

Derivations of Group Algebras with Applications

Kieran Hughes

Supervisor: Dr. Leo Creedon

A thesis presented for the degree of
Doctor of Philosophy



Submitted to Quality and Qualifications Ireland, June 2020

Abstract

Derivations of Group Algebras with Applications

This thesis is a study of derivations of group algebras. Derivations are shown to be trivial for semisimple group algebras of abelian groups. The derivations of a group algebra are classified in terms of the generators and defining relations of the group. If RG is a group ring, where R is commutative and S is a set of generators of G then necessary and sufficient conditions on a map from S to RG are established, such that the map can be extended to an R -derivation of RG . This theorem is utilised to construct a basis for the vector space of derivations of abelian group algebras, dihedral group algebras and quaternion group algebras.

Derivations of group algebras are considered as linear finite dynamical systems and their associated directed graphs are studied. The motivation for this comes from the fact that if $Der(KG)$ and $Der(KH)$ are not isomorphic as additive groups then KG and KH are not isomorphic as rings. It is shown that if R and S are ring isomorphic, then there is a bijection from $Der(R)$ onto $Der(S)$ such that corresponding derivations have isomorphic associated digraphs. Therefore properties of the linear finite dynamical system associated with a derivation can be used to distinguish between group rings.

Derivations of a group algebra form a Lie algebra and it is shown that this Lie algebra $Der(KG)$ is a complete Lie algebra, when G is a finite abelian group such that its Sylow p -subgroup is elementary abelian.

Derivations can be used to show that two group algebras are not isomorphic as rings. As an example dihedral and quaternion group algebras are contrasted by showing that their respective derivation Lie algebras have different dimension and centers of different dimension. The thesis concludes by giving an alternative proof of Deskins' Theorem using derivations.

Dedication

To my wife Laura and our children Lana and Keelan.

Declaration

I declare that this thesis has been composed solely by myself and that it has not been submitted, in whole or in part, in any previous application for a degree. Except where stated otherwise by reference or acknowledgement, the work presented is entirely my own.

Signed: _____ (Candidate) Date: _____

Signed: _____ (Supervisor) Date: _____

Acknowledgements

I would firstly like to thank my supervisor Leo Creedon. I am very grateful for all the time and effort that you have given to guiding, encouraging and motivating me throughout this journey. Preparing this thesis would have been impossible without all your advice, comments, suggestions and ideas. Leo you are always willing to take the time to help in whatever way you can. I hope that we will write many research papers together in the future.

I would like to thank all the staff and postgrads whom I have gotten to know over the past four years at IT Sligo. I can honestly say that I have immensely enjoyed the process of preparing this thesis and this is due in large part to the friends I have met along the way.

Thanks to Fergal Gallagher and Martin Mathieu for useful insights into group rings and derivations. I would also like to thank all the staff at IT Sligo who have been so helpful and in particular to Ursula Cox, Veronica Cawley and John Bartlett in the research office.

I gratefully acknowledge the funding received towards my PhD from the IT Sligo President's Bursary Fund and the IT Sligo Capacity Building Fund.

To my wife Laura, I am forever indebted to you for your boundless and steadfast love and support. Your friendship and encouragement make anything seem possible. Thank you.

Contents

List of Figures	ix
List of Tables	xi
List of Notation	xii
1 Introduction	1
2 Derivations of Group Algebras and Codes	7
2.1 Introduction	7
2.2 Derivations of Group Rings	10
2.3 Applications	19
2.3.1 Derivations of Commutative Group Algebras	19
2.3.2 Derivations of Dihedral Group Algebras	22
2.3.3 Applications to Coding Theory	29
3 Derivations of Modular Group Algebras and Codes	32
3.1 Derivations, Ideals and Homomorphisms	33
3.2 An Example: \mathbb{F}_2D_8	39
3.2.1 Derivations	41

3.2.2	Conjugation by Units	43
3.2.3	The Ideals of \mathbb{F}_2D_8	48
3.2.4	The Unit Group of \mathbb{F}_2D_8	56
3.3	Do Outer Derivations Become Inner?	59
3.4	Some Linear Algebra Results	62
3.5	Error Correcting Codes from Derivations	70
4	Graphs Of Derivations	80
4.1	Digraphs and Finite Dynamical Systems	81
4.2	The Digraph of a derivation of $\mathbb{F}_2(C_2 \times C_2)$	87
4.3	Digraphs of the Derivations of \mathbb{F}_2C_4	90
4.4	Permutations of Derivations	104
4.5	Automorphisms of Small Group Algebras	105
4.6	Distinguishing Group Algebras using Digraphs	118
5	Derivation Towers	131
5.1	Introduction	132
5.2	The Lie Algebra of Derivations of a Group Algebra	136
5.3	The Derivations of Modular Elementary Abelian Group Algebras are Complete	143
5.4	The Lie Derivation Algebra of Abelian Group Algebras	158
5.5	Derivations of Abelian p-Groups	168
6	Derivations and the Modular Isomorphism Problem	175
6.1	Derivations of $\mathbb{F}_{2^t}D_{2^{m+1}}$ and $\mathbb{F}_{2^t}Q_{2^{m+1}}$	176

6.1.1	The Derivation Algebra of $\mathbb{F}_{2^t}Q_{2^{m+1}}$	177
6.1.2	The Centers of the Derivation Algebras of the Dihedral and Quaternion Group Algebras	184
6.1.3	Using Derivations to Distinguish $\mathbb{F}_{2^t}D_{2^{m+1}}$ and $\mathbb{F}_{2^t}Q_{2^{m+1}}$. . .	189
6.2	The Ring of Constants and the Modular Isomorphism Problem	190
6.2.1	The Ring of Constants of Dihedral Group Algebras	193
6.2.2	The Ring of Constants of Quaternion Group Algebras	195
6.2.3	A proof of Deskins' Theorem using derivations	198
7	Conclusions and Future Work	200
7.1	Conclusions	200
7.2	Future Work	204
	Appendix	206
	Computing the Derivation Lie Algebra of \mathbb{F}_2D_{256}	207
	Bibliography	209

List of Figures

1.1	Finite modular group algebras within the class of rings and vector spaces	2
2.1	Generator matrix of the binary [24, 12, 8] code defined by the derivation d	29
2.2	The right hand block of a generator matrix of the binary [48, 24, 12] code defined by the derivation δ	30
3.1	The lattice of two-sided ideals of \mathbb{F}_2D_8	55
3.2	The subgraph of the graph Γ induced by $R_\infty(d)$ in Example 3.5.12, where Γ is the graph with the elements of \mathbb{F}_3C_6 as vertices and (u, v) is a directed edge if $Du = v$	79
4.1	The vertex 0 has preperiod 3 and period 4	86
4.2	$\Gamma(d_N)$, the digraph of d_N	90
4.3	$\Gamma(d_R)$, the digraph of d_R	90
4.4	$\Gamma(d)$, the digraph of d	91
4.5	The digraph of the derivation in class 1 of Table 4.1	95
4.6	The digraph of the 4 derivations in class 2 of Table 4.1	97

4.7	The digraph of the 2 derivations in class 3 of Table 4.1	97
4.8	The digraph of the 4 derivations in class 4 of Table 4.1	97
4.9	The digraph of the 3 derivations in class 5 of Table 4.1	98
4.10	The digraph of the 2 derivations in class 6 of Table 4.1	98
4.11	The digraph of the derivation in class 1 of Table 4.3	109
4.12	The digraph of the derivations in class 2 of Table 4.3	109
4.13	The digraph of the derivations in class 3 of Table 4.3	109
4.14	The digraph of the derivations in class 4 of Table 4.3	109
4.15	The digraph of the derivations in class 5 of Table 4.3	110
4.16	The digraph of the derivations in class 6 of Table 4.3	110
4.17	The digraph of the derivations in class 7 of Table 4.3	110
4.18	The digraph of the derivations in class 8 of Table 4.3	110
4.19	The digraph of the derivations in class 9 of Table 4.3	111
4.20	The digraph of the derivations in class 10 of Table 4.3	111
5.1	A Venn diagram showing examples of derivation algebras of finite group algebras for all possible subsets of the set of properties {complete, simple, perfect}.	143
1	The .bat used to run GAP	207
2	An attempt to calculate the derivation algebra of $\mathbb{F}_2 D_{256}$ using GAP.	208

List of Tables

3.1	The image of D_8 under conjugation by the units of \mathbb{F}_2D_8 , where $\zeta = 1 + x^2 \in \mathbb{F}_2D_8$	47
4.1	The elements of $Der(\mathbb{F}_2C_4)$ partitioned by conjugacy class	95
4.2	Derivations of the same class exhibited as conjugates	96
4.3	The conjugacy classes of the derivations of $\mathbb{F}_2(C_2 \times C_2)$	108
5.1	A table showing the dimension of $Der_i(\mathfrak{g})$, where $\mathfrak{g} = Der(KG)$ for selected small KG	144

Notation

$[0]_n$	The $n \times n$ matrix with each entry zero
$[E]_n$	The $n \times n$ matrix with each entry one
\circ	composition of maps
\otimes	The classical involution on KG defined by $\sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g g^{-1}$
$\lfloor x \rfloor$	The floor function of x , i.e. the greatest integer less than or equal to x
\iff	if and only if
\leftrightarrow	A correspondence
\oplus	The direct sum of
\otimes_K	The tensor product over K
\rtimes	A semidirect product of groups
\simeq	is isomorphic to
\sqcup	The disjoint union of sets
\times	The direct product of groups
A_L	The Lie algebra constructed from an associative algebra A by defining the Lie product as $[x, y] = xy - yx$, for all $x, y \in A$
$[a, b]$	The Lie commutator of a and b , that is $[a, b] = ab - ba$
$ G $	The number of elements in the group G
ann	The annihilator of
$Aut(KG)$	The group of K -algebra isomorphisms of the group algebra KG

$C(f(x))$	The companion matrix of the polynomial $f(x)$
$c_T(x)$	The characteristic polynomial of a linear transformation T
\mathcal{C}_Δ	The set of elements c of a ring R such that $d(c) = 0$ for all d in a subset Δ of $Der(R)$
\mathcal{C}_d	\mathcal{C}_Δ , when $\Delta = \{d\}$
$char$	The characteristic of a ring is the smallest positive integer n such that $\underbrace{1 + 1 + \cdots + 1}_{n \text{ summands}} = 0$. Otherwise the characteristic is 0
$CM_n(K)$	The vector space of $n \times n$ circulant matrices over a field K
C_n	The cyclic group of order n
conjugation	The conjugation of a by u , is the element $u^{-1}au$ and is denoted by a^u
$\mathcal{C}(R)$	The ring of constants of a ring R , $\{c \in R \mid d(c) = 0 \text{ for all } d \in Der(R)\}$
$C(A, R)$	The centraliser of A in the ring R
D_{2n}	The dihedral group of order $2n$
$[d]_{\mathcal{B}}$	The matrix representing the derivation d with respect to the basis \mathcal{B}
d_b	The inner derivation induced by the element b , that is $[b, -]$
$\Delta(G)$	The augmentation ideal of RG
$\Delta_R(G, H)$	The left ideal of RG generated by the set $\{h - 1 \mid h \in H\}$
derivation	An additive group homomorphism that obeys the Leibniz (product) rule
$Der(R)$	The set of all derivations on a ring R
dim	The dimension of a vector space
d^n	The map that is the composition of d with itself n times

∂_x	The derivation of a group algebra KG defined by $x \mapsto 1$ and $S \setminus \{x\} \mapsto 0$, where $x \in S$ and S is a minimum generating set for an abelian group G
$E(g)$	The integer sum of the exponents of $g = x_0^{e_0} x_1^{e_1} \dots x_{n-1}^{e_{n-1}}$, $E(g) = \sum_{i=0}^{n-1} e_i$
$\mathcal{E}(\Gamma)$	The set of edges (arcs) of the (directed) graph Γ
ϵ	The augmentation map from a group ring RG into the ring R
FDS	Finite dynamical system
\mathbb{F}_{p^n}	The field with p^n elements, where p is a prime number and n is a natural number
F_S	The free group on the set S
$F[x]$	The polynomial ring in the indeterminate x over the field F
$\Gamma(d)$	The directed graph associated with the derivation d
$GL(n, p^m)$	the group of invertible elements of $M(n, p^m)$
G/H	The quotient group G modulo H
$In(v)$	The number of arcs in a digraph whose second coordinate is v
inner	A derivation d of R is inner if for all $a \in R$, $d(a) = ba - ab$, for some $b \in R$
<i>involution</i>	An anti-automorphism of order 2 of a ring
K^*	The multiplicative group of the field K
<i>ker</i>	The kernel of a map
\mathfrak{L}'	$[\mathfrak{L}, \mathfrak{L}]$, the ideal of \mathfrak{L} generated by all products $[a, b]$, where $a, b \in \mathfrak{L}$
$\Lambda(Der(KG))$	The length of the longest cycle contained in the digraphs $\Gamma(d)$ for any $d \in Der(KG)$
$\Lambda(\Gamma)$	The circumference (length of the longest cycle) of a digraph Γ

Leibniz's rule	A map d obeys Leibniz's rule if $d(ab) = d(a)b + ad(b)$, for all $a, b \in R$
LFDS	Linear finite dynamical system
$M(n, p^m)$	The ring of $n \times n$ matrices over \mathbb{F}_{p^m}
$m_{T,v}(x)$	The unique monic polynomial of least degree such that $m_{T,v}(T)(v) = 0$
mod	modulo
\mathbb{N}	The set of natural numbers $\{1, 2, 3, \dots\}$
N_∞	The generalised null space of a linear transformation, defined in Section 3.4
$[n, k, \delta]$	A code of length n , dimension k and minimum distance δ
$\mathcal{O}(x)$	The orbit of the element x of an FDS, which is $\{f^n(x) \mid n = 0, 1, \dots\}$
$ord(f)$	The least positive integer r such that $f(X)$ divides $X^r - 1$
$Out(v)$	The number of arcs in a digraph whose first coordinate is v
outer	A derivation d of R is outer if it is not inner
$per(Der(KG))$	The maximum of the periods of the derivations of KG
$per(v)$	The length of the terminating cycle of the vertex v in an FDS
$pper(Der(KG))$	The maximum of the preperiods of the derivations of KG
$pper(v)$	The length of the shortest path from v to any vertex in the terminating cycle of v
p -regular	A finite group whose exponent is not divisible by the prime p
\mathbb{Q}	The field of rational numbers
$Q_{2^{m+1}}$	The generalised Quaternion group of order 2^{m+1}
R -derivation	A derivation d of RG such that R is contained within the ring of constants of d
RG	A ring with the group G as a basis over the ring R

R_∞	The generalised range space of a linear transformation, defined in Section 3.4
$\langle S \mid T \rangle$	The group with S as a generating set and T the set of relators
$T \upharpoonright_W$	The restriction of the map T to W
\mathcal{T}	A transversal is a complete set of representatives of left cosets of H in G
$\mathcal{UC}(R)$	$\mathcal{U}(R) \cap \mathcal{C}(R)$, the group of constants of R
unit	An invertible element
unital ring	A ring with a multiplicative identity element denoted by 1
VC_Δ	The subgroup of V defined by $V \cap \bigcap_{d \in \Delta} C_d$
$\mathcal{V}(\Gamma)$	The set of vertices of the (directed) graph Γ
word on S	An element of F_S the free group on S
wt	$wt(c)$ is the Hamming weight of a codeword c and $wt(g)$ is the number of nonzero exponents of the group element g
x'	The image of the element x under some derivation
\hat{x}	The group ring element $x + x^2 + \dots + x^n$, where n is the order of x
\mathbb{Z}	The set of integers, $\{\dots, -2, -1, 0, 1, 2, \dots\}$
$Z(G)$	The center of the group G

Chapter 1

Introduction

This thesis is an analysis of the structure and applications of derivations of finite group algebras. We are primarily motivated by the desire to better understand the underlying structure of the group algebra but also by the application to error correcting codes. These applications include the error correcting codes necessary for applications where the signal is subject to heavy interference (a high noise channel) and where there is a requirement to have low energy inputs for the transmitting device. Such applications include transmitting data from offshore wind and wave energy devices and the software for wireless body area networks (WBANs) (also known as body sensor networks (BSNs)). The WBAN application may be useful in the software applications needed in designing portable biomedical diagnostics and veterinary applications.

The codes used in these applications need to be particularly efficient. This is due both to the high levels of noise on the channel and due to the small size of the devices comprising the WBAN. In particular, it is desirable that they have no short cycles. Codes (in particular Low Density Parity Check Codes (LDPC) and Convolution Codes) can be constructed algebraically using group algebras [30].

Functions, namely derivations, defined on a group algebra are examined. The

motivation is to answer structural questions relating to group algebras and in particular: Does there exist a ring isomorphism between group algebras of two nonisomorphic groups over the same field? This thesis will primarily be concerned with finite group algebras of positive characteristic. This focus is again motivated by the application to error correcting codes. Particular attention will be given to finite modular group algebras. We start by discussing both key players, namely group algebras and derivations.

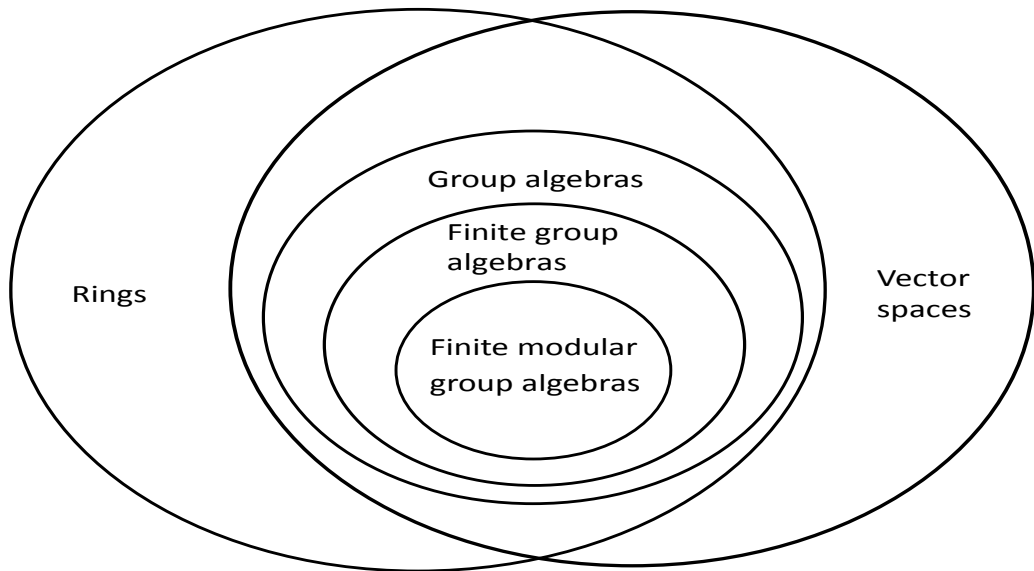


Figure 1.1: Finite modular group algebras within the class of rings and vector spaces

A group algebra can be considered as a ring, a vector space and a Lie algebra. Let G be a group and let K be a field. Then we shall denote the group algebra formed from K and G by KG . Considering group algebras as vector spaces has proven useful in the study of linear block codes. As an example, in [28], linear block codes have been generated from elements of group algebras of certain types (zero divisors and units).

Derivations are additive group homomorphisms. However they are not ring homomorphisms since they are in general not multiplicative. They do however,

obey a different multiplication rule known as Leibniz’s rule. As such, derivations are generalisations of the differentiation of real functions discovered by Leibniz and Newton.

In their 2014 paper “Linear codes using skew polynomials with automorphisms and derivations” [9] D. Boucher and F. Ulmer generalise codes as modules over skew polynomial rings of automorphism type to those skew polynomial rings whose multiplication is defined using an automorphism and a derivation. Codes constructed in this way have in some cases produced better distance bounds than that of other codes of the same length and dimension. This means that they can detect and or correct more errors in a transmission. They also introduce the notion of evaluation codes using these rings. M. Boulagouaz and A. Leroy in “ (σ, δ) -codes” [10] introduce the notion of cyclic $(f(t), \sigma, \delta)$ -codes, where $f(t)$ is an element of a skew polynomial ring. The use of derivations in coding theory has thus far been restricted to the setting of skew polynomial rings. A goal of this thesis is to better understand derivations of group rings. As a consequence this opens up the possibility to apply derivations to coding theory from a group rings perspective.

We begin our study of derivations of group algebras with some naive questions. Are there any derivations defined on group algebras? Assuming the set of derivations of a particular group algebra is non-empty: Are all the derivations of the group algebra inner derivations or do there exist outer derivations? What structure and size does the set of derivations have? These questions ultimately lead us to the central question of this thesis.

What, if anything can the set of derivations of a group algebra
(1.1)
tell us about the structure of the group algebra itself?

Chapter 2 introduces the notion of a group algebra and also defines a derivation of a ring. The set of derivations of a ring R , is denoted by $Der(R)$. Theorem 2.2.5

classifies the derivations of group algebras in terms of the generators and defining relations of the group. If RG is a group ring, where R is commutative and S is a set of generators of G then necessary and sufficient conditions on a map from S to RG are established, such that the map can be extended to an R -derivation of RG . If the group is abelian then our focus is directed towards studying modular group algebras. This is a consequence of the fact that the only derivation defined on a semisimple group algebra of an abelian group is the zero map. The derivations of finite group algebras are constructed and listed in the commutative case and in the case of dihedral groups. In the dihedral case, the inner derivations are also classified. Lastly, these results are applied to construct well known binary codes as images of derivations of group algebras. The results in this chapter were published in [12].

Derivations of a modular group algebra KG are the subject of Chapter 3. A subring of KG that will prove useful in this and subsequent chapters, namely the ring of constants, $\mathcal{C}(KG)$ is introduced. The connection between derivations and homomorphisms is studied and the concept of a differential ideal is introduced. The augmentation ideal $\Delta(G, H)$ is shown to be a differential ideal with respect to a derivation if and only if the image of the subgroup H under the derivation is contained in the augmentation ideal. As a consequence, $H \in \mathcal{C}(KG)$ implies that the augmentation ideal $\Delta(G, H)$ is a differential ideal. It is shown in Theorem 3.1.18 that a ring isomorphism from R to S induces an isomorphism of additive groups between $Der(R)$ and $Der(S)$. It is also shown in Section 3.1 that if two group algebras over K are isomorphic as K -algebras, then their respective derivation algebras are isomorphic as Lie algebras. These results provide a tool for gleaning information about the structure of a group algebra from that of its derivation algebra. As an example, if there are more derivations of KG than of KH , then KG and KH are not isomorphic as rings by Theorem 3.1.18. \mathbb{F}_2D_8 is studied as

an example of a modular group algebra. Its derivations, ideals and unit group are found as well as the image of an element of the group algebra under conjugation by units. It is shown that no outer derivation of KH becomes inner in KG , where H is a subgroup of G . This chapter concludes with a brief look at generating error correcting codes from derivations of modular group algebras.

A derivation of a commutative group algebra KG is considered as a linear finite dynamical system (LFDS) in Chapter 4. The resulting LFDS corresponds to a directed graph with the elements of KG as vertices and an arc between each vertex and its image under the derivation. As previously stated, the results of Chapter 3 provide a tool for gleaning information about the structure of a group algebra from that of its derivation algebra. Counting derivations can be used to show that group algebras are not isomorphic as rings. However, this may not always work since for example $\mathbb{F}_2(C_4 \times C_4)$ and $\mathbb{F}_2(C_2 \times C_8)$ both have 2^{32} derivations. Therefore we will seek to use other properties of the LFDSs associated with the derivations of group algebras to distinguish between the nonisomorphic group algebras. The maximum value of the preperiod of a LFDS is one such property and is used to show that $\mathbb{F}_2(C_4 \times C_4)$ and $\mathbb{F}_2(C_2 \times C_8)$ are not ring isomorphic. When the derivation is nilpotent, the maximum value of the preperiod corresponds to the nilpotency index of the derivation.

The set of derivations of a commutative group algebra over a finite field is again the subject of Chapter 5. However, this chapter studies the Lie algebra formed from this set of derivations by defining multiplication as the Lie commutator. This Lie algebra is known as the derivation algebra. The motivation comes from Theorem 3.1.20, which states that a K -algebra isomorphism between two finite group algebras implies that their derivation algebras are isomorphic as Lie algebras. It is shown that the derivation algebra of a commutative group algebra over a finite field has trivial center. A Lie algebra that has trivial center and whose

derivations are all inner is called complete. It is proven in Theorem 5.4.14 that if K is a finite field of characteristic p and G is a finite abelian group such that its Sylow p -subgroup is elementary abelian, then the derivation algebra of KG is complete.

A very interesting problem in group rings is whether the group ring determines the group. This question is referred to as the Isomorphism Problem of Group Rings [40]. The set of derivations of a group algebra can be trivial. For example the zero map is the only derivation of the semisimple group algebra \mathbb{F}_2C_n , where n is an odd integer. In contrast, by Theorem 2.3.4 of Chapter 2 the group algebra \mathbb{F}_pP where P is a finite abelian p -group always has non trivial derivations. This simple observation motivates the application of the results of Chapters 2 - 5 to the study of the Isomorphism Problem within the following context: Let P and Q be finite p -groups and K the field with p elements. The Modular Isomorphism Problem asks if the following statement is true:

$$KP \simeq KQ \implies P \simeq Q.$$

The Modular Isomorphism Problem was solved for abelian groups in 1956 by Deskins [14]. Chapter 6 begins by studying the derivation algebras of $\mathbb{F}_{2^t}D_{2^{m+1}}$ and $\mathbb{F}_{2^t}Q_{2^{m+1}}$. These results are then used to prove that $\mathbb{F}_{2^t}D_{2^{m+1}}$ and $\mathbb{F}_{2^t}Q_{2^{m+1}}$ are not isomorphic as K -algebras or in fact as rings. Therefore these group algebras do not provide a counterexample to the Modular Isomorphism Problem. The information discovered about derivations of group algebras provided the tools necessary to give an alternative proof of Deskins Theorem in Theorem 6.2.16.

Chapter 2

Derivations of Group Algebras and Codes

2.1 Introduction

Group rings and derivations of rings have both been studied for more than 60 years. For a history of group rings see Polcino Milies and Sehgal [40] and for a survey article on derivations see Ashraf, Ali, and Haetinger [3]. The results of Posner [41] and Herstein [24] attracted particular attention. Prime, semiprime and 2-torsion free rings were a focus of the resulting research.

Derivations of C^* -algebras have been studied by several authors. In [44], Sakai proved that every derivation of a simple C^* -algebra becomes inner in its multiplier algebra. Mathieu and Villena, in [36] study the structure of Lie derivations of C^* -algebras. In the 2000 paper Derivations on Group Algebras [19], Ghahramani, Runde and Willis, examine the first cohomology space of the group algebra $L^1(G)$, where G is a locally compact group. The derivation problem asks whether every derivation from $L^1(G)$ to $M(G)$ is inner, where G is a locally compact group and $M(G)$ is the multiplier algebra of $L^1(G)$. It was solved in the affirmative by

Losert [34]. The 2017 preprint “Derivations of Group Algebras”, [2] by Arutyunov, Mishchenko and Shtern describes the outer derivations of $L^1(G)$.

Group rings have been used to construct new codes as well as to study existing codes. In [28] Hurley and Hurley present techniques for constructing codes from group rings. The codes constructed consist primarily of two types, zero-divisor codes and unit-derived codes. The structure of group ring codes is examined in [27]. The author gives a decomposition of a group ring code into twisted group ring codes and proves the nonexistence of self-dual group ring codes in particular cases.

Derivations have also been employed in coding theory. In [9] codes are constructed as modules over skew polynomial rings, where the multiplication is defined by a derivation and an automorphism. In this chapter derivations of group algebras and their application to coding theory are considered.

However, there has not been as much research into derivations of group algebras with positive characteristic. Notable exceptions include Smith [49], Spiegel [50], Ferrero, Giambruno and Polcino Milies [17] and Artemovych, Bovdi and Salim [1]. In [17] the authors prove the following theorem.

Theorem 2.1.1. *[17] Let R be a semiprime ring and G a torsion group such that $[G : Z(G)] < \infty$, where $Z(G)$ denotes the center of G . Suppose that either $\text{char } R = 0$ or for every characteristic p of R , $p \nmid o(g)$, for all $g \in G$. Then every R -derivation of RG is inner.*

In this thesis we are particularly interested in finite group algebras. This is motivated in part by applications to error correcting codes. Theorems 2.1.1 and 2.3.1 direct our focus, in the commutative case, to the study of derivations of modular (nonsemisimple) group algebras with positive characteristic.

Theorem 2.2.2 shows that when K is an algebraic extension of a prime field

all derivations of a K -algebra are K -derivations. If RG is a group ring, where R is commutative and S is a set of generators of G then necessary and sufficient conditions on a map $f: S \rightarrow RG$ are established, in Theorem 2.2.5, such that f can be extended to an R -derivation of RG . Section 2.3 outlines some applications of the results of Section 2.2. All derivations of finite commutative group algebras of positive characteristic are determined in Theorem 2.3.4. If G is a finite abelian group and K a finite field of positive characteristic p then the image of a minimum set of generators of the Sylow p -subgroup of G under a derivation of KG can be chosen arbitrarily, however this is not always the case in the noncommutative setting. An inner derivation of a ring R maps $a \in R$ to $ba - ab$, for some element $b \in R$. In the case of finite dihedral group algebras of characteristic 2, a basis is given for the space of derivations in Theorem 2.3.11 and also for those that are inner in Theorem 2.3.13.

The extended binary Golay [24, 12, 8] code and the extended binary quadratic residue [48, 24, 12] code are both presented as images of derivations of group algebras in Section 2.3.3.

Definition 2.1.2. Notation: \mathbb{N} , \mathbb{Z} and \mathbb{Q} denote the natural numbers, the integers and the rational numbers, and \mathbb{F}_{p^n} denotes the finite field with p^n elements. The group ring RG denotes the set of all formal linear combinations of the form $\sum_{g \in G} a_g g$, of finite support where $a_g \in R$, together with the operations of addition (componentwise) and multiplication defined as $(\sum_{g \in G} a_g g)(\sum_{h \in G} b_h h) = \sum_{g, h \in G} a_g b_h gh$. We adopt the usual convention that empty sums are 0 and empty products are 1.

Definition 2.1.3. A *derivation* of a ring R is a mapping $d: R \rightarrow R$ satisfying

$$d(a + b) = d(a) + d(b), \quad \text{for all } a, b \in R. \quad (2.1)$$

$$d(ab) = d(a)b + ad(b), \quad \text{for all } a, b \in R. \quad (2.2)$$

Equation (2.2) is known as Leibniz's rule. Write $Der(R)$ for the set of derivations of a ring R . Note that if R is a unital ring then $d(1) = 0$, since $d(1) = d(1(1)) = d(1)1 + 1d(1)$.

Definition 2.1.4. Let $d \in Der(R)$ and $r \in R$ for a ring R . Then the map $r \cdot d: R \rightarrow R$ is defined as $a \mapsto rd(a)$ for all $a \in R$.

Lemma 2.1.5. Let Z be a central subring of a ring R . Then $Der(R)$ together with the action \cdot is a Z -module.

Definition 2.1.6. Let RG be a group ring. Then a derivation $d: RG \rightarrow RG$ is an R -derivation if $d(R) = \{0\}$.

Definition 2.1.7. Given a ring R and $a, b \in R$, define the *Lie commutator* $[a, b] = ab - ba$. A derivation d on a ring R is *inner* if for all $a \in R$ we have $d(a) = ba - ab$ for some $b \in R$. In this case we write $d = d_b$.

2.2 Derivations of Group Rings

In this section we establish necessary and sufficient conditions on a map $f: S \rightarrow RG$, such that f can be extended to an R -derivation of the group ring RG , where S is a set of generators of G and R is commutative. First, some identities and preliminary results are presented.

Lemma 2.2.1. *Let d be a derivation of a ring R . Then*

$$(i) \quad d\left(\prod_{i=1}^m a_i\right) = \sum_{i=1}^m \left(\left(\prod_{j=1}^{i-1} a_j \right) d(a_i) \left(\prod_{j=i+1}^m a_j \right) \right), \text{ for all } a_i \text{ in } R. \quad (2.3)$$

$$(ii) \quad d(a^m) = \sum_{i=0}^{m-1} a^i d(a) a^{(m-1-i)}, \text{ for all } a \in R \text{ and } m \in \mathbb{N}. \quad (2.4)$$

$$(iii) \quad \sum_{i=0}^{n-1} a^i d(a) a^{(n-1-i)} = 0, \text{ for all units } a \text{ in } R \text{ of order } n. \quad (2.5)$$

$$(iv) \quad d(a^k) = ka^{k-1}d(a), \text{ for all } a \in R \text{ which commute with } d(a) \text{ and } k \in \mathbb{N}. \quad (2.6)$$

$$(v) \quad d(a^k) = ka^{k-1}d(a), \text{ for all units } a \in R \text{ which commute with } d(a) \text{ and } k \in \mathbb{Z}. \quad (2.7)$$

Proof. (i) We will prove Equation 2.3 by induction on m .

Base case: $m = 1$. This is true as $d(a_1) = \sum_{i=1}^1 1d(a_1)1$.

Assume that $d(\prod_{i=1}^m a_i) = \sum_{i=1}^m \left(\left(\prod_{j=1}^{i-1} a_j \right) d(a_i) \left(\prod_{j=i+1}^m a_j \right) \right)$. Then

$$\begin{aligned} d\left(\prod_{i=1}^{m+1} a_i\right) &= d\left(\prod_{i=1}^m a_i\right)a_{m+1} + \left(\prod_{i=1}^m a_i\right)d(a_{m+1}) \\ &= \sum_{i=1}^m \left(\left(\prod_{j=1}^{i-1} a_j \right) d(a_i) \left(\prod_{j=i+1}^m a_j \right) \right) a_{m+1} + \left(\prod_{i=1}^m a_i \right) d(a_{m+1}) \\ &= \sum_{i=1}^{m+1} \left(\left(\prod_{j=1}^{i-1} a_j \right) d(a_i) \left(\prod_{j=i+1}^{m+1} a_j \right) \right). \end{aligned}$$

Therefore Equation 2.3 holds for all $m \in \mathbb{N}$.

(ii) Let $a_i = a$ in Equation 2.3. Then for all $m \in \mathbb{N}$

$$d(a^m) = \sum_{i=1}^m \left(\left(\prod_{j=1}^{i-1} a \right) d(a) \left(\prod_{j=i+1}^m a \right) \right) = \sum_{i=1}^m a^{i-1} d(a) a^{(m-i)} = \sum_{i=0}^{m-1} a^i d(a) a^{(m-1-i)}.$$

(iii) Setting $m = n$ in Equation 2.4 implies

$$0 = d(1) = d(a^n) = \sum_{i=0}^{n-1} a^i d(a) a^{(n-1-i)}.$$

(iv) Let a be an element of R that commutes with $d(a)$. Then using Equation 2.4

$$d(a^k) = \sum_{i=0}^{k-1} a^i d(a) a^{(k-1-i)} = \sum_{i=0}^{k-1} a^{k-1} d(a) = k a^{k-1} d(a).$$

(v) Let a be a unit which commutes with $d(a)$. Then a^{-1} is also a unit which commutes with $d(a)$ since $a^{-1}d(a) = a^{-1}d(a)aa^{-1} = a^{-1}ad(a)a^{-1} = d(a)a^{-1}$. Therefore $0 = d(1) = d(a^{-1}a) = d(a^{-1})a + a^{-1}d(a)$ and so $d(a^{-1}) = -a^{-1}d(a)a^{-1} = -a^{-2}d(a)$. Moreover, a^{-1} commutes with $d(a^{-1})$ since $a^{-1}d(a^{-1}) = a^{-1}(-a^{-2}d(a)) = -a^{-2}d(a)a^{-1} = d(a^{-1})a^{-1}$. Therefore for any positive integer k

$$d(a^{-k}) = d((a^{-1})^k) = k(a^{-1})^{k-1}d(a^{-1}) = k(a^{-k+1})(-a^{-2}d(a)) = -k(a^{-k-1})d(a).$$

Furthermore, $0 = d(1) = d(a^0) = 0a^{-1}d(a)$ and so Equation (2.7) holds for all integers k . □

The following Theorem shows that when K is an algebraic extension of a prime field all derivations of a K -algebra are K -derivations.

Theorem 2.2.2. *Let A be a K -algebra where K is an algebraic extension of a prime field F and let $d \in \text{Der}(A)$. Then $d(K) = \{0\}$ and d is a K -linear map.*

Proof. Let $d \in \text{Der}(A)$. If $\text{char}(F) > 0$ then for $b \in F$, $d(b) = d(1 + 1 + \cdots + 1) = d(1) + d(1) + \cdots + d(1) = bd(1) = b0 = 0$, and so $d(F) = 0$. Let $F = \mathbb{Q}$ and let $a, b \in \mathbb{Z}$ with $b > 0$. Note that $0 = d(0) = d(1 - 1) = d(1) + d(-1) = 0 + d(-1)$, so $d(-1) = 0$. Then $bd(a/b) = d(a/b) + \cdots + d(a/b) = d(a/b + \cdots + a/b) = d(a) =$

$\pm d(1 + \cdots + 1) = \pm(d(1) + \cdots + d(1)) = 0$. Therefore $d(a/b) = 0$, so $d(F) = 0$ for all prime fields F .

Let a be a nonzero element of K and let $m_a(x) = \sum_{j=0}^{n_a} b_{aj}x^j \in F[x]$ be the minimal polynomial of a over F . a is a central unit in K and so Equation 2.7 of Lemma 2.2.1 applies. Note that for $b \in F$ and $\alpha \in K$ we have $d(b\alpha) = bd(\alpha)$, since $d(F) = 0$. Thus applying a derivation d to $m_a(a) = 0$ and using Equation 2.7

$$\begin{aligned} 0 &= d(0) = d(m_a(a)) = d\left(\sum_{j=0}^{n_a} b_{aj}a^j\right) = \sum_{j=0}^{n_a} b_{aj}d(a^j) \\ &= \sum_{j=0}^{n_a} b_{aj}ja^{j-1}d(a) = \left(\sum_{j=1}^{n_a} b_{aj}ja^{j-1}\right)d(a) = q(a)d(a), \end{aligned}$$

where q is a polynomial in $F[x]$. Moreover, $q(a) \neq 0$ as this would contradict the minimality of the degree of $m_a(x)$. Therefore $d(a) = 0$, since $q(a)$ is invertible as it is a non zero element of the field K . Hence $d(K) = \{0\}$.

The K -linearity of d is immediate since d is additive and if $a \in A$ and $k \in K$ then $d(ka) = d(k)a + kd(a) = 0 + kd(a)$. \square

Corollary 2.2.3. *Let K be an algebraic extension of a prime field F . Let G be a torsion group such that $[G : Z(G)] < \infty$, where $Z(G)$ denotes the center of G . Suppose that either $\text{char}(K) = 0$ or that $\text{char}(K) = p > 0$, and p does not divide the order of g , for all $g \in G$. Then every derivation of KG is inner.*

Proof. By Theorem 2.2.2, every derivation of KG is a K -derivation and since every field is semiprime, Theorem 2.1.1 implies that every derivation of KG is inner. \square

Note that in Corollary 2.2.3 if “derivation” is replaced by “ K -derivation” then this is a special case of Theorem 2.1.1. Also the requirement that K is algebraic over F is necessary in Theorem 2.2.2 as the following example shows.

Example 2.2.4. Let $\mathbb{Q}(t)$ be a transcendental extension of the rationals (the field

of rational functions of t). Since $\mathbb{Q}(t)$ is a \mathbb{Q} -algebra, Theorem 2.2.2 implies that $d(\mathbb{Q}) = \{0\}$ for all derivations d of $\mathbb{Q}(t)$. However, by Proposition 5.2 of Chapter VIII in [33], there exists a nonzero derivation d of $\mathbb{Q}(t)$, since $\mathbb{Q}(t)$ is a finitely generated extension over \mathbb{Q} that is not separable algebraic.

Theorem 2.2.5. *Let $G = \langle S \mid T \rangle$ be a group, where S is a generating set and T a set of relators. Let F_S be the free group on S and $\phi: F_S \rightarrow G$ the homomorphism of F_S onto G . Let R be a commutative unital ring and f a map from S to RG . Then*

(i) *f can be uniquely extended to a map f^* from F_S to RG such that*

$$f^*(uv) = f^*(u)\phi(v) + \phi(u)f^*(v), \quad \text{for all } u, v \in F_S, \quad (2.8)$$

(ii) *the map f from S to RG can be extended to an R -derivation of RG if and only if $f^*(t) = 0$, for all $t \in T$,*

(iii) *if f can be extended to an R -derivation of RG , then this extension is unique.*

Proof. Let f be a map from S to RG . ϕ is the identity map on S , so for $s \in S$, $\phi(s^{-1}s) = \phi(s^{-1})\phi(s) = \phi(s^{-1})s = \phi(1) = 1$, so $\phi(s^{-1}) = s^{-1}$. Thus ϕ is the identity map on $S \cup S^{-1}$.

(i) We wish to extend f to $f^*: F_S \rightarrow RG$, which satisfies Equation 2.8.

Define $f^*: F_S \rightarrow RG$ as follows:

$$f^*(w_i) = \begin{cases} f(w_i) & \text{if } w_i \in S, \\ -w_i f(w_i^{-1}) w_i & \text{if } w_i \in S^{-1}, \\ 0 & \text{if } w_i = 1 \end{cases} \quad (2.9)$$

and letting $w = \prod_{i=1}^k w_i$, where $w_i \in S \cup S^{-1}$, define

$$f^*(w) = \sum_{i=1}^k \left(\left(\prod_{j=1}^{i-1} w_j \right) f^*(w_i) \left(\prod_{j=i+1}^k w_j \right) \right). \quad (2.10)$$

Let $0 \leq l \leq k$ and $u = \prod_{i=1}^l w_i$ and $v = \prod_{i=l+1}^k w_i$. Then by Equations 2.9 and 2.10

$$\begin{aligned} f^*(uv) &= \sum_{i=1}^k \left(\left(\prod_{j=1}^{i-1} w_j \right) f^*(w_i) \left(\prod_{j=i+1}^k w_j \right) \right) \\ &= \left(\sum_{i=1}^l \left(\prod_{j=1}^{i-1} w_j \right) f^*(w_i) \left(\prod_{j=i+1}^l w_j \right) \right) \prod_{j=l+1}^k w_j \\ &\quad + \prod_{j=1}^l w_j \sum_{i=l+1}^k \left(\prod_{j=l+1}^{i-1} w_j \right) f^*(w_i) \left(\prod_{j=i+1}^k w_j \right) \\ &= f^*(u) \prod_{j=l+1}^k \phi(w_j) + \prod_{j=1}^l \phi(w_j) f^*(v) \\ &= f^*(u) \phi(v) + \phi(u) f^*(v). \end{aligned}$$

Therefore f^* defined by Equations 2.9 and 2.10 satisfies Equation 2.8.

If w is a word on S , denote the reduced word by \bar{w} . In order for f^* to be well defined on F_S we need to show that $f^*(w) = f^*(\bar{w})$ for all words w on S . Let u, v be words on S and let $a \in S$.

Then by Equation 2.9, $f^*(a)a^{-1} + af^*(a^{-1}) = f(a)a^{-1} - aa^{-1}f(a)a^{-1} = 0$. Similarly, $f^*(a)a^{-1} + af^*(a^{-1}) = 0$ for all $a \in S^{-1}$. Let $a \in S \cup S^{-1}$. Then by Equation 2.10, $f^*(aa^{-1}) = 0$ and so by Equation 2.8

$$\begin{aligned} f^*(uaa^{-1}v) &= f^*(u)\phi(aa^{-1}v) + \phi(u)f^*(aa^{-1}v) \\ &= f^*(u)\phi(v) + \phi(u)f^*(aa^{-1})\phi(v) + \phi(uaa^{-1})f^*(v) = f^*(u)\phi(v) + \phi(u)f^*(v) = f^*(uv). \end{aligned}$$

Therefore $f^*(w) = f^*(\bar{w})$ for all words w on S . We now prove the uniqueness of

f^* .

Assume that there exists a map $f_* : F_S \rightarrow RG$, distinct from f^* which is also an extension of f and which also satisfies Equation 2.8. Let 1 be the identity element of F_S . Then $f_*(1) = f_*(1(1)) = f_*(1)1 + 1f_*(1)$, which implies that $f_*(1) = 0 = f^*(1)$. Let $s \in S$. Then $f_*(s) = f(s) = f^*(s)$ and $0 = f_*(s^{-1}s) = f_*(s^{-1})s + s^{-1}f_*(s)$. This implies that $f_*(s^{-1}) = -s^{-1}f_*(s)s^{-1} = f^*(s^{-1})$. Therefore there exists an element x of F_S , of positive length $c > 1$, such that $f^*(x) \neq f_*(x)$ and $f^*(z) = f_*(z)$ for all words z in F_S of length less than c . Write $x = \prod_{i=1}^c x_i$, where $x_i \in S \cup S^{-1}$. Thus $f^*(\prod_{i=1}^{c-1} x_i) = f_*(\prod_{i=1}^{c-1} x_i)$ and $f^*(x_c) = f_*(x_c)$, since $\prod_{i=1}^{c-1} x_i$ and x_c are both elements of F_S whose length is less than c . Therefore by Equation 2.8

$$f_*(x) = f_*\left(\prod_{i=1}^{c-1} x_i\right)\phi(x_c) + \phi\left(\prod_{i=1}^{c-1} x_i\right)f_*(x_c) = f^*\left(\prod_{i=1}^{c-1} x_i\right)\phi(x_c) + \phi\left(\prod_{i=1}^{c-1} x_i\right)f^*(x_c) = f^*(x).$$

This contradiction implies that f^* is the unique extension of f to F_S , such that $f^*(uv) = f^*(u)\phi(v) + \phi(u)f^*(v)$, for all $u, v \in F_S$. This proves (i).

(ii) Considering S as a subset of G , suppose that the map $f : S \rightarrow RG$ can be extended to an R -derivation d of RG . Then for any $s \in S$, $d(s) = f(s)$ and $0 = d(s^{-1}s) = d(s^{-1})s + s^{-1}d(s)$ and so $d(s^{-1}) = -s^{-1}d(s)s^{-1} = -s^{-1}f(s)s^{-1}$. Therefore $d(a) = f^*(a)$, for all $a \in S \cup S^{-1}$ by Equation 2.9. Let $t = \prod_{i=1}^m t_i \in T$, where $t_i \in S \cup S^{-1}$ for $i = 1, 2, \dots, m$. Then by Equations 2.10 and 2.3

$$f^*(t) = \sum_{i=1}^m \left(\left(\prod_{j=1}^{i-1} t_j \right) f^*(t_i) \left(\prod_{j=i+1}^m t_j \right) \right) = \sum_{i=1}^m \left(\left(\prod_{j=1}^{i-1} t_j \right) d(t_i) \left(\prod_{j=i+1}^m t_j \right) \right) = d(t) = 0.$$

This proves the implication in (ii).

Conversely, assume $f^*(t) = 0$, for all $t \in T$. Let $t \in T$. Then $\phi(t) = 1$ and $f^*(t^{-1}) = 0$, since $0 = f^*(tt^{-1}) = f^*(t)\phi(t^{-1}) + \phi(t)f^*(t^{-1}) = 0(1) + (1)f^*(t^{-1}) =$

$f^*(t^{-1})$. Let $\epsilon \in \{1, -1\}$. Then for all $w \in F_S$

$$\begin{aligned}
f^*(w^{-1}t^\epsilon w) &= f^*(w^{-1})\phi(t^\epsilon w) + \phi(w^{-1})f^*(t^\epsilon w) \\
&= f^*(w^{-1})\phi(t^\epsilon w) + \phi(w^{-1})f^*(t^\epsilon)\phi(w) + \phi(w^{-1}t^\epsilon)f^*(w) \quad (2.11) \\
&= f^*(w^{-1})\phi(w) + \phi(w^{-1})f^*(w) = f^*(w^{-1}w) = 0.
\end{aligned}$$

Let $N = \langle T^{F_S} \rangle$ be the normal closure of T . Any non-identity element n of N can be written as $\prod_{i=1}^k w_i^{-1}t_i^{\epsilon_i}w_i$, where $w_i \in F_S$, $t_i \in T$ and $\epsilon_i \in \{-1, 1\}$. Therefore by Equations 2.10 and 2.11

$$\begin{aligned}
f^*(n) &= f^*\left(\prod_{i=1}^k w_i^{-1}t_i^{\epsilon_i}w_i\right) \\
&= \sum_{i=1}^k \phi\left(\prod_{j=1}^{i-1} w_j^{-1}t_j^{\epsilon_j}w_j\right)f^*(w_i^{-1}t_i^{\epsilon_i}w_i)\phi\left(\prod_{j=i+1}^k w_j^{-1}t_j^{\epsilon_j}w_j\right) = 0.
\end{aligned}$$

Also $\phi(n) = 1$, for all $n \in N$ and so for any $w \in F_S$, $f^*(wn) = f^*(w)\phi(n) + \phi(w)f^*(n) = f^*(w)$. Let $g, h \in G = \langle S \mid T \rangle \simeq \frac{F_S}{\langle T^{F_S} \rangle}$ and let u, v be elements of F_S , such that $g = \phi(u)$ and $h = \phi(v)$. Extend $f: S \rightarrow RG$ to $\hat{f}: G \rightarrow RG$ by defining $\hat{f}(g) = f^*(u)$. Then $\hat{f}(gh) = f^*(uv) = f^*(u)\phi(v) + \phi(u)f^*(v) = \hat{f}(g)h + g\hat{f}(h)$. Suppose \tilde{f} is also an extension of f distinct from \hat{f} that satisfies $\tilde{f}(gh) = \tilde{f}(g)h + g\tilde{f}(h)$ for all $g, h \in G$. Let $l: G \rightarrow \mathbb{N}$ be the minimum length of an element of G , defined by $l(g) = \min\{k \mid g = \prod_{i=1}^k g_i, g_i \in S \cup S^{-1}\}$. Then there exists an $x \in G$ of minimum length such that $\tilde{f}(x) \neq \hat{f}(x)$. For all $s \in S$, $0 = \tilde{f}(ss^{-1}) = \tilde{f}(s)s^{-1} + s\tilde{f}(s^{-1})$ and $\tilde{f}(s) = \hat{f}(s)$. Thus $\tilde{f}(s^{-1}) = -s^{-1}\hat{f}(s)s^{-1} = -s^{-1}f(s)s^{-1} = f^*(s^{-1}) = \hat{f}(s^{-1})$. Therefore $\tilde{f}(g) = \hat{f}(g)$ for all $g \in G$ such that $l(g) < 2$ and so x can be written as $x = yz$, where $y, z \in G$ such that $l(y) < l(x)$ and $l(z) < l(x)$. Then $\tilde{f}(x) = \tilde{f}(yz) = \tilde{f}(y)z + y\tilde{f}(z) = \hat{f}(y)z + y\hat{f}(z) = \hat{f}(x)$. This contradiction implies that \hat{f} is the unique extension of f such that $\hat{f}(gh) = \hat{f}(g)h + g\hat{f}(h)$ for any $g, h \in G$. Extend \hat{f} , R -linearly to RG and denote this unique

extension also by \hat{f} . Let $\alpha = \sum_{g \in G} a_g g$ and $\beta = \sum_{h \in G} b_h h$ be elements of RG , where $a_g, b_h \in R$. Then $\hat{f}(\alpha + \beta) = \hat{f}(\alpha) + \hat{f}(\beta)$ as \hat{f} is an R -linear map. Moreover

$$\begin{aligned} \hat{f}(\alpha)\beta + \alpha\hat{f}(\beta) &= \left(\sum_{g \in G} a_g \hat{f}(g) \right) \left(\sum_{h \in G} b_h h \right) + \left(\sum_{g \in G} a_g g \right) \left(\sum_{h \in G} b_h \hat{f}(h) \right) \\ &= \sum_{g,h} a_g b_h \hat{f}(g)h + \sum_{g,h} a_g b_h g \hat{f}(h) = \sum_{g,h} a_g b_h (\hat{f}(g)h + g\hat{f}(h)) \\ &= \sum_{g,h} a_g b_h \hat{f}(gh) = \hat{f} \left(\sum_{g,h} a_g b_h gh \right) = \hat{f} \left(\sum_g a_g g \sum_h b_h h \right) = \hat{f}(\alpha\beta). \end{aligned}$$

Therefore the map \hat{f} obeys Leibniz's rule for all products of elements of RG and so is an R -derivation of RG . This proves (ii) and (iii). \square

Corollary 2.2.6. *Let $G = \langle S \mid T \rangle$ be a group, where S is a generating set and T a set of relators. Let F_S be the free group on S and $\phi: F_S \rightarrow G$ the homomorphism of F_S onto G . Let K be an algebraic extension of a prime field and f a map from S to KG . Then*

- (i) *f can be uniquely extended to a map f^* from F_S to KG that satisfies Equation 2.8,*
- (ii) *f can be extended to a derivation of KG if and only if $f^*(t) = 0$, for all $t \in T$,*
- (iii) *if f can be extended to a derivation of KG , then this extension is unique.*

Proof. By Theorem 2.2.2 all derivations of KG are K -derivations and so the result follows from Theorem 2.2.5. \square

Remark 2.2.7. The restriction that R be a commutative ring in Theorem 2.2.5 is necessary. To demonstrate this, let r_1, r_2 be noncommuting elements in a ring R and let G be the infinite cyclic group generated by $S = \{s\}$, that is the free group on S . Let $f: S \rightarrow RG$ be the map defined by $s \mapsto r_1$ and extend f to a

map $f^*: G \rightarrow RG$ as in Theorem 2.2.5 (i). Assume that f can be extended to an R -derivation d of RG . Then

$$d(s)r_2s + sd(r_2s) = r_1r_2s + sr_2d(s) = r_1r_2s + sr_2r_1 = (r_1r_2 + r_2r_1)s.$$

However

$$d(sr_2s) = r_2d(s^2) = r_2(r_1s + sr_1) = 2r_2r_1s.$$

Therefore the Leibniz rule does not apply since $d(sr_2s) \neq d(s)r_2s + sd(r_2s)$. This contradicts the assumption that f can be extended to an R -derivation of RG .

2.3 Applications

We will now apply the results of the previous sections to finite commutative group algebras in Section 2.3.1 and then to finite dihedral group algebras in Section 2.3.2. The study of finite group algebras is motivated in part by applications to coding theory which appear in Section 2.3.3, where the extended binary Golay [24, 12, 8] code and the extended binary quadratic residue [48, 24, 12] code are presented as images of derivations of group algebras.

2.3.1 Derivations of Commutative Group Algebras

The next result directs our study of derivations of commutative group algebras to the nonsemisimple case.

Theorem 2.3.1. *Let R be a commutative unital ring. Let H be a torsion central subgroup of a group G , where the order of h is invertible in R , for all $h \in H$. Then $d(R) = \{0\}$ if and only if $d(RH) = \{0\}$, for all $d \in \text{Der}(RG)$.*

Proof. Let d be any element of $\text{Der}(RG)$. Assume that $d(R) = \{0\}$. Let h be

an element of H of order s . Applying d to $h^s = 1$ implies $sh^{s-1}d(h) = 0$ by Equation 2.7 of Lemma 2.2.1. By assumption s is invertible in R and so s is also invertible in RG . Therefore $d(h) = 0$ for any $d \in \text{Der}(RG)$. Let $\alpha = \sum_{h \in H} a_h h$ be any element of RH . Then

$$d(\alpha) = d\left(\sum_{h \in H} a_h h\right) = \sum_{h \in H} d(a_h h) = \sum_{h \in H} a_h d(h) = \sum_{h \in H} a_h(0) = 0,$$

by Leibniz's rule since $d(R) = \{0\}$ and so $d(RH) = \{0\}$. The converse is immediate. \square

Corollary 2.3.2. *(i) Let G be a finite abelian group and F either the rational numbers or an algebraic extension of the rationals. Then FG has no nonzero derivations.*

(ii) Let H be a p -regular subgroup of a finite abelian group G and $F = \mathbb{F}_{p^n}$. Then all derivations of FG are FH -derivations.

Proof. For part (i) let $H = G$. In both cases F is a commutative unital ring and H is a torsion central subgroup of G , where the order of h is invertible in F for all $h \in H$. Also $d(F) = \{0\}$ for all $d \in \text{Der}(FG)$, by Theorem 2.2.2. Therefore the results follow from Theorem 2.3.1. \square

Note that (i) of this Corollary also follows from Theorem 2.1.1.

Remark 2.3.3. In Theorem 2.3.1, the requirement that the subgroup H is central is necessary. For example, there are 26 non zero derivations of $\mathbb{F}_3 D_8$. Moreover the 27 derivations of $\mathbb{F}_3 D_8$ are inner by Theorem 2.1.1 or Corollary 2.2.3.

In Theorem 2.3.4 we determine all derivations of finite commutative group algebras of positive characteristic p .

Theorem 2.3.4. *Let K be a finite field of positive characteristic p . Let $G \simeq H \times X$ be a finite abelian group, where H is a p -regular group and X is a p -group with the following presentation*

$$X = \langle x_1, \dots, x_n \mid x_k^{p^{m_k}} = 1, [x_k, x_l] = 1, \text{ for all } k, l \in \{1, 2, \dots, n\} \rangle,$$

where $n, m_k \in \mathbb{N}$. For $i, j \in \{1, \dots, n\}$, let $f_i: \{x_1, \dots, x_n\} \rightarrow KG$ be defined by

$$f_i(x_j) = \begin{cases} 1 & \text{if } i = j \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

Then f_i can be uniquely extended to a derivation of KG denoted by ∂_i . Moreover $Der(KG)$ is a vector space over K with basis $\{g\partial_i \mid g \in G, i = 1, \dots, n\}$.

Proof. By Corollary 2.3.2 (ii) all derivations of KG are KH -derivations. Let $S = \{x_1, \dots, x_n\}$ and let f be any map from S to KG . By Theorem 2.2.5 f can be uniquely extended to a map $f^*: F_S \rightarrow KG$ satisfying Equation 2.8. Moreover, f can be extended to a derivation of KG if and only if $f^*(t) = 0$ for $t \in \{[x_k, x_l], x_k^{p^{m_k}} \mid k, l = 1, 2, \dots, n\}$. Let $a, b \in S$. Then

$$\begin{aligned} f^*(a^{-1}b^{-1}ab) &= f^*(a^{-1})b^{-1}ab + a^{-1}f^*(b^{-1})ab + a^{-1}b^{-1}f^*(a)b + a^{-1}b^{-1}af^*(b) \\ &= -a^{-1}f(a)a^{-1}b^{-1}ab - a^{-1}b^{-1}f(b)b^{-1}ab + a^{-1}b^{-1}f(a)b + a^{-1}b^{-1}af(b) \\ &= -a^{-1}f(a) - b^{-1}f(b) + a^{-1}f(a) + b^{-1}f(b) = 0. \end{aligned}$$

Therefore $f^*([x_k, x_l]) = 0$, for all $k, l = 1, 2, \dots, n$. Also by Equation 2.10

$$f^*(x_k^{p^{m_k}}) = \sum_{i=1}^{p^{m_k}} \left(\left(\prod_{j=1}^{i-1} x_k \right) f^*(x_k) \left(\prod_{j=i+1}^{p^{m_k}} x_k \right) \right) = p^{m_k} x_k^{(p^{m_k}-1)} f^*(x_k) = 0,$$

since KG has characteristic p . Therefore any map $f: S \rightarrow KG$ can be uniquely extended to a derivation of KG . By Lemma 2.1.5 $Der(KG)$ is a vector space over K . Let $B = \{g\partial_i \mid g \in G, i = 1, \dots, n\}$. Any map $f: S \rightarrow KG$ can be written

as $\sum_{i=1}^n \sum_{g \in G} k_{i,g} g f_i$, where $k_{i,g} \in K$. The extension of f to a derivation of KG is $\sum_{i=1}^n \sum_{g \in G} k_{i,g} g \partial_i$. Therefore any derivation of KG can be written as a K -linear combination of the elements of B . Furthermore, if $(\sum_{i=1}^n \sum_{g \in G} k_{i,g} g \partial_i)(x_j) = 0$, then $\sum_{g \in G} k_{g,j} g = 0$, which implies $k_{g,j} = 0$ for all $g \in G$. Therefore the elements of B are K -linearly independent and so form a basis of $Der(KG)$. \square

Remark 2.3.5. Derivations of finite commutative group algebras $\mathbb{F}_{p^n}G$ are either the zero derivation (in the semisimple case by Corollary 2.3.2(ii)) or can be decomposed as in Theorem 2.3.4 as the sum of derivations of the group algebras of the cyclic direct factors of G .

As we will see in the next section, derivations of noncommutative finite group algebras are more involved.

2.3.2 Derivations of Dihedral Group Algebras

Let n be an integer greater than 2 and let D_{2n} denote the dihedral group with $2n$ elements and presentation $\langle x, y \mid x^n = y^2 = (xy)^2 = 1 \rangle$. This section classifies the derivations of the group algebra $\mathbb{F}_{2^m}D_{2n}$.

Definition 2.3.6. Let RG be a group ring. The *augmentation ideal* of RG , denoted by $\Delta(G)$, is the kernel of the homomorphism from RG to R defined by $\sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g$.

Lemma 2.3.7. [38, pp.113] *The centre of the group algebra KG has as a K -basis the set of all finite conjugacy class sums.* \square

Lemma 2.3.8. *If n is even, $Z(\mathbb{F}_{2^m}D_{2n})$, the center of $\mathbb{F}_{2^m}D_{2n}$ is a subspace of $\mathbb{F}_{2^m}D_{2n}$ of dimension $\frac{n}{2} + 3$ and a basis $\{1, x^{\frac{n}{2}}, x^1 + x^{-1}, x^2 + x^{-2}, \dots, x^{\frac{n}{2}-1} + x^{-\frac{n}{2}+1}, y + x^2y + x^4y + \dots + x^{n-2}y, xy + x^3y + x^5y + \dots + x^{n-1}y\}$.*

If n is odd, $Z(\mathbb{F}_{2^m}D_{2n})$ has dimension $\frac{n+3}{2}$ and a basis $\{1, x^1 + x^{-1}, x^2 + x^{-2}, \dots, x^{\frac{n-1}{2}} + x^{-\frac{n+1}{2}}, y + xy + x^2y + \dots + x^{n-1}y\}$.

Proof. If n is even the conjugacy classes of D_{2n} are as follows: $\{1\}$, $\{x^{\frac{n}{2}}\}$, $\{x^i, x^{-i}\}$, for $i = 1, 2, \dots, \frac{n}{2} - 1$, $\{y, x^2y, x^4y, \dots, x^{n-2}y\}$ and $\{xy, x^3y, x^5y, \dots, x^{n-1}y\}$. If n is odd the conjugacy classes of D_{2n} are as follows: $\{1\}$, $\{x^i, x^{-i}\}$, for $i = 1, 2, \dots, \frac{n-1}{2}$ and $\{y, xy, x^2y, \dots, x^{n-1}y\}$. The result follows from counting the conjugacy classes and by Lemma 2.3.7. \square

Corollary 2.3.9. *Let $C(y)$ and $C(xy)$ denote respectively the centralisers of y and xy in $\mathbb{F}_{2^m}D_{2n}$. Then the following are bases for $C(y)$ and $C(xy)$.*

Case (1): n is even

$$B_e(y) = \{1, x^{\frac{n}{2}}, y, x^{\frac{n}{2}}y\} \cup \{(x^i + x^{-i}), (x^i + x^{-i})y \mid i = 1, 2, \dots, \frac{n}{2} - 1\}$$

$$B_e(xy) = \{1, x^{\frac{n}{2}}, xy, x^{\frac{n}{2}}xy\} \cup \{(x^i + x^{-i}), x(x^i + x^{-i})y \mid i = 1, 2, \dots, \frac{n}{2} - 1\}.$$

Case (2): n is odd

$$B_o(y) = \{1, y\} \cup \{(x^i + x^{-i}), (x^i + x^{-i})y \mid i = 1, 2, \dots, \frac{n-1}{2}\}$$

$$B_o(xy) = \{1, xy\} \cup \{(x^i + x^{-i}), x(x^i + x^{-i})y \mid i = 1, 2, \dots, \frac{n-1}{2}\}.$$

Proof. Let $g \in D_{2n}$ and denote by $Orb(g^y)$ the subset $\{g, g^y\}$ of D_{2n} . The set $\{Orb(g^y) \mid g \in G\}$ is a partition of D_{2n} . The set of elements formed by taking the partition sums forms a basis $B_e(y)$ for $C(y)$, when n is even and $B_o(y)$, when n is odd. The map $\alpha: D_{2n} \rightarrow D_{2n}$ defined by $y \mapsto xy$ and $x \mapsto x$ is an automorphism of D_{2n} . Extend α \mathbb{F}_{2^m} -linearly to an \mathbb{F}_{2^m} -algebra automorphism of $\mathbb{F}_{2^m}D_{2n}$.

Let $c = a + by$, where $a, b \in \mathbb{F}_{2^m}\langle x \rangle$. Assume that $c \in C(y)$. Then $(a + by)y = y(a + by)$, which implies that $ay = ya$ and $by = yb$ and so $a, b \in Z(\mathbb{F}_{2^m}D_{2n})$. Therefore $\alpha(c) \in C(xy)$, since

$$xy\alpha(c) = xy(a + bxy) = axy + bxyxy = (a + bxy)xy = \alpha(c)xy.$$

Conversely, assume $\alpha(c) = a + bxy \in C(xy)$. Then

$$a^y xy + b^y = xy(a + bxy) = (a + bxy)xy = axy + b.$$

This implies $a = a^y$ and $b = b^y$ and so $c \in C(y)$. Therefore $c \in C(y)$ if and only if $\alpha(c) \in C(xy)$. Applying α to the basis $B_e(y)$ gives $B_e(xy)$ and applying α to $B_o(y)$ gives $B_o(xy)$. \square

Definition 2.3.10. Given a derivation d of $\mathbb{F}_{2^m}D_{2n}$, denote it by $d = d_{x',y'}$, where $x' = d(x)$ and $y' = d(y)$. Note that $d(x)$ and $d(y)$ uniquely determine this derivation.

By Lemma 2.1.5, $Der(\mathbb{F}_{2^m}D_{2n})$ forms a vector space over \mathbb{F}_{2^m} . The following Theorem exhibits a basis for $Der(\mathbb{F}_{2^m}D_{2n})$.

Theorem 2.3.11. *If n is even, $Der(\mathbb{F}_{2^m}D_{2n})$ has dimension $2n + 4$ and a basis*

$$\{d_{x',y'} \mid (x', y') \in \{(\lambda y, 0), (x\omega y, \omega) \mid \lambda \in B_e(xy), \omega \in B_e(y)\}\}.$$

If n is odd, $Der(\mathbb{F}_{2^m}D_{2n})$ has dimension $\frac{3n+1}{2}$ and a basis

$$\begin{aligned} &\{d_{x',y'} \mid (x', y') \in \{((x^i + x^{-i})y, 0), ((1+x)y, 1), (0, y), \\ &(x(x^i + x^{-i})y, x^i + x^{-i}), (0, (x^i + x^{-i})y) \mid i = 1, \dots, \frac{n-1}{2}\}\}. \end{aligned}$$

Proof. The relators of D_{2n} are y^2 , $(xy)^2$ and x^n . Therefore by Corollary 2.2.6, $f: \{x, y\} \rightarrow \mathbb{F}_{2^m}D_{2n}$ can be extended to a derivation of $\mathbb{F}_{2^m}D_{2n}$ if and only if $f^*(y^2) = f^*((xy)^2) = f^*(x^n) = 0$. $f^*(y^2) = 0$ if and only if $f(y) \in C(y)$. Also $f^*((xy)^2) = 0$ if and only if $f(x)y + xf(y) \in C(xy)$, since $f^*((xy)^2) = f^*(xy)xy + xyf^*(xy)$ and $f^*(xy) = f(x)y + xf(y)$. We now treat the cases where n is even and n is odd separately.

Case (1): n is even. $f^*(x^n) = f^*(x^{\frac{n}{2}}x^{\frac{n}{2}}) = f^*(x^{\frac{n}{2}})x^{\frac{n}{2}} + x^{\frac{n}{2}}f^*(x^{\frac{n}{2}}) = 0$, for all $f(x) \in \mathbb{F}_{2^m}D_{2n}$, since $x^{\frac{n}{2}} \in Z(\mathbb{F}_{2^m}D_{2n})$. Therefore $f: \{x, y\} \rightarrow \mathbb{F}_{2^m}D_{2n}$ can be extended to a derivation of $\mathbb{F}_{2^m}D_{2n}$ if and only if $f(y) \in C(y)$ and $f(x)y + xf(y) \in C(xy)$.

