$ by Lemma 2.1.

Lemma 4.20. $U(\mathbb{F}_{2^2}C_2) \simeq C_2^2 \times C_3$.

Proof. To form a field with p^n elements, it is necessary to find an irreducible polynomial $p(x)$ of degree n, with coefficients in $\mathbb{F}_p$. Then $\mathbb{F}_{p^n} \simeq \mathbb{F}_p[x]/\langle p(x)\rangle$.
Thus to form $\mathbb{F}_{2^2}$ we need to find an irreducible polynomial $p(x)$ of degree 2 over $\mathbb{F}_2$, that is, a polynomial of degree 2 without any roots in $\mathbb{F}_2$.
The possible polynomials are $p_1(x) = x^2$, $p_2(x) = 1 + x^2$, $p_3(x) = x + x^2$ and $p_4(x) = 1 + x + x^2$.
However $p_1(0) = 0$, $p_2(1) = 0$, $p_3(0) = 0$ and so these are not irreducible. In contrast, there are no roots of $p_4(x)$ in $\mathbb{F}_2$, i.e. no solutions of $1 + x + x^2 = 0$ in $\mathbb{F}_2$, so it is irreducible. We will call this polynomial $p(x)$.

Now $p(x)$ has a root in the field extension $\mathbb{F}_2[x]/\langle p(x)\rangle$. Let a be this root. Then $1 + a + a^2 = 0 \Rightarrow a^2 = -1 - a \Rightarrow a^2 = 1 + a$. Thus every polynomial in $\mathbb{F}_2[x]/\langle p(x)\rangle$ is a polynomial of degree at most 1.
The 4 polynomials, $\{0, 1, a, 1 + a\}$ are the elements of $\mathbb{F}_{2^2}$.

Looking at $\mathbb{F}_{2^2}C_2$ and labelling the elements of C_2 as $\{1, y\}$, the 16 elements of the groupring $\mathbb{F}_{2^2}C_2$ can be written as $\{0, y, ay, y + ay, 1, 1 + y, 1 +$

$ay, 1+y+ay, a, a+y, a+ay, a+y+ay, 1+a, 1+a+ay, 1+a+y+ay\}$.
$U \simeq V \times F^{\times}$ where V is the group of units of augmentation 1. The elements of augmentation 1 are $\{1, y, a+y+ay, 1+a+ay\}$.

Clearly both 1 and y are units as they are elements of C_2.
$(a+y+ay)^2 = a^2+y^2+a^2y^2 = (1+a)+1+(1+a)1 = 1$ and so $a+y+ay$ is a unit of order 2.
$(1+a+ay)^2 = 1^2+a^2+a^2y^2 = 1+(1+a)+(1+a)1 = 1$ so $1+a+ay$ is also a unit of order 2.

Thus V has 4 elements with at least two of order 2, so V $\simeq C_2^2$.
$U \simeq V \times F^{\times} \Rightarrow U \simeq C_2^2 \times C_3$. $|U| = 12$.

$Aut(U) \simeq Aut(C_2^2) \times Aut(C_3) \simeq D_6 \times C_2 \simeq D_{12}$. $|Aut(U)| = 12$.

Lemma 4.21. *[10] Let R be a commutative ring and let G, H be groups. Then $R(G \times H) \simeq (RG)H$ (the group ring of H over the ring RG).*

Proof. Let $f : (RG)H \to R(G\times H)$ be defined by $\sum_{h\in H}(\sum_{g\in G} a_{gh}g)h \mapsto \sum_{gh\in GH} a_{gh}gh$.
We show that this is a ring homomorphism.

Let $\alpha = \sum_{h\in H}(\sum_{g\in G} a_{gh}g)h$ and $\beta = \sum_{h\in H}(\sum_{g\in G} b_{gh}g)h \in (RG)H$.

Then $f(\alpha) + f(\beta) = \sum_{gh\in GH} a_{gh}gh + \sum_{gh\in GH} b_{gh}gh = \sum_{gh\in GH}(a_{gh} + b_{gh})gh$.

$\alpha + \beta = \sum_{h\in H}(\sum_{g\in G} a_{gh}g)h + \sum_{h\in H}(\sum_{g\in G} b_{gh}g)h = \sum_{h\in H}(\sum_{g\in G}(a_{gh} + b_{gh})g)h$.

Thus $f(\alpha+\beta)= \sum_{gh\in GH}(a_{gh} + b_{gh})gh = f(\alpha)+f(\beta)$.

$$\begin{aligned}
\alpha\beta &= \sum_{h_1\in H}(\sum_{g\in G} a_{gh_1}g)h_1 \sum_{h_2\in H}(\sum_{g\in G} b_{gh_2}g)h_2 = \sum_{h_1,h_2\in H}(\sum_{g\in G} a_{gh_1}g)(\sum_{g\in G} b_{gh_2}g)h_1h_2 \\
&= \sum_{v\in H}[\sum_{h_1h_2=v}(\sum_{g\in G} a_{gh_1}g)(\sum_{g\in G} b_{gh_2}g)]v = \sum_{v\in H}[\sum_{h_1h_2=v}(\sum_{g_1,g_2\in G} a_{g_1h_1}b_{g_2h_2}g_1g_2)]v \\
&= \sum_{v\in H}[\sum_{h_1h_2=v}(\sum_{u\in G}\sum_{g_1g_2=u} a_{g_1h_1}b_{g_2h_2}u)]v \\
&= \sum_{v\in H}[\sum_{u\in G}(\sum_{h_1h_2=v}\sum_{g_1g_2=u} a_{g_1h_1}b_{g_2h_2}u)]v.
\end{aligned}$$

Thus $f(\alpha\beta)= \sum_{uv\in GH}[\sum_{g_1g_2h_1h_2=uv} a_{g_1h_1}b_{g_2h_2}]uv$.

$$\begin{aligned}
\text{Now } f(\alpha)f(\beta) &= \sum_{gh\in GH} a_{gh}gh \sum_{gh\in GH} b_{gh}gh = \sum_{g_1h_1,g_2h_2\in GH} a_{g_1h_1}b_{g_2h_2}g_1h_1g_2h_2 \\
&= \sum_{k\in GH}[\sum_{g_1h_1g_2h_2=k} a_{g_1h_1}b_{g_2h_2}]k
\end{aligned}$$

Because G commutes with H, $k = g_1h_1g_2h_2 = g_1g_2h_1h_2 = uv$ and so $f(\alpha\beta)$=f(α)$f(\beta)$.
Thus f is a ring homomorphism. In fact f is a monomorphism, because if $f(\alpha) = 0$, then $\sum_{gh\in GH} a_{gh}gh = 0 \Rightarrow a_{gh} = 0 \ \forall\ gh \in GH \Rightarrow \alpha = 0$.
Also f is an epimorphism, because for $\gamma \in R(G\times H)$, $\gamma = \sum_{gh\in GH} a_{gh}gh$, there is an element $\alpha = \sum_{h\in H}(\sum_{g\in G} a_{gh}g)h \in RG(H)$ such that $f(\alpha) = \gamma$.
Thus f is an isomorphism, and $R(G \times H) \simeq (RG)H$.

Lemma 4.22. *[10] Let $\{R_i\}_{i\in I}$ be a family of rings and let $R = \bigoplus_{i\in I} R_i$. Then, for any group G, $RG \simeq (\bigoplus_{i\in I} R_i)G \simeq \bigoplus_{i\in I}(R_iG)$ as rings.*

Proof. Let $f : RG \to \bigoplus_{i\in I}(R_iG)$ be defined by $\sum\limits_{g\in G} a_g g \mapsto \sum\limits_{i\in I}\sum\limits_{g\in G} a_{ig}g$, where $a_g \in R$ and $a_{ig} \in R_i$. Let $\alpha = \sum\limits_{g\in G} a_g g$ and $\beta = \sum\limits_{g\in G} b_g g \in RG$.

Then $\alpha + \beta = \sum\limits_{g\in G} a_g g + \sum\limits_{g\in G} b_g g = \sum\limits_{g\in G}(a_g + b_g)g$.

So $f(\alpha + \beta) = \sum\limits_{i\in I}\sum\limits_{g\in G}(a_{ig} + b_{ig})g$.

Now $f(\alpha) = \sum\limits_{i\in I}\sum\limits_{g\in G} a_{ig}g$ and $f(\beta) = \sum\limits_{i\in I}\sum\limits_{g\in G} b_{ig}g$.

So $f(\alpha) + f(\beta) = \sum\limits_{i\in I}[\sum\limits_{g\in G} a_{ig} + \sum\limits_{g\in G} b_{ig}]g = \sum\limits_{i\in I}\sum\limits_{g\in G}(a_{ig} + b_{ig})g = f(\alpha + \beta)$.

$\alpha\beta = \sum\limits_{g\in G} a_g g \sum\limits_{g\in G} b_g g = \sum\limits_{g_1,g_2\in G} a_{g_1}b_{g_2}g_1g_2 = \sum\limits_{u\in G} c_u u$ where $c_u = \sum\limits_{g_1g_2=u} a_{g_1}b_{g_2}$.

Thus $\alpha\beta = \sum\limits_{u\in G}\sum\limits_{g_1g_2=u} a_{g_1}b_{g_2}$u.

f$(\alpha\beta) = \sum\limits_{i\in I}\sum\limits_{u\in G}[\sum\limits_{g_1g_2=u} a_{ig_1}b_{ig_2}]$u.

f$(\alpha)f(\beta) = \sum\limits_{i\in I}\sum\limits_{g\in G} a_{ig}g \sum\limits_{i\in I}\sum\limits_{g\in G} b_{ig}g$

Because multiplication is done componentwise over the summands R_i,

$$f(\alpha)f(\beta) = \sum_{i\in I}(\sum_{g\in G} a_{ig}g \sum_{g\in G} b_{ig}g) = \sum_{i\in I}(\sum_{g_1,g_2\in G} a_{ig_1}b_{ig_2}g_1g_2)$$

$$= \sum_{i\in I}(\sum_{v\in G} c_v v) \text{ (where } c_v = \sum_{g_1g_2=v} a_{ig_1}b_{ig_2}) = \sum_{i\in I}\sum_{v\in G}[\sum_{g_1g_2=v} a_{ig_1}b_{ig_2}]v$$

But $u = g_1g_2 = v \Rightarrow f(\alpha)f(\beta) = f(\alpha\beta)$ so f is a ring homormorphism.

f is a monomorphism, because if $f(\alpha) = 0$, then $\sum\limits_{i\in I}\sum\limits_{g\in G} a_{ig}g = 0 \Rightarrow a_{ig}g = 0\ \forall\ g \in G \Rightarrow a_{ig} = 0 \Rightarrow \alpha = 0$. f is an epimorphism, because for all $\gamma \in \bigoplus_{i\in I}(R_iG)$, $\gamma = \sum\limits_{i\in I}\sum\limits_{g\in G} a_{ig}g$, there is an element $\alpha = \sum\limits_{g\in G} a_g g \in RG$ such that $f(\alpha) = \gamma$. Thus f is an isomorphism, and $RG \simeq \bigoplus_{i\in I}(R_iG)$.

Example 4.23. $\mathbb{F}_2C_6$. $2|6$ *so Maschke's Theorem does not apply.*
However, by Lemma 4.21, $\mathbb{F}_2C_6 \simeq \mathbb{F}_2(C_3 \times C_2) \simeq (\mathbb{F}_2C_3)C_2 \simeq (\mathbb{F}_2 \oplus \mathbb{F}_{2^2})C_2$.
By Lemma 4.22, $(\mathbb{F}_2 \oplus \mathbb{F}_{2^2})C_2 \simeq \mathbb{F}_2C_2 \oplus \mathbb{F}_{2^2}C_2$.
Thus $U(\mathbb{F}_2C_6) \simeq U(\mathbb{F}_2C_2) \times U(\mathbb{F}_{2^2}C_2)$. *By Lemma 4.20* $U(\mathbb{F}_{2^2}C_2) \simeq C_2^2 \times C_3$, *so* $U(\mathbb{F}_2C_6) \simeq C_2 \times C_2^2 \times C_3 \simeq C_2^3 \times C_3$.
$|U| = 24$. *From direct calculations, it can be shown that the 24 elements of*

the unit group and their orders are:

element	*order*
1	*1*
x	*6*
x^2	*3*
x^3	*2*
x^4	*3*
x^5	*6*
$1+x^3+x^5$	*6*
$x+x^2+x^5$	*6*
$1+x+x^4$	*2*
$1+x^2+x^3$	*6*
$x+x^3+x^4$	*2*
$x^2+x^4+x^5$	*6*
$1+x^2+x^5$	*2*
$1+x+x^3$	*6*
$x+x^2+x^4$	*6*
$x^2+x^3+x^5$	*2*
$1+x^3+x^4$	*6*
$x+x^4+x^5$	*6*
$1+x+x^2+x^3+x^4$	*6*
$1+x+x^2+x^3+x^5$	*6*
$1+x+x^2+x^4+x^5$	*2*
$1+x+x^3+x^4+x^5$	*6*
$1+x^2+x^3+x^4+x^5$	*6*
$x+x^2+x^3+x^4+x^5$	*2*

$Aut(U) = Aut(C_2^3) \times Aut(C_3) \simeq GL_3(\mathbb{F}_2) \times C_2$. Hence $|Aut(U)| = 336$.

Lemma 4.24. *For $p \neq 2$, $\mathbb{F}_{p^k}C_2 \simeq \bigoplus_{i=1}^{2} \mathbb{F}_{p^k}$. The unit group of $\mathbb{F}_{p^k}C_2 \simeq C_{p^k-1}^2$.*

Proof. $p \nmid 2$ so Maschke's Theorem applies, and $\mathbb{F}_{p^k}$ must appear as a sum-

mand at least once in the Artin-Wedderburn decomposition.
Thus $\mathbb{F}_{p^k}C_2 \simeq \mathbb{F}_{p^k} \oplus \mathbb{F}_{p^k}$, because the group algebra has dimension 2.
It follows that the unit group is isomorphic to $C_{p^k-1} \times C_{p^k-1}$.

Lemma 4.25. *For $p \neq 2$, $\mathbb{F}_{p^k}C_2^n \simeq \bigoplus_{i=1}^{2^n} \mathbb{F}_{p^k}$. The unit group of $\mathbb{F}_{p^k}C_2^n \simeq C_{p^k-1}^{2^n}$.*

Proof. We proceed by induction. By Lemma 4.24 $\mathbb{F}_{p^k}C_2^1 \simeq \bigoplus_{i=1}^{2^1} \mathbb{F}_{p^k}$ so it is true for $n = 1$.
Assume that it is true for $n = m$. That is $\mathbb{F}_{p^k}C_2^m \simeq \bigoplus_{i=1}^{2^m} \mathbb{F}_{p^k}$.
Now we test for $n = m + 1$.

$\mathbb{F}_{p^k}C_2^{m+1} \simeq \mathbb{F}_{p^k}(C_2^m \times C_2) \simeq (\mathbb{F}_{p^k}C_2^m)C_2$ (by Lemma 4.21)
$\simeq (\bigoplus_{i=1}^{2^m} \mathbb{F}_{p^k})C_2 \simeq \bigoplus_{i=1}^{2^m} \mathbb{F}_{p^k}C_2$ (by Lemma 4.22)
$\simeq \bigoplus_{i=1}^{2^m} \bigoplus_{j=1}^{2} \mathbb{F}_{p^k} \simeq \bigoplus_{i=1}^{2^{m+1}} \mathbb{F}_{p^k}$.

It follows that the unit group is $C_{p^k-1}^{2^n}$.

Example 4.26. $\mathbb{F}_{17}C_2 \simeq \mathbb{F}_{17} \oplus \mathbb{F}_{17}$ *and* $U(\mathbb{F}_{17}C_2) \simeq C_{16}^2$.

Example 4.27. $\mathbb{F}_{3^2}C_2 \simeq \mathbb{F}_{3^2} \oplus \mathbb{F}_{3^2}$ *and* $U(\mathbb{F}_{3^2}C_2) \simeq C_8^2$.

Example 4.28. $\mathbb{F}_{3^4}C_2^3 \simeq \bigoplus_{i=1}^{2^3} F_{3^4} \simeq \bigoplus_{i=1}^{8} F_{3^4}$ *and* $U(\mathbb{F}_{3^4}C_2^3) \simeq C_{80}^8$.

Lemma 4.29. *[28] For a finite group algebra FG with $m \in F$, the number of elements of augmentation m is equal to $|F|^{|G|-1}$.*

Proof. Let ϵ be the usual augmentation map. Let $|F| = p^k$.
Let $A_m = \{\alpha \in FG | \epsilon(\alpha) = m\}$. and $A_{m+1} = \{\beta \in FG | \epsilon(\beta) = m + 1\}$.
Consider the map $f : A_m \to A_{m+1}$ defined by $f(\alpha) \mapsto \alpha + 1$. Clearly f is bijective. Thus A_m and A_{m+1} have the same order.

The map f can be applied to each A_m in turn and we will have $|A_0| = |A_1|$ = ... = $|A_{p^k-1}|$ so all the sets have the same order.
Thus the sets A_m partition the group algebra. Since there are p^k of them, the order of each set is $\frac{|F|^{|G|}}{|F|} = |F|^{|G|-1}$.

Lemma 4.30. *For a group algebra FG,* $|U| \leq |F|^{|G|}$ - $|F|^{|G|-1}$.
That is $|U| \leq |F|^{|G|-1}(|F|-1)$.

Proof. By Lemma 4.29 $|\triangle G| = |F|^{|G|-1}$ and these elements are all annihilated by $\hat{G}$, so that none of the elements of $\triangle G$ are units and thus $|U| \leq |F|^{|G|}$ - $|F|^{|G|-1}$.

Lemma 4.31. *[9]* $U(\mathbb{F}_{p^k}C_p^n) \simeq C_p^{k(p^n-1)} \times C_{p^k-1}$.

Example 4.32. *[9]* $U(\mathbb{F}_{2^2}C_2^2) \simeq C_2^{2(2^2-1)} \times C_{2^2-1} \simeq C_2^6 \times C_3$ *by Lemma 4.31.*

Example 4.33. *[9]* $U(\mathbb{F}_3C_3^2) \simeq C_3^{1(3^2-1)} \times C_{3^1-1} \simeq C_3^5 \times C_2$ *by Lemma 4.31.*

Example 4.34. $U(\mathbb{F}_{2^4}C_2) \simeq C_2^{4(2^1-1)} \times C_{2^4-1} \simeq C_2^4 \times C_{15}$. $|U| = 16.15 = 240$.
Note that $|\mathbb{F}_{2^4}C_2| = 256$. *Since* $|\triangle(G)| = 16$, *all of the elements of the group algebra are units except for the elements of* $\triangle(G)$.

Theorem 4.35. *Every element of a field of order q satisfies* $a^q = a$.

Proof. The non-zero elements in a field of order q form a group of order $q-1$ under multiplication, so by Lagrange's Theorem, $a^{q-1} = 1$ for any non-zero a in the field. Then $a^q = a$. But $0^q = 0$ also so it holds for all of the elements of the field.

Lemma 4.36. *For a group algebra* $\mathbb{F}_{2^k}C_p$ *with p a Mersenne prime such that* $p = (2^k)^n - 1$ *for some* $n \in \mathbb{Z}$, $U(\mathbb{F}_{2^k}C_p) \simeq C_p^m$ *for some* $m \in \mathbb{Z}$.

Proof. Let $\alpha = (a_1x^1 + a_2x^2 + ... + a_px^p) \in \mathbb{F}_{2^k}C_p$ with $a_i \in \mathbb{F}_{2^k}$.
Then $(\alpha)^{2^{kn}} = [(a_1x^1)^{2^{kn}} + (a_2x^2)^{2^{kn}} + ... + (a_px^p)^{2^{kn}}]$
$= [a_1^{2^{kn}}(x^1)^{2^{kn}} + a_2^{2^{kn}}(x^2)^{2^{kn}} + ... + a_p^{2^{kn}}(x^p)^{2^{kn}}]$

By Theorem 4.35, every element of a field of order p^k satisfies $a^{p^k} = a$. As a direct consequence we get $a^{2^{kn}} = \underbrace{((((a^{2^k})^{2^k})^{2^k}).....)^{2^k}}_{n \text{ times}} = a$.
Also, as $p = (2^k)^n - 1$, then $(x^i)^{2^{kn}-1} = 1$ because all non identity elements of the group have order $p = (2^k)^n - 1$. Thus $(x^i)^{2^{kn}} = x^i \ \forall \ i$.

Thus $[a_1^{2^{kn}}(x^1)^{2^{kn}} + a_2^{2^{kn}}(x^2)^{2^{kn}} + ... + a_p^{2^{kn}}(x^p)^{2^{kn}}] = (a_1x^1 + a_2x^2 + ... + a_px^p)$.
In other words we have $(\alpha)^{2^{kn}} = \alpha$.

This means that α is either a zero divisor, or is a unit of order dividing $(2^k)^n - 1$. Thus all units have order dividing p and as p is a prime, all non identity elements of the unit group have order p and so the unit group must be elementary abelian of structure C_p^m for some $m \in \mathbb{Z}$.

Example 4.37. *[9] In $\mathbb{F}_2C_3$ we have $2^2 - 1 = 3$.*
Thus by Lemma 4.36, $U(\mathbb{F}_2C_3) \simeq C_3^m$ and in fact must be C_3 because C_3^m with $m \geq 2$ has too many elements.

Example 4.38. *[9] In $\mathbb{F}_2C_7$ we have $2^3 - 1 = 7$.*
Thus by Lemma 4.36, $U(\mathbb{F}_2C_7) \simeq C_7^m$. By Lemma 4.30 $|U| \leq 64$, and so by order considerations $m = 1$ or $m = 2$.
If $m = 1$ then the only elements of order 7 are the group elements. One other element is $(1+x+x^2)$ which has inverse $(1+x^2+x^3+x^5+x^6)$. Thus $m = 2$, and $U(\mathbb{F}_2C_7) \simeq C_7^2$.

Lemma 4.39. *For a group algebra $\mathbb{F}_{p^k}C_m$ with $m \in \mathbb{N}$ such that $m|(p^k)^n - 1$ for some $n \in \mathbb{Z}$, then $U(\mathbb{F}_{p^k}C_m)$ is an abelian group of exponent m.*

Proof. Let $\alpha = (a_1x^1 + a_2x^2 + ... + a_mx^m)$ with $a_i \in \mathbb{F}_{p^k}$.
Then $(\alpha)^{p^{kn}} = [(a_1x^1)^{p^{kn}} + (a_2x^2)^{p^{kn}} + ... + (a_px^p)^{2^{kn}}] = [a_1^{p^{kn}}(x^1)^{p^{kn}} + a_2^{p^{kn}}(x^2)^{p^{kn}} + ... + a_m^{p^{kn}}(x^m)^{p^{kn}}]$.
By Theorem 4.35, every element of a field of order p^k satisfies $a^{p^k} = a$ and so $a^{p^{kn}} = \underbrace{((((a^{p^k})^{p^k})^{p^k}).....)^{p^k}}_{n\ times} = a$.
Because $m|(p^k)^n - 1$, then $(x^i)^{p^{kn}-1} = 1$ as all elements of the group have order dividing $(p^k)^n - 1$. Thus $(x^i)^{p^{kn}} = x^i \ \forall\ i$.
Thus $[a_1^{p^{kn}}(x^1)^{p^{kn}} + a_2^{p^{kn}}(x^2)^{p^{kn}} + ... + a_m^{p^{kn}}(x^m)^{p^{kn}}] = (a_1x^1 + a_2x^2 + ... + a_mx^m)$.
In other words we have $(\alpha)^{p^{kn}} = \alpha$.

Thus α is either a zero divisor, or is a unit of order dividing $(p^k)^n - 1 = m$. Thus all units have order dividing m. Furthermore, because C_m is contained

in the unit group, there is at least one element of order m and so the exponent of the unit group is m. Finally, the unit group must be abelian because the group algebra is commutative.

Example 4.40. *In $\mathbb{F}_3C_8$ we have $3^2 - 1 = 8$. By Lemma 4.39, $U(\mathbb{F}_3C_8)$ must have exponent 8.*
This greatly reduces the number of possible Artin-Wedderburn decompositions.
Clearly $\mathbb{F}_3$ is a summand by Corollary 4.14.
Also $\mathbb{F}_{3^2}$ is a possible summand because the unit group is C_8 which has exponent 8.
However, because the unit group of a field of order p^k is cyclic of order $p^k - 1$ such a cyclic group would contain at least one element of order $p^k - 1$. Thus all summands of the form $\mathbb{F}_{3^m}$ with $m \geq 3$ can be ruled out since the unit groups of such summands would necessarily contain elements with order greater than 8. Thus the only possible summands are $\mathbb{F}_3$ and $\mathbb{F}_{3^2}$.
This means that the only possible decompositions of $\mathbb{F}_3C_8$ are $\bigoplus_{i=1}^{6} \mathbb{F}_3 \oplus \mathbb{F}_{3^2}$ or $\bigoplus_{i=1}^{4} \mathbb{F}_3 \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{3^2}$ or $\bigoplus_{i=1}^{2} \mathbb{F}_3 \oplus \bigoplus_{i=1}^{3} \mathbb{F}_{3^2}$.

Definition For a group ring RG define $\{\triangle(G)+1\}$ to be the set of elements of augmentation 1.

Lemma 4.41. *The set $\{\triangle(G)+1\}$ forms a semigroup under multiplication.*

Proof. We check the 3 semigroup axioms.
(1) The multiplicative identity $1 \in \{\triangle(G)+1\}$.
(2) Let α, $\beta \in \{\triangle(G)+1\}$. Then $\epsilon(\alpha) = \epsilon(\beta) = 1$. As ϵ is a ring homomorphism, then $\epsilon(\alpha\beta) = \epsilon(\alpha).\epsilon(\beta) = 1.1 = 1$, and so $\{\triangle(G)+1\}$ is closed under multiplication.
(3) The set $\{\triangle(G)+1\}$ inherits associativity from the ring RG.
Thus $\{\triangle(G)+1\}$ is a semigroup.

Corollary 4.42. *The set $\{\triangle(G)+1\}$ forms a group under multiplication if and only if the set $\{\triangle(G)+1\}$ contains only invertible elements.*

Proof. Let $\{\triangle(G)+1\}$ contain only invertible elements and let $\alpha \in \{\triangle(G)+1\}$.
Then $\epsilon(\alpha\alpha^{-1}) = \epsilon(1) = 1 = \epsilon(\alpha).\epsilon(\alpha^{-1}) = 1.\epsilon(\alpha^{-1}) \Rightarrow \epsilon(\alpha^{-1}) = 1$. Thus $\{\triangle(G)+1\}$ is closed under inverses and so forms a group.

If $\{\triangle(G)+1\}$ contains a non-invertible element, then clearly $\{\triangle(G)+1\}$ does not form a group.

There are many group rings which contain non-invertible elements of augmentation 1, for example $\mathbb{F}_2C_3$.

Example 4.43. *[9]* $\mathbb{F}_2C_3$. *Let* $\mathbb{F}_2 = \{0,1\}$ *and* $C_3 = \{1, x, x^2\}$. *There are 4 elements of aumentation 1,* $\{1, x, x^2, 1+x+x^2\}$. *The element* $1+x+x^2 = \hat{G}$ *annihilates all elements of* $\triangle(G)$ *and so is a zero divisor and therefore not invertible. Thus* $\{\triangle(G)+1\}$ *is not a group within* $\mathbb{F}_2C_3$.

Lemma 4.44. $\mathbb{F}_2C_3$ *is the smallest group ring which contains a non-invertible element of augmentation 1.*

Proof. We check all possible smaller group rings.
In any group ring of the form $\mathbb{F}_{p^k}C_1$ there is only one element of augmentation 1, the group element 1, which clearly forms a group.
In $\mathbb{F}_2C_2$ there are two elements of augmentation 1, the two elements of C_2, which clearly form a group.

Example 4.45. *[9]* $\mathbb{F}_3C_5$. *This is a 5 dimensional vector space over* $\mathbb{F}_3$. *3 does not divide 5 so Maschke's Theorem applies and* $\mathbb{F}_3$ *must appear as a summand in the decomposition.* $U(\mathbb{F}_3) = C_2$ *but* C_2 *does not contain* C_5, *so there must be a different summand in the decomposition.*
$U(\mathbb{F}_{3^2}) = C_8$ *which does not contain* C_5.
$U(\mathbb{F}_{3^3}) = C_{26}$ *which does not contain* C_5.
It cannot be $M_2(\mathbb{F}_3)$ *as that would give a non-commutative group algebra.*
The only remaining possible summand is $\mathbb{F}_{3^4}$ *and its unit group is* C_{80} *which contains* C_5.
So the decomposition must be $\mathbb{F}_3 \oplus \mathbb{F}_{3^4}$ *which gives the 5 dimensions.*

The unit group is therefore $C_2 \times C_{80}$.

There are $3^5 = 243$ *elements in the group algebra. Thus there are* 243 - 160 = 83 *elements which are not units. There are 81 elements in* $\triangle(G)$*, 80 of which are zero divisors (as they are annihilated by* $\hat{G}$*) and the element zero. Thus there are two more zero divisors which do not have augmentation 0. These two elements are* $\hat{G} = (1+x+x^2+x^3+x^4)$ *and* $2\hat{G} = (2+2x+2x^2+2x^3+2x^4)$ *which have augmentation 2 and 1 respectively.*

Example 4.46. $\mathbb{F}_7C_3$. *This is a 3 dimensional vector space over* $\mathbb{F}_7$*. 7 does not divide 3 so Maschke's Theorem applies and* $\mathbb{F}_7$ *must appear as a summand in the decomposition. Thus the only possible decompositions are* $\bigoplus_{i=1}^{3} \mathbb{F}_7$ *or* $\mathbb{F}_7 \oplus \mathbb{F}_{7^2}$*. Checking whether the unit group of such decompositions could contain* C_3 *we see that both could.* $U(\bigoplus_{i=1}^{3} \mathbb{F}_7) = C_6^3$ *and* $U(\mathbb{F}_7 \oplus \mathbb{F}_{7^2}) = C_6 \times C_{48}$.

Now $U \simeq V \times F^\times$*, so for the first decomposition we have* $V \simeq C_6^2$ *and for the second decomposition we have* $V \simeq C_{48}$*. There are 49 elements of augmentation 1, so if there are at least two zero divisors in this set, then* $|V| < 48$*. The obvious candidates for these zero divisors are multiples of* $\hat{G} = 1 + x + x^2$ *which have augmentation 1. Now* $|G| = 3$*, and* $3^{-1} = 5$ *in* $F^\times$*. Consider* $5 + 5x + 5x^2 \in \{\triangle(G) + 1\}$.
$(5 + 5x + 5x^2)(1 + 6x) = 5 + 5x + 5x^2 + 30x + 30x^2 + 30 = 35 + 35x + 35x^2 = 0$.
Also $(1 + 3x + 4x^2) \in \{\triangle(G) + 1\}$ *and* $(1 + 3x + 4x^2)(1 + 2x + 4x^2) = 1 + 2x + 4x^2 + 3x + 6x^2 + 12 + 4x^2 + 8 + 16x = 21 + 21x + 14x^2 = 0$.
Thus there are at least 2 zero divisors of augmentation 1 and so $|V| < 48$ *and so* $V \simeq C_6^2$*. Thus the decomposition is* $\bigoplus_{i=1}^{3} \mathbb{F}_7$ *and the unit group is* C_6^3.

Example 4.47. *[9]* $\mathbb{F}_3C_4$*. Maschke's Theorem applies so* $\mathbb{F}_3$ *is a summand. However, the decomposition cannot be* $\bigoplus_{i=1}^{4} \mathbb{F}_3$ *as* C_4 *is not a subgroup of* $U(\mathbb{F}_3) = C_2$*. Also* $\mathbb{F}_{3^3}$ *cannot be the only other summand as* C_4 *is not a subgroup of* $U(\mathbb{F}_{3^3}) = C_{26}$.

Thus $\mathbb{F}_{3^2}$ must be a summand and so the decomposition is $\bigoplus_{i=1}^{2}\mathbb{F}_3 \oplus \mathbb{F}_{3^2}$. The unit group is therefore $C_2^2 \times C_8$.

Example 4.48. *[9] $\mathbb{F}_3C_6$. Maschke's theorem does not apply. However, Lemma 4.21 does and so we have $\mathbb{F}_3C_6 \simeq \mathbb{F}_3(C_2 \times C_3) \simeq (\mathbb{F}_3C_2)C_3 \simeq (\bigoplus_{i=1}^{2}\mathbb{F}_3)C_3$.*
By Lemma 4.22, $(\bigoplus_{i=1}^{2}\mathbb{F}_3)C_3 \simeq \mathbb{F}_3C_3 \oplus \mathbb{F}_3C_3$.
The unit group of $\mathbb{F}_3C_3$ is $C_3^2 \times C_2$ by Lemma 4.18 $\Rightarrow U(\mathbb{F}_3C_6) \simeq C_3^4 \times C_2^2$.
$Aut(U) = GL_4(\mathbb{F}_3) \times GL_2(\mathbb{F}_2)$.

Example 4.49. *$\mathbb{F}_3C_7$. Maschke's Theorem applies so $\mathbb{F}_3$ is a summand. However, the decomposition cannot be $\bigoplus_{i=1}^{7}\mathbb{F}_3$ as C_7 is not a subgroup of $U(\mathbb{F}_3) = C_2$. $\mathbb{F}_{3^2}$ cannot be the only other summand as C_7 is not a subgroup of $U(\mathbb{F}_{3^2}) = C_8$. Also $\mathbb{F}_{3^3}$ cannot be the only other summand as C_7 is not a subgroup of $U(\mathbb{F}_{3^3}) = C_{26}$. Similarly $\mathbb{F}_{3^4}$ cannot be the only other summand as C_7 is not a subgroup of $U(\mathbb{F}_{3^4}) = C_{80}$. By the same rationale $\mathbb{F}_{3^5}$ cannot be the only other summand as C_7 is not a subgroup of $U(\mathbb{F}_{3^5}) = C_{242}$.*
$\mathbb{F}_{3^6}$ must be a summand as C_7 can be a subgroup of $U(\mathbb{F}_{3^6}) = C_{728}$.
Thus the decomposition is $\mathbb{F}_3 \oplus \mathbb{F}_{3^6}$. The unit group is therefore $C_2 \times C_{728}$.

We now give a brief example of a non-commutative group algebra, where the group is non-abelian, and find the unit group by determining which elements are zero-divisors, which are units and the order of the units.

Example 4.50. *$\mathbb{F}_2D_6$. Let $D_6 = \{1, x, x^2, xy, x^2y, y\}$.*
Maschke does not apply. $|\mathbb{F}_2D_6| = 2^6 = 64$.

$D_6 < U(FG) \Rightarrow$ 6 divides $|U(FG)|$.

The 32 elements of $\triangle(G)$ are annihilated by $\hat{G}$, so the possible order of the unit group is 6, 12, 18, 24 or 30.

D_6 is a subgroup of U so U is non-abelian.

Also $U \simeq V \times F^{\times} \simeq V \times C_1 \Rightarrow V \simeq U$.

The 32 elements of augmentation 1 are as follows:

$1, x, x^2, xy, x^2y, y$ *(the 6 group elements).*

$1+x+x^2, 1+x+xy, 1+x+x^2y, 1+x+y, x+x^2+xy, x+x^2+x^2y, 1+x^2+xy, 1+x^2+x^2y, 1+x^2+y, 1+xy+x^2y, 1+xy+y, 1+x^2y+y, x+x^2+y, x+xy+x^2y, x+xy+y, x+x^2y+y, x^2+xy+x^2y, x^2+xy+y, x^2+x^2y+y, xy+x^2y+y$ *(20 trinomials).*

$1+x+x^2+y+xy, 1+x+x^2+y+x^2y, 1+x+x^2+xy+x^2, 1+x+y+xy+x^2y, 1+x^2+y+xy+x^2y, x+x^2+y+xy+x^2y$ *(6 5-nomials).*

Clearly the 6 group elements are all units. However, of the other 26 elements, it can be shown that the 20 trinomials are all zerodivisors. That leaves 12 elements. That leaves the 6 5-nomials. Are these 5-nomials units?

By multipying them by themselves it can be shown that they are in fact units with the following orders.

$1+x+x^2+y+xy$ *has order 2*

$1+x+x^2+y+x^2y$ *has order 2*

$1+x+x^2+xy+x^2$ *has order 2*

$1+x+y+xy+x^2y$ *has order 6*

$1+x^2+y+xy+x^2y$ *has order 6*

$x+x^2+y+xy+x^2y$ *has order 2.*

Thus there are 12 elements in the unit group, 2 elements of order 6, 2 elements of order 3, 7 elements of order 2 and the identity.
The only non-abelian groups of order 12 are A_4 and D_{12}. However A_4 doesn't have any elements of order 6.
Thus $U(\mathbb{F}_2D_6) \simeq D_{12}$.
Presenting D_{12} as $< a, b, c | a^3 = b^2 = c^2 = 1, a^b = a^{-1}, a^c = a, b^c = b >$, we can give an isomorphism between the two groups.

