UNIVERSITY OF THE
WITWATERSRAND,
JOHANNESBURG

On Derivations of Group Algebras

by
Peter Williams
(2321672)

Dissertation
Submitted in fulfilment of the requirements for the degree
Master of Science
in
Mathematics
in the Faculty of Science, University of the Witwatersrand, Johannesburg, South Africa

Supervisor: Prof. Y. Hardy
June 2025

Declaration

I declare that this dissertation is my own, unaided work. It is being submitted for the Degree of Master of Science at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination at any other University.

Peter Williams

(Signature of candidate)

5th day of June 20 25 at Braamfontein

Contents

List of Figures

List of Symbols

$\mathbb{N}$: the set of all natural numbers, including 0
$\mathbb{Z}$: the set of all integers
G: a finitely generated group
$[u]$: the conjugacy class of an element u of a group R: a ring
$\mathbb{F}$: a field
$R[G]$: the group algebra of a group G over a commutative unital ring R
$\tilde{\phi}$: the extension of a group homomorphism ϕ to a homomorphism of group algebras
d_x: the inner derivation induced by x
X: the finitely generated free group algebra with generating set (x)
$u_{(k)}$: the k^{th} initial section of a word $u \in X$

Chapter 1

Introduction

1.1 Overview

The purpose of this research is to study derivations of group algebras. A group algebra is constructed using a group G and a commutative ring R: it is the unital R-algebra produced freely from G, preserving the multiplicative structure of G. The notion of a derivation is intended to generalise the classical derivative function: to this end, a derivation is defined to be any function satisfying linearity and the Leibniz Rule, however, the Leibniz Rule may differ somewhat depending on how we define the action of the domain on the codomain. We will be considering derivations whose domain and codomain are a group algebra, however, with two slightly different approaches to the Leibniz Rule, leading to apparently vastly different theories before concluding by showing a surprising similarity between these approaches in one particular regard.

In Chapter 1 we will go on to define algebraic concepts and related results that will be relevant for the dissertation. We will conclude by introducing derivations and group algebras, both defined in their broadest sense. We also define inner derivations, a particular type of derivation which will be very significant.

In Chapter 2 we demonstrate useful results relating to group algebras. We show that the underlying group and ring may be embedded in a group algebra and that there is a correspondence between normal subgroups of the underlying group and ideals of the group algebra. Moreover, we demonstrate many results pertaining to the derivations and inner derivations of a group algebra, leading us to introduce the outer derivations: the quotient space of the derivations by

the inner derivations. It is here that we introduce the two different types of derivation that we will be considering moving forward, namely the standard derivation and Fox-derivation.

We focus on Fox-derivations in Chapter 3, more specifically on Fox-derivations of group algebras with the underlying ring $\mathbb{Z}$. We further study the correspondence between normal subgroups of G and ideals of $\mathbb{Z}[G]$, leading us to show that an ideal may be generated using the generators of its corresponding normal subgroup. We then increase our focus to group algebras $\mathbb{Z}[X]$ where X is a finitely generated free group. Within this framework we construct a notion analogous to differentiation on such a group algebra: a Fox-derivativion is constructed for each generator x_j of X that acts as the partial derivative with respect to x_j. These partial derivatives are shown to form a basis for all derivations of $\mathbb{Z}[X]$ and lead to results analogous to those from traditional differentiation including a Chain Rule and Taylor series. We conclude by studying the structure of $\mathbb{Z}[X]$ using the partial derivatives, specifically by determining properties of the powers of its fundamental ideal, which are shown to be strongly related to the lower central series of X.

Chapter 4 is dedicated to reviewing category theory. A category contains of a class of objects and a class of morphisms between these objects, intended to provide a general theory of mathematical structures and their relations. After defining the core concepts of category theory, we focus on a specific type of category, namely the groupoid of the adjoint action on a group G, denoted by Γ, whose objects are the elements of G and whose morphisms represent the adjoint action on G. We define a function known as a character on such a category, which will prove very significant moving forward. We also introduce subgroupoids of the groupoid of the adjoint action.