Let $f(y)$ and $f^*(xy)$ be arbitrary elements of $C(y)$ and $C(xy)$, respectively. Write $f(y) = \Omega = \sum_{i=1}^{n+2} r_i \omega_i$ and $f^*(xy) = \Lambda = \sum_{i=1}^{n+2} k_i \lambda_i$, where $r_i, k_i \in \mathbb{F}_{2^m}$, $\omega_i \in B_e(y)$ and $\lambda_i \in B_e(xy)$. Then $\Lambda = f^*(xy) = f(x)y + x\Omega$ and so $f(x) = \Lambda y + x\Omega y$. Therefore

$$Der(\mathbb{F}_{2^m}D_{2n}) = \{d_{(\Lambda y + x\Omega y, \Omega)}\} = \{d_{(\sum k_i \lambda_i y + \sum r_i x \omega_i y, \sum r_i \omega_i)}\}.$$

Define $B_e = \{d_{(\lambda y, 0)}, d_{(x\omega y, \omega)} \mid \lambda \in B_e(xy), \omega \in B_e(y)\}$. Then B_e is a spanning set for $Der(\mathbb{F}_{2^m}D_{2n})$, since $r_1 \cdot d_{(x_1, y_1)} + r_2 \cdot d_{(x_2, y_2)} = d_{(r_1 x_1 + r_2 x_2, r_1 y_1 + r_2 y_2)}$ for $r_1, r_2 \in \mathbb{F}_{2^m}$ and $x_1, x_2, y_1, y_2 \in \mathbb{F}_{2^m}D_{2n}$. We now show that the elements of B_e are linearly independent. Assume

$$\sum_{i=1}^{n+2} k_i d_{(\lambda_i y, 0)} + \sum_{i=1}^{n+2} r_i d_{(x\omega_i y, \omega_i)} = d_{(\sum k_i \lambda_i y + \sum r_i x \omega_i y, \sum r_i \omega_i)} = d_{(0, 0)}$$

This implies $r_i = k_i = 0$ for $i = 1, 2, \dots, n+2$. Therefore $Der(\mathbb{F}_{2^m}D_{2n})$ has a basis $B_e = \{d_{x', y'} \mid (x', y') \in \{(\lambda y, 0), (x\omega y, \omega) \mid \lambda \in B_e(xy), \omega \in B_e(y)\}\}$ and dimension $2n + 4$.

Case (2): n is odd. Let $f(x) = a + by$, where $a, b \in \mathbb{F}_{2^m}\langle x \rangle$. Assume that f can be extended to a derivation of $Der(\mathbb{F}_{2^m}D_{2n})$. So $f^*(x^n) = 0$. Applying Equation 2.10 gives

$$0 = \sum_{i=1}^n \left(\left(\prod_{j=1}^{i-1} x \right) f^*(x) \left(\prod_{j=i+1}^n x \right) \right) = \sum_{t=0}^{n-1} x^t (a + by) x^{n-1-t} = nax^{n-1} + \sum_{t=0}^{n-1} x^{2t+1} by.$$

Right multiplying this equation by x and using $n \equiv 1 \pmod{2}$ and $\sum_{t=0}^{n-1} x^{2t} =$

$(\sum_{t=0}^{n-1} x^t)^2 = n \sum_{t=0}^{n-1} x^t$ gives $a + \sum_{t=0}^{n-1} x^t b y = 0$. This implies that $a = 0$ and $b \in \Delta(\langle x \rangle)$. Therefore there is a third condition when n is odd, namely $f(x) = b y$, where $b \in \Delta(\langle x \rangle)$.

Let $f(y) = \Omega \in C(y)$ and let $f^*(xy) = \Lambda \in C(xy)$. Then $\Lambda = f^*(xy) = f(x)y + x\Omega$ and so $f(x) = \Lambda y + x\Omega y$. Therefore $Der(\mathbb{F}_{2^m} D_{2n}) = \{d_{(\Lambda y + x\Omega y, \Omega)} \mid \Lambda \in C(xy), \Omega \in C(y), \Lambda + x\Omega \in \Delta(\langle x \rangle)\}$. Write Λ and Ω as \mathbb{F}_{2^m} -linear combinations of $B_o(xy)$ and $B_o(y)$ respectively, that is

$$\begin{aligned} \Lambda &= k_1 1 + k_2 xy + \sum_{i=1}^{\frac{n-1}{2}} k_{3,i} (x^i + x^{-i}) + \sum_{i=1}^{\frac{n-1}{2}} k_{4,i} x (x^i + x^{-i}) y, \\ \Omega &= r_1 1 + r_2 y + \sum_{i=1}^{\frac{n-1}{2}} r_{3,i} (x^i + x^{-i}) + \sum_{i=1}^{\frac{n-1}{2}} r_{4,i} x (x^i + x^{-i}) y \quad \text{and so} \\ \Lambda + x\Omega &= k_1 1 + r_1 x + (k_2 + r_2) xy + \sum_{i=1}^{\frac{n-1}{2}} k_{3,i} (x^i + x^{-i}) \\ &\quad + \sum_{i=1}^{\frac{n-1}{2}} r_{3,i} x (x^i + x^{-i}) + \sum_{i=1}^{\frac{n-1}{2}} (k_{4,i} + r_{4,i}) x (x^i + x^{-i}) y. \end{aligned}$$

Then $(\Lambda + x\Omega) \in \Delta(\langle x \rangle)$ implies that $k_1 = r_1$, $k_2 = r_2$ and $k_{4,i} = r_{4,i}$, for $i = 1, 2, \dots, \frac{n-1}{2}$. Therefore $Der(\mathbb{F}_{2^m} D_{2n}) = \{d_{(\Lambda y + x\Omega y, \Omega)}\}$, where

$$\begin{aligned} \Lambda y + x\Omega y &= r_1 (1 + x)y + \sum_{i=1}^{\frac{n-1}{2}} k_{3,i} (x^i + x^{-i}) y + \sum_{i=1}^{\frac{n-1}{2}} r_{3,i} x (x^i + x^{-i}) y \\ \text{and } \Omega &= r_1 1 + r_2 y + \sum_{i=1}^{\frac{n-1}{2}} r_{3,i} (x^i + x^{-i}) + \sum_{i=1}^{\frac{n-1}{2}} r_{4,i} x (x^i + x^{-i}) y. \end{aligned}$$

Define $B_o = \{d_{x',y'}\}$ where $(x', y') \in \{((1+x)y, 1), ((x^i + x^{-i})y, 0), (x(x^i + x^{-i})y, x^i + x^{-i}), (0, y), (0, (x^i + x^{-i})y) \mid i = 1, 2, \dots, \frac{n-1}{2}\}$. B_o is a spanning set for $Der(\mathbb{F}_{2^m} D_{2n})$. The elements of B_o are linearly independent since $d_{(\Lambda y + x\Omega y, \Omega)} = d_{(0,0)}$ implies that $r_1 = r_2 = r_{3,i} = r_{4,i} = k_{3,i} = 0$, for $i = 1, 2, \dots, \frac{n-1}{2}$.

Therefore $Der(\mathbb{F}_{2^m} D_{2n})$ has a basis $B_o = \{d_{x',y'}\}$ where $(x', y') \in \{((1+x)$

$x)y, 1), ((x^i + x^{-i})y, 0), (x(x^i + x^{-i})y, x^i + x^{-i}), (0, y), (0, (x^i + x^{-i})y) \mid i = 1, 2, \dots, \frac{n-1}{2}\}$. Thus $Der(\mathbb{F}_{2^m}D_{2n})$ has dimension $3\binom{n-1}{2} + 2 = \frac{3n+1}{2}$. \square

Lemma 2.3.12. [42] *Let a and c be elements of a ring R and let d_c be the map from R to R defined by $d_c(a) = [c, a] = ca - ac$ for all $a \in R$. Then*

1. *The Lie commutator is anti-symmetric, i.e. $[a, b] = -[b, a]$.*
2. *The map d_c is an inner derivation for all $c \in R$.*
3. *$d_c = 0$ if and only if $c \in Z(R)$.*

We now give a basis for the set of inner derivations of $\mathbb{F}_{2^m}D_{2n}$.

Theorem 2.3.13. *The set of inner derivations of $\mathbb{F}_{2^m}D_{2n}$ is an \mathbb{F}_{2^m} -vector space with dimension $3\lfloor \frac{n-1}{2} \rfloor$ and basis*

$$\{d_b \mid b \in \{x^i \mid i = 1, 2, \dots, \lfloor \frac{n-1}{2} \rfloor\} \cup \{x^i y \mid i = 0, 1, \dots, 2\lfloor \frac{n-1}{2} \rfloor - 1\}\}.$$

Proof. By Lemma 2.3.12 the Lie commutator is anti-symmetric and so it is symmetric in characteristic 2. Let $a, b, c \in \mathbb{F}_{2^m}D_{2n}$. Then $d_{a+b}(c) = d_c(a+b) = d_c(a) + d_c(b) = d_a(c) + d_b(c)$ and so the inner derivations of $\mathbb{F}_{2^m}D_{2n}$ are closed under addition. If $k \in \mathbb{F}_{2^m}$, then $kd_b = d_{kb}$ and thus the inner derivations of $\mathbb{F}_{2^m}D_{2n}$ form a vector subspace of $Der(\mathbb{F}_{2^m}D_{2n})$. Let $B = \{x^i \mid i = 1, 2, \dots, \lfloor \frac{n-1}{2} \rfloor\} \cup \{x^i y \mid i = 0, 1, \dots, 2\lfloor \frac{n-1}{2} \rfloor - 1\}$.

Case(1) n is even. Write $n = 2c$. By Lemma 2.3.8, $Z(\mathbb{F}_{2^m}D_{2n})$ is a $(\frac{n}{2} + 3)$ -dimensional subspace of $\mathbb{F}_{2^m}D_{2n}$ with basis $B_Z = \{1, x^c, x+x^{-1}, x^2+x^{-2}, \dots, x^{(c-1)} + x^{(c+1)}, \sum_{i=0}^{c-1} x^{2i}y, \sum_{i=0}^{c-1} x^{2i+1}y\}$. The union of the disjoint sets B and B_Z is a basis for $\mathbb{F}_{2^m}D_{2n}$.

Case(2) n is odd. Write $n = 2c + 1$. By Lemma 2.3.8, $Z(\mathbb{F}_{2^m}D_{2n})$ is a $(\frac{n+3}{2})$ -dimensional subspace of $\mathbb{F}_{2^m}D_{2n}$ with basis $B_Z = \{1, x + x^{-1}, x^2 + x^{-2}, \dots, x^c + x^{-c}, \sum_{i=0}^{2c} x^i y\}$. Again, the disjoint union of B and B_Z is a basis for $\mathbb{F}_{2^m}D_{2n}$.

Write $a = z_a + \sum_{i=1}^{3\lfloor \frac{n-1}{2} \rfloor} a_i b_i$, where $z_a \in Z(\mathbb{F}_{2^m} D_{2n})$, $a_i \in \mathbb{F}_{2^m}$ and $b_i \in B$, for $i = 1, 2, \dots, 3\lfloor \frac{n-1}{2} \rfloor$. $d_c = 0$ if and only if $c \in Z(\mathbb{F}_{2^m} D_{2n})$ and so

$$d_a = d_{z_a} + \sum_{i=1}^{3\lfloor \frac{n-1}{2} \rfloor} d_{a_i b_i} = \sum_{i=1}^{3\lfloor \frac{n-1}{2} \rfloor} d_{a_i b_i}.$$

Therefore the set $\{d_b \mid b \in B\}$ spans the set of inner derivations of $\mathbb{F}_{2^m} D_{2n}$. Moreover, if $\sum_{i=1}^{3\lfloor \frac{n-1}{2} \rfloor} d_{a_i b_i} = d_0$ then $\sum_{i=1}^{3\lfloor \frac{n-1}{2} \rfloor} a_i b_i \in Z(\mathbb{F}_{2^m} D_{2n})$ which implies that $a_i = 0$, for $i = 1, 2, \dots, 3\lfloor \frac{n-1}{2} \rfloor$ and so the set $\{d_b \mid b \in B\}$ forms a basis for the vector space of inner derivations of $\mathbb{F}_{2^m} D_{2n}$. \square

The derivation problem asks whether every derivation from $L^1(G)$ to $M(G)$ is inner, where G is a locally compact group and $M(G)$ is the multiplier algebra of $L^1(G)$. It was solved by Losert [34]. We can ask a similar question for finite group algebras. Let KG be a group algebra where both K and G are finite. Are all derivations of KG inner? Theorems 2.3.11 and 2.3.13 show that the dimension of $Der(\mathbb{F}_{2^m} D_{2n})$ is greater than the dimension of the inner derivations of $\mathbb{F}_{2^m} D_{2n}$ and so not all derivations of $\mathbb{F}_{2^m} D_{2n}$ are inner. However does there exist an algebra $A \supset KG$ such that all derivations of KG become inner in A ? Theorem 2.3.15 answers this question.

Definition 2.3.14. [42] Let R be a ring and δ a derivation of R . The ring $R[x; \delta] = \left\{ \sum_{i=0}^n a_i x^i \mid n \in \mathbb{N}, a_i \in R \right\}$, where addition is performed componentwise and multiplication satisfies the relation $xa = ax + \delta(a)$, for all $a \in R$ is called a *differential polynomial ring*.

Theorem 2.3.15. *Let G be a finite group and KG be the group algebra over the finite field K . Let $A_d = \frac{KG[x; d]}{(x^2 - 1)}$, where $d \in Der(KG)$ and $(x^2 - 1)$ is the 2-sided ideal of $KG[x; d]$ generated by $x^2 - 1$. Then all derivations d of KG are inner on A_d .*

Proof. Let D_x be the inner derivation of A_d induced by x , that is $D_x: A_d \rightarrow A_d$, defined by $a \mapsto xa - ax$. By the multiplication relation of A_d defined in Definition 2.3.14, $xa - ax = ax + d(a) - ax = d(a)$. Therefore the restriction of D_x to KG is equal to d . \square

2.3.3 Applications to Coding Theory

Example 2.3.16. Let $C_{24} = \langle x \mid x^{24} = 1 \rangle$ and let $d: \mathbb{F}_2 C_{24} \rightarrow \mathbb{F}_2 C_{24}$ be the derivation defined by $x \mapsto 1 + x + x^3 + x^4 + x^5 + x^7 + x^9 + x^{12}$ (by Theorem 2.3.4 this uniquely defines a derivation). Then by Lemma 2.2.1, $d(x^{2n}) = 0$ and $d(x^{2n+1}) = x^{2n}d(x)$, for $n \in \{0, 1, \dots, 11\}$. The image of the group algebra under this derivation is a binary code of length 24 and dimension 12. A generator matrix G_{24} of this code is given in Figure 2.1.

Figure 2.1: Generator matrix of the binary $[24, 12, 8]$ code defined by the derivation d .

$$G_{24} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Permuting the columns of G_{24} using the permutation

$$(6, 19, 12, 10, 11, 22, 8, 21, 15, 16, 18, 9, 24, 13, 20)(7, 23, 17, 14)$$

and then transforming it to reduced row echelon form produces the matrix given

as the generator of the extended binary Golay code in [25]. So the image of \mathbb{F}_2C_{24} under the derivation is equivalent to the extended binary Golay [24, 12, 8] code. It has minimum distance 8 and is a doubly even and self dual extremal code.

Figure 2.2: The right hand block of a generator matrix of the binary [48, 24, 12] code defined by the derivation δ .

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

Example 2.3.17. Let $C_{48} = \langle x \mid x^{48} = 1 \rangle$ and $\delta: \mathbb{F}_2C_{48} \rightarrow \mathbb{F}_2C_{48}$ be the derivation defined by

$$x \mapsto 1 + x^{24} + x^{27} + x^{31} + x^{32} + x^{33} + x^{37} + x^{40} + x^{41} + x^{43} + x^{44} + x^{47}.$$

Again by Theorem 2.3.4 this uniquely defines a derivation of \mathbb{F}_2C_{48} . The image of the group algebra under this derivation is a binary [48, 24, 12] doubly even self

dual code (verified using GAP 4.8.6 [18]). It is equivalent to the extended binary quadratic residue code of length 48 [26]. A generator matrix for this code is given by the block matrix $[I_{24} \mid A]$, where I_{24} is the identity of the ring of 24×24 matrices over \mathbb{F}_2 and A is the matrix given in Figure 2.2.

Chapter 3

Derivations of Modular Group Algebras and Codes

In this chapter we examine the derivations of a modular group algebra KG and briefly discuss an application to the theory of error correcting codes. The ring of constants, $\mathcal{C}(KG)$ is introduced. This subring of KG will prove useful in this and subsequent chapters. Necessary and sufficient conditions on a subgroup H of G are given such that the augmentation ideal $\Delta(G, H)$ is a differential ideal. An implication of this result is that, H being contained within the ring of constants is a sufficient condition for the augmentation ideal $\Delta(G, H)$ to be a differential ideal.

It is shown in Theorem 3.1.18 that if $\phi: R \rightarrow S$ is a ring isomorphism, then $\Phi: Der(R) \rightarrow Der(S)$ defined by $d \mapsto \phi \circ d \circ \phi^{-1}$ is an isomorphism of additive groups. If KG and KH are isomorphic as K -algebras, then $Der(KG)$ and $Der(KH)$ are isomorphic as Lie algebras. An ideal of KG generated by constants of KG is shown in Corollary 3.1.16 to be a differential ideal for all derivations of KG .

Section 3.2 examines the modular group algebra \mathbb{F}_2D_8 . A basis for its derivation algebra is given and those derivations that are inner are identified. Table 3.1

combined with Lemma 3.2.22 gives all conjugates of elements of D_8 by units of \mathbb{F}_2D_8 . Summing these gives the conjugates of all elements of \mathbb{F}_2D_8 by units of \mathbb{F}_2D_8 . The ideals of \mathbb{F}_2D_8 are shown in Figure 3.1 and for specific ideals, the derivations that map the ideal to itself are identified. A presentation of the unit group of \mathbb{F}_2D_8 is also given.

The existence of an algebra A such that outer derivations of KG become inner on A , is discussed briefly in Section 3.3. It is shown in Lemma 3.3.3 that no outer derivation of KH becomes inner in KG , where H is a subgroup of G . A list of theorems from linear algebra that are used in the subsequent section and chapters is given in Section 3.4. The final section of this chapter looks at generating error correcting codes from derivations of modular group algebras.

3.1 Derivations, Ideals and Homomorphisms

Definition 3.1.1. Let R be a ring and H a subgroup of a group G . The *augmentation ideal* denoted by $\Delta_R(G, H)$ or $\Delta(G, H)$ is the left ideal of RG generated by the set $\{h - 1 \mid h \in H\}$. That is, $\Delta_R(G, H) = \left\{ \sum_{h \in H} \alpha_h (h - 1) \mid \alpha_h \in RG \right\}$. $\Delta(G, G)$ is denoted by $\Delta(G)$.

Lemma 3.1.2. [40] Let S be a set of generators of a subgroup H of a group G . Then, the set $\{s - 1 \mid s \in S\}$ is a set of generators of $\Delta(G, H)$ as a left ideal of RG .

Definition 3.1.3. Denote by $\mathcal{T} = \{q_i \mid i \in I\}$ a complete set of representatives of left cosets of H in G . The identity element is always chosen as the representative of H .

Proposition 3.1.4. [40] Let R be a ring and H a subgroup of a group G . Then the set $B_H = \{q(h - 1) \mid q \in \mathcal{T}, h \in H, h \neq 1\}$ is a basis of $\Delta_R(G, H)$ over R .

Lemma 3.1.5. [40] Let R be a ring and let H be a subgroup of a group G . Then the ideal $\Delta(G, H)$ is a two-sided ideal of RG if and only if H is a normal subgroup of G .

Proposition 3.1.6. [40] Let H be a normal subgroup of a group G . Then

1. The canonical group homomorphism $\psi: G \rightarrow G/H$ can be extended to an epimorphism $\psi: RG \rightarrow R(G/H)$ such that $\psi\left(\sum_{g \in G} a_g g\right) = \sum_{g \in G} a_g \psi(g)$
2. $\ker(\psi) = \Delta(G, H)$
3. $\frac{RG}{\Delta(G, H)} \simeq R(G/H)$

Definition 3.1.7. A *differential ring* is a unital ring R together with a distinguished derivation d of R , and is denoted by the pair (R, d) .

Definition 3.1.8. Let (A, d) be a differential ring. Then a (left / right / two-sided) ideal I of A is a *differential ideal* of (A, d) , if $d(a) \in I$, for all $a \in I$, i.e. $d(I) \subset I$. Also, I is a *differential (left / right / two-sided) ideal* of A , if $d(I) \subset I$, for all $d \in \text{Der}(A)$.

Lemma 3.1.9. Let I be a differential two-sided ideal of a differential ring (A, d) . Then $\bar{d}: A/I \rightarrow A/I$ defined by $\bar{d}(a + I) = d(a) + I$ is a derivation of A/I and is independent of the choice of representative in the coset. \square

Definition 3.1.10. Let (A, d) and (B, \bar{d}) be differential rings. A *differential homomorphism* ϕ from (A, d) to (B, \bar{d}) is a ring homomorphism which commutes with the derivations. That is, $\phi \circ d = \bar{d} \circ \phi$.

Lemma 3.1.11. Let I be a differential two-sided ideal of a ring A . Then the homomorphism $\phi: A \rightarrow A/I$ defined by $a \mapsto a + I$ is a differential homomorphism from (A, d) to $(A/I, \bar{d})$ for all $d \in \text{Der}(A)$.

Proof. Let $d \in \text{Der}(A)$ and let $\bar{d}: A/I \rightarrow A/I$ be defined by $\bar{d}(a + I) = d(a) + I$, where $a \in A$. Then by Lemma 3.1.9, $\bar{d} \in \text{Der}(A/I)$ and

$$(\bar{d} \circ \phi)a = \bar{d}(a + I) = d(a) + I = (\phi \circ d)(a). \quad \square$$

Lemma 3.1.12. *Let I and I_a both be (left / right / two-sided) ideals of a finite unital ring R such that I_a is the principal ideal generated by the element a and $I_a \subset I$. Then for any $d \in \text{Der}(R)$, $d(I_a) \subset I$ if and only if $d(a) \in I$.*

Proof. Let $d \in \text{Der}(R)$. Assume that $d(I_a) \subset I$. Then $d(a) \in I$ since $a \in I_a$. Conversely, assume that $d(a) \in I$. Let $\alpha \in I_a$ and write $\alpha = \sum_{i=1}^n r_i a s_i$ where $r_i, s_i \in R$, for $i = 1, 2, \dots, n$ and n is a positive integer. Then

$$d(\alpha) = \sum_{i=1}^n d(r_i a s_i) = \sum_{i=1}^n (d(r_i) a s_i + r_i d(a) s_i + r_i a d(s_i)).$$

If I_a and I are left ideals, then it can be assumed that $s_i = 1$ and so $d(s_i) = 0$. Also, $d(r_i)a \in I$, since $a \in I_a \subset I$ and $r_i d(a) \in I$, since it is assumed that $d(a) \in I$. Therefore $d(\alpha) = \sum_{i=1}^n (d(r_i)a + r_i d(a)) \in I$, since it is a sum of elements of I . Likewise, if I_a and I are right ideals, then then it can be assumed that $r_i = 1$. Also, $a d(s_i) \in I$ and $d(a)s_i \in I$ and so $d(\alpha) = \sum_{i=1}^n (d(a)s_i + a d(s_i)) \in I$. Finally, if I_a and I are two-sided ideals, then $d(\alpha) \in I$, since $d(r_i)a s_i, r_i d(a) s_i$ and $r_i a d(s_i)$ are all in I . Therefore in each case $d(\alpha) \in I$ and so $d(I_a) \subset I$. □

Lemma 3.1.13. *Let I be the (left / right / two-sided) ideal of a finite unital ring R generated by the elements a_1, a_2, \dots, a_n . Then $d(I) \subset I$ if and only if $d(a_j) \in I$ for all $j = 1, 2, \dots, n$.*

Proof. Let I_{a_j} be the principal ideal of R generated by a_j with the same sidedness as I . Then $I = I_{a_1} + I_{a_2} + \dots + I_{a_n}$. Assume that $d(I) \subset I$. For all $j = 1, 2, \dots, n$, $a_j \in I$ and so $d(a_j) \in I$. Conversely, assume that $d(a_j) \in I$ for all $j = 1, 2, \dots, n$.

Then $d(I_{a_j}) \subset I$, for all j by Lemma 3.1.12. Let $\alpha \in I$ and write $\alpha = \sum_{j=1}^n \alpha_j$, where $\alpha_j \in I_{a_j}$. Then $d(\alpha_j) \in I$ for all $j = 1, 2, \dots, n$ and so

$$d(\alpha) = d\left(\sum_{j=1}^n \alpha_j\right) = \sum_{j=1}^n d(\alpha_j) \in I.$$

□

Corollary 3.1.14. *Let H be a subgroup of a finite group G , let K be a finite field and let $d \in \text{Der}(KG)$. Then $\Delta(G, H)$ is a differential ideal of (KG, d) if and only if $d(H) \subset \Delta(G, H)$.*

Proof. Let $d \in \text{Der}(KG)$. $\Delta(G, H)$ is a left ideal of KG generated by the set $\{h - 1 \mid h \in H\}$. Therefore by Lemma 3.1.13, $\Delta(G, H)$ is a differential ideal of (KG, d) if and only if $d(h - 1) = d(h) \in \Delta(G, H)$, for all $h \in H$. □

Definition 3.1.15. Let d be a derivation of a unital ring R and let Δ be a subset of $\text{Der}(R)$. Then the subring of R defined by $\mathcal{C}_\Delta = \{c \in R \mid d(c) = 0 \text{ for all } d \in \Delta\}$ is called the *ring of constants of Δ* . If Δ is a set with one element d then \mathcal{C}_Δ will be denoted by \mathcal{C}_d and if $\Delta = \text{Der}(R)$ then \mathcal{C}_Δ will be denoted by $\mathcal{C}(R)$ and is then called the *ring of constants of R* .

Corollary 3.1.16. *Let K be a finite field and let G be a finite group. Let I be a (left / right / two-sided) ideal of KG generated by a subset of the ring of constants, $\mathcal{C}(KG)$. Then I is a differential ideal of KG .*

Proof. Let I be a (left / right / two-sided) ideal of KG generated by $C \subset \mathcal{C}(KG)$. The $d(C) = 0 \in I$, for all $d \in \text{Der}(KG)$. Therefore I is a differential ideal of KG , by Lemma 3.1.13. □

Corollary 3.1.17. *Let G be a finite group and let K be a finite field. Let H be a subgroup of G such that $H \subset \mathcal{C}(KG)$, the ring of constants of KG . Then $\Delta(G, H)$ is a differential ideal of KG .*

Proof. $\Delta(G, H)$ is a left ideal of KG generated by the set $\{h - 1 \mid h \in H\}$. The result now follows by Corollary 3.1.16. \square

Theorem 3.1.18. *Let R and S be rings and let $\phi: R \rightarrow S$ be a ring isomorphism. Let $\Phi: Der(R) \rightarrow Der(S)$ be defined by $d \mapsto \phi \circ d \circ \phi^{-1}$. Then Φ is an isomorphism of additive groups.*

Proof. Let $d \in Der(R)$. $\Phi(d) = \phi \circ d \circ \phi^{-1}$ is an additive map since it is the composition of additive maps. Let $\alpha, \beta \in R$ and let $a = \phi(\alpha)$ and $b = \phi(\beta)$. Then

$$\begin{aligned} \Phi(d)(ab) &= \phi \circ d \circ \phi^{-1}(ab) = \phi(d(\alpha\beta)) = \phi(d(\alpha)\beta + \alpha d(\beta)) \\ &= \phi(d(\alpha)\beta) + \phi(\alpha d(\beta)) = \phi(d(\alpha))\phi(\beta) + \phi(\alpha)\phi(d(\beta)) \\ &= \phi(d(\alpha))b + a\phi(d(\beta)) = \Phi(d)(a)b + a\Phi(d)(b). \end{aligned}$$

Therefore, $\Phi(d)$ satisfies Equations 2.1 and 2.2 and so is a derivation of S . The map $\Phi^{-1}: Der(S) \rightarrow Der(R)$ defined by $D \mapsto \phi^{-1} \circ D \circ \phi$ is a two-sided inverse of Φ and so Φ is a bijection. Let $d_1 \in Der(R)$. Then

$$\begin{aligned} \Phi(d + d_1)(\alpha) &= \phi(d + d_1)(a) = \phi(d(a) + d_1(a)) \\ &= \phi(d(a)) + \phi(d_1(a)) = \Phi(d)(\alpha) + \Phi(d_1)(\alpha). \end{aligned}$$

Therefore Φ preserves the additive group structure of $Der(R)$ and so is an additive group isomorphism. \square

Lemma 3.1.19. *Let p be a prime number, let \mathbb{F}_p be the field with p elements and let K be a finite field of characteristic p . Let G and H be finite p -groups and let $\phi: KG \rightarrow KH$ be a ring isomorphism. Then ϕ is an \mathbb{F}_p -algebra isomorphism.*

Proof. ϕ is a ring isomorphism and so is bijective. Let α be an arbitrary element of KH and let $a = \phi^{-1}(\alpha)$. Denote the multiplicative identity of KG and KH as

e_G and e_H respectively. Then

$$\phi(e_G)\alpha = \phi(e_G a) = \phi(a) = \phi(a e_G) = \alpha\phi(e_G).$$

Therefore $\phi(e_G) = e_H$. Also for any $k \in \mathbb{F}_p$

$$\phi(k e_G) = \sum_{i=1}^k \phi(e_G) = \sum_{i=1}^k e_H = k e_H.$$

Therefore $\phi(k e_G a) = \phi(k e_G)\phi(a) = k e_H\phi(a) = k\phi(a)$ and so ϕ is an \mathbb{F}_p -linear map. \square

Theorem 3.1.20. *Let $\phi: R \rightarrow S$ be a K -algebra isomorphism. Then $\Phi: Der(R) \rightarrow Der(S)$, defined by $d \mapsto \phi \circ d \circ \phi^{-1}$ is a Lie algebra isomorphism.*

Proof. Let $d, D \in Der(R)$ and let $k \in K$. By Theorem 3.1.18, $\Phi(d)$ is a derivation of S and Φ is an additive map. Therefore

$$\begin{aligned} \Phi(kd) &= \phi \circ kd \circ \phi^{-1} = k\phi \circ d \circ \phi^{-1} = k\Phi(d), \\ [\Phi(d), \Phi(D)] &= [\phi \circ d \circ \phi^{-1}, \phi \circ D \circ \phi^{-1}] = \phi \circ d \circ D \circ \phi^{-1} - \phi \circ D \circ d \circ \phi^{-1} \\ &= \phi \circ [d, D] \circ \phi^{-1} = \Phi([d, D]). \end{aligned}$$

Therefore Φ is a lie algebra homomorphism. Φ is a bijection by Theorem 3.1.18. \square

Theorem 3.1.21. *Let I be a differential two-sided ideal of a unital ring R and let $d \in Der(R)$. Let $\bar{d}: R/I \rightarrow R/I$ be defined by $\bar{d}(a + I) = d(a) + I$. Then $\Phi: Der(R) \rightarrow Der(R/I)$ defined by $d \mapsto \bar{d}$ is a Lie algebra homomorphism.*

Proof. $\bar{d} \in Der(R/I)$ for all $d \in Der(R)$ by Lemma 3.1.9. The homomorphism $\phi: R \rightarrow R/I$ defined by $a \mapsto a + I$ is differential by Lemma 3.1.11. Let $d, D \in$

$Der(R)$, let $k \in K$ and let $a \in R$. Then

$$\begin{aligned}
\Phi(d + D)(a + I) &= (d + D)(a) + I = d(a) + I + D(a) + I \\
&= \Phi(d)(a + I) + \Phi(D)(a + I), \\
\Phi(kd)(a + I) &= kd(a) + I = k(d(a) + I) = k\Phi(d)(a + I), \text{ and} \\
[\Phi(d), \Phi(D)](a + I) &= \Phi(d)(\Phi(D)(a + I)) - \Phi(D)(\Phi(d)(a + I)) \\
&= \Phi(d)(D(a) + I) - \Phi(D)(d(a) + I) \\
&= dD(a) + I - Dd(a) + I \\
&= [d, D](a) + I = \Phi([d, D])(a + I).
\end{aligned}$$

Therefore Φ is a Lie algebra homomorphism. □

Corollary 3.1.22. *Let K be a finite field and let N be a normal subgroup of a finite group G such that $d(N) \subset I = \Delta(G, N)$ for all $d \in Der(KG)$. Then $\Phi: Der(KG) \rightarrow Der(KG/I)$ defined by $d \mapsto \bar{d}$ is a Lie algebra homomorphism.*

Proof. I is a two-sided ideal of KG by Lemma 3.1.5 and is a differential ideal for all $d \in Der(KG)$ by Corollary 3.1.14. Therefore Φ is a Lie algebra homomorphism by Theorem 3.1.21. □

3.2 An Example: $\mathbb{F}_2 D_8$

Let D_8 be the dihedral group of order 8 with presentation

$$D_8 = \langle x, y \mid y^2 = x^4 = (xy)^2 = 1 \rangle.$$

Let $\hat{x} = 1 + x + x^2 + x^3$.

Remark 3.2.1. The group algebra $\mathbb{F}_2 D_8$ is purely modular in the sense that it has no nontrivial idempotents. This is a consequence of the following theorem and the fact that $|D_8| = 2^3$.

Theorem 3.2.2. [48, pp. 378] *If RG is the group ring of a finite group over a commutative unital ring R such that every prime divisor of the order of G is a non-unit of R and R has no nontrivial idempotents then RG has no nontrivial idempotents.*

Remark 3.2.3. The conjugacy classes of D_8 are: $\{1\}$, $\{x^2\}$, $\{x, x^3\}$, $\{y, x^2y\}$, $\{xy, x^3y\}$. Note that conjugation either fixes an element of D_8 or it multiplies it by x^2 .

Remark 3.2.4. Letting $n = 4$ in Lemma 2.3.8 implies the set $B_Z = \{1, x^2, x(1 + x^2), (1 + x^2)y, x(1 + x^2)y\}$, is a basis for $Z(\mathbb{F}_2D_8)$, the centre of \mathbb{F}_2D_8 .

Lemma 3.2.5. *Let I be the two-sided ideal generated by the element $1 + x^2$ of \mathbb{F}_2D_8 . Then $I = \Delta(D_8, \langle x^2 \rangle)$ and is a central nilpotent ideal of index 2 with the set $\{(1 + x^2), x(1 + x^2), y(1 + x^2), xy(1 + x^2)\}$ as a basis.*

Proof. $(1 + x^2)$ is central and so by Definition 3.1.1, $I = \Delta(D_8, \langle x^2 \rangle)$. $\mathcal{T} = \{1, x, y, xy\}$ is a complete set of representatives of left cosets of $\langle x^2 \rangle$ in D_8 . By Proposition 3.1.4, $\mathcal{B} = \{(1 + x^2), x(1 + x^2), (1 + x^2)y, x(1 + x^2)y\}$ is a basis for $\Delta(D_8, \langle x^2 \rangle)$. For any $b \in \mathcal{B}$, $b \in Z(\mathbb{F}_2D_8)$ such that $b^2 = 0$ and so $\Delta(D_8, \langle x^2 \rangle)$ is a central nilpotent ideal of index 2. □

Lemma 3.2.6. [38, pp.114] *Let G be a group and K a field.*

1. *If \mathbb{F} is an extension field of K , then $Z(\mathbb{F}G) \simeq \mathbb{F} \otimes_K Z(KG)$*
2. *If R is a subring of K and if M is a maximal ideal of R , then under the natural homomorphism $RG \rightarrow (R/M)G$ the centre $Z(RG)$ maps onto $Z((R/M)G)$.*

□

Definition 3.2.7. Let A be a subset of a ring R . The *centraliser* of A in R , denoted $C(A, R)$ is $\{r \in R \mid ra = ar, \forall a \in A\}$.

Remark 3.2.8. By letting $n = 4$ in Lemma 2.3.9 we get the following bases for $C(y, \mathbb{F}_2 D_8)$ and $C(xy, \mathbb{F}_2 D_8)$ respectively:

$$B_e(y) = \{1, x^2, y, x^2 y, (x + x^3), (x + x^3)y\} \quad (3.1)$$

$$B_e(xy) = \{1, x^2, xy, x^3 y, (x + x^3), (1 + x^2)y\}. \quad (3.2)$$

Remark 3.2.9. $B_e(y)$ contains units and so $\dim(C(y, \mathbb{F}_2 D_8) \cap \Delta(D_8)) \leq 5$. Let $B = \{1 + x^2, 1 + y, 1 + x^2 y, (x + x^3), (x + x^3)y\}$ and let $c_i \in \mathbb{F}_2$ for $i \in \{0, 1, 2, 3, 4\}$. Then

$$\begin{aligned} 0 &= c_0(1 + x^2) + c_1(1 + y) + c_2(1 + x^2 y) + c_3(x + x^3) + c_4(x + x^3)y \\ &= (c_0 + c_1 + c_2)1 + c_0 x^2 + c_1 y + c_2 x^2 y + c_3(x + x^3) + c_4(x + x^3)y. \end{aligned}$$

Thus $c_i = 0$, for $i \in \{0, 1, 2, 3, 4\}$ since $B_e(y)$ is a linearly independent set. Therefore B is also a linearly independent set. Each element of B commutes with y and has augmentation 0. Thus the \mathbb{F}_2 -span of B is a 5-dimensional subspace contained in $C(y, \mathbb{F}_2 D_8) \cap \Delta(D_8)$. Therefore B is a basis for $C(y, \mathbb{F}_2 D_8) \cap \Delta(D_8)$.

Likewise the set $\{1 + x^2, 1 + xy, 1 + x^3 y, (x + x^3), (1 + x^2)y\}$ is a basis for $C(xy, \mathbb{F}_2 D_8) \cap \Delta(D_8)$.

3.2.1 Derivations

Let x' and y' denote respectively the image of x and y under a given derivation. Letting $n = 4$ in Theorem 2.3.11 gives the following basis for $Der(\mathbb{F}_2 D_8)$ of size 12:

$$\mathcal{B} = \{d_{x', y'} \mid (x', y') \in \{(\lambda y, 0), (x\omega y, \omega) \mid \lambda \in B_e(xy), \omega \in B_e(y)\}\}, \quad (3.3)$$

Remark 3.2.10. Let $d \in Der(\mathbb{F}_2 D_8)$. Then d is a linear combination of elements

of \mathcal{B} in Equation (3.3). Therefore an element Λ of $C(xy, \mathbb{F}_2 D_8)$ and an element Ω of $C(y, \mathbb{F}_2 D_8)$ defines the derivation d by $d(x) = (\Lambda + x\Omega)y$ and $d(y) = \Omega$.

Remark 3.2.11. Write $x' = \sum_{i=0}^3 \sum_{j=0}^1 a_{i,j} x^i y^j$ and $y' = \sum_{i=0}^3 \sum_{j=0}^1 b_{i,j} x^i y^j$. Then by Equations (3.1) - (3.3):

1. $b_{1,0} = b_{3,0}$ and $b_{1,1} = b_{3,1}$
2. $a_{0,0} = a_{2,0}$ and $a_{3,1} = a_{1,1} + b_{0,0} + b_{2,0}$.

Remark 3.2.12. By Theorem 2.3.4, there are 2^{16} derivations of the commutative group algebra $\mathbb{F}_2(C_4 \times C_2)$, where C_n denotes the cyclic group of order n .

Lemma 3.2.13. *Let $D_8 = \langle x, y \mid y^2 = x^4 = (xy)^2 = 1 \rangle$ and let $d \in \text{Der}(\mathbb{F}_2 D_8)$. Write $x' = d(x) = a + by$ where $a, b \in \mathbb{F}_2 \langle x \rangle$. Then x' and x commute if and only if b is an element of the ideal $(1 + x^2)$ of $\mathbb{F}_2 \langle x \rangle$.*

Proof. Write $x' = d(x) = a + by$ where $a, b \in \mathbb{F}_2 \langle x \rangle$. Then

$$x'x + xx' = ax + byx + xa + xby = ax + ax + bx^3y + bxy = bx(1 + x^2)y.$$

Therefore, x' and x commute if and only if $b \in \text{Ann}(1 + x^2)$ in $\mathbb{F}_2 \langle x \rangle$. Considering the group algebra $\mathbb{F}_2 \langle x \rangle$, the ideal $(1 + x^2) \subset \text{Ann}(1 + x^2)$, since $1 + x^2$ is central and $(1 + x^2)^2 = 0$. Conversely, let $c = c_0 + c_1x + c_2x^2 + c_3x^3 \in \text{Ann}(1 + x^2)$. Then

$$0 = (1 + x^2)(c_0 + c_1x + c_2x^2 + c_3x^3) = (c_0 + c_2)(1 + x^2) + (c_1 + c_3)x(1 + x^2).$$

That is, $c_0 = c_2$ and $c_1 = c_3$ and so $c = (c_0 + c_1x)(1 + x^2)$. Therefore, $\text{Ann}(1 + x^2) \subset (1 + x^2)$ and so $\text{Ann}(1 + x^2) = (1 + x^2)$. Thus, x' and x commute if and only if b is in the ideal $(1 + x^2)$ of $\mathbb{F}_2 \langle x \rangle$. \square

The following basis for the vector space of inner derivations of \mathbb{F}_2D_8 is provided by letting $n = 4$ in Theorem 2.3.13:

$$\{d_b \mid b \in \{x, y, xy\}\}. \quad (3.4)$$

3.2.2 Conjugation by Units

Remark 3.2.14. [42, pp.71] Replacing the usual multiplication of an associative algebra A by the Lie commutator $[a_1, a_2]$ yields a nonassociative algebra which is a Lie algebra.

Definition 3.2.15. Let \mathfrak{D} denote the Lie algebra of \mathbb{F}_2D_8 formed by defining $[a, b] = ab - ba$, for all $a, b \in \mathbb{F}_2D_8$. Also, denote by $\mathfrak{D}' = [\mathbb{F}_2D_8, \mathbb{F}_2D_8]$ the set of all Lie commutators of elements of \mathbb{F}_2D_8 .

Remark 3.2.16. By Remark 3.2.3, group conjugation in D_8 either fixes an element of D_8 or it multiplies it by x^2 . For any $g, h \in D_8$, $[g, h] = gh + hg = h(g^h + g) = 0$ or $hg(1 + x^2)$. The Lie bracket is bilinear and so \mathfrak{D}' is contained in $(1 + x^2) = \Delta(D_8, \langle x^2 \rangle)$, which by Lemma 3.2.5 is a central nilpotent ideal of index 2.

We will now consider conjugation of an element of \mathbb{F}_2D_8 by units of \mathbb{F}_2D_8 .

Definition 3.2.17. Let u be a unit of a group algebra KG and a an element of KG . Then the *conjugation* of a by u , is the element $u^{-1}au$ and is denoted by a^u .

Lemma 3.2.18. a^2 is central for any element a of \mathbb{F}_2D_8 .

Proof. Write $a = \sum_{i=1}^8 a_i g_i$, where $a_i \in \mathbb{F}_2$ and $g_i \in D_8$. Then

$$a^2 = \left(\sum_{i=1}^8 a_i g_i \right) \left(\sum_{j=1}^8 a_j g_j \right) = \sum_{i,j=1}^8 a_i a_j g_i g_j = \sum_{i < j} a_i a_j (g_i g_j + g_j g_i) + \sum_{i=j} a_i^2 g_i^2.$$

These last 2 sums are central elements since

$$\sum_{i < j} a_i a_j (g_i g_j + g_j g_i) = \sum_{i < j} a_i a_j [g_i, g_j] \in \Delta(D_8, \langle x^2 \rangle) \subset Z(\mathbb{F}_2 D_8), \text{ by Remark 3.2.16}$$

$$\text{and } g_i^2 \in \{1, x^2\} \subset Z(\mathbb{F}_2 D_8).$$

Therefore, a^2 is the sum of 2 central elements and so is itself central. \square

Remark 3.2.19. The units of $\mathbb{F}_2 D_8$ are the elements of augmentation 1.

Lemma 3.2.20. *Let u be a unit of $\mathbb{F}_2 D_8$. Then $u^{-1} = u + z$ where $z \in \Delta(D_8, \langle x^2 \rangle)$.*

Proof. Write $u^{-1} = u + z$, for some $z \in \mathbb{F}_2 D_8$. Then $1 = u(u + z) = u^2 + uz$ and so $uz = u^2 + 1$. We know that u^2 is central by Lemma 3.2.18 and has augmentation 1. By Remark 3.2.4 the set $B_Z = \{1, x^2, x(1+x^2), (1+x^2)y, x(1+x^2)y\}$, is a basis for $Z(\mathbb{F}_2 D_8)$, the centre of $\mathbb{F}_2 D_8$. Therefore, by Lemma 3.2.5 we can write $u^2 = e + i$, where $e = 1$ or x^2 ($e \neq 1 + x^2$, since it has augmentation 1) and $i \in \Delta(D_8, \langle x^2 \rangle)$. This implies that $1 + u^2 = i$ or $(1 + x^2) + i$ and so $uz = 1 + u^2 \in \Delta(D_8, \langle x^2 \rangle)$. Thus, $z \in \Delta(D_8, \langle x^2 \rangle)$ since u is a unit. \square

Lemma 3.2.21. *Let u be a unit of $\mathbb{F}_2 D_8$ and $i \in \Delta(D_8, \langle x^2 \rangle)$. Then, $u + i$ is also a unit of $\mathbb{F}_2 D_8$ and $(u + i)^{-1} = u^{-1} + i$.*

Proof. Let $\epsilon: \mathbb{F}_2 D_8 \rightarrow \mathbb{F}_2$ be the augmentation map. Then $\epsilon(u + i) = \epsilon(u) + \epsilon(i) = 1 + 0 = 1$. Therefore $u + i$ is a unit. By Lemma 3.2.20, $u^{-1} = u + z$ for some $z \in \Delta(D_8, \langle x^2 \rangle)$ and so

$$(u + i)(u^{-1} + i) = uu^{-1} + ui + iu^{-1} + i^2 = 1 + ui + i(u + z) + 0 = 1 + [u, i] + iz.$$

However, $i = r(1 + x^2)$ for some $r \in \mathbb{F}_2 D_8$ (by Lemma 3.2.5) and so $[u, i] = (1 + x^2)[u, r] = 0$ by Remark 3.2.16. Also $iz = 0$, since $\Delta(D_8, \langle x^2 \rangle)^2 = 0$. Therefore $u^{-1} + i$ is the inverse of the unit $u + i$. \square

Lemma 3.2.22. *Let u be a unit of \mathbb{F}_2D_8 and $i \in \Delta(D_8, \langle x^2 \rangle)$. Then $a^{u+i} = a^u$, for all $a \in \mathbb{F}_2D_8$.*

Proof. Let g be an element of D_8 . Then,

$$g^{u+i} = (u+i)^{-1}g(u+i) = (u^{-1}+i)(gu+gi) = u^{-1}gu + u^{-1}gi + igu + igi.$$

Write $u^{-1} = u + z$, for some $z \in \Delta(D_8, \langle x^2 \rangle)$ and $i = r(1+x^2)$ for some $r \in \mathbb{F}_2D_8$.

$$u^{-1}gi + igu = ugi + zgi + igu = (1+x^2)(ugr + rgu)$$

since $zgi = 0$ as both z and i are in $\Delta(D_8, \langle x^2 \rangle)$. Write $r = r_c + r_n$, where r_c is the sum of elements in the support of r that commute with g and r_n is the sum of elements in the support of r that do not commute with g . Then

$$\begin{aligned} (1+x^2)(ugr + rgu) &= (1+x^2)(ugr_c + r_cgu) + (1+x^2)(ugr_n + r_ngu) \\ &= (1+x^2)(ugr_c + gr_cu) + (1+x^2)(ugr_n + x^2gr_nu) \\ &= (1+x^2)(ugr_c + gr_cu + ugr_n + gr_nu) \\ &= (1+x^2)([u, gr_c] + [u, gr_n]) = 0, \end{aligned}$$

by Remark 3.2.16. Moreover, $igi = 0$ as $\Delta(D_8, \langle x^2 \rangle)^2 = 0$. Therefore, $g^{u+i} = g^u$, for any $i \in \Delta(D_8, \langle x^2 \rangle)$.

Write $a = \sum_{j=1}^8 a_j g_j$, where $a_j \in \mathbb{F}_2$ and $g_j \in D_8$. Then

$$a^{u+i} = \sum_{j=1}^8 a_j g_j^{u+i} = \sum_{j=1}^8 a_j g_j^u = a^u.$$

□

Definition 3.2.23. Define

$$U/I = \{1, x, y, xy, 1+x+y, 1+x+xy, 1+y+xy, x+y+xy\}.$$

Then U/I is a set of representatives of the units of \mathbb{F}_2D_8 mod the ideal $I = \Delta(D_8, \langle x^2 \rangle)$, since $\mathbb{F}_2D_8/\Delta(D_8, \langle x^2 \rangle) \simeq \mathbb{F}_2(D_8/\langle x^2 \rangle)$ by Proposition 3.1.6.

Table 3.1 lists the image of the elements of D_8 under conjugation by the units of U/I . In the table ζ is the element $1+x^2$.

Remark 3.2.24. Table 3.1 combined with Lemma 3.2.22 gives all conjugates of elements of D_8 by units of \mathbb{F}_2D_8 . Partial sums of the entries in each row of Table 3.1 give all conjugates of elements of \mathbb{F}_2D_8 by units of \mathbb{F}_2D_8 . Therefore there are 8 inner automorphisms of \mathbb{F}_2D_8 . The exponent of the inner automorphism group of \mathbb{F}_2D_8 is 2. This has also been verified using GAP [18] and can also be calculated using Table 3.1. Therefore the inner automorphism group of \mathbb{F}_2D_8 is C_2^3 .

$g \in D_8$	1	x	x^2	x^3	y	xy	x^2y	x^3y
g^1	1	x	x^2	x^3	y	xy	x^2y	x^3y
g^x	1	x	x^2	x^3	x^2y	x^3y	y	xy
g^y	1	x^3	x^2	x	y	x^3y	x^2y	xy
g^{xy}	1	x^3	x^2	x	x^2y	xy	y	x^3y
g^{1+x+y}	1	$x^3 + \hat{xy}$	x^2	$x + \hat{xy}$	$x^2y + \zeta(x + xy)$	$xy + \zeta(x + y)$	$y + \zeta(x + xy)$	$x^3y + \zeta(x + y)$
g^{1+x+xy}	1	$x^3 + \hat{xy}$	x^2	$x + \hat{xy}$	$y + \zeta(x + xy)$	$x^3y + \zeta(x + y)$	$x^2y + \zeta(x + xy)$	$xy + \zeta(x + y)$
g^{1+y+xy}	1	$x + \hat{xy}$	x^2	$x^3 + \hat{xy}$	$x^2y + \zeta(x + xy)$	$x^3y + \zeta(x + y)$	$y + \zeta(x + xy)$	$xy + \zeta(x + y)$
g^{x+y+xy}	1	$x + \hat{xy}$	x^2	$x^3 + \hat{xy}$	$y + \zeta(x + xy)$	$xy + \zeta(x + y)$	$x^2y + \zeta(x + xy)$	$x^3y + \zeta(x + y)$

Table 3.1: The image of D_8 under conjugation by the units of \mathbb{F}_2D_8 , where $\zeta = 1 + x^2 \in \mathbb{F}_2D_8$.

Example 3.2.25 uses Table 3.1 to compute the conjugation of an element of \mathbb{F}_2D_8 by a unit of \mathbb{F}_2D_8 .

Example 3.2.25. let $a = 1 + x^2y + x^3y$, $v = x + x^2 + y$ and $u = 1 + x + y$ be elements of \mathbb{F}_2D_8 . Then $v = u + 1 + x^2$ and so by Lemma 3.2.22 $a^v = a^u$. Therefore using Table 3.1

$$\begin{aligned} a^v = a^u &= 1^u + (x^2y)^u + (x^3y)^u = 1 + y + (1 + x^2)(x + xy) + x^3y + (1 + x^2)(x + y) \\ &= 1 + y + x^3y + (1 + x^2)(y + xy) = 1 + xy + x^2y. \end{aligned}$$

Lemma 3.2.26. *Let z be a central element of a unital ring R and let $d \in \text{Der}(R)$. Then $d(z)$ is also be central in R .*

Proof. Let $a \in R$ and let z be any central element of R . Then

$$d(a)z + ad(z) = d(az) = d(za) = d(z)a + zd(a) = d(z)a + d(a)z.$$

Therefore, $d(a)z + ad(z) = d(z)a + d(a)z$ and subtracting $d(a)z$ from both sides gives $ad(z) = d(z)a$. □

3.2.3 The Ideals of \mathbb{F}_2D_8

Definition 3.2.27. Let RG be a group ring. Denote by \hat{G} the group ring element defined by $\hat{G} = \sum_{g \in G} g$.

Definition 3.2.28. Let S and T be sets of elements of the group ring RG . Define $(S, T) = \{(s, t) \mid s \in S \text{ and } t \in T\}$.

Definition 3.2.29. Let R be a finite ring. Then a *two sided ideal* I of R generated by the subset $A \subset R$ is the set all finite sums of the form ras , where $r, s, \in R$ and $a \in A$.

Remark 3.2.30. Let $\alpha \in \mathbb{F}_2\langle x \rangle$. Consider α as an element of \mathbb{F}_2D_8 . Then $\alpha \in \Delta(D_8, \langle x^2 \rangle)$ if and only if $\text{supp}(\alpha)$ contains an even number of both even and odd powers of x .

Definition 3.2.31. Define $b = 1 + (1 + x)(1 + y)$.

Lemma 3.2.32. *The set $\{1 + b, 1 + x^2, x(1 + x^2), y(1 + x^2), yx(1 + x^2)\}$ is a basis for the two-sided ideal $I = (1 + b) + \Delta(D_8, \langle x^2 \rangle)$ of \mathbb{F}_2D_8 .*

Proof. It is first shown that $(1 + g)(1 + b) \in \Delta(D_8, \langle x^2 \rangle)$ for all $g \in D_8$. Let $g = x^i$ for $i \in \{0, 1, 2, 3\}$. Then

$$(1 + g)(1 + b) = (1 + x^i)(1 + x)(1 + y) = (1 + x + x^i + x^{i+1})(1 + y) \in \Delta(D_8, \langle x^2 \rangle),$$

by Remark 3.2.30. Let $g = x^i y$ for $i \in \{0, 1, 2, 3\}$. Then

$$\begin{aligned} (1 + g)(1 + b) &= (1 + x^i y)(1 + x + y + xy) \\ &= 1 + x + y + xy + x^i y + x^{i-1} y + x^i + x^{i-1} \\ &= (1 + x + x^i + x^{i-1})(1 + y) \in \Delta(D_8, \langle x^2 \rangle), \text{ by Remark 3.2.30.} \end{aligned}$$

Therefore $(1 + g)(1 + b) \in \Delta(D_8, \langle x^2 \rangle)$, for all $g \in D_8$ and so $g(1 + b) = (1 + b) + z_1$, where $z_1 \in \Delta(D_8, \langle x^2 \rangle)$. Also, $(1 + b)(1 + g) = (1 + g)(1 + b) + [1 + b, 1 + g]$ and so $(1 + b)(1 + g) \in \Delta(D_8, \langle x^2 \rangle)$, by Remark 3.2.16. Thus $(1 + b)g = (1 + b) + z_2$, where $z_2 \in \Delta(D_8, \langle x^2 \rangle)$. By Lemma 3.2.5, the set $B = \{(1 + x^2), x(1 + x^2), y(1 + x^2), yx(1 + x^2)\}$ is a basis for $\Delta(D_8, \langle x^2 \rangle)$. Thus the principal ideal generated by $1 + b$ is contained in the \mathbb{F}_2 -linear span of $\{1 + b\} \cup B$. Therefore $\{1 + b\} \cup B$ is a basis for $I = (1 + b) + \Delta(D_8, \langle x^2 \rangle)$. \square

Remark 3.2.33. By Proposition 3.1.4, $B_1 = \{1 + x, 1 + x^2, 1 + x^3, 1 + y, 1 + xy, 1 + x^2y, 1 + x^3y\}$ is a basis for $\Delta(D_8)$. Let P be the invertible matrix shown in

Equation (3.5). Then multiplication by P^{-1} changes the basis for $\Delta(D_8)$ from B_1 to B_2 , where $B_2 = \{1 + xy, 1 + y, 1 + b, 1 + x^2, x(1 + x^2), y(1 + x^2), xy(1 + x^2)\}$.

$$P = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad P^{-1} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}. \quad (3.5)$$

Definition 3.2.34. The *classical involution* of KG , denoted by \otimes is a map from KG to KG defined by $(\sum_{g \in G} a_g g)^{\otimes} \mapsto \sum_{g \in G} a_g g^{-1}$.

Lemma 3.2.35. *The set $\{1 + y, 1 + b, (1 + x^2), x(1 + x^2), y(1 + x^2), xy(1 + x^2)\}$ is a basis for the two-sided ideal $I = (1 + y)$ of $\mathbb{F}_2 D_8$.*

Proof. $(1 + x)(1 + y) = 1 + b$ and $x^3(1 + y)xy + 1 + y = 1 + x^2$. Therefore the 5-dimensional ideal $(1 + b) + \Delta(D_8, \langle x^2 \rangle)$ is contained in the ideal $(1 + y)$. If $1 + y \in (1 + b) + \Delta(D_8, \langle x^2 \rangle)$, then $y = b + z$, where $z \in Z(\mathbb{F}_2 D_8)$. This is a contradiction since $y + b = x + xy \notin Z(\mathbb{F}_2 D_8)$ and so $1 + y \notin (1 + b) + \Delta(D_8, \langle x^2 \rangle)$. It is now shown that $1 + x \notin (1 + y)$ and so the dimension of $(1 + y)$ is 6.

Assume by way of contradiction that $1 + x \in (1 + y)$. Note that for $r_1, r_2 \in \mathbb{F}_2 \langle x \rangle$, $(r_1 + r_2 y)(1 + y) = (r_1 + r_2)(1 + y)$. Let $r, s, t \in \mathbb{F}_2 \langle x \rangle$. Then

$$r(1 + y)(s + ty) = r(s + ty + s^{\otimes} y + t^{\otimes}) = r(s + t^{\otimes}) + r(s^{\otimes} + t)y.$$

Therefore elements of the ideal $(1 + y)$ are sums of elements of the form $r(s + t^{\otimes}) +$

$r(s^{\otimes} + t)y$. Thus for some nonnegative integer n

$$\begin{aligned} 1 + x + 0y &= \sum_{i=0}^n r_i(s_i + t_i^{\otimes}) + \sum_{i=0}^n r_i(s_i^{\otimes} + t_i)y \\ &= \sum_{i=0}^n r_i(s_i + t_i^{\otimes} + s_i^{\otimes} + t_i), \text{ since } \sum_{i=0}^n r_i(s_i^{\otimes} + t_i) = 0. \end{aligned}$$

However, $\alpha + \alpha^{\otimes} \in \Delta(D_8, \langle x^2 \rangle)$ for all $\alpha \in \mathbb{F}_2 D_8$. Therefore $1 + x \in \Delta(D_8, \langle x^2 \rangle)$. This is a contradiction by Lemma 3.2.5 and so $1 + x \notin (1 + y)$.

By Remark 3.2.33, $\Delta(D_8)$ is a 7-dimensional ideal with basis $B_2 = \{1 + xy, 1 + y, 1 + b, 1 + x^2, x(1 + x^2), y(1 + x^2), xy(1 + x^2)\}$. Therefore $(1 + y)$ is a 6-dimensional ideal with basis $\{1 + y, 1 + b, 1 + x^2, x(1 + x^2), y(1 + x^2), xy(1 + x^2)\}$. \square

Remark 3.2.36. All Ideals of $\mathbb{F}_2 D_8$ are finitely generated.

Lemma 3.2.37. $\Delta(D_8, \langle x^2 \rangle)$ is a differential two-sided ideal of $\mathbb{F}_2 D_8$.

Proof. $\langle x^2 \rangle$ is a normal subgroup of D_8 and so $\Delta(D_8, \langle x^2 \rangle)$ is a two-sided ideal of $\mathbb{F}_2 D_8$ by Lemma 3.1.5. Let $d \in \text{Der}(\mathbb{F}_2 D_8)$. Then by Lemma 3.1.13, $\Delta(D_8, \langle x^2 \rangle) = (1 + x^2)$ is a differential ideal of $(\mathbb{F}_2 D_8, d)$ if and only if $d(1 + x^2) \in \Delta(D_8, \langle x^2 \rangle)$. However, $d(1 + x^2) = d(x^2) = [d(x), x] \in \Delta(D_8, \langle x^2 \rangle)$ by Remark 3.2.16. Therefore, $\Delta(D_8, \langle x^2 \rangle)$ is a differential ideal of $(\mathbb{F}_2 D_8, d)$ for all derivations d on $\mathbb{F}_2 D_8$. \square

Corollary 3.2.38. Let $d \in \text{Der}(\mathbb{F}_2 D_8)$ and let $I = \Delta(D_8, \langle x^2 \rangle)$. Define $\bar{d} : \mathbb{F}_2 D_8/I \rightarrow \mathbb{F}_2 D_8/I$ by $\bar{d}(a + I) = d(a) + I$. Then $\Phi : \text{Der}(\mathbb{F}_2 D_8) \rightarrow \text{Der}(\mathbb{F}_2 D_8/I)$ defined by $d \mapsto \bar{d}$ is a Lie algebra homomorphism.

Proof. I is a differential two-sided ideal of $\mathbb{F}_2 D_8$ by Lemma 3.2.37. The result now follows from Theorem 3.1.21. \square

Remark 3.2.39. Let $\Phi : \text{Der}(\mathbb{F}_2 D_8) \rightarrow \text{Der}(\mathbb{F}_2 D_8/I)$ be the map defined in Corollary 3.2.38. By Remark 3.2.10, $d \in \text{Der}(\mathbb{F}_2 D_8)$ is defined by an element $\Lambda \in C(xy, \mathbb{F}_2 D_8)$ and an element $\Omega \in C(y, \mathbb{F}_2 D_8)$. Thus by the Leibniz rule, $d(\mathbb{F}_2 D_8) \subset$

I if and only if $d(y) = \Omega \in I$ and $d(x) = (\Lambda + x\Omega)y \in I$. Therefore d is in the kernel of Φ if and only if $\Omega \in I$ and $\Lambda \in I$. By Lemma 3.2.5, I is a 4-dimensional ideal of \mathbb{F}_2D_8 . Therefore the kernel of Φ is an 8-dimensional vector space and so the image of Φ is a 4-dimensional vector space since by Theorem 2.3.11, $\dim(\text{Der}(\mathbb{F}_2D_8)) = 12$. By Proposition 3.1.6, $\mathbb{F}_2D_8/I \simeq \mathbb{F}_2(D_8/\langle x^2 \rangle) \simeq \mathbb{F}_2(C_2 \times C_2)$ and so $\text{Der}(\mathbb{F}_2D_8/I)$ is an 8-dimensional vector space by Theorem 2.3.4. Therefore Φ is not onto.

Lemma 3.2.40. *Let I be the two-sided ideal of \mathbb{F}_2D_8 generated by the element $1 + y$. Then I is a differential ideal of (\mathbb{F}_2D_8, d) if and only if $d(y) \in I$. Also, there are 2^{11} derivations d of \mathbb{F}_2D_8 such that I is a differential ideal of (\mathbb{F}_2D_8, d) .*

Proof. Let d be the derivation of \mathbb{F}_2D_8 defined by $\Lambda \in C(xy, \mathbb{F}_2D_8)$ and $\Omega \in C(y, \mathbb{F}_2D_8)$. By Lemma 3.1.13, I is a differential ideal of (\mathbb{F}_2D_8, d) if and only if $d(1 + y) = d(y) = \Omega \in I$ and so $\Omega \in I \cap C(y, \mathbb{F}_2D_8)$.

By Remark 3.2.8, $B_e(y) = \{1, x^2, y, x^2y, (x + x^3), (x + x^3)y\}$ is a basis for $C(y, \mathbb{F}_2D_8)$. The set $\mathcal{B} = \{1, 1 + x^2, 1 + y, 1 + x^2y, (x + x^3), (x + x^3)y\}$ is also a basis for $C(y, \mathbb{F}_2D_8)$, since $\text{span}(\mathcal{B}) = \text{span}(B_e(y))$ and \mathcal{B} also has size 6. $1 \notin I$ but the other elements of \mathcal{B} are in I by Lemma 3.2.35 and so $C(y, \mathbb{F}_2D_8) \cap I$ is a 5-dimensional subspace of \mathbb{F}_2D_8 .

Therefore Λ can be any element of $C(xy, \mathbb{F}_2D_8)$, which by Remark 3.2.8 is a 6-dimensional subspace of \mathbb{F}_2D_8 . Also, Ω can be any element of $C(y, \mathbb{F}_2D_8) \cap I$ which is a 5-dimensional subspace of \mathbb{F}_2D_8 . Thus there are 2^{11} derivations of \mathbb{F}_2D_8 that correspond to I being a differential ideal. \square

Remark 3.2.41. By Proposition 3.1.4, the set $\{1 + x, 1 + x^2, 1 + x^3, y(1 + x), y(1 + x^2), y(1 + x^3)\}$ is a basis for the ideal $\Delta(D_8, \langle x \rangle)$. Let $r \in \mathbb{F}_2\langle x \rangle$. Then $(1 + x)ry = ry + ryx^3 = ry(1 + x^3)$ and so $\Delta(D_8, \langle x \rangle)$ is in fact a two-sided ideal of \mathbb{F}_2D_8 of dimension 6.

Lemma 3.2.42. *There are 2^{10} derivations d of \mathbb{F}_2D_8 such that $(1+x)$ is a differential ideal of (\mathbb{F}_2D_8, d) .*

Proof. Let d be the derivation of \mathbb{F}_2D_8 defined by $\Lambda \in C(xy, \mathbb{F}_2D_8)$ and $\Omega \in C(y, \mathbb{F}_2D_8)$. Let $I = (1+x)$. Then by Lemma 3.1.13, $d(I) \subset I$ if and only if $d(1+x) = d(x) = (\Lambda + x\Omega)y \in I$.

Assume that I is a differential ideal with respect to d and so $(\Lambda + x\Omega) \in I$. $\Omega \in C(y, \mathbb{F}_2D_8)$ and so by Remark 3.2.8, $x\Omega = w_0x + w_1x^3 + w_2xy + w_3x^3y + w_4(1+x^2) + w_5(1+x^2)y$, for some $w_i \in \mathbb{F}_2$. Let $\rho = w_0 + w_1(1+x+x^3) + w_2xy + w_3x^3y$. By Remark 3.2.8, the set $B_e(xy) = \{1, x^2, xy, x^3y, (x+x^3), (1+x^2)y\}$ is a basis for $C(xy, \mathbb{F}_2D_8)$. Therefore $\rho \in C(xy, \mathbb{F}_2D_8)$. Also, $\rho + x\Omega = (w_0 + w_1)(1+x) + w_4(1+x^2) + w_5(1+x^2)y$ and so is an element of I . Let $z = \Lambda + \rho$. Then $(\Lambda + x\Omega) = (z + \rho + x\Omega) \in I$ and so $z \in C(xy, \mathbb{F}_2D_8) \cap I$. Therefore for any element Ω of $C(y, \mathbb{F}_2D_8)$, $\Lambda = \rho + z$, where $z \in C(xy, \mathbb{F}_2D_8) \cap I$.

It is now shown that $C(xy, \mathbb{F}_2D_8) \cap I = \Delta(D_8, \langle x^2 \rangle)$. By Remark 3.2.9, $\{1+x^2, 1+xy, 1+x^3y, (x+x^3), (1+x^2)y\}$ is a basis for $C(xy, \mathbb{F}_2D_8) \cap \Delta(D_8)$. Assume by way of contradiction that $1+xy \in I$. Then $1+x+(1+xy)x = 1+y \in I$ and so $(1+y) \subset I$. Appending $1+xy$ to the basis given in Lemma 3.2.35 for $(1+y)$ gives the basis B_2 given for $\Delta(D_8)$ in Remark 3.2.33. Therefore $I = \Delta(D_8)$ and so by Remark 3.2.41, $6 = \dim(I) = \dim(\Delta(D_8)) = 7$, a contradiction. Therefore $1+xy \notin I$ and so the dimension of $C(xy, \mathbb{F}_2D_8) \cap I$ is less than 5 and so $C(xy, \mathbb{F}_2D_8) \cap I = \Delta(D_8, \langle x^2 \rangle)$.