ω*:* $U(\mathbb{F}_2D_6) \to D_{12}$, ω*:*$x \mapsto a$

ω*:*$y \mapsto b$, ω*:*$1+x+y+xy+x^2y \mapsto ac$.

5 $U(FG)$ where F has char p and G is an abelian $p-group$

This Chapter begins with a look at the elements of V - the group of normalised units. Throughout the various examples and lemmas of the Chapter, a method is developed for finding the structure of V by counting the number of elements of V which divide different powers of p. The method is made more general and thus more useful as the Chapter progresses. The conclusion of the Chapter is a Theorem which gives the structure of V whenever F has characteristic p and G is an abelian $p-group$.

Lemma 5.1. *Let p be a prime. Let G be a direct product of n groups G_i, and let m_i be the number of elements x_i such that $(x_i)^{p^k} = 1$ (i.e elements of order dividing p^k) in G_i for $0 \leq i \leq n$. Then the number of elements of order dividing p^k in G is $\prod_{i=1}^{n} m_i$.*

Proof. Let $G' \simeq G_1 \times G_2$. There are m_1 elements of order dividing p^k in G_1 and m_2 elements of order dividing p^k in G_2. For each of the elements of order dividing p^k in G_1, we can form a new element of order dividing p^k in G by multiplying it by an element of order dividing p^k in G_2, and there are m_2 ways of doing this. Because there are m_1 elements of order dividing p^k in G_1, then there are $(m_1)(m_2)$ ways of getting an element of order dividing p^k in G'.

Now by iterating this process, and getting the direct sum of $G' \times G_3$, we see that the final number of elements of order dividing p^k in $G = \prod_{i=1}^{n} m_i$.

Lemma 5.2. *For $G = C_{p^m}$, there are p^k elements of order dividing p^k for $k \leq m$.*

Proof. Let $\phi(g) = g^{p^k} \ \forall \ g \in G$.

In a cyclic group C_{p^m}, the element $g^{p^{m-k}}$ has order dividing p^k and so do all of the elements of the subgroup generated by $g^{p^{m-k}}$, i.e. $\langle g^{p^{m-k}} \rangle$.

In fact this subgroup is the kernel of the homomorphism ϕ. To see this, let $g^i \in ker(\phi)$. Then $(g^i)^{p^k} = 1$. That is $g^{ip^k} = 1$. That is ip^k is a multiple

of p^m (the order of the group). That is i is a multiple of p^{m-k}. Thus the subgroup generated by $g^{p^{m-k}}$ is the kernel of the homomorphism.

As the generator of this kernel is of order p^k, then this group has p^k elements.

Firstly, we begin by asking when is the subgroup V equal to the set of elements of augmentation 1?

Lemma 5.3. *Let G be an abelian group. Then $V(\mathbb{F}_{p^k}G) = \{\triangle(G)+1\}$ if and only if G is a $p-$ group (i.e. a group of order p^α with $\alpha \geq 0$). Morevover, the exponent of V equals the exponent of G in this instance.*

Proof. Let the exponent of G be p^n.
Let $|G| = m$ and let $\alpha = a_1g_1 + a_2g_2 + ... + a_mg_m \in \{\triangle(G) + 1\}$.
Then $\alpha^{p^n} = (a_1^{p^n}g_1^{p^n} + a_2^{p^n}g_2^{p^n} + ... + a_m^{p^n}g_m^{p^n})$
$= (a_1^{p^n} + a_2^{p^n} + ... + a_m^{p^n}) = (a_1 + a_2 + ... + a_m)^{p^n} = (\epsilon(\alpha))^{p^n} = 1^{p^n} = 1.$
Thus α is a unit with order dividing p^n. Thus by Corollary 4.42, the set $\{\triangle(G) + 1\}$ forms a group under multiplication and since all elements have order dividing p^n, the exponent of the group divides p^n. Since $G < V$, $exp(V)$ $= p^n$.
In contrast, for a finite group algebra $\mathbb{F}_{p^k}G$, with G not a $p-group$, then we show that the set $\{\triangle(G) + 1\}$ contains at least one zero divisor.

Let $|G| = p^\alpha m$ where p does not divide m and let $m = q_1^{e_1}q_2^{e_2}...q_n^{e_n}$ with $q_1, ..., q_n$ distinct primes and with $e_1 \geq 1$ and $e_2, ...e_n \geq 0$.
By Sylow's Theorem, there exists a subgroup H of order $q_1^{e_1}$.
Then by Lemma 4.9, $\frac{1}{|H|}\hat{H}$ annihilates the elements of $(\triangle G, H)$ and so $\frac{1}{|H|}\hat{H}$ is a zero divisor.
Also $\epsilon(\frac{1}{|H|}\hat{H}) = \epsilon(\frac{1}{|H|}).\epsilon(\hat{H}) = \frac{1}{|H|}.|H| = 1 \Rightarrow \frac{1}{|H|}\hat{H} \in \{\triangle(G) + 1\}$ and so the set contains at least one zero divisor.

Corollary 5.4. *For a finite group algebra $\mathbb{F}_{p^k}G$, with G an abelian $p-$group, then $|U(\mathbb{F}_{p^k}G)| = ((p^k)^{|G|-1})(p^k - 1)$.*

Proof. By Lemma 4.17, $U(FG) = V \times F^{\times}$. By Lemma 5.3, $V \simeq \{\triangle(G)+1\}$. The order of $\{\triangle(G)+1\} = (p^k)^{|G|-1}$ by Lemma 4.29, so we get $|U(\mathbb{F}_{p^k}G)|$ $= |V|.|F^{\times}| = ((p^k)^{|G|-1})(p^k-1)$.

Lemma 5.5. *For $p \neq 2$, the group algebra $\mathbb{F}_{p^k}C_2$ contains exactly one zero divisor of augmentation 1.*

Proof. By Lemma 4.24 when $p \neq 2$, the unit group of $\mathbb{F}_{p^k}C_2 \simeq C^2_{p^k-1}$. Thus $V \simeq C_{p^k-1}$ and there are p^k elements of augmentation 1. By Lemma 5.3, the set $\{\triangle(G)+1\}$ contains at least one non-unit, and there can only be one because all of the other elements are units as $|V| = p^k$. The non-unit is $\frac{1}{2}\hat{C}_2$ (a zero-divisor).

Definition The injective homomorphism $\sigma : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, given by $\alpha \mapsto \alpha^p$ is surjective since $\mathbb{F}_{p^n}$ is finite and so is an isomorphism, and thus an automorphism. It is called the *Frobenius automorphism* which is denoted by σ_p. Iterating σ_p gives $\sigma_p^2(\alpha) = \sigma_p(\sigma_p(\alpha)) = (\alpha^p)^p = \alpha^{p^2}$.
Similarly $\sigma_p^i(\alpha) = \alpha^{p^i}$ $i = 0, 1, 2, ...$

Note that as a consequence of the Frobenius automorphism being surjective, we have that every element of $\mathbb{F}_{p^n}$ has a p^ith root for all i. We use this consequence in the examples below when counting the number of choices for field coefficients.

5.1 $U(FG)$ where $char(F) = 2$ and G is an abelian $2-$ group

In this section, we examine the case where $char(F) = 2$ and G is an abelian (but not an elementary abelian) 2-group.

Example 5.6. *$U(\mathbb{F}_2C_8)$. $U \simeq V$. $|V| = |\{\triangle(G)+1\}| = 128$ by Lemma 5.3. V is an abelian group with order 128 and exponent 8. The possible groups for V are $C_8^2 \times C_2$, $C_8 \times C_4^2$, $C_8 \times C_4 \times C_2^2$ and $C_8 \times C_2^4$. These four groups have 7, 7, 15 and 31 elements of order 2 respectively by Lemma 5.1. Again we count the elements of order 2 in V, to determine which of the groups it is.*

Let $\alpha = \sum_{i=0}^{7} a_i x^i \in V$ with $\alpha^2 = 1$. Then $\alpha^2 = \sum_{i=0}^{7} a_i x^{2i} = 1$. Note that in $\mathbb{F}_2$, $a_i^2 = a_i$. This is because the Frobenius Automorphism fixes the elements of the prime subfield.

$\alpha^2 = (a_0 + a_4)1 + (a_1 + a_5)x^2 + (a_2 + a_6)x^4 + (a_3 + a_7)x^6 = 1.$
The coefficient of 1 must be 1 and the other coefficients must be zero. Counting the possibilities, we see that there are 2 possibilities for each of the coefficients, giving a total of $2^4 = 16$ possible elements α such that $\alpha^2 = 1$. One of these elements is the identity of the group, and so there are 15 elements of order 2. They are: $x^4, 1+x^2+x^6, x^2+x^4+x^6, 1+x+x^5, x+x^4+x^5, 1+x+x^2+x^5+x^6, x+x^2+x^4+x^5+x^6, 1+x^3+x^7, x^4+x^3+x^7, 1+x+x^3+x^5+x^7, 1+x^2+x^3+x^6+x^7, x^4+x+x^3+x^5+x^7, x^4+x^2+x^3+x^6+x^7, 1+x^2+x^3+x^5+x^6+x^7, x^2+x^3+x^5+x^6+x^7$.

Thus, $U \simeq C_8 \times C_4 \times C_2^2$.

Lemma 5.7. $U(\mathbb{F}_{2^n}(C_2 \times C_4)) \simeq C_2^{5n} \times C_4^n \times C_{2^n-1}$.

Proof. $U(FG) \simeq V \times F^\times \simeq V \times C_{2^n-1}$
G is an abelian $2-$*group* and by Lemma 5.3 the group of normalised units V has order equal to $|\{1 + \triangle(G)\}|$ and V is an abelian group of exponent 4 (the exponent of G).

Thus $|V| = (2^n)^7 = 2^{7n}$ and $V \simeq C_2^a \times C_4^b$.
We now count the number of units of order dividing 2 in V.
Let $\alpha = a_0(1) + a_1(x) + a_2(x^2) + a_3(x^3) + a_4(y) + a_5(xy) + a_6(x^2y) + a_7(x^3y)$ $\in V$ with $\alpha^2 = 1$, $a_i \in \mathbb{F}_{2^n}$
Then $\alpha^2 = (a_0)^2(1) + (a_1)^2(x^2) + (a_2)^2(1) + (a_3)^2(x^2) + (a_4)^2(1) + (a_5)^2(x^2) +$ $(a_6)^2(1) + (a_7)^2(x^2)$
$= [(a_0)^2 + (a_2)^2 + (a_4)^2 + (a_6)^2]1 + [(a_1)^2 + (a_3)^2 + (a_5)^2 + (a_7)^2]x^2 = 1.$
Thus the coefficient of 1_G must be 1_F and the coefficient of x^2 must be 0_F.
Because there are 2^n elements in $\mathbb{F}_{2^n}$, there are 2^n ways in which each of the coefficients a_0, a_2, a_4 can occur and this determines what a_6 must be giving $(2^n)^3 = 2^{3n}$ possibilities for the coefficient of 1_G. Similarly there are 2^{3n} possibilities for the coefficient of x^2, giving a total of $(2^{3n})(2^{3n}) = 2^{6n}$ different elements α in V such that $\alpha^2 = 1$.
One of these elements is the identity, so there are $2^{6n} - 1$ elements of order 2 in V.
Recall that $|V| = 2^{7n}$ and $V \simeq C_2^a \times C_4^b$. Thus

(1) $a + 2b = 7n$ by considering the order of V.

But because of the number of elements of order 2, there must be a direct product of $6n$ groups, and so we have that

(2) $a + b = 6n$.

Subtracting (2) from (1) we get that $b = n$, and it follows that $a = 5n$.
Thus $V \simeq C_2^{5n} \times C_4^n$ and so $U \simeq C_2^{5n} \times C_4^n \times C_{2^n-1}$.

Lemma 5.8. *$U(\mathbb{F}_{2^n}C_4) \simeq C_2^n \times C_4^n \times C_{2^n-1}$.*

Proof. $U(FG) \simeq V \times F^\times \simeq V \times C_{2^n-1}$
G is a $2-group$ and by Lemma 5.3 the group of normalised units V has order equal to $|\{1 + \triangle(G)\}|$ and V is an abelian group of exponent 4 (the exponent of G).
Thus $|V| = (2^n)^3 = 2^{3n}$and $V \simeq C_2^a \times C_4^b$.
We now count the number of units of order 2 in V.
Let $\alpha = a_0(1) + a_1(x) + a_2(x^2) + a_3(x^3) \in V$ with $\alpha^2 = 1$, $a_i \in \mathbb{F}_{2^n}$
Then $\alpha^2 = (a_0)^2(1) + (a_1)^2(x^2) + (a_2)^2(1) + (a_3)^2(x^2)$

$= [(a_0)^2 + (a_2)^2]1 + [(a_1)^2 + (a_3)^2]x^2 = 1.$

Thus the coefficient of 1_G must be 1_F and the coefficient of x^2 must be 0_F.

There are 2^n ways in which the coefficients a_0 can occur and this determines what a_2 must be giving 2^n possibilities for the coefficient of 1_G. Similarly there are 2^n possibilities for the coefficient of x^2, giving a total of $(2^n)(2^n) = 2^{2n}$ different elements α in V such that $\alpha^2 = 1$.

One of these elements is the identity, so there are $2^{2n} - 1$ elements of order 2 in V.

Recall that $|V| = 2^{3n}$ and $V \simeq C_2^a \times C_4^b$. Thus

(1) $a + 2b = 3n$ by considering the order of V.

But because of the number of elements of order 2, there must be a direct product of $2n$ groups, and so we have that

(2) $a + b = 2n$.

Subtracting (2) from (1) we get that $b = n$, and it follows that $a = n$.

Thus $V \simeq C_2^n \times C_4^n$ and so $U \simeq C_2^n \times C_4^n \times C_{2^n-1}$.

5.2 $U(FG)$ where $char(F) = p$ and G is an abelian $p-group$

The techniques used in the previous section can be applied to group algebras with characteristic p where G is a $p-group$ but not elementary abelian.

Lemma 5.9. *Let* $FG = \mathbb{F}_p C_{p^2}$. *Then* $U(FG) \simeq C_p^{(p-1)^2} \times C_{p^2}^{p-1} \times C_{p-1}$.

Proof. $U(FG) \simeq V \times F^\times \simeq V \times C_{p-1}$.
G is a $p-group$ and by Lemma 5.3, $|V| = (p)^{p^2-1}$ and $V \simeq C_p^a \times C_{p^2}^b$, $b \geq 1$.
We now count the number of units of order p in V.
Let $\alpha = \sum_{i=0}^{p^2-1} a_i x^i \in V$ with $\alpha^p = 1$. Then $\alpha^p = \sum_{i=0}^{p^2-1} a_i^p x^{pi} = 1$.

Now the group element becomes x^{pi} and so the power of x is a multiple of p and there are p of those in C_{p^2}. We write this group element as x^{jp} for $0 \leq j \leq p-1$, and adding up the like terms we get
$\alpha^p = \sum_{j=0}^{p-1} \sum_{i=0}^{p-1} a_{ip+j} x^{jp} = 1$.

The coefficients of x^{0p} when $j = 0$ (i.e. $\sum_{i=0}^{p-1} a_{ip+0}$) must equal 1_F, and the coefficients of x^{jp} for $j \neq 0$ (i.e. $\sum_{i=0}^{p-1} a_{ip+j} x^{jp}$) must equal 0_F.
For each j, we have a different group element. For 1_G (when $j = 0$), there are p choices for a_{ip+0} for each $i \neq p-1$. Thus there are p^{p-1} choices for the coefficient of the group element x^{0p}. Similarly there are p^{p-1} choices for each of the coefficients of x^{jp} for $j \neq 0$, giving a total of $p^{(p-1)(p)} = p^{p^2-p}$ different elements α in V such that $\alpha^p = 1$.
Recall that $|V| = (p)^{p^2-1}$ and $V \simeq C_p^a \times C_{p^2}^b$, $b \geq 1$.
Thus

(1) $a + 2b = p^2 - 1$ by considering the order of V.

But because of the number of elements of order p, there must be a direct product of $p^2 - p$ groups, and so we have that

(2) $a + b = p^2 - p$.

Subtracting (2) from (1) we get that $b = p-1$, and it follows that $a = (p-1)^2$. Thus V$\simeq C_p^{(p-1)^2} \times C_{p^2}^{p-1}$ and so $U \simeq C_p^{(p-1)^2} \times C_{p^2}^{p-1} \times C_{p-1}$.

Now a further generalisation.

Lemma 5.10. *Let $FG = \mathbb{F}_{p^n} C_{p^m}$. The number of elements of order dividing p^k in V is $p^{n(p^m - p^{m-k})}$.*

Proof. To count the elements of order dividing p^k in V we first count how many elements of G are mapped to the identity under the homomorphism ϕ: $G \to G$ defined as $\phi(x) = x^{p^k}$.

In a cyclic group C_{p^m}, the element $x^{p^{m-k}}$ has order dividing p^k and so do all of the elements of the subgroup generated by $x^{p^{m-k}}$, i.e. $\langle x^{p^{m-k}} \rangle$.

In fact this subgroup is the kernel of the homomorphism ϕ. To see this, let $x^i \in ker(\phi)$. Then $(x^i)^{p^k} = 1$. That is $x^{ip^k} = 1$. That is ip^k is a multiple of p^m. That is i is a multiple of p^{m-k}. Thus the subgroup generated by $x^{p^{m-k}}$ is the kernel of the homomorphism. So we have that $\langle x^{p^{m-k}} \rangle \simeq C_{p^k} \simeq \ker(\phi)$.

As the generator of this kernel is of order p^k, then this group has p^k elements. The quotient group of this homomorphism has order p^{m-k}.

Thus the image group $H = \phi(G)$ is of order p^{m-k}.
Now let $\alpha = \sum a_n g_n \in V$ such that $\alpha^{p^k} = 1$. Then we can write α^{p^k} with coefficients from $\mathbb{F}_{p^n}$ and group elements from the image group $H = \phi(G)$.

Labelling the elements of the image group H as g_1, g_2, ..., $g_{|G/H|}$ where $g_1 = 1_G$, and relabelling the a's gives,
$\alpha^{p^k} = (\sum_{i=1}^{p^k} a_{1i}^{p^k}) g_1 + (\sum_{i=1}^{p^k} a_{2i}^{p^k}) g_2 + ... + (\sum_{i=1}^{p^k} a_{p^{m-k}i}^{p^k}) g_{p^{m-k}}$.

Now if $\alpha^{p^k} = 1$, then the coefficient of $g_1 = 1_G$ is 1_F and the coefficients of all other g_i is 0_F.
That is $\sum_{i=1}^{p^k} a_{1i}^{p^k} = 1_F$.
We have freedom to choose $p^k - 1$ elements of $\mathbb{F}_{p^n}$ but the last element will be determined so as to give a sum of 1_F .
So there are $(p^n)^{p^k-1}$ choices for the coefficient of g_1.
Similarly, there are $(p^n)^{p^k-1}$ choices for the coefficient of g_2 and each g_j up

to $g_{p^{m-k}}$.
Thus we have $[(p^n)^{p^k-1}]^{p^{m-k}} = p^{n(p^m-p^{m-k})}$ choices for α such that $\alpha^{p^k} = 1$.

This is the number of elements of V with order dividing p^k.

Lemma 5.11. *Let* $FG = \mathbb{F}_{p^n}C_{p^2}$. *Then* $U(FG) \simeq C_p^{n(p-1)^2} \times C_{p^2}^{n(p-1)} \times C_{p^n-1}$.

Proof. $U(FG) \simeq V \times F^\times \simeq V \times C_{p^n-1}$.
G is a $p-group$ and by Lemma 5.3, $|V| = (p^n)^{p^2-1} = p^{n(p^2-1)}$ and $V \simeq C_p^a \times C_{p^2}^b$, $b \geq 1$.
Thus (1) $a + 2b = n(p^2-1)$ by considering the order of V.
By Lemma 5.10 there are $p^{n(p^2-p^{2-1})} = p^{n(p^2-p)}$ elements of order dividing p in V.
But because of the number of elements of order p, there must be a direct product of $p^{n(p^2-p)}$ groups, and so we have that (2) $a + b = n(p^2-p)$.
That is (1) $a + 2b = n(p^2-1)$
and (2) $a + b = n(p^2-p)$.
Subtracting (2) from (1) we get that $b = n(p^2-1) - n(p^2-p) = np^2 - n - np^2 + pn = n(p-1)$, and it follows that a $= n(p-1)^2$.
Thus V$\simeq C_p^{n(p-1)^2} \times C_{p^2}^{n(p-1)}$ and so $U \simeq C_p^{n(p-1)^2} \times C_{p^2}^{n(p-1)} \times C_{p^n-1}$.

Example 5.12. *Let* $FG = \mathbb{F}_{5^4}C_{25}$. *Then by Lemma 5.11* $U(FG) \simeq C_5^{4(5-1)^2} \times C_{5^2}^{4(5-1)} \times C_{5^4-1} \simeq C_5^{64} \times C_{25}^{16} \times C_{624}$.

Example 5.13. *Let* $FG = \mathbb{F}_{2^2}C_4$. *Then by Lemma 5.11* $U(FG) \simeq C_2^{2(2-1)^2} \times C_{2^2}^{2(2-1)} \times C_{2^2-1} \simeq C_2^2 \times C_4^2 \times C_3$ *which is the same result as we got earlier.*

Lemma 5.14. *In the group* $G = \prod_{i=1}^{m} C_{p^i}^{d_i}$, *the number of elements with order dividing* p^k *(where* $1 \leq k < m$*) is* $p^{(\sum_{i=1}^{k} id_i + \sum_{i=k+1}^{m} kd_i)}$.
(The number of elements with order dividing p^k *(where* $k = 0$*) is 1. The number of elements with order dividing* p^k *(where* $k \geq m$*) is* $p^{\sum_{i=1}^{k} id_i} = |G|$*).*

Proof. For $1 \leq i \leq k$, the group C_{p^i} has exponent dividing p^k, and so all of the elements of C_{p^i} have order dividing p^k. Thus all of the elements of direct products of these individual groups will have order dividing p^k.
For $k+1 \leq i \leq m$, there are p^k elements in each of these factor groups C_{p^i} with order dividing p^k by Lemma 5.2.
Thus we get $p^{(\sum_{i=1}^{k} id_i + \sum_{i=k+1}^{m} kd_i)}$ elements with order dividing p^k.
Finally, the two trivial cases are where $k = 0$ or $k \geq m$.
If $k = 0$, we get that $p^0 = 1$ (the group identity) and only the group identity will have order dividing 1.
Second, if $k \geq m$, then as all of the elements of the group have order dividing p^m, it follows that all of the elements of the group have order dividing p^k which completes the proof.

The following Theorem gives the order of the unit group for a group algebra from an arbitrary abelian $p-group$.

Theorem 5.15. *Let* FG *be the group algebra* $\mathbb{F}_{p^n}(\prod_{i=1}^{m} C_{p^i}^{e_i})$ *and let* $\phi_i(g) = g^{p^i}\ \forall\ g \in G$.
Then $U(FG) \simeq \prod_{i=1}^{m} C_{p^i}^{n(|G/\ker(\phi_{i-1})| - 2n|G/ker(\phi_i)| + n|G/ker(\phi_{i+1})|)} \times C_{p^n-1}$.

Proof. By Lemma 5.3 all of the elements of $\{1 + \triangle G\}$ are units so $V = \{1 + \triangle G\}$ and moreover the exponent of V equals the exponent of G and so $V \simeq \prod_{i=1}^{m} C_{p^i}^{d_i}$.
We work out the structure of V by counting the number of elements in V with order dividing p^m, p^{m-1}, ... , and p^1.

First we count the number of elements of V with order dividing p^m.

Let $\alpha \in V$ such that $\alpha^{p^m} = 1$.
We can write α as $\sum_{i=1}^{m} \sum_{j=1}^{e_i} \sum_{k=1}^{p^i} a_{ijk} x_{ij}^k$ where $a_{ijk} \in \mathbb{F}_{p^n}$ and $x_{ij}^k \in G = \prod_{i=1}^{m} C_{p^i}^{e_i}$.
Now we count the number of choices for α such that $\alpha^{p^m} = 1$.
That is, such that $\sum_{i=1}^{m} \sum_{j=1}^{e_i} \sum_{k=1}^{p^i} a_{ijk}^{p^m} (x_{ij}^k)^{p^m} = 1$.
The Frobenius automorphism σ^m: $\mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ defined by $\sigma^m(a) = a^{p^m}$ permutes the elements of $\mathbb{F}_{p^n}$. Thus the field element $a_{ijk}^{p^m}$ is just the image of a_{ijk} under this bijection and in particular all elements of $\mathbb{F}_{p^n}$ are $p^m th$ roots.

Define the group endomorphism ϕ_i: $G \to G$ as $\phi_i(g) = g^{p^i}$.
In this case $\phi_m(g) = g^{p^m}$ and $(x_{ij}^k)^{p^m}$ is an element of the image. There are $|ker(\phi_m)|$ elements $g \in G$ such that $\phi_m(g) = 1_G$. Call this kernel H.
The First Isomorphism Theorem states that the image group of a group endomorphism $\phi_m(G)$ is isomorphic to the quotient group $G/ker\phi_m$ or G/H.
Labelling the elements of the image group as g_1, g_2, ..., $g_{|G/H|}$ where $g_1 = 1_G$, then we can write
$\alpha^{p^m} = (\sum_{i=1}^{|H|} a_{1i}^{p^m}) g_1 + (\sum_{i=1}^{|H|} a_{2i}^{p^m}) g_2 + ... + (\sum_{i=1}^{|H|} a_{|G/H|i}^{p^m}) g_{|G/H|}$.

Now if $\alpha^{p^m} = 1$, then the coefficient of $g_1 = 1_F$ and the coefficients of all other $g_i = 0_F$.
That is $\sum_{i=1}^{|H|} a_{1i}^{p^m} = 1_F$.
We have freedom to choose $|H| - 1$ elements of $\mathbb{F}_{p^n}$ but the last element will be determined so as to give a sum of 1_F .
Thus we have freedom to choose $|H| - 1$ elements from $\mathbb{F}_{p^n}$ and there are p^n choices for each element. So there are $(p^n)^{|H|-1}$ choices for the coefficient of g_1.
Similarly, there are $(p^n)^{|H|-1}$ choices for the coefficient of g_2 and each g_j up to $g_{|G/H|}$.
Thus we have $[(p^n)^{|H|-1}]^{|G/H|}$ choices for the α such that $\alpha^{p^m} = 1$.

So there are $[(p^n)^{|ker(\phi_m)|-1}]^{|G/ker(\phi_m)|} = p^{n|G|-n|G/ker(\phi_m)|}$ choices for α_m.

This is the number of elements of V with order dividing p^m.

According to Lemma 5.14 if $G = \prod_{i=1}^{m} C_{p^i}^{d_i}$, then the number of elements of G with order dividing p^k is $p^{(\sum_{i=1}^{k} id_i + \sum_{i=k+1}^{m} kd_i)}$.
Here we have that $V = \prod_{i=1}^{m} C_{p^i}^{d_i}$, and so the number of elements of V with order dividing p^m in V is $p^{\sum_{i=1}^{m} id_i}$.
But we have just worked out that the number of elements of V with order dividing p^m is $p^{n|G|-n|G/ker(\phi_m)|}$.
So we get the equation

(M) $$\sum_{i=1}^{m} id_i = n|G| - n|G/ker(\phi_m)|.$$

Next we count the number of elements of V with order dividing p^{m-1}.

Let $\beta \in V$ such that $\beta^{p^{m-1}} = 1$.
Define the group endomorphism ϕ_{m-1}: $G \to G$ as $\phi_{m-1}(g) = g^{p^{m-1}}$.
There are $|ker(\phi_{m-1})|$ elements $g \in G$ such that $\phi_{m-1}(g) = 1_G$. Call this kernel H_{m-1}.
The image group of $\phi_m(G)$ is isomorphic to the quotient group $G/ker\phi_{m-1}$ or G/H_{m-1}.
Labeling the elements of the image group as g_1, g_2, ..., $g_{|G/H_{m-1}|}$ where $g_1 = 1_G$, then
$\alpha^{p^{m-1}} = (\sum_{i=1}^{|H_{m-1}|} a_{1i}^{p^{m-1}})g_1 + (\sum_{i=1}^{|H_{m-1}|} a_{2i}^{p^{m-1}})g_2 + ... + (\sum_{i=1}^{|H_{m-1}|} a_{|G/H_{m-1}|i}^{p^{m-1}})g_{|G/H_{m-1}|}.$

Now if $\alpha^{p^{m-1}} = 1$, then the coefficient of g_1 is 1_F and the coefficients of all other g_i is 0_F.
That is $\sum_{i=1}^{|H_{m-1}|} a_{1i}^{p^{m-1}} = 1_F$.
Again we have freedom to choose $|H_{m-1}| - 1$ elements of $\mathbb{F}_{p^n}$ but the last element will be determined so as to give a sum of 1_F .
Thus we have freedom to choose $|H_{m-1}| - 1$ elements from $\mathbb{F}_{p^n}$ and there

are p^n choices for each element. So there are $(p^n)^{|H_{m-1}|-1}$ choices for the coefficient of g_1.

Similarly, there are $(p^n)^{|H_{m-1}|-1}$ choices for the coefficient of g_2 and each g_j up to $g_{|G/H_{m-1}|}$.

Thus we have $[(p^n)^{|H_{m-1}|-1}]^{|G/H_{m-1}|}$ choices for the β such that $\beta^{p^{m-1}} = 1$.

So there are $[(p^n)^{|ker(\phi_{m-1})|-1}]^{|G/ker(\phi_{m-1})|} = p^{n|G|-n|G/ker(\phi_{m-1})|}$ choices for β.

This is the number of elements of V with order dividing p^{m-1}.

According to Lemma 5.14 the number of elements of V with order dividing p^{m-1} is $p^{(\sum_{i=1}^{m-1} id_i + \sum_{i=m}^{m} (m-1)d_i)} = p^{(\sum_{i=1}^{m-1} id_i + (m-1)d_m)}$.

But we have also seen that the number of elements of V with order dividing p^{m-1} is $p^{n|G|-n|G/ker(\phi_{m-1})|}$.

So we get the equation

(M-1) $$\sum_{i=1}^{m-1} id_i + (m-1)d_m = n|G| - n|G/ker(\phi_{m-1})|.$$

We proceed in this way, each time counting the number of elements in V with order dividing p^i using Lemma 5.14 and also using the technique in this proof forming simultaneous equations with variables d_i until we reach equation (1).

These equations are:

(M) $$\sum_{i=1}^{m} id_i = n|G| - n|G/ker(\phi_m)|$$

(M-1) $$\sum_{i=1}^{m-1} id_i + \sum_{i=m}^{m} (m-1)d_i = n|G| - n|G/ker(\phi_{m-1})|$$

(M-2) $$\sum_{i=1}^{m-2} id_i + \sum_{i=m-1}^{m} (m-2)d_i = n|G| - n|G/ker(\phi_{m-2})|$$

.

.

(k) $$\sum_{i=1}^{k} id_i + \sum_{i=k+1}^{m} (k)d_i = n|G| - n|G/ker(\phi_k)|$$

(k-1) $$\sum_{i=1}^{k-1} id_i + \sum_{i=k}^{m} (k-1)d_i = n|G| - n|G/ker(\phi_{k-1})|$$

.

.

$$(3) \qquad \sum_{i=1}^{3} id_i + \sum_{i=4}^{m} 3d_i = n|G| - n|G/ker(\phi_3)|$$

$$(2) \qquad \sum_{i=1}^{2} id_i + \sum_{i=3}^{m} 2d_i = n|G| - n|G/ker(\phi_2)|$$

$$(1) \qquad \sum_{i=1}^{1} 1d_i + \sum_{i=2}^{m} 1d_i = n|G| - n|G/ker(\phi_1)|.$$

We now have m simultaneous equations in the m unknowns d_i for $1 \leq i \leq m$. Solving these equations enables us to know the value of each d_i and thus the structure of V. We will have this structure in terms of the orders of the quotient groups $|G/\ker(\phi_i)|$ which are easily calculated.

To solve the equations we begin with (M) and subtract (M-1). This isolates d_m. We get:

(M) - (M-1) =

$$\sum_{i=1}^{m} id_i \text{ - } \sum_{i=1}^{m-1} id_i \text{ - } (m-1)d_m = n|G| - n|G/ker(\phi_m)| \text{ - } n|G| + n|G/ker(\phi_{m-1})|$$

$$\Rightarrow md_m \text{ - } (m-1)d_m = n|G/ker(\phi_{m-1})| \text{ - } n|G/ker(\phi_m)|$$

$$\Rightarrow d_m = n|G/ker(\phi_{m-1})| \text{ - } n|G/ker(\phi_m)|.$$

Next we take (M-1) and subtract (M-2). This will isolate d_{m-1}. We get:

(M-1) - (M-2)=

$$\sum_{i=1}^{m-1} id_i + (m-1)d_m \text{ - } \sum_{i=1}^{m-2} id_i \text{ - } \sum_{i=m-1}^{m} (m-2)d_i$$
$$= n|G| - n|G/ker(\phi_{m-1})| \text{ - } n|G| + n|G/ker(\phi_{m-2})|$$
$$\Rightarrow (m-1)d_{m-1} + (m-1)d_m \text{ - } \sum_{i=m-1}^{m} (m-2)d_i$$
$$= n|G/ker(\phi_{m-2})| \text{ - } n|G/ker(\phi_{m-1})|$$
$$\Rightarrow (m-1)d_{m-1} \text{ - } (m-2)d_{m-1} + (m-1)d_m \text{ - } (m-2)d_m$$
$$= n|G/ker(\phi_{m-2})| \text{ - } n|G/ker(\phi_{m-1})|$$
$$\Rightarrow d_{m-1} + d_m = n|G/ker(\phi_{m-2})| \text{ - } n|G/ker(\phi_{m-1})|$$

But $d_m = n|G/ker(\phi_{m-1})| \text{ - } n|G/ker(\phi_m)|$ so we subtract this from both sides to get:

$$d_{m-1} = n|G/ker(\phi_{m-2})| \text{ - } n|G/ker(\phi_{m-1})| \text{ - } n|G/ker(\phi_{m-1})| + n|G/ker(\phi_m)|$$
$$d_{m-1} = n|G/ker(\phi_{m-2})| \text{ - } 2n|G/ker(\phi_{m-1})| + n|G/ker(\phi_m)|.$$

Proceeding in this way, we get each d_i in turn.

(k) - (k-1):

$$\sum_{i=1}^{k} id_i + \sum_{i=k+1}^{m} kd_i \text{ - } \sum_{i=1}^{k-1} id_i \text{ - } \sum_{i=k}^{m}(k-1)d_i$$
$$= n|G| - n|G/ker(\phi_k)| \text{ - } n|G| + n|G/ker(\phi_{k-1})|$$
$$\Rightarrow kd_k + \sum_{i=k+1}^{m} kd_i \text{ - } \sum_{i=k}^{m}(k-1)d_i$$
$$= n|G/ker(\phi_{k-1})| \text{ - } n|G/ker(\phi_k)|$$
$$\Rightarrow \sum_{i=k}^{m} kd_i \text{ - } \sum_{i=k}^{m}(k-1)d_i$$
$$= n|G/ker(\phi_{k-1})| \text{ - } n|G/ker(\phi_k)|$$
$$\Rightarrow \sum_{i=k}^{m} d_i = n|G/ker(\phi_{k-1})| \text{ - } n|G/ker(\phi_k)|$$

But the previous equation (k+1) - (k) will be $\sum_{i=k+1}^{m} d_i = n|G/ker(\phi_k)|$ - $n|G/ker(\phi_{k+1})|$. So we subtract this from both sides and we get:

$$d_k = n|G/ker(\phi_{k-1})| \text{ - } n|G/ker(\phi_k)| \text{ - } n|G/ker(\phi_k)| + n|G/ker(\phi_{k+1})|$$
$$\Rightarrow d_k = n|G/ker(\phi_{k-1})| \text{ - } 2n|G/ker(\phi_k)| + n|G/ker(\phi_{k+1})|.$$

We continue this process until we get:

$$d_1 = n|G/ker(\phi_0)| \text{ - } 2n|G/ker(\phi_1)| + n|G/ker(\phi_2)|.$$

Now we have expressed all of the d_i in terms of the orders of the quotient groups $|G/\ker(\phi_i)|$.

One last step will tidy the answer up.

We saw that $d_m = n|G/ker(\phi_{m-1})| \text{ - } n|G/ker(\phi_m)|$.

The right hand side of this equation is equal to $n|G/ker(\phi_{m-1})| \text{ - } 2n|G/ker(\phi_m)| + n|G/ker(\phi_{m+1})|$ (since $ker(\phi_m) = ker(\phi_{m+1}) = G$ because G has exponent p^m).