We focus on the standard derivations of group algebras over $\mathbb{C}$ in Chapter 5. The most significant result here is that every such derivation can be described using a locally finitely supported character of the groupoid of the adjoint action on the underlying group. In fact, the vector space of derivations of $\mathbb{C}[G]$ is shown to be isomorphic to the vector space of locally finitely supported characters of Γ. Furthermore, the inner derivations can easily be described using characters as well. The structural similarities between the derivations and characters are further explored, leading us to study the characters of the subgroupoids of Γ. This eventually leads to introducing a type of derivation known as the central derivation, which is guaranteed to be non-inner if it

is non-trivial. We generate a vector space by the central derivations, which consists entirely of non-inner derivations and which can be embedded in the outer derivations. We conclude the chapter by considering which groups allow for the construction of central derivations of $\mathbb{C}[G]$.

After having studied the Fox-derivations of $\mathbb{Z}[X]$ and standard derivations of $\mathbb{C}[G]$ separately, we demonstrate a similarity between these two concepts in Chapter 6. This hinges on the notion of a cochain complex, a sequence of abelian groups or modules along with homomorphisms between them whose consecutive compositions are zero. We find that the Fox-derivations, inner Fox-derivations and outer Fox-derivations of $\mathbb{Z}[X]$ are isomorphic to the 1-dimensional cocyles, 1-dimensional coboundaries and first cohomology group of X over $\mathbb{Z}[X]$ respectively. Similarly, the standard derivations, inner derivations and outer derivations of $\mathbb{C}[G]$ are isomorphic to the 1-dimensional cocyles, 1-dimensional coboundaries and first cohomology group of the cochain complex of the Cayley complex of the groupoid of the adjoint on G respectively.

1.2 Introductory Definitions

We begin by defining several algebraic structures that will be relevant for this project, following [1] for Definitions 1 to 15 and following [6] for Definition 16.

Definition 1. *A **group** $(G, *)$ is a set G equipped with a binary operation $* : G \times G \to G$, satisfying the following properties:*

- ***Associativity:** For all $g, h, k \in G$, $g * (h * k) = (g * h) * k$.*
- ***Identity element:** There exists an identity element $e \in G$, that is an element such that $e * g = g = g * e$ for all $g \in G$. It is elementary to observe that this element is unique. For greater rigour we may denote the identity of the group G by e_G.*
- ***Inverses:** For every $g \in G$ there exists an inverse $g^{-1} \in G$ such that $g * g^{-1} = e_G = g^{-1} * g$.*

*We may also write 0_G or 1_G for the identity. (The subscript may be omitted if it is not necessary.) If this operation is also commutative, i.e. $g * h = h * g$ for all $g, h \in G$, then G is called an **abelian group**.*

For the sake of convenience we will generally simply write gh and G instead of $g * h$ and $(G, *)$ respectively.

Definition 2. *Given a group G, a subset $H \subseteq G$ is a **subgroup** of G, denoted $H \leq G$, if it is also a group under the same operation. H is a **normal subgroup**, denoted $H \trianglelefteq G$, if $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.*

Proposition 1. *If H is a non-empty subset of a group G, then H is a subgroup of G if and only if $gh^{-1} \in H$ for all $g, h \in H$.*

Definition 3. *For any normal subgroup $N \trianglelefteq G$, the **left coset** of N with respect to g is the set $gN = \{gn : n \in N\}$. The right coset is $Ng = \{ng : n \in N\}$.*

Note 1. *Seeing as we consider only normal subgroups in the above definition, it is elementary to show that left and right cosets are in fact equal. Therefore, we need only consider left cosets. Note also that for two elements $g, h \in G$, $gN = hN$ if and only if $gh^{-1} \in N$.*

Definition 4. *For any normal subgroup $N \trianglelefteq G$, the **quotient group** of N is the group G/N with elements given by $G/N = \{gN : g \in G\}$ and operation $gN * hN = (gh)N$. The identity of G/N is $e_G N = N$.*

Note 2. *It must be stated that the operation on the quotient group is indeed well-defined: if we have $g, g', h, h' \in G$ such that $gN = g'N$ and $hN = h'N$, then $(gh)(g'h')^{-1} \in N$, i.e. $(gh)N = (g'h')N$ and so $gN * hN = g'N * h'N$.*