Let Ω be any element of the 6-dimensional subspace $C(y, \mathbb{F}_2D_8)$ and let z be any element of the 4-dimensional subspace $\Delta(D_8, \langle x^2 \rangle)$. Then $\Lambda = \rho + z \in C(xy, \mathbb{F}_2D_8)$ and $\Lambda + x\Omega = z + \rho + x\Omega \in I$, since both z and $\rho + x\Omega$ are in I . Therefore there are 2^{10} derivations of \mathbb{F}_2D_8 such that I is a differential ideal. \square

Lemma 3.2.43. *There are 2^{10} derivations d of \mathbb{F}_2D_8 for which the augmentation*

ideal $\Delta(D_8)$ is a differential ideal of (\mathbb{F}_2D_8, d) .

Proof. Let d be the derivation of \mathbb{F}_2D_8 defined by $\Lambda \in C(xy, \mathbb{F}_2D_8)$ and $\Omega \in C(y, \mathbb{F}_2D_8)$. The augmentation map is a ring homomorphism and so $\Delta(D_8)$ is a differential ideal with respect to d if and only if $d(x)$ and $d(y)$ are both in $\Delta(D_8)$. However, $d(x) = (\Lambda + x\Omega)y$ and $d(y) = \Omega$ are both in $\Delta(D_8)$ if and only if Λ and Ω are both in $\Delta(D_8)$. By Remark 3.2.9, $C(xy, \mathbb{F}_2D_8) \cap \Delta(D_8)$ and $C(y, \mathbb{F}_2D_8) \cap \Delta(D_8)$ are both 5-dimensional subspaces of \mathbb{F}_2D_8 . Therefore there are 2^{10} derivations of \mathbb{F}_2D_8 such that $\Delta(D_8)$ is a differential ideal. \square

Figure 3.1 shows the lattice of all two-sided ideals of \mathbb{F}_2D_8 . The inclusions were computed in GAP [18].

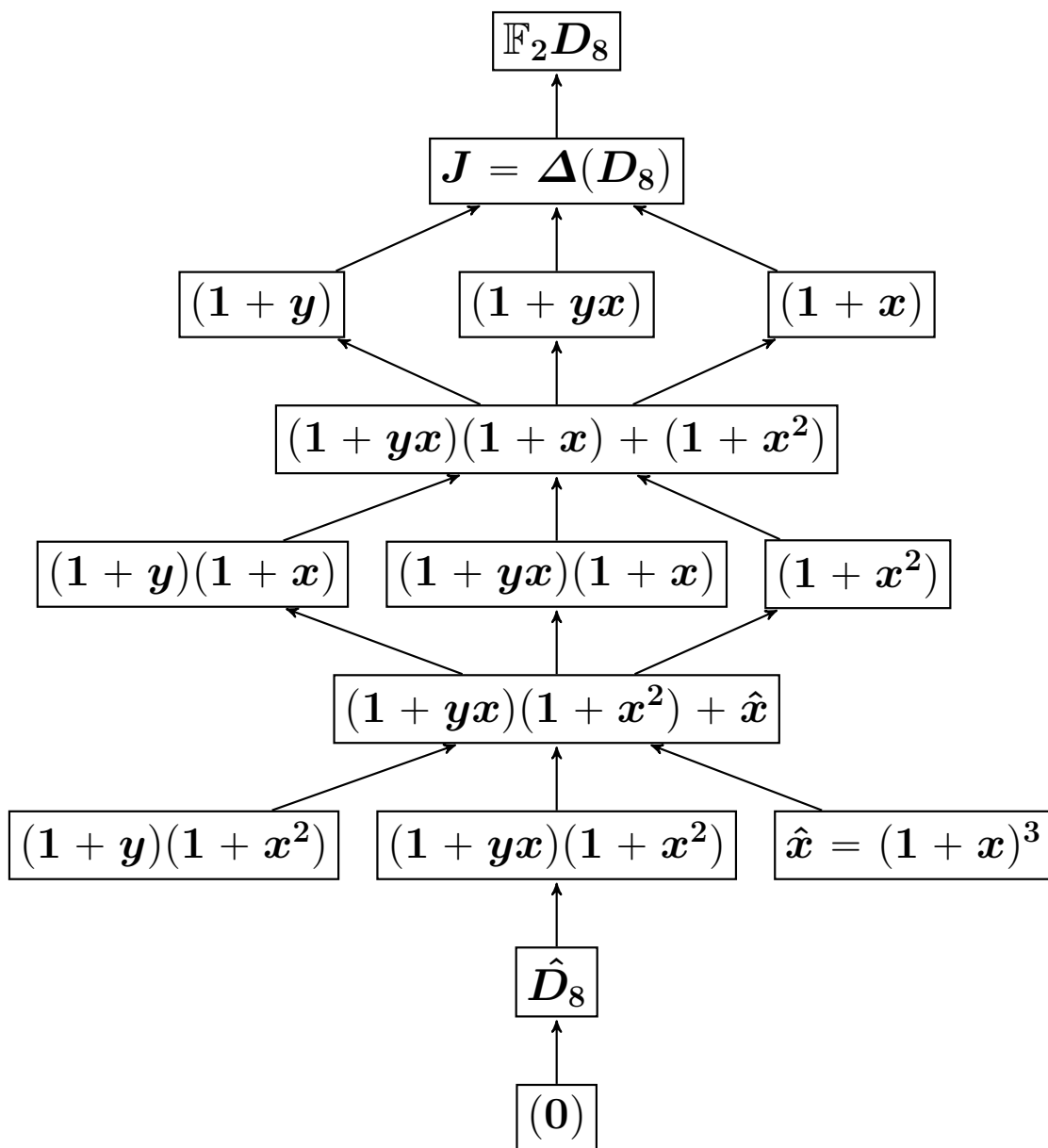


Figure 3.1: The lattice of two-sided ideals of $\mathbb{F}_2 D_8$

3.2.4 The Unit Group of \mathbb{F}_2D_8

Definition 3.2.44. An ideal I of a ring is a *nil ideal* if each of its elements is nilpotent, i.e. for all $a \in I$, $a^n = 0$ for some natural number n .

Definition 3.2.45. An ideal I of a ring is a *nilpotent ideal* if there exists a natural number n such that $I^n = (0)$.

Theorem 3.2.46. [40, pp. 110] *Let R be an Artinian ring. Then the Jacobson radical J is a nilpotent ideal of R and every nil ideal is nilpotent.*

Lemma 3.2.47. *Let I be a proper ideal of \mathbb{F}_2D_8 . Then $1 + I$ is a normal subgroup of the unit group of \mathbb{F}_2D_8 .*

Proof. The units of \mathbb{F}_2D_8 are the elements of augmentation 1 and so $\mathcal{U}(\mathbb{F}_2D_8) = 1 + \Delta(D_8)$. Therefore $\Delta(D_8)$ is the unique maximal ideal of \mathbb{F}_2D_8 and so $J = \Delta(D_8)$. By Theorem 3.2.46, J is nilpotent. Let n be the index of nilpotency of J . Then $I^n = 0$ for all proper ideals I of \mathbb{F}_2D_8 , since $I \subset J$.

Let a and b be elements of the ideal I . Then $(1+a)(1+b) = 1+a+b+ab \in 1+I$. Therefore $1+I$ is closed under multiplication. The inverse of the unit $1+b$ is given by $(1+b)^{-1} = \sum_{m=0}^{n-1} b^m \in 1+I$ since

$$\left(\sum_{m=0}^{n-1} b^m \right) (1+b) = (1+b) \left(\sum_{m=0}^{n-1} b^m \right) = 1 + b^n = 1.$$

Therefore $1+I$ is closed under inversion and so $1+I$ is a subgroup of $\mathcal{U}(\mathbb{F}_2D_8)$. Also, $1+I$ is a normal subgroup since for all $i \in I$ and $j \in J$

$$\begin{aligned} (1+j)(1+i)(1+j)^{-1} &= (1+j)(1+j)^{-1} + (1+j)(i)(1+j)^{-1} \\ &= 1 + (1+j)(i)(1+j)^{-1} \in 1+I. \end{aligned}$$

□

Lemma 3.2.48. Let $D_8 = \langle x, y \mid x^4 = y^2 = (xy)^2 = 1 \rangle$ and $b = 1 + (1+x)(1+y)$.

The following is a presentation of the unit group of $\mathbb{F}_2 D_8$, denoted by $\mathcal{U}(\mathbb{F}_2 D_8)$:

$$\begin{aligned} \mathcal{U}(\mathbb{F}_2 D_8) &= \left(\left((\langle b \rangle \times \langle bb^y \rangle) \rtimes \langle y \rangle \right) \times \langle x^2 \rangle \times \langle x^2 + \hat{x} \rangle \right) \rtimes \langle xy \rangle \\ &\simeq \left(\left((C_4 \times C_2) \rtimes C_2 \right) \times C_2 \times C_2 \right) \rtimes C_2, \end{aligned}$$

where the actions of the semidirect products are:

$$\begin{aligned} b^y &= (b^3)(bb^y), & (bb^y)^y &= bb^y, & b^{xy} &= (b)(bb^y)(x^2)(x^2 + \hat{x}), \\ (bb^y)^{xy} &= bb^y, & y^{xy} &= yx^2, & (x^2)^{xy} &= x^2, & (x^2 + \hat{x})^{xy} &= x^2 + \hat{x}. \end{aligned}$$

Proof. Let $\zeta = 1 + x^2$. By Lemma 3.2.47, $1 + (\zeta)$ is a normal subgroup of $\mathcal{U}(\mathbb{F}_2 D_8)$. By Lemma 3.2.5, $\Delta(D_8, \langle x^2 \rangle) = (\zeta)$ and is a central nilpotent ideal of index 2 with the set $S = \{\zeta, x\zeta, y\zeta, xy\zeta\}$ as a basis. Let $r, t \in \Delta(D_8, \langle x^2 \rangle)$. Then $(1+r)(1+t) = 1+r+t$ and so the set $1+S = \{1+s \mid s \in S\}$ generates $1+(\zeta)$. Also, $1+(\zeta)$ is an elementary abelian 2-group and so $1+(\zeta) \simeq C_2^4$.

Let $I = (1+b) + \Delta(D_8, \langle x^2 \rangle)$. By Lemma 3.2.32, the set $\{1+b, \zeta, x\zeta, y\zeta, xy\zeta\}$ is a basis for the 5-dimensional ideal I and by Lemma 3.2.35 $y \notin 1+I$. By Lemma 3.2.47, $1+I$ is a normal subgroup of $\mathcal{U}(\mathbb{F}_2 D_8)$ of order 2^5 . $b \in 1+I$ and $b \notin 1+(\zeta)$, which is a normal subgroup of $1+I$ of order 2^4 and so $1+I$ is generated by $\{b, 1+\zeta, 1+x\zeta, 1+y\zeta, 1+xy\zeta\}$. It is an abelian group as $\Delta(D_8, \langle x^2 \rangle)$ is central. Also

$$b^2 = (x+y+xy)(x+y+xy) = 1 + \hat{D}_8 = (1+\zeta)(1+x\zeta)(1+y\zeta)(1+xy\zeta).$$

The order of b is 4 since $b^3 = b + \hat{D}_8$ and $b^4 = b^2 + \hat{D}_8 = 1$. $by = (x+y+xy)y =$

$1 + x + xy$ and so

$$\begin{aligned}
bb^y &= (by)^2 = (1 + x + xy)(1 + x + xy) \\
&= 1 + x + xy + x + x^2 + x^2y + xy + y + 1 = x^2 + x^2y + y \\
&= 1 + \zeta + y\zeta = (1 + \zeta)(1 + y\zeta) \in Z(\mathbb{F}_2D_8).
\end{aligned}$$

Therefore $1 + I = \langle b \rangle \times \langle bb^y \rangle \times \langle 1 + \zeta \rangle \times \langle 1 + x\zeta \rangle \simeq C_4 \times C_2^3$.

By Lemma 3.2.35, the set $\{1 + y, 1 + b, \zeta, x\zeta, y\zeta, xy\zeta\}$ is a basis for the ideal $(1 + y)$. Therefore $1 + (1 + y)$ is a normal subgroup of $\mathcal{U}(\mathbb{F}_2D_8)$ of order 2^6 generated by the set $\{y, b, 1 + \zeta, 1 + x\zeta, 1 + y\zeta, 1 + xy\zeta\}$. $1 + (1 + y)$ is the product of the normal subgroup $1 + I$ and $\langle y \rangle$. y does not commute with b and $1 + I$ and $\langle y \rangle$ have trivial intersection. Thus $1 + (1 + y) = 1 + I \rtimes \langle y \rangle$. Also, $b^y = (b^3)(bb^y)$. $bb^y, 1 + \zeta$ and $1 + x\zeta$ are central and so

$$\begin{aligned}
1 + (1 + y) &= (\langle b \rangle \times \langle bb^y \rangle \times \langle 1 + \zeta \rangle \times \langle 1 + x\zeta \rangle) \rtimes \langle y \rangle \\
&= \left((\langle b \rangle \times \langle bb^y \rangle) \rtimes \langle y \rangle \right) \times \langle 1 + \zeta \rangle \times \langle 1 + x\zeta \rangle.
\end{aligned}$$

By Remark 3.2.33, the set $\{1 + xy, 1 + y, 1 + b, \zeta, x\zeta, y\zeta, xy\zeta\}$ is a basis for $\Delta(D_8)$. $1 + (1 + y)$ and $\langle xy \rangle$ have trivial intersection. Therefore $\mathcal{U}(\mathbb{F}_2D_8)$ is a group of order 2^7 generated by the set $\{xy, y, b, 1 + \zeta, 1 + x\zeta, 1 + y\zeta, 1 + xy\zeta\}$. Thus $\mathcal{U}(\mathbb{F}_2D_8)$ is the product of the normal subgroup $1 + (1 + y)$ and $\langle xy \rangle$.

$$\begin{aligned}
\mathcal{U}(\mathbb{F}_2D_8) &= \left(\left((\langle b \rangle \times \langle bb^y \rangle) \rtimes \langle y \rangle \right) \times \langle 1 + \zeta \rangle \times \langle 1 + x\zeta \rangle \right) \rtimes \langle xy \rangle \\
&\simeq \left(\left((C_4 \times C_2) \rtimes C_2 \right) \times C_2 \times C_2 \right) \rtimes C_2.
\end{aligned}$$

By Table 3.1, $b^{xy} = x^3 + xy + x^2y$. Also $(b)(bb^y)(1 + \zeta)(1 + x\zeta) = (1 + \hat{D}_8)b^y(1 + \hat{x}) = b^y(1 + \hat{x} + \hat{D}_8) = b^y(1 + \hat{x}y) = (x^3 + y + x^3y)(1 + \hat{x}y) = x^3 + \hat{x}y + y + \hat{x} + x^3y + \hat{x} = x^3 + xy + x^2y$. Therefore, $b^{xy} = (b)(bb^y)(1 + \zeta)(1 + x\zeta)$. Also $y^{xy} = xy^2xy = y(1 + \zeta)$

and $bb^y, 1 + \zeta$ and $1 + x\zeta$ are central and so commute with xy . \square

Remark 3.2.49. The structure of the unit group of the group algebra $\mathbb{F}_{2^k}D_8$ was found in [13].

3.3 Do Outer Derivations Become Inner?

In Theorem 2.3.15 it was shown that there exists an algebra $A \supset KG$ such that all derivations of KG become inner in A . In this section we show that derivations of KH do not become inner on KG , where H is a subgroup of G .

Let d be a derivation of A that is not inner. Does there exist an algebra $B \supset A$ such that the derivation d becomes inner when extended to B ? That is, does there exist an element b of B such that $d_b = d$ on A ? A necessary condition on d_b is that $d_b(A) \subset A$.

Lemma 3.3.1. *Let R be a commutative ring. Then a derivation of R is inner if and only if it is the zero map.*

Proof. let $a \in R$ and let d be an inner derivation of R . Then $d(a) = ba - ab = 0$, for some $b \in R$. If d is the zero map then $d(a) = 0a - a0$. \square

Definition 3.3.2. A derivation of a ring is called *outer* if it is not an inner derivation.

Theorem 3.3.3. *Let H be a subgroup of the group G and let R be a unital ring. Then there are no outer R -derivations of RH that become inner on RG .*

Proof. Let $g \in G$ and $h \in H$. Then $gh \in H \iff g \in H$ and $hg \in H \iff g \in H$. Therefore $[g, h] = gh - hg \in RH \iff [g, h] = 0$ or $g \in H$. Let $G_h = \{g \in G \mid [g, h] \in RH\} = H \cup \{g \in G \mid [g, h] = 0\}$.

Let $b \in RG$ and write $b = \sum_{g \in G} b_g g$. Assume that the restriction of d_b to RH is an R -derivation of RH . Then $d_b(RH)$ is contained in RH and so for any $h \in H$, $[b, h] = \sum_{g \in G_h} b_g [g, h] + \sum_{g \notin G_h} b_g [g, h] \in RH$. $\sum_{g \in G_h} b_g [g, h] \in RH$ and so $\sum_{g \notin G_h} b_g [g, h] \in RH$. However $\sum_{g \notin G_h} b_g [g, h]$ is an R -linear combination of elements of G that are not in H and so $\sum_{g \notin G_h} b_g [g, h] = 0$. Therefore

$$[b, h] = \sum_{g \in G_h} b_g [g, h] = \sum_{g \in H} b_g [g, h] = \left[\sum_{g \in H} b_g g, h \right] = [\beta, h],$$

where $\beta = \sum_{h \in H} b_h h \in RH$. By assumption the restriction of d_b to RH is an R -derivation of RH . Therefore for any $r \in R$ and $h \in H$

$$brh - rhb = [b, rh] = d_b(rh) = rd_b(h) = r[b, h] = rbh - rhb.$$

Thus $br = rb$ and so $\sum_{g \in G} b_g r g = br = rb = \sum_{g \in G} r b_g g$. Therefore b_g commutes with r for all $g \in G$ and so in particular b_g commutes with r for all $g \in H$ which implies that $\beta r = r \beta$ for all $r \in R$. Therefore d_β is an R -derivation of RH .

Let $a \in RH$ and write $a = \sum_{h \in H} a_h h$. Then

$$d_b(a) = d_b\left(\sum_{h \in H} a_h h\right) = \sum_{h \in H} a_h d_b(h) = \sum_{h \in H} a_h d_\beta(h) = d_\beta\left(\sum_{h \in H} a_h h\right) = d_\beta(a).$$

Therefore the restriction of d_b to RH is an inner derivation of RH and so no outer R -derivations of RH become inner on RG . \square

The following lemma and example show that although R -derivations of group rings do not become inner on larger group rings, derivation of ideals of group rings can become inner on the group ring.

Lemma 3.3.4. *Let $L = (1 + y)$ be the two-sided ideal of $\mathbb{F}_2 D_8$ generated by the*

element $1 + y$. Let $b \in \mathbb{F}_2 D_8$. Then the restriction of d_b to L denoted $d_b|_L$ is not inner on L if and only if $x \in \text{supp}(b)$.

Proof. Let $I = (1 + x^2)$ be the two-sided ideal of $\mathbb{F}_2 D_8$ generated by the element $1 + x^2$. By Lemma 3.2.5, I is a central nilpotent ideal of index 2 with the following set as a basis: $B_I = \{(1 + x^2), x(1 + x^2), y(1 + x^2), yx(1 + x^2)\}$. Let $B_L = B_I \cup \{(1 + y), (1 + y)x\}$. Then by Lemma 3.2.35, B_L is a basis for $L \supset I$. $L = I \oplus \mathbb{F}_2(1 + y) \oplus \mathbb{F}_2(1 + y)x$ and note that $[(1 + y), (1 + y)x] = (1 + y)(1 + y)x + (1 + y)x(1 + y) = 0 + (1 + y)(x + yx^3) = x + x^3 + yx + yx^3$ and so

$$\begin{aligned} [L, L] &= [I \oplus \mathbb{F}_2(1 + y) \oplus \mathbb{F}_2(1 + y)x, I \oplus \mathbb{F}_2(1 + y) \oplus \mathbb{F}_2(1 + y)x] \\ &= [\mathbb{F}_2(1 + y) \oplus \mathbb{F}_2(1 + y)x, \mathbb{F}_2(1 + y) \oplus \mathbb{F}_2(1 + y)x] \\ &= \{0\} \cup \{[1 + y, (1 + y)x]\} \cup \{[1 + y, (1 + y)x]\} = \{0, x + x^3 + yx + yx^3\}. \end{aligned}$$

Let $a \in L$ and $b \in \mathbb{F}_2 D_8$. Then $d_b(a) \in L$ since L is a two-sided ideal of $\mathbb{F}_2 D_8$ and so $d_b|_L$ is a derivation of L . B_L can be extended to a basis for $\mathbb{F}_2 D_8$ by appending the elements 1 and x . Write $b = b_0 1 + b_1 x + b_2 l$ for some $l \in L$ and $b_0, b_1, b_2 \in \mathbb{F}_2$ and $a = a_0(1 + y) + a_1(1 + y)x + a_2(z)$ where $z \in I$ and $a_0, a_1, a_2 \in \mathbb{F}_2$. Then

$$d_b(a) = [b_0 1 + b_1 x + b_2 l, a] = [b_0 1, a] + [b_1 x, a] + [b_2 l, a] = [b_1 x, a] + [b_2 l, a],$$

where $[b_2 l, a] \in [L, L]$. Also if $a \notin I$ then

$$\begin{aligned} [x, a] &= [x, a_0(1 + y)] + [x, a_1(1 + y)x] + [x, a_2 z] \\ &= a_0 x(1 + y) + a_0(1 + y)x + a_1 x(1 + y)x + a_1(1 + y)x^2 \\ &= a_0 yx(1 + x^2) + a_1 y(1 + x^2) \notin [L, L]. \end{aligned}$$

Therefore if $x \in \text{supp}(b)$ and $a \notin I$ then $d_b(a) \notin [L, L]$ and so d_b is not inner on L .

Conversely, if $x \notin \text{supp}(b)$ then $b_1 = 0$ and so $d_b = d_{b_0 1 + b_2 l} = d_{b_2 l}$, which is an inner derivation of L . \square

Example 3.3.5. Let $L = (1 + y)$ be the two-sided ideal of $\mathbb{F}_2 D_8$ generated by the element $1 + y$. The map $d_x: \mathbb{F}_2 D_8 \rightarrow \mathbb{F}_2 D_8$, defined by $c \mapsto xc - cx$ for all $c \in \mathbb{F}_2 D_8$ is an inner derivation of $\mathbb{F}_2 D_8$. Also for all $l \in L$, $d_x(l) = xl + lx \in L$ since L is a two-sided ideal and so the map $d_x \upharpoonright_L$ is a derivation of L . However, $d_x \upharpoonright_L$ is not inner as $d_x(1 + y) = d_x(y) = yx(1 + x^2) \notin [L, L] = \{0, x + x^3 + yx + yx^3\}$. Therefore $d_x \upharpoonright_L$ is a non-inner derivation of $L = (1 + y)$ that becomes inner on $\mathbb{F}_2 D_8$.

This example raises an interesting question: If I is a proper ideal of KG , does every derivation of I become inner on KG ?

3.4 Some Linear Algebra Results

This section contains known results from linear algebra and is included for later reference. It may be skipped if desired by the reader.

A derivation of a group algebra is a linear transformation, by Corollary 3.5.1. We wish to study the structure of these derivations and so we will employ some theorems from linear algebra to better understand how these derivations transform a group algebra. This section contains the main results used namely the primary decomposition theorem and the cyclic decomposition theorem. Both of these theorems allow us to decompose the group algebra, considered as a vector space, into a direct sum of derivation-invariant subspaces. These decompositions can be used to write the matrix representing the derivation in rational canonical form. Moreover, if the eigenvalues all lie in the field, then a Jordan form can also be achieved. In the case where the matrix cannot be written in Jordan form, it is still possible to write it in generalised Jordan form. We begin with some definitions and preliminary

results. Throughout this section we let T be a linear transformation on a vector space V .

Theorem 3.4.1. [52, pp. 17] *Let V be a finite-dimensional vector space and let $T: V \rightarrow W$ be a linear transformation. Then $\dim(\ker(T)) + \dim(\text{Im}(T)) = \dim(V)$.*

Definition 3.4.2. [52, pp. 111] The *T -annihilator* of a vector $v \in V$ denoted $m_{T,v}(x)$ is the unique monic polynomial of least degree such that $m_{T,v}(T)(v) = 0$.

Definition 3.4.3. [52, pp. 112] The *minimum polynomial* of T denoted $m_T(x)$ is the unique monic polynomial of least degree such that $m_T(T)(v) = 0$ for all $v \in V$.

Lemma 3.4.4. [52, pp. 112] *Let V be a vector space and let $T: V \rightarrow V$ be a linear transformation. Let $v_1, \dots, v_k \in V$ with T -annihilators $p_i(x) = m_{T,v_i}(x)$ for $i = 1, \dots, k$ and suppose that $p_1(x), \dots, p_k(x)$ are pairwise relatively prime. Then $v = v_1 + \dots + v_k$ has T -annihilator polynomial $m_{T,v}(x) = p_1(x) \dots p_k(x)$.*

Theorem 3.4.5. [52, pp. 113] *Let V be a finite-dimensional vector space and let $T: V \rightarrow V$ be a linear transformation. Then there is a vector $v \in V$ such that the T -annihilator $m_{T,v}(x)$ of v is equal to the minimum polynomial $m_T(x)$ of T .*

Definition 3.4.6. [52, pp. 114] Let A be a square matrix. The *characteristic polynomial* $c_A(x)$ of A is the polynomial $c_A(x) = \det(xI - A)$. Let V be a finite-dimensional vector space and let $T: V \rightarrow V$ be a linear transformation. Furthermore, let \mathcal{B} be any basis of V and let A be the matrix of T with respect to the basis \mathcal{B} , that is, $A = [T]_{\mathcal{B}}$. Then the *characteristic polynomial* $c_T(x)$ is the polynomial $c_T(x) = \det(xI - A)$.

Definition 3.4.7. [52, pp. 115] Let $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ be a monic polynomial in $\mathbb{F}[x]$ of degree $n \geq 1$. The *companion matrix* $C(f(x))$ of $f(x)$ is the

$n \times n$ matrix

$$C(f(x)) = \begin{bmatrix} -a_{n-1} & 1 & 0 & \dots & 0 \\ -a_{n-2} & 0 & 1 & \dots & 0 \\ & & \vdots & \ddots & \\ -a_1 & 0 & 0 & \dots & 1 \\ -a_0 & 0 & 0 & \dots & 0 \end{bmatrix}.$$

Theorem 3.4.8. [52, pp. 115] Let $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ be a monic polynomial and let $A = C(f(x))$ be its companion matrix. Let $V = \mathbb{F}^n$ for any field \mathbb{F} and let $T = T_A: V \rightarrow V$ be the linear transformation $T(v) = Av$. Let $v = [0 \ 0 \ \dots \ 0 \ 1]^T$ be the n^{th} standard basis vector. Then the subspace W of V defined by $W = \{g(T)(v) \mid g(x) \in \mathbb{F}[x]\}$ is V . Furthermore, $m_T(x) = m_{T,v}(x) = f(x)$.

Remark 3.4.9. [52, pp. 116] The characteristic polynomial of the companion matrix of a monic polynomial $f(x)$ is equal to $f(x)$. That is, $c_{C(f(x))}(x) = f(x)$.

Definition 3.4.10. [52, pp. 117] Let $T: V \rightarrow V$ be a linear transformation. A subspace W of V is *T-invariant* if $T(W) \subset W$, i.e., if $T(w) \in W$ for every $w \in W$.

Remark 3.4.11. The restriction of a linear transformation T to a T -invariant subspace W of V is a linear transformation, denoted $T \upharpoonright_W$.

Definition 3.4.12. [52, pp. 117] Let $T: V \rightarrow V$ be a linear transformation. Let $\mathcal{B} = \{v_1, \dots, v_k\}$ be a set of vectors in V . The *T-span* of \mathcal{B} is the subspace

$$W = \left\{ \sum_{i=1}^k p_i(T)(v_i) \mid p_i(x) \in \mathbb{F}[x] \right\}.$$

In this situation \mathcal{B} is said to *T-generate* W .

The image (range) of a linear transformation, denoted $Im(T)$ is a T -invariant subspace of V . Let $v \in Im(T)$. Then $v = Tw$ for some $w \in V$ and so $Tv = T(Tw) \in$

$Im(T)$. In fact, for each $k \in \mathbb{N}$ we have that $T^k(V)$ is a T -invariant subspace of V . This gives us a non-ascending sequence of T -invariant subspaces:

$$V \supset T(V) \supset T^2(V) \supset \dots$$

Since V is finite-dimensional this sequence must eventually stabilise. That is, there is a positive integer m such that $T^j(V) = T^m(V)$ for all $j \geq m$. We will refer to the image $T^m(V)$ as the *generalised range space* of T and denote it by $R_\infty(T)$ [22, pp. 411].

Remark 3.4.13. The fact that this non-ascending sequence of T -invariant subspaces must eventually stabilise, means that the restriction of T to $R_\infty(T)$, denoted by $T \upharpoonright_{R_\infty(T)}$ is an isomorphism.

Lemma 3.4.14. [52, pp. 117] *Let $T: V \rightarrow V$ be a linear transformation and let $p(x) \in \mathbb{F}[x]$ be any polynomial. Then $\ker(p(T)) = \{v \in V \mid p(T)(v) = 0\}$ is a T -invariant subspace of V .*

In particular, letting $p(T) = T^k$ for $k = 1, 2, \dots$ in Lemma 3.4.14 gives us a non-descending chain of T -invariant subspaces:

$$0 \subset \ker(T) \subset \ker(T^2) \subset \dots$$

Again, since V is finite-dimensional this sequence must eventually stabilise. That is, there is a positive integer m such that $\ker(T^j) = \ker(T^m)$ for all $j \geq m$. We will refer to $\ker(T^m)$ as the *generalised null space* of T and denote it by $N_\infty(T)$ [22, pp. 411].

Theorem 3.4.15. [22, pp. 412] *Let $T: V \rightarrow V$ be a linear transformation. Then*

$$V = R_\infty(T) \oplus N_\infty(T).$$

Theorem 3.4.16. [52, pp. 119] Let V be a finite-dimensional vector space and let $T: V \rightarrow V$ be a linear transformation. Then $m_T(x)$ divides $c_T(x)$ and every irreducible factor of $c_T(x)$ is an irreducible factor of $m_T(x)$.

Corollary 3.4.17. [52, pp. 119] A vector space V is T -generated by a single element if and only if $m_T(x) = c_T(x)$.

Definition 3.4.18. [52, pp. 123] Let $T: V \rightarrow V$ be a linear transformation. Then $V = W_1 \oplus \cdots \oplus W_k$ is a T -invariant direct sum if $V = W_1 \oplus \cdots \oplus W_k$ is the direct sum of W_1, \dots, W_k and each W_i is a T -invariant subspace. If $V = W_1 \oplus W_2$ is a T -invariant direct sum decomposition, then W_2 is called a T -invariant complement of W_1 .

We now state the Primary Decomposition Theorem, which allows a decomposition of a vector space into a direct sum of T -invariant subspaces.

Theorem 3.4.19 (Primary Decomposition Theorem). [52, pp. 125] Let V be a vector space and let $T: V \rightarrow V$ be a linear transformation. Let $m_T(x) = p_1(x) \cdots p_k(x)$ be the minimum polynomial of T , where the p_i are pairwise relatively prime polynomials. Let $W_i = \ker(p_i(T))$ for $i = 1, \dots, k$. Then each W_i is a T -invariant subspace and $V = W_1 \oplus \cdots \oplus W_k$.

Let $V = W_1 \oplus \cdots \oplus W_k$ be the T -invariant direct sum decomposition given by Theorem 3.4.19. Let U_i be a T -invariant subspace of W_i , for $i = 1, \dots, k$. Then $U = U_1 \oplus \cdots \oplus U_k$ is a T -invariant subspace of V , and every T -invariant subspace of V arises in this way [52, pp. 126].

Theorem 3.4.20. [52, pp. 129-130] Let V be a finite-dimensional vector space and let $T: V \rightarrow V$ be a linear transformation. Let $w_1 \in V$ be any vector with $m_{T, w_1}(x) = m_T(x)$ and let W_1 be the subspace of V , T -generated by w_1 . Then W_1 has a T -invariant complement W_2 , i.e., there is a T -invariant subspace W_2 of V such that $V = W_1 \oplus W_2$.

Definition 3.4.21. Let V be a finite-dimensional vector space and let $T: V \rightarrow V$ be a linear transformation. An ordered set $\mathcal{C} = \{w_1, \dots, w_k\}$ is a *rational canonical T -generating set* of V if the following conditions are satisfied:

1. $V = W_1 \oplus \dots \oplus W_k$ where W_i is the subspace of V that is T -generated by w_i
2. $p_i(x)$ is divisible by $p_{i+1}(x)$ for $i = 1, \dots, k-1$, where $p_i(x) = m_{T, w_i}(x)$ is the T -annihilator of w_i

We now state the Cyclic Decomposition Theorem.

Theorem 3.4.22 (Cyclic Decomposition Theorem). [52, pp. 132] *Let V be a finite-dimensional vector space and let $T: V \rightarrow V$ be a linear transformation. Then V has a rational canonical T -generating set $\mathcal{C} = \{w_1, \dots, w_k\}$. If $\mathcal{C}' = \{w'_1, \dots, w'_l\}$ is any rational canonical T -generating set of V , then $k = l$ and $p'_i(x) = p_i(x)$ for $i = 1, \dots, k$, where $p'_i(x) = m_{T, w'_i}(x)$ and $p_i(x) = m_{T, w_i}(x)$.*

Definition 3.4.23. An $n \times n$ matrix M is in *rational canonical form* if it is a block diagonal matrix of the form

$$M = \begin{bmatrix} C(p_1(x)) & & & \\ & C(p_2(x)) & & \\ & & \ddots & \\ & & & C(p_k(x)) \end{bmatrix}$$

where $C(p_i(x))$ denotes the companion matrix of $p_i(x)$, for some sequence of polynomials $p_1(x), p_2(x), \dots, p_k(x)$ with $p_i(x)$ divisible by $p_{i+1}(x)$ for $i = 1, 2, \dots, k-1$.

Definition 3.4.24. If T has rational canonical form as in Definition 3.4.23, then the sequence of polynomials $p_1(x), p_2(x), \dots, p_k(x)$ are called the *elementary divisors* of T .

Theorem 3.4.25. [52, pp. 134]

1. Let V be a finite-dimensional vector space and let $T: V \rightarrow V$ be a linear transformation. Then V has a basis \mathcal{B} such that $[T]_{\mathcal{B}} = M$ is in rational canonical form. Furthermore, M is unique.
2. Let A be an $n \times n$ matrix. Then A is similar to a unique matrix M in rational canonical form.

Corollary 3.4.26. [52, pp. 135] Let T have elementary divisors $\{p_1(x), \dots, p_k(x)\}$. Then $m_T(x) = p_1(x)$ and $c_T(x) = p_1(x)p_2(x) \dots p_k(x)$.

Definition 3.4.27. [52, pp. 137] A $k \times k$ matrix is called a *Jordan block* associated with the eigenvalue λ if it has the form

$$\begin{bmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda & 1 \\ & & & & \lambda \end{bmatrix}$$

A matrix J is said to be in *Jordan canonical form* if J is a block diagonal matrix with each J_i a Jordan block.

$$J = \begin{bmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_l \end{bmatrix}$$

Theorem 3.4.28. [52, pp. 138]

1. Let V be a finite-dimensional vector space over a field \mathbb{F} and let $T: V \rightarrow V$ be a linear transformation. Suppose that the characteristic polynomial of T

factors into a product of linear factors, $c_T(x) = (x - a_1)^{e_1} \dots (x - a_m)^{e_m}$.

Then V has a basis \mathcal{B} with $[T]_{\mathcal{B}} = J$ a matrix in Jordan canonical form. J is unique up to the order of the blocks.

2. Let A be an $n \times n$ matrix over a field \mathbb{F} . Suppose that $c_A(x)$ the characteristic polynomial of A , factors into a product of linear factors, $c_A(x) = (x - a_1)^{e_1} \dots (x - a_m)^{e_m}$. Then A is similar to a matrix J in Jordan canonical form. J is unique up to the order of the blocks.

When $c_T(x)$ does not factor into a product of linear factors we do not get a Jordan canonical form. However, there are generalisations of Definition 3.4.27 and Theorem 3.4.28 that can be used in this case.

Definition 3.4.29. A $kl \times kl$ matrix is called a *generalised Jordan block* if it has the form

$$\begin{bmatrix} C & N & & & \\ & C & N & & \\ & & \ddots & \ddots & \\ & & & C & N \\ & & & & C \end{bmatrix}$$

where there are k blocks of the $l \times l$ matrix $C = C(p(x))$ along the diagonal and N is a matrix with an entry of 1 in row l column 1 and all other entries being zero. A matrix \hat{J} is said to be in *generalised Jordan canonical form* if \hat{J} is a block diagonal matrix with each \hat{J}_i a generalised Jordan block.

$$\hat{J} = \begin{bmatrix} \hat{J}_1 & & & \\ & \hat{J}_2 & & \\ & & \ddots & \\ & & & \hat{J}_l \end{bmatrix}.$$

Theorem 3.4.30. [52, pp. 140]

1. Let V be a finite-dimensional vector space over a field \mathbb{F} and let $c_T(x)$ factor as $c_T(x) = p_1(x)^{e_1} \dots p_m(x)^{e_m}$ for irreducible polynomials $p_1(x), \dots, p_m(x)$. Then V has a basis \mathcal{B} with $[V]_{\mathcal{B}} = \hat{J}$ a matrix in generalised Jordan canonical form. \hat{J} is unique up to the order of the generalised Jordan blocks.
2. Let A be an $n \times n$ matrix over a field \mathbb{F} and let $c_A(x)$ factor as $c_A(x) = p_1(x)^{e_1} \dots p_m(x)^{e_m}$, for irreducible polynomials $p_1(x), \dots, p_m(x)$. Then A is similar to a matrix \hat{J} in generalised Jordan canonical form. \hat{J} is unique up to the order of the generalised Jordan blocks.

3.5 Error Correcting Codes from Derivations

In this section we will consider derivations of group rings KG , where K is a finite field and G is a finite abelian group. Let $d \in \text{Der}(KG)$. The next lemma shows that d is a \ker_d -module homomorphism and so it is also a K -linear transformation.

Lemma 3.5.1. *Let R be a ring. Then d is a \mathcal{C}_d -module homomorphism for all $d \in \text{Der}(R)$.*

Proof. Let $d \in \text{Der}(R)$, let $c \in \mathcal{C}_d$ and let $a \in R$. d is an additive group homomorphism. $d(c) = 0$ so $d(ca) = d(c)a + cd(a) = cd(a)$. □

Remark 3.5.2. Note that d is also a $\mathcal{C}(R)$ -module homomorphism for all $d \in \text{Der}(R)$.

Definition 3.5.3. Given a derivation $d: KG \rightarrow KG$, define $d^n: KG \rightarrow KG$ to be the composition of d with itself n times. That is, for all a in KG , $d^n(a) = \underbrace{d(d(\dots d(a) \dots))}_{n \text{ times}}$.

Remark 3.5.4. Let d be a derivation of KG . Then d^n is a K -linear transformation (K -module homomorphism) for all positive integers n .

Given a derivation d on a group algebra KG , the Primary Decomposition Theorem (Theorem 3.4.19) gives a way of producing d -invariant subspaces of KG .

Example 3.5.5. Let d be a derivation of a group algebra KG . Let $m_d(x) = p_1(x) \dots p_k(x)$ be the minimum polynomial of d , which factors as a product of pairwise relatively prime polynomials p_i . Moreover, let $W_i = \ker(p_i(d))$ for $i = 1, \dots, k$. Then applying The Primary Decomposition Theorem (Theorem 3.4.19) we get that each W_i is a d -invariant subspace and KG has the vector space decomposition $V = W_1 \oplus \dots \oplus W_k$.

In particular, By Theorem 3.4.15

$$KG = R_\infty(d) \oplus N_\infty(d).$$

Remark 3.5.6. [25, pp. 41, 47] A linear block code over a finite field K is a subspace of the vector space V of ordered n -tuples over K for some positive integer n . In particular, if $d: V \rightarrow V$ then the generalised range space of d , $R_\infty(d)$ is a linear block code over K .

Definition 3.5.7. A q -ary $[n, k, \delta]$ code is a code of length n , dimension k and minimum distance δ over a field of order q .

We will now consider particular derivations of the group ring \mathbb{F}_3C_6 where C_6 is the cyclic group of order 6 with presentation $\langle x \mid x^6 = 1 \rangle$. For a derivation d on \mathbb{F}_3C_6 we can choose any element of \mathbb{F}_3C_6 to be the image of x under d , by Theorem 2.3.4.

Example 3.5.8. Let $C_6 = \langle x \mid x^6 = 1 \rangle$ and let d be the derivation $d: \mathbb{F}_3C_6 \rightarrow \mathbb{F}_3C_6$ defined by $x \mapsto 1$. This is the classical derivative map over \mathbb{F}_3 . It is an \mathbb{F}_3 -linear

map or linear transformation and so can be represented by a 6×6 matrix over \mathbb{F}_3 . We will denote this matrix by $[d]_{\mathcal{B}}$, where $\mathcal{B} = \{1, x, x^2, x^3, x^4, x^5\}$ is a basis for \mathbb{F}_3C_6 . Note that

$$[d]_{\mathcal{B}} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^{\top} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^{\top},$$

$$[d]_{\mathcal{B}} \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}^{\top} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^{\top},$$

$$[d]_{\mathcal{B}} \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}^{\top} = \begin{bmatrix} 0 & 2 & 0 & 0 & 0 & 0 \end{bmatrix}^{\top},$$

$$[d]_{\mathcal{B}} \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}^{\top} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^{\top},$$

$$[d]_{\mathcal{B}} \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}^{\top} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}^{\top},$$

$$[d]_{\mathcal{B}} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}^{\top} = \begin{bmatrix} 0 & 0 & 0 & 0 & 2 & 0 \end{bmatrix}^{\top}.$$

In summary, $[d]_{\mathcal{B}} \begin{bmatrix} a_0 & a_1 & a_2 & a_3 & a_4 & a_5 \end{bmatrix}^{\top} = \begin{bmatrix} a_1 & 2a_2 & 0 & a_4 & 2a_5 & 0 \end{bmatrix}^{\top}$, for any $a_i \in \mathbb{F}_3$.

Thus the matrix $[d]_{\mathcal{B}}$ is given by

$$[d]_{\mathcal{B}} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

The matrix $[d]_{\mathcal{B}}$ acts on column vectors from the left. For example, let u be the column vector representing $1 + 2x^4$. Then the column vector representing the image of $1 + 2x^4$ under the derivation d is given by

$$[d]_{\mathcal{B}}u = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 2 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 2 \\ 0 \\ 0 \end{bmatrix}.$$

Example 3.5.9. Let d be the derivation $d: \mathbb{F}_3C_6 \rightarrow \mathbb{F}_3C_6$ defined by $x \mapsto 1 + x^2 + 2x^5$. Let $\mathcal{B} = \{1, x, x^2, x^3, x^4, x^5\}$. Then \mathcal{B} is a basis for \mathbb{F}_3C_6 . It can be shown by performing the computation as in Example 3.5.8 that the matrix representing d is given by

$$[d]_{\mathcal{B}} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 2 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 2 & 0 \\ 0 & 0 & 2 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 2 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

The minimal and characteristic polynomials of d were calculated using the computer algebra system Sage [43] and are as follows: $m_d(x) = (x + 1)(x + 2)(x^3)$ and $c_d(x) = (x + 1)(x + 2)(x^4)$. Let $\alpha = \sum_{i=0}^5 a_i x^i \in \mathbb{F}_3C_6$ and so α can be written as the vector $[a_0, a_1, a_2, a_3, a_4, a_5]^{\top}$ with respect to \mathcal{B} . Applying $m_d(x)$ gives $([d]_{\mathcal{B}}^5 + 2[d]_{\mathcal{B}}^3)[a_0, a_1, a_2, a_3, a_4, a_5]^{\top} = 0$. Using the Primary Decomposition Theorem (Theorem 3.4.19), $\mathbb{F}_3C_6 = E_2 \oplus E_1 \oplus N_{\infty}(d)$, where E_{λ} is the 1-dimensional

eigenspace associated with the eigenvalue λ and $N_\infty(d)$ is the d invariant subspace associated with the factor x^3 , that is $N_\infty(d) = \ker(d^3)$. The minimal polynomial factors into a product of linear factors and so by Theorem 3.4.28, we can find a basis \mathcal{B}' such that $[d]_{\mathcal{B}'}$ is in Jordan canonical form. We will now look at each eigenvalue separately. Firstly consider the eigenvalue 2. Let d_2 denote the restriction of d to E_2 . E_2 is a d -invariant subspace of \mathbb{F}_3C_6 and so d_2 is a linear transformation on the 1-dimensional subspace E_2 such that $p_2(d_2)(E_2) = 0$, where $p_2(x) = (x + 1)$. Therefore $m_{d_2}(x) = c_{d_2}(x) = (x + 1)$ and so the Jordan block associated with the eigenvalue 2 is $[2]$. Likewise the Jordan block associated with the eigenvalue 1 is $[1]$. Let d_R denote the restriction of d to $R_\infty(d)$. Then $m_{d_R}(x) = c_{d_R}(x) = (x + 1)(x + 2)$ and so by Theorem 3.4.28

$$[d_R]_B = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$$

where the basis B is given by $B = \{v_2, v_1\}$ and v_λ is the eigenvector associated with the eigenvalue λ . $v_1 = \begin{bmatrix} 1 & 2 & 1 & 2 & 1 & 2 \end{bmatrix}^\top$ and $v_2 = \begin{bmatrix} 0 & 2 & 2 & 0 & 1 & 1 \end{bmatrix}^\top$.

We now turn our attention to the generalised nullspace $N_\infty(d) = \ker(d^\infty)$. Let d_N denote the restriction of d to $N_\infty(d)$. We have $m_{d_N}(x) = x^3$ and $c_{d_N}(x) = x^4$. $N_\infty(d)$ is not d_N -generated by a single vector. Thus we can use the Cyclic Decomposition Theorem (Theorem 3.4.22) and Corollary 3.4.26 to write $N_\infty(d) = N_1 \oplus N_2$, where N_i is the subspace that is d_N -generated by w_i for $i = 1, 2$. We have that $m_{d_N, w_1}(x) = x^3$ and $m_{d_N, w_2}(x) = x$. $w_1 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}^\top$ d_N -generates N_1 and $w_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^\top$ d_N -generates N_2 .

We now have a basis $\mathcal{B}' = \{v_2, v_1, [d]_{\mathcal{B}'}^2 w_1, [d]_{\mathcal{B}'} w_1, w_1, w_2\}$ and can write the

matrix $[d]_{\mathcal{B}'}$ in Jordan canonical form

$$[d]_{\mathcal{B}'} = P^{-1}[d]_{\mathcal{B}}P = \left[\begin{array}{c|ccc|c} 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right], \quad \text{where} \quad P = \left[\begin{array}{cccccc} 0 & 1 & 2 & 0 & 0 & 1 \\ 1 & 2 & 0 & 2 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 2 & 2 & 0 & 0 & 0 \\ 2 & 1 & 0 & 2 & 0 & 0 \\ 2 & 2 & 0 & 0 & 1 & 0 \end{array} \right].$$

$R_{\infty}(d)$ is a 2 dimensional subspace of \mathbb{F}_3C_6 over \mathbb{F}_3 . A generator matrix for the ternary code $R_{\infty}(d)$ is $G = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 1 & 2 & 1 & 2 \\ 0 & 1 & 1 & 0 & 2 & 2 \end{bmatrix}$. The codewords (elements) of $R_{\infty}(d)$ are

$[000000], [121212], [212121], [011022], [102201], [220110], [022011], [110220], [201102]$.

The minimum distance of this code is 4 by inspection and so $R_{\infty}(d)$ is a 3-ary $[6, 2, 4]$ code. It is an optimal code as the Griesmer bound for a linear code of length 6 and dimension 2 over \mathbb{F}_3 is 4 [21].

Remark 3.5.10. Let KG be a finite group algebra, let $d \in \text{Der}(KG)$ and let \mathcal{B} be some listing of the elements of G . Then the generalised null space of $[d]_{\mathcal{B}}$ is not a good code since the multiplicative identity 1, is a vector of weight one that is mapped to 0 on the first iteration and so $1 \in N_{\infty}(d)$. Therefore $N_{\infty}(d)$ is a $[n, m, 1]$ code, where m is the algebraic multiplicity of the eigenvalue zero.

Example 3.5.11. Let d be the derivation $d: \mathbb{F}_3C_6 \rightarrow \mathbb{F}_3C_6$ defined by $x \mapsto 1 + x + 0x^2 + x^3 + x^4 + x^5$. Let $\mathcal{B} = \{1, x, x^2, x^3, x^4, x^5\}$. Then the matrix over \mathbb{F}_3

representing d with respect to \mathcal{B} is given by

$$\begin{aligned}
[d]_{\mathcal{B}} = & \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \\
& + \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 2 & 0 & 1 & 0 \\ 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 0 & 2 & 0 & 1 & 2 \\ 0 & 1 & 0 & 0 & 1 & 2 \\ 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 1 & 2 & 0 & 0 & 2 \end{bmatrix}.
\end{aligned}$$

The minimal and characteristic polynomials of d were calculated using the computer algebra system Sage. They were found to be $m_d(x) = x^3(x^2 + 1)$ and $c_d(x) = x^4(x^2 + 1)$. Using Theorem 3.4.15 we get $\mathbb{F}_3 C_6 = \ker(d^3) \oplus \ker(d^2 + 1) = R_\infty(d) \oplus N_\infty(d)$. The matrix $[d]_{\mathcal{B}}$ does not have a Jordan canonical form as the polynomial $x^2 + 1$ is irreducible over \mathbb{F}_3 . However, Theorem 3.4.30 states that we can find a basis \mathcal{B}' such that $[d]_{\mathcal{B}'}$ is in generalised Jordan canonical form. We will now look at each summand separately. Firstly consider $R_\infty(d)$. Let d_R denote the restriction of d to $R_\infty(d)$. $m_{d_R}(x) = c_{d_R}(x) = x^2 + 1$ and so by Theorem 3.4.30 and Definitions 3.4.29 and 3.4.7 the generalised Jordan block associated with $R_\infty(d)$ is

$$[d_R]_{\mathcal{B}} = [C(c_{d_R}(x))] = [C(x^2 + 1)] = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}$$

where the basis B is given by $B = \{dv, v\}$ and v is any vector of \mathbb{F}_3C_6 that d -generates $R_\infty(d)$ according to Definition 3.4.12. An example of such a vector v is $\begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}^\top$.

We now turn our attention to $N_\infty(d)$. Let d_N denote the restriction of d to $N_\infty(d)$. We have $m_{d_N}(x) = x^3$ and $c_{d_N}(x) = x^4$. Therefore $N_\infty(d)$ is not d -generated by a single vector. By the Cyclic Decomposition Theorem (Theorem 3.4.22) $N_\infty(d) = N_1 \oplus N_2$, where N_i is the subspace that is d -generated by w_i for $i = 1, 2$. By Theorem 3.4.22, $m_{D,w_1}(x) = x^3$ and $m_{D,w_2}(x) = x$. $w_1 = \begin{bmatrix} 0 & 1 & 2 & 0 & 2 & 1 \end{bmatrix}^\top$ and $w_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^\top$ are 2 such vectors.

Therefore $\mathcal{B}' = \{Dv, v, D^2w_1, Dw_1, w_1, w_2\}$ is a basis for \mathbb{F}_3C_6 such that $[d]_{\mathcal{B}'}$ is in generalised Jordan canonical form

$$[d]_{\mathcal{B}'} = P^{-1}[d]_{\mathcal{B}}P = \left[\begin{array}{c|ccc|c} 0 & 1 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right] \quad \text{where} \quad P = \left[\begin{array}{cccccc} 2 & 0 & 1 & 1 & 0 & 1 \\ 2 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 2 & 2 & 0 \\ 2 & 0 & 2 & 2 & 0 & 0 \\ 2 & 1 & 0 & 0 & 2 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \end{array} \right].$$

$R_\infty(d)$ is a 2 dimensional subspace of \mathbb{F}_3C_6 over \mathbb{F}_3 and so has 9 elements.

$$[d_R]_{\mathcal{B}} = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}, \quad \text{where } \mathcal{B} = \{dv, v\} \text{ and } v = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}^\top.$$

Therefore the orbit of dv and $dv + v$ under d are respectively

$$\begin{array}{cccccc} \begin{bmatrix} 1 & 0 \end{bmatrix}^\top & \rightarrow & \begin{bmatrix} 0 & 2 \end{bmatrix}^\top & \rightarrow & \begin{bmatrix} 2 & 0 \end{bmatrix}^\top & \rightarrow & \begin{bmatrix} 0 & 1 \end{bmatrix}^\top & \rightarrow & \begin{bmatrix} 1 & 0 \end{bmatrix}^\top & \text{and} \\ \begin{bmatrix} 1 & 1 \end{bmatrix}^\top & \rightarrow & \begin{bmatrix} 1 & 2 \end{bmatrix}^\top & \rightarrow & \begin{bmatrix} 2 & 2 \end{bmatrix}^\top & \rightarrow & \begin{bmatrix} 2 & 1 \end{bmatrix}^\top & \rightarrow & \begin{bmatrix} 1 & 1 \end{bmatrix}^\top. \end{array}$$

Therefore the graph of $R_\infty(d)$ consists of two 4-cycles and the fixed point 0. The matrix $[d_N]_{\mathcal{B}'}$ is nilpotent with an index of nilpotency of 3. This shows that after 3 iterations of d the group algebra has been mapped onto $R_\infty(d)$. That is $d^3(\mathbb{F}_3C_6) = R_\infty(d)$. The codewords (elements) of $R_\infty(d)$ are

$[000000], [112112], [010010], [221221], [020020], [211211], [102102], [122122], [201201]$.

The minimum distance of this code is 2 by inspection and so $R_\infty(d)$ is a 3-ary $[6, 2, 2]$ code.

In both this Example and Example 3.5.9 the generalised range space $R_\infty(d)$ is a d -invariant subspace of \mathbb{F}_3C_6 . However, by varying the derivation used, the minimum distance decreased from 4 to 2.

Example 3.5.12. Let d be the derivation $d: \mathbb{F}_3C_6 \rightarrow \mathbb{F}_3C_6$ defined by $x \mapsto 1 + x + 2x^2 + x^3 + x^4 + x^5$ where $C_6 = \langle x \mid x^6 = 1 \rangle$. Note that we have changed only the coefficient of the x^2 term in the image of x under d from the one used in Example 3.5.11. The matrix representing the \mathbb{F}_3 -linear transformation d with respect to the basis $\mathcal{B} = \{1, x, x^2, x^3, x^4, x^5\}$ is

$$[d]_{\mathcal{B}} = \begin{bmatrix} 0 & 1 & 2 & 0 & 1 & 1 \\ 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 2 & 2 & 0 & 1 & 2 \\ 0 & 1 & 1 & 0 & 1 & 2 \\ 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 1 & 2 & 0 & 2 & 2 \end{bmatrix}.$$

Using the method detailed in the previous examples a change of basis matrix

P is obtained and $[d]_{\mathcal{B}}$ can be written in Jordan canonical form.

$$P = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 2 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 2 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 2 & 0 & 0 \end{bmatrix} \quad \text{and} \quad P^{-1}[d]_{\mathcal{B}}P = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

$R_{\infty}(d)$ is a 2 dimensional subspace of \mathbb{F}_3C_6 . A graph with the elements of $R_{\infty}(d)$ as vertices and (u, v) as a directed edge if $[d]_{\mathcal{B}}u = v$ is given in Figure 3.2. The codewords (elements) of $R_{\infty}(d)$ are

$[000000], [110110], [220220], [121121], [201201], [011011], [212212], [022022], [102102]$.

The minimum distance of this code is 4 by inspection and so $R_{\infty}(d)$ is a 3-ary $[6, 2, 4]$ code. Let $a = 1 + x + x^3 + x^4$ ($[110110]$) and $b = 2 + x^2 + 2x^3 + x^5$ ($[201201]$). Then a and b are both elements of $R_{\infty}(d)$, however their product $ab = x + 2x^2 + x^4 + 2x^5$ ($[012012]$) is not an element of $R_{\infty}(d)$. This shows that in general $R_{\infty}(d)$ is not closed under multiplication.

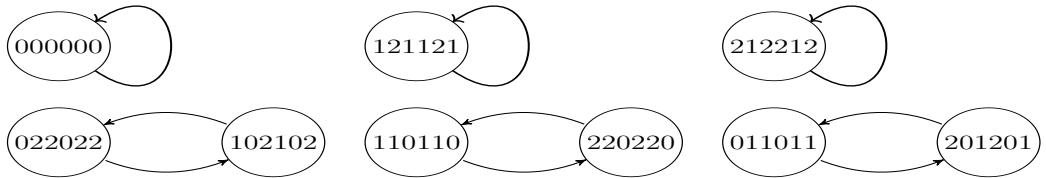


Figure 3.2: The subgraph of the graph Γ induced by $R_{\infty}(d)$ in Example 3.5.12, where Γ is the graph with the elements of \mathbb{F}_3C_6 as vertices and (u, v) is a directed edge if $Du = v$.

Chapter 4

Graphs Of Derivations

In this chapter the directed graphs of derivations of group algebras are explored, that is, a derivation of a group algebra is considered as a linear finite dynamical system (LFDS). The motivation for this comes from Theorem 3.1.18, which tells us that if $Der(KG)$ and $Der(KH)$ are not isomorphic as additive groups then KG and KH are not isomorphic as rings. It is shown in Theorem 4.1.8 that if $\phi: R \rightarrow S$ is a ring isomorphism, then there is a bijection from $Der(R)$ onto $Der(S)$ such that corresponding derivations have isomorphic associated digraphs. Therefore properties of the LFDS associated with a derivation can be used to distinguish between group rings. The groups considered in this chapter are abelian. In Section 4.1 the preperiod of $Der(\mathbb{F}_2G)$ is shown to be less than or equal to the size of the group G . Also, when $G = C_2 \times C_2$, this bound is attained.

The digraph of a particular element of $Der(\mathbb{F}_2(C_2 \times C_2))$ is studied and it is shown to contain a 7-cycle. The digraphs of $Der(\mathbb{F}_2C_4)$ are partitioned by conjugacy class in Table 4.1. Also, permutations of \mathbb{F}_2C_4 are exhibited such that conjugation by these permutations give a way of permuting between any pair of derivations of \mathbb{F}_2C_4 whose matrix representations with respect to a basis are similar. By way of contrast it is shown that no digraph of a derivation of \mathbb{F}_2C_4 contains a

7-cycle. Therefore by examining the properties of the digraphs of $\mathbb{F}_2(C_2 \times C_2)$ and \mathbb{F}_2C_4 , it has been shown that the group algebras are not isomorphic as rings.

It is shown in Section 4.4 that an involution of a group algebra KG permutes $Der(KG)$, however in the case when KG is not commutative it is not an element of $Aut(KG)$. The automorphism group of $\mathbb{F}_2(C_2 \times C_2)$ and the size of the automorphism group of $\mathbb{F}_2(C_4 \times C_4)$ are given in Section 4.5 as well as the unit group of $\mathbb{F}_2(C_4 \times C_4)$.

By Theorem 3.1.18, if KG and KH are isomorphic as rings then $|Der(KG)| = |Der(KH)|$. Thus counting derivations can be used to distinguish between group algebras. The smallest example where counting derivations does not suffice is for $\mathbb{F}_2(C_4 \times C_4)$ and $\mathbb{F}_2(C_2 \times C_8)$, where $|Der(\mathbb{F}_2(C_4 \times C_4))| = |Der(\mathbb{F}_2(C_2 \times C_8))| = 2^{32}$. Therefore other properties of $Der(KG)$ and $Der(KH)$ will need to be employed. The maximum nilpotency index is one property of the derivations of a group algebra that is investigated. It is shown in Lemma 4.6.5 that the maximum nilpotency index for $Der(\mathbb{F}_{2^n}C_{2^m})$ is $2^{m-1} + 1$. Maximum nilpotency index is then used to distinguish between $\mathbb{F}_2(C_4 \times C_4)$ and $\mathbb{F}_2(C_2 \times C_8)$. It is shown that the maximum nilpotency index of $\mathbb{F}_2(C_4 \times C_4)$ is 8, whereas the maximum nilpotency index of $\mathbb{F}_2(C_2 \times C_8)$ is at least 13.

4.1 Digraphs and Finite Dynamical Systems

Definition 4.1.1. [23] A *finite dynamical system* (FDS) is a pair (X, f) , where X is a finite set and f is a function from X to X .

Definition 4.1.2. Let (X, f) be an FDS and let $x \in X$. Then the *orbit* of x is defined to be $\mathcal{O}(x) = \{f^n(x) \mid n = 0, 1, \dots\}$, where $f^0(x) = x$.

Definition 4.1.3. [23] A *linear finite dynamical system* (LFDS) is an FDS, (V, f) ,

where V is a finite dimensional vector space over a finite field K and f is a K -linear map from V to V .

Definition 4.1.4. [23] Let (X, f) and (Y, g) be finite dynamical systems. An *FDS-morphism* is a map $\phi: X \rightarrow Y$ such that $\phi \circ f = g \circ \phi$. Therefore we have the following commuting diagram:

$$\begin{array}{ccc} X & \xrightarrow{\phi} & Y \\ f \downarrow & & \downarrow g \\ X & \xrightarrow{\phi} & Y \end{array}$$

(X, f) is *isomorphic* to (Y, g) if there exists a bijective FDS-morphism from X to Y .

Definition 4.1.5. A *directed graph* or *digraph* is an ordered pair $\Gamma = (\mathcal{V}(\Gamma), \mathcal{E}(\Gamma))$, where $\mathcal{V}(\Gamma)$ is a set whose elements are called vertices and $\mathcal{E}(\Gamma)$ is a set of ordered pairs on the set $\mathcal{V}(\Gamma)$, called directed edges or arcs.

A linear finite dynamical system, (V, f) has an associated digraph denoted $\Gamma(f)$, where $\mathcal{V}(\Gamma(f)) = \{v \mid v \in V\}$ and $\mathcal{E}(\Gamma(f)) = \{(v, f(v)) \mid v \in V\}$.

In order to study the dynamics of an FDS we seek a description of the set of orbits, $\{\mathcal{O}(x) \mid x \in X\}$. That is, we are looking for a description of the digraph associated with the FDS.

Definition 4.1.6. Let $\Gamma_1 = (\mathcal{V}(\Gamma_1), \mathcal{E}(\Gamma_1))$ and $\Gamma_2 = (\mathcal{V}(\Gamma_2), \mathcal{E}(\Gamma_2))$ be digraphs. An *isomorphism* ϕ between Γ_1 and Γ_2 is a bijection from $\mathcal{V}(\Gamma_1)$ onto $\mathcal{V}(\Gamma_2)$ such that $(a, b) \in \mathcal{E}(\Gamma_1)$ if and only if $(\phi(a), \phi(b)) \in \mathcal{E}(\Gamma_2)$. Note that the direction of the arcs is preserved.

Remark 4.1.7. [23] Isomorphic finite dynamical systems have isomorphic associated digraphs.

Theorem 4.1.8. *Let R and S be finite rings and let $\phi: R \rightarrow S$ be a ring isomorphism. Then there is a bijection Φ from $Der(R)$ onto $Der(S)$ such that $\Gamma(\Phi(d))$ and $\Gamma(d)$ are isomorphic digraphs, for all $d \in Der(R)$.*

Proof. By Theorem 3.1.18, $\Phi: Der(R) \rightarrow Der(S)$ defined by $d \mapsto \phi \circ d \circ \phi^{-1}$ is a bijection. By Definition 4.1.4, $\phi: R \rightarrow S$ is an FDS-isomorphism from (R, d) to $(S, \Phi(d))$, for all $d \in Der(R)$. Therefore by Remark 4.1.7, $\Gamma(d)$ and $\Gamma(\Phi(d))$ are isomorphic digraphs, for all $d \in Der(R)$. \square

Definition 4.1.9. [23] Let (X, f) and (Y, g) be FDS. Define the sum of (X, f) and (Y, g) , denoted by $(X, f) + (Y, g)$, to be the FDS $(X \sqcup Y, f \sqcup g)$, where $X \sqcup Y$ is the disjoint union of the sets X and Y and $f \sqcup g: X \sqcup Y \rightarrow X \sqcup Y$ defined by

$$(f \sqcup g)(a) = \begin{cases} f(a) & \text{if } a \in X, \\ g(a) & \text{if } a \in Y. \end{cases}$$

Definition 4.1.10. Let Γ_1 and Γ_2 be graphs. Define the sum of Γ_1 and Γ_2 , denoted $\Gamma_1 + \Gamma_2$ to be the graph with vertex set $\mathcal{V}(\Gamma_1) \sqcup \mathcal{V}(\Gamma_2)$ and edge set $\mathcal{E}(\Gamma_1) \sqcup \mathcal{E}(\Gamma_2)$.

Remark 4.1.11. Let (X, f) and (Y, g) be FDS. The digraph of the sum of (X, f) and (Y, g) is the sum of the digraphs of (X, f) and (Y, g) . That is $\Gamma(f \sqcup g) = \Gamma(f) + \Gamma(g)$.

Definition 4.1.12. [23] Let (X, f) and (Y, g) be FDS. Define the product of (X, f) and (Y, g) , denoted by $(X, f) \times (Y, g)$, to be the FDS $(X \times Y, f \times g)$, where $X \times Y$ is the cartesian product of the sets X and Y , and $(f \times g)(x, y) = (f(x), g(y))$.

Definition 4.1.13. [20] Let v_0 and v_l be vertices of a graph or digraph, Γ . Then a *path* from v_0 to v_l , of length l is a sequence v_0, v_1, \dots, v_l of vertices of Γ such that $(v_i, v_{i+1}) \in \mathcal{E}(\Gamma)$, for $i = 0, 1, \dots, l-1$. A *weak path* is a sequence v_0, v_1, \dots, v_l of vertices of a directed graph Γ such that either (v_i, v_{i+1}) or (v_{i+1}, v_i) is an arc in Γ , for $i = 0, 1, \dots, l-1$.

Definition 4.1.14. [20] A digraph is said to be *strongly connected* if there is a path between any pair of vertices and *weakly connected* if there is a weak path between any pair of vertices. An induced strongly / weakly connected subgraph of Γ that is maximal with respect to inclusion of vertices is called a *strong / weak component* of the digraph.

Definition 4.1.15. Let v be a vertex of a digraph Γ . The *out degree* of v , denoted $Out(v)$, is the number of arcs whose first coordinate is v , that is $Out(v) = |\{(v, a) \in E(\Gamma) \mid a \in V(\Gamma)\}|$. Similarly, the *in degree* of v , denoted $In(v)$, is the number of arcs whose second coordinate is v .

Definition 4.1.16. [20] A *cycle* is a strongly connected digraph such that $In(v) = Out(v) = 1$, for every vertex v .

Definition 4.1.17. The *circumference* of a digraph Γ is the length of the longest cycle in the graph and is denoted by $\Lambda(\Gamma)$.

Definition 4.1.18. Let (V, f) be an FDS. An element $t \in V$ is called a *terminal element* of the FDS if $f(t) = t$ and for all $v \in V$, $f^n(v) = t$ for some positive integer n .

Definition 4.1.19. [23] An FDS (V, f) is called a *tree* if it has a terminal element, t . For a tree (V, f) , define the *height* of any $v \in V$ as the least nonnegative integer $h(v)$ such that $f^{h(v)}(v) = t$. Define the *height* of the tree as $h(V) = \max\{h(v) \mid v \in V\}$.

Remark 4.1.20. Let the FDS, (V, f) be a tree. The associated digraph, $\Gamma(f)$ will also be referred to as a tree. Note that using the terminology from graph theory it would be called a directed rooted tree (in-tree) with an added loop (an arc from a vertex to itself) at the root (terminal vertex).

Definition 4.1.21. [23] The *order of a polynomial* $f \in K[X]$ denoted $ord(f)$ is the least positive integer r such that $f(X)$ divides $X^r - 1$. In [23] it was also noted

that if f is irreducible and such that $f(0) \neq 0$ and $\text{ord}(f) = e$, for any $s \in \mathbb{N}$, then $\text{ord}(f^s) = ep^t$, where $p = \text{char}(K)$ and t is the smallest integer satisfying $p^t \geq s$.

Definition 4.1.22. Let n be a positive integer and V an n -dimensional vector space over a field K with $B = \{b_1, b_2, \dots, b_n\}$ a basis for V . Let $d: V \rightarrow V$ be a K -linear map. Then define

$$[d]_B = \begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \dots & a_{n,n} \end{bmatrix}, \quad \text{where } d(b_j) = \sum_{i=1}^n a_{i,j} b_i.$$

Definition 4.1.23. Let V be a vector space. Then a map $N: V \rightarrow V$ is *nilpotent* if N^m is the zero map for some positive integer m . The least such integer m is called the *nilpotency index* of N .