Thus we can express $d_i = n|G/ker(\phi_{i-1})| \text{ - } 2n|G/ker(\phi_i)| + n|G/ker(\phi_{i+1})|$ for $1 \leq i \leq m$.

This completes the structure of V. Finally, $U \simeq V \times C_{p^n-1}$, which completes the proof.

Example 5.16. $\mathbb{F}_{5^4}C_{5^2}^1$.
In this example, $p = 5$, $n = 4$, $m = 2$, $e_1 = 0$, $e_2 = 1$.
Now $|G| = 5^2$.
To calculate the number of copies of C_{p^i}, *we need to calculate* $|G/ker(\phi_i)|$ *for* $0 \leq i \leq 3$.

$|ker(\phi_0)|$ = *the number of elements of order dividing* $5^0 = 1$ *in* G.
Clearly this is only the identity element in G.
Thus $|G/ker(\phi_0)| = 5^2$.

$|ker(\phi_1)|$ = *the number of elements of order dividing* 5^1 *in* G.
By Lemma 5.14 this is $5^{(\sum_{i=1}^{1} ie_i + \sum_{i=2}^{2} 1e_i)} = 5^{1(0)+1(1)} = 5^1$.
Thus $|G/ker(\phi_1)| = 5^{2-1} = 5^1$.

$|ker(\phi_2)| = 5^{\sum_{i=1}^{2} ie_i} = 5^{1(0)+2(1)} = 5^2$.
Thus $|G/ker(\phi_2)| = 5^{2-2} = 5^0 = 1$.

$|ker(\phi_3)| = 5^{\sum_{i=1}^{2} ie_i} = 5^{1(0)+2(1)} = 5^2$.
Thus $|G/ker(\phi_3)| = 5^{2-2} = 5^0 = 1$.

Now we can compute the individual numbers of direct copies of C_{p^i}.
Recall that $a_i = n|G/ker(\phi_{i-1})|$ - $2n|G/ker(\phi_i)|$ + $n|G/ker(\phi_{i+1})|$. $a_1 =$

$4(5^2) - 8(5^1) + 4(5^0) = 100 - 40 + 4 = 64$
$a_2 = 4(5^1) - 8(5^0) + 4(5^0) = 20 - 8 + 4 = 16$.

Thus $V \simeq C_5^{64} \times C_{5^2}^{16}$ *which is the same result as we got earlier doing it out by a different method.*

Example 5.17. $\mathbb{F}_{3^2}(C_{3^3}^2 \times C_{3^4}^5 \times C_{3^8})$.
In this example, $p = 3$, $n = 2$, $m = 8$, $e_3 = 2$, $e_4 = 5$, $e_8 = 1$. $e_i = 0 \, \forall$ *other* i.
Now $|G| = 3^{(3)(2)+(4)(5)+(8)(1)} = 3^{34}$.
To calculate the number of copies of C_{p^i}, *we need to calculate* $|G/ker(\phi_i)|$ *for* $0 \leq i \leq 9$.

$|ker(\phi_0)|$ = *the number of elements of order dividing* $3^0 = 1$ *in* G.
Clearly this is only the identity element in G.
Thus $|G/ker(\phi_0)| = 3^{34}$.

$|ker(\phi_1)|$ = *the number of elements of order dividing* 3^1 *in* G.
By Lemma 5.14 this is $3^{(\sum_{i=1}^{1} ie_i + \sum_{i=2}^{8} 1e_i)} = 3^{1(2)+1(5)+1(1)} = 3^8$.
Thus $|G/ker(\phi_1)| = 3^{34-8} = 3^{24}$.

$|ker(\phi_2)| = 3^{(\sum_{i=1}^{2} ie_i + \sum_{i=3}^{8} 2e_i)} = 3^{2(2)+2(5)+2(1)} = 3^{16}$.
Thus $|G/ker(\phi_2)| = 3^{34-16} = 3^{18}$.

$|ker(\phi_3)| = 3^{(\sum_{i=1}^{3} ie_i + \sum_{i=4}^{8} 3e_i)} = 3^{3(2)+3(5)+3(1)} = 3^{24}$.
Thus $|G/ker(\phi_3)| = 3^{34-24} = 3^8$.

$|ker(\phi_4)| = 3^{(\sum_{i=1}^{4} ie_i + \sum_{i=5}^{8} 4e_i)} = 3^{3(2)+4(5)+4(1)} = 3^{30}$.
Thus $|G/ker(\phi_4)| = 3^{34-30} = 3^4$.

$|ker(\phi_5)| = 3^{(\sum_{i=1}^{5} ie_i + \sum_{i=6}^{8} 5e_i)} = 3^{3(2)+4(5)+5(1)} = 3^{31}$.
Thus $|G/ker(\phi_5)| = 3^{34-31} = 3^3$.

$|ker(\phi_6)| = 3^{(\sum_{i=1}^{6} ie_i + \sum_{i=7}^{8} 6e_i)} = 3^{3(2)+4(5)+6(1)} = 3^{32}$.
Thus $|G/ker(\phi_6)| = 3^{34-32} = 3^2$.

$|ker(\phi_7)| = 3^{(\sum_{i=1}^{7} ie_i + \sum_{i=8}^{8} 7e_i)} = 3^{3(2)+4(5)+7(1)} = 3^{33}$.
Thus $|G/ker(\phi_7)| = 3^{34-33} = 3^1$.

$|ker(\phi_8)| = 3^{34}$ *because all elements in* G *have order dividing* 3^8.
Thus $|G/ker(\phi_8)| = 3^{34-34} = 3^0 = 1$.

$|ker(\phi_9)| = 3^{34}$ *because all elements in* G *have order dividing* 3^9.
Thus $|G/ker(\phi_9)| = 3^{34-34} = 3^0 = 1$.

Now we can compute the individual numbers of direct copies of C_{p^i}.
Recall that $a_i = n|G/ker(\phi_{i-1})|$ - $2n|G/ker(\phi_i)|$ + $n|G/ker(\phi_{i+1})|$.

$$a_1 = 2(3^{34}) - 4(3^{24}) + 2(3^{18}) = \textit{33353234456028200}$$
$$a_2 = 2(3^{24}) - 4(3^{18}) + 2(3^8) = \textit{563309404128}$$
$$a_3 = 2(3^{18}) - 4(3^8) + 2(3^4) = \textit{774814896}$$
$$a_4 = 2(3^8) - 4(3^4) + 2(3^3) = \textit{12852}$$
$$a_5 = 2(3^4) - 4(3^3) + 2(3^2) = \textit{72}$$
$$a_6 = 2(3^3) - 4(3^2) + 2(3^1) = \textit{24}$$
$$a_7 = 2(3^2) - 4(3^1) + 2(3^0) = \textit{8}$$
$$a_8 = 2(3^1) - 4(3^0) + 2(3^0) = \textit{4}.$$

Thus $V \simeq C_3^{33353234456028200} \times C_{3^2}^{563309404128} \times C_{3^3}^{774814896} \times C_{3^4}^{12852} \times C_{3^5}^{72} \times C_{3^6}^{24} \times C_{3^7}^{8} \times C_{3^8}^{4}$.

Corollary 5.18. *Let* $FG = \mathbb{F}_{2^n} C_{2^3}^1$. *Then* $U(FG) \simeq C_2^{2n} \times C_{2^2}^n \times C_{2^3}^n \times C_{2^n-1}$.

Proof. We use Theorem 5.15 and the same terminology. In this case p = 2, n = n, m = 3, $e_1 = 0$, $e_2 = 0$, $e_3 = 1$.
Now $|G| = 2^3$.
To calculate the number of copies of C_{p^i}, we need to calculate $|G/ker(\phi_i)|$ for $0 \leq i \leq 4$ (because $4 = m + 1 = 3 + 1$).

$|ker(\phi_0)|$ = the number of elements of order dividing $2^0 = 1$ in G.
Clearly this is only the identity element in G.
Thus $|G/ker(\phi_0)| = 2^3$.

$|ker(\phi_1)|$ = the number of elements of order dividing 2^1 in G.
By Lemma 5.14 this is $2^{(\sum_{i=1}^{1} ie_i + \sum_{i=2}^{3} 1e_i)} = 2^{1(0)+1(1)} = 2^1$.
Thus $|G/ker(\phi_1)| = 2^{3-1} = 2^2$.

$|ker(\phi_2)| = 2^{(\sum_{i=1}^{2} ie_i + \sum_{i=3}^{3} 2e_i)} = 2^{1(0)+2(1)} = 2^2$.
Thus $|G/ker(\phi_2)| = 2^{3-2} = 2^1$.

$|ker(\phi_3)| = 2^{\sum_{i=1}^{3} ie_i} = 2^{1(0)+2(0)+3(1)} = 2^3$.
Thus $|G/ker(\phi_3)| = 2^{3-3} = 2^0 = 1$.

$|ker(\phi_4)|$ is also clearly $= 2^3$.
Thus $|G/ker(\phi_4)| = 2^{3-3} = 2^0 = 1$.

Now we can compute the individual numbers of direct copies of C_{p^i}.
Recall that $a_i = n|G/ker(\phi_{i-1})|$ - $2n|G/ker(\phi_i)| + n|G/ker(\phi_{i+1})|$.

$a_1 = n(2^3) - 2n(2^2) + n(2^1) = 8\text{n} - 8\text{n} + 2\text{n} = 2\text{n}$
$a_2 = n(2^2) - 2n(2^1) + n(2^0) = 4\text{n} - 4\text{n} + \text{n} = \text{n}$
$a_3 = n(2^1) - 2n(2^0) + n(2^0) = 2\text{n} - 2\text{n} + \text{n} = \text{n}$

Thus $U(FG) \simeq C_2^{2n} \times C_{2^2}^n \times C_{2^3}^n \times C_{2^n-1}$.

6 Idempotents and the Decomposition of Semisimple Group Algebras

Idempotents play a very important role in the decomposition of a group algebra.

Lemma 6.1. *There are exactly two idempotents in a field F.*

Proof. $0^2 = 0$ and $1^2 = 1$ so these two elements of the field are idempotents. Let $e \in F$. If $e^2 = e$ and $e \neq 0$, then $e^{-1}e^2 = e^{-1}e \Rightarrow e = 1$. Thus there are exactly two idempotents in the field F, namely 0 and 1.

Lemma 6.2. *Let FG be a finite semisimple commutative group algebra which can be decomposed into a sum of n fields. Then the number of distinct idempotents in FG is 2^n.*

Proof. Let $e = (e_1, e_2, .., e_n) \in FG$ such that $e^2 =$ e. Then $e^2 = (e_1^2, e_2^2, .., e_n^2)$ $=$ e $\Rightarrow e_i =$e$_i^2$ $\forall$ i = 1,2,....,n, so the $e_i's$ are either 0 or 1. Thus there are 2^n idempotents in FG.

Lemma 6.3. *[28] Let R be a ring and $H \triangleleft G$. If $|H|$ is invertibile in R then letting $e_H = |H|^{-1}.\hat{H}$ we have*

$$RG \simeq RG.e_H \oplus RG(1 - e_H)$$

where $RG.e_H \simeq R(G/H)$ and $RG(1 - e_H) \simeq \triangle(G, H)$.

Example 6.4. $\mathbb{F}_2C_9$. *Maschke's Theorem applies so $\mathbb{F}_2$ appears as a summand in the decomposition. What summands could C_9 be a subgroup of?*

$U(\mathbb{F}_{2^2}) = C_3$ and $9 \not| 3$. $U(\mathbb{F}_{2^3}) = C_7$ and $9 \not| 7$.

$U(\mathbb{F}_{2^4}) = C_{15}$ and $9 \not| 15$. $U(\mathbb{F}_{2^5}) = C_{31}$ and $9 \not| 31$.

$U(\mathbb{F}_{2^6}) = C_{63}$ and $9|63$ so C_9 could be a subgroup of this unit group.

$U(\mathbb{F}_{2^7}) = C_{127}$ and $9 \not| 127$. $U(\mathbb{F}_{2^8}) = C_{255}$ and $9 \not| 255$.

Thus $\mathbb{F}_{2^6}$ must be a summand and so there are only two possible decompositions. They are $\bigoplus_{i=1}^{3} \mathbb{F}_2 \oplus \mathbb{F}_{2^6}$ and $\mathbb{F}_2 \oplus \mathbb{F}_{2^2} \oplus \mathbb{F}_{2^6}$.

If it is the first one, then the unit group is C_{63}. If it is the second one, then

the unit group is $C_{63} \times C_3$.
Let $C_9 = < x >$ *and let* H *be the subgroup of* C_9 *of order 3. Thus* $H \simeq C_3 = \{1, x^3, x^6\}$. $\hat{H} = 1 + x^3 + x^6$.
Now because H *is normal in* C_9 *and letting* $e_H = \frac{1}{|H|}.\hat{H}$ *we have* $\mathbb{F}_2C_9 \simeq \mathbb{F}_2C_9.e_H \oplus \mathbb{F}_2C_9.(1 - e_H)$.
By Lemma 6.3 $\mathbb{F}_2C_9.e_H \simeq \mathbb{F}_2(C_9/C_3) \simeq \mathbb{F}_2C_3$. *And we know that* $\mathbb{F}_2C_3 \simeq \mathbb{F}_2 \oplus \mathbb{F}_{2^2}$.
Thus $\mathbb{F}_2C_9.e_H$ *(which is one of the summands of the decomposition) is isomorphic to* $\mathbb{F}_2 \oplus \mathbb{F}_{2^2}$ *and so* $\mathbb{F}_2C_9 \simeq \mathbb{F}_2 \oplus \mathbb{F}_{2^6} \oplus \mathbb{F}_{2^2}$.
The unit group is $C_{63} \times C_3$.

Lemma 6.5. *In a ring* R *with identity* I, I *is the only invertible idempotent.*

Proof. Clearly $I^2 = I$. Let e be an invertible idempotent. Then $e.e^{-1} = I$ $\Rightarrow e^2.e^{-1} = I$. Thus I is the only invertible idempotent.

Lemma 6.6. *In* $M_2(\mathbb{F}_q)$ *(where* $q = p^k$*) there are* $q^2 + q + 2$ *idempotents.*

Proof. Firstly, there is an identity element $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ which is an idempotent and by the previous lemma it is the only invertible idempotent.
Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be a non-invertible idempotent in $M_2(\mathbb{F}_q)$.
Then $A^2 = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a^2 + bc & ab + bd \\ ca + dc & cb + d^2 \end{bmatrix}$
This gives the following simultaneous equations:

(1) $a^2 + bc = a$,
(2) $ab + bd = b \Rightarrow b(a + d) = b$,
(3) $ca + dc = c \Rightarrow c(a + d) = c$,and
(4) $cb + d^2 = d$.
(5) $det(A) = 0 \Rightarrow ad = bc$.

The proof is now divided into 3 parts.

The first part looks at the case where both b and c are invertible. Solving

(2) above (using the cancellation laws) we get $a + d = 1 \Rightarrow d = 1 - a$.
Now if $a = 1 \Rightarrow d = 1 - 1 = 0 \Rightarrow ad = 0$ but this is not possible as $ad = bc \neq 0$, so we must have $a \neq 1$. Thus $a \notin \{0, 1\}$.
Thus there are $q - 2$ choices for a and then d is determined by the choice for a.
Now we have $ad = bc$ and so $adc^{-1} = b$, and for each value of $c \neq 0$ there is a unique value of b (because a, b, c and $d \in$ the group $(\mathbb{F}_p)^\times$).
Thus there are $q - 1$ choices for c, and b is then determined. This gives $(q - 2)(q - 1) = q^2 - 3q + 2$ choices for A when both b and c are invertible.

The second part of the proof covers the case where either b or c is zero (but not both). From either (2) or (3) we get $a + d = 1 \Rightarrow d = 1 - a$.
Also $bc = 0$ (as one of them is zero) $\Rightarrow ad = 0 \Rightarrow a$ or $d = 0$.
If $a = 0$ then $d = 1$. Likewise if $d = 0$ then $a = 1$, so a is either 0 or 1.
Now we can count the number of choices. If $b = 0$, then c has $q - 1$ choices (not 0). If $b \neq 0$, then $c = 0$. There are $q - 1$ ways that $b \neq 0$. So there are $q - 1 + q - 1 = 2q - 2$ choices for b and c. Finally, for each of these distinct choices, there are 2 choices for a (1 or 0) and d is determined by a. Thus there are $2(2q - 2) = 4q - 4$ choices when either b or $c = 0$.

The last part of the proof covers the case where b and c are both zero. We have $bc = 0$, and by equation (1) and (4) above, $a = a^2$ and $d = d^2$. So the only possiblilities for a and d are that they are 0 or 1. The product ad must be zero, and so there are only 3 possibilities. They are: $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$.

Thus the total number of non invertible idempotents is $q^2 - 3q + 2 + 4q - 4 + 3$ $= q^2 + q + 1$.
When we include the only invertible idempotent I, we have $q^2 + q + 2$ idempotents.

Example 6.7. *In $M_2(\mathbb{F}_3)$ there are $3^2 + 3 + 2 = 14$ idempotents.*

These 14 idempotents can be divided into the three types plus the identity as per Lemma 6.6 writing each matrix in the form $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

The $3^2 - 3(3) + 2 = 2$ *matrices where* b *and* c *are units:* $\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix}$

The 4(3) - 4 = 8 matrices where one of b, c *is zero:*

$$\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 2 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 2 & 1 \end{bmatrix}$$

The 3 matrices where both b *and* c *are zero:* $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

The identity matrix $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Example 6.8. *In* $M_2(\mathbb{F}_{3^2})$ *there are* $9^2 + 9 + 2 = 92$ *idempotents.*

Corollary 6.9. *There are an infinite number of idempotents in* $M_2(F)$ *where* F *is an infinite field.*

Proof. Take the first case in Lemma 6.6 where b and c are both invertible. For the matrix to be an idempotent, the only limitation on a is that $a \neq 0$ or 1. Thus there are an infinite number of choices for a and an infinite number of idempotents.

6.1 Field Automorphisms

Definition A ring homomorphism f is a mapping from R_1 to R_2 such that for all α and $\beta \in R_1$,

$f(\alpha + \beta) = f(\alpha) + f(\beta)$ and $f(\alpha.\beta) = f(\alpha).f(\beta)$

Note that a field homomorphism is a ring homomorphism where R_1 and R_2 are fields. A field homomorphism which is an epimorphism and a monomorphism is a field isomorphism.

Definition [13] Let K be a field. An isomorphism σ of K with itself is called an *automorphism* of K. The collection of automorphisms of K is denoted $Aut(K)$. An automorphism σ is said to fix an element $\alpha \in K$ if $\sigma\alpha = \alpha$. If F is a subfield of K then an automorphism of K is said to fix F if it fixes all the elements of F.

Note that the prime subfield of any field is the field generated by $1 \in K$, and any automorphism σ takes 1 to 1 and so σ fixes all of the elements of the prime subfield. Hence any automorphism of K fixes its prime subfield. Thus F_p has only the trivial automorphism.

Definition [13] Let K/F be an extension of fields. The collection of automorphisms of K which fix F is denoted by $Aut(K/F)$.

Note that if F is the prime subfield of K then $Aut(K/F) = Aut(K)$. Also the collection of automorphisms forms a group as they contain the identity, are invertible and closed under composition. In general $Aut(K/F) < Aut(K)$.

Definition [13] The *degree* of a field extension K/F, denoted $[K : F]$, is the dimension of K as a vector space over F (i.e.$[K : F] = dim_F K$).

Definition [13] K is said to be *Galois* over F and K/F is a *Galois extension* if $|Aut(K/F)|$ is equal to the degree of F in K. If K/F is Galois the group $Aut(K/F)$ is called the *Galois group* of K/F and is denoted by $Gal(K/F)$.

Definition [13] The extension field K of F is called a *splitting field* for the polynomial $f(x) \in F[x]$ if $f(x)$ factors into linear factors (or *splits completely*) in $K[x]$ and $f(x)$ does not factor completely into linear factors over any proper subfield of K containing F.

Definition [13] A polynomial over F is called *separable* if it has no multiple roots.

Proposition 6.10. *[13] Let K be the splitting field over F of the polynomial $f(x) \in F[x]$. Then $|Aut(K/F)| \leq [K : F]$ with equality if $f(x)$ is separable over F.*

Note the extension of finite fields $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois since $\mathbb{F}_{p^n}$ is the splitting field over $\mathbb{F}_p$ of the separable polynomial $x^{p^n} - x$ [13]. Thus there are n automorphisms of $\mathbb{F}_{p^n}/\mathbb{F}_p$.

Definition [13] Let K/F be a Galois extension. If $\alpha \in K$ the elements $\sigma(\alpha)$ for σ in $Gal(K/F)$ are called the *conjugates* (or *Galois conjugates*) of α over F.

Definition [13] The injective homomorphism $\sigma : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ defined by $\alpha \mapsto \alpha^p$ is surjective since $\mathbb{F}_{p^n}$ is finite and so is an isomorphism, and thus an automorphism. It is called the *Frobenius* automorphism, which is denoted by σ_p. Iterating σ_p gives $\sigma_p^2(\alpha) = \sigma_p(\sigma_p(\alpha)) = (\alpha^p)^p = \alpha^{p^2}$.
Similarly $\sigma_p^i(\alpha) = \alpha^{p^i}$ $i = 0, 1, 2, ...$
Since $\sigma_p^n(\alpha) = \alpha^{p^n} = \alpha$, $\sigma_p^n = 1$ the identity automorphism. No lower power of α^p can be the identity, since this would imply that $\sigma_p^i(\alpha) = \alpha$ for some $i < n$, which is impossible since there are at most p^i roots of this equation. Thus σ_p has order $n = |Aut(K/F)|$, and so $Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is cyclic of order n with the Frobenius automorphism as the generator.

Definition [13] Let K/F be a field extension and let α be an element of K. The field trace of α from K to F is

$tr_{K/F}(\alpha) = \sum_\sigma \sigma(\alpha)$,

the sum of Galois conjugates of α.

Lemma 6.11. *Let α be an element of $\mathbb{F}_{p^n}$. Then $tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^n}}(\alpha) = \alpha$.*

Proof. The extension $\mathbb{F}_{p^n}/\mathbb{F}_{p^n}$ has only the trivial automorphism, so the sum of the Galois conjugates is equal to the element itself.

Definition [13] Let α be an element of K and let $[K : F] = n$. Consider K as a vector space over F. Define by T_α the action of α on K by left multiplication. T_α is an $F - linear$ map (ie $T_\alpha(x + y) = T_\alpha(x) + T_\alpha(y)$ and $T_\alpha(ax) = aT_\alpha(x)\ \forall\ x, y \in K$ and $a \in F$). The field trace $tr_{K/F}(\alpha)$ is equal to the trace of the $n \times n$ matrix of the $F - linear$ map T_α. This explains the use of the term trace for both maps.

We illustrate the equivalence of the two trace maps with the following example.

Example 6.12. *Consider the group algebra $\mathbb{F}_2C_7$. The field extension $\mathbb{F}_2(\zeta_7)$ containing a primitive 7^{th} root of unity is $\mathbb{F}_{2^3}$. The elements of $\mathbb{F}_{2^3}$ are $0, 1, a, a^2, 1+a, 1+a^2, a+a^2, 1+a+a^2$ with a as a primitive 7^{th} root of unity. This field extension can be considered as a 3-dimensional vector space over $\mathbb{F}_2$ with basis elements 1, a, a^2.*
A prime polynomial of degree 3 over the field $\mathbb{F}_2$ is $p(x) = x^3 + x + 1$, and taking a to be a root of this polynomial we see that the basis elements of the extension field containing this root are a^0, a^1, a^2 which are 1, a, a^2. Because a is a root of $p(x)$ we also get that $a^3 = a + 1$.
Let σ be the Frobenius automorphism so

$\sigma a = a^2.$
$\sigma^2 a = a^4 = aa^3 = a(1 + a) = a + a^2.$
$\sigma^3 a = a^8 = a.$

Thus the field trace of a from $\mathbb{F}_{2^3}$ to $\mathbb{F}_2$ is:

$tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(a) = a^2 + a + a^2 + a = 0.$

The 3×3 matrix of the linear map T_a is found by checking what the image of the 3 basis elements are. If we write the 3 basis elements as column vectors they are $1 = (1, 0, 0)^T$, $a = (0, 1, 0)^T$ and $a^2 = (0, 0, 1)^T$.

$a.1 = a = (0,1,0)^T$.

$a.a = a^2 = (0,0,1)^T$.

$a.a^2 = a^3 = 1 + a = (1,1,0)^T$.

The 3×3 *matrix of* $T_a = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$.

We can see that the trace of this matrix is 0.

Thus $tr(T_a) = tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(a) = 0$.

Lemma 6.13. *[13] Let* K *be a finite field extension of* F*. The field trace of* K *over* F *is a map from a field* K *to the subfield* F*.*

6.2 Group Representations and Group Characters

This section gives some preliminary results which allow the Artin-Wedderburn decomposition of FG (and hence $U(FG)$) to be found in the next section for all semisimple FG with G abelian.
To begin with it is necessary to establish the basic notation used in this section, and to define some terms.

Definition *[19] Let G be a group and F a field. A representation of G over F is a homomorphism μ from G to $GL_n(F)$. The degree of μ is the integer n. We use μg to denote the image of g in $GL_n(F)$.*

Definition *[19] Let V be a vector space over F and let G be a group. Then V is an $FG-$module if a multiplication gv ($g \in G$, $v \in V$) is defined, satisfying the following conditions for all $g, h \in G$, u, $v \in V$, and $\lambda \in F$:*

(1) $gv \in V$;
(2) $(gh)v = g(hv)$
(3) $1v = v$
(4) $\lambda(gv) = g(\lambda v)$
(5) $g(u+v) = gu + gv$

Note that conditions (1), (4) and (5) ensure that for all $g \in G$, the function $v \to gv$ is a linear transformation from V to itself and is thus an endomorphism of V.

Definition *[19] Let V be an $FG-$module, and let β be a basis of V. For each $g \in G$ let $[g]_\beta$ denote the matrix of the endomorphism $v \to gv$ of V, relative to the basis β.*

The connection between FG-modules and representations of G over F is revealed in the following result.

Theorem 6.14. *[19]*
(1) If $\mu : G \to GL_n(F)$ is a representation of G over F, and $V = F^n$, then V becomes an $FG-$module if we define the multiplication gv by

$gv = (\mu g)v$

Moreover, there is a basis β of V such that $\mu g = [g]_\beta$ for all $g \in G$.

(2) Assume that V is an $FG-$module and let β be a basis of V. Then the function

$g \to [g]_\beta$ *is a representation of G over F.*

Definition *An $FG-$module V is said to be irreducible if it is non-zero and it has no $FG-$submodules apart from 0 and V.*
Similarly, a representation $\mu : G \to GL_n(F)$ is irreducible if the corresponding $FG-$module F^n given by $gv = (\mu g)v$ is irreducible.

Definition *Suppose that V is an $FG-$module with a basis β. Then the character of V is the function $\chi : G \to F$ defined by*

$\chi(g) = tr[g]_\beta$ *$(g \in G)$.*

We say that χ is a character of G if χ is the character of some $FG-$module. Further, χ is an irreducible character of G if χ is the character of an irreducible $FG-$module.

We now use all of these ideas in the following section which will allow us to find the Wedderburn decomposition of FG for G abelian and also the primitive central orthogonal idempotents associated with each summand of the Wedderburn decomposition. By finding the decomposition, it will also be possible to find the structure of the unit group.

6.3 Cyclotomic Classes of G and the Primitive Central Orthogonal Idempotents of FG

Definition *[6] Let $|G| = n$ and $|F| = q$. Let the algebraic closure of F be denoted by $\hat{F}$. For every positive integer k coprime with q, ζ_k denotes a primitive k^{th} root of unity in $\hat{F}$ and $o_k = o_k(q)$ denotes the multiplicative order of $q(mod\ k)$.*

Lemma 6.15. *[6] The field extension $\mathbb{F}_q(\zeta_k)$ is $\mathbb{F}_{q^{o_k}}$.*

Let $g \in G$. The group $(\mathbb{Z}/n\mathbb{Z})^\times$ acts on G by $m \cdot g = g^m$. Let Q denote the subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ generated by q and consider Q acting on G by restriction of the previous action.

Definition *[6] The q-cyclotomic classes of G are the orbits of the elements of G under the action of Q on G. Denote by $C_q(g)$ the q-cyclotomic class containing g.*

$C_q(g) = \{g, g^q, g^{q^2}, ..., g^{q^o-1}\}$ where o is the multiplicative order of q mod n.

Definition *Let G be a cyclic group. The set G^* of irreducible characters of G is a group with the product: $(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g)$, for $\chi_1, \chi_2 \in G^*$ and $g \in G$.*

Note that these characters are taken over $\hat{F}$. Furthermore G^* and G are isomorphic and in particular G^* is cyclic and the generators of G^* are precisely the faithful representations of G.

Definition *[6] If G is cyclic, then let $C(G) = C_q(G)$ denote the q-cyclotomic classes of G^* that contain generators of G^*.*

Let $N \lhd G$ such that G/N is cyclic of order k and $C \in C_q(G/N)$.
If $\chi \in C$ then define

$\epsilon_C(G, N) = |G|^{-1} \sum_{g \in G} tr_{F(\zeta_k)/F}(\chi(\bar{g}))g^{-1}$

where $\bar{g}$ denotes the image of g in G/N.

Definition *[28] Let $R = \sum_{i=1}^{t} A_i$ be a decomposition of a semisimple ring as a direct sum of minimal two-sided ideals. Then there exists a family $\{e_1, e_2, ..., e_t\}$ of elements of R (with $A_i = Re_i = e_iR$), such that*

(i) e_i is a central idempotent.

(ii) If $i \neq j$ then $e_ie_j = 0$ (i.e. they are orthogonal).

(iii) $1 = e_1 + ... + e_t$.

(iv) e_i cannot be written as $e_i = e_j + e_k$ where e_j, e_k are non-zero central orthogonal idempotents.

The elements $\{e_1, e_2, ..., e_t\}$ defined above are called the primitive central orthogonal idempotents of R.

Lemma 6.16. *Let N be the trivial normal subgroup G of G. Then the primitive central idempotent associated with G/G is $e_G = |G|^{-1}\hat{G}$.*

Proof. The quotient group G/G contains only the trivial element and thus has only one irreducible character (the trivial character). Also the degree of the normal subgroup is 1, which is in the prime field, so the Galois group of automorphisms is just the trivial group and the trace is just the element itself. Thus

$\epsilon_C(G, G) = |G|^{-1} \sum_{g \in G} tr_{F(1)/F}(\chi(1))g^{-1} = |G|^{-1} \sum_{g \in G}(1)g^{-1} = |G|^{-1}\hat{G} = e_G$.

The following Theorem from Broche and del Rio gives a method for finding the Wedderburn decomposition of a group algebra where the characteristic of the field does not divide the order of G. Not only that but it also gives a method for finding the primitive central orthogonal idempotents associated with each summand. This technique is illustrated with a number of examples.

Theorem 6.17. *(Broche and del Rio) [6] If G is a finite abelian group of order n and F is a finite field of order q such that (q,n) = 1, the the map $(N, C) \rightarrow \epsilon_C(G, N)$ is a bijection from the set of pairs (N, C) with $N \triangleleft G$ such that G/N is cyclic of order k and $C \in C_q(G/N)$ to the set of primitive central*

idempotents of FG. Further for every $N \triangleleft G$ and $C \in C_q(G/N)$, $FG\epsilon_C(G,N)$ $\simeq F(\zeta_k)$ where $k = |G/N|$. Further, $\epsilon_C(G,N)$ does not depend on the choice of $\chi \in C$.

In other words, for each normal subgroup which has a cyclic quotient, and for each cyclotomic class which contains a generator of G^*, there is a summand in the Wedderburn decomposition, and this summand is isomorphic to $F(\zeta_k)$ where $k = |G/N|$. This technique not only finds the primitive central orthogonal idempotents associated with each summand, but it also gives us the Wedderburn decomposition.

Example 6.18. $\mathbb{F}_2C_3$. *$q = 2$ and $n = 3$.*
There are two normal subgroups with cyclic quotients, $H_1 \simeq C_1$ and $H_2 \simeq C_3$, giving $k = |G/H_1| = 3$ and $k = |G/H_2| = 1$ respectively.
If $k = 3$, then $F(\zeta_3) = \mathbb{F}_{2^{O_3}} = \mathbb{F}_{2^2}$ because the order of q (mod 3) is 2. i.e $q^2 = 2^2 = 1$ (mod 3).
If $k = 1$, then $F(\zeta_1) = \mathbb{F}_2$ because the primitive 1st root is the generator of the prime subfield.

The primitive central orthogonal idempotents are the blocks of the decomposition and are found using Broche and Del Rio's method as follows:

$G/H_1 \simeq C_3$. The table of irreducible characters of C_3 is as follows:

classes:	1	x	x^2
sizes :	1	1	1
χ_1	1	1	1
χ_2	1	ζ	ζ^2
χ_3	1	ζ^2	ζ

where ζ is a primitive cube root of unity in $\mathbb{F}_{2^2}$.

The group $(G/H_1)^*$ of irreducible characters of G/H_1 is $\{\chi_1, \chi_2, \chi_3\}$ with generator χ_2.
The group $(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/3\mathbb{Z})^\times = \{1,2\}$ acts on $(G/H_1)^*$ by $m \cdot g = g^m$.
Q is the subgroup of $(\mathbb{Z}/3\mathbb{Z})^\times$ generated by $q = 2$ and so $Q = \{1,2\}$. The

orbits of the elements of $(G/H_1)^*$ *under the action of* Q *on* $(G/H_1)^*$ *are* $\{\chi_1\}$ *and* $\{\chi_2, \chi_3\}$. *Of these two classes only* $\{\chi_2, \chi_3\}$ *contains a generator of* $(G/H_1)^*$ *and so this class is* $C(G/H_1)$.

Choosing χ_2 *as the character in* $C(G/H_1)$, *the primitive central idempotent associated with the summand* $\mathbb{F}_{2^2}$ *is*

$$\epsilon_C(G, H_1) = |G|^{-1} \sum_{g \in G} tr_{\mathbb{F}_{2^2}/\mathbb{F}_2}(\chi(\bar{g}))g^{-1}$$

$$= 1[tr_{\mathbb{F}_{2^2}/\mathbb{F}_2}(\chi_2(1))1 + tr_{\mathbb{F}_{2^2}/\mathbb{F}_2}(\chi_2(x))x^2 + tr_{\mathbb{F}_{2^2}/\mathbb{F}_2}(\chi_2(x^2))x]$$

$$= 1[tr_{\mathbb{F}_{2^2}/\mathbb{F}_2}(1)1 + tr_{\mathbb{F}_{2^2}/\mathbb{F}_2}(\zeta)x^2 + tr_{\mathbb{F}_{2^2}/\mathbb{F}_2}(\zeta^2)x]$$

Note that the Galois group, $Gal(\mathbb{F}_{2^2}/\mathbb{F}_2) \simeq C_2$ *and the only non trivial automorphism is the Frobenius automorphism* σ *which maps* α *to* α^2. *Thus the field trace of each of the above elements is the sum of both of their Galois conjugates.*
$tr_{\mathbb{F}_{2^2}/\mathbb{F}_2}(1) = 1+1 = 0$ *(as 1 is mapped to itself under both* σ *and* σ^2 *- the identity automorphism).*
$tr_{\mathbb{F}_{2^2}/\mathbb{F}_2}(\zeta) = \zeta + \zeta^2$. *Here* ζ *is a primitive cube root in the field* $\mathbb{F}_{2^2}$. *This field has elements* $\{0, 1, a, 1+a\}$ *where* $a^2 = 1 + a$ *and* $a^3 = a + 1 + a = 1$. *Thus the element* a *has order 3 so define* $\zeta = a$ *and* $\zeta^2 = 1 + a$.
Thus $tr_{\mathbb{F}_{2^2}/\mathbb{F}_2}(\zeta) = \zeta + \zeta^2 = a + 1 + a = 1$.
$tr_{\mathbb{F}_{2^2}/\mathbb{F}_2}(\zeta^2) = \zeta^2 + \zeta = 1$.

So $\epsilon_C(G, H_1) = 1[(0)1 + (1)x^2 + (1)x] = x + x^2$.

For $H_2 = G$, *the primitive central idempotent is* e_G *by Lemma 6.16.*

$\epsilon_C(G, H_2) = e_G = 1[1 + x + x^2]$.

So the two central primitive orthogonal idempotents of $\mathbb{F}_2C_3 \simeq \mathbb{F}_{2^2} \oplus \mathbb{F}_2$ *are* $x + x^2$ *and* $1 + x + x^2$ *which correspond to* $1 - e_G$ *and* e_G. *As there are just the two pairs* $(H_1, C(G/H_1))$ *and* $(H_2, C(G/H_2))$ *we see that by Theorem 6.17 the Wedderburn decomposition of* $\mathbb{F}_2C_3$ *is* $\mathbb{F}_{2^2} \oplus \mathbb{F}_2$ *and the unit group is* C_3.