Definition 5. *Given a group G, two elements $a, b \in G$ are **conjugate** if there exists some $g \in G$ such that $b = gag^{-1}$. (We can also write this as $b = a^g$.) This is an equivalence relation whose equivalence classes are called conjugacy classes. The conjugacy class of a is denoted by $[a]$.*

Definition 6. *A **ring** is an abelian group R under addition $+$ along with a multiplication operation $\cdot$ that satisfies the following properties:*

- ***Associativity:** For all $r, s, t \in R$, $r \cdot (s \cdot t) = (r \cdot s) \cdot t$.*
- ***Distributivity:** For all $r, s, t \in R$, $r \cdot (s + t) = r \cdot s + r \cdot t$ and $(r + s) \cdot t = r \cdot t + s \cdot t$.*

*We denote the additive identity element by 0. If there exists a multiplicative identity, then we denote this by 1 and R is called a **unital ring**. If multiplication is commutative, then R is a **commutative ring**. Subrings are defined analogously to subgroups.*

Definition 7. *The **characteristic** of a unital ring R is the smallest $n \in \mathbb{N}$*

such that:

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

We denote $\text{char}(R) = n$. *If no such* n *exists, then* $\text{char}(R) = 0$.

Definition 8. *Given a ring* R, *a subset* $I \subseteq R$ *is a* ***two-sided ideal*** *if* $0 \in I$, $x + y \in I$ *for all* $x, y \in I$ *and* $r \cdot x, x \cdot r \in I$ *for all* $r \in R$ *and* $x \in I$.

There are also weaker structures known as left and right ideals. When we refer simply to an ideal, we will mean a two-sided ideal.

Ideals may be equipped with a product. The product of two ideals I and J is:

$$IJ = \left\{ \sum_{i=1}^{n} x_i y_i : n \in \mathbb{N} \text{ and } x_i \in I, y_i \in J, \forall i \right\}.$$

The resulting IJ is itself an ideal. Furthermore, $IJ \subseteq I$ and $IJ \subseteq J$.

Definition 9. ***Quotient rings*** *can be formed similarly to quotient groups. For any two-sided ideal* I *of a ring* R, $R/I = \{r + I : r \in R\}$ *with operations* $(r + I) + (s + I) = (r + s) + I$ *and* $(r + I) \cdot (s + I) = (r \cdot s) + I$. *Similarly to quotient groups,* $r + I = s + I$ *if and only if* $r - s \in I$.

Note 3. *Again, it must be stated that the operations within the quotient ring are indeed well-defined. The addition of quotient rings is clearly well-defined following Note 2. Multiplication is also well-defined: if* $r, r', s, s' \in R$ *such that* $r + I = r' + I$ *and* $s + I = s' + I$, *then* $r \cdot s - r' \cdot s' \in I$ *and hence* $(r \cdot s) + I = (r' \cdot s') + I$, *meaning that* $(r + I) \cdot (s + I) = (r' + I) \cdot (s' + I)$.

Definition 10. *A* ***field*** *is a commutative unital ring where every non-zero element has a multiplicative inverse.*

Note 4. *The precise definition of a field differs somewhat between sources. Sometimes it is required for a field* $\mathbb{F}$ *that* $(\mathbb{F}\backslash\{0\}, \cdot)$ *is an abelian group. This excludes the one-element ring* $\{0\}$, *whereas Definition 10 does not.*

Definition 11. *Given a ring* R, *a* ***left R-module*** *is an abelian group* M *along with a left scalar multiplication operation over* R *that is associative and distributive, that is for all* $\alpha, \beta \in R$ *and* $a, b \in M$*:*

$$(\alpha \cdot \beta)a = \alpha(\beta a),$$
$$\alpha(a + b) = \alpha a + \alpha b,$$
$$(\alpha + \beta)a = \alpha a + \beta a.$$

Further, if R is a unital ring, then we require that for all $a \in M$:

$$1a = a.$$

*We say that R **acts** on M and that this scalar multiplication is an **R-action** on M.*

Right R-modules are defined similarly with right scalar multiplication. In the following, by "module" we will mean left module.