Definition 4.1.24. [23] Let V be a finite dimensional vector space over a field K . Then a nilpotent map $N: V \rightarrow V$ is a *pure nilpotent map* if the nilpotency index of N is equal to the dimension of the generalised null space N_∞ . This implies that the dimension of the kernel of N is 1 and that there exists a basis B of V such that the matrix $[N]_B$ has 1's in the superdiagonal (the diagonal just above the main diagonal) and 0's in all other positions.

Definition 4.1.25. Let G be a finite group and let K be a finite field. Let d be a derivation of KG , with associated digraph $\Gamma(d)$. Denote by $\Lambda(\text{Der}(KG))$ the length of the longest cycle contained in the digraphs $\Gamma(d)$ for any derivation d of KG . That is, $\Lambda(\text{Der}(KG)) = \max\{\Lambda(\Gamma(d)) \mid d \in \text{Der}(KG)\}$.

Definition 4.1.26. By the results of [23], the associated digraph of a LFDS is the product of a tree and a sum of cycles. Therefore the orbit of any vertex v terminates with a cycle, the length of this cycle is called the *period* of v and is denoted by

$per(v)$. The length of the shortest path from v to any vertex in the terminating cycle is called the *preperiod* of v and is denoted by $pper(v)$. Figure 4.1 illustrates an example of a vertex (vertex 0) with period 4 and preperiod 3. Let d be a derivation of a group algebra KG . Then the period (preperiod) of d , denoted $per(d)$ ($pper(d)$) is the maximum of the periods (preperiods) of the vertices of $\Gamma(d)$. Moreover, the period (preperiod) of $Der(KG)$, denoted $per(Der(KG))$ ($pper(Der(KG))$) is the maximum of the periods (preperiods) of the derivations of KG .

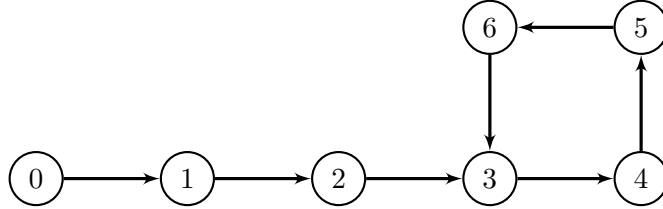


Figure 4.1: The vertex 0 has preperiod 3 and period 4

Lemma 4.1.27. *Let G be a group. Then the preperiod of $Der(\mathbb{F}_2G)$ is less than or equal to $|G|$.*

Proof. Let $d \in Der(\mathbb{F}_2G)$. Then by [23], $\Gamma(d) = \Gamma(N) \times \Gamma(B)$, where $\Gamma(N)$ is a tree and $\Gamma(B)$ is a sum of cycles. The preperiod of $Der(\mathbb{F}_2G)$ is the height of the tree $\Gamma(N)$. By Theorems 2 and 3 of [23] the preperiod of $Der(\mathbb{F}_2G)$ is less than or equal to $|G|$. \square

Remark 4.1.28. The preperiod of $Der(\mathbb{F}_2(C_2 \times C_2))$ attains the bound established in Lemma 4.1.27 as the following example shows.

Example 4.1.29. Let $d = y\partial_x + \partial_y$ be a derivation of $\mathbb{F}_2(C_2 \times C_2)$. Then by Lemma 4.1.27, the preperiod of $Der(\mathbb{F}_2(C_2 \times C_2)) \leq 4$. However, the preperiod of d is equal to 4, since $xy \mapsto 1 + x \mapsto y \mapsto 1 \mapsto 0$.

4.2 The Digraph of a derivation of $\mathbb{F}_2(\mathbf{C}_2 \times \mathbf{C}_2)$

In this section we look at the digraph of a particular element d of $Der(\mathbb{F}_2(\mathbf{C}_2 \times \mathbf{C}_2))$. It is shown that the digraph of d , denoted $\Gamma(d)$, contains a cycle of length 7. This property of the digraph $\Gamma(d)$ is used in Section 4.3 to contrast with the properties of the digraphs of the elements of $Der(\mathbb{F}_2\mathbf{C}_4)$.

The following Theorems from [23] will be used in this section. Let V be a finite dimensional vector space.

Definition 4.2.1. A nilpotent linear transformation $T: V \rightarrow V$ is *pure nilpotent* when its nilpotency index is equal to the dimension of V .

Theorem 4.2.2. [23] *Let $u: V \rightarrow V$ be a pure nilpotent map and let n be the dimension of V . The digraph of u is a tree of height n with terminal point zero. Each nonzero vector of the kernel belongs to a branch of height n of the tree. All points with height n are sources and all the points of height less than n have in degree q .*

Theorem 4.2.3. [23] *The graph of a nilpotent map is a product of pure trees whose heights correspond to the size of the blocks in the Jordan canonical form of the matrix representing the map.*

Theorem 4.2.4. [23] *Let (E, f) be a bijective FDS. Let $c_f(x) = P_1^{r_1} P_2^{r_2} \dots P_s^{r_s}$ be the characteristic polynomial of f , where the polynomials P_i are irreducible and pairwise relatively prime. Then the graph of f is the product of the graphs associated with each $P_i^{r_i}$. For each i , there is an additional decomposition of each preceding block into graphs of elementary components (rational decomposition).*

Definition 4.2.5. The order of a polynomial g denoted $ord(g)$, is defined to be the least positive integer r such that $g(x)$ divides $x^r - 1$.

Theorem 4.2.6. [23] Let K be a finite field of characteristic p with q elements. Let V be a vector space over K of finite dimension n . Let $T: V \rightarrow V$ be a bijective linear map. Suppose that the minimal polynomial of T is $f = g^s$, where g is an irreducible polynomial of degree m . Then the cycle structure of the graph of f is given by:

$$\Gamma(T) = 1 + \sum_{i=1}^s \frac{q^{mi} - q^{m(i-1)}}{r_i} C_{r_i},$$

where 1 is the 0-cycle, C_{r_i} is a cycle of length r_i and $r_i = \text{ord}(g^i)$.

Theorem 4.2.7. [23] Let (V, f) be a LFDS. Then the digraph of f is equal to the product of a tree, corresponding to the nilpotent part of f , by the cycles corresponding to the bijective part of f .

Example 4.2.8. Let $C_2 \times C_2 = \langle x, y \mid x^2 = y^2 = [x, y] = 1 \rangle$. Let d be the derivation of $\mathbb{F}_2(C_2 \times C_2)$ defined by $x \mapsto 1 + y + xy$ and $y \mapsto xy$. Then $d(1) = 0$ and $d(xy) = d(x)y + xd(y) = (1 + y + xy)y + x(xy) = y + 1 + x + y = 1 + x$. We now determine $\Gamma(d)$, the digraph of d . d is an \mathbb{F}_2 -linear transformation and so we can represent d as a 4×4 matrix over \mathbb{F}_2 . $C_2 \times C_2 = \{1, x, y, xy\}$ is a basis for $\mathbb{F}_2(C_2 \times C_2)$. For $i = 1, 2, 3, 4$, let v_i be the column vector of length 4 over \mathbb{F}_2 with 1 in position i and 0 in the other 3 positions. We use the following correspondence:

$$1 \leftrightarrow v_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad x \leftrightarrow v_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad y \leftrightarrow v_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \quad xy \leftrightarrow v_4 = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

Let $B = \{v_i \mid i = 1, 2, 3, 4\}$. Then B is a basis for the vector space \mathbb{F}_2^4 and so by

Definition 4.1.22

$$[d]_B = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}.$$

The characteristic polynomial $c_d(X)$ and the minimal polynomial $m_d(X)$ of $[d]_B$ were found using the computer algebra system SAGE [43] to be:

$$c_d(X) = m_d(X) = X(X^3 + X + 1). \quad (4.1)$$

Applying the Primary Decomposition Theorem 3.4.19 to d we can write the vector space $\mathbb{F}_2(C_2 \times C_2)$ as a direct sum of d -invariant subspaces. That is, $\mathbb{F}_2(C_2 \times C_2) = N_\infty \oplus R_\infty$, where $N_\infty = \ker(d)$ and $R_\infty = \ker(d^3 + d + I)$, where I is the identity map on $\mathbb{F}_2(C_2 \times C_2)$. Let d_N and d_R denote the restriction of d to N_∞ and R_∞ respectively.

We first look at N_∞ . $N_\infty = \ker(d)$ and so the nilpotency index of d_N is 1. Moreover, let $\alpha = a_01 + a_1x + a_2y + a_3xy \in \mathbb{F}_2(C_2 \times C_2)$. Then

$$\begin{aligned} d(\alpha) &= d(a_01 + a_1x + a_2y + a_3xy) = a_1(1 + y + xy) + a_2(xy) + a_3(1 + x) \\ &= (a_1 + a_3)(1) + a_3x + a_1y + (a_1 + a_2)xy. \end{aligned}$$

Therefore $d(\alpha) = 0$ if and only if $a_1 = a_2 = a_3 = 0$, that is, $d(\alpha) = 0$ if and only if $\alpha = 0$ or 1 . Thus the dimension of $N_\infty = \ker(d)$ is 1. This implies that the nilpotency index of d_N is equal to the dimension of N_∞ and so by Definition 4.1.24, d_N is a pure nilpotent map. Therefore by Theorem 4.2.2, the digraph of d_N , $\Gamma(d_N)$ is a tree of height 1 and terminal vertex 0. $\Gamma(d_N)$, the digraph of d_N is drawn in Figure 4.2.

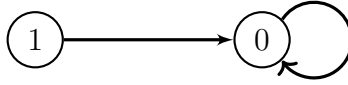


Figure 4.2: $\Gamma(d_N)$, the digraph of d_N

We now look at R_∞ . $R_\infty = \ker(d^3 + d + I)$ and so the minimal polynomial of d_R is $m_{d_R}(X) = X^3 + X + 1$. Neither 0 nor 1 is a root of $X^3 + X + 1$ and so $X^3 + X + 1$ is irreducible over \mathbb{F}_2 . Also $\text{ord}(X^3 + X + 1)$ was computed using SAGE [43] to be 7. Therefore by Theorem 4.2.6 the digraph of d_R is given by $\Gamma(d_R) = 1 + C_7$, where 1 is the loop at the node 0 and C_7 is a 7-cycle. $\Gamma(d_R)$, the digraph of d_R is drawn in Figure 4.3.

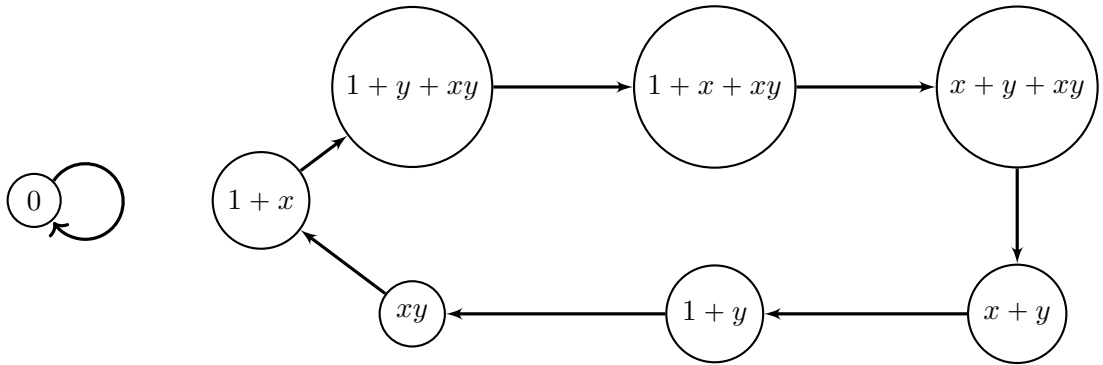


Figure 4.3: $\Gamma(d_R)$, the digraph of d_R

By Theorem 4.2.7 the digraph of the derivation d , $\Gamma(d)$ is the product of $\Gamma(d_R)$ with $\Gamma(d_N)$, that is, $\Gamma(d) = \Gamma(d_R) \times \Gamma(d_N)$ and is illustrated in Figure 4.4. The vertex (a, b) corresponds with the element $a + b$ of $\mathbb{F}_2(C_2 \times C_2)$.

4.3 Digraphs of the Derivations of \mathbb{F}_2C_4

In this section we look at the digraph of the elements of $\text{Der}(\mathbb{F}_2C_4)$. It is shown that none of the digraphs contain a cycle of length 7. Therefore the digraph $\Gamma(d)$ illustrated in Figure 4.4 is not isomorphic to the digraph of any element of $\text{Der}(\mathbb{F}_2C_4)$. The elements of $\text{Der}(\mathbb{F}_2C_4)$ are partitioned by conjugacy class and the associated

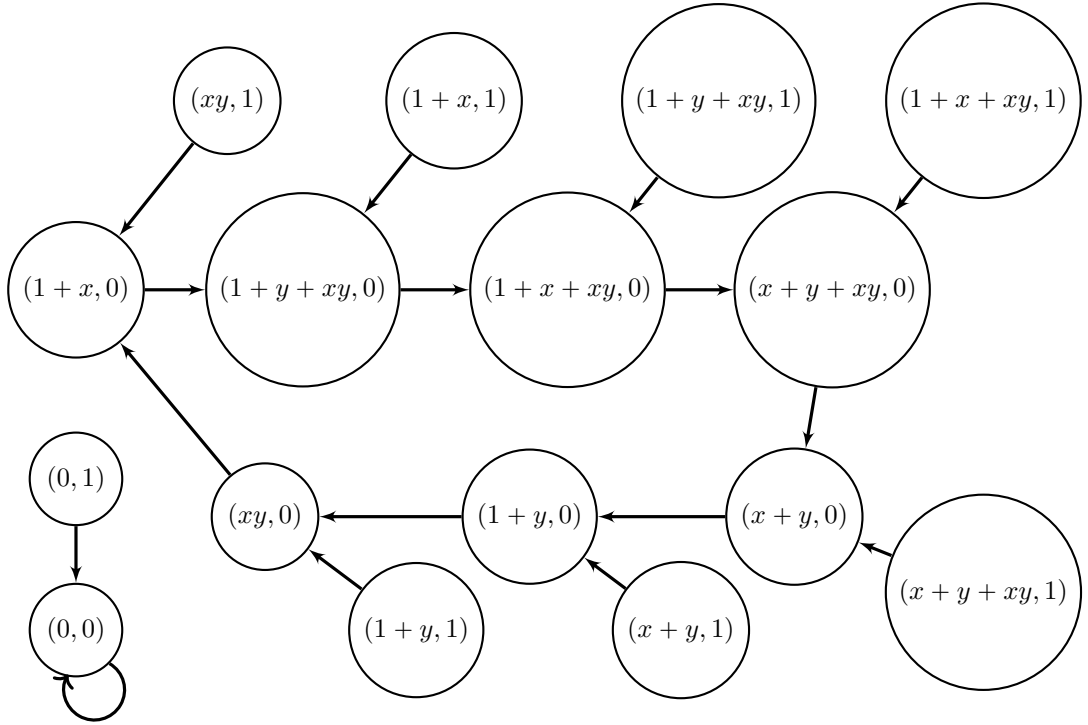


Figure 4.4: $\Gamma(d)$, the digraph of d

digraphs are drawn in Figures 4.5 - 4.10. Also, permutations of \mathbb{F}_2C_4 are exhibited such that conjugation by these permutations, maps any derivation of \mathbb{F}_2C_4 to any similar derivation of \mathbb{F}_2C_4 , that is the matrices representing the derivations are similar.

Example 4.3.1. Let $C_4 = \langle z \mid z^4 = 1 \rangle$. Let D be any derivation of \mathbb{F}_2C_4 and let $D(z) = a_01 + a_1z + a_2z^2 + a_3z^3$. Recall that for any derivation of a group algebra, $D(1) = 0$. D is an \mathbb{F}_2 -linear transformation and so we can represent D as a 4×4 matrix over \mathbb{F}_2 . For $i = 1, 2, 3, 4$, let v_i be the column vector of length 4 over \mathbb{F}_2 with a 1 in position i and a 0 in the other 3 positions. We use the following correspondence:

$$1 \leftrightarrow v_1 \quad z \leftrightarrow v_2 \quad z^2 \leftrightarrow v_3 \quad z^3 \leftrightarrow v_4.$$

Let $B = \{v_i \mid i = 1, 2, 3, 4\}$. Then B is a basis for the vector space \mathbb{F}_2^4 and so by

Definition 4.1.22

$$[D]_B = \begin{bmatrix} 0 & a_0 & 0 & a_2 \\ 0 & a_1 & 0 & a_3 \\ 0 & a_2 & 0 & a_0 \\ 0 & a_3 & 0 & a_1 \end{bmatrix}. \quad (4.2)$$

At least 2 of the 4 columns contain all zeros and so $\dim(N_\infty) \geq 2$, for all $D \in \text{Der}(\mathbb{F}_2C_4)$. Therefore by Theorem 3.4.15 $\dim(R_\infty) \leq 2$ and so there are not enough elements in R_∞ to form a 7-cycle. Therefore the digraph $\Gamma(D)$ cannot contain a 7-cycle for any $D \in \text{Der}(\mathbb{F}_2C_4)$. Let d be the derivation of $\mathbb{F}_2(C_2 \times C_2)$ defined in Example 4.2.8. Then $\Gamma(d)$ contains a 7-cycle and so it is not isomorphic to $\Gamma(D)$, for any $D \in \text{Der}(\mathbb{F}_2C_4)$. Therefore by Theorem 4.1.8, $\mathbb{F}_2(C_2 \times C_2)$ and \mathbb{F}_2C_4 are not isomorphic as rings.

Remark 4.3.2. Derivations and their associated digraphs have been used to show that two modular group algebras are not ring isomorphic. This has the potential to be a useful tool.

Definition 4.3.3. Let n be a positive integer and let A and B be $n \times n$ matrices over a field K . Then B is a *conjugate* of A , if there exists an invertible $n \times n$ matrix P over K , such that $B = P^{-1}AP$. The conjugacy classes partition the set of $n \times n$ matrices over a field K . Matrices that are in the same conjugacy class are called *similar*.

Remark 4.3.4. Let V be a finite dimensional vector space over a finite field K and let $f: V \rightarrow V$ be a K -linear map. Then f can be represented by a matrix over the field K which is dependant on the chosen basis. A change of basis matrix represents a bijective K -linear map and will induce an isomorphism of finite dynamical systems [23]. Thus by Remark 4.1.7 similar matrices have isomorphic associated digraphs.

Remark 4.3.5. Let G be a finite group of order n and K a finite field. Let $d \in \text{Der}(KG)$ and let P be a bijective K -linear map from KG to KG . Let B be a basis for the vector space K^n and define $[D]_B = [P^{-1}]_B[d]_B[P]_B$. By Remark 4.3.4 similar matrices have isomorphic associated digraphs. However, as Example 4.3.6 shows the matrix $[D]_B$ may not represent a derivation of KG , with respect to the basis B .

Example 4.3.6. Let $C_4 = \langle z \mid z^4 = 1 \rangle$ and let B be the basis for \mathbb{F}_2^4 as in Example 4.3.1. Moreover, let

$$M = \begin{bmatrix} 0 & a_0 & 0 & a_2 \\ 0 & a_1 & 0 & a_3 \\ 0 & a_2 & 0 & a_0 \\ 0 & a_3 & 0 & a_1 \end{bmatrix}, \quad [P]_B = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad [d]_B = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \quad \text{and} \quad [D]_B = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

where $a_i \in \mathbb{F}_2$ for $i = 0, 1, 2, 3$. By Equation 4.2 any derivation of \mathbb{F}_2C_4 is represented by the matrix M for some $a_i \in \mathbb{F}_2$. Note that d is the derivation of \mathbb{F}_2C_4 defined by $d(z) = z^3$. The matrix $[P^{-1}]_B[d]_B[P]_B$ was computed using SAGE [43] to be the matrix $[D]_B$ listed above. Note that $M \neq [D]_B$ for any $a_i \in \mathbb{F}_2$. Therefore $[D]_B$ does not represent a derivation of \mathbb{F}_2C_4 with respect to the basis B .

Remark 4.3.7. As stated in Example 4.3.6 any derivation of \mathbb{F}_2C_4 is represented by the matrix M for some $a_i \in \mathbb{F}_2$. The product of 2 such matrices is given by:

$$M_1M_2 = \begin{bmatrix} 0 & a_0 & 0 & a_2 \\ 0 & a_1 & 0 & a_3 \\ 0 & a_2 & 0 & a_0 \\ 0 & a_3 & 0 & a_1 \end{bmatrix} \begin{bmatrix} 0 & b_0 & 0 & b_2 \\ 0 & b_1 & 0 & b_3 \\ 0 & b_2 & 0 & b_0 \\ 0 & b_3 & 0 & b_1 \end{bmatrix} = \begin{bmatrix} 0 & a_0b_1 + a_2b_3 & 0 & a_0b_3 + a_2b_1 \\ 0 & a_1b_1 + a_3b_3 & 0 & a_1b_3 + a_3b_1 \\ 0 & a_0b_3 + a_2b_1 & 0 & a_0b_1 + a_2b_3 \\ 0 & a_1b_3 + a_3b_1 & 0 & a_1b_1 + a_3b_3 \end{bmatrix}.$$

The product M_1M_2 represents the derivation of \mathbb{F}_2C_4 defined by $z \mapsto (a_0b_1 + a_2b_3) + (a_1b_1 + a_3b_3)z + (a_0b_3 + a_2b_1)z^2 + (a_1b_3 + a_3b_1)z^3$. Therefore $\text{Der}(\mathbb{F}_2C_4)$ is closed

under composition. However as Example 4.3.8 shows, $Der(R)$ is not closed under composition for a general ring R . It would be interesting to find all KG such that $Der(KG)$ is closed under multiplication. In such cases $Der(KG)$ would form a K -algebra.

Example 4.3.8. Let $C_4 \times C_4 = \langle x, y \mid x^4 = y^4 = [x, y] = 1 \rangle$. Let ∂_x be the derivation of $\mathbb{F}_2(C_4 \times C_4)$ defined by $x \mapsto 1, y \mapsto 0$. Similarly Let ∂_y be the derivation of $\mathbb{F}_2(C_4 \times C_4)$ defined by $x \mapsto 0, y \mapsto 1$. Then

$$\begin{aligned}(\partial_x \circ \partial_y)(xy) &= \partial_x(x) = 1, \text{ and} \\(\partial_x \circ \partial_y)(x)y + x(\partial_x \circ \partial_y)(y) &= 0 + 0 = 0.\end{aligned}$$

Therefore $(\partial_x \circ \partial_y) \notin Der(\mathbb{F}_2(C_4 \times C_4))$, since it does not obey Leibniz's rule.

Remark 4.3.9. Let R be a unital ring. Then although $Der(R)$ is not closed under composition it does form a Lie algebra. This is the subject of Chapter 5.

Definition 4.3.10. Let n and m be positive integers and let p be a prime number. Denote by $M(n, p^m)$ the ring of $n \times n$ matrices over \mathbb{F}_{p^m} and by $GL(n, p^m)$ be the set of invertible elements of $M(n, p^m)$.

Definition 4.3.11. Let $A \in M(n, p^m)$. Define $C(A)$ to be the *centraliser* of A in $M(n, p^m)$. That is, $C(A) = \{M \in M(n, p^m) \mid MA = AM\}$.

Example 4.3.12. Let $C_4 = \langle z \mid z^4 = 1 \rangle$. By Theorem 2.3.4 a derivation of \mathbb{F}_2C_4 is defined by $d(z)$. We now consider conjugating the matrix representation of d by elements of $GL_4(\mathbb{F}_2)$. Table 4.1 shows the partition of $Der(\mathbb{F}_2C_4)$ according to conjugacy class. The contents of Table 4.1 were computed using SAGE [43].

Let $d \in Der(\mathbb{F}_2C_4)$. By Definition 4.3.11, $M^{-1}[d]_B M = [d]_B$, for all $M \in C([d]_B) \cap GL(4, 2)$. Moreover, let P be an element of $GL(4, 2)$, such that $P^{-1}[d]_B P = [D]_B$, for some $D \in Der(\mathbb{F}_2C_4)$. Then $(MP)^{-1}[d]_B(MP) = [D]_B$, for all

class	$d(z)$	$c_d(X)$	$m_d(X)$
1	0	X^4	X
2	$z^3, 1 + z^3, z^2 + z^3, 1 + z^2 + z^3$	$X^2(X + 1)^2$	$X(X + 1)^2$
3	$1, z^2$	X^4	X^2
4	$z, 1 + z, z + z^2, 1 + z + z^2$	$X^2(X + 1)^2$	$X(X + 1)$
5	$1 + z^2, z + z^3, 1 + z + z^2 + z^3$	X^4	X^2
6	$1 + z + z^3, z + z^2 + z^3$	X^4	X^3

Table 4.1: The elements of $Der(\mathbb{F}_2C_4)$ partitioned by conjugacy class

$M \in C([d]_B) \cap GL(4, 2)$. Let \mathcal{T} be a right transversal of $C([d]_B) \cap GL(4, 2)$ in $GL(4, 2)$. Then conjugating $[d]_B$ by an element of \mathcal{T} may not result in a matrix which represents a derivation with respect to the basis B . This was highlighted in Example 4.3.6. The non zero derivations of \mathbb{F}_2C_4 form 5 conjugacy classes. In Table 4.2 a representative $[d]$ is chosen for each of the 5 classes. For each representative and for every other derivation D in the same conjugacy class, a matrix P is given such that P conjugates $[d]$ to $[D]$.

The digraphs associated with the derivations in each conjugacy class are illustrated in Figures 4.5 - 4.10.

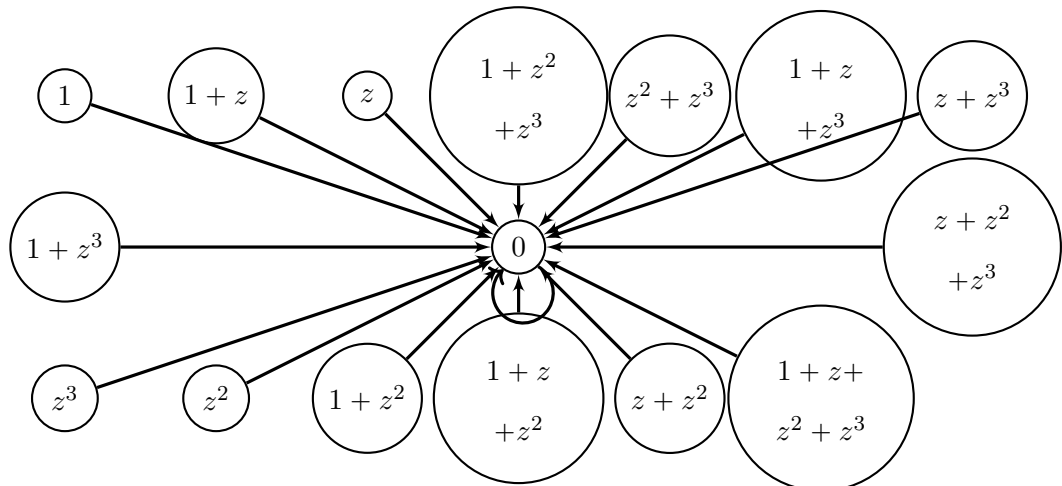


Figure 4.5: The digraph of the derivation in class 1 of Table 4.1

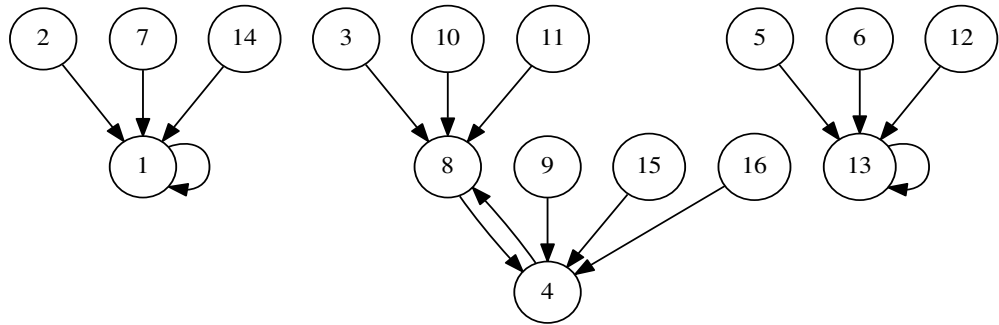


Figure 4.6: The digraph of the 4 derivations in class 2 of Table 4.1

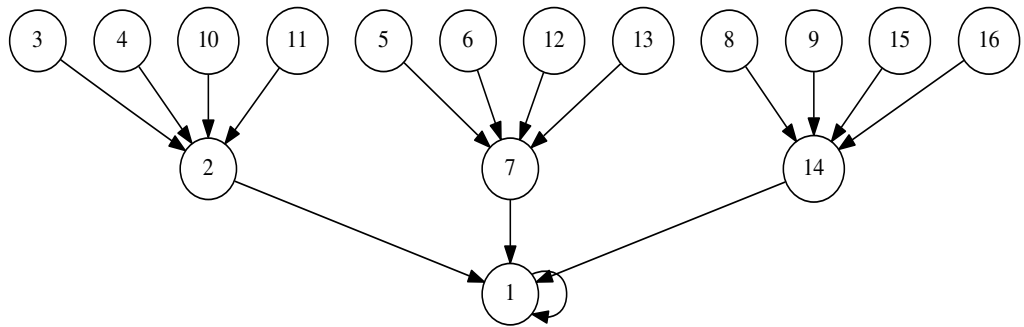


Figure 4.7: The digraph of the 2 derivations in class 3 of Table 4.1

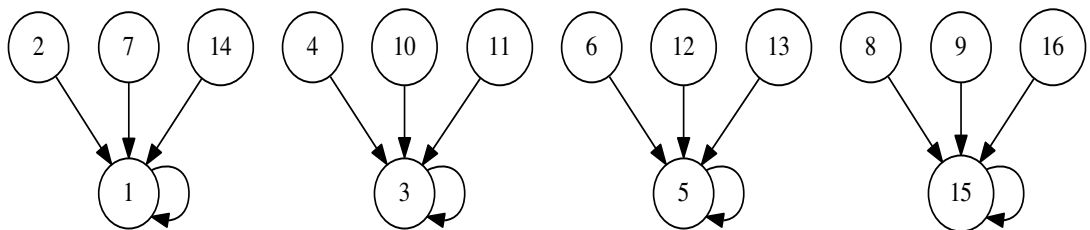


Figure 4.8: The digraph of the 4 derivations in class 4 of Table 4.1

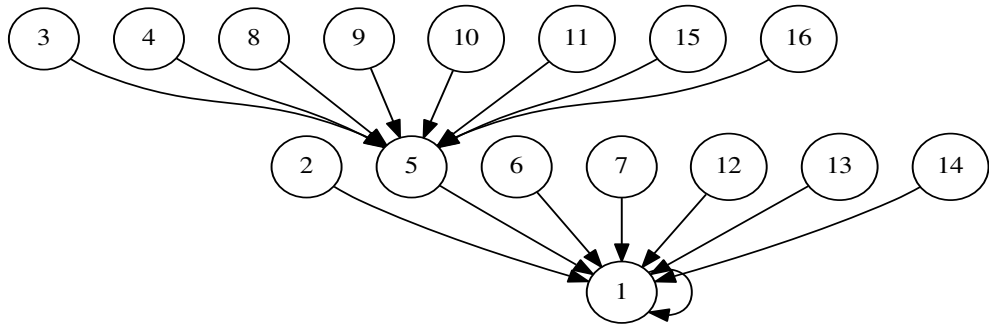


Figure 4.9: The digraph of the 3 derivations in class 5 of Table 4.1

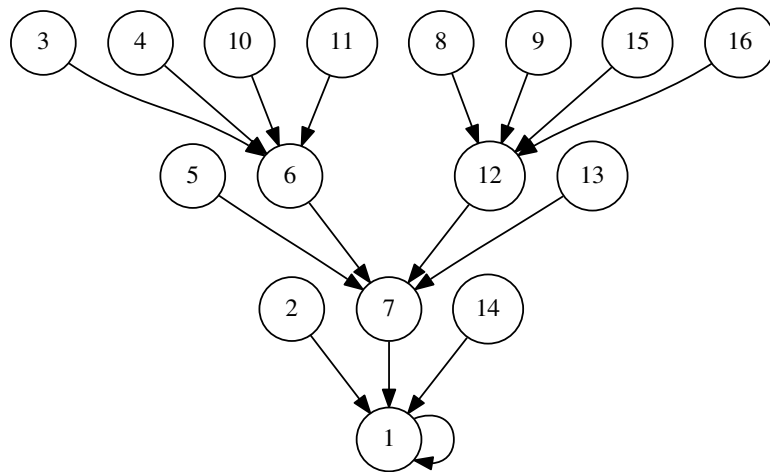


Figure 4.10: The digraph of the 2 derivations in class 6 of Table 4.1

Example 4.3.13. In Example 4.3.12 the graphs were computed using GAP [18]. In this example we show how the graphs of the derivations of \mathbb{F}_2C_4 defined by $d_{s,t}(z) = s + z + tz^2$, for $s, t \in \mathbb{F}_2$ can be determined using the Invariant Factor

Decomposition Algorithm [16, p. 480]. By Example 4.3.6

$$[d_{s,t}] = \begin{bmatrix} 0 & s & 0 & t \\ 0 & 1 & 0 & 0 \\ 0 & t & 0 & s \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Let $\mathbb{F}_2[x]$ be the polynomial ring over the indeterminate x and let I be the identity element of $M_4(\mathbb{F}_2)$, the full ring of 4×4 matrices over \mathbb{F}_2 . We now perform elementary row and column operations on $xI - [d_{s,t}]$ to transform $xI - [d_{s,t}]$ into the unique matrix of the form

$$\begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & f_1(x) & & \\ & & & & \ddots & \\ & & & & & f_m(x) \end{bmatrix}$$

such that $f_i(x) \in \mathbb{F}_2[x]$ for $i = 1, 2, \dots, m$ and $f_1(x) \mid f_2(x) \mid \dots \mid f_m(x)$.

$$\begin{aligned}
xI - [d_{s,t}] &= \begin{bmatrix} x & s & 0 & t \\ 0 & x+1 & 0 & 0 \\ 0 & t & x & s \\ 0 & 0 & 0 & x+1 \end{bmatrix} \xrightarrow{r_1+r_2+r_3 \mapsto r_2} \begin{bmatrix} x & s & 0 & t \\ x & x+s+t+1 & x & s+t \\ 0 & t & x & s \\ 0 & 0 & 0 & x+1 \end{bmatrix} \\
&\xrightarrow{c_2+c_3+c_4 \mapsto c_2} \begin{bmatrix} x & s+t & 0 & t \\ x & 1 & x & s+t \\ 0 & x+s+t & x & s \\ 0 & x+1 & 0 & x+1 \end{bmatrix} \xrightarrow{\substack{r_1 \leftrightarrow r_2 \\ c_1 \leftrightarrow c_2}} \begin{bmatrix} 1 & x & x & s+t \\ s+t & x & 0 & t \\ x+s+t & 0 & x & s \\ x+1 & 0 & 0 & x+1 \end{bmatrix} \xrightarrow{\substack{r_2+r_3 \mapsto r_3 \\ r_1+r_2+r_3+r_4 \mapsto r_4}} \\
&\begin{bmatrix} 1 & x & x & s+t \\ s+t & x & 0 & t \\ x & x & x & s+t \\ 0 & 0 & 0 & x+1 \end{bmatrix} \xrightarrow{\substack{(s+t)r_1+r_2 \mapsto r_2 \\ xr_1+r_3 \mapsto r_3}} \begin{bmatrix} 1 & x & x & s+t \\ 0 & (s+t+1)x & (s+t)x & s \\ 0 & x^2+x & x^2+x & (s+t)(x+1) \\ 0 & 0 & 0 & x+1 \end{bmatrix} \\
&\xrightarrow{c_2+c_3 \mapsto c_2} \begin{bmatrix} 1 & 0 & x & s+t \\ 0 & x & (s+t)x & s \\ 0 & 0 & x^2+x & (s+t)(x+1) \\ 0 & 0 & 0 & x+1 \end{bmatrix} \xrightarrow{\substack{r_2+r_4 \mapsto r_2 \\ c_2+c_4 \mapsto c_4}} \begin{bmatrix} 1 & 0 & x & s+t \\ 0 & x & (s+t)x & s+1 \\ 0 & 0 & x^2+x & (s+t)(x+1) \\ 0 & 0 & 0 & x+1 \end{bmatrix}.
\end{aligned}$$

Notice that the entries of the last 2 matrices are the same except for the entry in row 2 column 4, one of which is a 1 and the other a zero. Therefore we can transform $xI - [d_{s,t}]$ to

$$\begin{bmatrix} 1 & 0 & x & s+t \\ 0 & x & (s+t)x & 1 \\ 0 & 0 & x^2+x & (s+t)(x+1) \\ 0 & 0 & 0 & x+1 \end{bmatrix} \xrightarrow{\substack{c_4 \mapsto c_2, c_2 \mapsto c_3 \\ c_3 \mapsto c_4}} \begin{bmatrix} 1 & s+t & 0 & x \\ 0 & 1 & x & (s+t)x \\ 0 & (s+t)(x+1) & 0 & x^2+x \\ 0 & x+1 & 0 & 0 \end{bmatrix}$$

Note the entry in row 3 column 2. It is either 0 (if $s+t=0$) or performing the

row operation $r_3 + r_4 \mapsto r_3$ leaves the matrix unchanged except for changing the entry in row 3 column 2 to a 0. Therefore we can transform $xI - [d_{s,t}]$ to

$$\begin{aligned} & \begin{bmatrix} 1 & s+t & 0 & x \\ 0 & 1 & x & (s+t)x \\ 0 & 0 & 0 & x^2+x \\ 0 & x+1 & 0 & 0 \end{bmatrix} \xrightarrow{(x+1)r_2+r_4 \mapsto r_4} \begin{bmatrix} 1 & s+t & 0 & x \\ 0 & 1 & x & (s+t)x \\ 0 & 0 & 0 & x^2+x \\ 0 & 0 & x^2+x & (s+t)(x^2+x) \end{bmatrix} \\ & \xrightarrow{r_3 \leftrightarrow r_4} \begin{bmatrix} 1 & s+t & 0 & x \\ 0 & 1 & x & (s+t)x \\ 0 & 0 & x^2+x & (s+t)(x^2+x) \\ 0 & 0 & 0 & x^2+x \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x^2+x & 0 \\ 0 & 0 & 0 & x^2+x \end{bmatrix}. \end{aligned}$$

Therefore $f_1(x) = f_2(x) = x(x+1)$. The polynomials f_1 and f_2 are called the invariant factors of $[d_{s,t}]$. The elementary factors of $[d_{s,t}]$ are the set of factors of the invariant factors of $[d_{s,t}]$ [16, p. 494]. That is the set of elementary factors of $d_{s,t}$ is $\{x, x, (x+1), (x+1)\}$. $[d_{s,t}]$ has a Jordan form J , since the eigenvalues 0 and 1 are in the field. Therefore the Jordan blocks of J are $[0], [0], [1]$ and $[1]$. Thus by [23] the derivations $d_{s,t}$ are the derivations in class 4 of Example 4.3.12 and the graph associated with these derivations is illustrated in Figure 4.8.

Remark 4.3.14. The ring of constants of a unital ring R was defined in Definition 3.1.15. Let $C_4 = \langle z \mid z^4 = 1 \rangle$. Then the ring of constants of \mathbb{F}_2C_4 is given by $\mathcal{C}(\mathbb{F}_2C_4) = \{0, 1, z^2, 1 + z^2\}$.

Lemma 4.3.15. *Let $C_4 = \langle z \mid z^4 = 1 \rangle$ and let $c \in \mathcal{C}(\mathbb{F}_2C_4) = \{0, 1, z^2, 1 + z^2\}$. Furthermore, let $\rho_c: C_4 \rightarrow \mathbb{F}_2C_4$ be the map defined by $1 \mapsto 1$, $z \mapsto z + c$, $z^2 \mapsto z^2$ and $z^3 \mapsto z^2(z + c)$. Extend ρ_c , \mathbb{F}_2 -linearly to \mathbb{F}_2C_4 and denote this function also by ρ_c . Then*

- (i) ρ_c is a permutation of \mathbb{F}_2C_4 of order 2.

(ii) $\rho_c \circ d \circ \rho_c$ is a derivation of \mathbb{F}_2C_4 , where d is the derivation of \mathbb{F}_2C_4 defined by $d(z) = z$.

(iii) Every derivation of \mathbb{F}_2C_4 whose associated digraph is isomorphic to $\Gamma(d)$ is of the form $\rho_c \circ d \circ \rho_c$, for some $c \in \mathcal{C}(\mathbb{F}_2C_4)$.

Proof. (i) $\mathcal{C}(\mathbb{F}_2C_4)$ is the subspace of \mathbb{F}_2C_4 with basis $\{1, z^2\}$. ρ_c is the identity map on $\mathcal{C}(\mathbb{F}_2C_4)$, since it is an \mathbb{F}_2 -linear mapping which is the identity on a basis for $\mathcal{C}(\mathbb{F}_2C_4)$. Therefore $\rho_c(c) = c$ and $\rho_c(z^2c) = z^2c$. Thus

$$\begin{aligned}\rho_c^2(z) &= \rho_c(z + c) = \rho_c(z) + \rho_c(c) = z + c + c = z \text{ and} \\ \rho_c^2(z^3) &= \rho_c(z^2(z + c)) = \rho_c(z^3) + \rho_c(z^2c) = z^3 + z^2c + z^2c = z^3.\end{aligned}$$

Therefore ρ_c is a permutation of \mathbb{F}_2C_4 of order 2.

(ii) Let $D = \rho_c \circ d \circ \rho_c$. Then $D(z) = \rho_c \circ d \circ \rho_c(z) = \rho_c \circ d(z + c) = \rho_c(z) = z + c$. By Theorem 2.3.4 there is a unique derivation of \mathbb{F}_2C_4 which maps z to $z + c$. D is an \mathbb{F}_2 -linear map since it is the composition of \mathbb{F}_2 -linear maps. If $i \equiv 0 \pmod{2}$, then $D(z^i) = \rho_c \circ d \circ \rho_c(z^i) = \rho_c \circ d(z^i) = 0 = iz^{i-1}D(z)$. If $i \equiv 1 \pmod{2}$, then $D(z^i) = \rho_c \circ d \circ \rho_c(z^i) = \rho_c \circ d(z^i + z^{i-1}c) = \rho_c(z^i) = z^{i-1}(z + c) = iz^{i-1}D(z)$. Therefore $D(z^{i+j}) = (i + j)z^{i+j-1}D(z) = iz^{i-1}D(z)z^j + z^i j z^{j-1}D(z) = D(z^i)z^j + z^i D(z^j)$, for all integers i and j . Let $\alpha = \sum_{i=0}^3 a_i z^i$ and $\beta = \sum_{i=0}^3 b_i z^i$. Then

$$D(\alpha\beta) = \sum_{i=0}^3 \sum_{j=0}^3 a_i b_j D(z^{i+j}) = \sum_{i=0}^3 \sum_{j=0}^3 a_i b_j (D(z^i)z^j + z^i D(z^j)) = D(\alpha)\beta + \alpha D(\beta).$$

Therefore D is the unique derivation of \mathbb{F}_2C_4 which maps z to $z + c$.

(iii) The derivations of \mathbb{F}_2C_4 that have an associated digraph isomorphic to $\Gamma(d)$ are the 4 derivations of class 4 in Table 4.1. They are the derivations $\rho_c \circ d \circ \rho_c$ for $c \in \mathcal{C}(\mathbb{F}_2C_4)$. In Table 4.2, on the first row of class 4 the matrix P_1 represents ρ_{z^2} and P_2 represents ρ_1 . The matrix P_1 on the second row represents ρ_{1+z^2} . \square

Remark 4.3.16. Similarly it can be shown that conjugation by ρ_c permutes the derivations of class 2 of Table 4.1.

Lemma 4.3.17. *Let $C_4 = \langle z \mid z^4 = 1 \rangle$ and let $\rho: C_4 \rightarrow \mathbb{F}_2C_4$ be the map defined by $1 \mapsto 1$, $z \mapsto z^3$, $z^2 \mapsto z^2$ and $z^3 \mapsto z$. Extend ρ \mathbb{F}_2 -linearly to \mathbb{F}_2C_4 and denote this function also by ρ . Then ρ is a permutation of \mathbb{F}_2C_4 of order 2 and for $k \in \mathbb{F}_2$, conjugation by ρ permutes the derivations d and δ of \mathbb{F}_2C_4 , defined by $d(z) = 1 + k\hat{z}$ and $\delta(z) = z^2 + k\hat{z}$.*

Proof. ρ^2 is the identity map on \mathbb{F}_2C_4 , since it is an \mathbb{F}_2 -linear map that is the identity map on a basis for \mathbb{F}_2C_4 , namely the elements of the group C_4 . Therefore ρ is a permutation of \mathbb{F}_2C_4 of order 2.

Let $k \in \mathbb{F}_2$, let d be the derivation of \mathbb{F}_2C_4 defined by $d(z) = 1 + k\hat{z}$ and let $D = \rho \circ d \circ \rho$. We will now show that $D = \delta$, by showing that D is an \mathbb{F}_2 -linear map that agrees with δ on a basis for \mathbb{F}_2C_4 , namely C_4 . D is an \mathbb{F}_2 -linear map since it is the composition of \mathbb{F}_2 -linear maps. Note that $\rho(k\hat{z}) = k\hat{z}$ and so

$$\begin{aligned} \text{for } i \equiv 0 \pmod{2}, \quad D(z^i) &= \rho \circ d \circ \rho(z^i) = \rho \circ d(z^i) = 0 = iz^{i-1}(z^2 + k\hat{z}) = \delta(z^i) \\ \text{and for } i \equiv 1 \pmod{2}, \quad D(z^i) &= \rho \circ d \circ \rho(z^i) = \rho \circ d(z^{i+2}) = \rho((i+2)z^{i+1}(1 + k\hat{z})) \\ &= \rho(z^{i+1}(1 + k\hat{z})) = \rho(z^{i+1} + k\hat{z}) = z^{i+1} + k\hat{z} = z^{i-1}(z^2 + k\hat{z}) = iz^{i-1}\delta(z) = \delta(z^i). \end{aligned}$$

Therefore $D = \rho \circ d \circ \rho = \delta$, the unique derivation of \mathbb{F}_2C_4 which maps z to $z^2 + k\hat{z}$. This implies that $d = \rho \circ \delta \circ \rho$. Therefore conjugation by ρ permutes the derivations d and δ of \mathbb{F}_2C_4 . \square

Lemma 4.3.18. *Let $C_4 = \langle z \mid z^4 = 1 \rangle$ and let $\psi: C_4 \rightarrow \mathbb{F}_2C_4$ be the map defined by $1 \mapsto 1 + z + z^3$, $z \mapsto z^3$, $z^2 \mapsto 1$ and $z^3 \mapsto 1 + z + z^2$. Extend ψ , \mathbb{F}_2 -linearly to \mathbb{F}_2C_4 and denote this function also by ψ . Let d, D and δ be the derivations of \mathbb{F}_2C_4 defined by $d(z) = 1 + z^2$, $D(z) = z + z^3$ and $\delta(z) = \hat{z}$. Then ψ is a permutation of \mathbb{F}_2C_4 of order 3. Moreover, $D = \psi \circ d \circ \psi^2$ and $\delta = \psi^2 \circ d \circ \psi$.*

Proof. The proof follows along the same lines as those of Lemmas 4.3.15 and 4.3.17 and is omitted. \square

Remark 4.3.19. The conjugacy classes of the derivations of \mathbb{F}_2C_4 are given in Table 4.1. In Table 4.2 classes 2 and 4 have the same 3 permutation matrices P_1 and P_2 (note that there are 2 P_1 matrices as there are 2 rows in the table for these classes). These matrices represent ρ_c , where $c \in z^2, 1, 1 + z^2$. Therefore the maps ρ_c of Lemma 4.3.15 permute the derivations of Class 2 and 4 by conjugation. The map ρ of Lemma 4.3.17 permute the derivations of Class 3 and 6 by conjugation. The maps ψ and ψ^2 of Lemma 4.3.18 permute the derivations of Class 5 by conjugation. Therefore conjugation by these maps gives a way of permuting any pair of similar derivations of \mathbb{F}_2C_4 .

4.4 Permutations of Derivations

By Theorem 3.1.20, conjugation by $\theta \in \text{Aut}(KG)$ is a permutation on $\text{Der}(KG)$. The converse of this statement is not true. If conjugation by a map $\theta: KG \rightarrow KG$ permutes $\text{Der}(KG)$, then θ does not have to be an algebra automorphism of KG . The permutations ρ_c of Lemma 4.3.15 are not additive and so are not algebra automorphisms of \mathbb{F}_2C_4 . Example 4.4.2 presents another interesting example of a map $\theta \notin \text{Aut}(KG)$ such that conjugation by θ permutes $\text{Der}(KG)$.

Definition 4.4.1. An *involution* is defined to be an anti-automorphism of order 2 of a ring. Let θ be an involution on the group algebra KG . Then for $\alpha, \beta \in KG$

1. $\theta(\alpha + \beta) = \theta(\alpha) + \theta(\beta)$,
2. $\theta(\theta(\alpha)) = \alpha$,
3. $\theta(\alpha\beta) = \theta(\beta)\theta(\alpha)$.

Example 4.4.2. Let K be a finite field and G a finite non commutative group. Further, let θ be an involution of the group algebra KG and let g_1 and g_2 be non commuting elements of G . Then since θ is bijective, $\theta(g_1g_2) \neq \theta(g_2g_1)$ and so $\theta(g_2)\theta(g_1) \neq \theta(g_1)\theta(g_2)$. Therefore θ is not an automorphism of KG since $\theta(g_1g_2) = \theta(g_2)\theta(g_1) \neq \theta(g_1)\theta(g_2) = \theta(g_2g_1)$. We now show that $D = \theta^{-1} \circ d \circ \theta$ is a derivation of KG whenever d is a derivation of KG . Let $d \in \text{Der}(KG)$ and $\alpha, \beta \in KG$. Write $\alpha = \sum_{g \in G} a_g g$ and $\beta = \sum_{h \in G} b_h h$. Then since $\theta^{-1} = \theta$,

$$\begin{aligned} D(\alpha\beta) &= \theta \circ d \circ \theta(\alpha\beta) = \theta \circ d(\theta(\beta)\theta(\alpha)) = \theta\left(d(\theta(\beta))\theta(\alpha) + \theta(\beta)d(\theta(\alpha))\right) \\ &= \theta\left(d(\theta(\beta))\theta(\alpha)\right) + \theta\left(\theta(\beta)d(\theta(\alpha))\right) \\ &= \theta^2(\alpha)(\theta \circ d \circ \theta(\beta)) + (\theta \circ d \circ \theta(\alpha))\theta^2(\beta) = \alpha D(\beta) + D(\alpha)\beta. \end{aligned}$$

Therefore D is a derivation of KG . We have shown that conjugation by an involution θ is a permutation on $\text{Der}(KG)$ and $\theta \notin \text{Aut}(KG)$.

In particular, the classical involution θ of KG , defined by $\sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g g^{-1}$ is an example of an involution. θ does permute $\text{Der}(KG)$, however in the case when KG is not commutative it is not an element of $\text{Aut}(KG)$.

4.5 Automorphisms of Small Group Algebras

Lemma 4.5.1. Let $KG = \mathbb{F}_2(C_2 \times C_2)$, where $C_2 \times C_2 = \langle x, y \mid x^2 = y^2 = [x, y] = 1 \rangle$. Let $\theta_{(a,i,b,j)}: KG \rightarrow KG$ be the \mathbb{F}_2 -linear extension of the map from G into KG defined by

$$1 \mapsto 1, \quad x \mapsto a + i\hat{G}, \quad y \mapsto b + j\hat{G} \quad \text{and} \quad xy \mapsto ab + (i + j)\hat{G},$$

where $a \in \{x, y, xy\}$, $b \in \{x, y, xy\} \setminus \{a\}$ and $i, j \in \mathbb{F}_2$. Then $\theta_{(a,i,b,j)}$ are the automorphisms of KG and $\text{Aut}(KG) \simeq S_4$, the symmetric group on 4 objects.

Proof. Let $\mathcal{U}(KG)$ denote the unit group of KG . Then any automorphism of KG is an \mathbb{F}_2 -linear extension of a map from G into $\mathcal{U}(KG)$, such that $0 \mapsto 0$ and $1 \mapsto 1$. The units of KG are the elements of augmentation 1 and so $\{1, x, y, xy, 1 + \hat{G}, x + \hat{G}, y + \hat{G}, xy + \hat{G}\}$ is the set of elements of $\mathcal{U}(KG)$. Let θ be an automorphism of KG . Then θ is an \mathbb{F}_2 -linear extension of a map defined by

$$1 \mapsto 1, \quad x \mapsto u, \quad y \mapsto v \quad \text{and} \quad xy \mapsto uv,$$

where $u, v \in \mathcal{U}(KG)$. However θ is a bijection and so $u \neq 1$, $v \neq 1$ and $u \neq v$. Therefore write $u = 1 + z_1$ and $v = 1 + z_2$, where z_1 and z_2 are distinct elements of $\Delta(G) \setminus \{0\}$. Therefore

$$\theta(\hat{G}) = \theta(1) + \theta(x) + \theta(y) + \theta(xy) = 1 + 1 + z_1 + 1 + z_2 + (1 + z_1)(1 + z_2) = z_1 z_2.$$

$\theta(\hat{G}) \neq 0$, since $\theta(0) = 0$. $\hat{G} \in \text{ann}(\Delta(G))$ and $z^2 = 0$, for all $z \in \Delta(G)$. Thus $z_1 \neq \hat{G}$, $z_2 \neq \hat{G}$ and $z_2 \neq z_1 + \hat{G}$. This implies that $u = a + i\hat{G}$ and $v = b + j\hat{G}$, for some $a \in \{x, y, xy\}$, $b \in \{x, y, xy\} \setminus \{a\}$ and $i, j \in \mathbb{F}_2$ and so $\theta = \theta_{(a,i,b,j)}$.

Note that $\theta(\hat{G}) = \hat{G}$, since for some $g, h \in G$ such that $g \neq h$ and $i, j \in \mathbb{F}_2$,

$$\begin{aligned} z_1 z_2 &= (1 + u)(1 + v) = (1 + g + i\hat{G})(1 + h + j\hat{G}) \\ &= 1 + h + j\hat{G} + g + gh + j\hat{G} + i\hat{G} + i\hat{G} + 0 = 1 + g + h + gh = \hat{G}. \end{aligned}$$

Let $a \in \{x, y, xy\}$, $b \in \{x, y, xy\} \setminus \{a\}$ and $i, j \in \mathbb{F}_2$ and let $\theta = \theta_{(a,i,b,j)}$. We now show that $\theta \in \text{Aut}(KG)$. Let ϵ be the augmentation map of KG . Then $\epsilon(\alpha) = \alpha^2$, for any $\alpha \in KG$. Moreover, KG is commutative and so $\theta(gh) = \theta(g)\theta(h)$, for any

$g, h \in G$. Let $\alpha, \beta \in KG$ and write $\alpha = \sum_{g \in G} a_g g$ and $\beta = \sum_{h \in G} b_h h$. Then

$$\begin{aligned} \theta(\alpha\beta) &= \theta\left(\sum_{g \in G} \sum_{h \in G} a_g b_h gh\right) = \sum_{g \in G} \sum_{h \in G} a_g b_h \theta(gh) \\ &= \sum_{g \in G} \sum_{h \in G} a_g b_h \theta(g)\theta(h) = \sum_{g \in G} a_g \theta(g) \sum_{h \in G} b_h \theta(h) = \theta(\alpha)\theta(\beta). \end{aligned}$$

Therefore θ is an algebra endomorphism.

We will now show that θ is invertible and has order less than or equal to 4.

Recall that $\theta(\hat{G}) = \hat{G}$. There are 2 cases which we shall treat separately.

Case 1. $a \neq x$, $b \neq y$ and $ab \neq xy$.

There are 2 subcases. The first is $a = y$ and the second is $a = xy$.

Case 1(a). Let $a = y$ and $i, j \in \mathbb{F}_2$. Then $b = xy$, since $b \neq y$ and if $b = x$, then $ab = xy$. The order of $\theta_{(a,i,b,j)}$ is 3, since

$$\begin{aligned} \theta_{(a,i,b,j)}^3(x) &= \theta_{(a,i,b,j)}^2(y + i\hat{G}) = \theta_{(a,i,b,j)}(xy + (i+j)\hat{G}) = ab = x \text{ and} \\ \theta_{(a,i,b,j)}^3(y) &= \theta_{(a,i,b,j)}^2(xy + j\hat{G}) = \theta_{(a,i,b,j)}(x + i\hat{G}) = y. \end{aligned}$$

Case 1(b). $a = xy$ and $i, j \in \mathbb{F}_2$. Then $b = x$, since $b \neq y$. The order of $\theta_{(a,i,b,j)}$ is 3, since

$$\begin{aligned} \theta_{(a,i,b,j)}^3(x) &= \theta_{(a,i,b,j)}^2(xy + i\hat{G}) = \theta_{(a,i,b,j)}(y + j\hat{G}) = x \text{ and} \\ \theta_{(a,i,b,j)}^3(y) &= \theta_{(a,i,b,j)}^2(x + j\hat{G}) = \theta_{(a,i,b,j)}(xy + (i+j)\hat{G}) = y. \end{aligned}$$

Therefore the order of $\theta_{(a,i,b,j)}$ is 3 in Case 1.

Case 2. Either $a = x$ or $b = y$ or $ab = xy$.

Case 2(a) $a = x$: Then $\theta_{(a,i,b,j)}^2(x) = \theta_{(a,i,b,j)}(x + i\hat{G}) = x$.

Case 2(b) $a \neq x$ and $b = y$: Thus $a = xy$ and so $ab = x$. Therefore $\theta_{(a,i,b,j)}^2(x) = \theta_{(a,i,b,j)}(xy + i\hat{G}) = x + j\hat{G}$.

Case 2(c) $a \neq x$, $b \neq y$ and $ab = xy$: Thus $a = y$ and $b = x$. Therefore $\theta_{(a,i,b,j)}^2(x) =$

$$\theta_{(a,i,b,j)}(y + i\hat{G}) = x + (i + j)\hat{G}.$$

Therefore $\theta_{(a,i,b,j)}^2(x) = x + l\hat{G}$, for some $l \in \mathbb{F}_2$. Likewise it can be shown that $\theta_{(a,i,b,j)}^2(y) = y + m\hat{G}$, for some $m \in \mathbb{F}_2$ and so $\theta_{(a,i,b,j)}^4$ is the identity map.

Therefore $\theta_{(a,i,b,j)}$ is invertible and thus is an automorphism of KG . There are 6 elements $a + i\hat{G}$ and 4 elements $b + j\hat{G}$, where $a \in \{x, y, xy\}$, $b \in \{x, y, xy\} \setminus \{a\}$ and $i, j \in \mathbb{F}_2$. Thus $Aut(KG)$ is a group of order 24 such that the maximum order of an element is 4. Therefore $Aut(KG) \simeq S_4$, the symmetric group on 4 objects [18]. \square

Example 4.5.2. Let $KG = \mathbb{F}_2(C_2 \times C_2)$, where $C_2 \times C_2 = \langle x, y \mid x^2 = y^2 = [x, y] = 1 \rangle$. There are 2^8 derivations of KG by Theorem 2.3.4. Theorem 3.1.20 implies that the elements of $Aut(KG)$ permute the derivations of KG by conjugation. In this example, the graph isomorphism classes of the derivations of KG are determined and categorised by preperiod length. Let d be a derivation of KG and let $m_d(X) = X^m f(X)$, where $f(0) \neq 0$ be the minimal polynomial of d . Then the preperiod of d is m [23]. The 2^8 derivations of KG are partitioned into subsets via conjugation by automorphisms of KG . The associated digraph of a representative of each subset is also determined. [43] was used to perform these computations and the results are summarised in Table 4.3.

class	representative	pper	class	$c_d(X)$	$m_d(X)$
1	0	1	1	X^4	X
2	$xy\partial_y$	1	36	$X^2(X+1)^2$	$X(X+1)^2$
3	$y\partial_y$	1	28	$X^2(X+1)^2$	$X(X+1)$
4	$xy\partial_x + y\partial_y$	1	56	$X(X+1)(X^2+X+1)$	$X(X+1)(X^2+X+1)$
5	$xy\partial_x + (y+xy)\partial_y$	1	24	$X(X^3+X+1)$	$X(X^3+X+1)$
6	$(y+xy)\partial_y$	2	9	X^4	X^2
7	$x\partial_y$	2	12	X^4	X^2
8	$xy\partial_x + x\partial_y$	2	48	$X^2(X+1)^2$	$X^2(X+1)^2$
9	$(x+y+xy)\partial_y$	3	18	X^4	X^3
10	$y\partial_x + \partial_y$	4	24	X^4	X^4

Table 4.3: The conjugacy classes of the derivations of $\mathbb{F}_2(C_2 \times C_2)$

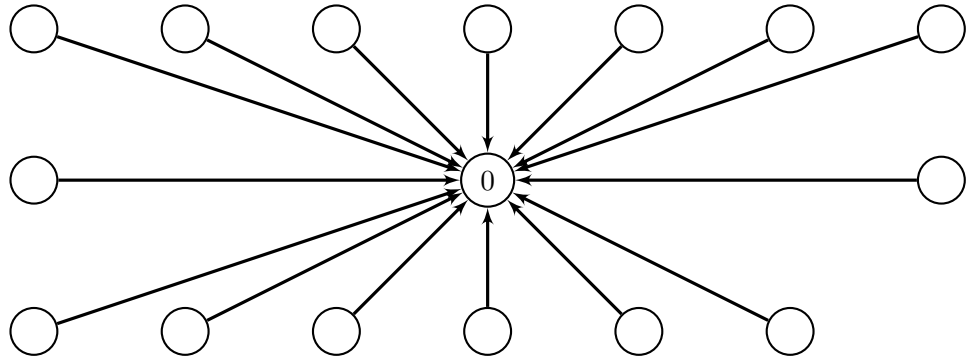


Figure 4.11: The digraph of the derivation in class 1 of Table 4.3

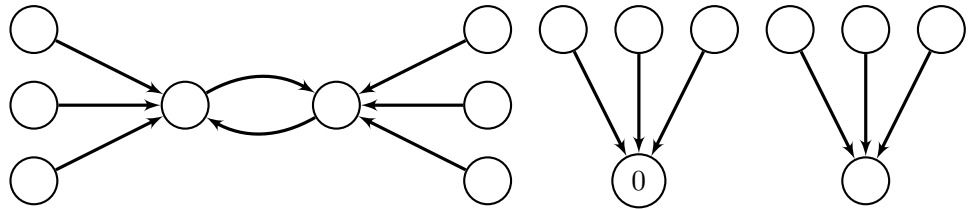


Figure 4.12: The digraph of the derivations in class 2 of Table 4.3

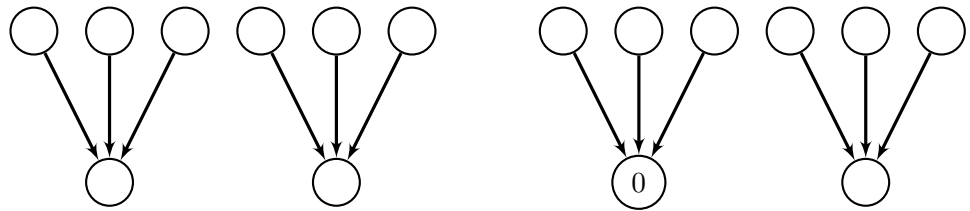


Figure 4.13: The digraph of the derivations in class 3 of Table 4.3

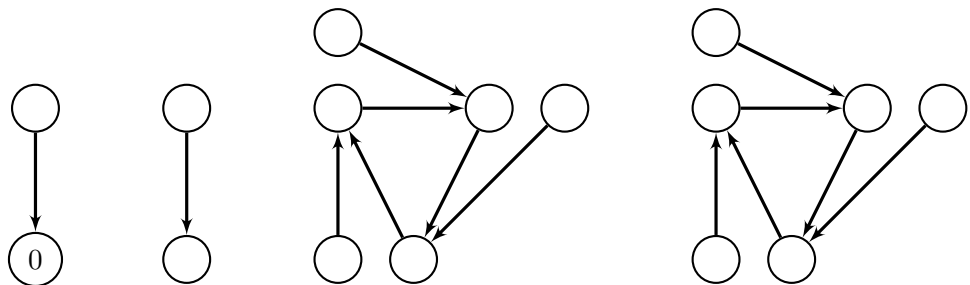


Figure 4.14: The digraph of the derivations in class 4 of Table 4.3

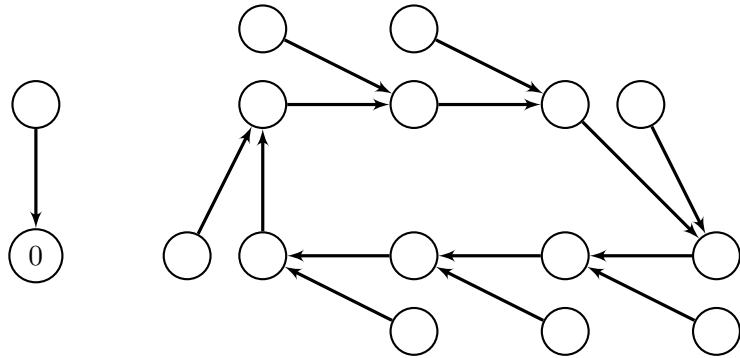


Figure 4.15: The digraph of the derivations in class 5 of Table 4.3

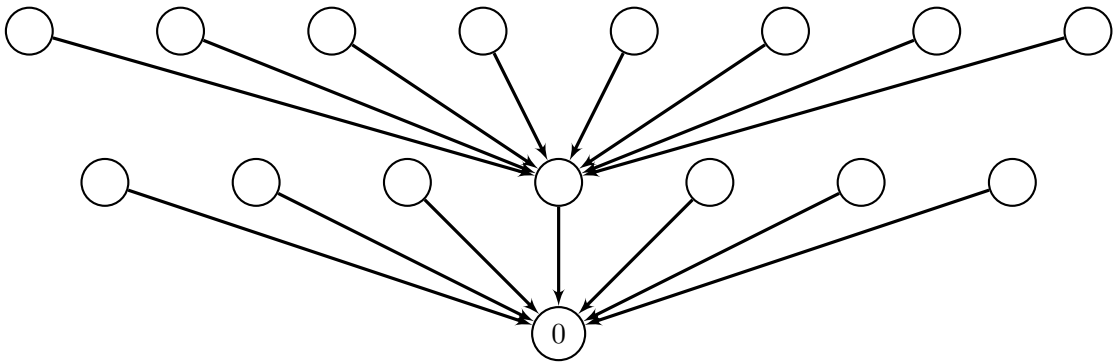


Figure 4.16: The digraph of the derivations in class 6 of Table 4.3

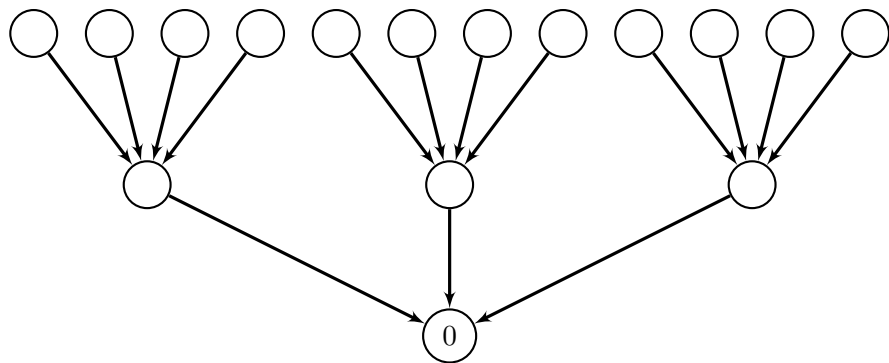


Figure 4.17: The digraph of the derivations in class 7 of Table 4.3

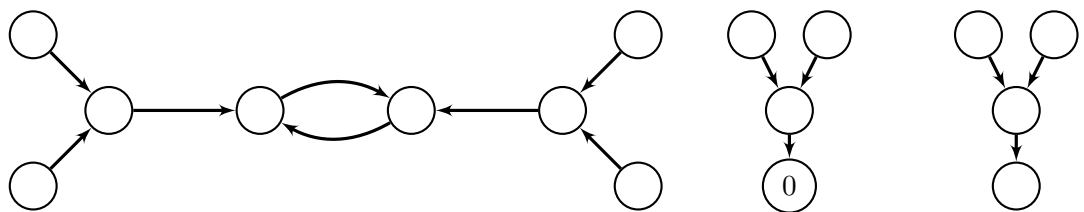


Figure 4.18: The digraph of the derivations in class 8 of Table 4.3

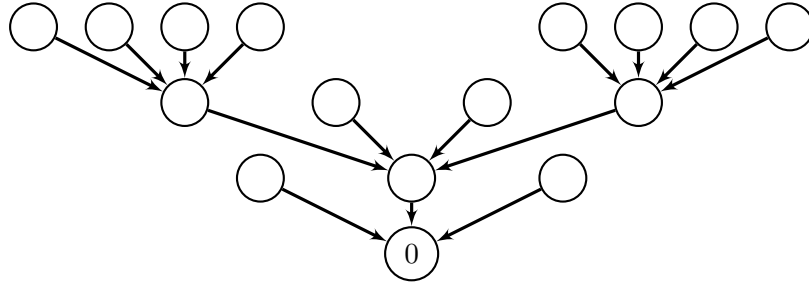


Figure 4.19: The digraph of the derivations in class 9 of Table 4.3

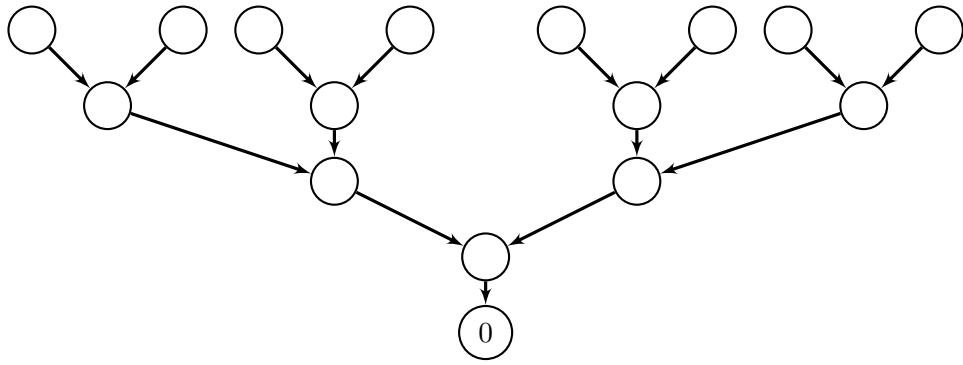


Figure 4.20: The digraph of the derivations in class 10 of Table 4.3

It can be seen from Figures 4.11 - 4.20, that $\text{per}(\text{Der}(\mathbb{F}_2(C_2 \times C_2))) = 7$ and $\text{pper}(\text{Der}(\mathbb{F}_2(C_2 \times C_2))) = 4$.