Example 6.19. $\mathbb{F}_{2^2}C_3$. $q = 4$ *and* $n = 3$. *Let* $\mathbb{F}_{2^2} = \{0, 1, a, 1 + a\}$.
Again there are two normal subgroups, $H_1 \simeq C_1$ *and* $H_2 \simeq C_3$, *giving* $k =$

$|G/H_1| = 3$ and $k = |G/H_2| = 1$ respectively.
If $k = 3$, then $F(\zeta_3) = \mathbb{F}_{(2^2)^1} = \mathbb{F}_{2^2}$ because the order of 4 (mod 3) is 1.
If $k = 1$, then $F(\zeta_1) = \mathbb{F}_{2^2}$ because the primitive 1st root is the generator of the prime subfield.

$G/H_1 \simeq C_3$. The table of irreducible characters of C_3 is as follows:

classes:	1	x	x^2
sizes :	1	1	1
χ_1	1	1	1
χ_2	1	ζ	ζ^2
χ_3	1	ζ^2	ζ

where ζ is a primitive cube root of unity in $\mathbb{F}_{2^2}$. Define $\zeta = a$.

The group $(G/H_1)^*$ of irreducible characters of G/H_1 is $\{\chi_1, \chi_2, \chi_3\}$ with generators χ_2 and χ_3.
The group $(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/3\mathbb{Z})^\times = \{1, 2\}$ acts on $(G/H_1)^*$ by $m \cdot g = g^m$.
Q is the subgroup of $(\mathbb{Z}/3\mathbb{Z})^\times$ generated by $q = 4 \equiv 1$(mod 3) and so $Q = \{1\}$.
The orbits of the elements of $(G/H_1)^*$ under the action of Q on $(G/H_1)^*$ are $\{\chi_1\}$, $\{\chi_2\}$ and $\{\chi_3\}$.
Of these classes both $\{\chi_2\}$ and $\{\chi_3\}$ contain a generator of $(G/H_1)^*$ and so we label them $C_1(G/H_1)$ and $C_2(G/H_1)$ respectively.

$$\epsilon_{C_1}(G, H_1) = |G|^{-1} \sum_{g \in G} tr_{\mathbb{F}_{2^2}/\mathbb{F}_{2^2}}(\chi(\bar{g}))g^{-1}$$

$$= 1[tr_{\mathbb{F}_{2^2}/\mathbb{F}_{2^2}}(\chi_2(1))1 + tr_{\mathbb{F}_{2^2}/\mathbb{F}_{2^2}}(\chi_2(x))x^2 + tr_{\mathbb{F}_{2^2}/\mathbb{F}_{2^2}}(\chi_2(x^2))x]$$

$$= 1[tr_{\mathbb{F}_{2^2}/\mathbb{F}_{2^2}}(1)1 + tr_{\mathbb{F}_{2^2}/\mathbb{F}_{2^2}}(\zeta)x^2 + tr_{\mathbb{F}_{2^2}/\mathbb{F}_{2^2}}(\zeta^2)x]$$

Note that the Galois group, $Gal(\mathbb{F}_{2^2}/\mathbb{F}_{2^2}) \simeq C_1$ and so only the trivial automorphism applies. Thus the field trace of each of the above elements is the element itself.

So $\epsilon_{C_1}(G, H_1) = 1[(1)1 + (a)x^2 + (1+a)x] = 1 + (1+a)x + ax^2$. This primitive central idempotent generates the first summand $\mathbb{F}_{2^2}$.

$\epsilon_{C_2}(G, H_1) = 1[tr_{\mathbb{F}_{2^2}/\mathbb{F}_{2^2}}(\chi_3(1))1 + tr_{\mathbb{F}_{2^2}/\mathbb{F}_{2^2}}(\chi_3(x))x^2 + tr_{\mathbb{F}_{2^2}/\mathbb{F}_{2^2}}(\chi_3(x^2))x]$

$= 1[tr_{\mathbb{F}_{2^2}/\mathbb{F}_{2^2}}(1)1 + tr_{\mathbb{F}_{2^2}/\mathbb{F}_{2^2}}(\zeta^2)x^2 + tr_{\mathbb{F}_{2^2}/\mathbb{F}_{2^2}}(\zeta)x]$

$= 1[(1)1 + (1+a)x^2 + ax] = 1 + ax + (1+a)x^2$. *This primitive central idempotent generates the second summand* $\mathbb{F}_{2^2}$.

For $H_2 = G$, *the primitive central idempotent is* e_G *by Lemma 6.16.*

$\epsilon_C(G, H_2) = e_G = 1[1 + x + x^2]$ *and this element generates the third and final summand* $\mathbb{F}_{2^2}$

Thus we see that by Theorem 6.17 the Wedderburn decomposition of $\mathbb{F}_{2^2}C_3$ *is* $\bigoplus_{i=1}^{3} \mathbb{F}_{2^2}$ *and the unit group is* C_3^3.

Example 6.20. $\mathbb{F}_2C_5$. *q = 2 and* $n = 5$.
There are two normal subgroups, $H_1 \simeq C_1$ *and* $H_2 \simeq C_5$, *giving* $k = |G/H_1|$ *= 5 and* $k = |G/H_2|$ *= 1 respectively.*
If k = 5, then $F(\zeta_5) = \mathbb{F}_{2^{O_5}} = \mathbb{F}_{2^4}$ *because the order of q(mod 5) is 4. i.e* q^4 $= 2^4 \equiv 1(mod\ 5)$.
If k = 1, then $F(\zeta_1) = \mathbb{F}_2$ *because the primitive* 1^{st} *root is the generator of the prime subfield.*

$G/H_1 \simeq C_5$. *The table of irreducible characters of* C_5 *is:*

classes:	1	x	x^2	x^3	x^4
sizes :	1	1	1	1	1
χ_1	1	1	1	1	1
χ_2	1	ζ	ζ^2	ζ^3	ζ^4
χ_3	1	ζ^2	ζ^4	ζ	ζ^3
χ_4	1	ζ^3	ζ	ζ^4	ζ^2
χ_5	1	ζ^4	ζ^3	ζ^2	ζ

where ζ *is a primitive* 5^{th} *root of unity in* $\mathbb{F}_{2^4}$.

The group $(G/H_1)^*$ *of irreducible characters of* G/H_1 *is* $\{\chi_1, \chi_2, \chi_3, \chi_4, \chi_5\}$ *with all of the elements being a generator except* χ_1.

The group $(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/5\mathbb{Z})^\times = \{1,2,3,4\}$ *acts on* $(G/H_1)^*$ *by* $m \cdot g = g^m$.
Q *is the subgroup of* $(\mathbb{Z}/5\mathbb{Z})^\times$ *generated by* $q = 2$ *and so* $Q = \{2,4,3,1\}$.
Now $\chi_2^2 = \chi_2\chi_2(x) = \chi_2(x)\chi_2(x) = \zeta\zeta = \zeta^2 = \chi_3(x)$.
Similarly, $\chi_2^4 = \chi_5$, $\chi_2^3 = \chi_4$ *and* $\chi_2^1 = \chi_2$.
Thus the orbits of the elements of $(G/H_1)^*$ *under the action of* Q *on* $(G/H_1)^*$ *are* $\{\chi_1\}$ *and* $\{\chi_2, \chi_3\, \chi_4, \chi_5\}$ *with only the second class containing a generator so this class is* $C(G/H_1)$.

Choosing χ_2 *as the character from* $C(G/H_1)$, *the primitive central idempotent associated with the summand* $\mathbb{F}_{2^4}$ *is*

$$\epsilon_C(G,H_1) = 1[tr_{\mathbb{F}_{2^4}/\mathbb{F}_2}(1)1 + tr_{\mathbb{F}_{2^4}/\mathbb{F}_2}(\zeta)x^4 + tr_{\mathbb{F}_{2^4}/\mathbb{F}_2}(\zeta^2)x^3 + tr_{\mathbb{F}_{2^4}/\mathbb{F}_2}(\zeta^3)x^2 + tr(\zeta^4)x]$$

The group of automorphisms $Gal(\mathbb{F}_{2^4}/\mathbb{F}_2) \simeq C_4$ *with the Frobenius automorphism* σ *which maps* α *to* α^2 *as the generator. Thus the field trace of each of the above elements is the sum of all four of their Galois conjugates.*
$tr_{\mathbb{F}_{2^4}/\mathbb{F}_2}(1) = 1+1+1+1 = 0$
$tr_{\mathbb{F}_{2^4}/\mathbb{F}_2}(\zeta) = \zeta + \zeta^2 + \zeta^3 + \zeta^4$.
Here ζ *is a primitive 5th root in* $\mathbb{F}_{2^4}$, *the field formed by the ring quotient* $\frac{\mathbb{F}_2[x]}{p(x)}$ *where* $p(x)$ *is the irreducible polynomial* $x^4 + x + 1$. *In this field the element* a^3 *has order 5 and so we set* $\zeta = a^3$.
It follows that $\zeta^2 = a^3 + a^2$, $\zeta^3 = a^3 + a$ *and* $\zeta^4 = a^3 + a^2 + a + 1$.
Thus $tr_{\mathbb{F}_{2^4}/\mathbb{F}_2}(\zeta) = \zeta + \zeta^2 + \zeta^3 + \zeta^4$
$= a^3 + (a^3 + a^2) + (a^3 + a) + a^3 + a^2 + a + 1 = 1$.
Similarly $tr_{\mathbb{F}_{2^4}/\mathbb{F}_2}(\zeta^2) = tr_{\mathbb{F}_{2^4}/\mathbb{F}_2}(\zeta^3) = tr_{\mathbb{F}_{2^4}/\mathbb{F}_2}(\zeta^4) = 1$.

So $\epsilon_C(G,H_1) = 1[(0)1 + (1)x^4 + (1)x^3 + (1)x^2 + (1)x] = x + x^2 + x^3 + x^4$.

For $H_2 = G = C_5$, *the primitive central idempotent is* $\epsilon_C(G,G) = e_G = 1 + x + x^2 + x^3 + x^4$ *by Lemma 6.16.*

Again there are only the two pairs $(H_1, C(G/H_1))$ *and* $(H_2, C(G/H_2))$ *and by Theorem 6.17 the Wedderburn decomposition of* $\mathbb{F}_2C_5$ *is* $\mathbb{F}_{2^4} \oplus \mathbb{F}_2$ *and the unit group is* C_{15}. *The two central primitive orthogonal idempotents are*

$x+x^2+x^3+x^4$ *and* $1+x+x^2+x^3+x^4$ *which again correspond to* $1-e_G$ *and* e_G*. When there are only two summands in the decomposition this is always going to be the case. Next we examine another case where there are more than two summands.*

Example 6.21. $\mathbb{F}_2C_7$*.* $q = 2$ *and* $n = 7$*.*
There are two normal subgroups, $H_1 \simeq C_1$ *and* $H_2 \simeq C_7$*, giving* $k = |G/H_1|$ $= 7$ *and* $k = |G/H_2| = 1$ *respectively.*
If $k = 7$*, then* $F(\zeta_7) = \mathbb{F}_{2^{O_7}} = \mathbb{F}_{2^3}$ *because the order of* q *(mod 7) is 3. i.e* q^3 $= 2^3 = 1$*(mod 7).*
If $k = 1$*, then* $F(\zeta_1) = \mathbb{F}_2$ *because the primitive* 1^{st} *root is in the prime subfield.*

$G/H_1 \simeq C_7$*. The table of irreducible characters of* C_7 *is:*

classes:	1	x	x^2	x^3	x^4	x^5	x^6
sizes :	1	1	1	1	1	1	1
χ_1	1	1	1	1	1	1	1
χ_2	1	ζ	ζ^2	ζ^3	ζ^4	ζ^5	ζ^6
χ_3	1	ζ^2	ζ^4	ζ^6	ζ	ζ^3	ζ^5
χ_4	1	ζ^3	ζ^6	ζ^2	ζ^5	ζ	ζ^4
χ_5	1	ζ^4	ζ	ζ^5	ζ^2	ζ^6	ζ^3
χ_6	1	ζ^5	ζ^3	ζ	ζ^6	ζ^4	ζ^2
χ_7	1	ζ^6	ζ^5	ζ^4	ζ^3	ζ^2	ζ

where ζ *is a primitive* 7^{th} *root of unity in* $\mathbb{F}_{2^3}$*.*

The group $(G/H_1)^*$ *of irreducible characters of* G/H_1 *is* $\{\chi_1, \chi_2, \chi_3, \chi_4, \chi_5, \chi_6, \chi_7\}$ *with all of the elements being a generator except* χ_1*.*
The group $(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/7\mathbb{Z})^\times = \{1, 2, 3, 4, 5, 6\}$ *acts on* $(G/H_1)^*$ *by* $m \cdot g$ $= g^m$*.*
Q *is the subgroup of* $(\mathbb{Z}/7\mathbb{Z})^\times$ *generated by* $q = 2$ *and so* $Q = \{2, 4, 1\}$*. Now* $\chi_2^2(x) = \chi_3(x)$*. Similarly,* $\chi_2^4 = \chi_5$ *and* $\chi_2^1 = \chi_2$*.* $\chi_4^2(x) = \chi_7(x)$*. Similarly,* $\chi_4^4 = \chi_6$ *and* $\chi_4^1 = \chi_4$*. Thus the orbits of the elements of* $(G/H_1)^*$ *under the*

action of Q *on* $(G/H_1)^*$ *are* $\{\chi_1\}$, $\{\chi_2, \chi_3\ , \chi_5\}$ *and* $\{\chi_4, \chi_7\ , \chi_6\}$.
This time there are two classes containing generators so we label them $C_1(G/H_1)$ $= \{\chi_2, \chi_3\ , \chi_5\}$ *and* $C_2(G/H_1) = \{\chi_4, \chi_7\ , \chi_6\}$.
Thus there are two pairs (H_1, C_1) *and* (H_1, C_2) *and so by Theorem 6.17 there are two summands isomorphic to* $\mathbb{F}_{2^3}$ *in the Wedderburn decomposition. The other summand is* $\mathbb{F}_2$ *which corresponds to the pair* $(H_2, C(G/G))$. *Thus the total decomposition of* $\mathbb{F}_2C_7$ *is* $\mathbb{F}_2 \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{2^3}$.

We can find the three primitive central orthogonal idempotents now. Choosing χ_2 *as the character from* $C_1(G/H_1)$, *we get*

$$\epsilon_{C_1}(G, H_1) = 1[tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\chi_2(1))1 + tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\chi_2(x))x^6 + tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\chi_2(x^2))x^5 + tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\chi_2(x^3))x^4 + tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\chi_2(x^4))x^3 + tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\chi_2(x^5))x^2 + tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\chi_2(x^6))x]$$

$$= 1[tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(1)1 + tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\zeta)x^6 + tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\zeta^2)x^5 + tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\zeta^3)x^4 + tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\zeta^4)x^3 + tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\zeta^5)x^2 + tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\zeta^6)x]$$

The group of automorphisms $Gal(\mathbb{F}_{2^3}/\mathbb{F}_2)$ *is isomorphic to* C_3 *with the Frobenius automorphism* σ *which maps* α *to* α^2 *as the generator. Thus the field trace of each of the above elements is the sum of the three Galois conjugates.*
$tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(1) = 1+1+1 = 1$
$tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\zeta) = \zeta + \zeta^2 + \zeta^4$.
Here ζ *is a primitive 7th root in* $\mathbb{F}_{2^3}$, *the field formed by the ring quotient* $\frac{\mathbb{F}_2[x]}{p(x)}$ *where p(x) is the irreducible polynomial* $x^3 + x + 1$. *In this field the element a has order 7 and so we set* $\zeta = a$. *It follows that* $\zeta^2 = a^2$ *and* $\zeta^4 = a + a^2$.
Thus $tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\zeta) = \zeta + \zeta^2 + \zeta^4$
$= a + (a^2) + (a + a^2) = 0$.
Similarly $tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\zeta^2) = tr(\zeta^4) = 0$.
Now $\sigma(1 + a) = 1 + a^2$, $\sigma^2(1 + a) = 1 + a + a^2$ *and* $\sigma^3(1 + a) = 1 + a$.
Thus $tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\zeta^3) = (1 + a) + (1 + a^2) + (1 + a + a^2) = 1$.
Similarly $tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\zeta^6) = tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\zeta^5) = 1$.

So $\epsilon_{C_1}(G, H_1) = 1[(1)1 + (0)x^6 + (0)x^5 + (1)x^4 + (0)x^3 + (1)x^2 + (1)x] = 1 + x + x^2 + x^4$.

Choosing χ_4 *as the character from* $C_2(G/H_1)$, *we get*

$\epsilon_{C_2}(G, H_1) = 1[tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\chi_4(1))1 + tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\chi_4(x))x^6 + tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\chi_4(x^2))x^5 + tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\chi_4(x^3))x^4 + tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\chi_4(x^4))x^3 + tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\chi_4(x^5))x^2 + tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\chi_4(x^6))x]$

$= 1[tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(1)1 + tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\zeta^3)x^6 + tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\zeta^6)x^5 + tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\zeta^2)x^4 + tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\zeta^5)x^3 + tr_{\mathbb{F}_{2^3}/\mathbb{F}_2}(\zeta)x^2 + tr(\zeta^4)x]$

$= 1[(1)1 + (1)x^6 + (1)x^5 + (0)x^4 + (1)x^3 + (0)x^2 + (0)x] = 1 + x^3 + x^5 + x^6$.
This is the idempotent associated with the second summand isomorphic to $\mathbb{F}_{2^3}$

For $H_2 = G = C_7$, *there is only one q-cyclotomic class* C *and thus only one summand. The primitive central idempotent is* $\epsilon_C(G, G) = e_G = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6$ *by Lemma 6.16.*

The three central primitive orthogonal idempotents of $\mathbb{F}_2C_7 \simeq \bigoplus_{i=1}^{2} \mathbb{F}_{2^3} \oplus \mathbb{F}_2$ *are* $1 + x^2 + x^4$, $1 + x^3 + x^5 + x^6$ *and* $1 + x + x^2 + x^3 + x^4 + x^5 + x^6$ *generating the summands* $\mathbb{F}_{2^3}$, $\mathbb{F}_{2^3}$ *and* $\mathbb{F}_2$ *respectively.*

If we take a close look at the elements of the direct sum of the two summands generated by the idempotents $1 + x^3 + x^5 + x^6$ *and* $1 + x + x^2 + x^3 + x^4 + x^5 + x^6$, *we will see that there is an isomorphism between this direct sum and the codewords of the Hamming (7,4,3) Code that we encountered in Example 1.12. The idempotent* $1 + x^3 + x^5 + x^6$ *generates a field of 8 elements. Multiplying this idempotent by the 7 group elements gives the following elements:*

$1 + x + x^5 + x^6$, $x + x^4 + x^6 + 1$, $x^2 + x^5 + 1 + x$, $x^3 + x^6 + x + x^2$, $x^4 + 1 + x^2 + x^3$, $x^5 + x + x^3 + x^4$ *and* $x^6 + x^2 + x^4 + x^5$.
We can also multiply by 0 to get 0.
Thus we get 8 distinct elements which complete the summand $\mathbb{F}_{2^3}$ *generated by the idempotent* $1 + x^3 + x^5 + x^6$.

We now reorder these 8 elements and display them and their corresponding vectors over $\mathbb{F}_2$ *in the following table*

$1+x^3+x^5+x^6$	1001011
$1+x+x^4+x^6$	1100101
$1+x+x^2+x^5$	1110010
$x+x^2+x^3+x^6$	0111001
$1+x^2+x^3+x^4$	1011100
$x+x^3+x^4+x^5$	0101110
$x^2+x^4+x^5+x^6$	0010111
0	0000000

The two elements of the summand $\mathbb{F}_2$ *generated by* $1+x+x^2+x^3+x^4+x^5+x^6$ *are* $1+x+x^2+x^3+x^4+x^5+x^6$ *and 0.*
Adding zero to the 8 earlier elements leaves them unchanged. Adding $1+x+x^2+x^3+x^4+x^5+x^6$ *to them changes the 1's to 0's and vice versa.*
Thus we get the further 8 elements with corresponding vectors as follows:

$x+x^2+x^4$	0110100
$x^2+x^3+x^5$	0011010
$x^3+x^4+x^6$	0001101
$1+x^4+x^5$	1000110
$x+x^5+x^6$	0100011
$1+x^2+x^6$	1010001
$1+x+x^3$	1101000
$1+x+x^2+x^3+x^4+x^5+x^6$	1111111

The 16 codewords in the Hamming (7,4,3) Code generated by the zero divisor $1+x+x^3$ *and the submodule* W *with basis* $S=\{1,x,x^2,x^3\}$ *that we encountered in Example 1.12 are:*

[0000000], [0001101], [0010111], [0011010],
[0100011], [0101110], [0110100], [0111001],
[1000110], [1001011], [1010001], [1011100],
[1100101], [1101000], [1110010], [1111111].

These are clearly the same as the 16 vectors in the direct sum $\mathbb{F}_{2^3} \oplus \mathbb{F}_2$.

Example 6.22. $\mathbb{F}_3 C_2^2$. *$q = 3$ and $n = 4$. Let $C_2^2 = \{1, x, y, xy\}$.*
Altogether there are 5 normal subgroups but only 4 of these have a cyclic quotient. They are:

$H_1 \simeq \langle x \rangle$ *of degree $k = 2$,*
$H_2 \simeq \langle y \rangle$ *also with $k = 2$,*
$H_3 \simeq \langle xy \rangle$ *with $k = 2$.*
$H_4 \simeq \langle x, y \rangle$ *with $k = 1$.*

If $k = 2$, then $F(\zeta_2) = \mathbb{F}_{3^{o_2}} = \mathbb{F}_{3^1}$ because the order of 3(mod 2) is 1.
If $k = 1$, then $F(\zeta_1) = \mathbb{F}_3$ because the primitive 1^{st} root is in the prime subfield.

$G/H_1 \simeq C_2$. The table of irreducible characters of C_2 is:

classes:	1	x
sizes :	1	1
χ_1	1	1
χ_2	1	ζ

where ζ is a primitive square root of unity in $\mathbb{F}_3$, i.e $\zeta = 2$.

The group $(G/H_1)^*$ of irreducible characters of G/H_1 is $\{\chi_1, \chi_2\}$ with generator χ_2.
The group $(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/4\mathbb{Z})^\times = \{1, 3\}$ acts on $(G/H_1)^*$ by $m \cdot g = g^m$.
Q is the subgroup of $(\mathbb{Z}/4\mathbb{Z})^\times$ generated by $q = 3$ and so $Q = \{3, 1\}$.
Now $\chi_2^3(x) = \chi_2(x)$ while $\chi_2^1 = \chi_2$ also.
Thus the orbits of the elements of $(G/H_1)^*$ under the action of Q on $(G/H_1)^*$ are $\{\chi_1\}$, $\{\chi_2\}$ with only $\{\chi_2\}$ containing a generator so we label it $C(G/H_1)$.

Note that the situation for the other two normal subgroups of degree 2 is the same so will use the same character when establishing the primitive idempotent associated with H_2 and H_3.

Thus there are three pairs (H_1, C), (H_2, C) *and* (H_3, C) *where* $C = \{\chi_2\}$.

By Theorem 6.17 there are then three summands isomorphic to $\mathbb{F}_3$ *in the Wedderburn decomposition. The other summand is also* $\mathbb{F}_3$ *which corresponds to the pair* $(H_4, C(G/G))$.
Thus the total decomposition of $\mathbb{F}_3 C_2^2$ *is* $\bigoplus_{i=1}^{4} \mathbb{F}_3$.

We can find the four primitive central orthogonal idempotents now.
Note that $H_1 \simeq \langle x \rangle$ *and so* G/H_1 *contains two cosets* $\{1, x\}$ *and* $\{y, xy\}$ *corresponding to 1 and* x *in the character table of* C_2. *Thus for instance* $\bar{x} = 1$ *and* $\bar{y} = x$ *where* $\bar{x}$ *is the image of* x *in* G/H_1. *Thus we have*

$$\begin{aligned}
&\epsilon_C(G, H_1) \\
&= 1[tr_{\mathbb{F}_3/\mathbb{F}_3}(\chi_2(1))1 + tr_{\mathbb{F}_3/\mathbb{F}_3}(\chi_2(\bar{x}))x + tr_{\mathbb{F}_3/\mathbb{F}_3}(\chi_2(\bar{y}))y + tr_{\mathbb{F}_3/\mathbb{F}_3}(\chi_2(\bar{xy}))xy] \\
&= 1[tr_{\mathbb{F}_3/\mathbb{F}_3}(1)1 + tr_{\mathbb{F}_3/\mathbb{F}_3}(1)x + tr_{\mathbb{F}_3/\mathbb{F}_3}(\zeta)y + tr_{\mathbb{F}_3/\mathbb{F}_3}(\zeta)xy] \\
&= 1[1 + 1x + 2y + 2xy]
\end{aligned}$$

Note that $\mathbb{F}_3/\mathbb{F}_3$ *has only the trivial automorphism so the Galois conjugate of each element is just the element itself. Thus* $tr_{\mathbb{F}_3/\mathbb{F}_3}(1) = 1$ *and* $tr_{\mathbb{F}_3/\mathbb{F}_3}(\zeta) = \zeta = 2$. *Similarly,* $H_1 \simeq \langle y \rangle$ *and here for instance* $\bar{y} = 1$. *Thus we have*

$$\begin{aligned}
&\epsilon_C(G, H_2) = 1[tr_{\mathbb{F}_3/\mathbb{F}_3}(\chi_2(1))1 + tr_{\mathbb{F}_3/\mathbb{F}_3}(\chi_2(\bar{x}))x + tr_{\mathbb{F}_3/\mathbb{F}_3}(\chi_2(\bar{y}))y + tr_{\mathbb{F}_3/\mathbb{F}_3}(\chi_2(\bar{xy}))xy] \\
&= 1[tr_{\mathbb{F}_3/\mathbb{F}_3}(1)1 + tr_{\mathbb{F}_3/\mathbb{F}_3}(\zeta)x + tr(1)y + tr_{\mathbb{F}_3/\mathbb{F}_3}(\zeta)xy] \\
&= 1[1 + 2x + 1y + 2xy]
\end{aligned}$$

$$\begin{aligned}
&\epsilon_C(G, H_3) = 1[tr_{\mathbb{F}_3/\mathbb{F}_3}(\chi_2(1))1 + tr_{\mathbb{F}_3/\mathbb{F}_3}(\chi_2(\bar{x}))x + tr_{\mathbb{F}_3/\mathbb{F}_3}(\chi_2(\bar{y}))y + tr_{\mathbb{F}_3/\mathbb{F}_3}(\chi_2(\bar{xy}))xy] \\
&= 1[tr_{\mathbb{F}_3/\mathbb{F}_3}(1)1 + tr_{\mathbb{F}_3/\mathbb{F}_3}(\zeta)x + tr_{\mathbb{F}_3/\mathbb{F}_3}(\zeta)y + tr(1)xy] \\
&= 1[1 + 2x + 2y + 1xy]
\end{aligned}$$

For $H_4 = G = C_2^2$, *there is only the trivial character in the character table of the quotient group and so* $C = \{\chi_1\}$. *The primitive central idempotent is* $\epsilon_C(G, G) = e_G = 1 + x + y + xy$.

The four central primitive orthogonal idempotents of $\mathbb{F}_3 C_2^2 \simeq \bigoplus_{i=1}^{4} \mathbb{F}_3$ *are:*
$1 + 1x + 2y + 2xy$,

$1 + 2x + 1y + 2xy$,
$1 + 2x + 2y + 1xy$ *and*
$1 + 1x + 1y + 1xy$.

Example 6.23. $\mathbb{F}_5 C_6$. *$q = 5$ and $n = 6$. Let $C_6 = \{1, x, x^2, x^3, x^4, x^5\}$. There are four normal subgroups all of them with cyclic quotients. They are:*

$H_1 \simeq \langle 1 \rangle$ *of degree 6 = k,*
$H_2 \simeq \langle x^3 \rangle$ *giving k = 3,*
$H_3 \simeq \langle x^2 \rangle$ *giving k = 2 and*
$H_4 \simeq \langle x \rangle$ *giving k = 1.*

If $k = 6$, then $\mathbb{F}_5(\zeta_6) = \mathbb{F}_{5^2}$ because the order of 5 (mod 6) is 2.
If $k = 3$, then $\mathbb{F}_5(\zeta_3) = \mathbb{F}_{5^2}$ because the order of 5 (mod 3) is 2.
If $k = 2$, then $\mathbb{F}_5(\zeta_2) = \mathbb{F}_5$ because the order of 5 (mod 2) is 1.
If $k = 1$, then $\mathbb{F}_5(\zeta_1) = \mathbb{F}_5$ because the primitive 1^{st} root is 1.

The first quotient is $G/H_1 \simeq C_6$. The table of irreducible characters of C_6 is:

classes:	1	x	x^2	x^3	x^4	x^5
sizes :	1	1	1	1	1	1
χ_1	1	1	1	1	1	1
χ_2	1	ζ	ζ^2	ζ^3	ζ^4	ζ^5
χ_3	1	ζ^2	ζ^4	1	ζ^2	ζ^4
χ_4	1	ζ^3	1	ζ^3	1	ζ^3
χ_5	1	ζ^4	ζ^2	1	ζ^4	ζ^2
χ_6	1	ζ^5	ζ^4	ζ^3	ζ^2	ζ

where ζ is a primitive 6^{th} root of unity in $\mathbb{F}_{5^2}$.

To find the value of ζ requires a little work. Firstly $p(x) = x^2 + x + 1$ is an irreducible polynomial of degree 2 over $\mathbb{F}_5[x]$. If we let $p(a) = 0$ then we get $a^2 = -a - 1 = 4a + 4$ and the field extension $\mathbb{F}_5(a) \simeq \mathbb{F}_{5^2}$.
The element 4 has order 2 because $4^2 = 16 \equiv 1 (\text{mod } 5)$. The element a has

order 3 because $a^2 = 4a + 4 \Rightarrow a^3 = a(4a + 4) = 4a^2 + 4a = 4(4 + 4a) + 4a = 16 + 16a + 4a = 1$.
By forming the subgroup generated by these two elements $\langle 4, a\rangle = \{1, a, 4a + 4, 4, 4a, 1 + a\}$ *we can easily find two elements of order 6 i.e.* $4a$ *and* $1 + a$. *Define* $\zeta = 4a$. *Then the orders of the elements of this subgroup are as follows:*

element	1	a	$4a + 4$	4	$4a$	$1 + a$
	1	ζ^4	ζ^2	ζ^3	ζ	ζ^5
order	1	3	3	2	6	6

Also we have $\zeta^2 = 4a + 4$, $\zeta^3 = 4$, $\zeta^4 = a$, $\zeta^5 = 1 + a$.

The group $(G/H_1)^*$ *of irreducible characters of* G/H_1 *is* $\{\chi_1, \chi_2, \chi_3, \chi_4, \chi_5, \chi_6\}$ *with generators* χ_2 *and* χ_6.
The group $(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/6\mathbb{Z})^\times = \{1, 5\}$ *acts on* $(G/H_1)^*$ *by* $m \cdot g = g^m$.
Q *is the subgroup of* $(\mathbb{Z}/6\mathbb{Z})^\times$ *generated by* $q = 5$ *and so* $Q = \{5, 1\}$.

Clearly $\chi_n^1 = \chi_n$.
$\chi_2^5(x) = \chi_6(x)$.
$\chi_3^5(x) = \chi_5(x)$.
$\chi_4^5(x) = \chi_4(x)$
$\chi_5^5(x) = \chi_3(x)$.
$\chi_6^5(x) = \chi_2(x)$

Thus the orbits of the elements of $(G/H_1)^*$ *under the action of* Q *on* $(G/H_1)^*$ *are* $\{\chi_1\}$, $\{\chi_2, \chi_6\}$,$\{\chi_4\}$ *and* $\{\chi_3, \chi_5\}$.
The two generators of $(G/H_1)^*$ *are* χ_2 *and* χ_6 *as these are the only two characters which have order 6.*
Thus there is only one q-cyclotomic class containing a generator so we label it $C(G/H_1) = \{\chi_2, \chi_6\}$.

Choosing χ_2 *as the character from* $C(G/H_1)$, *we get*

$$\epsilon_C(G, H_1) = 1[tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\chi_2(1))1 + tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\chi_2(x))x^5 + tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\chi_2(x^2))x^4 +$$

$tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\chi_2(x^3))x^3 + tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\chi_2(x^4))x^2 + tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\chi_2(x^5))x]$

$=1[tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(1)1 + tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\zeta)x^5 + tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\zeta^2)x^4 + tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\zeta^3)x^3 +$
$tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\zeta^4)x^2 + tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\zeta^5)x]$

The group of automorphisms $Gal(\mathbb{F}_{5^2}/\mathbb{F}_5)$ *is isomorphic to* C_2 *with the Frobenius automorphism* σ *which maps* α *to* α^5 *as the only non trivial automorphism.*

Thus the field trace of each of the above elements is the sum of both of its Galois conjugates.

$tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(1) = 1+1 = 2$

$tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\zeta) = \zeta + \zeta^5 = 4a + (1+a) = 1.$

$tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\zeta^2) = \zeta^2 + \zeta^4 = (4a+4) + a = 4.$

$tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\zeta^3) = \zeta^3 + \zeta^3 = 4 + 4 = 3.$

$tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\zeta^4) = 4$ *(same as* $tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\zeta^2)$*)*

$tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\zeta^5) = 1$ *(same as* $tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\zeta)$*)*

So $\epsilon_C(G, H_1) = 1[(2)1 + (1)x^5 + (4)x^4 + (3)x^3 + (4)x^2 + (1)x]$

$= 2 + x + 4x^2 + 3x^3 + 4x^4 + x^5.$

This is the primitive central orthogonal idempotent associated with the first summand $\mathbb{F}_{5^2}$*. It can be shown with a bit of calculation (not shown) that this element is indeed an idempotent in* $\mathbb{F}_5 C_6$*.*

The second quotient is $G/H_2 \simeq G/^3 \simeq C_3$*. The cosets for this quotient group are* $\{1, x^3\}$*,* $\{x, x^4\}$*,* $\{x^2, x^5\}$ *which will be labelled* $\{1, x, x^2\}$*.*

The table of irreducible characters of C_3 *is:*

classes:	1	x	x^2
sizes :	1	1	1
χ_1	1	1	1
χ_2	1	ζ	ζ^2
χ_3	1	ζ^2	ζ

where ζ *is a primitive cube root of unity in* $\mathbb{F}_{5^2}$*.*

We saw earlier in this example that $\mathbb{F}_{5^2}$ *can be constructed as the quotient ring of* $\mathbb{F}_5[x]/p(x)$ *where* $p(x) = x^2 + x + 1$ *and* a *is a root of* $p(x)$ *such that the element* a *has order 3.*
So we can set $\zeta = a$ *and we have* $\zeta^2 = 4a + 4$.
The group $(G/H_2)^*$ *of irreducible characters of* G/H_2 *is* $\{\chi_1, \chi_2, \chi_3\}$ *with generators* χ_2 *and* χ_3.

Recall that Q *is the subgroup of* $(\mathbb{Z}/6\mathbb{Z})^\times$ *generated by* $q = 5$ *and so* $Q = \{5, 1\}$.

$\chi_2^5(x) = \chi_3(x)$.
$\chi_3^5(x) = \chi_2(x)$.
Thus the orbits of the elements of $(G/H_2)^*$ *under the action of* Q *on* $(G/H_2)^*$ *are* $\{\chi_1\}$ *and* $\{\chi_2, \chi_3\}$.
Thus there is only one q-cyclotomic class containing a generator so we label it $C(G/H_2) = \{\chi_2, \chi_3\}$.

Choosing χ_2 *as the character from* $C(G/H_2)$, *we get*

$\epsilon_C(G, H_2) = 1[tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\chi_2(\bar{1}))1 + tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\chi_2(\bar{x}))x^5 + tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\chi_2(\bar{x^2}))x^4 +$
$tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\chi_2(\bar{x^3}))x^3 + tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\chi_2(\bar{x^4}))x^2 + tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\chi_2(\bar{x^5}))x]$

$=1[tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\chi_2(1))1 + tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\chi_2(x))x^5 + tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\chi_2(x^2))x^4 +$
$tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\chi_2(1))x^3 + tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\chi_2(x))x^2 + tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\chi_2(x^2))x]$

$=1[tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(1)1+tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\zeta)x^5+tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\zeta^2)x^4+tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(1)x^3+tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\zeta)x^2+$
$tr(\zeta^2)x]$

Again the Frobenius automorphism σ *which maps* α *to* α^5 *is the only non trivial automorphism so the field trace is the sum of both of its Galois conjugates.*
$tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(1) = 1+1 = 2$
$tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\zeta) = \zeta + \zeta^5 = a + (4 + 4a) = 4$.
$tr_{\mathbb{F}_{5^2}/\mathbb{F}_5}(\zeta^2) = \zeta^2 + \zeta^4 = (4a + 4) + a = 4$.