Definition 12. *Given two rings R and S, M is an **R-S-bimodule** if it is a left R-module and a right S-module such that the left- and right-actions associate, that is:*

$$(r \cdot_R m) \cdot_S s = r \cdot_R (m \cdot_S s)$$

for all $r \in R$, $m \in M$ and $s \in S$, where $\cdot_R$ and $\cdot_S$ are the R-action and S-action on M respectively.

Definition 13. *If R is a field in Definition 11, then M is a **vector space**.*

Definition 14. *An **algebra** A over a ring R is an R-module along with a multiplication operator $\cdot$ which is associative, distributive and commutative with scalar multiplication, that is for all $\alpha \in R$ and $a, b, c \in A$:*

$$\begin{aligned}(a \cdot b) \cdot c &= a \cdot (b \cdot c),\\ a \cdot (\alpha b + c) &= \alpha(a \cdot b) + (a \cdot c),\\ (\alpha a + b) \cdot c &= \alpha(a \cdot c) + (b \cdot c).\end{aligned}$$

Note 5. *Any algebra is also a ring.*

Definition 15. *Given a vector space or algebra V over R, a **basis** B is a linearly independent subset of V such that B spans V. Explicitly, this means that all elements of V can be represented as a finite linear combination of elements of B, using elements from R as coefficients.*

Definition 16. *A **Lie algebra** L over a field $\mathbb{F}$ is a vector space over $\mathbb{F}$ along with a Lie bracket (or Lie product) $[\cdot, \cdot]$ satisfying the following properties:*

- ***Bilinearity:*** *$[\alpha a + b, c] = \alpha[a, c] + [b, c]$ and $[a, \alpha b + c] = \alpha[a, b] + [a, c]$ for all $\alpha \in \mathbb{F}$ and $a, b, c \in L$.*
- ***Antisymmetry:*** *$[a, b] = -[b, a]$ for all $a, b \in L$.*

- ***Jacobi Identity:*** $[a,[b,c]]+[b,[c,a]]+[c,[a,b]]=0$ *for all* $a,b,c \in L$.

Definition 17. *Given a Lie algebra* L*, a sub-vector space* $I \subseteq L$ *is an* ***ideal*** *if* $[x,y] \in I$ *for all* $x \in I$ *and* $y \in L$.

Having defined these many algebraic structures, we introduce some particular types of mapping within these structures capturing the notion of linearity within these general structures, again following [1]:

Definition 18. *Given groups* G *and* H*, a mapping* $f : G \to H$ *is a* ***group homomorphism*** *if* $f(gh) = f(g)f(h)$ *for all* $g,h \in G$*, using the group operation of* G *on the left-hand side and the operation of* H *on the right.*

Definition 19. *Given rings* R *and* S*, a mapping* $f : R \to S$ *is a* ***ring homomorphism*** *if* $f(r+s) = f(r)+f(s)$ *and* $f(r \cdot s) = f(r) \cdot f(s)$ *for all* $r,s \in R$.

Definition 20. *Given* R*-modules* M *and* N*, a mapping* $f : M \to N$ *is a* ***module homomorphism*** *if* $f(m+n) = f(m)+f(n)$ *and* $f(rm) = rf(m)$ *for all* $m,n \in M$ *and* $r \in R$.

A similar definition can be made for algebra homomorphisms. Note that in any structure the mapping sending everything to 0 is a homomorphism. This is called the trivial homomorphism.

Definition 21. *A homomorphism of any structure is an* ***isomorphism*** *if it is a bijection. If an isomorphism exists between two structures* A *and* B*, then they are said to be* ***isomorphic****, denoted* $A \cong B$*. An isomorphism from a structure to itself is called an* ***automorphism****.*

Note 6. *For any structure as described in Definitions 1 to 14, the identity mapping is an automorphism, meaning that every structure is isomorphic to itself.*

Note 7. *The composition of homomorphisms is itself a homomorphism and the same holds for isomorphisms. Therefore, the relation of being isomorphic is transitive, meaning that if* $A \cong B$ *and* $B \cong C$*, then* $A \cong C$.