Lemma 4.5.3. *Let $KG = \mathbb{F}_2(C_4 \times C_4)$, where $C_4 \times C_4 = \langle x, y \mid x^4 = y^4 = [x, y] = 1 \rangle$. Then $B = \{(1+x^2), x(1+x^2), y(1+x^2), xy(1+x^2), (1+y^2), x(1+y^2), y(1+y^2), xy(1+y^2), (1+x^2)(1+y^2), x(1+x^2)(1+y^2), y(1+x^2)(1+y^2), xy(1+x^2)(1+y^2)\}$ is a basis for the kernel of the Frobenius endomorphism ψ of $\mathbb{F}_2(C_4 \times C_4)$. Moreover, as vector spaces, $KG = V \oplus \ker \psi$, where V is the \mathbb{F}_2 -linear span of $\{1, x, y, xy\}$.*

Proof. Let $\psi: \mathbb{F}_2(C_4 \times C_4) \rightarrow \mathbb{F}_2(C_4 \times C_4)$ be the Frobenius endomorphism defined by $\psi(\alpha) = \alpha^2$. Write $\alpha = \sum_{i=0}^3 \sum_{j=0}^3 a_{i,j} x^i y^j$. Then

$$\alpha^2 = \sum_{i \in \{0,2\}} \sum_{j \in \{0,2\}} a_{i,j} + \sum_{i \in \{1,3\}} \sum_{j \in \{0,2\}} a_{i,j} x^2 + \sum_{i \in \{0,2\}} \sum_{j \in \{1,3\}} a_{i,j} y^2 + \sum_{i \in \{1,3\}} \sum_{j \in \{1,3\}} a_{i,j} x^2 y^2.$$

This implies that $\alpha^2 = 0$ if and only if

$$\sum_{i \in \{0,2\}} \sum_{j \in \{0,2\}} a_{i,j} = 0, \quad \sum_{i \in \{1,3\}} \sum_{j \in \{0,2\}} a_{i,j} = 0, \quad \sum_{i \in \{0,2\}} \sum_{j \in \{1,3\}} a_{i,j} = 0 \quad \text{and} \quad \sum_{i \in \{1,3\}} \sum_{j \in \{1,3\}} a_{i,j} = 0.$$

Therefore $\ker(\psi)$ has dimension equal to 12.

Let $B = \{(1+x^2), x(1+x^2), y(1+x^2), xy(1+x^2), (1+y^2), x(1+y^2), y(1+y^2), xy(1+y^2), (1+x^2)(1+y^2), x(1+x^2)(1+y^2), y(1+x^2)(1+y^2), xy(1+x^2)(1+y^2)\}$. $b^2 = 0$ for all $b \in B$ and so the \mathbb{F}_2 -linear span of B is contained in $\ker(\psi)$. Let b_i be the i^{th} element of B in the above listing. Assume that $\gamma = \sum_{i=1}^{12} k_i b_i = 0$ for some $k_i \in \mathbb{F}_2$.

$x^2 y^2 \in \text{supp}(b_j) \iff j = 9$, $x^3 y^2 \in \text{supp}(b_j) \iff j = 10$, $x^2 y^3 \in \text{supp}(b_j) \iff j = 11$ and $x^3 y^3 \in \text{supp}(b_j) \iff j = 12$. Therefore $k_9 = k_{10} = k_{11} = k_{12} = 0$ and so it can be assumed that $\gamma = \sum_{i=1}^8 k_i b_i = 0$.

$y^2 \in \text{supp}(\gamma) \iff k_5 = 1$, $xy^2 \in \text{supp}(\gamma) \iff k_6 = 1$, $y^3 \in \text{supp}(\gamma) \iff k_7 = 1$ and $xy^3 \in \text{supp}(\gamma) \iff k_8 = 1$. Therefore $k_5 = k_6 = k_7 = k_8 = 0$ and so it can be assumed that $\gamma = \sum_{i=1}^4 k_i b_i = 0$.

$1 \in \text{supp}(\gamma) \iff k_1 = 1$, $x \in \text{supp}(\gamma) \iff k_2 = 1$, $y \in \text{supp}(\gamma) \iff k_3 = 1$ and $xy \in \text{supp}(\gamma) \iff k_4 = 1$. Therefore $k_1 = k_2 = k_3 = k_4 = 0$ and so $\sum_{i=1}^{12} k_i b_i = 0$ if and only if $k_i = 0$ for $i = 1, 2, \dots, 12$.

Therefore B is a linearly independent set of elements of $\ker(\psi)$ of size 12 and so B is a basis for $\ker(\psi)$.

Let $B_2 = \{1, x, y, xy\}$. $B_2 \subset G$ and so B_2 is a linearly independent set. Denote by V the \mathbb{F}_2 -linear span of B_2 . Let $v \in V$ and write $v = c_1 1 + c_2 x + c_3 y + c_4 xy$, where $c_i \in \mathbb{F}_2$. Then $v^2 = c_1 1 + c_2 x^2 + c_3 y^2 + c_4 x^2 y^2$ and so $v \in \ker(\psi)$ if and only if $c_i = 0$ for $i = 1, 2, 3$ and 4. Therefore extending B by the set $\{1, x, y, xy\}$ gives a basis for KG and so as vector spaces, $KG = V \oplus \ker \psi$. \square

Corollary 4.5.4. *Let $KG = \mathbb{F}_2(C_4 \times C_4)$, where $C_4 \times C_4 = \langle x, y \mid x^4 = y^4 = [x, y] = 1 \rangle$ and let $w = 1 + x + y + xy$. Let $\psi: \mathbb{F}_2(C_4 \times C_4) \rightarrow \mathbb{F}_2(C_4 \times C_4)$ be the Frobenius endomorphism defined by $\psi(\alpha) = \alpha^2$. Then $\text{ann}(w^2) = \ker \psi$.*

Proof. Let V be the \mathbb{F}_2 -linear span of $\{1, x, y, xy\}$. By Lemma 4.5.3 any element α of KG can be written as $v_1 + v_2(1 + x^2) + v_3(1 + y^2) + v_4(1 + x^2)(1 + y^2)$, where $v_i \in V$ for $i = 1, 2, 3$ and 4 . Let $v_1 = c_11 + c_2x + c_3y + c_4xy$. Then $\alpha w^2 = v_1 w^2 = (c_11 + c_2x + c_3y + c_4xy)w^2$. Note that $w^3 = \hat{G}$ and so the set $\{w^2, xw^2, yw^2, xyw^2\}$ is linearly independent. Therefore $\alpha w^2 = 0$ if and only if $c_i = 0$ for $i = 1, 2, 3$ and 4 . Thus $\text{ann}(w^2) = \ker \psi$. \square

Lemma 4.5.5. *The unit group of $\mathbb{F}_2(C_4 \times C_4)$, denoted $\mathcal{U}(\mathbb{F}_2(C_4 \times C_4))$ is isomorphic to $C_2^9 \times C_4^3$.*

Proof. The map $\epsilon: \mathbb{F}_2(C_4 \times C_4) \rightarrow \mathbb{F}_2(C_4 \times C_4)$ defined by $\alpha \mapsto \alpha^4$ is the augmentation map. Therefore the units of $\mathbb{F}_2(C_4 \times C_4)$ are the elements of augmentation 1 and so there are 2^{15} units in $\mathbb{F}_2(C_4 \times C_4)$. The unit group has exponent 4 and so $\mathcal{U}(\mathbb{F}_2(C_4 \times C_4)) \simeq C_2^n \times C_4^m$, for some positive integers m and n .

Let $\psi: \mathbb{F}_2(C_4 \times C_4) \rightarrow \mathbb{F}_2(C_4 \times C_4)$ be the Frobenius endomorphism defined by $\psi(\alpha) = \alpha^2$. Let V be the \mathbb{F}_2 -linear span of $\{1, x, y, xy\}$. By Lemma 4.5.3 $KG = V \oplus \ker \psi$ and so any unit of KG can be written as $v + z$, where v is an element of V of augmentation 1 and $z \in \ker \psi$. $(v + z)^2 = v^2 + z^2 = v^2$ and so the units of order dividing 2 are the 2^{12} elements $1 + z$ such that $z \in \ker(\psi)$. $C_2^n \times C_4^m$ has 2^{n+2m} elements, 2^{n+m} of which have order dividing 2 and so $n + 2m = 15$ and $n + m = 12$. Solving these equations simultaneously gives $n = 9$ and $m = 3$. \square

Lemma 4.5.6. *Let $KG = \mathbb{F}_2(C_4 \times C_4)$, where $C_4 \times C_4 = \langle x, y \mid x^4 = y^4 = [x, y] = 1 \rangle$. Let ψ be the algebra endomorphism from KG into KG defined by $\alpha \mapsto \alpha^2$. Let $u \in \{x, y, xy\}$, $v \in \{x, y, xy\} \setminus \{u\}$, $w = 1 + x + y + xy$ and let $r, s \in \ker(\psi)$. Define*

$\theta_{(u,m,r,v,n,s)}: KG \rightarrow KG$ to be the \mathbb{F}_2 -linear extension of the map from G into KG defined by $x^i y^j \mapsto (u + mw + r)^i (v + nw + s)^j$, for $i, j = 0, 1, 2, 3$ and $m, n \in \mathbb{F}_2$. Then θ is an algebra automorphism of KG if and only if $\theta = \theta_{(u,m,r,v,n,s)}$, for some u, m, r, v, n and s .

Proof. Let θ be an algebra automorphism of KG and let $\mathcal{U}(KG)$ denote the unit group of KG . Then θ is a permutation of $\mathcal{U}(KG)$ such that $\theta(1) = 1$. Let $\alpha = \sum_{i=0}^3 \sum_{j=0}^3 a_{i,j} x^i y^j$. θ is multiplicative and \mathbb{F}_2 -linear and so $\theta(\alpha) = \sum_{i=0}^3 \sum_{j=0}^3 a_{i,j} \theta(x)^i \theta(y)^j$. Thus θ is determined by $\theta(x)$ and $\theta(y)$. Moreover, since θ is an automorphism it preserves the order of a unit, that is, the order of $\theta(\mu)$ is equal to the order of μ for all $\mu \in \mathcal{U}(KG)$.

Let $w = 1 + x + y + xy$. By the proof of Lemma 4.5.5, any unit of KG can be written as $u + mw + r$, for some $u \in \{1, x, y, xy\}$, $m \in \mathbb{F}_2$ and $r \in \ker(\psi)$. Therefore $\theta(x) = u + mw + r$ and $\theta(y) = v + nw + s$, for some $u, v \in \{1, x, y, xy\}$, $m, n \in \mathbb{F}_2$ and $r, s \in \ker(\psi)$. $w^2 = 1 + x^2 + y^2 + x^2 y^2$ and so

$$\begin{aligned} \theta(w^2) &= \theta(1) + \theta(x)^2 + \theta(y)^2 + \theta(x)^2 \theta(y)^2 \\ &= 1 + u^2 + mw^2 + v^2 + nw^2 + (u^2 + mw^2)(v^2 + nw^2) \\ &= 1 + u^2 + mw^2 + v^2 + nw^2 + u^2 v^2 + nu^2 w^2 + mv^2 w^2 + mnw^4 \\ &= 1 + u^2 + mw^2 + v^2 + nw^2 + u^2 v^2 + nw^2 + mw^2 + 0 \\ &= 1 + u^2 + v^2 + u^2 v^2 = (1 + u^2)(1 + v^2), \end{aligned}$$

since $u^2 w^2 = v^2 w^2 = w^2$.

$w^2 \neq 0$ and so $\theta(w^2) \neq 0$ which implies that $u \neq 1$, $v \neq 1$ and $u \neq v$. Therefore $\theta = \theta_{(u,m,r,v,n,s)}$, for some $u \in \{x, y, xy\}$, $v \in \{x, y, xy\} \setminus \{u\}$, $m, n \in \mathbb{F}_2$ and $r, s \in \ker(\psi)$. Note that for $\theta = \theta_{(u,m,r,v,n,s)}$

$$\theta(w^2) = 1 + u^2 + v^2 + u^2 v^2 = w^2. \quad (4.3)$$

Conversely, let $\theta = \theta_{(u,m,r,v,n,s)}$, for some $u \in \{x, y, xy\}$, $v \in \{x, y, xy\} \setminus \{u\}$, $m, n \in \mathbb{F}_2$ and $r, s \in \ker(\psi)$. Let $g = x^i y^j$ and $h = x^l y^k$ be elements of the group G . Then

$$\theta(gh) = \theta(x^{i+l} y^{j+k}) = \theta(x)^{i+l} \theta(y)^{j+k} = \theta(x)^i \theta(y)^j \theta(x)^l \theta(y)^k = \theta(g)\theta(h).$$

Let $\alpha = \sum_{g \in G} a_g g$ and $\beta = \sum_{h \in G} b_h h$. Then

$$\begin{aligned} \theta(\alpha\beta) &= \theta\left(\sum_{g \in G} \sum_{h \in G} a_g b_h gh\right) = \sum_{g \in G} \sum_{h \in G} a_g b_h \theta(gh) = \sum_{g \in G} \sum_{h \in G} a_g b_h \theta(g)\theta(h) \\ &= \sum_{g \in G} a_g \theta(g) \sum_{h \in G} b_h \theta(h) = \theta(\alpha)\theta(\beta). \end{aligned}$$

Therefore θ is a ring endomorphism of KG .

Let α be any element of KG . It is now shown that $\theta(\alpha) = 0$ if and only if $\alpha = 0$ and hence θ is bijective. Let V be the \mathbb{F}_2 -linear span of the set $\{1, x, y, xy\}$. Let $v \in V$ and write $v = c_1 1 + c_2 x + c_3 y + c_4 xy$, where $c_i \in \mathbb{F}_2$. Then since $w = 1 + u + v + uv$

$$\begin{aligned} \theta(v) &\equiv c_1 1 + c_2(u + mw) + c_3(v + nw) + c_4(u + mw)(v + nw) \pmod{\ker \psi} \\ &\equiv c_1 1 + c_2 u + c_3 v + c_4 uv + (c_2 m + c_3 n + c_4 nu + c_4 mv)w \pmod{\ker \psi} \\ &\equiv c_1 1 + c_2 u + c_3 v + c_4 uv \\ &\quad + (c_2 m + c_3 n + c_4 nu + c_4 mv)(1 + u + v + uv) \pmod{\ker \psi} \\ &\equiv (c_1 + c_2 m + c_3 n)1 + (c_2 + c_2 m + c_3 n)u + (c_3 + c_2 m + c_3 n)v \\ &\quad + (c_4 + c_2 m + c_3 n)uv + c_4 nuw + c_4 mvw \pmod{\ker \psi}. \end{aligned}$$

Assume that $\theta(v) \equiv 0 \pmod{\ker \psi}$. Then $c_4(nu)w = c_4(mv)w = 0$, since $u^2 \in \text{supp}(uw)$, $u^2 \notin \text{supp}(vw)$, $v^2 \in \text{supp}(vw)$ and $v^2 \notin \text{supp}(uw)$. Thus $c_4 n = c_4 m = 0$.

There are 2 cases, the first is $c_4 = 0$ and the second is $m = n = 0$.

Case 1. $c_4 = 0$. The coefficient of uv equals 0 and so $c_2m + c_3n = 0$ and so $\theta(v) \equiv c_11 + c_2u + c_3v \pmod{\ker \psi}$ and so $c_1 = c_2 = c_3 = c_4 = 0$, since $1, u$ and v are distinct elements of G and so are linearly independent.

Case 2. $m = n = 0$. Then $\theta(v) \equiv c_11 + c_2u + c_3v + c_4uv \pmod{\ker \psi}$ and so again $c_1 = c_2 = c_3 = c_4 = 0$. Therefore $\theta(v) \in \ker \psi$ if and only if $v = 0$. Thus V is a θ -invariant subspace of KG .

By Lemma 4.5.3, α can be written as $\alpha = v_1 + v_2(1 + x^2) + v_3(1 + y^2) + v_4(1 + x^2)(1 + y^2)$, where $v_i \in V$ for $i = 1, 2, 3$ and 4. Assume that $\theta(\alpha) = 0$. Then using Equation 4.3, $0 = \theta(\alpha)\theta(w^2) = \theta(\alpha w^2) = \theta(v_1 w^2) = \theta(v_1)\theta(w^2) = \theta(v_1)w^2$ and so $\theta(v_1) \in \text{ann}(w^2)$. By Corollary 4.5.4, $\text{ann}(w^2) = \ker \psi$, hence $\theta(v_1) \in \ker \psi$ and so $v_1 = 0$. Therefore $\alpha = v_2(1 + x^2) + v_3(1 + y^2) + v_4(1 + x^2)(1 + y^2)$ and so

$$0 = \theta(\alpha)\theta((1 + x^2)) = \theta(\alpha(1 + x^2)) = \theta(v_3(1 + y^2)(1 + x^2)) = \theta(v_3 w^2) = \theta(v_3)w^2$$

$$\text{and } 0 = \theta(\alpha)\theta((1 + y^2)) = \theta(\alpha(1 + y^2)) = \theta(v_2 w^2) = \theta(v_2)w^2.$$

Therefore $\theta(v_2)$ and $\theta(v_3) \in \text{ann}(w^2) = \ker \psi$, hence $v_2 = v_3 = 0$. Thus $\alpha = v_4 w^2$ and $0 = \theta(\alpha) = \theta(v_4 w^2) = \theta(v_4)w^2$ which implies $\theta(v_4) \in \text{ann}(w^2) = \ker \psi$, hence $v_4 = 0$. Therefore $\theta(\alpha) = 0$ if and only if $\alpha = 0$. Thus θ is a bijection and so it is an algebra automorphism of KG . \square

Lemma 4.5.7. *Let $KG = \mathbb{F}_2(C_4 \times C_4)$, where $C_4 \times C_4 = \langle x, y \mid x^4 = y^4 = [x, y] = 1 \rangle$. Let ψ be the Frobenius endomorphism from KG into KG defined by $\alpha \mapsto \alpha^2$ and let θ be a map from KG to KG . Then θ is an algebra automorphism of KG if and only if*

1. $\theta|_G$ is a group isomorphism and
2. θ is the K -linear extension of $\theta|_G$ and
3. $\theta|_{\ker(\psi)}$ is injective.

Proof. Let θ be a map from KG to KG . Assume that $\theta|_G$ is a group isomorphism, that θ is the K -linear extension of $\theta|_G$ and also that $\theta|_{\ker(\psi)}$ is injective. Let $\alpha = \sum_{g \in G} a_g g$ and $\beta = \sum_{h \in G} b_h h$ be elements of KG . Then

$$\begin{aligned} \theta(\alpha\beta) &= \theta\left(\sum_{g \in G} \sum_{h \in G} a_g b_h gh\right) = \sum_{g \in G} \sum_{h \in G} a_g b_h \theta(gh) = \sum_{g \in G} \sum_{h \in G} a_g b_h \theta(g)\theta(h) \\ &= \sum_{g \in G} a_g \theta(g) \sum_{h \in G} b_h \theta(h) = \theta\left(\sum_{g \in G} a_g g\right)\theta\left(\sum_{h \in G} b_h h\right) = \theta(\alpha)\theta(\beta). \end{aligned}$$

Therefore θ is an algebra endomorphism. This implies that $\theta(k) = k$ for all $k \in \mathbb{F}_2$.

Let V be the \mathbb{F}_2 -linear span of the set $\{1, x, y, xy\}$. By Lemma 4.5.3, as vector spaces $KG = V \oplus \ker(\psi)$. θ maps units to units and so for any $g \in G$, we can write $\theta(g) = v_g + z_g$, where v_g is an element of V of augmentation 1 and $z_g \in \ker(\psi)$.

Let $v \in V$ and write $v = c_1 1 + c_2 x + c_3 y + c_4 xy$, where $c_i \in \mathbb{F}_2$. Then

$$\begin{aligned} \theta(v) &= c_1 \theta(1) + c_2 \theta(x) + c_3 \theta(y) + c_4 \theta(xy) \\ &\equiv c_1 1 + c_2 v_x + c_3 v_y + c_4 v_{xy} \pmod{\ker(\psi)}. \end{aligned}$$

Suppose $\theta(v) \in \ker(\psi)$. Then $c_1 1 + c_2 v_x + c_3 v_y + c_4 v_{xy} = 0$. The elements $1, v_x, v_y$ and v_{xy} all have augmentation 1 and so an even number of the c_i 's are equal to 1.

Case 1. None of the c_i 's are equal to 1. That is, $c_1 = c_2 = c_3 = c_4 = 0$.

Case 2. Two of the c_i 's are equal to 1. Therefore $v_g + v_h = 0$, for 2 distinct elements g, h of $\{1, x, y, xy\}$. Thus $\theta(g^2) = v_g^2 = v_h^2 = \theta(h^2)$, however this contradicts the assumption that $\theta|_G$ is a group isomorphism and so this case does not occur.

Case 3. All four of the c_i 's are equal to 1. Then $1 + v_x + v_y + v_{xy} = 0$. Let $w = 1 + x + y + xy$. Then w^2 is a nonzero element of $\ker(\psi)$ and $\theta(w^2) \neq 0$, since $\theta(0) = 0$ and $\theta|_{\ker(\psi)}$ is injective. Therefore $0 \neq \theta(w^2) = 1 + v_x^2 + v_y^2 + v_{xy}^2$ and so $1 + v_x + v_y + v_{xy} \neq 0$. Thus this case does not occur.

Therefore the only solution of $c_1 1 + c_2 v_x + c_3 v_y + c_4 v_x v_y = 0$ is $c_1 = c_2 = c_3 = c_4 = 0$ and so $\theta(v) \in \ker(\psi)$ implies $v = 0$. Thus V is a θ -invariant subspace of KG .

Let α be any element of KG and write $\alpha = v + z$, where $v \in V$ and $z \in \ker(\psi)$. Assume that $\theta(\alpha) = 0$. Then $0 = \theta(\alpha) = \theta(v) + \theta(z)$ which implies that $\theta(v) = \theta(z)$. Therefore $\theta(v) \in \ker(\psi)$, since $\theta(v)^2 = \theta(z)^2 = \theta(z^2) = \theta(0) = 0$ which implies that $v = 0$. Thus $\alpha = z \in \ker(\psi)$, which implies that $\alpha = 0$, since $\theta|_{\ker(\psi)}$ is injective. Therefore θ is an algebra endomorphism with kernel equal to $\{0\}$ and so θ is an algebra automorphism of KG .

Conversely, assume θ is an algebra automorphism of KG . Then by definition θ is a K -linear extension of $\theta|_G$ and $\theta|_{\ker(\psi)}$ is injective. Also $\theta(gh) = \theta(g)\theta(h)$ for any $g, h \in G$, since θ is an algebra automorphism. \square

Remark 4.5.8. The size of $\ker(\psi)$ was calculated using [18] to be 2^{12} . Therefore by Lemma 4.5.6 $Aut(\mathbb{F}_2(C_4 \times C_4))$ has size $3(2)(2^{12})(2)(2)(2^{12}) = 3(2^{27})$.

4.6 Distinguishing Group Algebras using Digraphs

Example 4.6.1. In this example the derivations of $\mathbb{F}_2 C_2$ are listed. Let $C_2 = \langle x \rangle$. By Theorem 2.3.4 the derivations of $\mathbb{F}_2 C_2$ are :

$$x \mapsto 0, \quad x \mapsto 1, \quad x \mapsto x, \quad x \mapsto 1 + x$$

The derivations are represented below by 2×2 matrices over \mathbb{F}_2 with respect to the basis $\mathcal{B} = \{1, x\}$:

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}. \quad (4.4)$$

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

is the matrix representation of $d(1+x) = 1+x$, where $d \in \text{Der}(\mathbb{F}_2C_2)$ such that $d(x) = 1+x$. There is only one nonzero nilpotent derivation of \mathbb{F}_2C_2 , namely the derivation defined by $x \mapsto 1$ and its index of nilpotency is 2.

Definition 4.6.2. Let $[0]_n$ be the $n \times n$ matrix, where each entry is zero and let $[E]_n$ be the $n \times n$ matrix, where each entry is one.

Example 4.6.3. Let K be the finite field with 2 elements. Let $G = \langle x \mid x^4 = 1 \rangle$ and let $\mathcal{B} = \{1, x, 1+x^2, x(1+x^2)\}$ be a basis of KG . Let H be the subgroup of G generated by x^2 and let $\bar{\mathcal{B}} = \{H, xH\}$ be a basis of $K(G/H)$. In this example the derivations of KG are listed as 2×2 block matrices, with respect to the basis \mathcal{B} . Each block is a 2×2 matrix over K . By Corollary 3.1.17, $\Delta(G, H)$ is a differential ideal of (KG, d) , for all derivations d of KG . Therefore by Lemma 3.1.11 any derivation D of KG has the form:

$$[D]_{\mathcal{B}} = \begin{bmatrix} [d]_{\bar{\mathcal{B}}} & [0]_2 \\ A & [d]_{\bar{\mathcal{B}}} \end{bmatrix},$$

where $d \in \text{Der}(\mathbb{F}_2(G/H))$ and so $[d]_{\bar{\mathcal{B}}}$ is one of the matrices listed in Equation 4.4 and A is a 2×2 matrix over K . Moreover, since $d(1) = 0$, the first column of $[D]_{\mathcal{B}}$ is all zeros and so A is also one of the matrices listed in Equation 4.4, that is, $A = [\delta]_{\bar{\mathcal{B}}}$, for some $\delta \in \text{Der}(\mathbb{F}_2C_2)$.

Definition 4.6.4. An $n \times n$ matrix M is called *circulant* if it is of the form:

$$M = \begin{bmatrix} a_0 & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \dots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \dots & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \dots & a_0 \end{bmatrix}.$$

Lemma 4.6.5. *Let K be the finite field of characteristic 2 and let $G = \langle x \mid x^{2^m} = 1 \rangle$, where m is a positive integer. Then the maximum nilpotency index for a derivation of KG is $2^{m-1} + 1$.*

Proof. Let $\mathcal{B} = \{1, x^2, \dots, x^{2^{m-2}}, x, x^3, \dots, x^{2^m-1}\}$. Then \mathcal{B} is a basis of KG . The first 2^{m-1} elements of \mathcal{B} in the above listing are in the ring of constants of KG . By Lemma 2.2.1, $d(x^{k+2}) = x^2d(x^k)$, for any integer k and so any derivation D of KG has the form:

$$[D]_{\mathcal{B}} = \begin{bmatrix} [0]_{2^{m-1}} & A \\ [0]_{2^{m-1}} & B \end{bmatrix},$$

where A and B are $2^{m-1} \times 2^{m-1}$ circulant matrices over K .

$$[D]_{\mathcal{B}}^2 = \begin{bmatrix} [0]_{2^{m-1}} & A \\ [0]_{2^{m-1}} & B \end{bmatrix} \begin{bmatrix} [0]_{2^{m-1}} & A \\ [0]_{2^{m-1}} & B \end{bmatrix} = \begin{bmatrix} [0]_{2^{m-1}} & AB \\ [0]_{2^{m-1}} & B^2 \end{bmatrix}, \text{ and}$$

$$[D]_{\mathcal{B}}^n = \begin{bmatrix} [0]_{2^{m-1}} & AB^{n-1} \\ [0]_{2^{m-1}} & B^n \end{bmatrix}, \quad \text{for all positive integers } n.$$

Therefore D is nilpotent if and only if B is nilpotent. Let $H = \langle y \rangle$ be the cyclic group of order 2^{m-1} . By [29] there is a bijective ring homomorphism between KH and the ring of $2^{m-1} \times 2^{m-1}$ circulant matrices over K . Therefore A and B correspond respectively to elements $\alpha, \beta \in KH$. Assume D is nilpotent. Then B and hence β is also nilpotent. Let $\psi: KH \rightarrow KH$ be the Frobenius endomorphism and let $\epsilon: KH \rightarrow K$ be the augmentation map. H is a 2-group of exponent 2^{m-1} and K is a field of characteristic 2 and so $\psi^{m-1}: KH \rightarrow K$ such that $\psi^{m-1} = \psi^{m-1} \circ \epsilon$, since for any $\alpha = \sum_{h \in H} a_h h \in KH$

$$\psi^{m-1}(\alpha) = \psi^{m-1}\left(\sum_{h \in H} a_h h\right) = \sum_{h \in H} \psi^{m-1}(a_h) \psi^{m-1}(h) = \psi^{m-1}\left(\sum_{h \in H} a_h\right) = \psi^{m-1} \circ \epsilon(\alpha).$$

ϵ is a ring endomorphism and so maps nilpotent elements to nilpotent elements. Since the image of ϵ is a field, ϵ maps nilpotent elements to 0 and so $\psi^{m-1}(\alpha) = 0$ for all nilpotent elements α . Therefore the elements of the augmentation ideal of KH are the nilpotent elements of KH . The augmentation ideal of KH is the ideal generated by $(1+y)$ and so $\beta = b(1+y)$, for some $b \in KH$. Thus $\beta^{2^{m-1}} = \psi^{m-1}(\beta) = (\psi^{m-1} \circ \epsilon)(\beta) = 0$ and $\alpha\beta^{2^{m-1}-1} = \alpha b^{2^{m-1}-1}(1+y)^{2^{m-1}-1} = \alpha b^{2^{m-1}-1}\hat{y} = k\hat{y}$, where $k = \epsilon(\alpha b^{2^{m-1}-1}) \in K$. By Section 3.1 of [29] and Definition 4.6.2, $B^{2^{m-1}-1} = k[E]_{2^{m-1}}$. Therefore

$$[D]_{\mathcal{B}}^{2^{m-1}} = \begin{bmatrix} [0]_{2^{m-1}} & AB^{2^{m-1}-1} \\ [0]_{2^{m-1}} & B^{2^{m-1}} \end{bmatrix} = \begin{bmatrix} [0]_{2^{m-1}} & k[E]_{2^{m-1}} \\ [0]_{2^{m-1}} & [0]_{2^{m-1}} \end{bmatrix}.$$

Choosing $\alpha = 1$ and $\beta = (1+y)$ implies $k = 1$ and so in this case $[D]_{\mathcal{B}}^{2^{m-1}} \neq 0$.

Also

$$[D]_{\mathcal{B}}^{2^{m-1}+1} = \begin{bmatrix} [0]_{2^{m-1}} & A \\ [0]_{2^{m-1}} & B \end{bmatrix} \begin{bmatrix} [0]_{2^{m-1}} & k[E]_{2^{m-1}} \\ [0]_{2^{m-1}} & [0]_{2^{m-1}} \end{bmatrix} = \begin{bmatrix} [0]_{2^{m-1}} & [0]_{2^{m-1}} \\ [0]_{2^{m-1}} & [0]_{2^{m-1}} \end{bmatrix}.$$

□

Definition 4.6.6. Let V be a finite dimensional vector space over a finite field K and let (V, f) and (V, g) be LFDS. Define $(V, f) * (V, g)$ to be the LFDS $(V \times V, f * g)$, where $V \times V$ is the cartesian product of the vector space V with itself and $f * g: V \times V \rightarrow V \times V$, defined by $(f * g)(u, v) = (f(u), g(u) + f(v))$. Also define the associated digraphs similarly, that is, $\Gamma_f * \Gamma_g = \Gamma_{f * g}$.

Lemma 4.6.7. *Let K be the finite field with 2 elements and let $G = \langle x \mid x^4 = 1 \rangle$. Let H be the subgroup of G generated by x^2 and let D be a K -linear map from KG to KG . Then*

(i) $D \in \text{Der}(KG)$ if and only if $[D]_{\mathcal{B}} = \left[\begin{array}{c|c} [d]_{\bar{\mathcal{B}}} & [0]_2 \\ \hline [\delta]_{\bar{\mathcal{B}}} & [d]_{\bar{\mathcal{B}}} \end{array} \right]$, where $d, \delta \in \text{Der}(K(G/H))$,
 $\mathcal{B} = \{1, x, 1 + x^2, x(1 + x^2)\}$ and $\bar{\mathcal{B}} = \{H, xH\}$.

(ii) For any $D \in \text{Der}(KG)$, $\Gamma_D \simeq \Gamma_d * \Gamma_\delta$, where d and δ are the derivations of $\text{Der}(K(G/H))$ defined by part (i).

Proof. (i) Let $D \in \text{Der}(KG)$ and let $\mathcal{B} = \{1, x, 1 + x^2, x(1 + x^2)\}$. Then

$$[D]_{\mathcal{B}} = \left[\begin{array}{c|c} A_1 & A_2 \\ \hline A_3 & A_4 \end{array} \right], \quad \text{where } A_1, \dots, A_4 \text{ are } 2 \times 2 \text{ matrices over } K.$$

By Corollary 3.1.17, $\Delta(G, H)$ is a differential ideal of (KG, D) , for all derivations D of KG . By Proposition 3.1.6, $\frac{KG}{\Delta(G, H)} \simeq K(G/H)$. Therefore by Lemma 3.1.11, $A_1 = [d]_{\bar{\mathcal{B}}}$, for some $d \in \text{Der}(K(G/H))$ and $A_2 = [0]_2$, the 2×2 matrix whose entries are all zeros. Moreover, $(1 + x^2) \in \mathcal{C}(KG)$ and so $D(\alpha(1 + x^2)) = D(\alpha)(1 + x^2)$ for all $\alpha \in KG$ and so $A_4 = A_1$. Lastly, since $d(1) = 0$, the first column of $[D]_{\mathcal{B}}$ is all zeros and so A_3 is also one of the matrices listed in Equation 4.4 and so $A_3 = [\delta]_{\bar{\mathcal{B}}}$, for some $\delta \in \text{Der}(K(G/H))$.

Conversely, let T be a K -linear map from KG to KG such that

$$[T]_{\mathcal{B}} = \left[\begin{array}{c|c} [d]_{\bar{\mathcal{B}}} & [0]_2 \\ \hline [\delta]_{\bar{\mathcal{B}}} & [d]_{\bar{\mathcal{B}}} \end{array} \right],$$

where $d, \delta \in \text{Der}(K(G/H))$, $\mathcal{B} = \{1, x, 1 + x^2, x(1 + x^2)\}$ and $\bar{\mathcal{B}} = \{H, xH\}$.

Then by Example 4.6.1

$$[d]_{\bar{\mathcal{B}}} = \begin{bmatrix} 0 & a_0 \\ 0 & a_1 \end{bmatrix} \text{ and } [\delta]_{\bar{\mathcal{B}}} = \begin{bmatrix} 0 & a_2 \\ 0 & a_3 \end{bmatrix}, \text{ for some } a_i \in K \text{ and so } [T]_{\mathcal{B}} = \begin{bmatrix} 0 & a_0 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & a_2 & 0 & a_0 \\ 0 & a_3 & 0 & a_1 \end{bmatrix}.$$

Let D be the derivation of KG defined by $D(x) = a_0 + a_1x + a_2(1+x^2) + a_3x(1+x^2)$. Then $D(1) = D(1+x^2) = 0$ and $D(x(1+x^2)) = D(x)(1+x^2) = a_0(1+x^2) + a_1x(1+x^2)$. Therefore

$$[D]_{\mathcal{B}} = \begin{bmatrix} 0 & a_0 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & a_2 & 0 & a_0 \\ 0 & a_3 & 0 & a_1 \end{bmatrix} \text{ and so } T \in \text{Der}(KG), \text{ since } T = D. \quad (4.5)$$

(ii) Let V be the subspace of KG with basis $\{1, x\}$. Let $\Phi: KG \rightarrow V \times V$, that is, Φ is a map from KG to the Cartesian product of the vector space V with itself. $\mathcal{B} = \{1, x, 1+x^2, x(1+x^2)\}$ is a basis of KG and so any $\alpha \in KG$ can be written uniquely as $\alpha = r + s(1+x^2)$, where $r, s \in V$. Define Φ by $r + s(1+x^2) \mapsto (r, s)$. Therefore Φ is a bijection from the vertex set of Γ_D to the vertex set of $\Gamma_{d*\delta}$. It is now shown that Φ is a graph isomorphism, that is, Φ is bijection between vertex set of Γ_D to the vertex set of $\Gamma_{d*\delta}$ that preserves adjacency. $D(\alpha) = D(r + s(1+x^2)) = D(r) + D(s)(1+x^2)$. By Equation 4.5 $D(r) = d(r) + \delta(r)(1+x^2)$ and $D(s) = d(s) + \delta(s)(1+x^2)$. Therefore

$$D(\alpha) = d(r) + \delta(r)(1+x^2) + d(s)(1+x^2) + \delta(s)(1+x^2)^2 = d(r) + (\delta(r) + d(s))(1+x^2).$$

Therefore $\Phi(D(\alpha)) = (d(r), \delta(r) + d(s))$. By Definition 4.6.6, $\Phi(\alpha) = (r, s)$ is adjacent to $(d(r), \delta(r) + d(s))$ in $\Gamma_{d*\delta}$ and so Φ preserves adjacency and thus is a graph isomorphism. \square

Definition 4.6.8. Let $CM_n(K)$ be the vector space of $n \times n$ circulant matrices over a field K . Define $g: CM_n(K) \rightarrow CM_n(K)$ by $g(C)_{i,j} = \begin{cases} C_{i,j} & \text{if } j > i \\ 0 & \text{otherwise.} \end{cases}$

That is $g(C)$ is given by the following upper triangular matrix:

$$g(C) = \begin{bmatrix} 0 & a_{n-1} & a_{n-2} & a_{n-3} & \dots & a_2 & a_1 \\ 0 & 0 & a_{n-1} & a_{n-2} & \dots & a_3 & a_2 \\ 0 & 0 & 0 & a_{n-1} & \dots & a_4 & a_3 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & a_{n-1} \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 \end{bmatrix}, \text{ where } C = \begin{bmatrix} a_0 & a_{n-1} & a_{n-2} & \dots & a_1 \\ a_1 & a_0 & a_{n-1} & \dots & a_2 \\ a_2 & a_1 & a_0 & \dots & a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & a_{n-3} & \dots & a_0 \end{bmatrix}.$$

Further if M is a block matrix consisting of blocks M_i for $i = 1, 2, \dots, m(n)$, such that $M_i \in CM_n(K)$ for each i . Then define $g(M)$ to be the block matrix whose blocks are $g(M_i)$ keeping the positions unchanged. That is:

$$g(M) = \begin{bmatrix} g(M_1) & g(M_2) & \dots & g(M_m) \\ g(M_{m+1}) & g(M_{m+2}) & \dots & g(M_{2m}) \\ \vdots & \vdots & & \vdots \\ g(M_{(n-1)m+1}) & g(M_{(n-1)m+2}) & \dots & g(M_{nm}) \end{bmatrix}, \text{ where}$$

$$M = \begin{bmatrix} M_1 & M_2 & \dots & M_m \\ M_{m+1} & M_{m+2} & \dots & M_{2m} \\ \vdots & \vdots & & \vdots \\ M_{(n-1)m+1} & M_{(n-1)m+2} & \dots & M_{nm} \end{bmatrix}.$$

Definition 4.6.9. Let Γ_1 and Γ_2 be graphs. A mapping $f: \mathcal{V}(\Gamma_1) \rightarrow \mathcal{V}(\Gamma_2)$ is a *homomorphism of graphs* if $f(u)$ and $f(v)$ are adjacent in Γ_2 , whenever u and v are adjacent in Γ_1 .

Definition 4.6.10. Let Γ_2 be a subgraph of a graph Γ_1 . A *retraction* is a homomorphism f from $\mathcal{V}(\Gamma_1) \rightarrow \mathcal{V}(\Gamma_2)$ such that the restriction, $f \upharpoonright_{\mathcal{V}(\Gamma_2)}$ of f to $\mathcal{V}(\Gamma_2)$ is the identity map.

Example 4.6.11. Let K be the finite field with 2 elements and let $G = \langle x, y \mid x^2 = y^2 = [x, y] = 1 \rangle$. Let $\mathcal{B} = \{1, x, y, xy\}$ and let d be an arbitrary derivation of KG . Then by Theorem 2.3.4, $d = a\partial_x + b\partial_y$, for some $a = \sum_{g \in G} a_g g$ and $b = \sum_{g \in G} b_g g$ where $a_g, b_g \in K$, for all $g \in G$. Therefore $d(1) = 0$, $d(x) = a$, $d(y) = b$ and $d(xy) = ay + bx$ and so

$$\begin{aligned} [d]_{\mathcal{B}} &= \begin{bmatrix} 0 & a_1 & b_1 & a_y + b_x \\ 0 & a_x & b_x & a_{xy} + b_1 \\ 0 & a_y & b_y & a_1 + b_{xy} \\ 0 & a_{xy} & b_{xy} & a_x + b_y \end{bmatrix} = \begin{bmatrix} 0 & a_1 & 0 & a_y \\ 0 & a_x & 0 & a_{xy} \\ 0 & a_y & 0 & a_1 \\ 0 & a_{xy} & 0 & a_x \end{bmatrix} + \begin{bmatrix} 0 & 0 & b_1 & b_x \\ 0 & 0 & b_x & b_1 \\ 0 & 0 & b_y & b_{xy} \\ 0 & 0 & b_{xy} & b_y \end{bmatrix} \\ &= \begin{bmatrix} [d_1]_{\bar{\mathcal{B}}} & [d_2]_{\bar{\mathcal{B}}} \\ [d_2]_{\bar{\mathcal{B}}} & [d_1]_{\bar{\mathcal{B}}} \end{bmatrix} + \begin{bmatrix} [0]_2 & c_1 \\ [0]_2 & c_2 \end{bmatrix}, \end{aligned}$$

where $d_1, d_2 \in \text{Der}(\mathbb{F}_2\langle x \rangle)$, $\bar{\mathcal{B}} = \{1, x\}$ and c_1 and c_2 are 2×2 circulant matrices over \mathbb{F}_2 .

Lemma 4.6.12. [31][pp. 8] *Let d be a derivation of a not necessarily associative algebra A and let $a, b \in A$. Then*

$$d^m(ab) = \sum_{i=0}^m \binom{m}{i} d^{m-i}(a)d^i(b), \quad \text{for any positive integer } m. \quad (4.6)$$

The following result is a direct consequence of the discussion in [31][pp. 186].

Lemma 4.6.13. *Let p be a prime number and let K be a finite field of characteristic p . Let G be a group and let d be a derivation of KG . Then d^{p^k} is a derivation of KG for all positive integers k .*

Remark 4.6.14. Let G and H be finite abelian p -groups and let K be the finite field with p elements. Suppose that KG and KH are isomorphic as rings. Then KG and KH have the same dimension as K -algebras and so $|G| = |H|$. By

Theorem 2.3.4, the vector space of derivations of KG has dimension $n|G|$, where n is the minimum number of generators of G . By Theorem 3.1.18, $Der(KG)$ and $Der(KH)$ are isomorphic as additive groups and so have the same dimension. This simple counting argument can sometimes be used to show that group algebras are not isomorphic as rings. For example $|Der(\mathbb{F}_2C_4)| = 2^4$ whereas $|Der(\mathbb{F}_2(C_2 \times C_2))| = 2^8$ and so by Theorem 3.1.18 or Theorem 4.1.8, \mathbb{F}_2C_4 and $\mathbb{F}_2(C_2 \times C_2)$ are not isomorphic as rings. The smallest example such that the above argument fails to distinguish between non-isomorphic group algebras is when the groups are $C_4 \times C_4$ and $C_2 \times C_8$ and the field K has 2 elements. Example 4.6.18 shows that these two group algebras are non-isomorphic using the graphs of their derivations.

Definition 4.6.15. Define the map $f: M_4(\mathbb{F}_2) \rightarrow M_4(\mathbb{F}_2)$ by

$$A = (a_{i,j}) \mapsto \begin{bmatrix} 0 & 0 & 0 & a_{3,2} \\ 0 & 0 & 0 & a_{4,2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Definition 4.6.16. Define the map $g: M_4(\mathbb{F}_2) \rightarrow M_4(\mathbb{F}_2)$ by

$$A = (a_{i,j}) \mapsto \begin{bmatrix} 0 & 0 & 0 & a_{2,3} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a_{4,3} \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Lemma 4.6.17. Let K be the finite field with 2 elements and let $G = \langle x, y \mid x^4 = y^4 = [x, y] = 1 \rangle$. Let D be a derivation of KG . Then D is nilpotent if and only if $D^8 = 0$.

Proof. Assume that D is a nilpotent derivation of KG . It can be shown that $\mathcal{B} = \{1, x, y, xy, (1+x^2), x(1+x^2), y(1+x^2), xy(1+x^2), (1+y^2), x(1+y^2), y(1+y^2),$

$xy(1+y^2), (1+x^2)(1+y^2), x(1+x^2)(1+y^2), y(1+x^2)(1+y^2), xy(1+x^2)(1+y^2)\}$, is a basis for KG . Let $H = \langle x^2, y^2 \rangle$ and further choose $\bar{\mathcal{B}} = \{H, xH, yH, xyH\}$ as a basis of $K(G/H)$. Let b_i be the i^{th} element of \mathcal{B} in the above listing. Then by Theorem 2.3.4, $D = r\partial_x + s\partial_y$ for some $r = \sum_{i=1}^{16} r_i b_i$ and $s = \sum_{i=1}^{16} s_i b_i$ where $r_i, s_i \in K$, for $i = 1, 2, \dots, 16$. Therefore

$$\begin{aligned} D(1) &= 0, \\ D(x) &= r = \sum_{i=1}^{16} r_i b_i, \\ D(y) &= s = \sum_{i=1}^{16} s_i b_i, \text{ and} \\ D(xy) &= D(x)y + xD(y) = ry + sx = \sum_{i=1}^{16} r_i b_i y + \sum_{i=1}^{16} s_i b_i x. \end{aligned}$$

Multiplying r by y and writing the product as a linear combination of the elements of \mathcal{B} implies

$$\begin{aligned} \sum_{i=1}^{16} r_i b_i y &= r_3 + r_4 x + r_1 y + r_2 xy + (r_7 + r_8 x + r_5 y + r_6 xy)(1 + x^2) \\ &\quad + ((r_{11} + r_3) + (r_{12} + r_4)x + r_9 y + r_{10} xy)(1 + y^2) \\ &\quad + ((r_{15} + r_7) + (r_{16} + r_8)x + (r_{13})y + (r_{14})xy)(1 + x^2)(1 + y^2). \end{aligned}$$

Multiplying s by x and writing the product as a linear combination of the elements of \mathcal{B} implies

$$\begin{aligned} \sum_{i=1}^{16} s_i b_i x &= s_2 + s_1 x + s_4 y + s_3 xy + ((s_6 + s_2) + s_5 x + (s_8 + s_4)y + s_7 xy)(1 + x^2) \\ &\quad + (s_{10} + s_9 x + s_{12} y + s_{11} xy)(1 + y^2) \\ &\quad + ((s_{14} + s_{10}) + s_{13} x + (s_{16} + s_{12})y + s_{15} xy)(1 + x^2)(1 + y^2). \end{aligned}$$

Therefore since $(1 + x^2), (1 + y^2)$ and $(1 + x^2)(1 + y^2)$ are in $\mathcal{C}(KG)$ and since

Assume that $d_1 \in \text{Der}(K(G/H))$ such that $d_1^4 = 0$. Therefore

$$[D]_{\mathcal{B}}^2 = \begin{bmatrix} [d_1]_{\mathcal{B}}^2 & [0]_4 & [0]_4 & [0]_4 \\ t_2 & [d_1]_{\mathcal{B}}^2 & [0]_4 & [0]_4 \\ t_3 & [0]_4 & [d_1]_{\mathcal{B}}^2 & [0]_4 \\ t_4 & t_3 & t_2 & [d_1]_{\mathcal{B}}^2 \end{bmatrix}, \text{ for some } 4 \times 4 \text{ matrices } t_i.$$

Recall that $d_1^4 = 0$ and so squaring $[D]_{\mathcal{B}}^2$ gives

$$[D]_{\mathcal{B}}^4 = \begin{bmatrix} [0]_4 & [0]_4 & [0]_4 & [0]_4 \\ w_2 & [0]_4 & [0]_4 & [0]_4 \\ w_3 & [0]_4 & [0]_4 & [0]_4 \\ w_4 & w_3 & w_2 & [0]_4 \end{bmatrix}, \text{ for some } 4 \times 4 \text{ matrices } w_i.$$

Therefore

$$[D]_{\mathcal{B}}^8 = \begin{bmatrix} [0]_4 & [0]_4 & [0]_4 & [0]_4 \\ [0]_4 & [0]_4 & [0]_4 & [0]_4 \\ [0]_4 & [0]_4 & [0]_4 & [0]_4 \\ [w_3, w_2] & [0]_4 & [0]_4 & [0]_4 \end{bmatrix}. \quad (4.7)$$

It has been verified by SageMath [43], that for each nilpotent derivation $d_1 \in \text{Der}(K(G/H))$ and any derivations $d_2, d_3 \in \text{Der}(K(G/H))$, $[w_3, w_2] = [0]_4$. \square

Example 4.6.18. Let $C_8 \times C_2 = \langle x, y \mid x^8 = y^2 = [x, y] = 1 \rangle$ and let d be the derivation of \mathbb{F}_2G defined by $x \mapsto xy$ and $y \mapsto 1 + y + xy + x + x^3$. It can be shown that $B = \{1, x, y, xy, (1+x^2), x(1+x^2), y(1+x^2), xy(1+x^2), (1+x^2)^2, x(1+x^2)^2, y(1+x^2)^2, xy(1+x^2)^2, (1+x^2)^3, x(1+x^2)^3, y(1+x^2)^3, xy(1+x^2)^3\}$ is a basis for $\mathbb{F}_2(C_8 \times C_2)$. The matrix representation $[d]_B$ of d with respect to the basis B and its Jordan form $[J]_B$ are given below. The Jordan form of $[d]_B$ was calculated

using SageMath [43]. The diagonal entries of $[J]_B$ are all zeros. Therefore d is a nilpotent derivation of $\mathbb{F}_2(C_8 \times C_2)$. The largest Jordan block of $[J]_B$ has length 13 and so $d^{12} \neq 0$ and $d^{13} = 0$. Recall that Lemma 4.6.17 states that $D^8 = 0$ for any nilpotent derivation D of $\mathbb{F}_2(C_4 \times C_4)$. We have shown that the digraph $\Gamma(d)$ associated with the derivation d of $\mathbb{F}_2(C_8 \times C_2)$ is not isomorphic to $\Gamma(\delta)$ for any $\delta \in \text{Der}(\mathbb{F}_2(C_4 \times C_4))$. Therefore by Theorem 4.1.8, $\mathbb{F}_2(C_8 \times C_2)$ is not isomorphic to $\mathbb{F}_2(C_4 \times C_4)$.

$$[d]_B = \begin{bmatrix} 0 & 0 & 1 & 0 & | & 0 & 0 & 0 & 0 & | & 0 & 0 & 0 & 0 & | & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & | & 0 & 0 & 0 & 0 & | & 0 & 0 & 0 & 0 & | & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & | & 0 & 0 & 0 & 0 & | & 0 & 0 & 0 & 0 & | & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & | & 0 & 0 & 0 & 0 & | & 0 & 0 & 0 & 0 & | & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & | & 0 & 0 & 1 & 0 & | & 0 & 0 & 0 & 0 & | & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & | & 0 & 0 & 0 & 0 & | & 0 & 0 & 0 & 0 & | & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & | & 0 & 0 & 1 & 1 & | & 0 & 0 & 0 & 0 & | & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & | & 0 & 1 & 1 & 1 & | & 0 & 0 & 0 & 0 & | & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & | & 0 & 0 & 0 & 1 & | & 0 & 0 & 1 & 0 & | & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & | & 0 & 0 & 1 & 0 & | & 0 & 0 & 0 & 0 & | & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & | & 0 & 0 & 0 & 1 & | & 0 & 0 & 1 & 1 & | & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & | & 0 & 0 & 0 & 0 & | & 0 & 1 & 1 & 1 & | & 0 & 0 & 0 & 0 \end{bmatrix}, \quad [J]_B = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & | & 0 & | & 0 & | & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & | & 0 & | & 0 & | & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & | & 0 & | & 0 & | & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & | & 0 & | & 0 & | & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & | & 0 & | & 0 & | & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & | & 0 & | & 0 & | & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & | & 0 & | & 0 & | & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & | & 0 & | & 0 & | & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & | & 0 & | & 0 & | & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & | & 0 & | & 0 & | & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & | & 0 & | & 0 & | & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & | & 0 & | & 0 & | & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & | & 0 & | & 0 & | & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & | & 0 & | & 0 & | & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & | & 0 & | & 0 & | & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & | & 0 & | & 0 & | & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & | & 0 & | & 0 & | & 0 \end{bmatrix}$$

Chapter 5

Derivation Towers

This chapter considers the set of derivations of a commutative group algebra over a finite field. The Lie algebra formed from this set by defining multiplication as the Lie commutator is shown to have trivial center. Also, the Lie algebra of derivations of the group algebra KG is complete, when K is a finite field of characteristic p and G is a finite abelian group such that its Sylow p -subgroup is elementary abelian.

Group algebras have a rich structure and have been studied by many mathematicians. Particular attention has been devoted to the characteristic 0 case. Connections between properties of a group algebra and properties of the underlying group have been established. In this chapter group rings are studied via the Lie algebra of derivations of the group algebra. Let G be a finite abelian group and let K be a finite field. The set of derivations of the group algebra KG is denoted by $Der(KG)$. A Lie algebra is formed from this set by defining multiplication as the Lie commutator and is denoted by \mathfrak{g} . Let A be an associative and commutative algebra over a field K . Then the Lie algebra formed by taking the tensor product of A with a nonzero K -vector space of commuting K -derivations of A is a Witt type algebra and is studied in [39]. Therein necessary and sufficient conditions are given for this Lie algebra to be simple. Further results on these Lie algebras can be found

in [32]. It is shown in [37] that a complete Lie algebra can be decomposed into a direct sum of simple complete ideals. If the derivation algebra of a Lie algebra is perfect and has trivial center then it is complete [51].

Definitions and lemmas on Lie algebras which will be useful are introduced in Section 5.1 as well as the aforementioned result from [51]. In Section 5.2 it is shown that the derivations of KG are a proper subset of the Lie derivations of KG . A basis for the K -vector space of derivations of KG is given and the Lie algebra $\mathfrak{g} = Der(KG)$ is shown to have trivial center. Modular elementary abelian group algebras are shown in Theorem 5.3.8 to be complete. Extensions of this result are explored in Section 5.4. Let d be a derivation of KG and let H be a subgroup of an abelian group G . It is shown that the augmentation ideal $\Delta(G, H)$ is a differential ideal of the ring (KG, d) if and only if the image of H under d is contained within the augmentation ideal $\Delta(G, H)$. This provides a method for constructing a proper nonzero ideal of the Lie algebra $Der(KG)$ from $\Delta(G, H)$, when the Sylow p -subgroup of G is not elementary abelian. In Example 5.4.3 a derivation of $\mathbb{F}_2(C_4 \times C_2)$ is constructed and is proven to be outer by showing that it does not map this ideal into itself. Therefore Theorem 5.3.8 does not extend to all finite commutative group algebras. However as Example 5.4.4 shows the existence of an ideal of \mathfrak{g} constructed from $\Delta(G, H)$ does not imply that \mathfrak{g} is not complete. However, it is shown in Theorem 5.4.14 that $Der(KG)$ is a complete Lie algebra, when G is a finite abelian group such that its Sylow p -subgroup is elementary abelian.

5.1 Introduction

We begin with a brief introduction to Lie algebras.

Definition 5.1.1. [31] A *Lie algebra* \mathfrak{L} is a not necessarily associative algebra

over a field such that its multiplication, denoted by $[\ , \]$, satisfies the following conditions:

$$[x, x] = 0 \quad \text{and} \quad (5.1)$$

$$[x, [y, z]] + [z, [x, y]] + [y, [z, x]] = 0. \quad (5.2)$$

Equation (5.2) is known as the Jacobi identity.

Definition 5.1.2. Let A and B be subspaces of a Lie algebra \mathfrak{L} . Define $[A, B]$ to be the subspace spanned by the set $\{[a, b] \mid a \in A, b \in B\}$. A subspace I of \mathfrak{L} is an *ideal* of \mathfrak{L} if and only if $[I, \mathfrak{L}] \subseteq I$.

Definition 5.1.3. Let \mathfrak{L} be a Lie algebra. Define $\mathfrak{L}' = \mathfrak{L}^{(1)}$ to be $[\mathfrak{L}, \mathfrak{L}]$, the ideal of \mathfrak{L} generated by all products $[a, b]$, where $a, b \in \mathfrak{L}$. Further define $\mathfrak{L}^{(k)} = [\mathfrak{L}^{(k-1)}, \mathfrak{L}^{(k-1)}]$, where k is a positive integer. The *derived series* of ideals of \mathfrak{L} is $\mathfrak{L} \supseteq \mathfrak{L}' \supseteq \mathfrak{L}^{(2)} \supseteq \dots \supseteq \mathfrak{L}^{(k)} \supseteq \dots$. A Lie algebra \mathfrak{L} is said to be *solvable* if $\mathfrak{L}^{(k)} = 0$, for some positive integer k .

Definition 5.1.4. Let \mathfrak{L} be a Lie algebra over a field K and let D be a map from \mathfrak{L} to \mathfrak{L} . Then D is a (*Lie*) *derivation* of \mathfrak{L} if D is K -linear and satisfies the follow identity known as Leibniz's rule for any $a, b \in \mathfrak{L}$:

$$D([a, b]) = [D(a), b] + [a, D(b)]. \quad (5.3)$$

Also denote by $Der(\mathfrak{L})$ the set of (Lie) derivations of \mathfrak{L} . A derivation $d \in Der(\mathfrak{L})$ is called *inner* if for all $b \in \mathfrak{L}$, $d(b) = [a, b]$ for some $a \in \mathfrak{L}$.

Definition 5.1.5. Let S be a subset of a Lie algebra \mathfrak{L} . Define the centraliser of S in \mathfrak{L} , denoted $C(S, \mathfrak{L})$ to be the set of elements c of \mathfrak{L} such that $[s, c] = 0$, for all $s \in S$. $C(S, \mathfrak{L})$ is a subalgebra of the Lie algebra \mathfrak{L} by [31].

Definition 5.1.6. Let \mathfrak{L} be a Lie algebra. Define the *center* of \mathfrak{L} , denoted by $C(\mathfrak{L})$ to be the set of elements c of \mathfrak{L} such that $[a, c] = 0$, for all $a \in \mathfrak{L}$. The center, $C(\mathfrak{L})$ is an ideal of \mathfrak{L} , by [31]. \mathfrak{L} is called *abelian* if $\mathfrak{L}' = 0$.

Definition 5.1.7. Let A be an associative algebra. A Lie algebra, denoted by A_L is constructed from A by defining the Lie product as $[x, y] = xy - yx$, for all $x, y \in A$.

The next lemma shows that $Der(A)$ forms a Lie algebra for any not necessarily associative algebra A .

Lemma 5.1.8. [31] *Let A be a not necessarily associative algebra. Then $Der(A)$, the set of derivations of A is a (Lie) subalgebra of E_L , where E is the algebra of linear transformations of the vector space A .*

Definition 5.1.9. A Lie algebra \mathfrak{L} is called *simple* if it has no nonzero proper ideals and $\mathfrak{L}' = \mathfrak{L}$.

Definition 5.1.10. A Lie algebra, \mathfrak{L} is called *perfect* if it equals its own commutator ideal, that is $\mathfrak{L}' = \mathfrak{L}$.

Definition 5.1.11. [31] A Lie algebra, \mathfrak{L} is called *complete* if its center is $\{0\}$ and all its derivations are inner.

Theorem 5.1.12. [51] *Let \mathfrak{L} be a perfect Lie algebra with center $\{0\}$. Then the derivation algebra $Der(\mathfrak{L})$ is complete.*

Lemma 5.1.13. [47] *Let \mathfrak{L} be a Lie algebra with center $\{0\}$, and let D_1 be the derivation algebra of \mathfrak{L} and let D_0 be the algebra of all inner derivations of \mathfrak{L} . Then*

1. \mathfrak{L} is isomorphic to D_0
2. D_0 is an ideal of D_1

3. The centraliser of D_0 in D_1 is $\{0\}$

Definition 5.1.14. [35] Let \mathfrak{L} be a finite dimensional Lie algebra with center $\{0\}$. For $i \geq 1$, let $Der_i(\mathfrak{L}) = Der(Der_{i-1}(\mathfrak{L}))$, where $Der_0(\mathfrak{L}) = \mathfrak{L}$. Then by Lemma 5.1.13 each $Der_i(\mathfrak{L})$ has center $\{0\}$ and is an ideal of $Der_{i+1}(\mathfrak{L})$ and so:

$$\mathfrak{L} = Der_0(\mathfrak{L}) \triangleleft Der_1(\mathfrak{L}) \triangleleft Der_2(\mathfrak{L}) \triangleleft \dots$$

This sequence is called the *derivation tower* of \mathfrak{L} . In [47] it is shown that $Der_n(\mathfrak{L})$ has only inner derivations for some n . So Lemma 5.1.13 implies that $Der_n(\mathfrak{L}) \simeq Der_{n+j}(\mathfrak{L})$, for all $j \geq 1$. In other words the sequence stabilises. The minimal n such that the sequence stabilises is called the *height* of the derivation tower.

Special cases of Lemmas 5.1.15 and 5.1.16 are used in the proofs of Section 5.3.

Lemma 5.1.15. Let \mathfrak{g} be a Lie algebra and let $r, s, c \in \mathfrak{g}$ and let $D \in Der(\mathfrak{g})$ such that $D(r) = [c, r]$ and $D([r, s]) = [c, [r, s]]$. Then $D(s) - [c, s] \in C(r, \mathfrak{g})$.

Proof. The Lie bracket is anticommutative and so applying D to $0 = [r, s] + [s, r]$ and using the Jacobi identity gives

$$\begin{aligned} 0 &= D([r, s]) + [D(s), r] + [s, D(r)] = [c, [r, s]] + [D(s), r] + [s, [c, r]] \\ &= [c, [r, s]] + [D(s), r] - [r, [s, c]] - [c, [r, s]] \\ &= [D(s), r] - [[c, s], r] = [D(s) - [c, s], r], \end{aligned}$$

since the bracket is bilinear. Therefore $D(s) - [c, s] \in C(r, \mathfrak{g})$, □

Lemma 5.1.16. Let \mathfrak{g} be a Lie algebra over a field K and let $r, s, c \in \mathfrak{g}$, such that $[r, s] = ks$, for some $k \in K$. Further, let $D \in Der(\mathfrak{g})$ such that $D(r) = [c, r]$. Then $[r, b] = kb$, where $b = D(s) - [c, s]$.

Proof. Applying D to $0 = [r, s] - ks$ gives

$$0 = [D(r), s] + [r, D(s)] - kD(s) = [[c, r], s] + [r, [c, s] + b] - k([c, s] + b). \quad (5.4)$$

However by the Jacobi identity

$$[[c, r], s] = -[s, [c, r]] = [r, [s, c]] + [c, [r, s]] = [r, [s, c]] + [c, ks].$$

Substituting into Equation (5.4) gives

$$\begin{aligned} 0 &= [r, [s, c]] + [c, ks] + [r, [c, s]] + [r, b] - k[c, s] - kb \\ &= [r, [s, c]] - [r, [s, c]] + k[c, s] - k[c, s] + [r, b] - kb = [r, b] - kb. \end{aligned}$$

Therefore $[r, b] = kb$. □

5.2 The Lie Algebra of Derivations of a Group Algebra

It is shown that all derivations of a group algebra (as defined in [12] and elsewhere) are Lie derivations but the converse is false in general. In particular, finite commutative group algebras are considered and a basis for the K -vector space of derivations of these group algebras is presented in Theorem 2.3.4. Theorem 5.2.9 shows that the Lie algebra of derivations of a finite commutative group algebra has trivial center.

Lemma 5.2.1. *Let K be a finite field, let G be a group and let $\mathfrak{L} = KG_L$. Then $Der(KG) \subseteq Der(\mathfrak{L})$.*

Proof. Let $a, b \in \mathfrak{L}$ and $d \in Der(KG)$. By Theorem 2.2 of [12] d is a K -linear map

from KG to KG . Moreover

$$\begin{aligned} d([a, b]) &= d(ab - ba) = d(ab) - d(ba) \\ &= d(a)b + ad(b) - d(b)a - bd(a) = [d(a), b] + [a, d(b)]. \end{aligned}$$

Therefore $d \in \text{Der}(\mathfrak{L})$. □

Example 5.2.5 shows that in general $\text{Der}(KG) \neq \text{Der}(\mathfrak{L})$.

The following notation is used for the rest of this chapter.

Notation 5.2.2. Let K be a finite field of positive characteristic p and let G be a finite abelian group. So $G \simeq H \times X$, where H is a p -regular group and X is an abelian p -group with the following presentation

$$X = \langle x_0, x_1, \dots, x_{n-1} \mid x_k^{p^{m_k}} = 1, x_k^{-1}x_l^{-1}x_kx_l = 1, \text{ for all } k, l \in \{0, 1, \dots, n-1\} \rangle,$$

where n and m_k are positive integers.

Definition 5.2.3. Let G be a finite abelian group. Using the above notation, for $j \in \{0, 1, \dots, n-1\}$ define the set $S = \{x_i \mid i = 0, 1, \dots, n-1\}$ and define $S_j = S \setminus \{x_j\}$. Also, define G_j to be $H \times \tilde{X}$, where \tilde{X} is the subgroup of G generated by S_j . Thus $\bigcap_{i=0}^{n-1} G_i = H$.

Remark 5.2.4. Theorem 2.3.4 gives a basis for the K -vector space of derivations of KG . By Lemma 2.2.1, $\partial_{x_i}(x_i^m) = mx_i^{m-1}$ and $\partial_{x_i}(x_j^m) = 0$, for all $j \neq i$.

It is now shown that equality does not hold in Lemma 5.2.1.

Example 5.2.5. Let \mathbb{F}_2 be the field with 2 elements and let $C_4 = \langle x \mid x^4 = 1 \rangle$ be the cyclic group with 4 elements. Then by Theorem 2.3.4, $\{g\partial_x \mid g \in C_4\}$ is a K -vector space basis for $\text{Der}(\mathbb{F}_2C_4)$. Therefore $\text{Der}(\mathbb{F}_2C_4)$ has dimension 4.