So $\epsilon_C(G, H_2) = 1[(2)1 + (4)x^5 + (4)x^4 + (2)x^3 + (4)x^2 + (4)x]$

$= 2 + 4x + 4x^2 + 2x^3 + 4x^4 + 4x^5$.

This is the primitive central orthogonal idempotent associated with the second summand $\mathbb{F}_{5^2}$.

Again, it can be shown that this element is actually an idempotent in $\mathbb{F}_5 C_6$.

The third quotient is $G/H_3 \simeq G/\langle x^2 \rangle \simeq C_2$. *The cosets for this quotient group are* $\{1, x^2, x^4\}$ *and* $\{x, x^3, x^5\}$ *which will be labelled 1 and x respectively.*

The table of irreducible characters of C_2 *is:*

classes:	1	x
sizes :	1	1
χ_1	1	1
χ_2	1	ζ

where ζ *is a square root of unity in* $\mathbb{F}_{5^2}$ *i.e.* $\zeta = 4$.

The group $(G/H_3)^*$ *of irreducible characters of* G/H_3 *is* $\{\chi_1, \chi_2\}$ *with generator* χ_2.

Recall that Q is the subgroup of $(\mathbb{Z}/6\mathbb{Z})^\times$ *generated by* $q = 5$ *and so* $Q = \{5, 1\}$.

$\chi_2^5(x) = \chi_2(x)$.

Thus the orbits of the elements of $(G/H_3)^*$ *under the action of Q on* $(G/H_3)^*$ *are* $\{\chi_1\}$ *and* $\{\chi_2\}$.

Thus there is only one q-cyclotomic class containing a generator so we label it $C(G/H_3) = \{\chi_2\}$.

$\epsilon_C(G, H_3) = 1[tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(\bar{1}))1 + tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(\bar{x}))x^5 + tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(\bar{x^2}))x^4$
$+tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(\bar{x^3}))x^3 + tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(\bar{x^4}))x^2 + tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(\bar{x^5}))x]$
$=1[tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(1))1+tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(x))x^5+tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(1))x^4+tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(x))x^3+$
$tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(1))x^2 + tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(x))x]$
$=1[tr_{\mathbb{F}_5/\mathbb{F}_5}(1)1 + tr_{\mathbb{F}_5/\mathbb{F}_5}(\zeta)x^5 + tr_{\mathbb{F}_5/\mathbb{F}_5}(1)x^4 + tr_{\mathbb{F}_5/\mathbb{F}_5}(\zeta)x^3 + tr_{\mathbb{F}_5/\mathbb{F}_5}(1)x^2 +$
$tr_{\mathbb{F}_5/\mathbb{F}_5}(\zeta)x]$

There is only the trivial automorphism so $tr_{\mathbb{F}_5/\mathbb{F}_5}(1) = 1$ *and* $tr_{\mathbb{F}_5/\mathbb{F}_5}(\zeta) = \zeta = 4$.

So $\epsilon_C(G, H_3) = 1[(1)1 + (4)x^5 + (1)x^4 + (4)x^3 + (1)x^2 + (4)x]$

$= 1 + 4x + 1x^2 + 4x^3 + 1x^4 + 4x^5$.

This is the primitive central orthogonal idempotent associated with one of the two summands $\mathbb{F}_5$.

Again, it can be shown that this element is actually an idempotent in $\mathbb{F}_5C_6$.

The fourth quotient is $G/H_4 \simeq G/G$ *and the cyclic quotient is the trivial group with only the trivial character. As we have seen before, this quotient yields the primitive idempotent* $e_G = 1 + x + x^2 + x^3 + x^4 + x^5$.

This idempotent generates the final summand $\mathbb{F}_5$.

By Theorem 6.17 the Wedderburn decomposition of $\mathbb{F}_5C_6 = \bigoplus_{i=1}^{2} \mathbb{F}_{5^2} \oplus \bigoplus_{i=1}^{2} \mathbb{F}_5$ *and the primitive central orthogonal idempotents are:*

$2 + x + 4x^2 + 3x^3 + 4x^4 + x^5$,

$2 + 4x + 4x^2 + 2x^3 + 4x^4 + 4x^5$,

$1 + 4x + 1x^2 + 4x^3 + 1x^4 + 4x^5$ *and*

$1 + x + x^2 + x^3 + x^4 + x^5$.

6.4 The Isomorphism Problem

[28] The Isomorphism problem concerns the following question:

Given two groups G and H and a field K, is it true that the existence of an isomorphism $KG \simeq KH$ implies that $G \simeq H$?

The answer to this question is no. In his paper [9] The Unit Group of Small Group Algebras and the Minimum Counterexample to the Isomorphism Problem, Leo Creedon gives the minimum counterexample to this problem. The non-isomorphic groups C_4 and C_2^2 have the same group algebra over $\mathbb{F}_5$. This proof was non-constructive.
Here we will find the primitive central orthogonal idempotents of each group algebra and exhibit an isomorphism between them.

First we find the primitive idempotents of $\mathbb{F}_5 C_4$ using Broche and del Rio's method from the previous section. $q = 5$ and $n = 4$. Let $C_4 = \{1, x, x^2, x^3\}$. There are three normal subgroups with cyclic quotients. They are:

$H_1 \simeq \langle 1 \rangle$ of degree $4 = k$,
$H_2 \simeq \langle x^2 \rangle$ giving $k = 2$,
$H_3 \simeq \langle x \rangle$ giving $k = 1$.

If $k = 4$, then $\mathbb{F}_5(\zeta_4) = \mathbb{F}_5$ because the order of 5 $(mod\ 4)$ is 1.
If $k = 2$, then $\mathbb{F}_5(\zeta_2) = \mathbb{F}_5$ because the order of 5 $(mod\ 2)$ is 1.
If $k = 1$, then $\mathbb{F}_5(\zeta_1) = \mathbb{F}_5$ because the primitive 1^{st} root is 1 which is in $\mathbb{F}_5$.

The first quotient is $G/H_1 \simeq C_4$. The table of irreducible characters of C_4 is:

classes:	1	x	x^2	x^3
$sizes:$	1	1	1	1
χ_1	1	1	1	1
χ_2	1	ζ	ζ^2	ζ^3
χ_3	1	ζ^2	1	ζ^2
χ_4	1	ζ^3	ζ^2	ζ

where ζ is a primitive 4^{th} root of unity in $\mathbb{F}_5$.
Define $\zeta = 2$. Then $\zeta^2 = 4$ and $\zeta^3 = 3$.

The group $(G/H_1)^*$ of irreducible characters of G/H_1 is $\{\chi_1, \chi_2, \chi_3, \chi_4\}$ with generators χ_2 and χ_4.
The group $(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/4\mathbb{Z})^\times = \{1, 3\}$ acts on $(G/H_1)^*$ by $m \cdot g = g^m$.
Q is the subgroup of $(\mathbb{Z}/4\mathbb{Z})^\times$ generated by $q = 5 = 1(\text{mod } 5)$ and so $Q = \{1\}$.

Clearly $\chi_n^1 = \chi_n$.

Thus the orbits of the elements of $(G/H_1)^*$ under the action of Q on $(G/H_1)^*$ are $\{\chi_1\}$, $\{\chi_2\}$, , $\{\chi_3\}$ and $\{\chi_4\}$.
The two generators of $(G/H_1)^*$ are χ_2 and χ_4 as these are the only two characters which have order 4.
Thus there are two q-cyclotomic classes containing a generator so we label them $C_1(G/H_1) = \{\chi_2\}$ and $C_2(G/H_1) = \{\chi_4\}$. This means that there are two summands isomorphic to $\mathbb{F}_5$ associated with the normal subgroup H_1.
The first one of these summands has the following idempotent:

$\epsilon_{C_1}(G, H_1) = |G|^{-1}[tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(1))1 + tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(x))x^3 + tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(x^2))x^2 + tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(x^3))x]$

$=4[(1)1 + (\zeta)x^3 + (\zeta^2)x^2 + (\zeta^3)x]$

$= 4[(1)1 + (2)x^3 + (4)x^2 + (3)x]$

$= 4 + 3x^3 + x^2 + 2x$

$= 4 + 2x + x^2 + 3x^3.$

(Note that since the Galois group of $\mathbb{F}_5$ over $\mathbb{F}_5$ contains only the trivial automorphism,the field trace of each element is just the element itself).
This then is the primitive central orthogonal idempotent associated with the first summand $\mathbb{F}_5$ associated with H_1.

$\epsilon_{C_2}(G, H_1) = |G|^{-1}[tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_4(1))1 + tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_4(x))x^3 + tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_4(x^2))x^2 + tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_4(x^3))x]$

$=4[(1)1 + (\zeta^3)x^3 + (\zeta^2)x^2 + (\zeta)x]$

$= 4[(1)1 + (3)x^3 + (4)x^2 + (2)x]$

$= 4 + 2x^3 + x^2 + 3x = 4 + 3x + x^2 + 2x^3$

This then is the primitive central orthogonal idempotent associated with the second summand $\mathbb{F}_5$ associated with H_1.

The second quotient is $G/H_2 \simeq G/\langle x^2 \rangle \simeq C_2$. $H_2 = \{1, x^2\}$ so the cosets for the quotient are $1H_1 = 1\{1, x^2\}$ and $xH_2 = 1\{1, x^2\}$. These cosets are labelled $\{1, x\}$.

The table of irreducible characters of C_2 is:

classes:	1	x
$sizes:$	1	1
χ_1	1	1
χ_2	1	ζ

where ζ is a square root of unity in $\mathbb{F}_5$. Thus $\zeta = 4$.

Again $Q = \{1\}$ and so the orbits of the elements of $(G/H_2)^*$ under the action of Q on $(G/H_2)^*$ are $\{\chi_1\}$ and $\{\chi_2\}$ with only one q-cyclotomic class containing a generator so we label it $C(G/H_2) = \{\chi_2\}$.

$\epsilon_C(G, H_2) = 4[tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(\bar{1}))1 + tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(\bar{x}))x^3 + tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(\bar{x^2}))x^2 +$
$\mathrm{tr}_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(\bar{x^3}))x^1]$
$= 4[(\chi_2(1))1 + (\chi_2(x))x^3 + (\chi_2(1))x^2 + (\chi_2(x))x]$

$=4[(1)1 + (\zeta)x^3 + (1)x^2 + (\zeta)x]$

$=4[1 + 4x^3 + 1x^2 + 4x]$

$= 4 + x + 4x^2 + x^3.$

This is the primitive central orthogonal idempotent associated with the summand $\mathbb{F}_5$ assocoated with H_3.

The third quotient is $G/H_3 \simeq G/G$ and the cyclic quotient is the trivial group with only the trivial character. By Lemma 6.16 this quotient yields the primitive idempotent $e_G = |G|^{-1}[1 + x + x^2 + x^3] = 4 + 4x + 4x^2 + 4x^3$. This idempotent generates the final summand $\mathbb{F}_5$.

By Theorem 6.17 the Wedderburn decomposition of $\mathbb{F}_5C_4 \simeq \bigoplus_{i=1}^{4} \mathbb{F}_5$ and the primitive central orthogonal idempotents are:

$e_1 = 4 + 2x + x^2 + 3x^3$,

$e_2 = 4 + 3x + x^2 + 2x^3$,

$e_3 = 4 + x + 4x^2 + x^3$ and

$e_4 = 4 + 4x + 4x^2 + 4x^3$.

Thus $\mathbb{F}_5C_4 \simeq \bigoplus_{i=1}^{4} \mathbb{F}_5^4 \simeq \bigoplus_{i=1}^{4} \mathbb{F}_5C_4e_i \simeq \bigoplus_{i=1}^{4} \mathbb{F}_5e_i$.

Next find the idempotents of $\mathbb{F}_5C_2^2$. Again $q = 5$ and $n = 4$. Let $C_2^2 = \{1, x, y, xy\}$.

There are four normal subgroups with cyclic quotients. They are:

$H_1 \simeq \langle x \rangle$ of degree $k = 2$,

$H_2 \simeq \langle y \rangle$ giving $k = 2$,

$H_3 \simeq \langle xy \rangle$ giving $k = 2$ and

$H_4 \simeq C_2^2$ giving $k = 1$

If $k = 2$, then $\mathbb{F}_5(\zeta_2) = \mathbb{F}_5$ because the order of 5 $(mod\ 2)$ is 1.
If $k = 1$, then $\mathbb{F}_5(\zeta_1) = \mathbb{F}_5$ because the primitive 1^{st} root is 1 which is in $\mathbb{F}_5$.

The first quotient is $G/H_1 \simeq G/\langle x \rangle \simeq C_2$. $H_2 = \{1, x\}$ so the cosets for the quotient are $1H_1 = 1\{1, x\}$ and $yH_2 = y\{1, x\}$. These cosets are labelled $\{1, x\}$.

The quotient qroups G/H_1, G/H_2 and G/H_3 are isomorphic to C_2. The table of irreducible characters of C_2 is:

classes:	1	x
$sizes:$	1	1
χ_1	1	1
χ_2	1	ζ

where ζ is a primitive square root of unity in $\mathbb{F}_5$, i.e $\zeta = 4$.

The group $(G/H_1)^*$ of irreducible characters of G/H_1 is $\{\chi_1, \chi_2\}$ with generator χ_2.
The group $(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/4\mathbb{Z})^\times = \{1, 3\}$ acts on $(G/H_1)^*$ by $m \cdot g = g^m$.
Q is the subgroup of $(\mathbb{Z}/4\mathbb{Z})^\times$ generated by $q = 5 = 1 \pmod 4$ and so $Q = \{1\}$.
Thus the orbits of the elements of $(G/H_1)^*$ under the action of Q on $(G/H_1)^*$ are $\{\chi_1\}$ and $\{\chi_2\}$ with only $\{\chi_2\}$ containing a generator so we label it $C = C(G/H_1) = \{\chi_2\}$.

Note that the situation for the other two normal subgroups of degree 2 is the same so will use the same character when establishing the primitive idempotent associated with H_2 and H_3.
Thus there are three pairs (H_1, C), (H_2, C) and (H_3, C) where $C = \{\chi_2\}$.

By Theorem 6.17 there are then three summands isomorphic to $\mathbb{F}_5$ in the Wedderburn decomposition. The other summand is also $\mathbb{F}_5$ which corresponds to the pair $(H_4, C(G/G))$.
Thus the total decomposition of $\mathbb{F}_5 C_2^2$ is $\bigoplus_{i=1}^4 \mathbb{F}_5$.

We can now find the four primitive central orthogonal idempotents.

$\epsilon_C(G, H_1) = |G|^{-1}[tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(1))1 + tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(\bar{x}))x + tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(\bar{y}))y + tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(\bar{xy}))xy]$
$=4^{-1}[(1)1 + (1)x + (\zeta)y + (\zeta)xy]$
$=4[1 + 1x + 4y + 4xy] = 4 + 4x + y + xy.$

$\mathbb{F}_5$ has only the trivial automorphism so the Galois conjugate of each element is just the element itself. Thus $tr(1) = 1$ and $tr(\zeta) = \zeta = 4$. Similarly,

$\epsilon_C(G, H_2) = |G|^{-1}[tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(1))1 + tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(\bar{x}))x + tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(\bar{y}))y + tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(\bar{xy}))xy]$

$=4^{-1}[(1)1 + (\zeta)x + (1)y + (\zeta)xy]$

$=4[1 + 4x + 1y + 4xy] = 4 + x + 4y + xy$

$\epsilon_C(G, H_3) =|G|^{-1}[tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(1))1 + tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(\bar{x}))x + tr_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(\bar{y}))y +$
$\mathrm{tr}_{\mathbb{F}_5/\mathbb{F}_5}(\chi_2(\bar{xy}))xy]$

$=4^{-1}[(1)1 + (\zeta)x + (\zeta)y + (1)xy]$

$=4[1 + 4x + 4y + 1xy] = 4 + x + y + 4xy.$

For $H_4 = \mathrm{G} = C_2^2$, the primitive central idempotent is $\epsilon_C(G, G) = e_G = 4 + 4x + 4y + 4xy$ by Lemma 6.16.

The four central primitive orthogonal idempotents of $\mathbb{F}_5C_2^2 \simeq \bigoplus_{i=1}^4 \mathbb{F}_5$ are:

$f_1 = 4 + 4x + y + xy,$

$f_2 = 4 + x + 4y + xy,$

$f_3 = 4 + x + y + 4xy$ and

$f_4 = 4 + 4x + 4y + 4xy.$

Now every element of $\mathbb{F}_5C_2^2$ can be written as a linear combination of these four primitive idempotents.
Thus for $\alpha \in \mathbb{F}_5C_2^2$ we have $\alpha = a_1f_1 + a_2f_2 + a_3f_3 + a_4f_4$.
Similarly, every element of $\mathbb{F}_5C_4$ can be written as a linear combination of its four primitve idempotents.
In this way, we can exhibit a ring isomorphism between the two group algebras as follows:

$f : \mathbb{F}_5C_4 \to \mathbb{F}_5C_2^2$

$f : a_1e_1 + a_2e_2 + a_3e_3 + a_4e_4 \mapsto a_1f_1 + a_2f_2 + a_3f_3 + a_4f_4.$

Note the similarity of the decomposition of $\mathbb{F}_5C_2^2$ to the decomposition of $\mathbb{F}_3C_2^2$ done in Example 6.22. This leads to the following Lemma.

Lemma 6.24. *For p odd, $\mathbb{F}_{p^n}C_2^2 \simeq \bigoplus_{i=1}^4 \mathbb{F}_{p^n} \simeq \bigoplus_{i=1}^4 \mathbb{F}_{p^n}e_i$ and the primitive central orthogonal idempotents associated with each summand are:*

$e_1 = \epsilon_C(G, \langle x \rangle) = |G|^{-1}[1 + x + (p-1)y + (p-1)xy]$,
$e_2 = \epsilon_C(G, \langle y \rangle) = |G|^{-1}[1 + (p-1)x + y + (p-1)xy]$,
$e_3 = \epsilon_C(G, \langle xy \rangle) = |G|^{-1}[1 + (p-1)x + (p-1)y + xy]$ *and*
$e_4 = \epsilon_C(G, \langle x, y \rangle) = |G|^{-1}[1 + x + y + xy]$.

Proof. By Lemma 4.25 $\mathbb{F}_{p^n} C_2^2 \simeq \bigoplus_{i=1}^{2^2} \mathbb{F}_{p^n} \simeq \bigoplus_{i=1}^{4} \mathbb{F}_{p^n}$.
Let $C_2^2 = \{1, x, y, xy\}$. There are 5 normal subgroups but only 4 of these have a cyclic quotient. They are:

$H_1 \simeq \langle x \rangle$ of degree $k = 2$,
$H_2 \simeq \langle y \rangle$ also with $k = 2$,
$H_3 \simeq \langle xy \rangle$ with k =2.
$H_4 \simeq \langle x, y \rangle$ with $k = 1$.

If $k = 2$, then $\mathbb{F}_{p^n}(\zeta_2) = \mathbb{F}_{p^n}$ because the order of p^n $(mod\ 2)$ is 1.
If $k = 1$, then $\mathbb{F}_{p^n}(\zeta_1) = \mathbb{F}_{p^n}$ because the primitive 1^{st} root is 1 which is in $\mathbb{F}_{p^n}$.

The table of irreducible characters of C_2 is:

classes:	1	x
$sizes:$	1	1
χ_1	1	1
χ_2	1	ζ

where ζ is a primitive square root of unity in $\mathbb{F}_{p^n}$.
One such root is $\zeta = p - 1$ because $(p-1)(p-1) = p^2 - 2p + 1 = 1(mod\ p)$.
Thus define $\zeta = p - 1$.

The group $(G/H_1)^*$ of irreducible characters of G/H_1 is $\{\chi_1, \chi_2\}$ with generator χ_2.
The group $(\mathbb{Z}/4\mathbb{Z})^\times = \{1, 3\}$ acts on $(G/H_1)^*$ by $m \cdot g = g^m$.
Q is the subgroup of $(\mathbb{Z}/4\mathbb{Z})^\times$ generated by $q = p$.
Now p^n is odd so either $p^n = 1(mod\ 4)$ $Q = \{1\}$ or $p^n = 3\ (mod\ 4) \Rightarrow Q = \{3, 1\}$.

$\chi_1^1 = \chi_1$ and $\chi_1^3 = \chi_1$.

$\chi_2^1 = \chi_2$ and $\chi_2^3 = \chi_2$ also.

Thus either way the orbits of the elements of $(G/H_1)^*$ under the action of Q on $(G/H_1)^*$ are $\{\chi_1\}$ and $\{\chi_2\}$ with only $\{\chi_2\}$ containing a generator so we label it $C(G/H_1)$.

Note that the situation for the other two normal subgroups of degree 2 is the same so we will use the same character when establishing the primitive idempotent associated with H_2 and H_3.
Thus there are three pairs (H_1, C), (H_2, C) and (H_3, C) where $C = \{\chi_2\}$. Recall that $\bar{x}$ is the image of x in the quotient group G/H_1 and so $\bar{x} = 1$, while $\bar{y} = x\bar{y} = x$ (the element of order 2 in the quotient group G/H_1. So we have that

$\epsilon_C(G, H_1) = |G|^{-1}[tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^n}}(\chi_2(1))1 + tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^n}}(\chi_2(\bar{x}))x + tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^n}}(\chi_2(\bar{y}))y + tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^n}}(\chi_2(x\bar{y}))xy]$
$= |G|^{-1}[(1)1 + (1)x + (\zeta)y + (\zeta)xy]$
$= |G|^{-1}[1 + 1x + (p-1)y + (p-1)xy].$

The extension $\mathbb{F}_{p^n}/\mathbb{F}_{p^n}$ has only the trivial automorphism so the galois conjugate of each element is just the element itself. Thus $tr(1) = 1$ and $tr(\zeta) = \zeta = p - 1$. Similarly,

$\epsilon_C(G, H_2) = |G|^{-1}[tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^n}}(\chi_2(1))1 + tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^n}}(\chi_2(\bar{x}))x + tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^n}}(\chi_2(\bar{y}))y + tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^n}}(\chi_2(x\bar{y}))xy]$
$= |G|^{-1}[(1)1 + (\zeta)x + (1)y + (\zeta)xy]$
$= |G|^{-1}[1 + (p-1)x + 1y + (p-1)xy]$

$\epsilon_C(G, H_3) = [tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^n}}(\chi_2(1))1 + tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^n}}(\chi_2(\bar{x}))x + tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^n}}(\chi_2(\bar{y}))y + tr_{\mathbb{F}_{p^n}/\mathbb{F}_{p^n}}(\chi_2(x\bar{y}))xy]$
$= |G|^{-1}[(1)1 + (\zeta)x + (\zeta)y + (1)xy]$
$= |G|^{-1}[1 + (p-1)x + (p-1)y + 1xy].$

For $H_4 = G = C_2^2$, the primitive central idempotent is $\epsilon_C(G, G) = e_G = |G|^{-1}[1 + x + y + xy]$ by Lemma 6.16 which completes the proof.

Example 6.25. *Consider the elements of* $\mathbb{F}_{3^2}C_2^2$ *where* $\mathbb{F}_{3^2} = \{0, 1, 2, a, 2a, 1+a, 2+a, 1+2a, 2+2a\}$ *and* $C_2^2 = \{1, x, y, xy\}$. *By Lemma 6.24 the primitive central idempotents are* $1+x+2y+2xy$, $1+2x+y+2xy$, $1+2x+2y+xy$ *and* $1+x+y+xy$. *Then each element of* $\mathbb{F}_{3^2}C_2^2$ *can be written as a linear combination of the primitive central idempotents. For example the element* $(2+a)1+(a)x+(2+a)y+(2)xy$ *can be written as:* $(1+a)[1+x+2y+2xy]$ $+ a[1+2x+y+2xy] + 2a[1+2x+2y+xy] + 0[1+x+y+xy]$.

In the table which follows, we show the unit group for selected commutative group algebras. We list the Wedderburn decomposition or the decomposition as the direct sum of group algebras where applicable. Note that p is an odd prime in this table.

6.5 Table of $U(FG)$ for selected group algebras (G abelian)

FG	**|FG|**	**Decomposition**	**U(FG)**	**|U(FG)|**
$\mathbb{F}_2C_1$	2	$\mathbb{F}_2$	C_1	1
$\mathbb{F}_{p^n}C_1$	p^n	$\mathbb{F}_{p^n}$	C_{p^n-1}	p^n-1
$\mathbb{F}_2C_2$	4		C_2	2
$\mathbb{F}_3C_2$	9	$\bigoplus_{i=1}^{2}\mathbb{F}_3$	C_2^2	4
$\mathbb{F}_{2^2}C_2$	16		$C_2^2\times C_3$	12
$\mathbb{F}_5C_2$	25	$\bigoplus_{i=1}^{2}\mathbb{F}_5$	C_4^2	16
$\mathbb{F}_7C_2$	49	$\bigoplus_{i=1}^{2}\mathbb{F}_7$	C_6^2	36
$\mathbb{F}_{2^3}C_2$	64		$C_2^3\times C_7$	56
$\mathbb{F}_{3^2}C_2$	81	$\bigoplus_{i=1}^{2}\mathbb{F}_{3^2}$	C_8^2	64
$\mathbb{F}_{2^4}C_2$	256		$C_2^4\times C_{15}$	240
$\mathbb{F}_{5^2}C_2$	625	$\bigoplus_{i=1}^{2}\mathbb{F}_{5^2}$	C_{24}^2	16
$\mathbb{F}_{3^3}C_2$	729	$\bigoplus_{i=1}^{2}\mathbb{F}_{3^3}$	C_{26}^2	676
$\mathbb{F}_{p^n}C_2$	p^{2n}	$\bigoplus_{i=1}^{2}\mathbb{F}_{p^n}$	$C_{p^n-1}^2$	$(p^n-1)^2$
$\mathbb{F}_{2^k}C_2$	2^{2k}		$C_2^k\times C_{2^k-1}$	$2^k(2^k-1)$
$\mathbb{F}_2C_3$	8	$\mathbb{F}_2\oplus\mathbb{F}_{2^2}$	C_3	3
$\mathbb{F}_3C_3$	27		$C_2\times C_3^2$	18
$\mathbb{F}_{2^2}C_3$	64	$\bigoplus_{i=1}^{3}\mathbb{F}_{2^2}$	C_3^3	27
$\mathbb{F}_5C_3$	125	$\mathbb{F}_5\oplus\mathbb{F}_{5^2}$	$C_4\times C_{24}$	96
$\mathbb{F}_7C_3$	343	$\bigoplus_{i=1}^{3}\mathbb{F}_7$	C_6^3	216
$\mathbb{F}_{2^3}C_3$	512	$\mathbb{F}_{2^3}\oplus\mathbb{F}_{2^6}$	$C_7\times C_{63}$	441
$\mathbb{F}_{3^2}C_3$	729		$C_8\times C_3^4$	648
$\mathbb{F}_2C_4$	16		$C_2\times C_4$	8
$\mathbb{F}_3C_4$	81	$\bigoplus_{i=1}^{2}\mathbb{F}_3\oplus\mathbb{F}_{3^2}$	$C_2^2\times C_8$	32
$\mathbb{F}_{2^2}C_4$	256		$C_2^2\times C_4^2\times C_3$	192
$\mathbb{F}_5C_4$	625	$\bigoplus_{i=1}^{4}\mathbb{F}_5$	C_4^4	256

Continued on next page

Table 3 – continued from previous page

FG	**|FG|**	**Decomposition**	**U(FG)**	**|U(FG)|**
$\mathbb{F}_2C_2^2$	16		C_2^3	8
$\mathbb{F}_3C_2^2$	81	$\bigoplus_{i=1}^4 \mathbb{F}_3$	C_2^4	16
$\mathbb{F}_{2^2}C_2^2$	256		$C_2^6 \times C_3$	192
$\mathbb{F}_5C_2^2$	625	$\bigoplus_{i=1}^4 \mathbb{F}_5$	C_4^4	256
$\mathbb{F}_2C_5$	32	$\mathbb{F}_2 \oplus \mathbb{F}_{2^4}$	C_{15}	15
$\mathbb{F}_3C_5$	243	$\mathbb{F}_3 \oplus \mathbb{F}_{3^4}$	$C_2 \times C_{80}$	160
$\mathbb{F}_2C_6$	64	$\mathbb{F}_2C_2 \oplus \mathbb{F}_{2^2}C_2$	$C_2^3 \times C_3$	24
$\mathbb{F}_3C_6$	729	$\bigoplus_{i=1}^2 \mathbb{F}_3C_3$	$C_2^2 \times C_3^4$	324
$\mathbb{F}_2C_7$	128	$\mathbb{F}_2 \oplus \bigoplus_{i=1}^2 \mathbb{F}_{2^3}$	C_7^2	49
$\mathbb{F}_3C_7$	2187	$\mathbb{F}_3 \oplus \mathbb{F}_{3^6}$	$C_2 \times C_{728}$	1452
$\mathbb{F}_2C_8$	256		$C_2^2 \times C_4 \times C_8$	128
$\mathbb{F}_2(C_2 \times C_4)$	256		$C_2^5 \times C_4$	128
$\mathbb{F}_3(C_2 \times C_4)$	6561	$\bigoplus_{i=1}^4 \mathbb{F}_3 \oplus \bigoplus_{i=1}^2 \mathbb{F}_{3^2}$	$C_2^4 \times C_4^2$	1024
$\mathbb{F}_2C_2^3$	256		C_2^7	128
$\mathbb{F}_2C_9$	512	$\mathbb{F}_2 \oplus \mathbb{F}_{2^2} \oplus \mathbb{F}_{2^6}$	$C_3 \times C_{63}$	189
$\mathbb{F}_2C_3^2$	512	$\mathbb{F}_2 \oplus \bigoplus_{i=1}^4 \mathbb{F}_{2^2}$	C_3^4	81
$\mathbb{F}_2C_{11}$	2048	$\mathbb{F}_2 \oplus \mathbb{F}_{2^{10}}$	C_{1023}	1023
$\mathbb{F}_3C_{11}$	177147	$\mathbb{F}_3 \oplus \bigoplus_{i=1}^2 \mathbb{F}_{3^5}$	$C_2 \times C_{242}^2$	117128

Table 3: Table of $U(FG)$ for selected group algebras (G abelian)

7 Perlis Walker Theorem - Finding $U(FG)$

If the unit group of a finite semisimple commutative group algebra is all that is required then a simple method to find this is to use the Perlis Walker theorem. We do this by finding the Wedderburn decomposition and from this determine the structure of the unit group.

Before introducing the theorem, there are a few terms to define, some of which have been defined in earlier Chapters also.

Definition [13] The extension field K of F is called a *splitting field* for the polynomial $f(x) \in F[x]$ if $f(x)$ factors into linear factors (or *splits completely*) in $K[x]$ and $f(x)$ does not factor completely into linear factors over any proper subfield of K containing F.

Definition [13] The element $\alpha \in K$ is said to be *algebraic* over F if α is a root of some nonzero polynomial $f(x) \in F[x]$. The extension K/F is said to be *algebraic* if every element of K is algebraic over F.

Definition The field $\bar{F}$ is called an *algebraic closure* of F if $\bar{F}$ is algebraic over F and if every polynomial $f(x) \in F[x]$ splits completely in $\bar{F}[x]$.

Definition [13] Let K be a splitting field of $x^n - 1 \in F[x]$. A generator of the cyclic group of all n^{th} roots of unity is called a *primitive n^{th} root of unity*.

The next Lemma gives a method for constructing extension fields formed by adjoining a primitive root to a field.

Lemma 7.1. *[6] Let F be a field of order q and let the algebraic closure of F be denoted by $\bar{F}$. Let ζ_d be a primitive d^{th} root of unity in $\bar{F}$ and let $o_d = o_d(q)$ denote the multiplicative order of q (mod d). Then $F(\zeta_d) \simeq F_{q^{o_d}}$ the field of order q^{o_d}.*

Theorem 7.2. *[28] (Perlis-Walker 1950) Let G be a finite abelian group of order n and let K be a field such that $char(K) \not| n$. Then*

$$KG \simeq \bigoplus_{d|n} \bigoplus_{i=1}^{a_d} K(\zeta_d)$$

where ζ_d denotes a primitive root of unity of order d and $a_d = \frac{n_d}{[K(\zeta_d):K]}$. In this formula, n_d denotes the number of elements of order d in G.

In words, the theorem states that for each divisor d of $|G|$, we have a_d direct summands of the extension field $K(\zeta_d)$ in the decomposition. We can find the extension field $K(\zeta_d)$ by using Lemma 7.1.

Corollary 7.3. *[28] Let G be an abelian group of order n and K a field such that $char(K) \not| n$. If K contains a primitive root of order n then*

$$KG \simeq \bigoplus_{i=1}^{n} K.$$

Proof. If K contains a primitive root of unity of order n, then $K(\zeta_d) = K$, for all $d|n$. There will be n_d copies of K for each divisor d, and so there are n copies of K in the decomposition.

We can now demonstrate the use of the theorem in the following examples.

Example 7.4. $\mathbb{F}_{2^3}C_3$.
$|G| = n = 3$. *There are two divisors of 3, namely 1 and 3.*
$\mathbb{F}_{2^3}(\zeta_1) = \mathbb{F}_{2^3}$ *because* $\mathbb{F}_{2^3}$ *contains a* 1^{st} *root of unity.*

$a_1 = \frac{n_1}{[K(\zeta_1):K]} = \frac{1}{1} = 1$. *Thus we get one copy of the field* $\mathbb{F}_{(2^3)}$.

$\mathbb{F}_{2^3}(\zeta_3) = \mathbb{F}_{(2^3)^2} = \mathbb{F}_{2^6}$ *because the multiplicative order of 8 (mod 3) is 2 . That is* $8^2 = 64 \equiv 1 (mod\ 3)$.

$a_3 = \frac{n_3}{[K(\zeta_3):K]} = \frac{2}{2} = 1$. *Thus we get one copy of the field* $\mathbb{F}_{(2^3)^2}$.

Thus the Wedderburn decomposition of $\mathbb{F}_{2^3}C_3$ *is* $\mathbb{F}_{2^3} \oplus \mathbb{F}_{(2^3)^2}$.

Example 7.5. $\mathbb{F}_2C_9$.
$|G| = n = 9$. *There are three divisors of 9, namely 1, 3 and 9.*

$\mathbb{F}_2(\zeta_1) = \mathbb{F}_2$ *and there is only one copy of this field in the decomposition.*
$\mathbb{F}_2(\zeta_3) = \mathbb{F}_{2^2}$ *because the multiplicative order of 2 (mod 3) is 2 . That is* 2^2 $= 4 \equiv 1 (mod\ 3)$.

$a_3 = \frac{n_3}{[K(\zeta_3):K]} = \frac{2}{2} = 1.$ *Thus we get one copy of the field* $\mathbb{F}_{2^2}$.

$\mathbb{F}_2(\zeta_9) = \mathbb{F}_{2^6}$ *because the multiplicative order of 2 (mod 9) is 6 . That is* 2^6 $= 64 \equiv 1 (mod\ 9)$.

$a_9 = \frac{n_9}{[K(\zeta_9):K]} = \frac{6}{6} = 1.$ *Thus we get one copy of the field* $\mathbb{F}_{2^6}$.

Thus the Wedderburn decomposition of $\mathbb{F}_2 C_9$ *is* $\mathbb{F}_2 \oplus \mathbb{F}_{2^2} \oplus \mathbb{F}_{2^6}$.

Example 7.6. $\mathbb{F}_2 C_3^2$
$|G| = n = 9$. *Again, there are three divisors of 9, namely 1, 3 and 9. However, this time there are 8 elements of order 3 and zero elements of order 9.*
$\mathbb{F}_2(\zeta_1) = \mathbb{F}_2$ *and there is only one copy of this field in the decomposition.*
$\mathbb{F}_2(\zeta_3) = \mathbb{F}_{2^2}$ *because the multiplicative order of the field (mod 3) is 2 . That is* $2^2 = 4 \equiv 1$ *(mod 3).*

$a_3 = \frac{n_3}{[K(\zeta_3):K]} = \frac{8}{2} = 4.$ *Thus we get four copies of the field* $\mathbb{F}_{2^2}$.

Thus the Wedderburn decomposition of $\mathbb{F}_2 C_3^2$ *is* $\mathbb{F}_2 \oplus \bigoplus_{i=1}^{4} \mathbb{F}_{2^2}$.

7.1 A General Approach

Instead of dealing with specific group algebras we can generalise the results by applying them to arbitrary fields of order p^n (mod exponent(G)) where G is an abelian group. This systematic approach will look at each abelian group in turn, outlining the group's elements and their orders. Then we can classify the possible group algebras according to the order of the field (mod the exponent of the group). In this way, we can list the general decomposition for each class of field where Maschke's Theorem applies. If Maschke's theorem does not apply then we can use Theorem 5.15 to give the structure of the unit group.