Definition 22. *When considering structures that have a zero element, the* ***kernel*** *of a mapping is the set of all elements mapped to zero. In the case of a mapping* $\phi : G \to H$ *between groups the kernel is given by* $\ker(\phi) = \{g \in G : \phi(g) = e_H\}$*. When considering structures with addition and multiplication, the kernel of* $\phi : R \to S$ *is* $\ker(\phi) = \{r \in R : \phi(r) = 0_S\}$.

The study of homomorphisms is the study of structure because they preserve structure between their domains and codomains. This means that if $f : G \to H$ is a group homomorphism, then $f(e_G) = e_H$ and $f(g^{-1}) = (f(g))^{-1}$ for all $g \in G$. Similarly, if $f : R \to S$ is a ring homomorphism, then $f(0_R) = 0_S$ and $f(-r) = -f(r)$ for all $r \in R$. Moreover, if R and S are both unital and f is surjective, then $f(1_R) = 1_S$ and $f\left(r^{-1}\right) = (f(r))^{-1}$ for all $r \in R$ such that r^{-1} exists in R. Similar results exist for all the relevant structures.

Furthermore, isomorphisms preserve structure and guarantee equal cardinality. For this reason, isomorphic structures can in a sense be considered equivalent.

Lastly, we obtain the following useful result, again taken from [1]:

Theorem 1. *The kernel of any group homomorphism $f : G \to H$ is a normal subgroup of G and conversely every normal subgroup of G is the kernel of some such homomorphism. Similarly, the kernel of any ring homomorphism $f : R \to S$ is a two-sided ideal of R and conversely every two-sided ideal of R is the kernel of some such homomorphism.*

The proof of this theorem is straightforward. The group homomorphism ϕ such that a normal subgroup is its kernel is $\phi : G \to G/N$ defined by $\phi(g) = gN$ for all $g \in G$. Similarly for two-sided ideals, the ring homomorphism φ is given by $\varphi(r) = r + I$.

Having introduced homomorphisms, a type of mapping analogous to linear maps, we now define another type of mapping, this time generalising differentiation in a more general setting. For this we must consider an algebra A over some ring R along with an A-bimodule (i.e. an A-A-bimodule) E. We will denote the left-action on E by $\cdot$ and the right-action on E by $\times$. Then, from [11]:

Definition 23. *A **derivation** from A to E is a group homomorphism $d : A \to E$ obeying the Leibniz Rule. That is, for all $a, b \in A$:*

$$\begin{aligned} d(a+b) &= d(a) + d(b), \\ d(ab) &= d(a) \times b + a \cdot d(b). \end{aligned}$$

If A has a multiplicative identity element, then we further require that d be a module homomorphism, that is for any $\alpha \in R$ and $a \in A$:

$$d(\alpha a) = \alpha 1 \cdot d(a).$$

While we have been very specific in requiring d to be a group or module homomorphism, these are both intended to capture the idea of linearity within their respective contexts. Therefore, we may say that d is a linear mapping obeying the Leibniz Rule.

Note 8. *For any derivation d, $d(0) = 0$. Further, if the domain has a multiplicative identity element, then $d(1) = 0$.*

Definition 24. *For all $x \in E$, we define the mapping $d_x : A \to E$ as follows:*

$$d_x(a) = x \times a - a \cdot x \qquad \forall a \in A.$$

*A mapping defined like this will always be a derivation and is called an **inner derivation**.*

This approach to defining derivations generally follows the introduction to [3]. The most usual way of considering derivations, though, is to let $E = A$, that is to consider derivations as mappings $d : A \to A$. Indeed, we will only be considering this case: whenever we refer to a derivation in the following, unless specifically stated otherwise, we will be referring to a mapping with the same domain and codomain. Further, the most common approach within this framework is to define the left- and right-actions of A on itself to simply be its native multiplication, that is $a \cdot b = ab = a \times b$ for all $a, b \in A$. Under this framework, the Leibniz Rule becomes:

$$d(ab) = d(a)b + ad(b) \tag{1.1}$$

and the definition of inner derivations becomes:

$$d_a(b) = ab - ba. \tag{1.2}$$

This is an intuitive way of defining the left- and right-actions. We will in part follow this approach, however, not entirely. There is another intuitive way of defining the actions of A on itself, utilising homomorphisms.