Let $\mathfrak{L} = (\mathbb{F}_2C_4)_L$ and let f be an arbitrary \mathbb{F}_2 -linear map from \mathbb{F}_2C_4 to \mathbb{F}_2C_4 . Then since \mathbb{F}_2C_4 is a commutative algebra all multiplications in \mathfrak{L} are zero. Also $f([a, b]) = f(0) = 0 = [f(a), b] + [a, f(b)]$, for any $a, b \in \mathfrak{L}$. Therefore $f \in Der(\mathfrak{L})$ for all \mathbb{F}_2 -linear maps f . f is a linear transformation and so can be represented by a 4×4 matrix over \mathbb{F}_2 and so $Der(\mathfrak{L})$ has dimension 16. Thus $Der(\mathfrak{L}) \not\subseteq Der(\mathbb{F}_2C_4)$.

Let ι be the identity map on \mathfrak{L} . Then ι is K -linear and $\iota([a, b]) = \iota(0) = 0$ and $[\iota(a), b] + [a, \iota(b)] = 0 + 0 = 0$. Thus $\iota \in Der(\mathfrak{L})$. However, $\iota \notin Der(\mathbb{F}_2C_4)$, since for any units a, b in \mathbb{F}_2C_4 , $\iota(ab) = ab \neq 0 = ab + ab = \iota(a)b + a\iota(b)$.

Definition 5.2.6. Let \mathbb{F} be the prime subfield of the finite field K and let $g \in G$. Then g can be written as $g = xh$, where $x = \prod_{i=0}^{n-1} x_i^{r_i} \in X$ and $h \in H$. Define

$$R_j: G \rightarrow \mathbb{F} \text{ by } g = \prod_{i=0}^{n-1} x_i^{r_i} h \mapsto r_j \pmod{p}, \text{ for } j = 0, 1, \dots, n-1.$$

Remark 5.2.7. Let $g \in G$ and so g can be written as $g = x_j^{r_j} y h$, where $y = \prod_{i \neq j} x_i^{r_i} \in X$ and $h \in H$. Then $\partial_{x_j}(g) = \partial_{x_j}(x_j^{r_j} y h) = \partial_{x_j}(x_j^{r_j}) y h + x_j^{r_j} \partial_{x_j}(y) h + x_j^{r_j} y \partial_{x_j}(h)$. However by Theorem 2.3.4 and Lemma 2.1 of [12], $\partial_{x_j}(x_j^{r_j}) = r_j x_j^{r_j-1}$ and $\partial_{x_j}(y) = 0$. Furthermore by Theorem 3.1 of [12], $\partial_{x_j}(h) = 0$. Therefore $\partial_{x_j}(g) = r_j x_j^{r_j-1} y h = R_j(g) x_j^{-1} g$. Thus $\partial_{x_j}(g) = 0 \iff g \in G_j$.

The following identities are used throughout this chapter.

Lemma 5.2.8. *Let K be a finite field of positive characteristic p and let G be a finite abelian group such that its Sylow p -subgroup is generated by $\{x_0, x_1, \dots, x_{n-1}\}$. Let $\alpha, \beta \in KG$. Then for $i, j \in \{0, 1, \dots, n-1\}$*

$$[\partial_{x_i}, \partial_{x_j}] = 0, \tag{5.5}$$

$$[\alpha \partial_{x_i}, \beta \partial_{x_j}] = \alpha \partial_{x_i}(\beta) \partial_{x_j} - \beta \partial_{x_j}(\alpha) \partial_{x_i} \text{ and} \tag{5.6}$$

$$[\partial_{x_i}, \beta \partial_{x_j}] = \partial_{x_i}(\beta) \partial_{x_j}. \tag{5.7}$$

Proof. Let $i, j \in \{0, 1, \dots, n-1\}$ and let $g \in G$. By Equation (5.1), Equation (5.5) is immediate when $i = j$. Let $i \neq j$. Then by Remark 5.2.7

$$\begin{aligned}\partial_{x_i}\partial_{x_j}(g) &= \partial_{x_i}(R_j(g)x_j^{-1}g) = R_j(g)x_j^{-1}\partial_{x_i}(g) = R_j(g)x_j^{-1}R_i(g)x_i^{-1}g \\ &= R_i(g)x_i^{-1}R_j(g)x_j^{-1}g = R_i(g)x_i^{-1}\partial_{x_j}(g) = \partial_{x_j}(R_i(g)x_i^{-1}g) = \partial_{x_j}\partial_{x_i}(g).\end{aligned}$$

Therefore $[\partial_{x_i}, \partial_{x_j}](g) = 0$ for any $g \in G$. Hence $[\partial_{x_i}, \partial_{x_j}] = 0$, for any $i, j \in \{0, 1, \dots, n-1\}$, since G is a K -vector space basis for KG .

Let $\alpha, \beta \in KG$. Then since KG is commutative

$$\begin{aligned}[\alpha\partial_{x_i}, \beta\partial_{x_j}] &= \alpha\partial_{x_i}(\beta\partial_{x_j}) - \beta\partial_{x_j}(\alpha\partial_{x_i}) \\ &= \alpha\partial_{x_i}(\beta)\partial_{x_j} + \alpha\beta\partial_{x_i}\partial_{x_j} - \beta\partial_{x_j}(\alpha)\partial_{x_i} - \alpha\beta\partial_{x_j}\partial_{x_i} \\ &= \alpha\partial_{x_i}(\beta)\partial_{x_j} - \beta\partial_{x_j}(\alpha)\partial_{x_i} + \alpha\beta[\partial_{x_i}, \partial_{x_j}] \\ &= \alpha\partial_{x_i}(\beta)\partial_{x_j} - \beta\partial_{x_j}(\alpha)\partial_{x_i}, \text{ since } [\partial_{x_i}, \partial_{x_j}] = 0.\end{aligned}$$

In particular letting $\alpha = 1$ in Equation (5.6), gives Equation (5.7). \square

Theorem 5.2.9. *Let K be a finite field and let G be a finite abelian group. Then $Der(KG)$ has trivial center.*

Proof. Let G be a finite abelian group such that its Sylow p -subgroup is generated by $\{x_0, x_1, \dots, x_{n-1}\}$ and let $\mathcal{B} = \{g\partial_{x_i} \mid g \in G, i = 0, 1, \dots, n-1\}$. Then by Theorem 2.3.4, \mathcal{B} is a K -vector space basis for $\mathfrak{g} = Der(KG)$. Let a be an arbitrary element of the center of \mathfrak{g} and so a can be written as $a = \sum_{i=0}^{n-1} \sum_{g \in G} a_{i,g} g \partial_{x_i}$, where $a_{i,g} \in K$. By Equation (5.7), $[\partial_{x_j}, g\partial_{x_i}] = \partial_{x_j}(g)\partial_{x_i}$ and so for any $j \in$

$\{0, 1, \dots, n-1\}$

$$\begin{aligned} 0 &= [\partial_{x_j}, a] = [\partial_{x_j}, \sum_{i=0}^{n-1} \sum_{g \in G} a_{i,g} g \partial_{x_i}] = \sum_{i=0}^{n-1} \sum_{g \in G} a_{i,g} [\partial_{x_j}, g \partial_{x_i}] \\ &= \sum_{i=0}^{n-1} \sum_{g \in G} a_{i,g} \partial_{x_j}(g) \partial_{x_i} = \sum_{i=0}^{n-1} \left(\sum_{g \in G} a_{i,g} \partial_{x_j}(g) \right) \partial_{x_i}. \end{aligned}$$

Therefore $\sum_{g \in G} a_{i,g} \partial_{x_j}(g) = 0$, for all $i, j \in \{0, 1, \dots, n-1\}$, since $\partial_{x_i} \in \mathcal{B}$ for all i . Let G_j be the group defined in Definition 5.2.3. Then by Remark 5.2.7, $0 = \sum_{g \in G} a_{i,g} \partial_{x_j}(g) = \sum_{g \notin G_j} a_{i,g} R_j(g) x_j^{-1} g$. Multiplying this equation by x_j gives $\sum_{g \notin G_j} a_{i,g} R_j(g) g = 0$ and since G_j is a subset of G , the elements of G_j are linearly independent in KG and so $a_{i,g} R_j(g) = 0$, for all $g \notin G_j$ and $i \in \{0, 1, \dots, n-1\}$. By Definition 5.2.6, $R_j(g) \neq 0 \pmod{p}$, for all $g \notin G_j$. Therefore for any $j \in \{0, 1, \dots, n-1\}$, $a_{i,g} = 0$ for all $g \notin G_j$ and $i \in \{0, 1, \dots, n-1\}$.

Let $g \in G$. If $g \notin H = \bigcap_{j=0}^{n-1} G_j$, then $g \notin G_j$ for some $j \in \{0, 1, \dots, n-1\}$ and so

$a_{i,g} = 0$ for all $g \notin H$ and $i \in \{0, 1, \dots, n-1\}$. Thus we can write $a = \sum_{i=0}^{n-1} \sum_{g \in H} a_{i,g} g \partial_{x_i}$. Note that for $g \in H$, $\partial_{x_j}(g) = 0$, for all j (by Theorem 3.1 of [12]). Hence, for any $j \in \{0, 1, \dots, n-1\}$, by Equation (5.6)

$$\begin{aligned} 0 &= [a, x_j \partial_{x_j}] = \left[\sum_{i=0}^{n-1} \sum_{g \in H} a_{i,g} g \partial_{x_i}, x_j \partial_{x_j} \right] = \sum_{i=0}^{n-1} \sum_{g \in H} a_{i,g} [g \partial_{x_i}, x_j \partial_{x_j}] \\ &= \sum_{i=0}^{n-1} \sum_{g \in H} a_{i,g} (g \partial_{x_i}(x_j) \partial_{x_j} - x_j \partial_{x_j}(g) \partial_{x_i}) = \sum_{i=0}^{n-1} \sum_{g \in H} a_{i,g} g \partial_{x_i}(x_j) \partial_{x_j} = \sum_{g \in H} a_{j,g} g \partial_{x_j}. \end{aligned}$$

The set $\{g \partial_{x_j} \mid g \in H, j \in \{0, 1, \dots, n-1\}\}$ is linearly independent, since it is a subset of \mathcal{B} . Therefore $a_{j,g} = 0$, for all $g \in H$ and $j \in \{0, 1, \dots, n-1\}$. Thus $a = 0$ and so $\mathfrak{g} = \text{Der}(KG)$ has trivial center. \square

Definition 5.2.10 is used in the statement of Theorem 5.2.11.

Definition 5.2.10. Let G be a multiplicative abelian group, let K^+ be the additive group of a field K and let $\lambda \in \text{Hom}(G, K^+)$. Define $\lambda^\# : KG \rightarrow KG$ by $\sum_{g \in G} k_g g \mapsto \sum_{g \in G} k_g \lambda(g)g$.

Theorem 5.2.11. [39] *Let G be a multiplicative abelian group, let $A = K[G]$, and let Λ be a non zero K -subspace of $\text{Hom}(G, K^+)$. Then $\Delta = \Lambda^\#$ is a nonzero K -vector space of commuting derivations of A and $A \otimes \Delta = A\Delta$ is a simple Lie algebra if and only if $G^A = \langle 1 \rangle$ and $\dim_K \Lambda \geq 2$ when $\text{char}K = 2$.*

Remark 5.2.12. Let K be a finite field of positive characteristic p and let G be a finite abelian group such that its Sylow p -subgroup is generated by $\{x_0, x_1, \dots, x_{n-1}\}$. Let $\Lambda = \text{Hom}(G, K^+)$ and for $i = 0, 1, \dots, n-1$ let λ_i be the element of Λ such that $\lambda_i(x_i) = 1$ and $\lambda_i(x_j) = 0$ for all $j \neq i$. By Definition 5.2.10 and Theorem 5.2.11 $\lambda_i^\# = x_i \partial_{x_i}$. Therefore $\{x_i \partial_{x_i} \mid i = 0, 1, \dots, n-1\} \subseteq \Delta = \Lambda^\#$ and so $A\Delta = A \otimes \Delta = \text{Der}(KG)$. Let $KG = \mathbb{F}_{p^m} C_p^n$. Then $G^A = \{g \in G \mid \lambda(g) = 0 \text{ for all } \lambda \in \Lambda\} = \langle 1 \rangle$, since for any $g \in G \setminus \{1\}$, $\partial_{x_j}(g) \neq 0$, for some $j = 0, 1, \dots, n-1$. Conversely, let $h \in G$ and so $\text{ord}(h) = p^l r$, where $p \nmid r$. If $l > 1$ or $r > 1$, then $1 \neq h^p \in G^A$. Therefore by Theorem 5.2.11, $\text{Der}(KG)$ is simple if and only $KG = \mathbb{F}_{p^m} C_p^n$, where $n > 1$, if $p = 2$.

The main result of Section 5.4 is the following:

Theorem 5.4.14. *Let K be a finite field of characteristic p and let G be a finite abelian group such that $G = X \times H$, where X is an elementary abelian p -group and H is a p -regular group. Then $\text{Der}(KG)$ is a complete Lie algebra.*

It is often useful when studying algebraic properties to have examples of algebraic structures that possess these properties. To this end, Figure 5.1 is a Venn diagram partitioning $\text{Der}(KG)$ by the properties of being complete, simple or perfect Lie algebras, where G is a finite group and K is a finite field. Examples are

given in Figure 5.1 of each of these subsets and are fully classified in the simple case.

It is clear from the definitions that all simple Lie algebras are perfect. The group algebras KG such that $Der(KG)$ is simple are classified in Theorem 5.2.11.

By Theorem 5.4.14, the simple Lie algebras are complete, as are the Lie algebras $Der(\mathbb{F}_3C_6)$, $Der(\mathbb{F}_2C_2)$ and $Der(\mathbb{F}_2C_6)$. In Example 5.4.4, $Der(\mathbb{F}_2(C_4 \times C_4 \times C_2))$ is shown to be complete. $Der(\mathbb{F}_2(C_4 \times C_2))$ is shown to be noncomplete in Example 5.4.3. The Lie algebras $Der(\mathbb{F}_2(C_4 \times C_4))$, $Der(\mathbb{F}_2C_4)$ and $Der(\mathbb{F}_2C_8)$ were verified to be noncomplete using GAP [18].

The perfectness or nonperfectness of all of these examples was also verified using GAP [18].

Lemma 5.2.13. *Let K be a finite field of characteristic p and let G be the direct product of $n > 1$ copies of the cyclic group of order p . Further, let $\mathfrak{g} = Der(KG)$. Then the derivation algebra $Der(\mathfrak{g})$ is complete.*

Proof. By Theorem 5.2.9, \mathfrak{g} has trivial center. By [39], $Der(KG)$ is simple and so it is perfect. Therefore by Theorem 5.1.12 the derivation algebra $Der(\mathfrak{g})$ is complete. □

Lemma 5.2.13 motivates the following question: When is $\mathfrak{g} = Der(KG)$ complete? Table 5.1 illustrates the dimensions of $Der_i(\mathfrak{g})$ where $\mathfrak{g} = Der(KG)$, for small KG . The dimensions were computed using GAP [18]. By Lemma 5.1.13, the derivation tower stabilises and so the dimensions of $Der_i(\mathfrak{g})$ will cease to increase for some i . It can be seen from Table 5.1 that the tower stabilises quickly ($i < 6$) for the small group algebras chosen. Memory restrictions on the computer used prevented the computation of $dim(Der_2(\mathfrak{g}))$, where $\mathfrak{g} = Der(\mathbb{F}_2C_{128})$. A pattern that seems to emerge from Table 5.1 is that $\mathfrak{g} = Der(KG)$ is complete when G is elementary abelian.

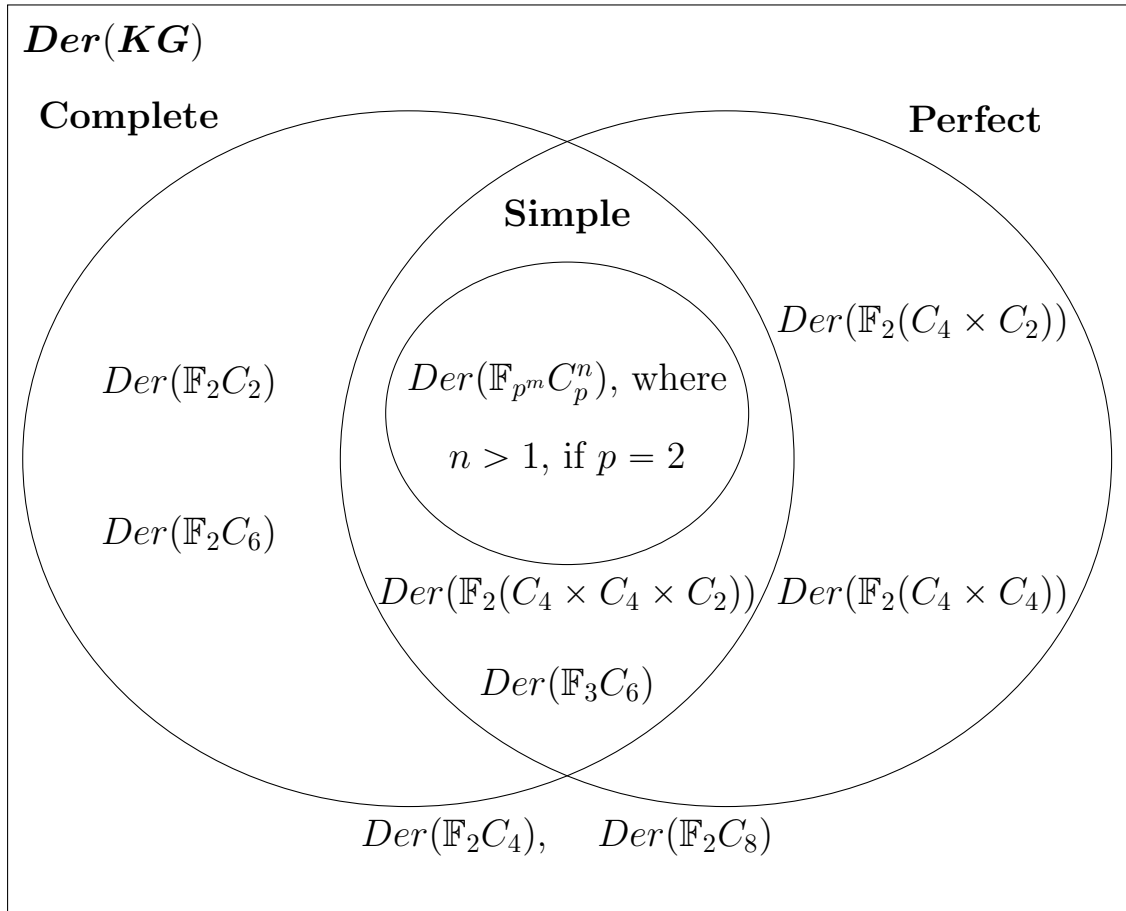


Figure 5.1: A Venn diagram showing examples of derivation algebras of finite group algebras for all possible subsets of the set of properties {complete, simple, perfect}.

5.3 The Derivations of Modular Elementary Abelian Group Algebras are Complete

Let p be a prime number, let n be a positive integer and let K be a finite field of positive characteristic p . Furthermore, let G be the direct product of n copies of the cyclic group of order p . Let \mathfrak{g} be the Lie algebra of derivations of KG and let $\mathcal{B} = \{g\partial_{x_i} \mid g \in G, i \in \{0, \dots, n-1\}\}$. Then by Theorem 2.3.4, \mathcal{B} is a K -vector space basis of $\mathfrak{g} = Der(KG)$. The main Theorem of this section shows that \mathfrak{g} is a complete Lie algebra.

Definition 5.3.1. Let a be a nonzero element of a Lie algebra \mathfrak{g} over a field K

\mathfrak{g}	i	0	1	2	3	4	5	6
$Der(\mathbb{F}_2C_2)$	$dim(Der_i(\mathfrak{g}))$	2	2	2	2	2	2	2
$Der(\mathbb{F}_2C_4)$	$dim(Der_i(\mathfrak{g}))$	4	6	6	6	6	6	6
$Der(\mathbb{F}_2(C_2 \times C_2))$	$dim(Der_i(\mathfrak{g}))$	8	8	8	8	8	8	8
$Der(\mathbb{F}_2C_8)$	$dim(Der_i(\mathfrak{g}))$	8	12	14	14	14	14	14
$Der(\mathbb{F}_2(C_4 \times C_2))$	$dim(Der_i(\mathfrak{g}))$	16	18	18	18	18	18	18
$Der(\mathbb{F}_2C_2^3)$	$dim(Der_i(\mathfrak{g}))$	24	24	24	24	24	24	24
$Der(\mathbb{F}_2D_8)$	$dim(Der_i(\mathfrak{g}))$	12	16	16	16	16	16	16
$Der(\mathbb{F}_2Q_8)$	$dim(Der_i(\mathfrak{g}))$	10	26	29	29	29	29	29
$Der(\mathbb{F}_2C_{16})$	$dim(Der_i(\mathfrak{g}))$	16	24	28	28	28	28	28
$Der(\mathbb{F}_2(C_8 \times C_2))$	$dim(Der_i(\mathfrak{g}))$	32	36	36	36	36	36	36
$Der(\mathbb{F}_2(C_4 \times C_4))$	$dim(Der_i(\mathfrak{g}))$	32	40	40	40	40	40	40
$Der(\mathbb{F}_2C_2^4)$	$dim(Der_i(\mathfrak{g}))$	64	64	64	64	64	64	64
$Der(\mathbb{F}_2C_{32})$	$dim(Der_i(\mathfrak{g}))$	32	48	56	56	56	56	56
$Der(\mathbb{F}_2(C_{16} \times C_2))$	$dim(Der_i(\mathfrak{g}))$	64	72	72	72	72	72	72
$Der(\mathbb{F}_2(C_8 \times C_4))$	$dim(Der_i(\mathfrak{g}))$	64	80	80	80	80	80	80
$Der(\mathbb{F}_2(C_4^2 \times C_2))$	$dim(Der_i(\mathfrak{g}))$	96	96	96	96	96	96	96
$Der(\mathbb{F}_2C_{64})$	$dim(Der_i(\mathfrak{g}))$	64	96	112	112	112	112	112
$Der(\mathbb{F}_2C_{128})$	$dim(Der_i(\mathfrak{g}))$	128	192	?				
$Der(\mathbb{F}_2C_2^n)$	$dim(Der_i(\mathfrak{g}))$	$n2^n$?					

Table 5.1: A table showing the dimension of $Der_i(\mathfrak{g})$, where $\mathfrak{g} = Der(KG)$ for selected small KG .

and let V be the 1-dimensional K -vector subspace of \mathfrak{g} generated by a . Define the *range* of a , denoted $R(a)$ to be $[V, \mathfrak{g}]$. $R(a)$ is a K -vector subspace of \mathfrak{g} .

Recall the set $S = \{x_i \mid i = 0, 1, \dots, n-1\}$ which was defined in Definition 5.2.3.

Lemma 5.3.2. *The set $\{g\partial_{x_i} \mid g \in G_j, x_i \in S\}$ is a K -vector space basis for the centraliser of ∂_{x_j} in \mathfrak{g} .*

Proof. Let b be an arbitrary element of \mathfrak{g} and write $b = \sum_{i=0}^{n-1} \sum_{e=0}^{p-1} \beta_{i,e} x_j^e \partial_{x_i}$, where

$\beta_{i,e} \in KG_j$. Then by Equation (5.7)

$$[\partial_{x_j}, b] = \sum_{i=0}^{n-1} \sum_{e=0}^{p-1} [\partial_{x_j}, \beta_{i,e} x_j^e \partial_{x_i}] = \sum_{i=0}^{n-1} \sum_{e=0}^{p-1} \beta_{i,e} \partial_{x_j} (x_j^e) \partial_{x_i} = \sum_{i=0}^{n-1} \sum_{e=0}^{p-1} \beta_{i,e} e x_j^{e-1} \partial_{x_i}.$$

Therefore $b \in C(\partial_{x_j}, \mathfrak{g})$ if and only if $\sum_{e=1}^{p-1} \beta_{i,e} e x_j^{e-1} = 0$, that is, if and only if $\beta_{i,e} = 0$, for all $i = 0, 1, \dots, n-1$ and $e = 1, 2, \dots, p-1$. Thus $b \in C(\partial_{x_j}, \mathfrak{g})$ if and only if $b = \sum_{i=0}^{n-1} \beta_{i,0} \partial_{x_i}$, where $\beta_{i,0} \in KG_j$. This implies that the set $\{g \partial_{x_i} \mid g \in G_j, x_i \in S\}$ is a K -vector space basis for $C(\partial_{x_j}, \mathfrak{g})$. \square

Lemma 5.3.3. $C(\partial_{x_0}, \mathfrak{g}) \bigcap_{j=0}^{n-1} C(x_j \partial_{x_0}, \mathfrak{g}) = \{0\}$.

Proof. Let $b \in C(\partial_{x_0}, \mathfrak{g}) \bigcap_{j=0}^{n-1} C(x_j \partial_{x_0}, \mathfrak{g})$. Therefore by Lemma 5.3.2, $b = \sum_{i=0}^{n-1} \beta_i \partial_{x_i}$, for some $\beta_i \in KG_0$. Thus for any $j \in \{0, 1, \dots, n-1\}$

$$0 = [b, x_j \partial_{x_0}] = \sum_{i=0}^{n-1} [\beta_i \partial_{x_i}, x_j \partial_{x_0}] = \beta_j \partial_{x_0}.$$

Therefore $\beta_j = 0$, for all $j \in \{0, 1, \dots, n-1\}$ and so $b = 0$. \square

Lemma 5.3.4. *The set $\{\partial_{x_i} \mid i = 0, 1, \dots, n-1\}$ is a K -vector space basis for $\bigcap_{i=0}^{n-1} C(\partial_{x_i}, \mathfrak{g})$.*

Proof. By Lemma 5.3.2, for each $i \in \{0, 1, \dots, n-1\}$ the set $\{g \partial_{x_j} \mid g \in G_i, x_j \in S\}$ is a K -vector space basis for $C(\partial_{x_i}, \mathfrak{g})$. This K -vector space basis is a subset of \mathcal{B} for each $i \in \{0, 1, \dots, n-1\}$. Therefore the set $\bigcap_{i=0}^{n-1} \{g \partial_{x_j} \mid g \in G_i, x_j \in S\}$ is a K -vector space basis for $\bigcap_{i=0}^{n-1} C(\partial_{x_i}, \mathfrak{g})$. However

$$\bigcap_{i=0}^{n-1} \{g \partial_{x_j} \mid g \in G_i, x_j \in S\} = \{g \partial_{x_j} \mid g \in \bigcap_{i=0}^{n-1} G_i, x_j \in S\} = \{\partial_{x_j} \mid x_j \in S\}.$$

\square

Definition 5.3.5. Let G be the direct product of n copies of the cyclic group of order p , where $S = \{x_i \mid i = 0, 1, \dots, n-1\}$ is a generating set for G . Let $g \in G$ and write $g = x_0^{e_0} x_1^{e_1} \dots x_{n-1}^{e_{n-1}}$, where $e_i \in \{0, 1, \dots, p-1\}$ for $i \in \{0, 1, \dots, n-1\}$. Define the *weight* of g , denoted $wt(g)$ to be the number of nonzero exponents of g , that is, $wt(g) = \sum_{e_i \neq 0} 1$. Also, define the *exponent sum* of g , denoted $E(g)$ to be the integer sum of the exponents of g , that is, $E(g) = \sum_{i=0}^{n-1} e_i$.

Lemmas 5.3.6 and 5.3.7 are now established before the proof of Theorem 5.3.8 is given.

Lemma 5.3.6. *Let p be a prime number, let n be a positive integer and let K be a finite field of positive characteristic p . Let G be the direct product of n copies of the cyclic group of order p , where $S = \{x_i \mid i = 0, 1, \dots, n-1\}$ is a generating set for G . Let $\mathfrak{g} = Der(KG)$ and let $\mathcal{B} = \{g\partial_{x_i} \mid g \in G, x_i \in S\}$ and so \mathcal{B} is a K -vector space basis for \mathfrak{g} . Further, Let $D \in Der(\mathfrak{g})$ and let $g \in G$ such that $wt(g) \leq 1$ and so $g = x_j^e$, for some $j \in \{0, 1, \dots, n-1\}$ and $e \in \{0, 1, \dots, p-1\}$. Write $D(g\partial_{x_0}) = \sum_{i=0}^{n-1} \alpha_{i,g} \partial_{x_i}$, where $\alpha_{i,g} \in KG$. Then for all $i \in \{0, 1, \dots, n-1\}$*

$$\partial_{x_0}(\alpha_{i,x_j^e}) = x_j^e \partial_{x_0}(\alpha_{i,1}) - \partial_{x_0}(x_j) e x_j^{e-1} \alpha_{j,1} + e \partial_{x_0}(x_j) \alpha_{i,x_j^{e-1}}. \quad (5.8)$$

$$\text{Also, } \alpha_{i,g} = g \alpha_{i,1}, \quad \text{for all } i \in \{1, 2, \dots, n-1\}. \quad (5.9)$$

Proof. Let $g \in G$ such that $wt(g) \leq 1$ and so $g = x_j^e$, for some $j \in \{0, 1, \dots, n-1\}$ and $e \in \{0, 1, \dots, p-1\}$. Then by Equation (5.7),

$$[\partial_{x_0}, x_j^e \partial_{x_0}] = \partial_{x_0}(x_j^e) \partial_{x_0} = \partial_{x_0}(x_j) e x_j^{e-1} \partial_{x_0}.$$

Therefore $0 = [\partial_{x_0}, x_j^e \partial_{x_0}] - \partial_{x_0}(x_j) e x_j^{e-1} \partial_{x_0}$. Applying D to this equation gives

$$\begin{aligned} 0 &= [D(\partial_{x_0}), x_j^e \partial_{x_0}] + [\partial_{x_0}, D(x_j^e \partial_{x_0})] - \partial_{x_0}(x_j) e D(x_j^{e-1} \partial_{x_0}) \\ &= \sum_{i=0}^{n-1} [\alpha_{i,1} \partial_{x_i}, x_j^e \partial_{x_0}] + \sum_{i=0}^{n-1} [\partial_{x_0}, \alpha_{i,x_j^e} \partial_{x_i}] - \partial_{x_0}(x_j) e \sum_{i=0}^{n-1} \alpha_{i,x_j^{e-1}} \partial_{x_i}. \end{aligned}$$

Therefore by Equations (5.6) and (5.7)

$$\begin{aligned} 0 &= \sum_{i=0}^{n-1} \left(\alpha_{i,1} \partial_{x_i}(x_j^e) \partial_{x_0} - x_j^e \partial_{x_0}(\alpha_{i,1}) \partial_{x_i} + \partial_{x_0}(\alpha_{i,x_j^e}) \partial_{x_i} - \partial_{x_0}(x_j) e \alpha_{i,x_j^{e-1}} \partial_{x_i} \right) \\ &= \alpha_{j,1} e x_j^{e-1} \partial_{x_0} - x_j^e \sum_{i=0}^{n-1} \partial_{x_0}(\alpha_{i,1}) \partial_{x_i} + \sum_{i=0}^{n-1} \partial_{x_0}(\alpha_{i,x_j^e}) \partial_{x_i} - \partial_{x_0}(x_j) e \sum_{i=0}^{n-1} \alpha_{i,x_j^{e-1}} \partial_{x_i}. \end{aligned}$$

Equating the coefficients of ∂_{x_0} gives

$$\begin{aligned} \alpha_{j,1} e x_j^{e-1} - x_j^e \partial_{x_0}(\alpha_{0,1}) + \partial_{x_0}(\alpha_{0,x_j^e}) - \partial_{x_0}(x_j) e \alpha_{0,x_j^{e-1}} &= 0 \quad \text{and so} \\ \partial_{x_0}(\alpha_{0,x_j^e}) &= x_j^e \partial_{x_0}(\alpha_{0,1}) - \alpha_{j,1} e x_j^{e-1} + \partial_{x_0}(x_j) e \alpha_{0,x_j^{e-1}}. \end{aligned} \quad (5.10)$$

Equating the coefficients of ∂_{x_i} , for $i > 0$ gives

$$\begin{aligned} -x_j^e \partial_{x_0}(\alpha_{i,1}) + \partial_{x_0}(\alpha_{i,x_j^e}) - \partial_{x_0}(x_j) e \alpha_{i,x_j^{e-1}} &= 0 \quad \text{and so} \\ \partial_{x_0}(\alpha_{i,x_j^e}) &= x_j^e \partial_{x_0}(\alpha_{i,1}) + \partial_{x_0}(x_j) e \alpha_{i,x_j^{e-1}}. \end{aligned} \quad (5.11)$$

Equations (5.10) and (5.11) combine to give Equation (5.8).

Let $k \in \{1, 2, \dots, n-1\}$. Then by Equation (5.6), $[x_k^e \partial_{x_0}, x_0 \partial_{x_0}] = x_k^e \partial_{x_0}$.

Applying D gives

$$\begin{aligned} 0 &= [D(x_k^e \partial_{x_0}), x_0 \partial_{x_0}] + [x_k^e \partial_{x_0}, D(x_0 \partial_{x_0})] - D(x_k^e \partial_{x_0}) \\ &= \sum_{i=0}^{n-1} [\alpha_{i,x_k^e} \partial_{x_i}, x_0 \partial_{x_0}] + \sum_{i=0}^{n-1} [x_k^e \partial_{x_0}, \alpha_{i,x_0} \partial_{x_i}] - \sum_{i=0}^{n-1} \alpha_{i,x_k^e} \partial_{x_i}. \end{aligned}$$

Therefore by Equations (5.6) and (5.7)

$$\begin{aligned}
& \sum_{i=0}^{n-1} \left(\alpha_{i,x_k^e} \partial_{x_i}(x_0) \partial_{x_0} - x_0 \partial_{x_0}(\alpha_{i,x_k^e}) \partial_{x_i} + x_k^e \partial_{x_0}(\alpha_{i,x_0}) \partial_{x_i} - \alpha_{i,x_0} \partial_{x_i}(x_k^e) \partial_{x_0} - \alpha_{i,x_k^e} \partial_{x_i} \right) \\
&= \alpha_{0,x_k^e} \partial_{x_0} - x_0 \sum_{i=0}^{n-1} \partial_{x_0}(\alpha_{i,x_k^e}) \partial_{x_i} + \sum_{i=0}^{n-1} x_k^e \partial_{x_0}(\alpha_{i,x_0}) \partial_{x_i} - \alpha_{k,x_0} e x_k^{e-1} \partial_{x_0} - \sum_{i=0}^{n-1} \alpha_{i,x_k^e} \partial_{x_i} \\
&= 0.
\end{aligned}$$

Therefore

$$\begin{aligned}
0 &= (\alpha_{0,x_k^e} - x_0 \partial_{x_0}(\alpha_{0,x_k^e}) + x_k^e \partial_{x_0}(\alpha_{0,x_0}) - \alpha_{k,x_0} e x_k^{e-1} - \alpha_{0,x_k^e}) \partial_{x_0} \\
&\quad + (-x_0 \partial_{x_0}(\alpha_{i,x_k^e}) + x_k^e \partial_{x_0}(\alpha_{i,x_0}) - \alpha_{i,x_k^e}) \partial_{x_i}.
\end{aligned} \tag{5.12}$$

Equating the coefficients of ∂_{x_0} gives

$$-x_0 \partial_{x_0}(\alpha_{0,x_k^e}) + x_k^e \partial_{x_0}(\alpha_{0,x_0}) - \alpha_{k,x_0} e x_k^{e-1} = 0. \tag{5.13}$$

and equating the coefficients of ∂_{x_i} for $i > 0$ gives

$$-x_0 \partial_{x_0}(\alpha_{i,x_k^e}) + x_k^e \partial_{x_0}(\alpha_{i,x_0}) - \alpha_{i,x_k^e} = 0. \tag{5.14}$$

Letting $i > 0$, $j = 0$ and $e = 1$ in Equation (5.8) implies

$$\partial_{x_0}(\alpha_{i,x_0}) = x_0 \partial_{x_0}(\alpha_{i,1}) + \alpha_{i,1}. \tag{5.15}$$

It remains to prove Equation (5.9). The proof is divided into 4 cases, namely when $g = 1$, $g = x_0$, $g \in \{x_k^e \mid k \in \{1, 2, \dots, n-1\}, e \in \{1, 2, \dots, p-1\}\}$ and $g \in \{x_0^e \mid e \in \{2, 3, \dots, p-1\}\}$.

Case (1): $g = 1$. For all $i \in \{1, 2, \dots, n-1\}$, $\alpha_{i,g} = \alpha_{i,1} = g\alpha_{i,1}$.

Case (2): $g = x_0$. Letting $i = 0$ and $j = k > 0$ in Equation (5.8) implies

$$\partial_{x_0}(\alpha_{0,x_k^e}) = x_k^e \partial_{x_0}(\alpha_{0,1}) - ex_k^{e-1} \alpha_{k,1}. \quad (5.16)$$

Letting $i = j = 0$ and $e = 1$ in Equation (5.8) implies

$$\partial_{x_0}(\alpha_{0,x_0}) = x_0 \partial_{x_0}(\alpha_{0,1}) - \alpha_{0,1} + \alpha_{0,1} = x_0 \partial_{x_0}(\alpha_{0,1}). \quad (5.17)$$

Using Equations (5.16) and (5.17) in Equation (5.13) gives

$$\begin{aligned} 0 &= -x_0(x_k^e \partial_{x_0}(\alpha_{0,1}) - ex_k^{e-1} \alpha_{k,1}) + x_k^e(x_0 \partial_{x_0}(\alpha_{0,1})) - \alpha_{k,x_0} ex_k^{e-1} \\ &= ex_0 x_k^{e-1} \alpha_{k,1} - \alpha_{k,x_0} ex_k^{e-1} = ex_k^{e-1}(x_0 \alpha_{k,1} - \alpha_{k,x_0}). \end{aligned}$$

for any $e \in \{0, 1, \dots, p-1\}$. Letting $e = 1$ implies $\alpha_{k,x_0} = x_0 \alpha_{k,1}$. Therefore Equation (5.9) holds for $g = x_0$.

Case (3): $g \in \{x_k^e \mid k \in \{1, 2, \dots, n-1\}, e \in \{1, 2, \dots, p-1\}\}$. Letting $i > 0$ and $j = k > 0$ in Equation (5.8) implies

$$\partial_{x_0}(\alpha_{i,x_k^e}) = x_k^e \partial_{x_0}(\alpha_{i,1}). \quad (5.18)$$

Using Equations (5.18) and (5.15) in Equation (5.14) gives

$$\begin{aligned} 0 &= -x_0(x_k^e \partial_{x_0}(\alpha_{i,1})) + x_k^e(x_0 \partial_{x_0}(\alpha_{i,1}) + \alpha_{i,1}) - \alpha_{i,x_k^e} \\ &= x_k^e \alpha_{i,1} - \alpha_{i,x_k^e}. \end{aligned}$$

Therefore Equation (5.9) holds for $g \in \{x_k^e \mid k \in \{1, 2, \dots, n-1\}, e \in \{1, 2, \dots, p-1\}\}$.

Case (4): $g \in \{x_0^e \mid e \in \{2, 3, \dots, p-1\}\}$. Equation (5.21) will be useful in proving

Equation (5.9) in this case and is now established. By Equation (5.6),

$$[x_0 \partial_{x_0}, x_0^e \partial_{x_0}] = x_0 e x_0^{e-1} \partial_{x_0} - x_0^e \partial_{x_0} = (e-1)x_0^e \partial_{x_0}.$$

Applying D gives

$$\begin{aligned} 0 &= [D(x_0 \partial_{x_0}), x_0^e \partial_{x_0}] + [x_0 \partial_{x_0}, D(x_0^e \partial_{x_0})] - (e-1)D(x_0^e \partial_{x_0}) \\ &= \sum_{i=0}^{n-1} [\alpha_{i,x_0} \partial_{x_i}, x_0^e \partial_{x_0}] + \sum_{i=0}^{n-1} [x_0 \partial_{x_0}, \alpha_{i,x_0^e} \partial_{x_i}] - (e-1) \sum_{i=0}^{n-1} \alpha_{i,x_0^e} \partial_{x_i}. \end{aligned}$$

Therefore by Equation (5.6)

$$\begin{aligned} \alpha_{0,x_0} e x_0^{e-1} \partial_{x_0} - x_0^e \sum_{i=0}^{n-1} \partial_{x_0}(\alpha_{i,x_0}) \partial_{x_i} + \sum_{i=0}^{n-1} x_0 \partial_{x_0}(\alpha_{i,x_0^e}) \partial_{x_i} \\ - \alpha_{0,x_0^e} \partial_{x_0} - (e-1) \sum_{i=0}^{n-1} \alpha_{i,x_0^e} \partial_{x_i} = 0. \end{aligned}$$

Equating the coefficients of ∂_{x_i} for $i > 0$ gives

$$-x_0^e \partial_{x_0}(\alpha_{i,x_0}) + x_0 \partial_{x_0}(\alpha_{i,x_0^e}) - (e-1)\alpha_{i,x_0^e} = 0. \quad (5.19)$$

Letting $i > 0$ and $j = 0$ in Equation (5.8) implies

$$\partial_{x_0}(\alpha_{i,x_0^e}) = x_0^e \partial_{x_0}(\alpha_{i,1}) + e\alpha_{i,x_0^{e-1}}. \quad (5.20)$$

Using Equations (5.15) and (5.20) in Equation (5.19) gives

$$\begin{aligned} 0 &= -x_0^e (x_0 \partial_{x_0}(\alpha_{i,1}) + \alpha_{i,1}) + x_0 (x_0^e \partial_{x_0}(\alpha_{i,1}) + e\alpha_{i,x_0^{e-1}}) - (e-1)\alpha_{i,x_0^e} \\ &= -x_0^e \alpha_{i,1} + e x_0 \alpha_{i,x_0^{e-1}} - (e-1)\alpha_{i,x_0^e}. \end{aligned}$$

Therefore

$$(e - 1)\alpha_{i,x_0^e} = ex_0\alpha_{i,x_0^{e-1}} - x_0^e\alpha_{i,1}. \quad (5.21)$$

It is now shown by induction on e that Equation (5.9) holds for $g \in \{x_0^e \mid e \in \{1, 2, \dots, p-1\}\}$. Case (2) is the base case ($e = 1$). Let $r \in \{2, 3, \dots, p-1\}$ and assume that $\alpha_{i,x_0^{r-1}} = x_0^{r-1}\alpha_{i,1}$, for all $i \in \{1, 2, \dots, n-1\}$. Then by Equation (5.21)

$$(r - 1)\alpha_{i,x_0^r} = rx_0\alpha_{i,x_0^{r-1}} - x_0^r\alpha_{i,1} = rx_0(x_0^{r-1}\alpha_{i,1}) - x_0^r\alpha_{i,1} = (r - 1)x_0^r\alpha_{i,1}.$$

Therefore $\alpha_{i,x_0^r} = x_0^r\alpha_{i,1}$, since $r - 1 \in K^*$. Thus by induction $\alpha_{i,x_0^e} = x_0^e\alpha_{i,1}$, for all $i \in \{1, 2, \dots, n-1\}$ and $e \in \{1, 2, \dots, p-1\}$. This completes the proof. \square

Lemma 5.3.7. *Let p be a prime number, let n be a positive integer and let K be a finite field of positive characteristic p . Let G be the direct product of n copies of the cyclic group of order p , where $S = \{x_i \mid i = 0, 1, \dots, n-1\}$ is a generating set for G . Also, let $D \in \mathfrak{g} = \text{Der}(\mathfrak{g})$ and $g \in G$. Suppose that there exists distinct elements t and j of $\{0, 1, \dots, n-1\}$ and an element c of \mathfrak{g} such that*

$$(i) \quad g = x_t^m g', \text{ for some } m \in \mathbb{F}_p^* \text{ and } g' \in G_t,$$

$$(ii) \quad D(h\partial_{x_j}) = [c, h\partial_{x_j}], \text{ for all } h \in G \text{ where } E(h) < E(g),$$

$$(iii) \quad D(x_t\partial_{x_t}) = [c, x_t\partial_{x_t}].$$

Then $D(g\partial_{x_j}) - [c, g\partial_{x_j}] = k_t\partial_{x_t}$, where $k_t \in K$ and $k_t = 0$ if $m \neq p-1$.

Proof. Assume that there exists distinct elements t and j of $\{0, 1, \dots, n-1\}$ and an element c of \mathfrak{g} such that conditions (i) – (iii) are satisfied. By Equation (5.7), $[\partial_{x_i}, g\partial_{x_j}] = \partial_{x_i}(g)\partial_{x_j}$. Note that $\partial_{x_i}(g) = 0$ or $\partial_{x_i}(g) = k\tilde{g}$, where $k \in K$ and $E(\tilde{g}) = E(g) - 1$. Therefore $D(\partial_{x_i}(g)\partial_{x_j}) = [c, \partial_{x_i}(g)\partial_{x_j}]$. Also $D(\partial_{x_i}) = [c, \partial_{x_i}]$, by condition (ii). Therefore letting $r = \partial_{x_i}$ and $s = g\partial_{x_j}$ in Lemma 5.1.15 implies

$b = D(g\partial_{x_j}) - [c, g\partial_{x_j}] \in C(\partial_{x_i}, \mathfrak{g})$, for all $i \in \{0, 1, \dots, n-1\}$. Therefore by Lemma 5.3.4, $b = \sum_{i=0}^{n-1} k_i \partial_{x_i}$, where $k_i \in K$. Note that $g = x_t^m h$, for some $m \in \mathbb{F}_p^*$, $h \in G_t$ and $t \neq j$ and so by Equation (5.6)

$$[x_t \partial_{x_t}, g\partial_{x_j}] = x_t \partial_{x_t}(x_t^m h) \partial_{x_j} - g\partial_{x_j}(x_t) \partial_{x_t} = m x_t^m h \partial_{x_j} - 0 = m g \partial_{x_j}.$$

Letting $r = x_t \partial_{x_t}$, $s = g\partial_{x_j}$ and $k = m$ in Lemma 5.1.16 implies $[x_t \partial_{x_t}, b] = mb$.

Thus

$$0 = mb - [x_t \partial_{x_t}, b] = m \sum_{i=0}^{n-1} k_i \partial_{x_i} - \sum_{i=0}^{n-1} k_i [x_t \partial_{x_t}, \partial_{x_i}] = m \sum_{i=0}^{n-1} k_i \partial_{x_i} + k_t \partial_{x_t}.$$

Therefore $k_i = 0$ for all $i \neq t$, since $m \in \mathbb{F}_p^*$ and so $0 = (m+1)k_t \partial_{x_t}$. If $m \neq p-1$, then $(m+1) \in \mathbb{F}_p^*$ and so $k_t = 0$. Therefore $b = k_t \partial_{x_t}$, where $k_t \in K$ and $k_t = 0$ if $m \neq p-1$. \square

Theorem 5.3.8. *Let p be a prime number, let n be a positive integer and let K be a finite field of positive characteristic p . Let G be the direct product of n copies of the cyclic group of order p . Then $Der(KG)$ is a complete Lie algebra (i.e. its center is trivial and all its derivations are inner).*

Proof. Let $\mathfrak{g} = Der(KG)$. By Theorem 5.2.9, \mathfrak{g} has trivial center and so it remains to show that all derivations of \mathfrak{g} are inner.

Let $S = \{x_i \mid i = 0, 1, \dots, n-1\}$ be a generating set for G and let $\mathcal{B} = \{g\partial_{x_i} \mid g \in G, x_i \in S\}$. Then by Theorem 2.3.4, \mathcal{B} is a K -vector space basis for \mathfrak{g} . For $j \in \{0, 1, \dots, n-1\}$, let S_j and G_j be respectively the set and the group defined in Definition 5.2.3. Let $g \in G$ and let D be an element of $Der(\mathfrak{g})$. Write $D(g\partial_{x_0}) = \sum_{i=0}^{n-1} \alpha_{i,g} \partial_{x_i}$, where $\alpha_{i,g} \in KG$. We will prove that D is the inner derivation induced by

$$c = \sum_{i=0}^{n-1} (\alpha_{0,x_i} - x_i \alpha_{0,1}) \partial_{x_i}.$$

The following is an outline of the proof. It is shown that $D(d) = [c, d]$, for all $d \in \mathfrak{g}$.

The proof is divided into five steps

- (i) $d = g\partial_{x_0}$, for all $g \in G$ such that $E(g) \leq 1$, where $E(g)$ is defined in Definition 5.3.5.
- (ii) $d = g\partial_{x_l}$, for all $l \in \{1, 2, \dots, n-1\}$ and $g \in G$ such that $E(g) \leq 1$. This step is superfluous when $n = 1$ and so we assume $n > 1$.
- (iii) $d = g\partial_{x_i}$, for all $i \in \{0, 1, \dots, n-1\}$ and $g \in G$ such that $wt(g) \leq 1$. This step is superfluous when $p = 2$ and so we assume $p > 2$.
- (iv) $d \in \mathcal{B}$. This step is superfluous when $n = 1$, since in this case $wt(g) \leq 1$ for all $g \in G$ and so we assume $n > 1$.
- (v) d is an arbitrary element of \mathfrak{g} .

Step (i): Let $g \in G$ such that $E(g) \leq 1$ and so $g = x_j^l$, for some $j \in \{0, 1, \dots, n-1\}$ and $l \in \{0, 1\}$. We will prove that $D(g\partial_{x_0}) = [c, g\partial_{x_0}]$. By Equation (5.6)

$$\begin{aligned} [c, g\partial_{x_0}] &= \sum_{i=0}^{n-1} [(\alpha_{0,x_i} - x_i\alpha_{0,1})\partial_{x_i}, x_j^l\partial_{x_0}] \\ &= \sum_{i=0}^{n-1} (\alpha_{0,x_i} - x_i\alpha_{0,1})\partial_{x_i}(x_j^l)\partial_{x_0} - \sum_{i=0}^{n-1} x_j^l\partial_{x_0}(\alpha_{0,x_i} - x_i\alpha_{0,1})\partial_{x_i}. \end{aligned}$$

Note that by the Leibniz rule $\partial_{x_0}(x_i\alpha_{0,1}) = \partial_{x_0}(x_i)\alpha_{0,1} + x_i\partial_{x_0}(\alpha_{0,1})$. In Equation (5.8), let $i = 0$ and $e = 1$. Then $\partial_{x_0}(\alpha_{0,x_j}) = x_j\partial_{x_0}(\alpha_{0,1}) - \alpha_{j,1} + \partial_{x_0}(x_j)\alpha_{0,1}$. Relabelling j as i gives $\partial_{x_0}(\alpha_{0,x_i}) = x_i\partial_{x_0}(\alpha_{0,1}) - \alpha_{i,1} + \partial_{x_0}(x_i)\alpha_{0,1}$. Thus, $\partial_{x_0}(\alpha_{0,x_i} - x_i\alpha_{0,1}) = \partial_{x_0}(\alpha_{0,x_i}) - \partial_{x_0}(x_i\alpha_{0,1}) = -\alpha_{i,1}$. Therefore

$$\begin{aligned} [c, g\partial_{x_0}] &= l(\alpha_{0,x_j} - x_j\alpha_{0,1})\partial_{x_0} - x_j^l(-\alpha_{0,1})\partial_{x_0} - \sum_{i=1}^{n-1} x_j^l(-\alpha_{i,1})\partial_{x_i} \\ &= l(\alpha_{0,x_j} - x_j\alpha_{0,1})\partial_{x_0} + x_j^l\alpha_{0,1}\partial_{x_0} + \sum_{i=1}^{n-1} \alpha_{i,x_j^l}\partial_{x_i}, \quad (\text{by Equation 5.9}). \end{aligned}$$

If $l = 0$, then $g = 1$ and

$$[c, g\partial_{x_0}] = [c, \partial_{x_0}] = 0 + \alpha_{0,1}\partial_{x_0} + \sum_{i=1}^{n-1} (\alpha_{i,1})\partial_{x_i} = \sum_{i=0}^{n-1} \alpha_{i,1}\partial_{x_i} = D(g\partial_{x_0}).$$

If $l = 1$, then $g = x_j$ and

$$[c, g\partial_{x_0}] = (\alpha_{0,x_j} - x_j\alpha_{0,1})\partial_{x_0} + x_j\alpha_{0,1}\partial_{x_0} + \sum_{i=1}^{n-1} \alpha_{i,x_j}\partial_{x_i} = \sum_{i=0}^{n-1} \alpha_{i,x_j}\partial_{x_i} = D(g\partial_{x_0}).$$

Therefore $D(g\partial_{x_0}) = [c, g\partial_{x_0}]$, for all $g \in G$ such that $E(g) \leq 1$.

Step (ii): This step is superfluous when $n = 1$ and so we assume $n > 1$. Let $l \in \{1, 2, \dots, n-1\}$, $g \in G$ such that $E(g) \leq 1$ and let $b = D(g\partial_{x_l}) - [c, g\partial_{x_l}]$. It will be shown that $b = 0$. The cases when $g \neq x_0$ and $g = x_0$ are treated separately.

Case (1): $g \neq x_0$. Let $h \in G$ such that $E(h) \leq 1$. Then

$$[h\partial_{x_0}, g\partial_{x_l}] = h\partial_{x_0}(g)\partial_{x_l} - g\partial_{x_l}(h)\partial_{x_0} = -g\partial_{x_l}(h)\partial_{x_0}.$$

Note that $\partial_{x_l}(h) = 0$ or 1 and so by the linearity of D and Step (i), $D(-g\partial_{x_l}(h)\partial_{x_0}) = [c, -g\partial_{x_l}(h)\partial_{x_0}]$ and also $D(h\partial_{x_0}) = [c, h\partial_{x_0}]$. Therefore letting $r = h\partial_{x_0}$ and $s = g\partial_{x_l}$ in Lemma 5.1.15 implies $b \in C(h\partial_{x_0}, \mathfrak{g})$, for all $h \in G$ such that $E(h) \leq 1$. Therefore by Lemma 5.3.3, $b = 0$.

Case (2): $g = x_0$. By Equation (5.7), for all $i \in \{0, 1, \dots, n-1\}$

$$[\partial_{x_i}, x_0\partial_{x_l}] = \partial_{x_i}(x_0)\partial_{x_l} = \begin{cases} \partial_{x_l} & \text{if } i = 0 \\ 0 & \text{if } i \neq 0. \end{cases}$$

By Case (1) and Step (i), $D(\partial_{x_i}) = [c, \partial_{x_i}]$ for all $i \in \{0, 1, \dots, n-1\}$. Thus, letting $r = \partial_{x_i}$ and $s = x_0\partial_{x_l}$ in Lemma 5.1.15 implies $b \in C(\partial_{x_i}, \mathfrak{g})$, for all $i \in \{0, 1, \dots, n-1\}$. Therefore by Lemma 5.3.4, $b = \sum_{i=0}^{n-1} k_i\partial_{x_i}$, where $k_i \in K$. By

Step (i) $D(x_0\partial_{x_0}) = [c, x_0\partial_{x_0}]$ and by Equation (5.6), $[x_0\partial_{x_0}, x_0\partial_{x_l}] = x_0\partial_{x_l}$. Letting $r = x_0\partial_{x_0}$, $s = x_0\partial_{x_l}$ and $k = 1$ in Lemma 5.1.16 implies $[x_0\partial_{x_0}, b] = b$. Then, by Equation (5.7)

$$0 = b + [b, x_0\partial_{x_0}] = \sum_{i=0}^{n-1} k_i \partial_{x_i} + \sum_{i=0}^{n-1} k_i [\partial_{x_i}, x_0\partial_{x_0}] = \sum_{i=0}^{n-1} k_i \partial_{x_i} + k_0 \partial_{x_0} = 2k_0 \partial_{x_0} + \sum_{i=1}^{n-1} k_i \partial_{x_i}.$$

If $p > 2$, then $k_i = 0$ for all $i \in \{0, 1, \dots, n-1\}$ and so $b = 0$. If $p = 2$, then $k_i = 0$ for all $i \neq 0$ and so $b = k_0 \partial_{x_0}$. However, by Equation (5.6), $[x_0\partial_{x_0} + x_l\partial_{x_l}, x_0\partial_{x_l}] = x_0\partial_{x_l} - x_0\partial_{x_l} = 0$. By Step (i), $D(x_0\partial_{x_0}) = [c, x_0\partial_{x_0}]$ and by Case (1), $D(x_l\partial_{x_l}) = [c, x_l\partial_{x_l}]$. Therefore by the K -linearity of D and the Lie bracket, $D(x_0\partial_{x_0} + x_l\partial_{x_l}) = [c, x_0\partial_{x_0} + x_l\partial_{x_l}]$. Letting $r = x_0\partial_{x_0} + x_l\partial_{x_l}$ and $s = x_0\partial_{x_l}$ in Lemma 5.1.15 implies $b \in C(x_0\partial_{x_0} + x_l\partial_{x_l}, \mathfrak{g})$. Thus $0 = [b, x_0\partial_{x_0} + x_l\partial_{x_l}] = [k_0\partial_{x_0}, x_0\partial_{x_0} + x_l\partial_{x_l}] = k_0\partial_{x_0}$ and so $b = 0$. Therefore $b = 0$ for all primes p and so $D(g\partial_{x_i}) = [c, g\partial_{x_i}]$ for all $i \in \{0, 1, \dots, n-1\}$ and for all $g \in G$ such that $E(g) \leq 1$.

Step (iii): This step is superfluous when $p = 2$ and so it is assumed that $p > 2$. Let $g \in G$ such that $wt(g) \leq 1$ and so $g = x_q^e$ for some $q \in \{0, 1, \dots, n-1\}$ and $e \in \{0, 1, \dots, p-1\}$. Let $b_e = D(x_q^e \partial_{x_j}) - [c, x_q^e \partial_{x_j}]$, where $j \in \{0, 1, \dots, n-1\}$. It is now shown by induction on e that $b_e = 0$, for all $e \in \{0, 1, \dots, p-1\}$.

Base case ($e = 0$): It was shown in Steps (i) and (ii) that $D(\partial_{x_j}) = [c, \partial_{x_j}]$, for all $j \in \{0, 1, \dots, n-1\}$ and so $b_0 = 0$. Let $v \in \{1, 2, \dots, p-1\}$ and assume that $b_{v-1} = 0$. Then for all $i \in \{0, 1, \dots, n-1\}$, Equation (5.7) gives

$$[\partial_{x_i}, x_q^v \partial_{x_j}] = \partial_{x_i}(x_q^v) \partial_{x_j} = \begin{cases} vx_q^{v-1} \partial_{x_j} & \text{if } i = q \\ 0 & \text{otherwise.} \end{cases}$$

Also, $D(vx_q^{v-1} \partial_{x_j}) = vD(x_q^{v-1} \partial_{x_j}) = v[c, x_q^{v-1} \partial_{x_j}] = [c, vx_q^{v-1} \partial_{x_j}]$, since both D and the Lie bracket are K -linear and $b_{v-1} = 0$ by assumption. Therefore, letting $q = \partial_{x_i}$ and $s = x_q^v \partial_{x_j}$ in Lemma 5.1.15, implies $b_v \in C(\partial_{x_i}, \mathfrak{g})$, for all $i \in \{0, 1, \dots, n-1\}$.

Thus by Lemma 5.3.4, $b_v = \sum_{i=0}^{n-1} k_i \partial_{x_i}$, for some $k_i \in K$.

If $n = 1$, then $b_v = k_0 \partial_{x_0} = k_j \partial_{x_j}$. It is now shown that $b_v = k_j \partial_{x_j}$, for $n > 1$. Assume $n > 1$. Then, $[x_l \partial_{x_m}, x_q^v \partial_{x_j}] = 0$, for any $l, m \in \{0, 1, \dots, n-1\}$ such that $l \neq j$ and $m \neq q$. Thus, letting $r = x_l \partial_{x_m}$ and $s = x_q^v \partial_{x_j}$ in Lemma 5.1.15, implies $b_v \in C(x_l \partial_{x_m}, \mathfrak{g})$, for all $l \neq j$ and $m \neq q$. Therefore by Equation (5.7)

$$0 = [b_v, x_l \partial_{x_m}] = \sum_{i=0}^{n-1} [k_i \partial_{x_i}, x_l \partial_{x_m}] = k_l \partial_{x_m}.$$

Thus $k_l = 0$ for all $l \neq j$ and so $b_v = k_j \partial_{x_j}$. Therefore we have shown that $b_v = k_j \partial_{x_j}$, for all positive integers n .

Also

$$[x_q \partial_{x_q}, x_q^v \partial_{x_j}] = v x_q^v \partial_{x_j} - x_q^v \partial_{x_j} (x_q) \partial_{x_q} = \begin{cases} (v-1) x_q^v \partial_{x_j} & \text{if } j = q \\ v x_q^v \partial_{x_j} & \text{if } j \neq q. \end{cases}$$

Letting $r = x_q \partial_{x_q}$, $s = x_q^v \partial_{x_j}$ and $k = \begin{cases} v-1 & \text{if } j = q \\ v & \text{if } j \neq q \end{cases}$ in Lemma 5.1.16 implies

$[x_q \partial_{x_q}, b_v] = k b_v$ and so if $j = q$

$$0 = (v-1) k_j \partial_{x_j} + [k_j \partial_{x_j}, x_q \partial_{x_q}] = (v-1) k_j \partial_{x_j} + k_j \partial_{x_j} (x_q) \partial_{x_q} = v k_j \partial_{x_j}$$

and if $j \neq q$

$$0 = v k_j \partial_{x_j} + [k_j \partial_{x_j}, x_q \partial_{x_q}] = v k_j \partial_{x_j} + k_j \partial_{x_j} (x_q) \partial_{x_q} = v k_j \partial_{x_j}.$$

Therefore in either case $v k_j \partial_{x_j} = 0$ and so $k_j = 0$, since $v \in \mathbb{F}_p^*$. Thus $b_v = 0$ and so by induction $b_e = 0$ for all $e \in \{0, 1, \dots, p-1\}$. Therefore it has now been shown that $D(g \partial_{x_i}) = [c, g \partial_{x_i}]$ for all $i \in \{0, 1, \dots, n-1\}$ and for all $g \in G$ such that

$wt(g) \leq 1$.

Step (iv): This step is superfluous when $n = 1$, since in this case $wt(g) \leq 1$ for all $g \in G$ and so we assume $n > 1$. Let $H = \{h \in G \mid wt(h) \geq 2\}$. It is now shown that $D(g\partial_{x_i}) = [c, g\partial_{x_i}]$ for all $i \in \{0, 1, \dots, n-1\}$ and for all $g \in H$. Let j be a fixed element of $\{0, 1, \dots, n-1\}$ and let $b_g = D(g\partial_{x_j}) - [c, g\partial_{x_j}]$, for all $g \in H$. The proof will proceed by induction on the exponent sum of the elements of H . Base case : $E(g) = 2$ and so $g = x_u x_v$ for some distinct $u, v \in \{0, 1, \dots, n-1\}$. At least one of u and v is distinct from j . Without loss of generality it is assumed that $u \neq j$. Letting $t = u$, $m = 1$ and $g' = x_v$ in Lemma 5.3.7 implies $b_g = k_u \partial_{x_u}$. There are 3 cases which are treated separately.

Case (1): $p > 2$. Then by Lemma 5.3.7, $b_g = 0$, since $m = 1 < p - 1$.

Case (2): $p = 2$ and $v \neq j$. Letting $t = v$, $m = 1$ and $g' = x_u$ in Lemma 5.3.7 implies $b_g = k_v \partial_{x_v}$. Thus $b_g = k_u \partial_{x_u} = k_v \partial_{x_v}$ and so $b_g = 0$.

Case (3): $p = 2$ and $v = j$. $[x_u \partial_{x_j}, x_u x_j \partial_{x_j}] = \partial_{x_j}$ and so letting $r = x_u \partial_{x_j}$ and $s = x_u x_j \partial_{x_j}$ in Lemma 5.1.15 implies $b_g \in C(x_u \partial_{x_j}, \mathfrak{g})$. Therefore $0 = [k_u \partial_{x_u}, x_u \partial_{x_j}] = k_u \partial_{x_j}$ and so $k_u = 0$ which implies that $b_g = 0$.

Therefore $b_g = 0$ in each case and so $D(g\partial_{x_j}) = [c, g\partial_{x_j}]$, for all $g \in H$ such that $E(g) = 2$.

Let w be an integer greater than or equal to 2. Assume that $D(h\partial_{x_j}) = [c, h\partial_{x_j}]$ for all $h \in H$ such that $E(h) \leq w$. Let $g \in H$ such that $E(g) = w + 1$. There are 3 cases which are treated separately.

Case (1): There exist $u, v \in \{0, 1, \dots, n-1\}$ distinct from j and each other such that $g \notin G_u$ and $g \notin G_v$. Therefore letting $t = u$ in Lemma 5.3.7 implies $b_g = k_u \partial_{x_u}$ and letting $t = v$ in Lemma 5.3.7 implies $b_g = k_v \partial_{x_v}$. Thus $b_g = k_u \partial_{x_u} = k_v \partial_{x_v}$ and so $b_g = 0$.

Case (2): $g = x_j^e x_u^m$ for some $e, m \in \{1, 2, \dots, p-1\}$ such that $m \neq p-1$ and $j \neq u \in \{0, 1, \dots, n-1\}$. Then letting $t = u$ in Lemma 5.3.7, gives $b_g = 0$.

Case (3): $g = x_j^e x_u^{p-1}$, for some $e \in \{1, 2, \dots, p-1\}$ and $j \neq u \in \{0, 1, \dots, n-1\}$. Then letting $t = u$ in Lemma 5.3.7, gives $b_g = k_u \partial_{x_u}$. Also $[x_u \partial_{x_j}, x_j^e x_u^{p-1} \partial_{x_j}] = e x_j^{e-1} \partial_{x_j}$ and so letting $r = x_u \partial_{x_j}$ and $s = x_j^e x_u^{p-1} \partial_{x_j}$ in Lemma 5.1.15 implies $b_g \in C(x_u \partial_{x_j}, \mathfrak{g})$. Therefore $0 = [k_u \partial_{x_u}, x_u \partial_{x_j}] = k_u \partial_{x_j}$ and so $k_u = 0$ which implies that $b_g = 0$.

Therefore, in each case $b_g = 0$ and so $D(g \partial_{x_j}) = [c, g \partial_{x_j}]$ for all $g \in H$ such that $E(g) = w + 1$. Thus by induction, $D(g \partial_{x_j}) = [c, g \partial_{x_j}]$ for all $g \in H$ and for any $j \in \{0, 1, \dots, n-1\}$. Hence $D(d) = [c, d]$ for all $d \in \mathcal{B}$.

Step (v): By Definition 5.1.4, D is a K -linear map and since \mathcal{B} is a K -vector space basis for \mathfrak{g} , D is the inner derivation induced by c .

Therefore since D was an arbitrary element of $Der(\mathfrak{g})$, all derivations of \mathfrak{g} are inner and so $\mathfrak{g} = Der(KG)$ is a complete Lie algebra. \square

5.4 The Lie Derivation Algebra of Abelian Group Algebras

In this Section, $\mathfrak{g} = Der(KG)$ is considered, firstly when G is a finite abelian p -group which is not elementary abelian and secondly when $G = X \times H$, where X is an elementary abelian p -group and H is a p -regular abelian group.

Let H be a subgroup of an abelian group G such that H is contained within the ring of constants of KG . Then it is shown that the augmentation ideal, $\Delta(G, H)$ is a differential ideal of (KG, d) , for all derivations d of KG . This result allows for the construction of a proper nonzero ideal of $Der(KG)$ from $\Delta(G, H)$, when the Sylow p -subgroup of G is not elementary abelian. If $Der(KG)$ is complete, then every element of $Der(KG)$ must map this ideal into itself. Example 5.4.3 shows that when $KG = \mathbb{F}_2(C_4 \times C_2)$, this is not the case. Therefore Theorem 5.3.8

does not extend to all finite commutative group algebras. However, it is shown in Example 5.4.4, that $Der(\mathbb{F}_2(C_4 \times C_4 \times C_2))$ is complete. Thus, the Sylow p -subgroup of G not being elementary abelian does not imply the existence of outer derivations. Theorem 5.4.14 proves that $Der(KG)$ is a complete Lie algebra, when G be a finite abelian group such that $G = X \times H$, where X is an elementary abelian p -group and H is a p -regular group.

Definition 5.4.1. Let R be a ring. Define the *ring of constants* of R to be the set of elements of R whose image under any derivation of R is zero and is denoted by $\mathcal{C}(R)$.