A further two corollaries to the Perlis Walker Theorem will help us with this process.

Corollary 7.7. *Let G be a finite abelian group of order n and exponent e. Let K be a field such that $char(K) \nmid e$. Then*

$KG \simeq \bigoplus_{d|e} \bigoplus_{i=1}^{a_d} K(\zeta_d)$, *where ζ_d denotes a primitive d^{th} root of unity, $a_d = \frac{n_d}{[K(\zeta_d):K]}$ and n_d denotes the number of elements of order d in G.*

Proof. The exponent e is a factor of $n = |G|$. $char(K)$ is a prime and so if $char(K) \nmid e$, then $char(K) \nmid n$ and so Perlis Walker's Theorem applies. Thus $KG \simeq \bigoplus_{d|n} \bigoplus_{i=1}^{a_d} K(\zeta_d)$.
Now if d_i is a divisor of n such that $d_i \nmid e$, then n_{d_i} (the number of elements of order d_i) $= 0 \Rightarrow a_{d_i} = \frac{0}{[K(\zeta_{d_i}):K]} = 0$.
Thus there will be no summands in the decomposition resulting from divisors of $|G|$ that do not divide e.
As a result we have $KG \simeq \bigoplus_{d|e} \bigoplus_{i=1}^{a_d} K(\zeta_d)$.

Corollary 7.8. *Let G be an abelian group of order n and exponent e. Let K be a field such that $char(K) \nmid e$. If K contains a primitive root of order e then*

$KG \simeq \bigoplus_{i=1}^{n} K$.

Proof. If K contains a primitive root of unity of order e, then $K(\zeta_d) = K$, for all $d|e$. There will be n_d copies of K for each divisor d, and all of the elements of G are divisors of e, and so there are n copies of K in the decomposition. Note that Corollary 7.8 is G. Higman's Theorem from 1940 [16].

Recall Lemma 7.1 states that $F(\zeta_d) \simeq F_{q^{o_d}}$ the field of order q^{o_d} where ζ_d is a primitive d^{th} root of unity in $\bar{F}$ and $o_d = o_d(q)$ denotes the multiplicative order of q mod d.
A corollary to Lemma 7.1 now allows us to use all of these results to determine the decomposition of whole classes of group algebras.

Corollary 7.9. *For a group G with exponent e, the degrees of the field extensions in the Wedderburn decomposition will be the same for all group algebras arising from fields whose orders are equivalent (mod e). Let F be a field of order q. Let G be an abelian group of order n and exponent e.*
Let $q \equiv r(mod\ e)$ and let d be a divisor of e. Then $q \equiv r(mod\ d)$ and $o_d(q)$ $= o_d(r)$.

Proof. Let ζ_d be a primitive d^{th} root of unity in $\bar{F}$ and let $o_d = o_d(q)$ denote the multiplicative order of $q(mod\ d)$.
$q \equiv r(mod\ e) \Rightarrow q = r + ke$ for some $k \in \mathbb{Z}$. d is a divisor of $e \Rightarrow e = dl$ for some $l \in \mathbb{Z}$. So we can write $q = r + kdl = r + md$ (where $m = kl$) and so q $\equiv r(mod\ d)$.
Thus the multiplicative order of $q(mod\ d)$ = the multiplicative order of $r(mod$ $d)$ and we can write it as $o_d(q) = o_d(r)$.

Example 7.10. *Consider the group algebras of C_3 with fields of order 8, 5 and 2.*
$8 \equiv 5 \equiv 2(mod\ 3)$. $\mathbb{F}_{2^3}C_3 \simeq \mathbb{F}_{2^3} \oplus \mathbb{F}_{(2^3)^2}$. *Similarly* $\mathbb{F}_5C_3 \simeq \mathbb{F}_5 \oplus \mathbb{F}_{(5)^2}$. *Also* $\mathbb{F}_2C_3 \simeq \mathbb{F}_2 \oplus \mathbb{F}_{(2)^2}$.

Using this method, it quickly becomes apparent that when $q \equiv 1(mod$ $e)$ or $q \equiv$ -1$(mod\ e)$ that we get certain Wedderburn decompositions. The following pair of Lemmas confirm this and using these two results we will cut down on our work still further.

Lemma 7.11. *Let F be a field of order q. Let G be an abelian group of order n and exponent e. Then if $q \equiv 1(mod\ e)$, $FG \simeq \bigoplus_{i=1}^{n} F$.*

Proof. Since $q \equiv 1(mod\ e)$, char $F \nmid e$.
$q \equiv 1(mod\ e) \Rightarrow e \mid q-1$. But $F^{\times} \simeq C_{q-1}$ and e divides $q-1$, and so F contains a primitive e^{th} root of unity. Thus by Corollary 7.8 $FG \simeq \bigoplus_{i=1}^{n} F$.

Lemma 7.12. *Let F be a field of order q and let G be an abelian group of order n and exponent e. Let m be the number of elements of order dividing 2 in G. Then if $q \equiv$ -1(mod e), $FG \simeq \bigoplus_{i=1}^{m} F_q \oplus \bigoplus_{i=1}^{(n-m)/2} F_{q^2}$.*

Proof. First of all
$F_q(\zeta_1) = F_q$ because F_q contains a 1^{st} root of unity. $a_1 = \frac{n_1}{[K(\zeta_1):K]} = \frac{1}{1} = 1$.

Thus we get one copy of F_q associated with the element of order 1.

Now $q \equiv$ -1(mod e) so by Corollary 7.9, $q(mod\ d) \equiv -1(mod\ d)$. Also $o_d(q)$ $= o_d(-1)$. When $d = 2$ we have that $(-1)^1 \equiv 1$(mod 2) and so $o_2(q) = 1$. And so we will get a copy of the field F_q for each element of order 2. Note if m is the number of elements of order dividing 2, there are $m-1$ elements of order 2 (i.e. we exclude the identity). $a_2 = \frac{n_2}{[K(\zeta_2):K]} = \frac{m-1}{1} =$ m-1. Thus

we get $m-1$ copies of F_q associated with the elements of order 2. Combined with the other copy of F_q for the identity we have m copies of F_q so far. That is $\bigoplus_{i=1}^{m} F_q$.

Now if $d > 2$, we do not have $(-1)^1 \equiv 1(mod\ d)$ because if d > 2 and $(-1)^1$ $\equiv 1(mod\ d)$ we have $-1^1 \equiv 1(mod\ d) \Rightarrow -2^1 \equiv 0(mod\ d) \Rightarrow 2^1 \equiv 0(mod\ d)$ $\Rightarrow d = 2$ which contradicts that $d > 2$.
However for all of the other elements of order d (i.e. $d > 2$) in the group we do have that $(-1)^2 \equiv 1(mod\ d)$ and there are $n-m$ of these elements. Thus there are (n-m)/2 copies of the field F_{q^2} in the decomposition.
Thus $FG \simeq \bigoplus_{i=1}^{m} F_q \oplus \bigoplus_{i=1}^{(n-m)/2} F_{q^2}$.

Example 7.13. *Let FG be $\mathbb{F}_7(C_2 \times C_4 \times C_8)$ and FH be $\mathbb{F}_7(C_4^3)$. Then G has $2^3 = 8$ elements of order dividing 2, and so does H. Thus $m = 8$.*

Also 7 ≡ -1(mod 8) and 7 ≡ -1(mod 4) and so for both group algebras the decomposition is $\bigoplus_{i=1}^{8} \mathbb{F}_7 \oplus \bigoplus_{i=1}^{(64-8)/2} \mathbb{F}_{7^2}$ *by Lemma 7.12.*
That is $\mathbb{F}_7(C_2 \times C_4 \times C_8) \simeq \mathbb{F}_7(C_4^3) \simeq \bigoplus_{i=1}^{8} \mathbb{F}_7 \oplus \bigoplus_{i=1}^{28} \mathbb{F}_{7^2}$.

Theorem 7.14. *Given two non-isomorphic abelian groups G and H each with order n, and a field F of order q such that $q \equiv 1(mod\ n)$, then $FG \simeq FH$.*

Proof. $q = 1(mod\ n) \Rightarrow n \mid q-1$. But $F^\times \simeq C_{q-1}$ and n divides $q-1$, and so F contains a primitive n^{th} root of unity. Thus by Corollary 7.3 $FG \simeq \bigoplus_{i=1}^{n} F$. Similarly $FH \simeq \bigoplus_{i=1}^{n} F$. Thus $FG \simeq FH$.

Example 7.15. *Let $G = C_8$ and let $H = C_2 \times C_4$. Let $F = \mathbb{F}_{3^2}$. Then by Lemma 7.14 $\mathbb{F}_{3^2}C_8 \simeq \mathbb{F}_{3^2}(C_2 \times C_4)$.*

Example 7.16. *Let $G = C_9$ and let $H = C_3^2$. Let $F = \mathbb{F}_{19}$. Then by Lemma 7.14 $\mathbb{F}_{19}C_9 \simeq \mathbb{F}_{19}C_3^2$.*

Conjecture If $FG \simeq FH$ and G and H are non-isomorphic abelian groups of order n, then $q \equiv 1(mod\ n)$ where $|F| = q$.

This conjecture is false. The minimum counterexample is the following pair of group algebras:

$$\mathbb{F}_5C_{12} \simeq \mathbb{F}_5(C_2 \times C_6)\ (\simeq \bigoplus_{i=1}^{4} \mathbb{F}_5 \oplus \bigoplus_{i=1}^{4} \mathbb{F}_{5^2}) \text{ but } |F| \equiv 5(mod\ 12).$$

7.2 $U(FG)$ where Maschke's Theorem does not apply

Now we look at the non-Maschke cases. Again let G be an abelian group. Let p be the characteristic of the field and let e be the order of the group. Let the prime decomposition of e be $q_1^{k_1}.....q_j^{k_j}p^n$ and let $G \simeq H_1 \times H_2$ where $|H_1| = q_1^{k_1}.....q_j^{k_j}$ and $|H_2| = p^n$.

In this case we find $(FH_1)H_2$. For the group algebra FH_1 Maschke's theorem applies, and we can decompose FH_1 into its Wedderburn decomposition using the rules given above. Thus we are left with a sum of group algebras of the form $F'H_2$ where F' is an extension of the field F and so F' will also have characteristic p. Now there are two distinct scenarios. If H_2 is an elementary abelian p-group then we can use Lemma 4.31 to find the structure of the unit group.

Recall that Lemma 4.31 states that

$$U(\mathbb{F}_{p^k}C_p^n) \simeq C_p^{k(p^n-1)} \times C_{p^k-1}.$$

If on the other hand H_2 is not an elementary abelian p group, but is a different type of abelian $p-group$ then we can use Theorem 5.15 to find the structure of the unit group.

Recall that Theorem 5.15 states that if FG is the group algebra $\mathbb{F}_{p^n}(\prod_{i=1}^{m} C_{p^i}^{e_i})$, then

$$U(FG) \simeq \prod_{i=1}^{m} C_{p^i}^{n(|G/\ker(\phi_{i-1})|-2|G/ker(\phi_i)|+|G/ker(\phi_{i+1})|)} \times C_{p^n-1}$$

where $\phi_i(g) = g^{p^i} \ \forall \ g \in G$.

Also we can find the order of each $F'H_2$ by the following Lemma.

Lemma 7.17. *[9] If F is a finite field of order p^k and G is a finite abelian $p-$group of order p^n, then the group of normalised units V is a finite abelian $p-$ group of order $|F|^{|G|-1}$ and exponent dividing p^n. Thus $|U(\mathbb{F}_{p^k}G)| = ((p^k)^{|G|-1})(p^k-1)$.*

7.3 The Unit Groups

Now we can begin to find the unit group of abelian group algebras for specific groups and generalise our results to all fields. In each of the following let q denote the order of the field.

Lemma 7.18. *Let* $FG \simeq \mathbb{F}_q\mathbf{C_2}$. *Then:*

If $q \equiv 0(mod\ 2)$, *the unit group* $U \simeq U(\mathbb{F}_qC_2) \simeq C_2^n \times C_{2^n-1}$.

If $q \equiv 1(mod\ 2)$, *then* $\mathbb{F}_qC_2 \simeq \bigoplus_{i=1}^{2} \mathbb{F}_q$.

Proof. By Corollary 7.9 we only need to look at fields of order $q(mod\ 2)$.
If $q \equiv 0(mod\ 2)$, then $q = 2^n$. Maschke does not apply so there is no Wedderburn decomposition but by Lemma 4.31 the unit group $U \simeq U(\mathbb{F}_qC_2) \simeq C_2^n \times C_{2^n-1}$.
If $q \equiv 1(mod\ 2)$, then $\mathbb{F}_qC_2 \simeq \bigoplus_{i=1}^{2} \mathbb{F}_q$ by Lemma 7.11.

Lemma 7.19. *Let* $FG \simeq \mathbb{F}_q\mathbf{C_3}$. *Then:*

If $q \equiv 0(mod\ 3)$, *the unit group* $U(\mathbb{F}_qC_3) \simeq C_3^n \times C_{3^n-1}$ *where* $q = 3^n$.

If $q \equiv 1(mod\ 3)$, *then* $\mathbb{F}_qC_3 \simeq \bigoplus_{i=1}^{3} \mathbb{F}_q$.

If $q \equiv 2(mod)$, *then* $\mathbb{F}_qC_3 \simeq \mathbb{F}_q \oplus \mathbb{F}_{q^2}$.

Proof. Again we need only check fields of order q $(mod\ 3)$. Let C_3 be

element	1	x	x^2
order	1	3	3

If $q \equiv 0(mod\ 3)$, then $q = 3^n$. By Lemma 4.31 the unit group $U(\mathbb{F}_qC_3) \simeq C_3^n \times C_{3^n-1}$.
If $q \equiv 1(mod\ 3)$, then $\mathbb{F}_qC_3 \simeq \bigoplus_{i=1}^{3} \mathbb{F}_q$ by Lemma 7.11.
If $q \equiv 2(mod\ 3)$, then $\mathbb{F}_qC_3 \simeq \mathbb{F}_q \oplus \mathbb{F}_{q^2}$ by Lemma 4.16 or Lemma 7.12.

Lemma 7.20. *Let* $FG \simeq \mathbb{F}_q\mathbf{C_4}$. *Then:*

If $q \equiv 0(mod\ 4)$, *then* $U(\mathbb{F}_{2^n}C_4) \simeq C_2^n \times C_4^n \times C_{2^n-1}$ *where* $q = 2^n$, $n \geq 2$.

If $q \equiv 1(mod\ 4)$, *then* $F_qC_4 \simeq \bigoplus_{i=1}^{4} \mathbb{F}_q$.

If $q \equiv 2(mod\ 4)$, *then* $U(\mathbb{F}_2C_4) \simeq C_2 \times C_4$.

If $q \equiv 3(mod\ 4)$, *then* $F_qC_4 \simeq \bigoplus_{i=1}^{2} \mathbb{F}_q \oplus \mathbb{F}_{q^2}$.

Proof. Let the elements of C_4 be

element	1	x	x^2	x^3
order	1	4	2	4

If $q \equiv 0(mod\ 4)$, then $q = 2^n$ with $n \geq 2$. Maschke does not apply so there is no Wedderburn decomposition. However, we can still determine the structure of the unit group and by Lemma 5.8, $U(\mathbb{F}_{2^n}C_4) \simeq C_2^n \times C_4^n \times C_{2^n-1}$.
If $q \equiv 1(mod\ 4)$, then $F_qC_4 \simeq \bigoplus_{i=1}^4 \mathbb{F}_q$ by Lemma 7.11.
If $q \equiv 2(mod\ 4)$, then $q = \mathbb{F}_2$ is the only possible field. $U \simeq V \times F^\times \simeq V$. C_4 is a 2-group and so by Lemma 5.3, V is an abelian group of exponent dividing 4, and $|V| = 8$. Further C_4 is a subgroup of V and so there is only one group which satisfies those citeria, and we have $U(\mathbb{F}_2C_4) \simeq C_2 \times C_4$.
If $q \equiv 3(mod\ 4)$, then by Lemma 7.12, $F_qC_4 \simeq \bigoplus_{i=1}^2 \mathbb{F}_q \oplus \mathbb{F}_{q^2}$ because there are 2 elements of order dividing 2 in C_4.

Lemma 7.21. *Let $FG \simeq \mathbb{F}_q\mathbf{C_2^2}$. Then:*

If $q \equiv 0(mod\ 2)$, then the unit group is $C_2^{3n} \times C_{2^n-1}$ where $q = 2^n$, $n \geq 1$.

If $q \equiv 1(mod\ 2)$, then $F_qC_2^2 \simeq \bigoplus_{i=1}^4 \mathbb{F}_q$.

Proof. If $q \equiv 0(mod\ 2)$, then $q = 2^n$ with $n \geq 1$. By Lemma 4.31 the unit group is $C_2^{3n} \times C_{2^n-1}$.
If $q \equiv 1(mod\ 2)$, then $F_qC_2^2 \simeq \bigoplus_{i=1}^4 \mathbb{F}_q$ by Lemma 7.11.

Lemma 7.22. *Let $FG \simeq \mathbb{F}_q\mathbf{C_5}$. Then:*

If $q \equiv 0(mod\ 5)$, then the unit group is $C_5^n \times C_{5^n-1}$, where $q = 5^n$.
If $q \equiv 1(mod\ 5)$, then $\mathbb{F}_qC_5 \simeq \bigoplus_{i=1}^5 \mathbb{F}_q$.
If $q \equiv 2(mod\ 5)$, then $\mathbb{F}_qC_5 \simeq \mathbb{F}_q \oplus \mathbb{F}_{q^4}$.
If $q \equiv 3(mod\ 5)$, then $\mathbb{F}_qC_5 \simeq \mathbb{F}_q \oplus \mathbb{F}_{q^4}$.
If $q \equiv 4(mod\ 5)$, then $\mathbb{F}_qC_5 \simeq \mathbb{F}_q \oplus \bigoplus_{i=1}^2 \mathbb{F}_{q^2}$.

Proof. Let C_5 be

element	1	x	x^2	x^3	x^4
order	1	5	5	5	5

If $q \equiv 0(mod\ 5)$, then $q = 5^n$. By Lemma 4.31 the unit group is $C_5^n \times C_{5^n-1}$.
If $q \equiv 1(mod\ 5)$, then $\mathbb{F}_q C_5 \simeq \bigoplus_{i=1}^{5} \mathbb{F}_q$ by Lemma 7.11.
If $q \equiv 2(mod\ 5)$, by the Perlis Walker Theorem, we take the divisors d of $|C_5|$, and find the order of $q(mod\ d)$. The only divisor of $|C_5|$ is 5, and $2^4 = 1(mod\ 5)$ and so the field extension is $\mathbb{F}_{q^4}$. Thus $\mathbb{F}_q C_5 \simeq \mathbb{F}_q \oplus \mathbb{F}_{q^4}$.
If $q \equiv 3(mod\ 5)$, then by Perlis Walker we have $q^4 = 1(mod\ 5)$, and so $\mathbb{F}_q C_5 \simeq \mathbb{F}_q \oplus \mathbb{F}_{q^4}$.
If $q \equiv 4(mod\ 5)$, then $\mathbb{F}_q C_5 \simeq \mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^2}$ by Lemma 7.12.

Lemma 7.23. *Let $FG \simeq \mathbb{F}_q \mathbf{C_6}$. Then:*

$q \not\equiv 0(mod\ 6)$.

If $q \equiv 1(mod\ 6)$, then $\mathbb{F}_q C_6 \simeq \bigoplus_{i=1}^{6} \mathbb{F}_q$.

If $q \equiv 2(mod\ 6)$, then $\mathbb{F}_q C_6 \simeq \mathbb{F}_{2^n} C_2 \oplus \mathbb{F}_{2^{n^2}} C_2 \simeq \mathbb{F}_{2^n} C_2 \oplus \mathbb{F}_{2^{2n}} C_2$ and the unit group is $C_2^n \times C_{2^n-1} \times C_2^{2n} \times C_{2^{2n}-1}$,where $q = 2^n$, n odd.

If $q \equiv 3(mod\ 6)$, then the unit group is $C_3^n \times C_{3^n-1} \times C_3^n \times C_{3^n-1}$, where $q = 3^n$.

If $q \equiv 4(mod\ 6)$, then the unit group is $C_2^{3n} \times C_{2^n-1}^3$, where $q = 2^n$.

If $q \equiv 5(mod\ 6)$, then $F_q C_6 \simeq \bigoplus_{i=1}^{2} \mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^2}$.

Proof. Let the elements of C_6 be as follows

element	1	x	x^2	x^3	x^4	x^5
order	1	6	3	2	3	6

To decompose this group algebra as a sum of group algebras we use the fact that $C_6 \simeq C_2 \times C_3$.
Clearly $q \not\equiv 0(mod\ 6)$ because the order of a field cannot be a composite number.
If $q \equiv 1(mod\ 6)$, then $\mathbb{F}_q C_6 \simeq \bigoplus_{i=1}^{6} \mathbb{F}_q$ by Lemma 7.11.

If $q \equiv 2(mod\ 6)$, then $\mathbb{F}_q C_6 \simeq (\mathbb{F}_q C_3) C_2 \simeq (\mathbb{F}_q \oplus \mathbb{F}_{q^2}) C_2$ [because q $\equiv 2(mod\ 6) \Rightarrow q \equiv 2(mod\ 3)$] $\simeq \mathbb{F}_q C_2 \oplus \mathbb{F}_{q^2} C_2$.
If $q \equiv 2(mod\ 6)$ then q is an even number and a power of a prime $\Rightarrow q = 0(mod\ 2)$. Also $q^2 \equiv 0(mod\ 2)$.
Looking at the powers of 2, we have $2 \equiv 2(mod\ 6)$. $2^2 \equiv 4(mod\ 6)$. $2^3 \equiv$

$2(mod\ 6)$, and the cycle begins again. Thus the consecutive powers of 2 are alternately $2(mod\ 6)$ and $4(mod\ 6)$. We can say that for $q \equiv 2(mod\ 6)$ then q must be of the form 2^n with n odd. For example if $n = 3$, then $q = 32$. Letting $q = 2^n$, the group algebra is isomorphic to $\mathbb{F}_{2^n}C_2 \oplus \mathbb{F}_{2^{2n}}C_2$ and the unit group is $C_2^n \times C_{2^n-1} \times C_2^{2n} \times C_{2^{2n}-1}$ by Lemma 4.31.

If $q \equiv 3(mod\ 6)$, then $\mathbb{F}_qC_6 \simeq (\mathbb{F}_qC_2)C_3 \simeq (\bigoplus_{i=1}^2 \mathbb{F}_q)C_3$ [because $q \equiv 3(mod\ 6) \Rightarrow q \equiv 1(mod\ 2)$] $\simeq \bigoplus_{i=1}^2 \mathbb{F}_qC_3$. Now $q \equiv 0(mod\ 3)$, and so q is a power of 3. Letting $q = 3^n$, the unit group is $C_3^n \times C_{3^n-1} \times C_3^n \times C_{3^n-1}$ by Lemma 4.31.

If $q \equiv 4(mod\ 6)$, then $\mathbb{F}_qC_6 \simeq (\mathbb{F}_qC_3)C_2 \simeq (\bigoplus_{i=1}^3 \mathbb{F}_q)C_2$ [because $q \equiv 4(mod\ 6) \Rightarrow q \equiv 1(mod\ 3)$] $\simeq \bigoplus_{i=1}^3 \mathbb{F}_qC_2$. Now $q \equiv 4(mod\ 6) \Rightarrow q \equiv 0\ mod\ 2$, so q is a power of 2. Letting $q = 2^n$, the unit group is $\prod_{i=1}^3 (C_2^n \times C_{2^n-1})$ by Lemma 4.31. This is $C_2^{3n} \times C_{2^n-1}^3$.

If $q \equiv 5(mod\ 6)$, then $F_qC_6 \simeq \bigoplus_{i=1}^2 \mathbb{F}_q \oplus \bigoplus_{i=1}^2 \mathbb{F}_{q^2}$ by Lemma 7.12.

Lemma 7.24. *Let $FG \simeq \mathbb{F}_q\mathbf{C_7}$. Then:*

If $q \equiv 0(mod\ 7)$, then the unit group is $C_7^n \times C_{7^n-1}$, where $q = 7^n$.
If $q \equiv 1(mod\ 7)$, then $\mathbb{F}_qC_7 \simeq \bigoplus_{i=1}^7 \mathbb{F}_q$.
If $q \equiv 2(mod\ 7)$, then $\mathbb{F}_qC_7 \simeq \mathbb{F}_q \oplus \bigoplus_{i=1}^2 \mathbb{F}_{q^3}$.
If $q \equiv 3(mod\ 7)$, then $\mathbb{F}_qC_7 \simeq \mathbb{F}_q \oplus \mathbb{F}_{q^6}$.
If $q \equiv 4(mod\ 7)$, then $\mathbb{F}_qC_7 \simeq \mathbb{F}_q \oplus \bigoplus_{i=1}^2 \mathbb{F}_{q^3}$.
If $q \equiv 5(mod\ 7)$, then $\mathbb{F}_qC_7 \simeq \mathbb{F}_q \oplus \mathbb{F}_{q^6}$.
If $q \equiv 6(mod\ 7)$, then $\mathbb{F}_qC_7 \simeq \mathbb{F}_q \oplus \bigoplus_{i=1}^3 \mathbb{F}_{q^2}$.

Proof. Let the elements of C_7 be as follows

element	1	x	x^2	x^3	x^4	x^5	x^6
order	1	6	6	6	6	6	6

If $q \equiv 0(mod\ 7)$, then $q = 7^n$. By Lemma 4.31 the unit group is $C_7^n \times C_{7^n-1}$.
If $q \equiv 1(mod\ 7)$, then $\mathbb{F}_qC_7 \simeq \bigoplus_{i=1}^7 \mathbb{F}_q$ by Lemma 7.11.
If $q \equiv 2(mod\ 7)$, then we use the Perlis Walker Theorem. Note that the exponent of G is 7, and the only divisors are 1 and 7. We find that $o_7(2) =$

3, and there are $6/3 = 2$ copies of $\mathbb{F}_{q^3}$ in the direct summation. Then $\mathbb{F}_q C_7 \simeq \mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^3}$.

If $q \equiv 3(mod\ 7)$, we have $o_7(3) = 6$, and there is $6/6 = 1$ copy of $\mathbb{F}_{q^6}$ in the summand. Thus $\mathbb{F}_q C_7 \simeq \mathbb{F}_q \oplus \mathbb{F}_{q^6}$.

If $q \equiv 4(mod\ 7)$, we have $o_7(4) = 3$, and there are $6/3 = 2$ copies of $\mathbb{F}_{q^3}$ in the summand. Thus $\mathbb{F}_q C_7 \simeq \mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^3}$.

If $q \equiv 5(mod\ 7)$, $o_7(q) = 6 \Rightarrow \mathbb{F}_q(\zeta_7) = \mathbb{F}_{q^6}$ and there is $6/6 = 1$ copies of $\mathbb{F}_{q^6}$ in the summand. Thus $\mathbb{F}_q C_7 \simeq \mathbb{F}_q \oplus \mathbb{F}_{q^6}$.

If $q \equiv 6(mod\ 7)$, then $o_7(q) = 2 \Rightarrow \mathbb{F}_q(\zeta_7) = \mathbb{F}_{q^2}$ and there are $6/2 = 3$ copies of $\mathbb{F}_{q^2}$ in the summand. Thus $\mathbb{F}_q C_7 \simeq \mathbb{F}_q \oplus \bigoplus_{i=1}^{3} \mathbb{F}_{q^2}$. Alternatively we can use Lemma 7.12 when $q \equiv 6(mod\ 7)$.

Lemma 7.25. *Let $FG \simeq \mathbb{F}_{\mathbf{q}}\mathbf{C_8}$. Then:*

If $q \equiv 0(mod\ 8)$, then $U \simeq C_2^{2n} \times C_{2^2}^n \times C_{2^3}^n \times C_{2^n-1}$, where $q = 2^n$, $n \geq 3$.

If $q \equiv 1(mod\ 8)$, then $\mathbb{F}_q C_8 \simeq \bigoplus_{i=1}^{8} \mathbb{F}_q$.

If $q \equiv 2(mod\ 8)$, then $U(\mathbb{F}_2 C_8) \simeq C_8 \times C_4 \times C_2^2$.

If $q \equiv 3(mod\ 8)$, then $\mathbb{F}_q C_8 \simeq \bigoplus_{i=1}^{2} \mathbb{F}_q \oplus \bigoplus_{i=1}^{3} \mathbb{F}_{q^2}$.

If $q \equiv 4(mod\ 8)$, then $U \simeq U(\mathbb{F}_{2^2} C_8) \simeq C_2^4 \times C_{2^2}^2 \times C_{2^3}^2 \times C_3$.

If $q \equiv 5(mod\ 8)$, then $\mathbb{F}_q C_8 \simeq \bigoplus_{i=1}^{4} \mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^2}$.

$q \not\equiv 6(mod\ 8)$.

If $q \equiv 7(mod\ 8)$, then $\mathbb{F}_q C_8 \simeq \bigoplus_{i=1}^{2} \mathbb{F}_q \oplus \bigoplus_{i=1}^{3} \mathbb{F}_{q^2}$.

Proof. Let the elements of C_8 be as follows

element	1	x	x^2	x^3	x^4	x^5	x^6	x^7
order	1	8	4	8	2	8	4	8

If $q \equiv 0(mod\ 8)$, then $q = 2^n$ with $n \geq 3$. Maschke does not apply. However by Lemma 5.18 $U \simeq C_2^{2n} \times C_{2^2}^n \times C_{2^3}^n \times C_{2^n-1}$.

If $q \equiv 1(mod\ 8)$, then $\mathbb{F}_q C_8 \simeq \bigoplus_{i=1}^{8} \mathbb{F}_q$ by Lemma 7.11.

If $q \equiv 2(mod\ 8)$, then the only possible field is $\mathbb{F}_2$ and by Lemma 5.6 $U(\mathbb{F}_2 C_8) \simeq C_8 \times C_4 \times C_2^2$.

If $q \equiv 3(mod\ 8)$, then we use Perlis Walker to establish the decomposition. The divisors of 8 are 1, 2, 4 and 8.
For $d = 8$, we have $3^2 = 9 \equiv 1(mod\ 8)$ so $\mathbb{F}_q(\zeta_8) \simeq \mathbb{F}_{q^2}$ and there are $4/2 =$ 2 copies of $\mathbb{F}_{q^2}$.
For $d = 4$, we have $3^2 = 9 \equiv 1(mod\ 4)$ so $\mathbb{F}_q(\zeta_4) \simeq \mathbb{F}_{q^2}$ and there is $2/2 = 1$ copy of $\mathbb{F}_{q^2}$.
For $d = 2$, we have $3 = 1\ (mod\ 2)$ so $\mathbb{F}_q(\zeta_2) \simeq \mathbb{F}_q$ and there is $1/1 = 1$ copy of $\mathbb{F}_q$. The other summand is $\mathbb{F}_q$ from the element of order 1.
Thus $\mathbb{F}_q C_8 \simeq \bigoplus_{i=1}^{2} \mathbb{F}_q \oplus \bigoplus_{i=1}^{3} \mathbb{F}_{q^2}$.

If $q \equiv 4(mod\ 8)$, then the only possible field is $\mathbb{F}_{2^2}$. By Lemma 5.18 we get $U \simeq U(\mathbb{F}_{2^2} C_8) \simeq C_2^4 \times C_{2^2}^2 \times C_{2^3}^2 \times C_3$.

If $q \equiv 5(mod\ 8)$, then
For $d = 8$, $5^2 = 25 \equiv 1\ (mod\ 8)$ and there are $4/2 = 2$ copies of $\mathbb{F}_{q^2}$.
For $d = 4$, $5 \equiv 1(mod\ 4)$ and there are $2/1 = 2$ copies of $\mathbb{F}_q$.
For $d = 2$, $5 \equiv 1(mod\ 2)$ and there are $1/1 = 1$ copy of $\mathbb{F}_q$.
The other summand is $\mathbb{F}_q$ from the element of order 1.
Thus $\mathbb{F}_q C_8 \simeq \bigoplus_{i=1}^{4} \mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^2}$.

Clearly q $\not\equiv 6(mod\ 8)$.

If $q \equiv 7(mod\ 8)$, then by Lemma 7.12 $\mathbb{F}_q C_8 \simeq \bigoplus_{i=1}^{2} \mathbb{F}_q \oplus \bigoplus_{i=1}^{3} \mathbb{F}_{q^2}$.

Lemma 7.26. *Let* $FG \simeq \mathbb{F}_{\mathbf{q}}\mathbf{C}_{\mathbf{2}}^{\mathbf{3}}$. *Then:*

If $q \equiv 0(mod\ 2)$, then the unit group is $C_2^{7n} \times C_{2^n-1}$, where $q = 2^n$,$n \geq 1$.

If $q \equiv 1(mod\ 2)$, then $F_q C_2^2 \simeq \bigoplus_{i=1}^{8} \mathbb{F}_q$.

Proof. The exponent of this group is 2.

If $q \equiv 0(mod\ 2)$, then $q = 2^n$ with $n \geq 1$. By Lemma 4.31 the unit group is $C_2^{7n} \times C_{2^n-1}$.

If $q \equiv 1(mod\ 2)$, then $F_q C_2^2 \simeq \bigoplus_{i=1}^{8} \mathbb{F}_q$ by Lemma 7.11.

Lemma 7.27. *Let* $FG \simeq \mathbb{F}_{\mathbf{q}}(\mathbf{C_2} \times \mathbf{C_4})$. *Then:*

If $q \equiv 0(mod\ 4)$, *then* $U \simeq C_2^{5n} \times C_4^n \times C_{2^n-1}$, *where* $q = 2^n$,$n \geq 2$.

If $q \equiv 1(mod\ 4)$, *then* $\mathbb{F}_q(C_2 \times C_4) \simeq \bigoplus_{i=1}^{8} \mathbb{F}_q$.

If $q \equiv 2(mod\ 4)$, *then* $U \simeq C_2^5 \times C_4$.

If $q \equiv 3(mod\ 4)$, *then* $\mathbb{F}_q(C_2 \times C_4) \simeq \bigoplus_{i=1}^{4} \mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^2}$. *The unit group is* $C_{q-1}^4 \times C_{q^2-1}^2$.

Proof. Let the elements of $C_2 \times C_4$ be

element	1	x	x^2	x^3	y	xy	x^2y	x^3y
order	1	4	2	4	2	4	2	4

If $q \equiv 0(mod\ 4)$, then $q = 2^n$ with $n \geq 2$. Maschke does not apply. However, by Lemma 5.7 $U \simeq C_2^{5n} \times C_4^n \times C_{2^n-1}$.

If $q \equiv 1(mod\ 4)$, then $\mathbb{F}_q(C_2 \times C_4) \simeq \bigoplus_{i=1}^{8} \mathbb{F}_q$ by Lemma 7.11.

If $q \equiv 2(mod\ 4)$, then the only possible field is $\mathbb{F}_2$ and by Lemma 5.7, $U \simeq C_2^5 \times C_4$.

If $q \equiv 3(mod\ 4)$, then $\mathbb{F}_q(C_2 \times C_4) \simeq \bigoplus_{i=1}^{4} \mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^2}$ by Lemma 7.12. The unit group is $C_{q-1}^4 \times C_{q^2-1}^2$.

Lemma 7.28. *Let* $FG \simeq \mathbb{F}_{\mathbf{q}}\mathbf{C_9}$. *Then:*

If $q \equiv 0(mod\ 9)$, *then* $U \simeq C_3^{4n} \times C_9^{2n} \times C_{3^n-1}$, *where* $q = 3^n$,$n \geq 2$.

If $q \equiv 1(mod\ 9)$, *then* $\mathbb{F}_q C_9 \simeq \bigoplus_{i=1}^{9} \mathbb{F}_q$.

If $q \equiv 2(mod\ 9)$, *then* $\mathbb{F}_q C_9 \simeq \mathbb{F}_q \oplus \mathbb{F}_{q^2} \oplus \mathbb{F}_{q^6}$. *The unit group is* $C_{q-1} \times C_{q^2-1} \times C_{q^6-1}$.

If $q \equiv 3(mod\ 9)$, *then* $U \simeq C_3^4 \times C_9^2 \times C_2$.

If $q \equiv 4(mod\ 9)$, *then* $\mathbb{F}_q C_9 \simeq \bigoplus_{i=1}^{3} \mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^3}$. *The unit group is* $C_{q-1}^3 \times C_{q^3-1}^2$.

If $q \equiv 5(mod\ 9)$, *then* $\mathbb{F}_q C_9 \simeq \mathbb{F}_q \oplus \mathbb{F}_{q^2} \oplus \mathbb{F}_{q^6}$. *The unit group is* $C_{q-1} \times C_{q^2-1} \times C_{q^6-1}$.

$q \not\equiv 6(mod\ 9)$.