Given two ring homomorphisms $f, g : A \to A$, we can define $a \cdot b = f(a)b$ and $a \times b = ag(b)$ for $a, b \in A$. Then $\cdot$ and $\times$ are indeed actions on A, meaning that the Leibniz Rule becomes:

$$d(ab) = d(a)g(b) + f(a)d(b) \tag{1.3}$$

and the definition of inner derivations becomes:

$$d_a(b) = ag(b) - f(b)a. \tag{1.4}$$

In fact, the earlier approach of simply defining the actions to be multiplication can be seen as following this homomorphism approach, using the identity mapping for both homomorphisms. This way of defining the actions utilising homomorphisms will be crucial moving forward in this research, specifically for introducing what we call "Fox-derivations".

While all above working considered the structures with no restrictions, for the remaining purposes of this research, when discussing groups we focus only on finitely generated discrete groups:[1] these are groups G with discrete elements and a finite generating set $S \subset G$ such that all elements of G can be represented as finite combinations (under the group operation) of elements from S and their inverses. This leads to the focus of this research, the group algebra:

Definition 25. *Given a finitely generated group G and a commutative ring R, the **group algebra** of G is denoted $R[G]$ and consists of all finitely supported functions $f : G \to R$. Explicitly, this means that the set $\{g \in G : f(g) \neq 0\}$ is finite. Addition and multiplication of $f_1, f_2 \in R[G]$ are defined as follows:*

$$\begin{aligned}(f_1 + f_2)(g) &= f_1(g) + f_2(g) \quad \forall g \in G \\ (f_1 \cdot f_2)(g) &= \sum_{h \in G} f_1\left(gh^{-1}\right) f_2(h) \quad \forall g \in G.\end{aligned}$$

Definition 25 is the most precise definition of group algebras, however, there is an equivalent formulation which is more commonly used, representing the elements of the group algebra as linear combinations. This is the formulation we will be using throughout the dissertation:

Definition 26. *Given a finitely generated group G and a commutative ring R, the **group algebra** of G over R is denoted $R[G]$ and consists of all formal finite linear combinations $\sum_{g \in G} a_g g$, where $a_g \in R$ for all $g \in G$. Addition and multiplication are defined as follows:*

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g)\, g,$$

[1] By discrete group, we mean a group with a discrete topology.

$$\left(\sum_{g\in G} a_g g\right)\cdot\left(\sum_{g\in G} b_g g\right)=\sum_{g\in G}\left(\sum_{h\in G} a_{gh^{-1}}b_h\right)g,$$

using addition and multiplication from R respectively.

Note 9. *When we refer to "finite linear combinations" in the above definition, this means that $a_g \neq 0_R$ for only a finite number of $g \in G$. Any term with coefficient 0_R can be disregarded within the sum.*

These two definitions are equivalent: Definition 26 is merely representing the function $f \in R[G]$ as $\sum_{g\in G} f(g)g$.

Note 10. *If we relax R in Definitions 25 and 26 to be a ring without demanding commutativity, then $R[G]$ is known as a* ***group ring****.*

Note 11. *Though the definition of the group algebra does not demand that the ring R be unital, we will only be considering the case of a commutative unital ring.*

The above definition is from [7], however, multiplication in the group algebra is defined slightly differently in [4]: $\left(\sum_{g\in G} a_g g\right)\cdot\left(\sum_{g\in G} b_g g\right)=\sum_{g,h\in G}(a_g b_h)gh$, using multiplication from R and the group operation as needed on the right-hand side. These are equivalent definitions via the substituion $g = gh^{-1}$:

$$\sum_{g\in G}\sum_{h\in G}(a_g b_h)gh=\sum_{g\in G}\sum_{h\in G}(a_{gh^{-1}}b_h)\left(gh^{-1}\right)h=\sum_{g\in G}\left(\sum_{h\in G} a_{gh^{-1}}b_h\right)g.$$

The formulation of multiplication from [4] is perhaps more intuitive, however, it is not as explicit in expressing the product as an element of the group algebra. These definitions will both be used, depending on the task at hand.