Lemma 5.4.2. Let K be a finite field, let G be a finite abelian group and let $c_1, c_2 \in \mathcal{C}(KG)$. Then for all $a, b \in Der(KG)$

$$[c_1a, c_2b] = c_1c_2[a, b] \quad (5.22)$$

Proof.

$$[c_1a, c_2b] = c_1a(c_2b) - c_2b(c_1a) = c_1c_2a(b) - c_2c_1b(a) = c_1c_2[a, b].$$

□

Example 5.4.3. Let K be the finite field with 2 elements and let $G = \langle x, y \mid x^4 = y^2 = x^{-1}y^{-1}xy = 1 \rangle$. By Theorem 2.3.4 the set $\{g\partial_x, h\partial_y \mid g, h \in G\}$ is a basis for $\mathfrak{g} = Der(KG)$. Let $S = \{\partial_x, x\partial_x, y\partial_x, xy\partial_x, \partial_y, x\partial_y, y\partial_y, x^2\partial_x + xy\partial_y\}$ and so $S \cup x^2S$ is another basis for \mathfrak{g} . Let $D : \mathfrak{g} \rightarrow \mathfrak{g}$ be the K -linear extension of the map defined by $s \mapsto 0$ and $x^2s \mapsto x^2s$ for all $s \in S$. It is shown that D is an element $Der(\mathfrak{g})$ that is not inner and so $Der(KG)$ is not a complete Lie algebra.

Let \mathfrak{s} be the K -span of S . It can be easily checked that \mathfrak{s} is a Lie subalgebra of \mathfrak{g} . Let $a, b \in S$ and let $[a, b] = c$ and so $c \in \mathfrak{s}$. Thus $D(a) = D(b) = D(c) = 0$. It

is now shown that D obeys Equation (5.3) (Leibniz's rule) on the products $[a, b]$, $[a, x^2b]$ and $[x^2a, x^2b]$.

$$\begin{aligned}
& [D(a), b] + [a, D(b)] + D(c) = [0, b] + [a, 0] + 0 = 0, \\
& [D(a), x^2b] + [a, D(x^2b)] + D(x^2[a, b]) \\
& = [0, x^2b] + [a, x^2b] + D(x^2c) = x^2[a, b] + x^2c = 0, \\
& [D(x^2a), x^2b] + [x^2a, D(x^2b)] + D([a, b]) = [x^2a, x^2b] + [x^2a, x^2b] + D(c) = 0.
\end{aligned} \tag{5.23}$$

Let $a, b \in \mathfrak{g}$ and so $a = a_0 + x^2a_1$ and $b = b_0 + x^2b_1$ for some $a_0, a_1, b_0, b_1 \in \mathfrak{s}$. Then $[a, b]$ is a K -linear combination of products of the form in Equation (5.4.3). Therefore by Equation (5.4.3), $D([a, b]) = [D(a), b] + [a, D(b)]$ and so $D \in \text{Der}(\mathfrak{g})$.

Let $H = \langle x^2 \rangle$ and let $I = \{u\partial_x + v\partial_y \mid u, v \in \Delta(G, H)\}$. It is shown that I is an ideal of \mathfrak{g} . $\Delta(G, H)$ is an ideal of KG and so it is closed under addition and scalar multiplication. Thus I is a subspace of \mathfrak{g} .

Let $d \in \mathfrak{g}$ and let $z \in I$ and so $z = z_0\partial_x + z_1\partial_y$, for some $z_0, z_1 \in \Delta(G, H)$. Therefore

$$[z, d] = [z_0\partial_x, d] + [z_1\partial_y, d] = z_0\partial_x(d) + d(z_0)\partial_x + z_1\partial_y(d) + d(z_1)\partial_y.$$

Note that $\partial_x(d)$ and $\partial_y(d)$ are in \mathfrak{g} and $z_0, z_1 \in \Delta(G, H)$ so $z_0\partial_x(d), z_1\partial_y(d) \in I$. Also, $H \subset \mathcal{C}(KG)$ and so by Corollary 3.1.17, $\Delta(G, H)$ is a differential ideal of (KG, d) , for all derivations d of KG . Therefore $d(z_0), d(z_1) \in \Delta(G, H)$ and so $d(z_0)\partial_x, d(z_1)\partial_y \in I$. Thus $[z, d] \in I$ and so I is an ideal of \mathfrak{g} . However, $\partial_x + x^2\partial_x \in I$ and $D(\partial_x + x^2\partial_x) = D(\partial_x) + D(x^2\partial_x) = x^2\partial_x \notin I$ and so D is not inner.

Example 5.4.4. Let K be the finite field with 2 elements and let $G = \langle x_0, x_1, x_2 \mid x_0^4 = x_1^4 = x_2^4 = x_i^{-1}x_j^{-1}x_ix_j = 1 \rangle$. Let $\mathfrak{g} = \text{Der}(KG)$. Then, by Theorem 5.2.9, \mathfrak{g} has a trivial center. It has been verified using GAP [18], that the dimension of both

$Der(\mathfrak{g})$ and \mathfrak{g} is 96. Therefore all derivations of \mathfrak{g} are inner and so \mathfrak{g} a complete Lie algebra.

Definition 5.4.5. Let K be a finite field of characteristic p and let G be a finite abelian group such that $G = X \times H$, where X is an elementary abelian p -group and H is a p -regular group. Let $\mathfrak{g} = Der(KG)$, $D \in Der(\mathfrak{g})$ and $h \in H$. Define the maps $f(D, h): \mathfrak{g} \rightarrow \mathfrak{g}$ by $a \mapsto D(ha) - hD(a)$.

Remark 5.4.6. Fix $D \in Der(\mathfrak{g})$ and $h \in H$. Denote $f(D, h)$ by f . Then for $a, b \in \mathfrak{g}$ and $k \in K$

$$\begin{aligned} f(a + b) &= D(ha + hb) - hD(a + b) = D(ha) + D(hb) - hD(a) - hD(b) \\ &= f(a) + f(b), \\ f(ka) &= D(hka) - hD(ka) = D(kha) - hkD(a) = k(D(ha) - hD(a)) = kf(a). \end{aligned}$$

Therefore the maps $f(D, h)$ are K -linear.

Lemma 5.4.7. Let K be a finite field of characteristic p and let G be a finite abelian group such that $G = X \times H$, where X is an elementary abelian p -group and H is a p -regular group. Let $\mathfrak{g} = Der(KG)$. Then $f(D, h)([a, b]) = [f(D, h)(a), b] = [a, f(D, h)(b)]$, for all $D \in Der(\mathfrak{g})$, $h \in H$ and $a, b \in \mathfrak{g}$.

Proof. Fix $D \in Der(\mathfrak{g})$ and $h \in H$. Denote $f(D, h)$ by f . Note that $H \subset \mathcal{C}(KG)$ and so by Lemma 5.4.2, $h[a, b] = [ha, b] = [a, hb]$ for all $a, b \in \mathfrak{g}$. Applying D to $h[a, b]$ gives

$$\begin{aligned} D(h[a, b]) &= D[ha, b] = [D(ha), b] + [ha, D(b)] \\ &= [hD(a), b] + [f(a), b] + h[a, D(b)] \\ &= h([D(a), b] + [a, D(b)]) + [f(a), b] \\ &= h(D[a, b]) + [f(a), b]. \end{aligned}$$

Therefore $f([a, b]) = [f(a), b]$. The bracket is antisymmetric and f is K -linear and so $f([a, b]) = f(-[b, a]) = -f([b, a]) = -[f(b), a] = [a, f(b)]$. \square

Corollary 5.4.8. *Let $a, b \in \mathfrak{g}$ such that a is in the centraliser of b in \mathfrak{g} . Then $f(D, h)(a)$ is also in the centraliser of b in \mathfrak{g} , for all $D \in \text{Der}(\mathfrak{g})$ and $h \in H$.*

Proof. Let $a \in C(b, \mathfrak{g})$, $D \in \text{Der}(\mathfrak{g})$ and $h \in H$. Then by Lemma 5.4.7, $[f(D, h)(a), b] = f(D, h)([a, b]) = f(D, h)(0) = 0$. Therefore, for all $D \in \text{Der}(\mathfrak{g})$ and $h \in H$ $a \in C(b, \mathfrak{g})$ implies $f(D, h)(a) \in C(b, \mathfrak{g})$. \square

Note that in Lemmas 5.4.9 and 5.4.10, the usual convention for an empty intersection is used, that is $S \bigcap_{k \in \emptyset} T_k = S$, for all subsets S and T_k of a set.

Lemma 5.4.9. *Let K be a finite field of characteristic p and let G be a finite abelian group such that $G = X \times H$, where X is an elementary abelian p -group with minimum generating set $\{x_i \mid i = 0, 1, \dots, n-1\}$ and H is a p -regular group. Let $\mathfrak{g} = \text{Der}(KG)$. Then*

$$\bigcap_{j=0}^{n-1} C(\partial_{x_j}, \mathfrak{g}) \bigcap_{m=1}^{n-1} C(x_m \partial_{x_m}, \mathfrak{g}) = \mathcal{C}(KG) \partial_{x_0}.$$

Proof. Let $a \in \mathfrak{g}$ and write $a = \sum_{i=0}^{n-1} \alpha_i \partial_{x_i}$, for some $\alpha_i \in KG$. Then for all $j = 0, 1, \dots, n-1$

$$[\partial_{x_j}, a] = \sum_{i=0}^{n-1} [\partial_{x_j}, \alpha_i \partial_{x_i}] = \sum_{i=0}^{n-1} \partial_{x_j}(\alpha_i) \partial_{x_i}.$$

Therefore $a \in \bigcap_{j=0}^{n-1} C(\partial_{x_j}, \mathfrak{g})$ if and only if $\partial_{x_j}(\alpha_i) = 0$, for all $i, j = 0, 1, \dots, n-1$, that is $\alpha_i \in \mathcal{C}(KG)$, for $i = 0, 1, \dots, n-1$. Thus the lemma is proved for the case $n = 1$. Assume $n > 1$ and $a \in \bigcap_{j=0}^{n-1} C(\partial_{x_j}, \mathfrak{g})$. Then for all $m = 1, 2, \dots, n-1$

$$[a, x_m \partial_{x_m}] = \sum_{i=0}^{n-1} [\alpha_i \partial_{x_i}, x_m \partial_{x_m}] = \sum_{i=0}^{n-1} \alpha_i \partial_{x_i}(x_m) \partial_{x_m} = \alpha_m \partial_{x_m}.$$

Therefore $a \in \bigcap_{j=0}^{n-1} C(\partial_{x_j}, \mathfrak{g}) \bigcap_{m=1}^{n-1} C(x_m \partial_{x_m}, \mathfrak{g})$ if and only if $\alpha_m = 0$, for all $m = 1, 2, \dots, n-1$, that is $a = \alpha_0 \partial_{x_0}$, where $\alpha_0 \in \mathcal{C}(KG)$. \square

Lemma 5.4.10. *Let K be a finite field of characteristic p and let G be a finite abelian group such that $G = X \times H$, where X is an elementary abelian p -group with minimum generating set $\{x_i \mid i = 0, 1, \dots, n-1\}$ and H is a p -regular group. Let $\mathfrak{g} = \text{Der}(KG)$. Then*

$$\bigcap_{j=1}^{n-1} C(\partial_{x_j}, \mathfrak{g}) \bigcap_{m=0}^{n-1} C(x_m \partial_{x_m}, \mathfrak{g}) = \mathcal{C}(KG) x_0 \partial_{x_0}.$$

Proof. Let $a \in \mathfrak{g}$ and write $a = \sum_{i=0}^{n-1} \alpha_i \partial_{x_i}$, where $\alpha_i \in KG$. Then for all $m = 0, 1, \dots, n-1$

$$\begin{aligned} [a, x_m \partial_{x_m}] &= \sum_{i=0}^{n-1} [\alpha_i \partial_{x_i}, x_m \partial_{x_m}] = \sum_{i=0}^{n-1} (\alpha_i \partial_{x_i}(x_m) \partial_{x_m} - x_m \partial_{x_m}(\alpha_i) \partial_{x_i}) \\ &= \alpha_m \partial_{x_m} - \sum_{i=0}^{n-1} x_m \partial_{x_m}(\alpha_i) \partial_{x_i} \\ &= (\alpha_m - x_m \partial_{x_m}(\alpha_m)) \partial_{x_m} - \sum_{i \neq m} x_m \partial_{x_m}(\alpha_i) \partial_{x_i}. \end{aligned}$$

Therefore $a \in \bigcap_{m=0}^{n-1} C(x_m \partial_{x_m}, \mathfrak{g})$ if and only if $\alpha_m = x_m \partial_{x_m}(\alpha_m)$ and $\partial_{x_m}(\alpha_i) = 0$, for all $i \neq m$, that is, $\alpha_i = \gamma_i x_i$, where $\gamma_i \in \mathcal{C}(KG)$, for $i = 0, 1, \dots, n-1$. Thus the lemma is proved for the case $n = 1$. Assume $n > 1$ and $a \in \bigcap_{m=0}^{n-1} C(x_m \partial_{x_m}, \mathfrak{g})$. Then for all $j = 1, 2, \dots, n-1$

$$[\partial_{x_j}, a] = \sum_{i=0}^{n-1} [\partial_{x_j}, \alpha_i \partial_{x_i}] = \sum_{i=0}^{n-1} \partial_{x_j}(\alpha_i) \partial_{x_i} = \sum_{i=0}^{n-1} \gamma_i \partial_{x_j}(x_i) \partial_{x_i} = \gamma_j \partial_{x_j}.$$

Therefore $a \in \bigcap_{j=1}^{n-1} C(\partial_{x_j}, \mathfrak{g}) \bigcap_{m=0}^{n-1} C(x_m \partial_{x_m}, \mathfrak{g})$ if and only if $\gamma_j = 0$, for all $j = 1, 2, \dots, n-1$, that is, $a = \gamma_0 x_0 \partial_{x_0}$, where $\gamma_0 \in \mathcal{C}(KG)$. \square

Lemma 5.4.11. *Let K be a finite field of characteristic p and let G be a finite abelian group such that $G = X \times H$, where X is an elementary abelian p -group with minimum generating set $\{x_i \mid i = 0, 1, \dots, n-1\}$ and H is a p -regular group. Let $\mathfrak{g} = \text{Der}(KG)$. Then $D(ha) = hD(a)$, for all $D \in \text{Der}(\mathfrak{g})$, $h \in H$ and $a \in \mathfrak{g}$.*

Proof. Fix $D \in \text{Der}(\mathfrak{g})$, $h \in H$ and denote $f(D, h)$ by f . It is shown that $f = 0$. Let $\rho \in \mathcal{C}(KG)$. Then by Lemma 5.4.9, $\rho\partial_{x_0} \in \mathcal{C}(KG)\partial_{x_0} = \bigcap_{j=0}^{n-1} C(\partial_{x_j}, \mathfrak{g}) \bigcap_{k=1}^{n-1} C(x_k\partial_{x_k}, \mathfrak{g})$. Therefore by Corollary 5.4.8, $f(\rho\partial_{x_0})$ is also an element of $\mathcal{C}(KG)\partial_{x_0}$ and so $f(\rho\partial_{x_0}) = \gamma_\rho\partial_{x_0}$, where $\gamma_\rho \in \mathcal{C}(KG)$. Moreover, by Lemma 5.4.10, $\rho x_0\partial_{x_0} \in \mathcal{C}(KG)x_0\partial_{x_0} = \bigcap_{j=1}^{n-1} C(\partial_{x_j}, \mathfrak{g}) \bigcap_{k=0}^{n-1} C(x_k\partial_{x_k}, \mathfrak{g})$. Therefore by Corollary 5.4.8, $f(\rho x_0\partial_{x_0}) = \tau_\rho x_0\partial_{x_0}$, where $\tau_\rho \in \mathcal{C}(KG)$. However, by Lemma 5.4.7

$$\gamma_\rho\partial_{x_0} = f(\rho\partial_{x_0}) = f([\rho\partial_{x_0}, x_0\partial_{x_0}]) = [\rho\partial_{x_0}, f(x_0\partial_{x_0})] = \rho[\partial_{x_0}, \tau_1 x_0\partial_{x_0}] = \tau_1 \rho\partial_{x_0}$$

and so $\gamma_\rho = \tau_1 \rho$ for all $\rho \in \mathcal{C}(KG)$.

The following formula is established by induction on the nonnegative integer m .

$$D(h^m\partial_{x_0}) = h^m D(\partial_{x_0}) + m\tau_1 h^{m-1}\partial_{x_0}. \quad (5.24)$$

Base case: Let $m = 0$. $D(h^0\partial_{x_0}) = h^0 D(\partial_{x_0}) + 0\tau_1 h^{-1}\partial_{x_0}$. Assume that Equation (5.24) holds for $m = k-1$. Then

$$\begin{aligned} D(h^k\partial_{x_0}) &= hD(h^{k-1}\partial_{x_0}) + f(h^{k-1}\partial_{x_0}) \\ &= h(h^{k-1}D(\partial_{x_0}) + (k-1)\tau_1 h^{k-2}\partial_{x_0}) + \gamma_{h^{k-1}}\partial_{x_0} \\ &= h^k D(\partial_{x_0}) + (k-1)\tau_1 h^{k-1}\partial_{x_0} + \tau_1 h^{k-1}\partial_{x_0} = h^k D(\partial_{x_0}) + k\tau_1 h^{k-1}\partial_{x_0}. \end{aligned}$$

Therefore Equation (5.24) holds for $m = k$ and so by induction it holds for all m . Letting m equal to the order of h , (denoted $\text{ord}(h)$) in Equation (5.24) implies $\text{ord}(h)\tau_1 h^{-1}\partial_{x_0} = 0$. Therefore $\tau_1 = 0$, since $\text{ord}(h)h^{-1}$ is a unit in KG . Thus

$f(x_0\partial_{x_0}) = \tau_1 x_0 \partial_{x_0} = 0$ and $f(\rho\partial_{x_0}) = \gamma_\rho \partial_{x_0} = \tau_1 \rho \partial_{x_0} = 0$, for all $\rho \in \mathcal{C}(KG)$. Also $\tau_\rho = 0$, for all $\rho \in \mathcal{C}(KG)$, since

$$0 = [f(\partial_{x_0}), \rho x_0 \partial_{x_0}] = [\partial_{x_0}, f(\rho x_0 \partial_{x_0})] = [\partial_{x_0}, \tau_\rho x_0 \partial_{x_0}] = \tau_\rho [\partial_{x_0}, x_0 \partial_{x_0}] = \tau_\rho \partial_{x_0}.$$

It has now been shown that $f(\rho\partial_{x_0}) = f(\rho x_0 \partial_{x_0}) = 0$, for all $\rho \in \mathcal{C}(KG)$.

Assume that $n = 1$ and $p = 2$. Then for any $g \in G$, either $g \in \mathcal{C}(KG)$ or $g \in x_0 \mathcal{C}(KG)$ and so in either case $f(g\partial_{x_0}) = 0$. Therefore $f = 0$, since it is K -linear and is zero on a basis for \mathfrak{g} .

It is now assumed that if $n = 1$ then $p > 2$. For any $j > 0$ and $m \geq 0$

$$f(x_j^m \partial_{x_j}) = f([\partial_{x_0}, x_0 x_j^m \partial_{x_j}]) = [f(\partial_{x_0}), x_0 x_j^m \partial_{x_j}] = [0, x_0 x_j^m \partial_{x_j}] = 0.$$

Let $a \in \mathfrak{g}$ and write $a = \sum_{i=0}^{n-1} \alpha_i \partial_{x_i}$, where $\alpha_i \in KG$ for all i . It is now shown that a can be written as a sum of products of elements whose image under f is zero.

Case 1 : $\alpha_i \in KG_j$ for some j . Then $[\partial_{x_j}, x_j \alpha_i \partial_{x_i}] = \alpha_i \partial_{x_i}$.

Case 2a : $\alpha_i \notin KG_j$ for any j and $n > 1$. Then for $t \neq i$, $[x_t \partial_{x_t} \alpha_i \partial_{x_i}] = k \alpha_i \partial_{x_i}$, where $k \in K^*$.

Case 2b : $\alpha_i \notin KG_j$ for any j , $n = 1$ and $p > 2$. Then $\alpha_0 = x_0^e \tilde{\alpha}_0$, where $\tilde{\alpha}_0 \in KG_0$.

If $e > 1$, then $(e-1)^{-1} [x_0 \partial_{x_0}, x_0^e \tilde{\alpha}_0 \partial_{x_0}] = (e-1)^{-1} (e x_0^e \tilde{\alpha}_0 \partial_{x_0} - x_0^e \tilde{\alpha}_0 \partial_{x_0}) = x_0^e \tilde{\alpha}_0 \partial_{x_0} = \alpha_0 \partial_{x_0}$. If $e = 1$, then $[2^{-1} \partial_{x_0}, x_0^2 \tilde{\alpha}_0 \partial_{x_0}] = 2^{-1} 2 x_0 \tilde{\alpha}_0 = \alpha_0 \partial_{x_0}$.

Therefore $a = \sum_j [b_j, c_j]$, for some $b_j, c_j \in \mathfrak{g}$ such that $f(b_j) = 0$ and so

$$f(a) = f\left(\sum_j [b_j, c_j]\right) = \sum_j f([b_j, c_j]) = \sum_j [f(b_j), c_j] = \sum_j [0, c_j] = 0.$$

□

Definition 5.4.12. Let I be an ideal of a Lie algebra \mathfrak{L} . Then I is a *characteristic ideal* of \mathfrak{L} if $d(I) \subseteq I$ for all $d \in \text{Der}(\mathfrak{L})$. This definition can be found in [37, pp.

5474]

Lemma 5.4.13. *Let K be a finite field of characteristic p and let G be a finite abelian group such that $G = X \times H$, where X is an elementary abelian p -group with minimum generating set $\{x_i \mid i = 0, 1, \dots, n-1\}$ and H is a p -regular group. Then the set*

$$I = \left\{ \sum_{i=0}^{n-1} \alpha_i \partial_{x_i} \mid \alpha_i \in \Delta(G, H), \text{ for } i = 0, 1, \dots, n-1 \right\} \quad (5.25)$$

is a characteristic ideal of $\mathfrak{g} = \text{Der}(KG)$.

Proof. By Lemma 3.1.2, the set $\{h-1 \mid h \in H\}$ is a set of generators of $\Delta(G, H)$ as an ideal of KG . Let $b \in I$. Then $b = \sum_{i=0}^{n-1} \sum_{h \in H} (h-1) \beta_{i,h} \partial_{x_i}$, where $\beta_{i,h} \in KG$. Let $D \in \text{Der}(\mathfrak{g})$. Then by Lemma 5.4.11, $D(ha) = hD(a)$ for all $a \in \mathfrak{g}$. Therefore

$$D(b) = \sum_{i=0}^{n-1} \sum_{h \in H} D((h-1) \beta_{i,h} \partial_{x_i}) = \sum_{i=0}^{n-1} \sum_{h \in H} (h-1) D(\beta_{i,h} \partial_{x_i}) \in I.$$

□

Theorem 5.4.14. *Let K be a finite field of characteristic p and let G be a finite abelian group such that $G = X \times H$, where X is an elementary abelian p -group and H is a p -regular group. Then $\text{Der}(KG)$ is a complete Lie algebra.*

Proof. Let $\mathfrak{g} = \text{Der}(KG)$. By Lemma 5.2.9, \mathfrak{g} has trivial center and so it remains to show that all derivations of \mathfrak{g} are inner.

Let $\Phi: KG \rightarrow KG$ be the K -linear extension of the group homomorphism defined by $x \mapsto x$ and $h \mapsto 1$, for all $x \in X$ and $h \in H$. Therefore, $\ker(\Phi)$ is the augmentation ideal $\Delta(G, H)$. Let $\{x_i \mid i = 0, 1, \dots, n-1\}$ be a minimum generating set for X and let $a = \sum_{i=0}^{n-1} \alpha_i \partial_{x_i} \in \mathfrak{g}$. Define $\phi: \mathfrak{g} \rightarrow \mathfrak{g}$ by $a \mapsto \sum_{i=0}^{n-1} \Phi(\alpha_i) \partial_{x_i}$. ϕ is a Lie algebra homomorphism since, $\phi(a) = 0$, if and only if, $\Phi(\alpha_i) = 0$, for all

$i = 0, 1, \dots, n-1$ and so $\ker(\phi) = I$, where I is the characteristic ideal of \mathfrak{g} defined by Equation (5.25).

Fix $D \in \text{Der}(\mathfrak{g})$. Let $\mathfrak{h} = \mathfrak{g}/I$ and define $d: \mathfrak{h} \rightarrow \mathfrak{h}$ by $d(\phi(a)) = \phi(D(a))$, for all $a \in \mathfrak{g}$. Let $a, b \in \mathfrak{g}$ such that $\phi(a) = \phi(b)$, then $D(a-b) \in \ker(\phi)$, since $a-b \in \ker(\phi) = I$, which is a characteristic ideal of \mathfrak{g} . Therefore $d(\phi(a)) - d(\phi(b)) = d(\phi(a-b)) = \phi(D(a-b)) = 0$ and so the map d is well defined. Moreover, d is a linear map as it is the composition of the linear maps ϕ and D . Also, d satisfies the Leibniz rule, since for any $a, b \in \mathfrak{g}$

$$\begin{aligned} d([\phi(a), \phi(b)]) &= d(\phi[a, b]) = \phi(D[a, b]) = \phi([D(a), b] + [a, D(b)]) \\ &= [\phi(D(a)), \phi(b)] + [\phi(a), \phi(D(b))] \\ &= [d(\phi(a)), \phi(b)] + [\phi(a), d(\phi(b))]. \end{aligned}$$

Therefore $d \in \text{Der}(\mathfrak{h})$. By Theorem 5.3.8, \mathfrak{h} is complete and so d is inner, induced by some element $\phi(c) \in \mathfrak{h}$. It has been shown that the following diagram commutes:

$$\begin{array}{ccc} \mathfrak{g} & \xrightarrow{D} & \mathfrak{g} \\ \phi \downarrow & & \downarrow \phi \\ \mathfrak{h} & \xrightarrow{d} & \mathfrak{h} \end{array}$$

$\phi(D(a)) = d(\phi(a)) = [\phi(c), \phi(a)] = \phi([c, a])$ and so $D(a) - [c, a] \in \ker(\phi)$. Let $\delta = D - ad(c)$ and so $\delta: \mathfrak{g} \rightarrow I$ is an element of $\text{Der}(\mathfrak{g})$. Consider the restriction of δ to \mathfrak{h} , denoted by $\delta \upharpoonright_{\mathfrak{h}}$. Let $r, s \in \mathfrak{h}$, $k \in K$ and $H_1 = H \setminus \{1\}$. Then

$$\begin{aligned} \delta \upharpoonright_{\mathfrak{h}}(r) &= \sum_{h \in H_1} (h-1)r_h, & \delta \upharpoonright_{\mathfrak{h}}(kr) &= \sum_{h \in H_1} (h-1)kr_h, \\ \delta \upharpoonright_{\mathfrak{h}}(s) &= \sum_{h \in H_1} (h-1)s_h, & \delta \upharpoonright_{\mathfrak{h}}(r+s) &= \sum_{h \in H_1} (h-1)(r_h + s_h), \end{aligned} \tag{5.26}$$

for some $r_h, s_h \in \mathfrak{h}$. Define the maps $\delta_h: \mathfrak{h} \rightarrow \mathfrak{h}$ by $r \mapsto r_h$, for all $h \in H_1$. Then by

Equation (5.26), δ_h is K -linear. Also by Equation (5.26)

$$\begin{aligned}
\sum_{h \in H_1} (h-1)\delta_h([r, s]) &= \delta \upharpoonright_{\mathfrak{h}}([r, s]) = [\delta \upharpoonright_{\mathfrak{h}}(r), s] + [r, \delta \upharpoonright_{\mathfrak{h}}(s)] \\
&= \sum_{h \in H_1} (h-1)[r_h, s] + \sum_{h \in H} (h-1)[r, s_h] \\
&= \sum_{h \in H_1} (h-1)([r_h, s] + [r, s_h]) \\
&= \sum_{h \in H_1} (h-1)([\delta_h(r), s] + [r, \delta_h(s)]).
\end{aligned}$$

Therefore for all $h \in H_1$, δ_h satisfies liebniz's rule and so is an element of $Der(\mathfrak{h})$.

Thus δ_h is inner induced by some element of \mathfrak{h} , denoted by t_h . Thus

$$\delta \upharpoonright_{\mathfrak{h}}(r) = \sum_{h \in H_1} (h-1)r_h = \sum_{h \in H_1} (h-1)\delta_h(r) = \sum_{h \in H_1} (h-1)[t_h, r] = \left[\sum_{h \in H_1} (h-1)t_h, r \right].$$

Denote $\sum_{h \in H_1} (h-1)t_h$ by t . Then, by Lemma 5.4.11, for any $h \in H$ and any $r \in \mathfrak{h}$

$$\delta(hr) = h\delta(r) = h[t, r] = [t, hr],$$

and so δ is inner induced by t . Therefore $D(a) = [c, a] + \delta(a) = [c, a] + [t, a] = [c + t, a]$ and hence D is inner induced by $c + t$. \square

5.5 Derivations of Abelian p-Groups

Lemma 5.5.1. *Der($\mathbb{F}_{p^t}C_{p^n}$) is a perfect Lie algebra for all prime numbers $p > 2$.*

Proof. Let $\mathfrak{g} = Der(\mathbb{F}_{p^t}C_{p^n})$, let $C_{p^n} = \langle x \rangle$ and let $\mathcal{B} = \{x^i \partial_x \mid i = 0, 1, \dots, p^n - 1\}$.

Then by Theorem 2.3.4, \mathcal{B} is a basis for \mathfrak{g} . It is shown that each element of \mathcal{B} is a product in \mathfrak{g} . There are 2 cases which are treated separately.

Case 1: $x^i \partial_x$, where $i \not\equiv -1 \pmod{p}$. Then

$$[(i+1)^{-1} \partial_x, x^{i+1} \partial_x] = (i+1)^{-1} \partial_x (x^{i+1}) \partial_x - 0 = (i+1)^{-1} (i+1) x^i \partial_x = x^i \partial_x.$$

Case 2: $x^i \partial_x$, where $i \equiv -1 \pmod{p}$. Then $i-1$ is invertible since $p > 2$ and so

$$\begin{aligned} [(i-1)^{-1} x \partial_x, x^i \partial_x] &= (i-1)^{-1} (x \partial_x (x^i) \partial_x - x^i \partial_x (x) \partial_x) \\ &= (i-1)^{-1} (i x x^{i-1} \partial_x - x^i \partial_x) = (i-1)^{-1} (i-1) x^i \partial_x = x^i \partial_x. \end{aligned}$$

Therefore all elements of \mathcal{B} are in \mathfrak{g}' and so $\mathfrak{g}' = \mathfrak{g}$. □

Definition 5.5.2. A set S of elements of a Lie algebra \mathfrak{L} , *generate* \mathfrak{L} if the smallest subalgebra of \mathfrak{L} containing the set S is \mathfrak{L} .

Lemma 5.5.3. *Let \mathfrak{g} be a Lie algebra and let $a, b, c, d \in \mathfrak{g}$, such that $[a, b] = d$. Further, let $D \in \text{Der}(\mathfrak{g})$ such that $D(a) = [c, a]$ and $D(b) = [c, b]$. Then $D(d) = [c, d]$.*

Proof. This is a direct consequence of the Jacobi identity. Applying D to $d = [a, b]$ gives

$$D(d) = [D(a), b] + [a, D(b)] = [[c, a], b] + [a, [c, b]] = [c, [a, b]] = [c, d].$$

□

Lemma 5.5.4. *Let S be a generating set for a Lie algebra \mathfrak{g} . Further, let $D \in \text{Der}(\mathfrak{g})$ such that $D(s) = [c, s]$, for all $s \in S$. Then D is the inner derivation of \mathfrak{g} , induced by c .*

Proof. Let $T = \{t \in \mathfrak{g} \mid D(t) = [c, t]\}$ and let $a = [t_0, t_1]$, where $t_0, t_1 \in T$. Then by Lemma 5.5.3, $a \in T$. Therefore $T = \mathfrak{g}$, since $S \subseteq T$ and S generates \mathfrak{g} . □

Lemma 5.5.5. *Der*($\mathbb{F}_{p^t}C_{p^n}$) is a complete Lie algebra for all prime numbers $p > 3$.

Proof. Let $C_{p^n} = \langle x \rangle$ and let $\mathfrak{g} = \text{Der}(\mathbb{F}_{p^t}C_{p^n})$. Then $\mathcal{B} = \{x^i\partial_x \mid i = 0, 1, \dots, p^n - 1\}$ is a basis for \mathfrak{g} . By Theorem 5.2.9, \mathfrak{g} has trivial center and so it remains to show that all derivations of \mathfrak{g} are inner. Multiplication of elements of \mathcal{B} is given by the following equation.

$$[x^i\partial_x, x^j\partial_x] = x^i j x^{j-1} \partial_x - x^j i x^{i-1} \partial_x = (j - i)x^{i+j-1} \partial_x. \quad (5.27)$$

Therefore $x^m\partial_x$ is not in the support of any element of the range of $x^i\partial_x$ if and only if $m \equiv 2i - 1 \pmod{p}$. Let $D \in \text{Der}(\mathfrak{g})$ and write $D(\partial_x) = \sum_{i=0}^{p^n-1} k_i x^i \partial_x$, where $k_i \in \mathbb{F}_p$. Then

$$[D(\partial_x), x\partial_x] = \sum_{i=0}^{p^n-1} k_i [x^i\partial_x, x\partial_x] = \sum_{i=0}^{p^n-1} k_i (1 - i)x^i \partial_x.$$

Applying D to the equation $\partial_x = [\partial_x, x\partial_x]$, gives $D(\partial_x) = [D(\partial_x), x\partial_x] + [\partial_x, D(x\partial_x)]$. Equating the coefficients of $x^m\partial_x$, where $m \equiv -1 \pmod{p}$ implies $k_m = k_m(1 - (-1)) + 0$, since $x^m\partial_x$ is not in the support of any element of the range of ∂_x and so $k_m = 0$. Therefore $D(\partial_x) \in R(\partial_x)$ and so $D(\partial_x) = [c, \partial_x]$, for some $c \in \mathfrak{g}$.

Let $\beta_i\partial_x = D(x^i\partial_x) - [c, x^i\partial_x]$, for all $i \in \{0, 1, \dots, p^n - 1\}$ and so $\beta_0 = 0$.

Applying D to Equation (5.27) implies

$$\begin{aligned} 0 &= (i - j)D(x^{i+j-1}\partial_x) + [D(x^i\partial_x), x^j\partial_x] + [x^i\partial_x, D(x^j\partial_x)] \\ &= (i - j)[c, x^{i+j-1}\partial_x] + (i - j)\beta_{i+j-1}\partial_x + [[c, x^i\partial_x], x^j\partial_x] \\ &\quad + [\beta_i\partial_x, x^j\partial_x] + [x^i\partial_x, [c, x^j\partial_x]] + [x^i\partial_x, \beta_j\partial_x] \\ &= (i - j)[c, x^{i+j-1}\partial_x] + (i - j)\beta_{i+j-1}\partial_x + [x^i\partial_x, [x^j\partial_x, c]] + [c, [x^i\partial_x, x^j\partial_x]] \\ &\quad + [\beta_i\partial_x, x^j\partial_x] - [x^i\partial_x, [x^j\partial_x, c]] + [x^i\partial_x, \beta_j\partial_x]. \end{aligned}$$

Therefore

$$(i - j)\beta_{i+j-1}\partial_x + [\beta_i\partial_x, x^j\partial_x] + [x^i\partial_x, \beta_j\partial_x] = 0. \quad (5.28)$$

By Equation (5.27), $[a, \zeta b] = [\zeta a, b] = \zeta[a, b]$, for any $\zeta \in \mathbb{F}_{p^t}\langle x^p \rangle$.

Letting $j = 1$ and $i = 0$ in Equation (5.28), implies $0\partial_x = \beta_0\partial_x = [\partial_x, \beta_1\partial_x]$ and so $\beta_1 \in \mathbb{F}_{p^t}\langle x^p \rangle$.

Letting $j = 2$ and $i = 0$ in Equation (5.28), implies $2\beta_1\partial_x = [\partial_x, \beta_2\partial_x]$ and hence $\beta_2 = 2x\beta_1 + \bar{\beta}_2$, where $\bar{\beta}_2 \in \mathbb{F}_{p^t}\langle x^p \rangle$.

Letting $j = 2$ and $i = 1$ in Equation (5.28), implies

$$\begin{aligned} 0 &= -\beta_2\partial_x + [\beta_1\partial_x, x^2\partial_x] + [x\partial_x, \beta_2\partial_x] \\ &= -2x\beta_1\partial_x - \bar{\beta}_2\partial_x + \beta_1[\partial_x, x^2\partial_x] + [x\partial_x, 2x\beta_1\partial_x] + [x\partial_x, \bar{\beta}_2\partial_x] \\ &= -2x\beta_1\partial_x - \bar{\beta}_2\partial_x + \beta_1 2x\partial_x + 2\beta_1[x\partial_x, x\partial_x] + \bar{\beta}_2[x\partial_x, \partial_x] = -2\bar{\beta}_2\partial_x. \end{aligned}$$

Therefore $\bar{\beta}_2 = 0$ and so $\beta_2 = 2x\beta_1$.

Letting $j = 3$ and $i = 0$ in Equation (5.28), implies $3\beta_2\partial_x = [\partial_x, \beta_3\partial_x]$ and hence $\beta_3 = 3x\beta_2 + \bar{\beta}_3$, where $\bar{\beta}_3 \in \mathbb{F}_{p^t}\langle x^p \rangle$. Thus $\beta_3 = 6x^2\beta_1 + \bar{\beta}_3$.

Letting $j = 3$ and $i = 1$ in Equation (5.28), implies

$$\begin{aligned} 0 &= -2\beta_3\partial_x + [\beta_1\partial_x, x^3\partial_x] + [x\partial_x, \beta_3\partial_x] \\ &= -12x^2\beta_1\partial_x - 2\bar{\beta}_3\partial_x + \beta_1[\partial_x, x^3\partial_x] + \beta_1[x\partial_x, 6x^2\partial_x] + \bar{\beta}_3[x\partial_x, \partial_x] \\ &= -12x^2\beta_1\partial_x - 2\bar{\beta}_3\partial_x + \beta_1 3x^2\partial_x + \beta_1 6x^2\partial_x - \bar{\beta}_3\partial_x = -3x^2\beta_1\partial_x - 3\bar{\beta}_3\partial_x. \end{aligned}$$

Therefore $\beta_1 = \bar{\beta}_3 = 0$ and so $0 = \beta_0 = \beta_1 = \beta_2 = \beta_3$.

$x^2\partial_x$ and $x^3\partial_x$ generate the Lie algebra \mathfrak{g} , since for any $m \not\equiv 2 \pmod{p}$ by Equation (5.27), $[x^2\partial_x, x^m\partial_x] = (m - 2)x^{m+1}\partial_x$ and for any $m \equiv 2 \pmod{p}$, $[x^3\partial_x, x^{m-1}\partial_x] = -2x^{m+1}\partial_x$. Therefore by Corollary 5.5.4, D is an inner derivation

of \mathfrak{g} . Thus, since D is a arbitrary derivation, \mathfrak{g} is a complete Lie algebra. \square

Lemma 5.5.6. *Let p be an odd prime and let $G = \langle x_0, x_1 \mid x_0^{p^2} = x_1^p = x_0^{-1}x_1^{-1}x_0x_1 = 1 \rangle \simeq C_{p^2} \times C_p$. Then the set $\{\partial_{x_0}, x_0\partial_{x_1}, x_0^{p^2-1}x_1^{p-1}\partial_{x_0}\}$ generates $Der(\mathbb{F}_{p^t}G)$ as a Lie algebra.*

Proof. Let $\mathfrak{g} = Der(\mathbb{F}_{p^t}G)$ and let $\mathcal{B} = \{g\partial_{x_i} \mid g \in G, i = 0, 1\}$. Then by Theorem 2.3.4, \mathcal{B} is a basis for \mathfrak{g} . Let \mathfrak{s} be the subalgebra of \mathfrak{g} generated by the set $\{\partial_{x_0}, x_0\partial_{x_1}, x_0^{p^2-1}x_1^{p-1}\partial_{x_0}\}$. Then $\partial_{x_1} \in \mathfrak{s}$ since, $[\partial_{x_0}, x_0\partial_{x_1}] = \partial_{x_1}$. Let i be an integer such that $x_0^i x_1^{p-1} \partial_{x_0} \in \mathfrak{s}$. Then $x_0^i x_1^j \partial_{x_0} \in \mathfrak{s}$, for all $j = 0, 1, \dots, p-1$, since $[\partial_{x_1}, x_0^i x_1^j \partial_{x_0}] = j x_0^i x_1^{j-1} \partial_{x_0}$. Thus in particular $x_0^{p^2-1} \partial_{x_0} \in \mathfrak{s}$.

It is now shown that $x_0^i x_1^j \partial_{x_0} \in \mathfrak{s}$, for all $i = 0, 1, \dots, p^2-1$ and $j = 0, 1, \dots, p-1$. Let $i \not\equiv -1 \pmod{p}$. Then, $[(i+1)^{-1} \partial_{x_0}, x_0^{i+1} x_1^{p-1} \partial_{x_0}] = x_0^i x_1^{p-1} \partial_{x_0}$. Now let $i \equiv -1 \pmod{p}$. Then, $[x_0^{p^2-1} \partial_{x_0}, x_0^{i+2} x_1^{p-1} \partial_{x_0}] = 2x_0^i x_1^{p-1} \partial_{x_0}$. Therefore $x_0^i x_1^{p-1} \partial_{x_0} \in \mathfrak{s}$, for all $i = 0, 1, \dots, p^2-1$ since, $p > 2$ and $x_0^{p^2-1} x_1^{p-1} \partial_{x_0} \in \mathfrak{s}$. However, it has already been shown that for $j = 0, 1, \dots, p-1$, $x_0^i x_1^j \partial_{x_0} \in \mathfrak{s}$, whenever $x_0^i x_1^{p-1} \partial_{x_0} \in \mathfrak{s}$. Therefore $x_0^i x_1^j \partial_{x_0} \in \mathfrak{s}$, for all $i = 0, 1, \dots, p^2-1$ and $j = 0, 1, \dots, p-1$.

Also, for any i and j , $[x_0^i x_1^j \partial_{x_0}, x_0 \partial_{x_1}] = x_0^i x_1^j \partial_{x_1} - j x_0^{i+1} x_1^{j-1} \partial_{x_0}$ and so $x_0^i x_1^j \partial_{x_1} \in \mathfrak{s}$ since $j x_0^{i+1} x_1^{j-1} \partial_{x_0} \in \mathfrak{s}$. Therefore $\mathcal{B} \subseteq \mathfrak{s}$ and so $\mathfrak{s} = \mathfrak{g}$. \square

Lemma 5.5.7. *Let p be a prime number, let $G = \langle x_0, x_1 \mid x_0^{p^2} = x_1^p = x_0^{-1}x_1^{-1}x_0x_1 = 1 \rangle \simeq C_{p^2} \times C_p$ and let $\mathfrak{g} = Der(\mathbb{F}_{p^t}G)$. Then $D(\partial_{x_0}) \in R(\partial_{x_0})$, for all $D \in Der(\mathfrak{g})$.*

Proof. $[\partial_{x_0}, x_0^i x_1^j \partial_{x_k}] = i x_0^{i-1} x_1^j \partial_{x_k}$ and so $R(\partial_{x_0}) = \{x_0^i x_1^j \partial_{x_k} \mid i \not\equiv -1\}$. Let $D \in Der(\mathfrak{g})$ and write $D(\partial_{x_0}) = \sum_{i,j,k} a_{i,j,k} x_0^i x_1^j \partial_{x_k}$. Applying D to $[\partial_{x_0}, x_0 \partial_{x_0}] = \partial_{x_0}$

implies

$$\begin{aligned}
0 &= D(\partial_{x_0}) + [x_0 \partial_{x_0}, D(\partial_{x_0})] + [x_0 \partial_{x_0}, D(\partial_{x_0})] \\
&= \sum_{i,j,k} a_{i,j,k} x_0^i x_1^j \partial_{x_k} + \sum_{i,j,k} a_{i,j,k} [x_0 \partial_{x_0}, x_0^i x_1^j \partial_{x_k}] + [x_0 \partial_{x_0}, D(\partial_{x_0})] \\
&= \sum_{i,j,k} a_{i,j,k} (1 + i - \delta_{0,k}) x_0^i x_1^j \partial_{x_k} + [x_0 \partial_{x_0}, D(\partial_{x_0})],
\end{aligned}$$

where δ is the Kronecker delta function. Therefore $\sum_{i,j,k} a_{i,j,k} (1 + i - \delta_{0,k}) x_0^i x_1^j \partial_{x_k} \in R(\partial_{x_0})$ and so for $i \equiv -1 \pmod{p}$, $0 = a_{i,j,k} (1 + i - \delta_{0,k}) = a_{i,j,k} (\delta_{0,k})$. Thus $a_{i,j,0} = 0$, for all j and $i \equiv -1 \pmod{p}$. Therefore $D(\partial_{x_0}) = \sum_{i \neq -1, j, k} a_{i,j,k} x_0^i x_1^j \partial_{x_k} + \sum_{i \equiv -1, j} a_{i,j,1} x_0^i x_1^j \partial_{x_1}$.

Let $m \in \{0, 1, \dots, p-1\}$. Then applying D to $[\partial_{x_0}, x_1^m \partial_{x_1}] = 0$ implies $[D(\partial_{x_0}), x_1^m \partial_{x_1}] + [\partial_{x_0}, D(x_1^m \partial_{x_1})] = 0$ and so $[D(\partial_{x_0}), x_1^m \partial_{x_1}] \in R(\partial_{x_0})$. Therefore

$$\sum_{i \neq -1, j, k} a_{i,j,k} [x_0^i x_1^j \partial_{x_k}, x_1^m \partial_{x_1}] + \sum_{i \equiv -1, j} a_{i,j,1} [x_0^i x_1^j \partial_{x_1}, x_1^m \partial_{x_1}] \in R(\partial_{x_0}).$$

Note that $\sum_{i \neq -1, j, k} a_{i,j,k} [x_0^i x_1^j \partial_{x_k}, x_1^m \partial_{x_1}] \in R(\partial_{x_0})$ since the exponent of x_0 in each summand is not congruent to -1 modulo p and so

$$\sum_{i \equiv -1, j} a_{i,j,1} [x_0^i x_1^j \partial_{x_1}, x_1^m \partial_{x_1}] = \sum_{i \equiv -1, j} a_{i,j,1} (m - j) x_0^i x_1^{m+j-1} \partial_{x_1} \in R(\partial_{x_0}).$$

Therefore $a_{i,j,1} (m - j) = 0$, for all $j, m \in \{0, 1, \dots, p-1\}$ and so $a_{i,j,1} = 0$, for all $j \neq m$. Letting $m = 0$ and then letting $m = 1$ implies $a_{i,j,1} = 0$, for all $i \equiv -1 \pmod{p}$. Thus $D(\partial_{x_0}) = \sum_{i \neq -1, j, k} a_{i,j,k} x_0^i x_1^j \partial_{x_k} \in R(\partial_{x_0})$. \square

Lemma 5.5.8. *Let p be a prime number and let K be a finite field of characteristic p . Let G be a finite abelian group, let X be the Sylow p -subgroup of G and let $Y < G$ such that $G = X \times Y$. Let $S = \{x_i \mid i = 0, 1, \dots, n-1\}$ be a minimum generating set for X and let $H = \langle x_0^p \rangle \times \langle x_1^p \rangle \times \dots \times \langle x_{n-1}^p \rangle \times Y$. Then KH is the ring of*

constants of KG .

Proof. Let $i, j \in \{0, 1, \dots, n-1\}$. Then $\partial_{x_i}(x_j^p) = 0$ and by Corollary 2.3.2 $\partial_{x_i}(y) = 0$, for all $y \in Y$. Therefore $d(h) = 0$, for all $d \in \text{Der}(KG)$ and $h \in H$ and so $KH \subseteq \mathcal{C}(KG)$.

Let $L = \left\{ \prod_{i=0}^{n-1} x_i^{r_i} \mid r_i \in \{0, 1, \dots, p-1\} \right\}$. Then L is a transversal of H in G . Let $\alpha \in \mathcal{C}(KG)$ and write $\alpha = \sum_{l \in L} a_l l$, where $a_l \in KH$. Then, by Definition 5.2.6

$$0 = \partial_{x_i}(\alpha) = \sum_{l \in L} a_l \partial_{x_i}(l) = \sum_{l \neq 1} a_l R_i(l) x_i^{-1} l = \sum_{l \neq 1} a_l R_i(l) l,$$

for all $i \in \{0, 1, \dots, n-1\}$. Let $1 \neq l \in L$. Then $R_i(l) \neq 0$, for some i and so $a_l = 0$, for all $l \neq 1$. Thus $\alpha = a_1 \in KH$. Therefore $\mathcal{C}(KG) \subseteq KH$ and so $\mathcal{C}(KG) = KH$. \square

Chapter 6

Derivations and the Modular Isomorphism Problem

This chapter begins by examining the derivation algebras of $\mathbb{F}_{2^t}D_{2^{m+1}}$ and $\mathbb{F}_{2^t}Q_{2^{m+1}}$. A basis for the derivation algebra of $\mathbb{F}_{2^t}Q_{2^{m+1}}$ is found and its dimension is shown to be $2^{m+1} + 2$. In Section 6.1.2 the centers of the derivation algebras are computed. $Der(\mathbb{F}_{2^t}D_{2^{m+1}})$ is shown to have trivial center, whereas the dimension of the center of $Der(\mathbb{F}_{2^t}Q_{2^{m+1}})$ is 2. These results are used in Section 6.1.3 to show that $\mathbb{F}_{2^t}D_{2^{m+1}}$ and $\mathbb{F}_{2^t}Q_{2^{m+1}}$ are not isomorphic as rings.

The ring of constants of a group algebra is a subring of the group algebra and is studied in Section 6.2. A ring homomorphism preserves subrings and so the restriction of a ring homomorphism to the ring of constants is a ring homomorphism. Groups of constants are also considered and are used to show once again that $\mathbb{F}_2(C_4 \times C_4)$ and $\mathbb{F}_2(C_2 \times C_8)$ are not isomorphic as rings. The ring of constants of an abelian p -group algebra over \mathbb{F}_p is shown to be the image of the group algebra under the Frobenius endomorphism. The Modular Isomorphism Problem is an important open problem in the area of group rings. It was solved for abelian groups in 1956 by Deskins [14]. The chapter concludes by giving an alternative

proof of Deskins' Theorem using derivations.

6.1 Derivations of $\mathbb{F}_{2^t}D_{2^{m+1}}$ and $\mathbb{F}_{2^t}Q_{2^{m+1}}$

Let n be an integer greater than 2 and let D_{2n} denote the dihedral group with $2n$ elements and presentation $\langle x, y \mid x^n = y^2 = (xy)^2 = 1 \rangle$.

Let m be a positive integer greater than 1 and let $Q_{2^{m+1}}$ denote the generalised quaternion group with 2^{m+1} elements and presentation $\langle a, b \mid b^2 = a^{2^{m-1}}, abab^{-1} = 1 \rangle$.

Remark 6.1.1. A presentation of the generalised quaternion group $Q_{2^{m+1}}$ often includes the relator a^{2^m} which is now shown to be redundant.

$$\begin{aligned} b(b^2)b^{-1} &= b^2 & (b^2 &= a^{2^{m-1}}) \\ b(a^{2^{m-1}})b^{-1} &= a^{2^{m-1}} & (ba &= a^{-1}b) \\ a^{-(2^{m-1})}bb^{-1} &= a^{2^{m-1}} \\ a^{-(2^{m-1})} &= a^{2^{m-1}} \end{aligned}$$

Therefore $b^4 = a^{2^m} = 1$.

Let m be an integer greater than 1 and let \mathbb{F}_{2^t} be a finite field with 2^t elements. Assuming that $\mathbb{F}_{2^t}D_{2^{m+1}}$ and $\mathbb{F}_{2^t}Q_{2^{m+1}}$ are isomorphic as rings, then Theorem 3.1.18 states that $Der(\mathbb{F}_{2^t}D_{2^{m+1}})$ and $Der(\mathbb{F}_{2^t}Q_{2^{m+1}})$ are isomorphic as additive groups. In this Section it is shown that no such isomorphism exists and so the group rings $\mathbb{F}_{2^t}D_{2^{m+1}}$ and $\mathbb{F}_{2^t}Q_{2^{m+1}}$ are not isomorphic as rings. This is a known result which can also be found in [4] and [8].

Using $n = 2^m$ in Theorem 2.3.11 implies that the dimension of the vector space of derivations of $\mathbb{F}_{2^t}D_{2^{m+1}}$ is $2n + 4 = 2^{m+1} + 4$.

6.1.1 The Derivation Algebra of $\mathbb{F}_{2^t}Q_{2^{m+1}}$

Theorem 6.1.3 refers to the maps f^* and the classical involution of a group algebra. The definitions of these maps are now recalled.

Definition 6.1.2. Let $G = \langle S \mid T \rangle$ be a group, where S is a generating set and T is a set of defining relations for G . Let F_S be the free group on S . Let R be a commutative unital ring and f a map from S to RG . Define $f^*: F_S \rightarrow RG$ as follows:

$$f^*(w_i) = \begin{cases} f(w_i) & \text{if } w_i \in S, \\ -w_i f(w_i^{-1}) w_i & \text{if } w_i \in S^{-1}, \\ 0 & \text{if } w_i = 1 \end{cases} \quad (6.1)$$

and letting $w = \prod_{i=1}^k w_i$, where $w_i \in S \cup S^{-1}$, define

$$f^*(w) = \sum_{i=1}^k \left(\left(\prod_{j=1}^{i-1} w_j \right) f^*(w_i) \left(\prod_{j=i+1}^k w_j \right) \right). \quad (6.2)$$

Definition 3.2.34 is repeated here for ease of access.

Definition 3.2.34. The *classical involution* of KG , denoted by \circledast is a map from KG to KG defined by $(\sum_{g \in G} a_g g)^{\circledast} \mapsto \sum_{g \in G} a_g g^{-1}$.

Let $\mathfrak{g} = \text{Der}(\mathbb{F}_{2^t}Q_{2^{m+1}})$, let $d \in \mathfrak{g}$ and let $d(a) = r + sb$, where $r, s \in \mathbb{F}_{2^t}\langle a \rangle$. Then for $j \in \{1, 2, \dots, 2^{m-1} - 1\}$

$$\begin{aligned} d(a^{2^j}) &= \sum_{i=0}^{2^j-1} a^i d(a) a^{2^j-i-1} = \sum_{i=0}^{2^j-1} a^i (r + sb) a^{2^j-i-1} \\ &= \sum_{i=0}^{2^j-1} a^{2^j-1-i} r + \sum_{i=0}^{2^j-1} a^{2^j-2i} sb = 2^j a^{2^j-1} r + a^{1-2^j} \sum_{i=0}^{2^j-1} a^{2i} sb \\ &= a^{1-2^j} \sum_{i=0}^{2^j-1} a^{2i} sb. \end{aligned} \quad (6.3)$$

Theorem 6.1.3. *The dimension of the vector space of derivations of $\mathbb{F}_{2^t}Q_{2^{m+1}}$ is $2^{m+1} + 2$.*

Proof. The relators chosen for $Q_{2^{m+1}}$ are $a^{2^{m-1}}b^2$ and $abab^{-1}$. Therefore by Theorem 2.2.5, $f: \{a, b\} \rightarrow \mathbb{F}_{2^t}Q_{2^{m+1}}$ can be extended to a derivation of $\mathbb{F}_{2^t}Q_{2^{m+1}}$ if and only if

$$f^*(a^{2^{m-1}}b^2) = 0 \text{ and} \quad (6.4)$$

$$f^*(abab^{-1}) = 0. \quad (6.5)$$

Assume that f can be extended to a derivation of $\mathbb{F}_{2^t}Q_{2^{m+1}}$ and write $f(a) = r + sb$ and $f(b) = u + vb$, where $r, s, u, v \in \mathbb{F}_{2^t}\langle a \rangle$. Write $r = \sum_{i=0}^{2^m-1} r_i a^i$, $s = \sum_{i=0}^{2^m-1} s_i a^i$, $u = \sum_{i=0}^{2^m-1} u_i a^i$ and $v = \sum_{i=0}^{2^m-1} v_i a^i$, where $r_i, s_i, u_i, v_i \in \mathbb{F}_{2^t}$. By Equations (6.2) and (6.4) and since $b^2 = a^{2^{m-1}}$ is a central unit in $\mathbb{F}_{2^t}Q_{2^{m+1}}$,

$$0 = f^*(a^{2^{m-1}}b^2) = f^*(a^{2^{m-1}})b^2 + a^{2^{m-1}}f^*(b^2) = f^*(a^{2^{m-1}}) + f^*(b^2).$$

Therefore by Definition 6.1.2, Equation (6.3) and denoting $\sum_{i=0}^{2^{m-1}-1} a^{2i}$ by $\widehat{a^2}$

$$\begin{aligned} 0 &= f^*(a^{2^{m-1}}) + f(b)b + bf(b) \\ &= a^{2^{m-1}+1} \sum_{i=0}^{2^{m-1}-1} a^{2i} sb + (u + vb)b + b(u + vb) \\ &= sa\widehat{a^2}b + ub + vb^2 + u^{\otimes}b + v^{\otimes}b^2 \\ &= (v + v^{\otimes})a^{2^{m-1}} + (sa\widehat{a^2} + u + u^{\otimes})b. \end{aligned}$$

Now by Equations (6.5), (6.2) and (6.1)

$$\begin{aligned}
0 &= f^*(abab^{-1}) = f(a)bab^{-1} + af(b)ab^{-1} + abf(a)b^{-1} + abaf^*(b^{-1}) \\
&= (r + sb)bab^{-1} + a(u + vb)ab^{-1} + ab(r + sb)b^{-1} + abab^{-1}f(b)b^{-1} \\
&= (r + sb)bab^{-1} + a(u + vb)ab^{-1} + ab(r + sb)b^{-1} + abab^{-1}(u + vb)b^{-1} \\
&= ra^{-1} + sab + ua^2b^3 + v + r^{\otimes}a + s^{\otimes}ab + ub^3 + v \\
&= ra^{-1} + sab + ua^2a^{2^{m-1}}b + r^{\otimes}a + s^{\otimes}ab + ua^{2^{m-1}}b \\
&= ra^{-1} + r^{\otimes}a + ((s + s^{\otimes})a + ua^{2^{m-1}}(1 + a^2))b.
\end{aligned}$$

Therefore the map f can be extended to a derivation of $\mathbb{F}_{2^t}Q_{2^{m+1}}$ if and only if

$$v + v^{\otimes} = 0, \quad (6.6)$$

$$saa^{\widehat{2}} + u + u^{\otimes} = 0, \quad (6.7)$$

$$ra^{-1} + r^{\otimes}a = 0, \text{ and} \quad (6.8)$$

$$(s + s^{\otimes}) + ua^{2^{m-1}}(a^{-1} + a) = 0. \quad (6.9)$$

Each of these equations will be considered. First note that for any element $c = \sum_{i=0}^{2^m-1} c_i a^i$ of $\mathbb{F}_{2^t}\langle a \rangle$,

$$c + c^{\otimes} = \sum_{i=0}^{2^m-1} (c_i + c_{-i})a^i = \sum_{i=0}^{2^{m-1}-1} (c_i + c_{-i})(a^i + a^{-i}) = \sum_{i=1}^{2^{m-1}-1} (c_i + c_{-i})(a^i + a^{-i}). \quad (6.10)$$

By Equations (6.6) and (6.10)

$$0 = v + v^{\otimes} = \sum_{i=1}^{2^{m-1}-1} (v_i + v_{-i})(a^i + a^{-i}).$$

$a^i + a^{-i} = 0$ if and only if $i = 0$ or $i = 2^{m-1}$. Thus $v_i = v_{-i}$, for $i = 1, \dots, 2^{m-1} - 1$

and so

$$v = v_0 + v_{2^{m-1}}a^{2^{m-1}} + \sum_{i=1}^{2^{m-1}-1} v_i(a^i + a^{-i}). \quad (6.11)$$

Equation (6.8) shall be considered next.

$$\begin{aligned} 0 &= ra^{-1} + r^{\otimes}a = \sum_{i=0}^{2^m-1} r_{i+1}a^{i+1}a^{-1} + \sum_{i=0}^{2^m-1} r_{-(i-1)}a^{i-1}a = \sum_{i=0}^{2^m-1} (r_{i+1} + r_{-i+1})a^i \\ &= \sum_{i=0}^{2^{m-1}-1} (r_{i+1} + r_{-i+1})(a^i + a^{-i}) = \sum_{i=1}^{2^{m-1}-1} (r_{i+1} + r_{-i+1})(a^i + a^{-i}). \end{aligned}$$

Therefore $r_{i+1} = r_{-i+1}$, for $i = 1, 2, \dots, 2^{m-1} - 1$ and so

$$r = r_1a + r_{2^{m-1}+1}a^{2^{m-1}+1} + \sum_{i=1}^{2^{m-1}-1} r_{i+1}(a^{i+1} + a^{-i+1}). \quad (6.12)$$

Now consider Equation (6.7). Let $k_0 = \sum_{i=0}^{2^{m-1}-1} s_{2i}$ and let $k_1 = \sum_{i=0}^{2^{m-1}-1} s_{2i+1}$. Then $sa\hat{a}^2 = k_1\hat{a}^2 + k_0a\hat{a}^2$. Also, 1 is not in the support of $u + u^{\otimes}$ and so by Equation (6.7), 1 is not in the support of $sa\hat{a}^2$, hence $k_1 = 0$. Therefore by Equation (6.10)

$$0 = sa\hat{a}^2 + u + u^{\otimes} = k_0a\hat{a}^2 + \sum_{i=1}^{2^{m-1}-1} (u_i + u_{-i})(a^i + a^{-i}).$$

Furthermore, for any i , a^{2i} is not in the support of $a\hat{a}^2$ and so

$$u_{2i} + u_{-2i} = 0, \quad \text{for } i = 1, 2, \dots, 2^{m-2} - 1 \text{ and} \quad (6.13)$$

$$k_0 = u_{2i+1} + u_{-2i-1}, \quad \text{for } i = 0, 1, \dots, 2^{m-2} - 1. \quad (6.14)$$

Thus using Equation (6.13)

$$u = u_0 + u_{2^{m-1}}a^{2^{m-1}} + \sum_{i=1}^{2^{m-2}-1} u_{2i}(a^{2i} + a^{-2i}) + \sum_{i=0}^{2^{m-1}-1} u_{2i+1}a^{2i+1}. \quad (6.15)$$

By Equation (6.14)

$$\begin{aligned}
\sum_{i=0}^{2^{m-1}-1} u_{2i+1} a^{2i+1} &= \sum_{i=0}^{2^{m-2}-1} u_{2i+1} a^{2i+1} + \sum_{i=0}^{2^{m-2}-1} u_{-(2i+1)} a^{-(2i+1)} \\
&= \sum_{i=0}^{2^{m-2}-1} u_{2i+1} a^{2i+1} + \sum_{i=0}^{2^{m-2}-1} (u_{2i+1} + k_0) a^{-(2i+1)} \\
&= \sum_{i=0}^{2^{m-2}-1} u_{2i+1} (a^{2i+1} + a^{-(2i+1)}) + \sum_{i=0}^{2^{m-2}-1} k_0 a^{-(2i+1)}.
\end{aligned}$$

Therefore by Equation (6.15)

$$u = u_0 + u_{2^{m-1}} a^{2^{m-1}} + \sum_{i=1}^{2^{m-1}-1} u_i (a^i + a^{-i}) + \sum_{i=0}^{2^{m-2}-1} k_0 a^{-2i-1}. \quad (6.16)$$

Equation (6.9) shall now be considered. Using Equation (6.10)

$$0 = (s + s^{\otimes}) + u a^{2^{m-1}} (a^{-1} + a) = \sum_{i=0}^{2^m-1} (s_i + s_{-i} + u_{2^{m-1}+i+1} + u_{2^{m-1}+i-1}) a^i. \quad (6.17)$$

$a^{2^{m-1}}$ is not in the support of $s + s^{\otimes}$ and so 1 is not in the support of $u(a^{-1} + a)$.

Thus $u_1 + u_{-1} = 0$ and so by Equation (6.14), $k_0 = u_{2i+1} + u_{-(2i+1)} = 0$, for $i = 0, 1, \dots, 2^{m-2} - 1$. Also, $s_i + s_{-i} = u_{2^{m-1}+i+1} + u_{2^{m-1}+i-1}$, for all $i = 0, 1, \dots, 2^m - 1$.

Thus since $k_1 = 0$

$$\begin{aligned}
0 &= \sum_{i=0}^{2^{m-1}-1} s_{2i+1} = \sum_{i=0}^{2^{m-2}-1} (s_{2i+1} + s_{-(2i+1)}) = \sum_{i=0}^{2^{m-2}-1} (u_{2^{m-1}+2i+2} + u_{2^{m-1}+2i}) \\
&= \left(\sum_{i=0}^{2^{m-2}-2} u_{2^{m-1}+2i+2} \right) + u_{2^{m-1}+2(2^{m-2}-1)+2} + u_{2^{m-1}+2(0)} + \sum_{i=1}^{2^{m-2}-1} u_{2^{m-1}+2i} \\
&= \sum_{i=1}^{2^{m-2}-1} (u_{2^{m-1}+2i} + u_{2^{m-1}+2i}) + u_0 + u_{2^{m-1}} = u_0 + u_{2^{m-1}}.
\end{aligned}$$

Therefore $u_0 = u_{2^{m-1}}$ and since $k_0 = 0$, Equation (6.16) can be written as

$$u = u_0(1 + a^{2^{m-1}}) + \sum_{i=1}^{2^{m-1}-1} u_i(a^i + a^{-i}). \quad (6.18)$$

So $u_i = u_{-i}$ for all i and by Equation (6.17), $s_i + s_{-i} = u_{2^{m-1}+i+1} + u_{2^{m-1}+i-1}$, for $i = 1, 2, \dots, 2^{m-1}-1$. Thus $s_i + s_{-i} = u_{2^{m-1}-i-1} + u_{2^{m-1}-i+1}$, for $i = 1, 2, \dots, 2^{m-1}-1$.