If $q \equiv 7(mod\ 9)$, *then* $\mathbb{F}_q C_9 \simeq \bigoplus_{i=1}^{3} \mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^3}$. *The unit group is* $C_{q-1}^3 \times C_{q^3-1}^2$.

If $q \equiv 8$ *then* $\mathbb{F}_q C_9 \simeq \mathbb{F}_q \oplus \bigoplus_{i=1}^{4} \mathbb{F}_{q^2}$. *The unit group is* $C_{q-1} \times C_{q^2-1}^4$.

Proof. Let the elements of C_9 be

element	1	x	x^2	x^3	x^4	x^5	x^6	x^7	x^8
order	1	9	9	3	9	9	3	9	9

If $q \equiv 0(mod\ 9)$, then $q = 3^n$ with $n \geq 2$. Maschke does not apply. However, by Lemma 5.11 $U \simeq C_3^{4n} \times C_9^{2n} \times C_{3^n-1}$.

If $q \equiv 1(mod\ 9)$, then $\mathbb{F}_q C_9 \simeq \bigoplus_{i=1}^{9} \mathbb{F}_q$ by Lemma 7.11.

If $q \equiv 2(mod\ 9)$, then as by Example 7.5 and Corollary 7.9, $\mathbb{F}_q C_9 \simeq \mathbb{F}_q \oplus \mathbb{F}_{q^2} \oplus \mathbb{F}_{q^6}$. The unit group is $C_{q-1} \times C_{q^2-1} \times C_{q^6-1}$.

If $q \equiv 3(mod\ 9)$, then the only possiblility for the field is $\mathbb{F}_3$ as all larger powers of 3 will be multiples of 9 and so will be $= 0(mod\ 9)$. Maschke does not apply. However, by Lemma 5.11 $U \simeq C_3^4 \times C_9^2 \times C_2$.

If $q \equiv 4(mod\ 9)$, then $4^3 = 1(mod\ 9)$ and there are $6/3 = 2$ copies of $\mathbb{F}_{q^3}$.
Also $4 \equiv 1(mod\ 3)$ and there are $2/1 = 2$ copies of $\mathbb{F}_q$ plus another copy of $\mathbb{F}_q$ for the identity element.
Thus $\mathbb{F}_q C_9 \simeq \bigoplus_{i=1}^{3} \mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^3}$. The unit group is $C_{q-1}^3 \times C_{q^3-1}^2$.

If $q \equiv 5(mod\ 9)$, then $5^6 = 1(mod\ 9)$ and there is $6/6 = 1$ copy of $\mathbb{F}_{q^6}$.
Also $5^2 \equiv 1(mod\ 3)$ and there is $2/2 = 1$ copy of $\mathbb{F}_{q^2}$ plus another copy of $\mathbb{F}_q$ for the identity element.
Thus $\mathbb{F}_q C_9 \simeq \mathbb{F}_q \oplus \mathbb{F}_{q^2} \oplus \mathbb{F}_{q^6}$. The unit group is $C_{q-1} \times C_{q^2-1} \times C_{q^6-1}$.

Now q $\not\equiv 6(mod\ 9)$ as all powers of 3 will be either equivalent to $0(mod\ 9)$ or $3(mod\ 9)$.

If $q \equiv 7(mod\ 9)$, then $7^3 = 1(mod\ 9)$ and there are $6/3 = 2$ copies of $\mathbb{F}_{q^3}$.
Also $7 \equiv 1(mod\ 3)$ and there are $2/1 = 2$ copies of $\mathbb{F}_q$ plus another copy of $\mathbb{F}_q$ for the identity element.
Thus $\mathbb{F}_q C_9 \simeq \bigoplus_{i=1}^{3} \mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^3}$. The unit group is $C_{q-1}^3 \times C_{q^3-1}^2$.

If $q \equiv 8 \equiv$ -1$(mod\ 9)$, then $(-1)^2 \equiv 1\ (mod\ 9)$ and there are $6/2 = 3$ copies of $\mathbb{F}_{q^2}$.

Also $8 \equiv 2\ (mod\ 3) \equiv$ -1$(mod\ 3)$ then $(-1)^2 \equiv 1\ (mod\ 3)$ and there are $2/1 = 2$ copies of $\mathbb{F}_{q^2}$ plus another copy of $\mathbb{F}_q$ for the identity element. Alternatively we can use Lemma 7.12. Either way we have $\mathbb{F}_q C_9 \simeq \mathbb{F}_q \oplus \bigoplus_{i=1}^{4} \mathbb{F}_{q^2}$. The unit group is $C_{q-1} \times C_{q^2-1}^4$.

Lemma 7.29. *Let* $FG \simeq \mathbb{F}_q \mathbf{C_3^2}$. *Then:*

If $q \equiv 0(mod\ 3)$, *then the unit group is* $C_3^{8n} \times C_{3^n-1}$, *where* $q = 3^n$ *with* $n \geq 1$.

If $q \equiv 1(mod\ 3)$, *then* $\mathbb{F}_q C_3^2 \simeq \bigoplus_{i=1}^{9} \mathbb{F}_q$.

If $q \equiv 2(mod\ 3)$, *then the unit group is* $C_{q-1} \times C_{q^2-1}^4$.

Proof. If $q \equiv 0(mod\ 3)$, then $q = 3^n$ with $n \geq 1$. By Lemma 4.31 the unit group is $C_3^{8n} \times C_{3^n-1}$.
If $q \equiv 1(mod\ 3)$, then $\mathbb{F}_q C_3^2 \simeq \bigoplus_{i=1}^{9} \mathbb{F}_q$ by Lemma 7.11.
If $q \equiv 2(mod\ 3)$, then by Lemma 7.12, $\mathbb{F}_q C_3^2 \simeq \mathbb{F}_q \oplus \bigoplus_{i=1}^{4} \mathbb{F}_{q^2}$ because there is only one element of order dividing 2 in G, namely the identity. The unit group is $C_{q-1} \times C_{q^2-1}^4$.

Lemma 7.30. *Let* $FG \simeq \mathbb{F}_q \mathbf{C_{10}}$. *Then:*
$q \not\equiv 0(mod\ 10)$
If $q \equiv 1(mod\ 10)$, *then* $\mathbb{F}_q C_{10} \simeq \bigoplus_{i=1}^{10} \mathbb{F}_q$.
If $q \equiv 2(mod\ 10)$, *then the unit group is* $C_2^{5(4n-3)} \times C_{2^{4n-3}-1} \times C_{2^{4(4n-3)}-1}$, *where* $q = 2^{4n-3}$ *for* $n \geq 1$.
If $q \equiv 3(mod\ 10)$, *then* $\mathbb{F}_q C_{10} \simeq \bigoplus_{i=1}^{2} \mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^4}$ *and the unit group is* $C_{q-1}^2 \times C_{q^4-1}^2$.
If $q \equiv 4(mod\ 10)$, *then* $U \simeq C_2^{5(4n-2)} \times C_{2^{4n-2}-1} \times C_{2^{2(4n-2)}-1}^2$, *where* $q = 2^{4n-2}$ *for* $n \geq 1$.
If $q \equiv 5(mod\ 10)$, *then the unit group is* $C_5^{2(4n)} \times C_{5^n-1}^2$, *where* $q = 5^n$.
If $q \equiv 6(mod\ 10)$, *then the unit group is* $C_2^{5(n)} \times C_{2^n-1}^5$,*where* $q = 2^{4n}$ *for* $n \geq 1$.
If $q \equiv 7(mod\ 10)$, *then* $\mathbb{F}_q C_{10} \simeq \bigoplus_{i=1}^{2} \mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^4}$ *and the unit group is* $C_{q-1}^2 \times C_{q^4-1}^2$.
If $q \equiv 8(mod\ 10)$, *then* $U \simeq C_2^{5(4n-1)} \times C_{2^{4n-1}-1} \times C_{2^{4(4n-1)}-1}$, *where* $q =$

2^{4n-1} *for* $n \geq 1$.
If $q \equiv 9(mod\ 10)$, *then the unit group is* $C_{q-1}^2 \times C_{q^2-1}^4$.

Proof. Let the elements of C_{10} be

element	1	x	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9
order	1	10	5	10	5	2	5	10	5	10

We can write $C_{10} \simeq C_2 \times C_5$.
For fields of even order, the order of the field must be a power of 2.
Note that $2^1 \equiv 2(mod\ 10)$, $2^2 \equiv 4(mod\ 10)$, $2^3 \equiv 8(mod\ 10)$, $2^4 \equiv 6(mod\ 10)$, and then we go back full circle because $2^5 \equiv 2(mod\ 10)$.
As a result, $2^1 \equiv 2^5 \equiv 2^9 \equiv 2^{4n-3} \equiv 2(mod\ 10)$ for $n \geq 1$.
Similarly, $2^2 \equiv 2^6 \equiv 2^{10} \equiv 2^{4n-2} \equiv 4(mod\ 10)$ for $n \geq 1$.
Similarly, $2^3 \equiv 2^7 \equiv 2^{11} \equiv 2^{4n-1} \equiv 8(mod\ 10)$ for $n \geq 1$.
Finally, $2^4 \equiv 2^8 \equiv 2^{12} \equiv 2^{4n} \equiv 6(mod\ 10)$ for $n \geq 1$.
We use this in the following descriptions of the unit groups for different fields.
Now q $\not\equiv 0(mod\ 10)$ because q must be a power of a prime.

If $q \equiv 1(mod\ 10)$, then $\mathbb{F}_q C_{10} \simeq \bigoplus_{i=1}^{10} \mathbb{F}_q$ by Lemma 7.11.

If $q \equiv 2(mod\ 10)$, then $\mathbb{F}_q C_{10} \simeq (\mathbb{F}_q C_5)C_2 \simeq (\mathbb{F}_q \oplus \mathbb{F}_{q^4})C_2 \simeq \mathbb{F}_q C_2 \oplus \mathbb{F}_{q^4} C_2$.
Now q must be a power of 2, and from the above calculation we can write q as 2^{4n-3} for $n \geq 1$.
By Lemma 4.31 the unit group is $C_2^{5(4n-3)} \times C_{2^{4n-3}-1} \times C_{2^{4(4n-3)}-1}$.

If $q \equiv 3(mod\ 10)$, then by Perlis Walker,
For $d = 10$, $3^4 = 1(mod\ 10)$ and there is $4/4 = 1$ copy of $\mathbb{F}_{q^4}$.
For $d = 5$, $3^4 = 1(mod\ 5)$ and there is $4/4 = 1$ copy of $\mathbb{F}_{q^4}$.
For $d = 2$, $3 = 1(mod\ 2)$ and there is $1/1 = 1$ copy of $\mathbb{F}_q$.
For $d = 1$, we have a copy of $\mathbb{F}_q$.
Thus $\mathbb{F}_q C_{10} \simeq \bigoplus_{i=1}^{2} \mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^4}$ and the unit group is $C_{q-1}^2 \times C_{q^4-1}^2$.

If $q \equiv 4(mod\ 10)$, we use the same method as for $q = 2(mod\ 10)$ except here q can be written as 2^{4n-2} for $n \geq 1$. The unit group is $C_2^{5(4n-2)} \times C_{2^{4n-2}-1}$

$\times C^2_{2^{2(4n-2)}-1}$.

If $q \equiv 5(mod\ 10)$, then $\mathbb{F}_qC_{10} \simeq (\mathbb{F}_qC_2)C_5 \simeq (\mathbb{F}_q \oplus \mathbb{F}_q)C_5 \simeq \mathbb{F}_qC_5 \oplus \mathbb{F}_qC_5$. Now q must be a power of 5.
By Lemma 4.31 the unit group is $C_5^{2(4n)} \times C^2_{5^n-1}$.

If $q \equiv 6(mod\ 10)$, we use the same method as for $q = 2(mod\ 10)$ except here q can be written as 2^{4n} for $n \geq 1$. $U \simeq C_2^{5(n)} \times C^5_{2^n-1}$,where $q = 2^{4n}$.

If $q \equiv 7(mod\ 10)$, then by Perlis Walker,
For $d = 10$, $7^4 \equiv 1(mod\ 10)$ and there is $4/4 = 1$ copy of $\mathbb{F}_{q^4}$.
For $d = 5$, $7 \equiv 2(mod\ 5)$ and $2^4 = 1(mod\ 5)$. There is $4/4 = 1$ copy of $\mathbb{F}_{q^4}$.
For $d = 2$, $7 \equiv 1(mod\ 2)$ and there is $1/1 = 1$ copy of $\mathbb{F}_q$.
For $d = 1$, we have a copy of $\mathbb{F}_q$.
Thus $\mathbb{F}_qC_{10} \simeq \bigoplus_{i=1}^2 \mathbb{F}_q \oplus \bigoplus_{i=1}^2 \mathbb{F}_{q^4}$ and the unit group is $C^2_{q-1} \times C^2_{q^4-1}$.

If $q \equiv 8(mod\ 10)$, we use the same method as for $q = 2(mod\ 10)$ except here q can be written as 2^{4n-1} for $n \geq 1$. The unit group is $C_2^{5(4n-1)} \times C_{2^{4n-1}-1}$ $\times C_{2^{4(4n-1)}-1}$.

If $q \equiv 9(mod\ 10)$, then $\mathbb{F}_qC_{10} \simeq \bigoplus_{i=1}^2 \mathbb{F}_q \oplus \bigoplus_{i=1}^4 \mathbb{F}_{q^2}$ by Lemma 7.12. The unit group is $C^2_{q-1} \times C^4_{q^2-1}$.

Note that for $FG \simeq \mathbb{F}_q\mathbf{C_{11}}$, the decompositions and the unit groups are in the table which follows this section. The method used here is the same as for other cyclic groups where the order is a prime. We use Perlis Walker and find the order of q $(mod\ 11)$.

Lemma 7.31. *Let $FG \simeq \mathbb{F}_q\mathbf{C_{12}}$. Then:*
$q \not\equiv 0(mod\ 12)$.
If $q \equiv 1(mod\ 12)$ then $\mathbb{F}_qC_{12} \simeq \bigoplus_{i=1}^{12} \mathbb{F}_q$.
If $q \equiv 2(mod\ 12)$, then the unit group of $\mathbb{F}_2C_{12}$ is $C_2^3 \times C_4^3 \times C_3$.
If $q \equiv 3(mod\ 12)$, then $\mathbb{F}_qC_{12} \simeq \bigoplus_{i=1}^2 \mathbb{F}_{3^n}C_3 \oplus \mathbb{F}_{3^{2n}}C_3$. The unit group is $C_3^{8n} \times C^2_{3^n-1} \times C_{3^{2n}-1}$, where $q = 3^n$ for n odd.
If $q \equiv 4(mod\ 12)$, then $U(\bigoplus_{i=1}^3 \mathbb{F}_{2^n}C_4) \simeq C_2^{3n} \times C_4^{3n} \times C^3_{2^n-1}$, where $q =$

2^n *for* n *even.*

If $q \equiv 5(mod\ 12)$*, then* $\mathbb{F}_q C_{12} \simeq \bigoplus_{i=1}^{4} \mathbb{F}_q \oplus \bigoplus_{i=1}^{4} \mathbb{F}_{q^2}$*. The unit group is* $C_{q-1}^4 \times C_{q^2-1}^4$.

$q \not\equiv 6(mod\ 12)$.

If $q \equiv 7(mod\ 12)$*, then* $\mathbb{F}_2 C_{12} \simeq \bigoplus_{i=1}^{6} \mathbb{F}_q \oplus \bigoplus_{i=1}^{3} \mathbb{F}_{q^2}$*. The unit group is* $C_{q-1}^6 \times C_{q^2-1}^3$.

If $q \equiv 8(mod\ 12)$*, then* $U(\mathbb{F}_{2^n} C_4 \oplus \mathbb{F}_{2^{2n}} C_4) \simeq C_2^n \times C_4^n \times C_{2^n-1} \times C_2^{2n} \times C_4^{2n} \times C_{2^{2n}-1} \simeq C_2^{3n} \times C_4^{3n} \times C_{2^n-1} \times C_{2^{2n}-1}$*. Thus* $|U| = (2^{9n})(2^n-1)(2^{2n}-1)$*, where* $q = 2^n$ *for* n *odd and* $n \geq 3$.

If $q \equiv 9(mod\ 12)$*, then the unit group is* $C_3^{4(2n)} \times C_{3^n-1}^2 \times C_{3^{2n}-1}$*, where* $q = 3^n$ *for* n *even.*

$q \not\equiv 10(mod\ 12)$.

If $q \equiv 11(mod\ 12)$*, then* $\mathbb{F}_q C_{12} \simeq \bigoplus_{i=1}^{2} \mathbb{F}_q \oplus \bigoplus_{i=1}^{5} \mathbb{F}_{q^2}$ *and the unit group is* $C_{q-1}^2 \times C_{q^2-1}^5$.

Proof. Let the elements of C_{12} be

element	1	x	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	x^{10}	x^{11}
order	1	12	6	4	3	12	2	12	3	4	6	12

If $|F|(mod\ 12)$ is an even number, then the order of the field must be a power of 2.

Note that $2^1 \equiv 2(mod\ 12)$, $2^2 \equiv 4(mod\ 12)$, $2^3 \equiv 8(mod\ 12)$ and then we go back to 4 again because $2^4 \equiv 4(mod\ 12)$.

As a result, $2^2 \equiv 2^4 \equiv 2^6 \equiv 2^n \equiv 4(mod\ 12)$ for n even.

Similarly, $2^3 \equiv 2^5 \equiv 2^7 \equiv 2^n \equiv 8(mod\ 12)$ for n odd where $n \geq 3$.

Note that this forces all of the powers of 2 (> 1) to be either $\equiv 4(mod\ 12)$ or $\equiv 8(mod\ 12)$, and so in particular we cannot have $q \equiv 6(mod\ 12)$ or $q \equiv 10(mod\ 12)$.

Similarly, if $|F|(mod\ 12)$ is a multiple of 3, then the order of the field must be a power of 3.

Note that $3^1 \equiv 3(mod\ 12)$, $3^2 \equiv 9(mod\ 12)$, $3^3 \equiv 3(mod\ 12)$ and $3^4 \equiv 9(mod\ 12)$. This forces all of the powers of 3 to be either $\equiv 3(mod\ 12)$ or $\equiv 9(mod$

12).
As a result, $3^1 \equiv 3^3 \equiv 3^5 \equiv 3^7 \equiv 3^n \equiv 3(mod\ 12)$ for n odd.
And $3^2 \equiv 3^4 \equiv 3^6 \equiv 3^n \equiv 9(mod\ 12)$ for n even.
We use this in the following descriptions of the unit groups.

Now $q \not\equiv 0(mod\ 12)$ because q cannot be a multiple of 12 as 12 is a composite number and q must be the power of a prime.

If $q \equiv 1(mod\ 12)$ then $\mathbb{F}_q C_{12} \simeq \bigoplus_{i=1}^{12} \mathbb{F}_q$ by Lemma 7.11.

If $q \equiv 2(mod\ 12)$, then there is only one possible field. That is $\mathbb{F}_2$.
$\mathbb{F}_2 C_{12} \simeq (\mathbb{F}_2 C_3)C_4 \simeq (\mathbb{F}_2 \oplus \mathbb{F}_{2^2})C_4 \simeq \mathbb{F}_2 C_4 \oplus \mathbb{F}_{2^2} C_4$.
From our study of the group algebras of C_4 earlier we know that the unit groups of these two summands are $C_2 \times C_4$ and $C_2^2 \times C_4^2 \times C_3$ respectively. Thus the unit group of $\mathbb{F}_2 C_{12}$ is the direct product of these two which is $C_2^3 \times C_4^3 \times C_3$.

If $q \equiv 3(mod\ 12)$, then $\mathbb{F}_q C_{12} \simeq (\mathbb{F}_q C_4)C_3 \simeq (\bigoplus_{i=1}^{2} \mathbb{F}_q \oplus \mathbb{F}_{q^2})C_3 \simeq \bigoplus_{i=1}^{2} \mathbb{F}_q C_3 \oplus \mathbb{F}_{q^2} C_3$.
Now the order of the field q must be a power of 3 where that power is odd, and so we can write $q = 3^n$ for n odd. So the decomposition is $\bigoplus_{i=1}^{2} \mathbb{F}_{3^n} C_3 \oplus \mathbb{F}_{3^{2n}} C_3$. By Lemma 4.31 the unit group is $C_3^{8n} \times C_{3^n-1}^2 \times C_{3^{2n}-1}$.

If $q \equiv 4(mod\ 12)$, then $\mathbb{F}_q C_{12} \simeq (\mathbb{F}_q C_3)C_4 \simeq (\bigoplus_{i=1}^{3} \mathbb{F}_q)C_4 \simeq \bigoplus_{i=1}^{3} \mathbb{F}_q C_4$.
Now the order of the field q must be a power of 2, and only every second power of 2 is equal to $4(mod\ 12)$, so we can write $q = 2^n$ for n even.
Thus $\mathbb{F}_q C_{12} \simeq \bigoplus_{i=1}^{3} \mathbb{F}_{2^n} C_4$. Now, because C_4 is a 2-group, by Lemma 5.8, $U(\bigoplus_{i=1}^{3} \mathbb{F}_{2^n} C_4) \simeq C_2^{3n} \times C_4^{3n} \times C_{2^n-1}^3$.

If $q \equiv 5(mod\ 12)$, then Maschke's Theorem applies, and we can use Perlis Walker to find the Wedderburn decomposition. The divisors of 12 are 12, 6, 4, 3 , 2 and 1.
For $d = 12$, we have $5^2 \equiv 1(mod\ 12)$ and there are $4/2 = 2$ copies of $\mathbb{F}_{q^2}$.
For $d = 6$, we have $5^2 \equiv 1(mod\ 6)$ and there is $2/2 = 1$ copy of $\mathbb{F}_{q^2}$.
For $d = 4$, we have $5 \equiv 1(mod\ 4)$ and there is $2/1 = 2$ copies of $\mathbb{F}_q$.

For $d = 3$, we have $5^2 \equiv 1(mod\ 3)$ and there is $2/2 = 1$ copy of $\mathbb{F}_{q^2}$.
For $d = 2$, we have $5 \equiv 1(mod\ 2)$ and there is $1/1 = 1$ copy of $\mathbb{F}_q$.
For $d = 1$, we have another copy of $\mathbb{F}_q$.
Thus $\mathbb{F}_q C_{12} \simeq \bigoplus_{i=1}^{4} \mathbb{F}_q \oplus \bigoplus_{i=1}^{4} \mathbb{F}_{q^2}$.
The unit group is $C_{q-1}^4 \times C_{q^2-1}^4$.

Now $q \not\equiv 6(mod\ 12)$, because q would have to be divisible by 3 and 2, and q cannot be a composite number.

If $q \equiv 7(mod\ 12)$, then we again use Perlis Walker to find the Wedderburn decomposition.
For $d = 12$, we have $7^2 \equiv 1(mod\ 12)$ and there are $4/2 = 2$ copies of $\mathbb{F}_{q^2}$.
For $d = 6$, we have $7 \equiv 1(mod\ 6)$ and there are $2/1 = 2$ copies of $\mathbb{F}_q$.
For $d = 4$, we have $7^2 \equiv 1(mod\ 4)$ and there is $2/2 = 1$ copy of $\mathbb{F}_{q^2}$.
For $d = 3$, we have $7 \equiv 1(mod\ 3)$ and there are $2/1 = 2$ copies of $\mathbb{F}_q$.
For $d = 2$, we have $7 \equiv 1(mod\ 2)$ and there is $1/1 = 1$ copy of $\mathbb{F}_q$.
For $d = 1$, we have another copy of $\mathbb{F}_q$.
Thus $\mathbb{F}_2 C_{12} \simeq \bigoplus_{i=1}^{6} \mathbb{F}_q \oplus \bigoplus_{i=1}^{3} \mathbb{F}_{q^2}$.
The unit group is $C_{q-1}^6 \times C_{q^2-1}^3$.

If $q \equiv 8(mod\ 12)$, then $\mathbb{F}_q C_{12} \simeq (\mathbb{F}_q C_3)C_4 \simeq (\mathbb{F}_q \oplus \mathbb{F}_{q^2})C_4 \simeq \mathbb{F}_q C_4 \oplus \mathbb{F}_{q^2} C_4$. Now the order of the field q must be a power of 2, and every second power of 2 is equal to $8(mod\ 12)$ starting with 2^3, so we can write $q = 2^n$ for n odd and $n \geq 3$.
Thus $\mathbb{F}_q C_{12} \simeq \mathbb{F}_{2^n} C_4 \oplus \mathbb{F}_{2^{2n}} C_4$. Now, because C_4 is a 2-group, by Lemma 5.8, $U(\mathbb{F}_{2^n} C_4 \oplus \mathbb{F}_{2^{2n}} C_4) \simeq C_2^n \times C_4^n \times C_{2^n-1} \times C_2^{2n} \times C_4^{2n} \times C_{2^{2n}-1} \simeq C_2^{3n} \times C_4^{3n} \times C_{2^n-1} \times C_{2^{2n}-1}$.

If $q \equiv 9(mod\ 12)$, then $\mathbb{F}_q C_{12} \simeq (\mathbb{F}_q C_4)C_3 \simeq (\bigoplus_{i=1}^{4} \mathbb{F}_q)C_3 \simeq \bigoplus_{i=1}^{4} \mathbb{F}_q C_3$.
Now the order of the field q must be a power of 3 where that power is even, and so we can write $q = 3^n$ for n even. By Lemma 4.31 the unit group is $C_3^{4(2n)} \times C_{3^n-1}^2 \times C_{3^{2n}-1}$.

Now $q \not\equiv 10(mod\ 12)$, because the order of a field cannot be a composite

number.

If $q \equiv 11(mod\ 12)$, then $q \equiv$ -1$(mod\ 12)$, and we can use Lemma 7.12. Because there are two elements of order dividing 2, then we have two copies of $\mathbb{F}_q$ in the decomposition and all of the other summands will be $\mathbb{F}_{q^2}$.
Thus $\mathbb{F}_q C_{12} \simeq \bigoplus_{i=1}^{2} \mathbb{F}_q \oplus \bigoplus_{i=1}^{5} \mathbb{F}_{q^2}$ and the unit group is $C_{q-1}^2 \times C_{q^2-1}^5$.

Lemma 7.32. *Let* $FG \simeq \mathbb{F}_{\mathbf{q}}(\mathbf{C_2} \times \mathbf{C_6})$. *Then:*
$q \not\equiv 0(mod\ 6)$.
If $q \equiv 1(mod\ 6)$, *then* $\mathbb{F}_q(C_2 \times C_6) \simeq \bigoplus_{i=1}^{12} \mathbb{F}_q$ *and the unit group is* C_{q-1}^{12}.
If $q \equiv 2(mod\ 6)$, *then the unit group is* $C_2^{9(2n-1)} \times C_{2^{2n-1}-1} \times C_{2^{2(2n-1)}-1}$, *where* $q = 2^{2n-1}$.
If $q \equiv 3(mod\ 6)$, *then* $\mathbb{F}_q(C_2 \times C_6) \simeq \bigoplus_{i=1}^{4} \mathbb{F}_{3^n} C_3$ *and the unit group is* $C_3^{4n} \times C_{3^n-1}^4$, *where* $q = 3^n$.
If $q \equiv 4(mod\ 6)$, *then* $\mathbb{F}_q(C_2 \times C_6) \simeq \bigoplus_{i=1}^{3} \mathbb{F}_{2^{2n}} C_2^2$ *and the unit group is* $C_2^{9(2n)} \times C_{2^{2n}-1}^3$, *where* $q = 2^{2n}$.
If $q \equiv 5(mod\ 6)$, *then* $\mathbb{F}_2 C_{12} \simeq \bigoplus_{i=1}^{4} \mathbb{F}_q \oplus \bigoplus_{i=1}^{4} \mathbb{F}_{q^2}$ *and the unit group is* $C_{q-1}^4 \times C_{q^2-1}^4$.

Proof. Let the elements of $C_2 \times C_6$ be

element	1	x	x^2	x^3	x^4	x^5	y	xy	x^2y	x^3y	x^4y	x^5y
order	1	6	3	2	3	6	2	6	3	2	3	6

If $|F|(mod\ 6)$ is an even number, then the order of the field must be a power of 2.
Note that $2^1 \equiv 2(mod\ 6)$, $2^2 \equiv 4(mod\ 6)$, and then we go back to 2 again because $2^3 \equiv 2(mod\ 12)$.
As a result, $2^1 \equiv 2^3 \equiv 2^5 \equiv 2^{2n-1} \equiv 2(mod\ 6)$ for $n \in \mathbb{N}$.
Similarly, $2^2 \equiv 2^4 \equiv 2^6 \equiv 2^{2n} \equiv 4(mod\ 6)$ for $n \in \mathbb{N}$.
Note that this forces all of the powers of 2 to be either $\equiv 2(mod\ 6)$ or $\equiv 4(mod\ 6)$, and so in particular we cannot have q$\equiv 0(mod\ 6)$. We use this in the following descriptions of the unit groups.

If $q \equiv 1(mod\ 6)$, then $\mathbb{F}_q(C_2 \times C_6) \simeq \bigoplus_{i=1}^{12} \mathbb{F}_q$ by Lemma 7.11 and the unit

group is C_{q-1}^{12}.

If $q \equiv 2(mod\ 6)$, then $\mathbb{F}_q(C_2 \times C_6) \simeq \mathbb{F}_q(C_3 \times C_2^2) \simeq (\mathbb{F}_q C_3)C_2^2 \simeq (\mathbb{F}_q \oplus \mathbb{F}_{q^2})C_2^2$ $\simeq \mathbb{F}_q C_2^2 \oplus \mathbb{F}_{q^2} C_2^2$.
Now q must be a power of 2, and every second power of 2 will be equal to $2(mod\ 6)$ starting with 2^1, and so we can write $q = 2^{2n-1}$.
Thus our decomposition is $\mathbb{F}_{2^{2n-1}} C_2^2 \oplus \mathbb{F}_{2^{2(2n-1)}} C_2^2$.
By Lemma 4.31 the unit group is $C_2^{9(2n-1)} \times C_{2^{2n-1}-1} \times C_{2^{2(2n-1)}-1}$.

If $q \equiv 3(mod\ 6)$, then $\mathbb{F}_q(C_2 \times C_6) \simeq \mathbb{F}_q(C_2^2 \times C_3) \simeq (\mathbb{F}_q C_2^2)C_3 \simeq (\bigoplus_{i=1}^4 \mathbb{F}_q)C_3$.
Now q must be a power of 3, and so we write $q = 3^n$.
Thus our decomposition is $\bigoplus_{i=1}^4 \mathbb{F}_{3^n} C_3$ and by Lemma 4.31 the unit group is $C_3^{4n} \times C_{3^n-1}^4$.

If $q \equiv 4(mod\ 6)$, then $\mathbb{F}_q(C_2 \times C_6) \simeq \mathbb{F}_q(C_3 \times C_2^2) \simeq (\mathbb{F}_q C_3)C_2^2 \simeq (\bigoplus_{i=1}^3 \mathbb{F}_q)C_2^2$ $\simeq \bigoplus_{i=1}^3 (\mathbb{F}_q C_2^2)$.
We can write $q = 2^{2n}$ and our decomposition is $\bigoplus_{i=1}^3 \mathbb{F}_{2^{2n}} C_2^2$.
By Lemma 4.31 the unit group is $C_2^{9(2n)} \times C_{2^{2n}-1}^3$.

If $q \equiv 5(mod\ 6)$, then $q \equiv$ -1$(mod\ 6)$, and we use Lemma 7.12. There are 4 elements of order dividing 2, so we have 4 copies of $\mathbb{F}_q$ and all of the other summands will be $\mathbb{F}_{q^2}$.
Thus $\mathbb{F}_2 C_{12} \simeq \bigoplus_{i=1}^4 \mathbb{F}_q \oplus \bigoplus_{i=1}^4 \mathbb{F}_{q^2}$ and the unit group is $C_{q-1}^4 \times C_{q^2-1}^4$.

For $FG \simeq \mathbb{F}_\mathbf{q}\mathbf{C_{13}}$, the decomposition and unit groups for each field are shown in the General Table of $U(FG)$ at the end of this section.

Similarly for $FG \simeq \mathbb{F}_\mathbf{q}\mathbf{C_{14}}$, the results are shown in the General Table of $U(FG)$ at the end of this section. Note that this group is similar to C_{10} in that it is cyclic with only two divisors.

For $FG \simeq \mathbb{F}_\mathbf{q}\mathbf{C_{15}}$, Note the following:
When $q \equiv 3$, 6, 9 or $12(mod\ 15)$, then q will be a power of 3 and the group algebra decomposes as a sum of group algebras with C_3 as the group. We

then use Lemma 4.31 to find the unit group.
When $q \equiv 5$ or $10(mod\ 15)$, q will be a power of 5, and the group algebra decomposes as a sum of group algebras with C_5 as the group. We again use Lemma 4.31 to find the unit group.
For all other values of q, we can use Perlis Walker to find the Wedderburn decomposition and thus the unit group.
The results for C_{15} are shown in the General Table of $U(FG)$ which follows.

In the table which follows, we show the general unit group of all of the group algebras for abelian groups with order up to 15. The table also shows the Wedderburn decomposition and the decomposition into group algebras where appropriate.

7.4 General Table of $U(FG)$ (G abelian)

G	$\lvert\mathbf{F}\rvert$ *mod* **exp(G)**	$\lvert\mathbf{F}\rvert$	**FG**	**U(FG)**	$\lvert\mathbf{U(FG)}\rvert$
C_1	0	q	$\mathbb{F}_q$	C_{q-1}	$q-1$
C_2	0	2^n		$C_2^n \times C_{2^n-1}$	$2^n(2^n-1)$
C_2	1	q	$\bigoplus_{i=1}^{2} \mathbb{F}_q$	C_{q-1}^2	$(q-1)^2$
C_3	0	3^n		$C_3^n \times C_{3^n-1}$	$3^n(3^n-1)$
C_3	1	q	$\bigoplus_{i=1}^{3} \mathbb{F}_q$	C_{q-1}^3	$(q-1)^3$
C_3	2	q	$\mathbb{F}_q \oplus \mathbb{F}_{q^2}$	$C_{q-1} \times C_{q^2-1}$	$(q-1)(q^2-1)$
C_4	0	2^n		$C_2^n \times C_4^n \times C_{2^n-1}$	$(2^{3n})(2^n-1)$
C_4	1	q	$\bigoplus_{i=1}^{4} \mathbb{F}_q$	C_{q-1}^4	$(q-1)^4$
C_4	2	2		$C_2 \times C_4$	8
C_4	3	q	$\bigoplus_{i=1}^{2} \mathbb{F}_q \oplus \mathbb{F}_{q^2}$	$C_{q-1}^2 \times C_{q^2-1}$	$(q-1)(q^2-1)$
C_2^2	0	2^n		$C_2^{3n} \times C_{2^n-1}$	$(2^{3n})(2^n-1)$
C_2^2	1	q	$\bigoplus_{i=1}^{4} \mathbb{F}_q$	C_{q-1}^4	$(q-1)^4$
C_5	0	5^n		$C_5^n \times C_{5^n-1}$	$5^n(5^n-1)$
C_5	1	q	$\bigoplus_{i=1}^{5} \mathbb{F}_q$	C_{q-1}^5	$(q-1)^5$
C_5	2	q	$\mathbb{F}_q \oplus \mathbb{F}_{q^4}$	$C_{q-1} \times C_{q^4-1}$	$(q-1)(q^4-1)$
C_5	3	q	$\mathbb{F}_q \oplus \mathbb{F}_{q^4}$	$C_{q-1} \times C_{q^4-1}$	$(q-1)(q^4-1)$
C_5	4	q	$\mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^2}$	$C_{q-1} \times C_{q^2-1}^2$	$(q-1)(q^2-1)^2$
C_6	1	q	$\bigoplus_{i=1}^{6} \mathbb{F}_q$	C_{q-1}^6	$(q-1)^6$

Continued on next page

Table 4 – continued from previous page

G	$\lvert\mathbf{F}\rvert$ *mod* **exp(G)**	$\lvert\mathbf{F}\rvert$	**FG**	**U(FG)**	$\lvert\mathbf{U(FG)}\rvert$
C_6	2	2^n n odd	$\mathbb{F}_{2^n}C_2 \oplus \mathbb{F}_{2^{2n}}C_2$	$C_2^{3n} \times C_{2^{2n}-1} \times C_{2^n-1}$	$(2^{3n})(2^n - 1)(2^{2n}-1)$
C_6	3	3^n	$\bigoplus_{i=1}^{2} \mathbb{F}_{3^n}C_3$	$C_3^{2n} \times C_{3^n-1}^2$	$(3^{2n})(3^n-1)^2$
C_6	4	2^n n even	$\bigoplus_{i=1}^{3} \mathbb{F}_{2^k}C_2$	$C_2^{3n} \times C_{2^n-1}^3$	$(2^{3n})(2^n-1)^3$
C_6	5	q	$\bigoplus_{i=1}^{2} \mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^2}$	$C_{q-1}^2 \times C_{q^2-1}^2$	$(q-1)^2(q^2-1)^2$
C_7	0	7^n		$C_7^n \times C_{7^n-1}$	$7^n(7^n-1)$
C_7	1	q	$\bigoplus_{i=1}^{7} \mathbb{F}_q$	C_{q-1}^7	$(q-1)^7$
C_7	2	q	$\mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^3}$	$C_{q-1} \times C_{q^3-1}^2$	$(q-1)(q^3-1)^2$
C_7	3	q	$\mathbb{F}_q \oplus \mathbb{F}_{q^6}$	$C_{q-1} \times C_{q^6-1}$	$(q-1)(q^6-1)$
C_7	4	q	$\mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^3}$	$C_{q-1} \times C_{q^3-1}^2$	$(q-1)(q^3-1)^2$
C_7	5	q	$\mathbb{F}_q \oplus \mathbb{F}_{q^6}$	$C_{q-1} \times C_{q^6-1}$	$(q-1)(q^6-1)$
C_7	6	q	$\mathbb{F}_q \oplus \bigoplus_{i=1}^{3} \mathbb{F}_{q^2}$	$C_{q-1} \times C_{q^2-1}^3$	$(q-1)(q^2-1)^3$
C_8	0	2^n $n \geq 3$		$C_2^{2n} \times C_4^n \times C_8^n \times C_{2^n-1}$	$(2^{7n})(2^n-1)$
C_8	1	q	$\bigoplus_{i=1}^{8} \mathbb{F}_q$	C_{q-1}^8	$(q-1)^8$
C_8	2	2		$C_2^2 \times C_4 \times C_8$	128
C_8	3	q	$\bigoplus_{i=1}^{2} \mathbb{F}_q \oplus \bigoplus_{i=1}^{3} \mathbb{F}_{q^2}$	$C_{q-1}^2 \times C_{q^2-1}^3$	$(q-1)^2(q^2-1)^3$
C_8	4	2^2		$C_2^4 \times C_4^2 \times C_8^2 \times C_3$	$(2^{14})(3)$
C_8	5	q	$\bigoplus_{i=1}^{4} \mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^2}$	$C_{q-1}^4 \times C_{q^2-1}^2$	$(q-1)^4(q^2-1)^2$

Continued on next page

Table 4 – continued from previous page

G	$\lvert\mathbf{F}\rvert$ *mod* **exp(G)**	$\lvert\mathbf{F}\rvert$	**FG**	**U(FG)**	$\lvert\mathbf{U(FG)}\rvert$
C_8	7	q	$\bigoplus_{i=1}^{2}\mathbb{F}_q \oplus \bigoplus_{i=1}^{3}\mathbb{F}_{q^2}$	$C_{q-1}^2 \times C_{q^2-1}^3$	$(q-1)^2(q^2-1)^3$
$C_2 \times C_4$	0	2^n $n \geq 2$		$C_2^{5n} \times C_4^n \times C_{2^n-1}$	$(2^{7n})(2^n-1)$
$C_2 \times C_4$	1	q	$\bigoplus_{i=1}^{8}\mathbb{F}_q$	C_{q-1}^8	$(q-1)^8$
$C_2 \times C_4$	2	2		$C_2^5 \times C_4$	128
$C_2 \times C_4$	3	q	$\bigoplus_{i=1}^{4}\mathbb{F}_q \oplus \bigoplus_{i=1}^{2}\mathbb{F}_{q^2}$	$C_{q-1}^4 \times C_{q^2-1}^2$	$(q-1)^4(q^2-1)^2$
C_2^3	0	2^n		$C_2^{7n} \times C_{2^n-1}$	$(2^{7n})(2^n-1)$
C_2^3	1	q	$\bigoplus_{i=1}^{8}\mathbb{F}_q$	C_{q-1}^8	$(q-1)^8$
C_9	0	3^n $n \geq 2$		$C_3^{4n} \times C_9^{2n} \times C_{3^n-1}$	$(3^{8n})(3^n-1)$
C_9	1	q	$\bigoplus_{i=1}^{9}\mathbb{F}_q$	C_{q-1}^9	$(q-1)^9$
C_9	2	q	$\mathbb{F}_q \oplus \mathbb{F}_{q^2} \oplus \mathbb{F}_{q^6}$	$C_{q-1} \times C_{q^2-1} \times C_{q^6-1}$	$(q-1)(q^2-1)(q^6-1)$
C_9	3	3		$C_3^4 \times C_9^2 \times C_2$	$(2)(3^8)$
C_9	4	q	$\bigoplus_{i=1}^{3}\mathbb{F}_q \oplus \bigoplus_{i=1}^{2}\mathbb{F}_{q^3}$	$C_{q-1}^3 \times C_{q^3-1}^2$	$(q-1)^3(q^3-1)^2$

Continued on next page

Table 4 – continued from previous page

G	$\lvert\mathbf{F}\rvert$ *mod* **exp(G)**	$\lvert\mathbf{F}\rvert$	**FG**	**U(FG)**	$\lvert\mathbf{U(FG)}\rvert$
C_9	5	q	$\mathbb{F}_q \oplus \mathbb{F}_{q^2} \oplus \mathbb{F}_{q^6}$	$C_{q-1} \times C_{q^2-1} \times C_{q^6-1}$	$(q-1)(q^2-1)(q^6-1)$
C_9	7	q	$\bigoplus_{i=1}^{3} \mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^3}$	$C_{q-1}^3 \times C_{q^3-1}^2$	$(q-1)^3(q^3-1)^2$
C_9	8	q	$\mathbb{F}_q \oplus \bigoplus_{i=1}^{4} \mathbb{F}_{q^2}$	$C_{q-1} \times C_{q^2-1}^4$	$(q-1)(q^2-1)^4$
C_3^2	0	3^n		$C_3^{8n} \times C_{3^n-1}$	$(3^{8n})(3^n-1)$
C_3^2	1	q	$\bigoplus_{i=1}^{9} \mathbb{F}_q$	C_{q-1}^9	$(q-1)^9$
C_3^2	2	q	$\mathbb{F}_q \oplus \bigoplus_{i=1}^{4} \mathbb{F}_{q^2}$	$C_{q-1} \times C_{q^2-1}^4$	$(q-1)(q^2-1)^4$
C_{10}	1	q	$\bigoplus_{i=1}^{10} \mathbb{F}_q$	C_{q-1}^{10}	$(q-1)^{10}$
C_{10}	2	$q = 2^{4n-3}$ $n \geq 1$	$\mathbb{F}_q C_2 \oplus \mathbb{F}_{q^4} C_2$	$C_2^{5(4n-3)} \times C_{2^{4n-3}-1} \times C_{2^{4(4n-3)}-1}$	$(2^{5(4n-3)})(2^{4n-3}-1)(2^{4(4n-3)}-1)$
C_{10}	3	q	$\bigoplus_{i=1}^{2} \mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^4}$	$C_{q-1}^2 \times C_{q^4-1}^2$	$(q-1)^2(q^4-1)^2$
C_{10}	4	$q = 2^{4n-2}$ $n \geq 1$	$\mathbb{F}_q C_2 \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^2} C_2$	$C_2^{5(4n-2)} \times C_{2^{4n-2}-1} \times C_{2^{2(4n-2)}-1}^2$	$(2^{5(4n-2)})(2^{4n-2}-1)(2^{2(4n-2)}-1)^2$
C_{10}	5	$q = 5^n$ $n \geq 1$	$\bigoplus_{i=1}^{2} \mathbb{F}_q C_5$	$C_5^{2(4n)} \times C_{5^n-1}^2$	$(5^{2(4n)})(5^n-1)^2$
C_{10}	6	$q = 2^{4n}$ $n \geq 1$	$\bigoplus_{i=1}^{5} \mathbb{F}_q C_2$	$C_2^{5(n)} \times C_{2^n-1}^5$	$(2^{5(n)})(2^n-1)^5$
C_{10}	7	q	$\bigoplus_{i=1}^{2} \mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^4}$	$C_{q-1}^2 \times C_{q^4-1}^2$	$(q-1)^2(q^4-1)^2$

Continued on next page

Table 4 – continued from previous page

G	$\lvert\mathbf{F}\rvert$ *mod* **exp(G)**	$\lvert\mathbf{F}\rvert$	**FG**	**U(FG)**	$\lvert\mathbf{U(FG)}\rvert$
C_{10}	8	$q = 2^{4n-1}$ $n \geq 1$	$\mathbb{F}_q C_2 \oplus \mathbb{F}_{q^4} C_2$	$C_2^{5(4n-1)} \times C_{2^{4n-1}-1} \times C_{2^{4(4n-1)}-1}$	$(2^{5(4n-1)})(2^{4n-1}-1)(2^{4(4n-1)}-1)$
C_{10}	9	q	$\bigoplus_{i=1}^{2} \mathbb{F}_q \oplus \bigoplus_{i=1}^{4} \mathbb{F}_{q^2}$	$C_{q-1}^2 \times C_{q^2-1}^4$	$(q-1)^2(q^2-1)^4$
C_{11}	0	11^n		$C_{11}^n \times C_{11^n-1}$	$11^n(11^n-1)$
C_{11}	1	q	$\bigoplus_{i=1}^{11} \mathbb{F}_q$	C_{q-1}^{11}	$(q-1)^7$
C_{11}	2	q	$\mathbb{F}_q \oplus \mathbb{F}_{q^{10}}$	$C_{q-1} \times C_{q^{10}-1}$	$(q-1)(q^{10}-1)$
C_{11}	3	q	$\mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^5}$	$C_{q-1} \times C_{q^5-1}^2$	$(q-1)(q^5-1)^2$
C_{11}	4	q	$\mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^5}$	$C_{q-1} \times C_{q^5-1}^2$	$(q-1)(q^5-1)^2$
C_{11}	5	q	$\mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^5}$	$C_{q-1} \times C_{q^5-1}^2$	$(q-1)(q^5-1)^2$
C_{11}	6	q	$\mathbb{F}_q \oplus \mathbb{F}_{q^{10}}$	$C_{q-1} \times C_{q^{10}-1}$	$(q-1)(q^{10}-1)$
C_{11}	7	q	$\mathbb{F}_q \oplus \mathbb{F}_{q^{10}}$	$C_{q-1} \times C_{q^{10}-1}$	$(q-1)(q^{10}-1)$
C_{11}	8	q	$\mathbb{F}_q \oplus \mathbb{F}_{q^{10}}$	$C_{q-1} \times C_{q^{10}-1}$	$(q-1)(q^{10}-1)$
C_{11}	9	q	$\mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^5}$	$C_{q-1} \times C_{q^5-1}^2$	$(q-1)(q^5-1)^2$
C_{11}	10	q	$\mathbb{F}_q \oplus \bigoplus_{i=1}^{5} \mathbb{F}_{q^2}$	$C_{q-1} \times C_{q^2-1}^5$	$(q-1)(q^2-1)^5$
C_{12}	1	q	$\bigoplus_{i=1}^{12} \mathbb{F}_q$	C_{q-1}^{12}	$(q-1)^{12}$
C_{12}	2	2	$\mathbb{F}_2 C_4 \oplus \mathbb{F}_{2^2} C_4$	$C_2^3 \times C_4^3 \times C_3$	$(2^9)(3)$
C_{12}	3	3^n n odd	$\bigoplus_{i=1}^{2} \mathbb{F}_{3^n} C_3 \oplus \mathbb{F}_{3^{2n}} C_3$	$C_3^{8n} \times C_{3^n-1}^2 \times C_{3^{2n}-1}$	$(3^{8n})(3^n-1)^2(3^{2n}-1)$
C_{12}	4	2^n n even	$\bigoplus_{i=1}^{3} \mathbb{F}_{2^n} C_4$	$C_2^{3n} \times C_4^{3n} \times C_{2^n-1}^3$	$(2^{9n})(2^n-1)^3$
C_{12}	5	q	$\bigoplus_{i=1}^{4} \mathbb{F}_q \oplus \bigoplus_{i=1}^{4} \mathbb{F}_{q^2}$	$C_{q-1}^4 \times C_{q^2-1}^4$	$(q-1)^4(q^2-1)^4$

Continued on next page

Table 4 – continued from previous page

G	$\lvert\mathbf{F}\rvert$ *mod* **exp(G)**	$\lvert\mathbf{F}\rvert$	**FG**	**U(FG)**	$\lvert\mathbf{U(FG)}\rvert$
C_{12}	7	q	$\bigoplus_{i=1}^{6}\mathbb{F}_q \oplus \bigoplus_{i=1}^{3}\mathbb{F}_{q^2}$	$C_{q-1}^{6} \times C_{q^2-1}^{3}$	$(q-1)^4(q^2-1)^4$
C_{12}	8	2^n n odd, $n \geq 3$	$\mathbb{F}_{2^n}C_4 \oplus \mathbb{F}_{2^{2n}}C_4$	$C_2^{3n} \times C_4^{3n} \times C_{2^n-1} \times C_{2^{2n}-1}$	$(2^{9n})(2^n - 1)(2^{2n}-1)$
C_{12}	9	3^n n even	$\bigoplus_{i=1}^{4}\mathbb{F}_{3^n}C_3$	$C_3^{4(2n)} \times C_{3^n-1}^{2} \times C_{3^{2n}-1}$	$(3^{4(2n)})(3^n - 1)^2(3^{2n}-1)$
C_{12}	11	q	$\bigoplus_{i=1}^{2}\mathbb{F}_q \oplus \bigoplus_{i=1}^{5}\mathbb{F}_{q^2}$	$C_{q-1}^{2} \times C_{q^2-1}^{5}$	$(q-1)^2(q^2-1)^5$
$C_2 \times C_6$	1	q	$\bigoplus_{i=1}^{12}\mathbb{F}_q$	C_{q-1}^{12}	$(q-1)^{12}$
$C_2 \times C_6$	2	$q = 2^{2n-1}$	$\mathbb{F}_{2^{2n-1}}C_2^2 \oplus \mathbb{F}_{2^{2(2n-1)}}C_2^2$	$C_2^{9(2n-1)} \times C_{2^{2n-1}-1} \times C_{2^{2(2n-1)}-1}$	$(2^{9(2n-1)})(2^{2n-1}-1)(2^{2(2n-1)}-1)$
$C_2 \times C_6$	3	$q = 3^n$	$\bigoplus_{i=1}^{4}\mathbb{F}_{3^n}C_3$	$C_3^{4n} \times C_{3^n-1}^{4}$	$(3^{4n})(3^n-1)^4$
$C_2 \times C_6$	4	2^{2n} $n \geq 1$	$\bigoplus_{i=1}^{3}\mathbb{F}_{2^{2n}}C_2^2$	$C_2^{18n} \times C_{2^{2n}-1}^{3}$	$(2^{18n})(2^{2n}-1)^3$
$C_2 \times C_6$	5	q	$\bigoplus_{i=1}^{4}\mathbb{F}_q \oplus \bigoplus_{i=1}^{4}\mathbb{F}_{q^2}$	$C_{q-1}^{4} \times C_{q^2-1}^{4}$	$(q-1)^4(q^2-1)^4$
C_{13}	0	13^n		$C_{13}^{n} \times C_{13^n-1}$	$(13^n)(13^n-1)$
C_{13}	1	q	$\bigoplus_{i=1}^{13}\mathbb{F}_q$	C_{q-1}^{13}	$(q-1)^3$

Continued on next page

Table 4 – continued from previous page

G	$\lvert\mathbf{F}\rvert$ *mod* **exp(G)**	$\lvert\mathbf{F}\rvert$	**FG**	**U(FG)**	$\lvert\mathbf{U(FG)}\rvert$
C_{13}	2	q	$\mathbb{F}_q \oplus \mathbb{F}_{q^{12}}$	$C_{q-1} \times C_{q^{12}-1}$	$(q-1)(q^{12}-1)$
C_{13}	3	q	$\mathbb{F}_q \oplus \bigoplus_{i=1}^{4} \mathbb{F}_{q^3}$	$C_{q-1} \times C_{q^3-1}^4$	$(q-1)(q^3-1)^4$
C_{13}	4	q	$\mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^6}$	$C_{q-1} \times C_{q^6-1}^2$	$(q-1)(q^6-1)^2$
C_{13}	5	q	$\mathbb{F}_q \oplus \bigoplus_{i=1}^{3} \mathbb{F}_{q^4}$	$C_{q-1} \times C_{q^4-1}^3$	$(q-1)(q^4-1)^3$
C_{13}	6	q	$\mathbb{F}_q \oplus \mathbb{F}_{q^{12}}$	$C_{q-1} \times C_{q^{12}-1}$	$(q-1)(q^{12}-1)$
C_{13}	7	q	$\mathbb{F}_q \oplus \mathbb{F}_{q^{12}}$	$C_{q-1} \times C_{q^{12}-1}$	$(q-1)(q^{12}-1)$
C_{13}	8	q	$\mathbb{F}_q \oplus \bigoplus_{i=1}^{3} \mathbb{F}_{q^4}$	$C_{q-1} \times C_{q^4-1}^3$	$(q-1)(q^4-1)^3$
C_{13}	9	q	$\mathbb{F}_q \oplus \bigoplus_{i=1}^{4} \mathbb{F}_{q^3}$	$C_{q-1} \times C_{q^3-1}^4$	$(q-1)(q^3-1)^4$
C_{13}	10	q	$\mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^6}$	$C_{q-1} \times C_{q^6-1}^2$	$(q-1)(q^6-1)^2$
C_{13}	11	q	$\mathbb{F}_q \oplus \mathbb{F}_{q^{12}}$	$C_{q-1} \times C_{q^{12}-1}$	$(q-1)(q^{12}-1)$
C_{13}	12	q	$\mathbb{F}_q \oplus \bigoplus_{i=1}^{6} \mathbb{F}_{q^2}$	$C_{q-1} \times C_{q^2-1}^6$	$(q-1)(q^2-1)^6$
C_{14}	1	q	$\bigoplus_{i=1}^{14} \mathbb{F}_q$	C_{q-1}^{14}	$(q-1)^{14}$
C_{14}	2	$q = 2^{3n-2}$ $n \geq 1$	$\mathbb{F}_q C_2 \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^3} C_2$	$C_2^{7(3n-2)} \times C_{2^{3n-2}-1} \times C_{2^{3(3n-2)}-1}^2$	$(2^{7(3n-2)})(2^{3n-2}-1)(2^{3(3n-2)}-1)^2$
C_{14}	3	q	$\bigoplus_{i=1}^{2} \mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^6}$	$C_{q-1}^2 \times C_{q^6-1}^2$	$(q-1)^2(q^6-1)^2$
C_{14}	4	$q = 2^{3n-1}$ $n \geq 1$	$\mathbb{F}_q C_2 \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^3} C_2$	$C_2^{7(3n-1)} \times C_{2^{3n-1}-1} \times C_{2^{3(3n-1)}-1}^2$	$(2^{7(3n-1)})(2^{3n-1}-1)(2^{3(3n-1)}-1)^2$
C_{14}	5	q	$\bigoplus_{i=1}^{2} \mathbb{F}_q \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^6}$	$C_{q-1}^2 \times C_{q^6-1}^2$	$(q-1)^2(q^6-1)^2$
C_{14}	7	$q = 7^n$, $n \geq 1$	$\bigoplus_{i=1}^{2} \mathbb{F}_q C_7$	$C_7^{2(6n)} \times C_{7^n-1}^2$	$(7^{2(6n)})(7^n-1)^2$

Continued on next page

Table 4 – continued from previous page

G	$\lvert\mathbf{F}\rvert$ *mod* **exp(G)**	$\lvert\mathbf{F}\rvert$	**FG**	**U(FG)**	$\lvert\mathbf{U}(\mathbf{FG})\rvert$
C_{14}	8	$q = 2^{3n}$ $n \geq 1$	$\bigoplus_{i=1}^{7} \mathbb{F}_q C_2$	$C_2^{7(3n)} \times C_{2^{3n}-1}^{7}$	$(2^{7(3n)})(2^{3n}-1)^7$
C_{14}	9	q	$\bigoplus_{i=1}^{2} \mathbb{F}_q \oplus \bigoplus_{i=1}^{4} \mathbb{F}_{q^3}$	$C_{q-1}^2 \times C_{q^3-1}^4$	$(q-1)^2(q^3-1)^4$
C_{14}	11	q	$\bigoplus_{i=1}^{2} \mathbb{F}_q \oplus \bigoplus_{i=1}^{4} \mathbb{F}_{q^3}$	$C_{q-1}^2 \times C_{q^3-1}^4$	$(q-1)^2(q^3-1)^4$
C_{14}	13	q	$\bigoplus_{i=1}^{2} \mathbb{F}_q \oplus \bigoplus_{i=1}^{6} \mathbb{F}_{q^2}$	$C_{q-1}^2 \times C_{q^2-1}^6$	$(q-1)^2(q^2-1)^6$
C_{15}	1	q	$\bigoplus_{i=1}^{15} \mathbb{F}_q$	C_{q-1}^{15}	$(q-1)^{12}$
C_{15}	2	q	$\mathbb{F}_q \oplus \mathbb{F}_{q^2} \oplus \bigoplus_{i=1}^{3} \mathbb{F}_{q^4}$	$C_{q-1} \times C_{q^2-1} \times C_{q^4-1}^3$	$(q-1)(q^2-1)(q^4-1)^3$
C_{15}	3	$q = 3^{4n-3}$ $n \geq 1$	$\mathbb{F}_q C_3 \oplus \mathbb{F}_{q^4} C_3$	$C_3^{10(4n-3)} \times C_{3^{4n-3}-1} \times C_{3^{4(4n-3)}-1}$	$(3^{10(4n-3)})(3^{4n-3}-1)(3^{4(4n-3)}-1)$
C_{15}	4	q	$\mathbb{F}_q \oplus \bigoplus_{i=1}^{7} \mathbb{F}_{q^2}$	$C_{q-1} \times C_{q^2-1}^7$	$(q-1)(q^2-1)^7$
C_{15}	5	$q = 5^{2n-1}$ $n \geq 1$	$\mathbb{F}_q C_5 \oplus \mathbb{F}_{q^2} C_5$	$C_5^{12(2n-1)} \times C_{5^{(2n-1)}-1} \times C_{5^{2(2n-1)}-1}$	$(5^{12(2n-1)})(5^{(2n-1)}-1)(5^{2(2n-1)}-1)$
C_{15}	6	$q = 3^{4n}$, $n \geq 1$	$\bigoplus_{i=1}^{5} \mathbb{F}_q C_3$	$C_3^{10(4n)} \times C_{3^{4n}-1}^5$	$(3^{10(4n)})(3^{4n}-1)^5$
C_{15}	7	q	$\bigoplus_{i=1}^{3} \mathbb{F}_q \oplus \bigoplus_{i=1}^{3} \mathbb{F}_{q^4}$	$C_{q-1}^3 \times C_{q^4-1}^3$	$(q-1)^3(q^4-1)^3$
C_{15}	8	q	$\mathbb{F}_q \oplus \mathbb{F}_{q^2} \oplus \bigoplus_{i=1}^{3} \mathbb{F}_{q^4}$	$C_{q-1} \times C_{q^2-1} \times C_{q^4-1}^3$	$(q-1)(q^2-1)(q^4-1)^3$

Continued on next page

Table 4 – continued from previous page

G	$\lvert\mathbf{F}\rvert$ *mod* **exp(G)**	$\lvert\mathbf{F}\rvert$	**FG**	**U(FG)**	$\lvert\mathbf{U(FG)}\rvert$
C_{15}	9	$q = 3^{4n-2}$ $n \geq 1$	$\mathbb{F}_q C_3 \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{q^2} C_3$	$C_3^{10(4n-2)} \times C_{3^{4n-2}-1} \times C_{3^{2(4n-2)}-1}^2$	$(3^{10(4n-2)})(3^{4n-2}-1)(3^{2(4n-2)}-1)^2$
C_{15}	10	$q = 5^{2n}$ $n \geq 1$	$\bigoplus_{i=1}^{3} \mathbb{F}_q C_5$	$C_5^{12(2n)} \times C_{5^{(2n)}-1}^3$	$(5^{12(2n)})(5^{(2n)}-1)^3$
C_{15}	11	q	$\bigoplus_{i=1}^{5} \mathbb{F}_q \oplus \bigoplus_{i=1}^{5} \mathbb{F}_{q^2}$	$C_{q-1}^5 \times C_{q^2-1}^5$	$(q-1)^5(q^2-1)^5$
C_{15}	12	$q = 3^{4n-1}$ $n \geq 1$	$\mathbb{F}_q C_3 \oplus \mathbb{F}_{q^4} C_3$	$C_3^{10(4n-1)} \times C_{3^{4n-1}-1} \times C_{3^{4(4n-1)}-1}$	$(3^{10(4n-1)})(3^{4n-1}-1)(3^{4(4n-1)}-1)$
C_{15}	13	q	$\bigoplus_{i=1}^{3} \mathbb{F}_q \oplus \bigoplus_{i=1}^{3} \mathbb{F}_{q^4}$	$C_{q-1}^3 \times C_{q^4-1}^3$	$(q-1)^3(q^4-1)^3$
C_{15}	14	q	$\mathbb{F}_q \oplus \bigoplus_{i=1}^{7} \mathbb{F}_{q^2}$	$C_{q-1} \times C_{q^2-1}^7$	$(q-1)(q^2-1)^7$

Table 4: General Table of U(FG)

8 Conclusion

The first task in this masters project involved understanding the challenges posed in finding good linear error correcting codes for digital communication. The Introduction Chapter highlights the role that abstract algebra and in particular group rings can play in this. Throughout this thesis, the aim is to improve our understanding of the structure of group rings and thus the underlying structure of code subspaces. In setting out to achieve this a number of related areas have been researched.

The task of finding the automorphisms of groups seems like a very simple problem, but is in fact quite complicated, and it continues to exercise mathematicians today. Journal papers by Curran and Bidwell [2], [3] and [11] as well as Hillar and Rhea [17] give a good insight into how to approach the same problem from different angles. Results in this area make up Chapters 2 and 3 and there are tables at the end of each Chapter showing the automorphism groups of small abelian and non-abelian groups. At the end of Chapter 3, the interesting question of terminating automorphism towers is explored, and a table is provided showing the automorphism tower of selected groups.

The next stage of this masters project involved looking at group algebras, decomposing them and finding unit groups. Again, the initial challenge was getting immersed in the basics of the subject, exploring the structures of group algebras, finding which elements decomposed in to which summands and how these elements formed unit groups. Chapter 4 gives many examples of this detailed exploration. It is at this stage that some very satisfying results are obtained.

One of these results is Theorem 5.15. This Theorem gives a method for finding the unit group of any group algebra FG where F has characteristic p and G is an abelian $p-group$. This Theorem has its origins in the basic technique used to find the unit group of $\mathbb{F}_{2^2}(C_2 \times C_4)$ in Example 5.7. The method used involves counting the elements of order p^n in the normalised unit group. Throughout Chapter 5 this counting technique is generalised to larger and more complex abelian $p-groups$ and as a result the notation

becomes more complicated. In order to find a method that can be easily applied to all abelian $p-groups$ it was necessary to find a concise notation. This was achieved, writing the orders of the factor groups in terms of the kernels of homomorphisms and so the result is Theorem 5.15.

Another satisfying result is the adaptation of the Perlis Walker Theorem in Chapter 7, looking at $exponent(G)$ instead of $|G|$, and looking at $|F|$ modulo $\exp(G)$ rather than $|F|$. These are presented as corollaries to the Perlis Walker Theorem. By using these corollaries it is possible to complete a general table (using the results of Theorem 5.15 as well in places) which gives the structure of the unit group for all commutative group algebras. This table is completed for all commutative group algebras FG where $|G| < 16$ and where the order of F is any prime power. This table can be extended easily as the methods used can be applied to all commutative group algebras. The corollaries, the general table and the work involved in building the table make up Chapter 7.

Now not only has this extension of the Perlis Walker Theorem been useful for completing the table, but it has also showed a number of counterexamples to the Isomorphism Problem (where $FG \simeq FH$ but $G \ncong H$), and indeed has revealed two whole classes of counterexamples. This is yet another satisfying result and is worthy of further exploration.

A surprising result not mentioned in the thesis (because it was already developed more thoroughly by Broche and del Rio [6]) is as follows:

Let FG be a group algebra where G is cyclic of order n and where n and $char(F)$ are co-prime. For example, the group algebra $\mathbb{F}_2C_{11}$. Multiply the order of F by itself repeatedly, calculating the result$(mod\ 11)$ until we get back to the start. The result is a cycle of length 10 which is (2, 4, 8, 5, 10, 9, 7, 3, 6, 1) (if we keep going we get 2 again). Identifying the elements of C_{11} with $\mathbb{Z}_{11}$, we can see that the other element of $\mathbb{Z}_{11}$ is (0) which gives a cycle of length 1 when we multiply it by 2. The lengths of these cycles corresponds to the decomposition of $\mathbb{F}_2C_{11}$ which is $\mathbb{F}_2 \oplus \mathbb{F}_{2^{10}}$. This technique can be applied to other group algebras FG of this type. For example $\mathbb{F}_2C_7$. The

first cycle is (2, 4, 1). Then we take another element of $\mathbb{Z}_7$ such as 3 and begin a new cycle. We get (3, 6, 5) and are done. Then (0) gives the last cycle. Again this corresponds to the decomposition of $\mathbb{F}_2 C_7$ which is $\mathbb{F}_2 \oplus \bigoplus_{i=1}^{2} \mathbb{F}_{2^3}$ (i.e. two 3-cycles and one 1-cycle).

Although independently discovered, this method is well known, and involves *cyclotomic classes* of G. Broche and Del Rio's paper explains it in detail, and using character theory the technique can be applied to non-cyclic groups and finds not only the Wedderburn decomposition but also the primitive central orthogonal idempotents associated with each summand.

In Chapter 6, this technique is applied and the primitive idempotents for some group algebras are found. This section of the thesis has useful implications for coding theory as it unravels the structure of these group algebras in more detail and suggests an alternative method for constructing codes. For instance, in Example 6.21 we get the Wedderburn decomposition of $\mathbb{F}_2 C_7$, and find that $1 + x^3 + x^5 + x^6$ is an idempotent associated with a summand isomorphic to $\mathbb{F}_{2^3}$. The idempotent $\hat{G}$ is associated with the summand isomorphic to $\mathbb{F}_2$. Computation shows that the direct sum of these two summands gives a sub-module of order 16, which is isomorphic as a vector space to the Hamming (7,4,3) code described in Example 1.12. Note that the element $1 + x^3 + x^5 + x^6$ can be written as a vector in F_2^7 as $[1, 0, 0, 1, 0, 1, 1]$, while $\hat{G}$ can be written as $[1, 1, 1, 1, 1, 1, 1]$. The technique for finding the primitive central idempotents is fully explained in Chapter 6, and a table at the end of the Chapter gives the decomposition and unit group of selected group algebras.

In conclusion, the main achievements of this thesis are in Theorem 5.15 and two of the corollaries to the Perlis Walker Theorem, namely Corollary 7.7 and Corollary 7.9. These results allow for a deeper understanding of the structure of group algebras and in turn their applications for coding theory.

References

[1] *S.S. Abhyankar and C. Christensen,* Semidirect Products: $x \mapsto ax+b$ as a First Example, *Mathematics Magazine, Vol. 75, No. 4 (2002) 284-289.*

[2] *J.N.S. Bidwell,* Computing Automorphisms of Finite Groups, *PhD Thesis, University of Otago, (2006).*

[3] *J.N.S. Bidwell and M.J. Curran,* Automorphisms of Finite Abelian Groups, *Mathematical Proceedings of the Royal Irish Academy 110A (2010), 55-71.*

[4] *R.E. Blahut,* Algebraic Codes for Data Transmission *Cambridge University Press,(2003).*

[5] *D. Bollman and H. Ramirez,* On the Enumeration of Matrices over Finite Commutative Rings, *The American Mathematical Monthly, Volume 76, No. 9 (1969), 1019-1023.*

[6] *O. Broche and A. del Rio,* Wedderburn decomposition of finite group algebras, *Finite fields and Their Applications (2007), 71-79.*

[7] *D.M. Burton,* Elementary Number Theory, *William C. Brown Publishers, 4th ed. Dubuque, 184-205, (1989).*

[8] *J.H. Conway,* Atlas of finite groups: maximal subgroups and ordinary characters for simple groups, *Oxford, Clarendon Press (1985).*

[9] *L. Creedon,* The Unit Group of Small Group Algebras and the Minimum Counterexample to the Isomorphism Problem, *International Journal of Pure and Applied Mathematics, Volume 49 No. 4 (2008), 531-537.*

[10] *L. Creedon,* A Course in Group Rings, *NUI Galway Lecture Notes (2004).*

[11] *M.J. Curran,* Automorphisms of Semidirect Products, *Mathematical Proceedings of the Royal Irish Academy 108A (2008), 205-210.*

[12] *J. Dieudonne,* On the Automorphisms of the Classical Groups, *Memoirs of the American Mathematical Society (1951).*

[13] *D.S. Dummit and R.M.Foote,* Abstract Algebra, *John Wiley and Sons, Inc, 3rd Edition (2004).*

[14] *The GAP Group,* GAP – Groups, Algorithms, and Programming, *Version 4.6.2; 2013. (http://www.gap-system.org).*

[15] *J.D. Hamkins,* Every Group has a Terminating Transfinite Automorphism Tower, *Proceedings of the American Mathematical Society, vol. 126, iss. 11, pp. 3223-3226, (1998)*

[16] *G. Higman,* The Units of Group Rings, *Proc. London Math. Soc.,46, No. 2 (1940), 231-248.*

[17] *C.J. Hillar and D.L. Rhea,* Automorphisms of Finite Abelian Groups, *The American Mathematical Monthly 11 (2007), 917-23.*

[18] *P. Hurley and T. Hurley,* Codes from Zero Divisors and Units in Group Rings, *International Journal of Information and Coding Theory, Vol. 1, No. 1, (2009), 57-87.*

[19] *G. James and M. Liebeck,* Representations and Characters of Groups, *Cambridge University Press (1993).*

[20] *B.R. McDonald,* Finite Rings with Identity, *Marcel Dekker, Inc (1974).*

[21] *I. McLoughlin,* Dihedral Codes, *PhD Thesis, National University of Ireland, (2009).*

[22] *G.A. Millar,* Automorphisms of the Dihedral Groups, *Proceedings of the National Academy of Sciences U.S.A. 28 (1942), 368-371.*

[23] *G.A. Millar,* Possible Groups Of Automorphisms, *Proceedings of the National Academy of Sciences U.S.A. 29 (1943), 49-52.*

[24] *V. Naik,* Transpose-Inverse Map *[online] Available from <http://groupprops.subwiki.org/w/index.php?title=Transpose-inverse_map&oldid=49130.> (2014). [Accessed 12/01/2014].*

[25] *NPTEL Institute of Technology Madras,* Mod-01 Lec-03 Dual of Linear Block Codes, *[online] Available from: <http://youtu.be/aHW1K-r7CGQ> (2012). [Accessed 20/11/2013].*

[26] *B. Peirce* Linear Associative Algebra, *American Journal of Mathematics, 4 (1881) pp. 97229.*

[27] *V. Pless and W.C.Huffman,* Handbook of Coding Theory Vol. 1, *Elsevier, (1998).*

[28] *C. Polcino Milies and S. K. Sehgal,* An Introduction to Group Rings, *Kluwer Academic Publishers (2002).*

[29] *D.J.S. Robinson,* A Course in The Theory of Groups, *Springer-Verlag, (1993).*

[30] *S. Thomas,* The Automorphism Tower Problem, *Proceedings of the American Mathematical Society, Vol. 95, No.2 (1985) 166-168.*

[31] *W.C. Waterhouse,* Automorphisms of $GL_n(R)$, *Proceedings of the American Mathematical Society, Vol. 79, No. 3, (1980).*

[32] *E. W. Weisstein,* Primitive Root, *From MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com/PrimitiveRoot.html (2014). [Accessed 16/07/2014].*

[33] *H. Wielandt,* Eine Verallgemeinerung der invarianten Untergruppen, *Math. Z. 45 p. 209244 (1939).*

Bibliography

P. Danchev, Units in Abelian Group Algebras Over Indecomposable Rings, *CUBO A Mathematical Journal Vol.14, 01, (2012) 49-54.*

R.A. Ferraz and C. Polcino Milies, Idempotents in Group Algebras and Minimal Abelian Codes, *Finite Fields and Their Applications 13, (2007), 382-393.*

I.N. Herstein, Topics in Algebra,*John Wiley and Sons, Inc, 2nd. Edition (1975).*

I. McLoughlin, A Group Ring Construction of the $[48, 24, 12]$ Type II Linear Block Code, *Designs, Codes and Cryptography, An International Journal, Volume 63, No. 1 (2012),29-41.*

W.K. Nicholson, Linear Algebra with Applications, *PWS Publishing Company, 3rd Edition, (1990).*

R. Schmidt, Subgroup Lattices of Groups, *de Gruyter, (1994).*