1. Recall that $\sum_{i=0}^{2^{m-1}-1} s_{2i} = k_0 = 0$ and so

$$\begin{aligned} s_0 &= \sum_{i=1}^{2^{m-1}-1} s_{2i} = s_{2^{m-1}} + \sum_{i=1}^{2^{m-2}-1} (s_{2i} + s_{-2i}) \\ &= s_{2^{m-1}} + \sum_{i=1}^{2^{m-2}-1} (u_{2^{m-1}-2i-1} + u_{2^{m-1}-2i+1}) = s_{2^{m-1}} + u_{2^{m-1}-1} + u_1, \end{aligned}$$

since the first summand of the i^{th} term of the sum cancels with the second summand of the $i+1^{\text{st}}$ term of the sum. Therefore

$$s = s_{2^{m-1}}(1 + a^{2^{m-1}}) + u_{2^{m-1}-1} + u_1 + \sum_{i=1}^{2^{m-1}-1} s_i(a^i + a^{-i}) + \sum_{i=1}^{2^{m-1}-1} (u_{2^{m-1}-i-1} + u_{2^{m-1}-i+1})a^{-i}.$$

Let $j = i - 2$. Then

$$\begin{aligned} \sum_{i=1}^{2^{m-1}-1} (u_{2^{m-1}-i-1} + u_{2^{m-1}-i+1})a^{-i} &= \sum_{i=1}^{2^{m-1}-1} u_{2^{m-1}-i-1}a^{-i} + \sum_{j=-1}^{2^{m-1}-3} u_{2^{m-1}-j-1}a^{-j-2} \\ &= \sum_{i=1}^{2^{m-1}-3} u_{2^{m-1}-i-1}(a^{-i} + a^{-i-2}) \\ &\quad + u_1 a^{2^{m-1}+2} + u_0 a^{2^{m-1}+1} + u_{2^{m-1}} a^{-1} + u_{2^{m-1}-1} a^{-2}. \end{aligned}$$

However by Equation (6.18), $u_{2^m-1} = u_0$ and so

$$\begin{aligned}
& u_{2^{m-1}-1} + u_1 + \sum_{i=1}^{2^{m-1}-1} (u_{2^{m-1}-i-1} + u_{2^{m-1}-i+1})a^{-i} \\
&= u_0(a^{2^{m-1}+1} + a^{-1}) + u_1(1 + a^{2^{m-1}+2}) + u_{2^{m-1}-1}(1 + a^{-2}) \\
&+ \sum_{i=1}^{2^{m-1}-3} u_{2^{m-1}-i-1}(a^{-i} + a^{-i-2}).
\end{aligned}$$

Therefore

$$\begin{aligned}
s &= s_{2^{m-1}}(1 + a^{2^{m-1}}) + \sum_{i=1}^{2^{m-1}-1} s_i(a^i + a^{-i}) + \sum_{i=1}^{2^{m-1}-3} u_{2^{m-1}-i-1}(a^{-i} + a^{-i-2}) \\
&+ u_0(a^{2^{m-1}+1} + a^{-1}) + u_1(1 + a^{2^{m-1}+2}) + u_{2^{m-1}-1}(1 + a^{-2}).
\end{aligned} \tag{6.19}$$

Therefore by Equations (6.12), (6.18), (6.19) and (6.11), f can be extended to a derivation of $\mathbb{F}_{2^t}Q_{2^{m+1}}$ if and only if

$$\begin{aligned}
r &= r_1a + r_{2^{m-1}+1}a^{2^{m-1}+1} + \sum_{i=1}^{2^{m-1}-1} r_{i+1}(a^{i+1} + a^{-i+1}), \\
u &= u_0(1 + a^{2^{m-1}}) + \sum_{i=1}^{2^{m-1}-1} u_i(a^i + a^{-i}), \\
s &= s_{2^{m-1}}(1 + a^{2^{m-1}}) + \sum_{i=1}^{2^{m-1}-1} s_i(a^i + a^{-i}) + \sum_{i=1}^{2^{m-1}-3} u_{2^{m-1}-i-1}(a^{-i} + a^{-i-2}) \\
&+ u_0(a^{2^{m-1}+1} + a^{-1}) + u_1(1 + a^{2^{m-1}+2}) + u_{2^{m-1}-1}(1 + a^{-2}) \quad \text{and} \\
v &= v_0 + v_{2^{m-1}}a^{2^{m-1}} + \sum_{i=1}^{2^{m-1}-1} v_i(a^i + a^{-i}),
\end{aligned} \tag{6.20}$$

where $r_1, r_2, \dots, r_{2^{m-1}+1}$, $s_1, s_2, \dots, s_{2^{m-1}}$, $u_0, u_1, \dots, u_{2^{m-1}-1}$ and $v_0, v_1, \dots, v_{2^{m-1}}$ are elements of \mathbb{F}_{2^t} . Therefore by counting the coefficients the dimension of the vector space of derivations of $\mathbb{F}_{2^t}Q_{2^{m+1}}$ is $2^{m-1} + 1 + 2^{m-1} + 2^{m-1} + 2^{m-1} + 1 = 2^{m+1} + 2$. \square

Remark 6.1.4. Equations (6.20) can be used to form a basis for the derivation

algebra of $\mathbb{F}_{2^t}Q_{2^{m+1}}$.

6.1.2 The Centers of the Derivation Algebras of the Dihedral and Quaternion Group Algebras

In this subsection the centers of $Der(\mathbb{F}_{2^t}D_{2^{m+1}})$ and $Der(\mathbb{F}_{2^t}Q_{2^{m+1}})$ are found.

Definition 6.1.5. Let I be the ideal of $\mathbb{F}_{2^t}Q_{2^{m+1}}$ generated by $1 + a^2$ and let J be the ideal of $\mathbb{F}_{2^t}Q_{2^{m+1}}$ generated by $\hat{a}^2 = \sum_{i=0}^{2^m-1} a^{2^i}$.

Remark 6.1.6. Let $\alpha \in \mathbb{F}_{2^t}Q_{2^{m+1}}$ and write $\alpha = x + yb$, where $x, y \in \mathbb{F}_{2^t}\langle a \rangle$. Then

$$(1+a^2)(x+yb) = x(1+a^2)+yb+yba^{-2} = x(1+a^2)+yba^{-2}(1+a^2) = (x+ya^2b)(1+a^2).$$

Thus the two-sided ideal I is the principal left ideal generated by the element $1 + a^2$. Also $J I = 0$, since \hat{a}^2 is central and $\hat{a}^2(1 + a^2) = 0$. Let $\beta = \sum_{i=0}^{2^m-1} c_i a^i + \sum_{i=0}^{2^m-1} k_i a^i b \in Ann(I)$, where $c_i, k_i \in \mathbb{F}_{2^t}$. Therefore

$$0 = \beta(1 + a^2) = \sum_{i=0}^{2^m-1} ((c_i + c_{i-2})a^i + (k_i + k_{i-2})a^i b),$$

which implies $c_i = c_{i-2}$ and $k_i = k_{i-2}$ for $i = 0, 1, \dots, 2^m - 1$. Therefore $\beta = c_0 \hat{a}^2 + c_1 a \hat{a}^2 + k_0 \hat{a}^2 b + k_1 a \hat{a}^2 b$ and so $\beta \in J$. Therefore J is the annihilator of I in $\mathbb{F}_{2^t}Q_{2^{m+1}}$.

Remark 6.1.7. Let $E = \{e \in \mathbb{F}_{2^t}\langle a^2 \rangle \mid |supp(e)| \text{ is even}\}$. Then $E \subset I$ since $(1 + a^2 + a^4 + \dots + a^{2^i-2})(1 + a^2) = 1 + a^{2^i} \in I$, for any integer i . Thus $aE \subset I$. Note that for any integer i , $a^i + a^{-i}$ is either in E or aE and so $a^i + a^{-i} \in I$. Let $d \in Der(\mathbb{F}_{2^t}Q_{2^{m+1}})$ and write $d(a) = r + sb$ and $d(b) = u + vb$, where $r, s, u, v \in$

$\mathbb{F}_{2^t}\langle a \rangle$. Then by Equations (6.20),

$$\begin{aligned} r &= r_1 a + r_{2^{m-1}+1} a + r_{2^{m-1}+1} a(1 + a^{2^{m-1}}) + \sum_{i=1}^{2^{m-1}-1} r_{i+1} (a^{i+1} + a^{-i+1}) \\ &= (r_1 + r_{2^{m-1}+1}) a + r_{2^{m-1}+1} a e_0 + \sum_{i=1}^{2^{m-1}-1} r_{i+1} e_i, \end{aligned}$$

where $e_j \in E \subset I$ for $j = 0, 1, \dots, 2^{m-1} - 1$. Similar computation for u, s and v give

$$\begin{aligned} r &= (r_1 + r_{2^{m-1}+1}) a + \bar{r}, \text{ where } \bar{r} \in I, \\ u &\in I, \\ s &\in I, \text{ and} \\ v &= (v_0 + v_{2^{m-1}}) + \bar{v}, \text{ where } \bar{v} \in I. \end{aligned} \tag{6.21}$$

Lemma 6.1.8. $\widehat{a}^2 \in \mathcal{C}(\mathbb{F}_{2^t} Q_{2^{m+1}})$.

Proof. Let $d \in \text{Der}(\mathbb{F}_{2^t} Q_{2^{m+1}})$ and let $d(a) = r + sb$, where $r, s \in \mathbb{F}_{2^t}\langle a \rangle$. Then by Equation (6.3)

$$d(a^{2^m-2j}) = a^{1-(2^m-2j)} \sum_{i=0}^{(2^m-2j)-1} a^{2i} sb = a^{1+2j} \sum_{i=0}^{2^m-2j-1} a^{2i} sb.$$

Letting $k = i + 2j$ gives

$$d(a^{2^m-2j}) = a^{1+2j} \sum_{k=2j}^{2^m-1} a^{2(k-2j)} sb = a^{1-2j} \sum_{k=2j}^{2^m-1} a^{2k} sb. \tag{6.22}$$

Also

$$\sum_{i=0}^{2^m-1} a^{2i} = \sum_{i=0}^{2^{m-1}-1} a^{2i} + \sum_{i=2^{m-1}}^{2^m-1} a^{2i} = \widehat{a}^2 + \widehat{a}^2 = 0. \tag{6.23}$$

Thus by Equation (6.23), adding Equations (6.3) and (6.22) gives

$$d(a^{2j}) + d(a^{2^m-2j}) = a^{1-2j} \sum_{i=0}^{2^m-1} a^{2i} sb = a^{1-2j} (0) sb = 0. \tag{6.24}$$

Therefore Letting $k = -i + 2^{m-1}$ gives

$$\begin{aligned}
d(\widehat{a^2}) &= \sum_{i=0}^{2^{m-1}-1} d(a^{2^i}) = \sum_{i=0}^{2^{m-2}-1} d(a^{2^i}) + \sum_{i=2^{m-2}}^{2^{m-1}-1} d(a^{2^i}) \\
&= \sum_{i=0}^{2^{m-2}-1} d(a^{2^i}) + \sum_{k=1}^{2^{m-2}} d(a^{2^{m-2k}}) \\
&= d(1) + d(a^{2^{m-1}}) + \sum_{i=1}^{2^{m-2}-1} \left(d(a^{2^i}) + d(a^{2^{m-2i}}) \right) \\
&= 0 + a^{1-2^{m-1}} \sum_{i=0}^{2^{m-1}-1} a^{2^i} sb + 0 = a^{1-2^{m-1}} \widehat{a^2} sb = 0,
\end{aligned}$$

since by Remark 6.1.7, $s \in I$ and J is the annihilator of I . □

Remark 6.1.9. Recall from Definition 3.1.8 that an ideal I of a ring R is a differential ideal of R if $d(I) \subset I$ for all $d \in \text{Der}(R)$. By Lemma 6.1.8 and Corollary 3.1.16, J is a differential ideal of $\mathbb{F}_{2^t}Q_{2^{m+1}}$.

Lemma 6.1.10. Let $\delta \in \mathfrak{g} = \text{Der}(\mathbb{F}_{2^t}Q_{2^{m+1}})$ and write $\delta(a) = w + xb$ and $\delta(b) = y + zb$, where $w, x, y, z \in \mathbb{F}_{2^t}\langle a \rangle$. Then δ is in the center of \mathfrak{g} if and only if $x = y = 0$, $w = c_1 a \widehat{a^2}$ and $z = c_2 \widehat{a^2}$, where $c_1, c_2 \in \mathbb{F}_{2^t}$.

Proof. Let d be an arbitrary element of \mathfrak{g} and write $d(a) = r + sb$ and $d(b) = u + vb$, where $r, s, u, v \in \mathbb{F}_{2^t}\langle a \rangle$.

Assume that δ is in the center of \mathfrak{g} , denoted by $Z(\mathfrak{g})$. Then $[\delta, d] = 0$, that is, $\delta(d(a)) + d(\delta(a)) = 0$ and $\delta(d(b)) + d(\delta(b)) = 0$.

Let $v = 1$ and $r = s = u = 0$ and so $d(a) = 0$ and $d(b) = b$. Then

$$0 = \delta(d(a)) + d(\delta(a)) = \delta(0) + d(w + xb) = d(w) + d(x)b + xd(b) = xb, \text{ and}$$

$$0 = \delta(d(b)) + d(\delta(b)) = \delta(b) + d(y + zb) = y + zb + zd(b) = y.$$

Therefore $x = y = 0$.

Let $r = a$ and $s = u = v = 0$ and so $d(a) = a$ and $d(b) = 0$. Write $w = \sum_{i=0}^{2^m-1} w_i a^i$ and $z = \sum_{i=0}^{2^m-1} z_i a^i$. Then

$$0 = \delta(d(a)) + d(\delta(a)) = \delta(a) + d(w) = w + \sum_{i=0}^{2^m-1} w_i d(a^i) = w + \sum_{\text{odd } i} w_i a^i, \text{ and}$$

$$0 = \delta(d(b)) + d(\delta(b)) = 0 + d(zb) = d(z)b = \sum_{i=0}^{2^m-1} z_i d(a^i)b = \sum_{\text{odd } i} z_i a^i b.$$

Therefore $w_i = 0$ for all even i and $z_i = 0$ for all odd i .

Let $v = a + a^{-1}$ and $r = s = u = 0$ and so $d(a) = 0$ and $d(b) = (a + a^{-1})b$.

Then

$$\begin{aligned} 0 &= \delta(d(b)) + d(\delta(b)) = \delta((a + a^{-1})b) + d(zb) \\ &= \delta(a + a^{-1})b + (a + a^{-1})\delta(b) + zd(b) \\ &= \delta(a + a^{-1})b + (a + a^{-1})zb + z(a + a^{-1})b = \delta(a + a^{-1})b. \end{aligned}$$

Thus by Equation (6.1), $0 = \delta(a) + \delta(a^{-1}) = w + a^{-1}wa^{-1}$ and so $w(1 + a^2) = 0$.

Therefore $w \in J$. However, $w_i = 0$ for all even i and so $w = c_1 a \widehat{a}^2$, where $c_1 \in \mathbb{F}_{2^t}$.

Let $s = a + a^{-1}$ and $r = u = v = 0$ and so $d(a) = (a + a^{-1})b$ and $d(b) = 0$. By Lemma 6.1.8, $\widehat{a}^2 \in \mathcal{C}(\mathbb{F}_{2^t} Q_{2^{m+1}})$ and so

$$\begin{aligned} 0 &= \delta(d(a)) + d(\delta(a)) = \delta((a + a^{-1})b) + d(c_1 a \widehat{a}^2) \\ &= \delta(a + a^{-1})b + (a + a^{-1})\delta(b) + c_1 \widehat{a}^2 d(a) \\ &= c_1 a \widehat{a}^2 b + a^{-1}(c_1 a \widehat{a}^2) a^{-1} b + (a + a^{-1})zb + c_1 \widehat{a}^2 (a + a^{-1})b \\ &= (a + a^{-1})zb. \end{aligned}$$

Therefore, $z(1 + a^2) = 0$ and so $z \in J$. However, $z_i = 0$ for all odd i and so $z = c_2 \widehat{a}^2$, where $c_2 \in \mathbb{F}_{2^t}$.

Conversely, let $\delta \in \mathfrak{g}$ and assume $\delta(a) = c_1 a \widehat{a}^2$ and $\delta(b) = c_2 \widehat{a}^2 b$, where $c_1, c_2 \in \mathbb{F}_{2^t}$. Therefore $\delta(x) \in J$, for all $x \in \mathbb{F}_{2^t} Q_{2^{m+1}}$. Let $z \in I$ and so by Remark 6.1.6, $z = \bar{z}(1 + a^2)$, for some $\bar{z} \in \mathbb{F}_{2^t} Q_{2^{m+1}}$. Also, $\delta(1 + a^2) = \delta(a)a + a\delta(a) = c_1 \widehat{a}^2 + c_1 \widehat{a}^2 = 0$. Hence $\delta(z) = \delta(\bar{z}(1 + a^2)) = \delta(\bar{z})(1 + a^2) = 0$, since $\delta(\bar{z}) \in J$ and J is the annihilator of I . Therefore $\delta(I) = 0$. By Remark 6.1.7, $s \in I$ and $r = \tilde{r}a + \bar{r}$, where $\tilde{r} \in \mathbb{F}_{2^t}$ and $\bar{r} \in I$. Therefore

$$\begin{aligned} \delta(d(a)) + d(\delta(a)) &= \delta(r + sb) + d(c_1 a \widehat{a}^2) \\ &= \delta(\tilde{r}a + \bar{r}) + \delta(s)b + s\delta(b) + c_1 \widehat{a}^2(r + sb) \\ &= \tilde{r}(c_1 a \widehat{a}^2) + 0 + 0b + s(c_2 \widehat{a}^2 b) + c_1 \widehat{a}^2(\tilde{r}a + \bar{r} + sb) \\ &= \tilde{r}(c_1 a \widehat{a}^2) + 0 + c_1 \widehat{a}^2(\tilde{r}a) + 0 + 0 = 0. \end{aligned}$$

Also by Remark 6.1.7, $u \in I$ and $v = \tilde{v} + \bar{v}$, where $\tilde{v} \in \mathbb{F}_{2^t}$ and $\bar{v} \in I$. Thus $\delta(u) = \delta(v) = 0$. Therefore

$$\begin{aligned} \delta(d(b)) + d(\delta(b)) &= \delta(u + vb) + d(c_2 \widehat{a}^2 b) = 0 + v\delta(b) + c_2 \widehat{a}^2 d(b) \\ &= v(c_2 \widehat{a}^2 b) + c_2 \widehat{a}^2 (u + vb) = c_2 \widehat{a}^2 (u) = 0. \end{aligned}$$

Therefore δ is in the center of \mathfrak{g} . □

Lemma 6.1.11. *The derivation algebra $Der(\mathbb{F}_{2^t} D_{2^{m+1}})$ has trivial center.*

Proof. Let $\mathfrak{g} = Der(\mathbb{F}_{2^t} D_{2^{m+1}})$ and let d be an element of \mathfrak{g} . Then by Theorem 3.11 of [12], $d(x) = \Lambda y + x\Omega y$ and $d(y) = \Omega$, where $\Lambda \in C(xy)$, the centraliser of xy in $\mathbb{F}_{2^t} D_{2^{m+1}}$ and $\Omega \in C(y)$, the centraliser of y in $\mathbb{F}_{2^t} D_{2^{m+1}}$.

Let $\delta \in \mathfrak{g}$ and so $\delta(x) = \rho y + x\sigma y$ and $\delta(y) = \sigma$, where $\rho \in C(xy)$ and $\sigma \in C(y)$. Assume that δ is in the center of \mathfrak{g} and so $[\delta, d] = 0$.

Let $\Omega = 0$ and $\Lambda = 1$ and so $d(x) = y$ and $d(y) = 0$. Therefore

$$0 = \delta(d(y)) + d(\delta(y)) = \delta(0) + d(\sigma) = d(\sigma), \text{ and}$$

$$0 = \delta(d(x)) + d(\delta(x)) = \delta(y) + d(\rho y + x\sigma y) = \sigma + d(\rho)y + y\sigma y = d(\rho)y.$$

Therefore $d(\sigma) = d(\rho) = 0$.

Let $\Omega = y$ and $\Lambda = xy$ and so $d(x) = 0$ and $d(y) = y$. Therefore

$$0 = \delta(d(y)) + d(\delta(y)) = \delta(y) + d(\sigma) = \sigma, \text{ and}$$

$$0 = \delta(d(x)) + d(\delta(x)) = \delta(0) + d(\rho y) = \rho d(y) = \rho y.$$

Therefore $\sigma = \rho = 0$ and so δ is the zero derivation. Hence $Der(\mathbb{F}_{2^t}D_{2^{m+1}})$ has trivial center. \square

6.1.3 Using Derivations to Distinguish $\mathbb{F}_{2^t}D_{2^{m+1}}$ and $\mathbb{F}_{2^t}Q_{2^{m+1}}$

Assuming that $\mathbb{F}_{2^t}D_{2^{m+1}}$ and $\mathbb{F}_{2^t}Q_{2^{m+1}}$ are isomorphic as rings, then Theorem 3.1.18 states that $Der(\mathbb{F}_{2^t}D_{2^{m+1}})$ and $Der(\mathbb{F}_{2^t}Q_{2^{m+1}})$ are isomorphic as additive groups. The results of Sections 6.1.1 and 6.1.2 are now used to show that no such isomorphism exists and so the group rings $\mathbb{F}_{2^t}D_{2^{m+1}}$ and $\mathbb{F}_{2^t}Q_{2^{m+1}}$ are not isomorphic as rings.

Lemma 6.1.12. $\mathbb{F}_{2^t}D_{2^{m+1}}$ and $\mathbb{F}_{2^t}Q_{2^{m+1}}$ are not isomorphic as rings.

Proof. By Theorem 2.3.11 the dimension of $Der(\mathbb{F}_{2^t}D_{2^{m+1}})$ is $2n + 4 = 2^{m+1} + 4$. By Theorem 6.1.3 the dimension of $Der(\mathbb{F}_{2^t}Q_{2^{m+1}})$ is $2^{m+1} + 2$. Therefore by Theorem 3.1.18, $\mathbb{F}_{2^t}D_{2^{m+1}}$ is not isomorphic to $\mathbb{F}_{2^t}Q_{2^{m+1}}$ as rings. \square

Alternatively using the results of Section 6.1.2 we can show that they are not isomorphic as K -algebras.

Proof. By Lemma 6.1.11 the dimension of the center of $Der(\mathbb{F}_{2^t}D_{2^{m+1}})$ is 0, whereas by Lemma 6.1.10 the dimension of the center of $Der(\mathbb{F}_{2^t}Q_{2^{m+1}})$ is 2. Therefore by Theorem 3.1.20, $\mathbb{F}_{2^t}D_{2^{m+1}}$ is not isomorphic to $\mathbb{F}_{2^t}Q_{2^{m+1}}$ as K -algebras. \square

6.2 The Ring of Constants and the Modular Isomorphism Problem

Remark 6.2.1. Let $\phi: R \rightarrow T$ be a ring homomorphism. Then the restriction of ϕ to a subring S of R is a ring homomorphism from S into T .

Definition 6.2.2. Let R be a ring with 1. Denote the group of units (invertible elements) of R by $\mathcal{U}(R)$.

Definition 3.1.15 is repeated here for ease of access.

Definition 3.1.15. Let d be a derivation of a unital ring R and let Δ be a subset of $Der(R)$. Then the subring of R defined by $\mathcal{C}_\Delta = \{c \in R \mid d(c) = 0 \text{ for all } d \in \Delta\}$ is called the *ring of constants of Δ* . If Δ is a set with one element d then \mathcal{C}_Δ will be denoted by \mathcal{C}_d and if $\Delta = Der(R)$ then \mathcal{C}_Δ will be denoted by $\mathcal{C}(R)$ and is then called the *ring of constants of R* .

Lemma 6.2.3. Let R be a ring with 1 and let V be a subgroup of the unit group of R . Then $V \cap \bigcap_{d \in \Delta} \mathcal{C}_d$ is a subgroup of V for all subsets Δ of $Der(R)$.

Proof. Let $d \in Der(R)$ and let $H = V \cap \mathcal{C}_d$. Then H is non empty as 1 is an element of both V and \mathcal{C}_d . Let $u, v \in H$. Then $d(uv) = d(u)v + ud(v) = 0 + 0 = 0$ and so $uv \in H$. Also, $0 = d(1) = d(uu^{-1}) = d(u)u^{-1} + ud(u^{-1})$ and so $u^{-1} \in H$. Thus H is a subgroup of V . Therefore $V \cap \bigcap_{d \in \Delta} \mathcal{C}_d$ is a subgroup of V for all subsets Δ of $Der(R)$, since it is an intersection of subgroups of V . \square

Definition 6.2.4. Let R be a ring with 1, let V be a subgroup of $\mathcal{U}(R)$ and let Δ be a subset of $Der(R)$. Then denote by VC_Δ the subgroup of V defined by $V \cap \bigcap_{d \in \Delta} \mathcal{C}_d$. If Δ is a set with one element d then VC_Δ will be denoted by VC_d and if $\Delta = Der(R)$ then VC_Δ will be denoted by $VC(R)$. Also, define the *group of constants of R* , denoted by $\mathcal{UC}(R)$ to be $\mathcal{U}(R) \cap \mathcal{C}(R)$.

Remark 6.2.5. Let K be a finite field and let G be a finite group. Then for $a, b \in Z(KG)$ and $\alpha \in KG$

$$\begin{aligned}\alpha(a + b) &= \alpha a + \alpha b = a\alpha + b\alpha = (a + b)\alpha, \text{ and} \\ \alpha ab &= a\alpha b = ab\alpha.\end{aligned}$$

Therefore $Z(KG)$ is a subalgebra of KG .

Lemma 6.2.6. *Let K be a finite field and let G be a finite group. Then $\mathcal{C}(KG)$ the ring of constants of KG , is a subalgebra of $Z(KG)$, the center of KG .*

Proof. Let α be an element of KG such that $\alpha \notin Z(KG)$. Then there exists an element β of KG such that $[\beta, \alpha] \neq 0$. Thus $d_\beta(\alpha) \neq 0$, where d_β is the inner derivation of KG induced by β . Therefore $\alpha \notin \mathcal{C}(KG)$ and so $\mathcal{C}(KG) \subset Z(KG)$.

Let $a, b \in \mathcal{C}(KG)$ and let $k \in K$. Then for any $d \in Der(KG)$

$$\begin{aligned}d(ab) &= d(a)b + ad(b) = (0)b + a(0) = 0 + 0 = 0, \\ d(a + b) &= d(a) + d(b) = 0 + 0 = 0, \\ d(ka) &= kd(a) = k(0) = 0.\end{aligned}$$

Therefore $\mathcal{C}(KG)$ is a subalgebra of $Z(KG)$. □

Lemma 6.2.7. *Let G and H be a finite abelian groups, let K be a finite field and let V be a subgroup of $\mathcal{U}(KG)$. Let $\phi: KG \rightarrow KH$ be a ring homomorphism*

such that $I = \ker(\phi)$ is a differential ideal of the differential ring (KG, d) . Define $\bar{d}: KG/I \rightarrow KG/I$ by $\bar{d}(a + I) = d(a) + I$. Let Δ be a subset of $Der(KG)$, let $\bar{\Delta} = \{\bar{d} \mid d \in \Delta\}$ and let $\bar{V} = \phi(V)$. Then the restriction of ϕ to VC_{Δ} is a group homomorphism to $\bar{V}C_{\bar{\Delta}}$.

Proof. By Lemma 3.1.9, $\bar{d} \in Der(KG/I)$ and by Lemma 3.1.11, $\phi \circ d = \bar{d} \circ \phi$. Therefore the restriction of ϕ to VC_d is a group homomorphism to $\bar{V}C_{\bar{d}}$. Thus the restriction of ϕ to VC_{Δ} is a group homomorphism to $\bar{V}C_{\bar{\Delta}}$ since $VC_{\Delta} = \bigcap_{d \in \Delta} VC_d$. \square

Remark 6.2.8. Let G and H be finite groups (not necessarily abelian) and let K be a finite field. Let $\phi: KG \rightarrow KH$ be a ring isomorphism, let $d \in Der(KG)$ and define $\bar{d} = \phi \circ d \circ \phi^{-1}$. Then by Theorem 3.1.20, $\bar{d} \in Der(KH)$. Let Δ be a subset of $Der(KG)$ and let $\bar{\Delta} = \{\bar{d} \mid d \in \Delta\}$. Let V be a subgroup of $\mathcal{U}(KG)$ and let $\bar{V} = \phi(V)$. Then the restriction of ϕ to VC_{Δ} is a group isomorphism onto $\bar{V}C_{\bar{\Delta}}$. In particular the unit group of the ring of constants of KG is isomorphic to the unit group of the ring of constants of KH .

In Section 4.6, it was shown that all nilpotent derivations of $\mathbb{F}_2C_4 \times C_4$ have a nilpotency index less than or equal to 8 and also that there is a nilpotent derivation of $\mathbb{F}_2C_8 \times C_2$ that has a nilpotency index of 13. This shows that the group algebras are not isomorphic as K -algebras. It is now shown that they are not isomorphic as rings by computing their respective unit groups of constants.

Example 6.2.9. Let $G = \langle x, y \mid x^4 = y^4 = x^{-1}y^{-1}xy = 1 \rangle$ and let K be the field with 2 elements. Then $\mathcal{C}(KG)$ is the K -span of $\{1, x^2, y^2, x^2y^2\}$. Therefore $\mathcal{UC}(KG) = \{1, x^2, y^2, x^2y^2, 1+z, x^2+z, y^2+z, x^2y^2+z\}$, where $z = (1+x^2)(1+y^2)$. $(a+z)^2 = a^2$ for all $a \in KG$ and so $\mathcal{UC}(KG) \simeq C_2^3$ since it has exponent 2.

Example 6.2.10. Let $H = \langle x, y \mid x^8 = y^2 = x^{-1}y^{-1}xy = 1 \rangle$ and let K be the field with 2 elements. Then $\mathcal{C}(KH)$ is the K -span of $\{1, x^2, x^4, x^6\}$. Therefore

$\mathcal{UC}(KH) = \{1, x^2, x^4, x^6, 1+z, x^2+z, x^4+z, x^6+z\}$, where $z = (1+x^2)(1+x^4)$. $(a+z)^2 = a^2$ for all $a \in KH$ and so $\mathcal{UC}(KH) \simeq C_4 \times C_2$ since it is an abelian group of order 8 with elements of order 4 but none of order 8.

Examples 6.2.9 and 6.2.10 show that $\mathcal{UC}(KG)$ and $\mathcal{UC}(KH)$ are not isomorphic as groups and so by Remark 6.2.8, KG and KH are not isomorphic as rings.

Theorem 6.2.11. [40] *Let $\theta: G \rightarrow H$ be a group homomorphism. Then there exists a unique ring homomorphism, $\Theta: RG \rightarrow RH$ such that $\Theta(g) = \theta(g)$, for all $g \in G$. If R is commutative, then Θ is a homomorphism of R -algebras. Moreover, if θ is an epimorphism (monomorphism), then Θ is an epimorphism (monomorphism).*

6.2.1 The Ring of Constants of Dihedral Group Algebras

Let K be a finite field of characteristic 2 and let $D_{2^{m+1}} = \langle x, y \mid x^{2^m} = y^2 = (xy)^2 = 1 \rangle$ be the dihedral group of order 2^{m+1} , where $m \in \{2, 3, 4, \dots\}$. In this section $\mathcal{C}(KD_{2^{m+1}})$, the ring of constants of the dihedral group algebra $KD_{2^{m+1}}$ is calculated.

Theorem 6.2.12. *Let K be a finite field of characteristic 2 and let $D_{2^{m+1}}$ be the dihedral group of order 2^{m+1} , where $m \in \{2, 3, 4, \dots\}$. Then the set*

$$\mathcal{B} = \{1, x^{2^i} + x^{-2^i} \mid i = 1, 2, \dots, 2^{m-2} - 1\}$$

is a basis for $\mathcal{C}(KD_{2^{m+1}})$, the ring of constants of $KD_{2^{m+1}}$.

Proof. By Lemma 6.2.6, $\mathcal{C}(KD_{2^{m+1}}) \subset Z(KD_{2^{m+1}})$. By Lemma 2.3.8, $Z(KD_{2^{m+1}})$ is a $2^{m-1} + 3$ dimensional subspace of $KD_{2^{m+1}}$ with the set $\{1, x^{2^{m-1}}, x^1 + x^{-1}, x^2 + x^{-2}, \dots, x^{2^{m-1}-1} + x^{2^{m-1}+1}, \widehat{x^2}y, x\widehat{x^2}y\}$ acting as a basis. Let V be the K -span of \mathcal{B} . It is now shown that $V \subset \mathcal{C}(KD_{2^{m+1}})$.

Let $d \in \text{Der}(KD_{2m+1})$ and write $d(x) = a + by$, where $a, b \in K\langle x \rangle$. Then by Lemma 2.2.1

$$\begin{aligned} d(x^i) &= \sum_{j=0}^{i-1} x^j(a + by)x^{i-j-1} = \sum_{j=0}^{i-1} x^{i-1}a + x^{1-i} \sum_{j=0}^{i-1} x^{2j}by \\ &= ix^{i-1}a + x^{1-i} \sum_{j=0}^{i-1} x^{2j}by. \end{aligned} \quad (6.25)$$

Therefore $d(x^i) = ix^{i-1}a + \gamma y$, for some $\gamma \in K\langle x \rangle$. Also $0 = d(1) = d(x^i x^{-i})$ and so $d(x^{-i}) = x^{-i}d(x^i)x^{-i}$. Therefore

$$\begin{aligned} d(x^i + x^{-i}) &= ix^{i-1}a + \gamma y + x^{-i}(ix^{i-1}a + \gamma y)x^{-i} \\ &= ix^{i-1}a + \gamma y + ix^{i-1}ax^{-2i} + \gamma y = ix^{i-1}a(1 + x^{-2i}). \end{aligned} \quad (6.26)$$

By Equation (6.26), $d(x^{2i} + x^{-2i}) = 0$ for $i = 1, 2, \dots, 2^{m-2} - 1$. Also $d(1) = 0$ and so $V \subset \mathcal{C}(KD_{2m+1})$.

It is now shown that $\mathcal{C}(KD_{2m+1}) \subset V$. Let $c \in \mathcal{C}(KD_{2m+1})$ and write $c = k_0 \widehat{x^2}y + k_1 x \widehat{x^2}y + \zeta$, where $k_0, k_1 \in K$ and $\zeta \in K\langle x \rangle$. Theorem 2.3.11 gives a basis for $\text{Der}(KD_{2m+1})$. Let d_1 be the derivation of KD_{2m+1} defined by $d_1(x) = 0$ and $d_1(y) = y$. This implies $d_1(K\langle x \rangle) = 0$ and so

$$0 = d_1(c) = d_1(k_0 \widehat{x^2}y + k_1 x \widehat{x^2}y + \zeta) = k_0 \widehat{x^2}d_1(y) + k_1 x \widehat{x^2}d_1(y) + 0 = k_0 \widehat{x^2}y + k_1 x \widehat{x^2}y.$$

Therefore $k_0 = k_1 = 0$ and so $c \in \mathcal{C}(KD_{2m+1}) \cap K\langle x \rangle$.

Let d_2 be the derivation of KD_{2m+1} defined by $d_2(x) = x + y$ and $d_2(y) = y$. Letting $i = 2^{m-1}$, $a = x$ and $b = 1$ in Equation (6.25) gives

$$d_2(x^{2^{m-1}}) = 2^{m-1}x^{2^{m-1}} + x^{1-2^{m-1}} \sum_{j=0}^{2^{m-1}-1} x^{2j}y = 0 + xx^{2^{m-1}} \widehat{x^2}y = x \widehat{x^2}y. \quad (6.27)$$

Letting $a = x$ in Equation (6.26) gives

$$d_2(x^i + x^{-i}) = ix^i(1 + x^{-2i}) = x^i + x^{-i}, \text{ for odd } i. \quad (6.28)$$

It has been shown that $c \in \mathcal{C}(KD_{2m+1}) \cap K\langle x \rangle$ and so c can be written as $c = c_0x^{2^{m-1}} + \sum_{i=1}^{2^{m-2}} c_i(x^{2^{i-1}} + x^{-(2^{i-1})}) + v$, where $c_j \in K$ for $j \in \{0, 1, \dots, 2^{m-2}\}$ and $v \in V \subset \mathcal{C}(KD_{2m+1})$. Therefore by Equations (6.27) and (6.28)

$$\begin{aligned} 0 &= d_2(c) = c_0d_2(x^{2^{m-1}}) + \sum_{i=1}^{2^{m-2}} c_id_2(x^{2^{i-1}} + x^{-(2^{i-1})}) + d_2(v) \\ &= c_0x\widehat{x}^2y + \sum_{i=1}^{2^{m-2}} c_i(x^{2^{i-1}} + x^{-(2^{i-1})}) + 0. \end{aligned}$$

Therefore $c_j = 0$, for $j \in \{0, 1, \dots, 2^{m-2}\}$ and so $\mathcal{C}(KD_{2m+1}) \subset V$. \mathcal{B} is a linearly independent set and so \mathcal{B} is a basis for $V = \mathcal{C}(KD_{2m+1})$. \square

6.2.2 The Ring of Constants of Quaternion Group Algebras

Let K be a finite field of characteristic 2 and let m be a positive integer greater than 1. Let Q_{2m+1} denote the generalised quaternion group with 2^{m+1} elements and presentation $\langle a, b \mid b^2 = a^{2^{m-1}}, abab^{-1} = 1 \rangle$.

Lemma 6.2.13. *The set*

$$\{1, a^{2^{m-1}}, \widehat{a^2}b, a\widehat{a^2}b\} \cup \{a^i + a^{-i} \mid i = 1, 2, \dots, 2^{m-1} - 1\}$$

forms a basis for $Z(KQ_{2m+1})$.

Proof. By Lemma 2.3.7, the set of all finite conjugacy class sums forms a basis for $Z(KQ_{2m+1})$. Let $g, h \in Q_{2m+1}$ and write $g = a^ib^j$ and $h = a^kb^l$, where $i, k \in$

$\{0, 1, \dots, 2^m - 1\}$ and $j, l \in \{0, 1\}$. Then

$$\begin{aligned} g^h &= h^{-1}gh = b^{-l}a^{-k}a^i a^k b^l = b^{-l}a^i b^l = a^{(-1)^l i}, \quad \text{for } j = 0, \\ g^h &= b^{-l}a^{-k}a^i b a^k b^l = b^{-l}a^{i-2k} b b^l = a^{(-1)^l(i-2k)} b^{-l} b b^l = a^{(-1)^l(i-2k)} b, \quad \text{for } j = 1. \end{aligned}$$

Therefore the $2^{m-1} + 3$ conjugacy classes are:

$$\begin{aligned} &\{1\}, \{a^{2^{m-1}}\}, \{a^i, a^{-i}\} \text{ for } i = 1, 2, \dots, 2^{m-1} - 1, \\ &\{a^{2^j} b \mid j = 0, 1, \dots, 2^{m-1} - 1\} \text{ and } \{a^{2^{j+1}} b \mid j = 0, 1, \dots, 2^{m-1} - 1\}. \end{aligned}$$

The result follows by summing over each class and the fact that $\sum_{j=0}^{2^{m-1}-1} a^{2^j} = \widehat{a}^2$. \square

Theorem 6.2.14. *Let K be a finite field of characteristic 2 and let $Q_{2^{m+1}}$ be the generalised quaternion group of order 2^{m+1} , where $m \in \{2, 3, 4, \dots\}$. Then the set*

$$\mathcal{B} = \{1, b^2, a^{2^i} + a^{-2^i} \mid i = 1, 2, \dots, 2^{m-2} - 1\}$$

is a basis for $\mathcal{C}(KQ_{2^{m+1}})$.

Proof. By Lemma 6.2.6, $\mathcal{C}(KQ_{2^{m+1}}) \subset Z(KQ_{2^{m+1}})$. By Lemma 6.2.13, $Z(KQ_{2^{m+1}})$ is a $2^{m-1} + 3$ dimensional subspace of $KQ_{2^{m+1}}$ with the set $\{1, b^2, \widehat{a}^2 b, a\widehat{a}^2 b\} \cup \{a^i + a^{-i} \mid i = 1, 2, \dots, 2^{m-1} - 1\}$ acting as a basis. Let V be the K -span of \mathcal{B} . It is now shown that $V \subset \mathcal{C}(KQ_{2^{m+1}})$.

Let $d \in \text{Der}(KQ_{2^{m+1}})$. Write $d(a) = r + sb$ and $d(b) = u + vb$, where $r, s, u, v \in K\langle a \rangle$. By Equation (6.20) $u, v \in Z(KQ_{2^{m+1}})$. Therefore

$$d(b^2) = (u + vb)b + b(u + vb) = ub + vb^2 + bu + bvb = 0. \quad (6.29)$$

Also

$$d(a^i) = \sum_{j=0}^{i-1} a^j(r + sb)a^{i-j-1} = \sum_{j=0}^{i-1} a^{i-1}r + \gamma b = ia^{i-1}r + \gamma b, \quad (6.30)$$

for some $\gamma \in K\langle a \rangle$. Also $0 = d(1) = d(a^i a^{-i})$ and so $d(a^{-i}) = a^{-i}d(a^i)a^{-i}$.

Therefore

$$\begin{aligned} d(a^i + a^{-i}) &= ia^{i-1}r + \gamma b + a^{-i}(ia^{i-1}r + \gamma b)a^{-i} \\ &= ia^{i-1}r + \gamma b + ia^{i-1}ra^{-2i} + \gamma b = ia^{i-1}r(1 + a^{-2i}). \end{aligned} \quad (6.31)$$

By Equation (6.31), $d(a^{2i} + a^{-2i}) = 0$ for $i = 1, 2, \dots, 2^{m-2} - 1$. Also $d(1) = 0$ and $d(b^2) = 0$ by Equation (6.29) and so $V \subset \mathcal{C}(KQ_{2^{m+1}})$.

It is now shown that $\mathcal{C}(KQ_{2^{m+1}}) \subset V$. Let $c \in \mathcal{C}(KQ_{2^{m+1}})$ and write $c = k_0 \widehat{a^2}b + k_1 a \widehat{a^2}b + z$, where $k_0, k_1 \in K$ and $z \in K\langle a \rangle$. Let d_1 be the derivation of $KQ_{2^{m+1}}$ defined by letting $r = s = u = 0$ and $v = 1$ in Equation (6.20). Thus $d_1(a) = 0$ and $d_1(b) = b$. This implies $d_1(K\langle a \rangle) = 0$ and so

$$0 = d_1(c) = d_1(k_0 \widehat{a^2}b + k_1 a \widehat{a^2}b + z) = k_0 \widehat{a^2}d_1(b) + k_1 a \widehat{a^2}d_1(b) + 0 = k_0 \widehat{a^2}b + k_1 a \widehat{a^2}b.$$

Therefore $k_0 = k_1 = 0$ and so $c \in Z(KQ_{2^{m+1}}) \cap K\langle a \rangle$. Therefore c can be written as $c = \sum_{i=1}^{2^{m-2}} c_i(a^{2i-1} + a^{-(2i-1)}) + v$, where $c_i \in K$ for $i \in \{1, 2, \dots, 2^{m-2}\}$ and $v \in V \subset \mathcal{C}(KQ_{2^{m+1}})$. Let d_2 be the derivation of $KQ_{2^{m+1}}$ defined by letting $s = u = v = 0$ and $r = a$ in Equation (6.20). Thus $d_2(a) = a$ and $d_2(b) = 0$. Letting $r = a$ in Equation (6.31) implies $d_2(a^i + a^{-i}) = a^i(1 + a^{-2i}) = a^i + a^{-i}$, for odd i and so

$$\begin{aligned} 0 &= d_2(c) = d_2\left(\sum_{i=1}^{2^{m-2}} c_i(a^{2i-1} + a^{-(2i-1)}) + v\right) \\ &= \sum_{i=1}^{2^{m-2}} c_i d_2(a^{2i-1} + a^{-(2i-1)}) + d_2(v) = \sum_{i=1}^{2^{m-2}} c_i(a^{2i-1} + a^{-(2i-1)}). \end{aligned}$$

Therefore $c_i = 0$, for $i \in \{1, 2, \dots, 2^{m-2}\}$ and so $\mathcal{C}(KQ_{2^{m+1}}) \subset V$. \mathcal{B} is a linearly independent set and so \mathcal{B} is a basis for $V = \mathcal{C}(KQ_{2^{m+1}})$. \square

Corollary 6.2.15. *$KD_{2^{m+1}}$ and $KQ_{2^{m+1}}$ are not isomorphic as rings.*

Proof. By Theorem 6.2.12 the dimension of $\mathcal{C}(KD_{2^{m+1}})$ is 2^{m-2} . By Theorem 6.2.14 the dimension of $\mathcal{C}(KQ_{2^{m+1}})$ is $2^{m-2} + 1$. A ring isomorphism preserves subrings and so the restriction of a ring isomorphism to the ring of constants is a ring isomorphism. Therefore $KD_{2^{m+1}}$ and $KQ_{2^{m+1}}$ are not isomorphic as rings. \square

6.2.3 A proof of Deskins' Theorem using derivations

The Modular Isomorphism Problem asks if the following statement is true:

$$KP \simeq KQ \implies P \simeq Q,$$

where P and Q are finite p -groups and K is the field with p elements. It was solved for abelian groups in 1956 by Deskins [14]. Since then there have been some further developments. The following list of cases where the Modular Isomorphism Problem has been solved can be found in [8]:

- abelian p -groups (Deskins' Theorem) [14]
- p -groups of class 2 with elementary abelian commutator subgroup [45]
- metacyclic p -groups, where $p > 3$ [5] and [46]
- 2-groups of maximal class [11]
- p -groups of maximal class, $p \neq 2$, when $|G| \leq p^{p+1}$ and G contains an abelian maximal subgroup [7]
- elementary abelian-by-cyclic groups [6]

- p -groups with center of index p^2 [15]

It has also been solved for p -groups containing a cyclic subgroup of index p^2 and groups of order p^5 and 2^7 [8].

An alternative proof to the theorem of Deskins' is now given using derivations.

Theorem 6.2.16. *Let G and H be finite abelian p -groups and let K be the field with p elements. Then KG is ring isomorphic to KH if and only if the groups G and H are isomorphic.*

Proof. By way of contradiction, assume G and H are minimal non-isomorphic p -groups such that KG is ring isomorphic to KH . Let $\phi: KG \rightarrow KH$ be a ring isomorphism. Then KG and KH have the same dimension as K -algebras and so $|G| = |H| = p^m$, for some non-negative integer m . By Theorem 2.3.4, the vector space of derivations of KG has dimension np^m , where n is the minimum number of generators of G . By Theorem 3.1.18, $Der(KG)$ and $Der(KH)$ are isomorphic as additive groups and so have the same dimension. Therefore G and H have the same number of generators in their decomposition using the fundamental theorem of finite abelian groups. Let A^p denote the group $\{a^p \mid a \in A\}$, for any abelian group A . Then by Lemma 5.5.8, $\mathcal{C}(KG) = K(G^p)$. The restriction of ϕ to the ring of constants $\mathcal{C}(KG)$ of KG is a ring isomorphism onto $\mathcal{C}(KH)$. Therefore there is a ring isomorphism from $K(G^p)$ onto $K(H^p)$. By the minimality assumption $G^p \simeq H^p$. This implies G and H are isomorphic groups which is a contradiction. Therefore $KG \simeq KH$ implies $G \simeq H$. The converse follows from Theorem 6.2.11. □

Chapter 7

Conclusions and Future Work

7.1 Conclusions

The primary aim of this thesis is to improve our understanding of the structure of group algebras. The methodology implemented was to study certain functions defined on the group algebras, namely derivations. For the most part the group algebras studied were finite and of positive characteristic. This focus was motivated by a potential application to error correcting codes. Also particular attention was given to finite modular group algebras. Recall Question 1.1 from Chapter 1:

What, if anything can the set of derivations of a group algebra
tell us about the structure of the group algebra itself? (1.1 revisited)

However, in order to be in a position to answer this question, we must first establish a good understanding of the derivations defined on the group algebra. For a particular group algebra, KG : Do derivations of KG exist? Are the derivations K -derivations? Do outer derivation exist? When are there only trivial derivations? How many derivations are there? What structure do they possess? Given a function on KG can you decide whether it is a derivation or not? These questions are

answered in Chapter 2. The zero map is always a derivation of KG . Theorem 2.2.2 shows that when K is an algebraic extension of a prime field all derivations of a K -algebra are K -derivations. Corollary 2.2.3 states if K is an algebraic extension of a prime field F , G is a torsion group whose center is of finite index and if $\text{char}(K) = 0$ or $\text{char}(K) = p > 0$, and p does not divide the order of g , for all $g \in G$, then every derivation of KG is inner. By Theorem 2.3.1 if R is a commutative unital ring and H is a torsion central subgroup of a group G , where the order of h is invertible in R , for all $h \in H$, then $d(R) = \{0\}$ if and only if $d(RH) = \{0\}$, for all $d \in \text{Der}(RG)$. Therefore if R is an algebraic extension of a prime field, the only derivation is the trivial derivation. In Theorem 2.3.4 a basis for the vector space of derivations of a finite commutative group algebra of positive characteristic is found. Theorem 2.2.5 classifies the derivations of group algebras in terms of the generators and defining relations of the group. If RG is a group ring, where R is commutative and S is a set of generators of G then necessary and sufficient conditions on a map from S to RG are established, such that the map can be extended to an R -derivation of RG . This theorem provides a way of deciding if a particular function on KG is a derivation or not.

We continue to explore the connection between a group algebra KG and its derivations $\text{Der}(KG)$ in Chapter 3. Corollary 3.1.14 shows that the augmentation ideal $\Delta(G, H)$ is a differential ideal with respect to a derivation if and only if the image of the subgroup H under the derivation is contained in the augmentation ideal. A consequence of this theorem is: H is a group of constants implies the augmentation ideal $\Delta(G, H)$ is a differential ideal. The Lie algebra of derivations of a group algebra is an interesting subject to study in its own right. However, the usefulness of studying the derivation Lie algebra to glean structural information regarding the group algebra is derived from the following 3 theorems:

Theorem 3.1.18. *Let R and S be rings and let $\phi: R \rightarrow S$ be a ring isomorphism.*

Let $\Phi: \text{Der}(R) \rightarrow \text{Der}(S)$ be defined by $d \mapsto \phi \circ d \circ \phi^{-1}$. Then Φ is an isomorphism of additive groups.

Theorem 3.1.20. *Let $\phi: R \rightarrow S$ be a K -algebra isomorphism. Then $\Phi: \text{Der}(R) \rightarrow \text{Der}(S)$, defined by $d \mapsto \phi \circ d \circ \phi^{-1}$ is a Lie algebra isomorphism.*

Theorem 4.1.8. *Let R and S be finite rings and let $\phi: R \rightarrow S$ be a ring isomorphism. Then there is a bijection Φ from $\text{Der}(R)$ onto $\text{Der}(S)$ such that $\Gamma(\Phi(d))$ and $\Gamma(d)$ are isomorphic digraphs, for all $d \in \text{Der}(R)$.*

The contrapositive statements of these theorems have been utilised in this thesis to prove that group algebras are not isomorphic (as rings or sometimes K -algebras).

A simple example of this technique is counting the derivations of KG . If $|\text{Der}(KG)| \neq |\text{Der}(KH)|$, then KG and KH are not isomorphic as rings. However, as was discussed in Chapter 4 this may not always distinguish the group algebras. For instance, $\mathbb{F}_2(C_4 \times C_4)$ and $\mathbb{F}_2(C_2 \times C_8)$ both have 2^{32} derivations. As a consequence, a different approach was required. In Chapter 4 a derivation was considered as a linear finite dynamical system (LFDS). This allowed for the comparison of properties of the LFDSs associated with the derivations of group algebras. It is then possible to distinguish between 2 group algebras by contrasting these LFDSs. As an example of this technique, the maximum value of the preperiod of a LFDS of a nilpotent derivation of $\mathbb{F}_2(C_4 \times C_4)$ is less than or equal to 8, whereas there is a nilpotent derivation of $\mathbb{F}_2(C_2 \times C_8)$ which has a maximum preperiod of 13. Therefore $\mathbb{F}_2(C_4 \times C_4)$ and $\mathbb{F}_2(C_2 \times C_8)$ are not isomorphic as rings.

Theorem 3.1.20, states that a K -algebra isomorphism between 2 finite group algebras implies that their derivation Lie algebras are isomorphic as Lie algebras. This theorem in the context of Question 1.1, motivates the study of the vector space of derivations of a group algebra as a Lie algebra, where the multiplication

is defined as the Lie commutator. It is shown that the derivation Lie algebra of a commutative group algebra over a finite field has trivial center. Theorem 5.4.14 proves that if K is a finite field of characteristic p and G is a finite abelian group such that its Sylow p -subgroup is elementary abelian, then all the derivations of $\mathfrak{g} = \text{Der}(KG)$ are inner and so \mathfrak{g} is a complete Lie algebra.

The Modular Isomorphism Problem was solved for abelian groups in 1956 by Deskins [14]. However it is still an important open problem for nonabelian groups. The Modular Isomorphism Problem asks if the following statement is true:

$$KP \simeq KQ \implies P \simeq Q,$$

where P and Q are finite p -groups and K is the field with p elements. Chapter 6 uses derivations to rule out the dihedral and generalised quaternion group algebras as possible counterexamples to the Modular Isomorphism Problem. Section 6.1 compares and contrasts the vector space of derivations of $\mathbb{F}_{2^t}D_{2^{m+1}}$ and $\mathbb{F}_{2^t}Q_{2^{m+1}}$. A basis of size $2^{m+1} + 2$ is exhibited for the vector space of derivations of $\mathbb{F}_{2^t}Q_{2^{m+1}}$. In Theorem 2.3.11 a basis of size $2^{m+1} + 4$ was found for the vector space of derivations of $\mathbb{F}_{2^t}D_{2^{m+1}}$. Therefore by Theorem 3.1.18, $\mathbb{F}_{2^t}D_{2^{m+1}}$ and $\mathbb{F}_{2^t}Q_{2^{m+1}}$ are not isomorphic as rings. The centers of the respective derivation Lie algebras are found in Section 6.1.2. It was shown that $\text{Der}(\mathbb{F}_{2^t}D_{2^{m+1}})$ has a trivial center, whereas the center of $\text{Der}(\mathbb{F}_{2^t}Q_{2^{m+1}})$ is 2 dimensional. This fact was used in Section 6.1.3 to show that $\mathbb{F}_{2^t}D_{2^{m+1}}$ and $\mathbb{F}_{2^t}Q_{2^{m+1}}$ are not isomorphic as K -algebras. Moreover, in Section 6.2 derivations of group algebras were used to give an alternative proof of Deskins' Theorem.

7.2 Future Work

Theorem 2.2.5 was applied to finite commutative group algebras in Section 2.3.1 and to dihedral group algebras of characteristic 2 in Section 2.3.2. However, it may be possible to derive an algorithm to generate a basis for $Der(KG)$ in general. Note that using GAP Version 4.8.6, to compute the derivation Lie algebra of \mathbb{F}_2D_{256} results in a memory allocation error. The memory allocated to GAP was 2000 megabytes. Appendix 7.2 gives the details of the commands that were run. However Theorem 2.3.11, gives a basis for the vector space of derivations of \mathbb{F}_2D_{256} . Thus it may be possible to use Theorem 2.2.5 to generate a basis for the derivation algebra of a group algebra in a computer algebra system like GAP [18] or SageMath [43]. Even if this is not feasible in general it seems likely to be possible for a selection of group algebras.

Section 2.3.3 exhibits well known extremal codes as the image of a derivation of a group algebra. Thus at least in certain cases derivations can be considered as generating good codes. However not much was known about derivations of finite group algebras of positive characteristic and so as a result this idea was not explored much within this thesis. However, the results contained within this thesis make exploring the idea of generating codes from derivations more accessible. This endeavour would benefit from the aforementioned algorithm for generating a basis for $Der(KG)$. Considering a derivation as generating a linear block code, the dimension of the ring of constants represents the redundancy of the code. Let $d_0, d_1, \dots, d_{n-1} \in Der(KG)$ for some group algebra KG and let f be a polynomial in n indeterminates. Then, the image of $f(d_0, d_1, \dots, d_n)$ can be considered as a code of length $|G|$ over K .

The results of Chapter 6 demonstrate that properties of the derivation algebras of group algebras can be very useful in gleaning information about the structure

of the group algebra itself. It has been shown that derivations can be used to distinguish between group algebras and also to give an alternative proof to the Modular Isomorphism Problem, for abelian groups. This gives a partial answer to Question 1.1. This question has not been explored fully. There have been developed within this thesis a number of invariants of a group algebra KG based on derivations.

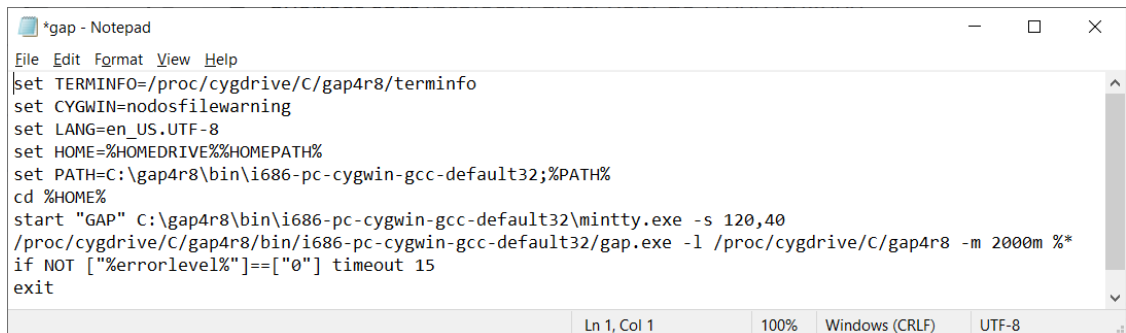
1. The number of derivations, $|Der(KG)|$
2. The maximum preperiod (period) of a derivation
3. The dimensions of the derivation Lie algebras in the derivation tower of KG
4. The center of the Lie algebra $Der(KG)$
5. The ring of constants, $\mathcal{C}(KG)$

This is not an exhaustive list and others may also prove useful. It would be very interesting to apply these and other invariants to the Modular Isomorphism Problem.

Appendix

Computing the Derivation Lie Algebra of $\mathbb{F}_2 D_{256}$

GAP version 4.8.6 was used to try to compute the derivation Lie algebra of $\mathbb{F}_2 D_{256}$. The .bat file was used to run the GAP program is shown in Figure 1. Note the command line argument `-m 2000m`. This allocates 2000 megabytes of memory to the process.



```
*gap - Notepad
File Edit Format View Help
set TERMINFO=/proc/cygdrive/C/gap4r8/terminfo
set CYGWIN=nodosfilewarning
set LANG=en_US.UTF-8
set HOME=%HOMEDRIVE%\%HOMEPATH%
set PATH=C:\gap4r8\bin\i686-pc-cygwin-gcc-default32;%PATH%
cd %HOME%
start "GAP" C:\gap4r8\bin\i686-pc-cygwin-gcc-default32\mintty.exe -s 120,40
/proc/cygdrive/C/gap4r8/bin/i686-pc-cygwin-gcc-default32/gap.exe -l /proc/cygdrive/C/gap4r8 -m 2000m %*
if NOT ["%errorlevel%"]==["0"] timeout 15
exit
```

Figure 1: The .bat used to run GAP

Figure 2 shows the commands that were run in the GAP console. The Small-Group(256, 539) is the Dihedral group of order 256. The group algebra $\mathbb{F}_2 D_{256}$ is then constructed using the function “GroupRing”. It is then attempted to construct the derivation Lie algebra $Der(\mathbb{F}_2 D_{256})$. However, an error occurs: “Error, reached the pre-set memory limit”. Note that a basis for $Der(\mathbb{F}_2 D_{256})$ is given in Theorem 2.3.11.

```

/proc/cygdrive/C/gap4r8/bin/i686-pc-cygwin-gcc-default32/gap.exe -l /proc/cygdrive/C/gap4r8 -m 2000m
GAP 4.8.6, 12-Nov-2016, build of 2016-11-12 16:12:02 (GMTST)
http://www.gap-system.org
Architecture: i686-pc-cygwin-gcc-default32
Libs used: gmp, readline
Loading the library and packages ...
Components: trans 1.0, prim 2.1, small* 1.0, id* 1.0
Packages:  AClib 1.2, Alnuth 3.0.0, AtlasRep 1.5.1, AutPGrp 1.6, Browse 1.8.6, CRISP 1.4.4, Cryst 4.1.12,
          CrystCat 1.1.6, CTbllib 1.2.2, FactInt 1.5.3, FGA 1.3.1, GAPDoc 1.5.1, IO 4.4.6, IRREDSOL 1.3.1,
          LAGUNA 3.7.0, Polenta 1.3.7, Polycyclic 2.11, RadRoot 2.7, ResClasses 4.5.0, Sophus 1.23, Spinsym 1.5,
          TomLib 1.2.6, Utils 0.43
Try '??help' for help. See also '?copyright', '?cite' and '?authors'
gap> structureDescription(SmallGroup(256,539));
"D256"
gap> KG := GroupRing(GF(2), SmallGroup(256,539));
<algebra-with-one over GF(2), with 8 generators>
gap> DerKG := Derivations(Basis(KG));
Error, reached the pre-set memory limit
(change it with the -o command line option) in
null[i] := ShallowCopy( row ); at /proc/cygdrive/C/gap4r8/lib/matrix.gi:3199 called from
NullMat( n ^ 2, n ^ 3, R ) at /proc/cygdrive/C/gap4r8/lib/alglie.gi:679 called from
<function "unknown">( <arguments> )
called from read-eval loop at line 3 of *stdin*
you can 'return;'
brk>

```

Figure 2: An attempt to calculate the derivation algebra of $\mathbb{F}_2 D_{256}$ using GAP.

Bibliography

- [1] Artemovych, Orest D., Bovdi, Victor A., and Salim, Mohamed A. “Derivations of group rings”. In: *Acta Sci. Math. (Szeged)* 86.1-2 (2020), pp. 51–72. ISSN: 0001-6969. DOI: 10.14232/actasm-019-664-x. URL: <https://doi.org/10.14232/actasm-019-664-x>.
- [2] Arutyunov, AA, Mishchenko, AS, and Shtern, AI. “Derivations of Group Algebras”. In: *arXiv preprint arXiv:1708.05005* (2017).
- [3] Ashraf, M, Ali, S, and Haetinger, C. “On Derivations in Rings and their Applications”. In: *The Aligarh Bulletin Of Maths* 25.2 (Jan. 2006), pp. 79–107.
- [4] Bagiński, Czesław. “Modular group algebras of 2-groups of maximal class”. In: *Communications in algebra* 20.5 (1992), pp. 1229–1241.
- [5] Bagiński, Czesław. “The isomorphism question for modular group algebras of metacyclic p -groups”. In: *Proceedings of the American Mathematical Society* 104.1 (1988), pp. 39–42.
- [6] Bagiński, Czesław. “On the isomorphism problem for modular group algebras of elementary abelian-by-cyclic p -groups”. In: *Colloquium Mathematicae*. Vol. 82. 1. 1999, pp. 125–136.

- [7] Bagiński, Czesław and Caranti, A. “The modular group algebras of p -groups of maximal class”. In: *Canadian Journal of Mathematics* 40.6 (1988), pp. 1422–1435.
- [8] Bagiński, Czesław and Konovalov, Alexander. “The modular isomorphism problem for finite p -groups with a cyclic subgroup of index p^2 ”. In: *arXiv preprint math/0607292* (2006).
- [9] Boucher, Delphine and Ulmer, Felix. “Linear codes using skew polynomials with automorphisms and derivations”. In: *Designs, codes and cryptography* 70.3 (2014), pp. 405–431.
- [10] Boulagouaz, M and Leroy, André. “(Sigma-Delta) Codes”. In: *arXiv preprint arXiv:1304.6518* (2013).
- [11] Carlson, Jon F. “Periodic modules over modular group algebras”. In: *Journal of the London Mathematical Society* 2.3 (1977), pp. 431–436.
- [12] Creedon, L. and Hughes, K. “Derivations on group algebras with coding theory applications”. In: *Finite Fields and Their Applications* 56 (2019), pp. 247–265. ISSN: 1071-5797. DOI: 10.1016/j.ffa.2018.11.005. URL: <http://www.sciencedirect.com/science/article/pii/S107157971830145X>.
- [13] Creedon, Leo and Gildea, Joe. “The structure of the unit group of the group algebra $F_2k D_8$ ”. In: *Canad. Math. Bull* 54.2 (2011), pp. 237–243.
- [14] Deskins, W.E. “Finite abelian groups with isomorphic group algebras”. In: *Duke Mathematical Journal* 23.1 (1956), pp. 35–40.
- [15] Drensky, Vesselin. “The isomorphism problem for modular group algebras of groups with large centres”. In: *Contemp. Math* 93 (1989), pp. 145–153.
- [16] Dummit, David S and Foote, Richard M. *Abstract Algebra*. 3rd ed. Wiley Hoboken, 2004. ISBN: 978-0-471-43334-7.

- [17] Ferrero, Miguel, Giambruno, Antonio, and Milies, César Polcino. “A note on derivations of group rings”. In: *Canadian Mathematical Bulletin* 38.4 (1995), pp. 434–437.
- [18] *GAP – Groups, Algorithms, and Programming, Version 4.9.2*. The GAP Group. 2018. URL: <https://www.gap-system.org>.
- [19] Ghahramani, Fereidoun, Runde, Volker, and Willis, George. “Derivations on group algebras”. In: *Proceedings of the London Mathematical Society* 80.2 (2000), pp. 360–390.
- [20] Godsil, Chris and Royle, Gordon F. *Algebraic graph theory*. Vol. 207. Springer Science & Business Media, 2013.
- [21] Grassl, Markus. *Bounds on the minimum distance of linear codes and quantum codes*. <http://www.codetables.de>. Accessed May 18, 2020.
- [22] Hefferon, Jim. *Linear Algebra*. 3rd ed. 2003. URL: <http://joshua.smcvt.edu/linearalgebra/book.pdf>.
- [23] Hernández Toledo, René A. “Linear finite dynamical systems”. In: *Communications in Algebra* 33.9 (2005), pp. 2977–2989.
- [24] Herstein, IN. “A note on derivations”. In: *Canad. Math. Bull* 21.3 (1978), pp. 369–370.
- [25] Hill, Raymond. *A first course in coding theory*. 1st ed. Oxford: Clarendon Pr., 1986. ISBN: 0198538030.
- [26] Houghten, Sheridan K. et al. “The extended quadratic residue code is the only (48, 24, 12) self-dual doubly-even code”. In: *IEEE Transactions on Information Theory* 49.1 (2003), pp. 53–59. ISSN: 00189448. DOI: 10.1109/TIT.2002.806146.
- [27] Hughes, G. “Structure theorems for group ring codes with an application to self-dual codes”. In: *Designs, Codes and Cryptography* 24.1 (2001), pp. 5–14.

- [28] Hurley, Paul and Hurley, Ted. “Codes from zero-divisors and units in group rings”. In: *International Journal of Information and Coding Theory* 1.1 (2009), pp. 57–87.
- [29] Hurley, Ted. “Group rings and rings of matrices”. In: *Int. J. Pure Appl. Math* 31.3 (2006), pp. 319–335.
- [30] Hurley, Ted, McEvoy, Paul, and Wenus, Jakub. “Algebraic constructions of LDPC codes with no short cycles”. In: *International Journal of Information and Coding Theory* 1.3 (2010), pp. 285–297.
- [31] Jacobson, Nathan. *Lie algebras*. 10. Courier Corporation, 1979.
- [32] Jordan, David A. “On the simplicity of Lie algebras of derivations of commutative algebras”. In: *Journal of Algebra* 228.2 (2000), pp. 580–585.
- [33] Lang, Serge. *Algebra, volume 211 of Graduate texts in mathematics*. Springer-Verlag, New York, 2002. ISBN: 038795385X.
- [34] Losert, Viktor. “The derivation problem for group algebras”. In: *Annals of Mathematics* 168.1 (2008), pp. 221–246. ISSN: 0003486X.
- [35] Luks, Eugene M. “Derivation towers of Lie algebras”. In: *Journal of Algebra* 61.1 (1979), pp. 281–288.
- [36] Mathieu, Martin and Villena, Armando R. “The structure of Lie derivations on C^* -algebras”. In: *Journal of Functional Analysis* 202.2 (2003), pp. 504–525.
- [37] Meng, Dao Ji. “Some results on complete Lie algebras”. In: *Communications in Algebra* 22.13 (1994), pp. 5457–5507.
- [38] Passman, Donald S. *The Algebraic Structure of Group Rings*. New York: Dover Publications, 2011. ISBN: 978-0-486-48206-4.

- [39] Passman, DS. “Simple Lie algebras of Witt type”. In: *Journal of Algebra* 206.2 (1998), pp. 682–692.
- [40] Polcino Milies, César and Sehgal, Sudarshan K. *An Introduction to Group Rings*. 1st ed. Springer Science & Business Media, 2002.
- [41] Posner, Edward C. “Derivations in prime rings”. In: *Proceedings of the American Mathematical Society* 8.6 (1957), pp. 1093–1100.
- [42] Rowen, Louis H. *Ring Theory*. Student Ed. London: Academic Press, 2012. ISBN: 0-12-599840-6.
- [43] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 7.5.1)*. <http://www.sagemath.org>. 2018.
- [44] Sakai, S. “Derivations of simple C*-algebras, II”. In: *Bull. Soc. Math. France* 99 (1971), pp. 259–263.
- [45] Sandling, Robert. “The isomorphism problem for group rings: a survey”. In: *Orders and their applications*. Springer, 1985, pp. 256–288.
- [46] Sandling, Robert. “The modular group algebra problem for metacyclic p -groups”. In: *Proceedings of the American Mathematical Society* 124.5 (1996), pp. 1347–1350.
- [47] Schenkman, Eugene. “A theory of subinvariant Lie algebras”. In: *American Journal of Mathematics* 73.2 (1951), pp. 453–474.
- [48] Sehgal, Sudarshan K. and Zassenhaus, Hans J. “Group Rings Without Non-trivial Idempotents”. In: *Archiv der Mathematik* 28 (1977), pp. 378–379. DOI: 10.1007/BF01223938.
- [49] Smith, Martha K. “Derivations of group algebras of finitely-generated, torsion-free, nilpotent groups”. In: *Houston J. Math.* 4.2 (1978), pp. 277–288.

- [50] Spiegel, Eugene. “Derivations of integral group rings”. In: *Communications in Algebra* 22.8 (1994), pp. 2955–2959.
- [51] Su, Yucai and Zhu, Linsheng. “Derivation algebras of centerless perfect Lie algebras are complete”. In: *Journal of Algebra* 285.2 (2005), pp. 508–515.
- [52] Weintraub, Steven H. *A Guide to Advanced Linear Algebra*. Washington DC: The Mathematical Association of America, 2014. ISBN: 9780883859674. DOI: 10.5948/UP09780883859674. URL: <http://universitypublishingonline.org/ref/id/maa/CB09780883859674>.