Chapter 2

Review of Group Algebras

We consider an arbitrary group algebra $R[G]$. The ring R and group G can be embedded into $R[G]$ by identifying $r = r1_G$ for each $r \in R$ and $g = 1_R g$ for each $g \in G$, where 0_R and 1_R are the identity elements of R and 1_G is identity in G. Addition and multiplication in R correspond with addition and multiplication in $R[G]$ and the group operation in G corresponds with multiplication in G. That is:

$$r1_G + s1_G = (r+s)1_G, \tag{2.1}$$

$$(r1_G) \cdot (s1_G) = (rs)1_G, \tag{2.2}$$

$$(1_R g) \cdot (1_R h) = 1_R(gh). \tag{2.3}$$

for all $r, s \in R$ and $g, h \in G$.

Equation (2.1) is immediate by Definition (26). Equation (2.2) and (2.3) require more elaboration. We will show the working for (2.2) only to demonstrate the reasoning behind such results:

We can write $r1_G = \sum_{g \in G} a_g g$ where $a_{1_G} = r$ and $a_g = 0_R$ otherwise. Similarly, $s1_G = \sum_{g \in G} b_g g$ where $b_{1_G} = s$ and $b_g = 0_R$ otherwise. Thus, following Definition 26, multiplication in $R[G]$ yields:

$$(r1_G) \cdot (s1_G) = \sum_{g \in G} \left(\sum_{h \in G} a_{gh^{-1}} b_h \right) g.$$

But $a_{gh^{-1}}$ is non-zero only if $gh^{-1} = 1_G$, that is if $h = g$. Similarly, b_g is

non-zero only if $g = 1_G$. So:

$$\begin{aligned}(r1_G) \cdot (s1_G) &= \sum_{g \in G} \left(\sum_{h \in G} a_{gh^{-1}} b_h \right) g \\ &= \sum_{g \in G} (a_{1_G} b_g)\, g \\ &= (a_{1_G} b_{1_G})\, 1_G \\ &= (rs) 1_G.\end{aligned}$$

Equation (2.3) can be proved similarly. Since R and G can be embedded so effectively, we will henceforth consider them to be subsets of $R[G]$.

Proposition 2. *The group algebra is an algebra over R with scalar multiplication given by $r \sum_{g \in G} a_g g = \sum_{g \in G} (r a_g)\, g$. The additive identity element of RG is given by 0_R and multiplicative identity is given by 1_G.*

This means that addition in the group algebra is commutative and associative and multiplication is associative, distributive and commutative with scalar multiplication. The proof for this is very straightforward.

Note 12. *The group G is a basis of $R[G]$. Since G is chosen to be finitely generated, it is countable and can therefore be enumerated: $G = \{g_1, g_2, ...\}$ is a useful way of expressing the basis of RG. We will use the convention that $g_1 = e_G$.*

Note 13. *Using the embeddings mentioned before, R is a subalgebra of $R[G]$ and G is a multiplicative group in $R[G]$.*

We can obtain several results regarding addition and multiplication in the group algebra that are convenient for later work:

Lemma 1. *For all $r \in R$, $h \in G$ and $\sum_{g \in G} a_g g \in R[G]$, the following equations hold:*

$$\begin{aligned}r \cdot \sum_{g \in G} a_g g &= \sum_{g \in G} (r a_g)\, g, \\ h \cdot \sum_{g \in G} a_g g &= \sum_{g \in G} a_g (hg),\end{aligned}$$

as do the analogous equations multiplying r and h on the right rather than the left.

This lemma helps in demonstrating the following proposition, which will be-

come useful when we introduce derivations and start including functions within the sums in $R[G]$.

Note 14. *The first equation of the following proposition follows from the adjunction between sets and R-modules, which is a special case of the adjunction discussed in greater detail in Note 16.*

Proposition 3. *For any functions $\phi, \psi : G \to R[G]$:*

$$\sum_{g\in G} a_g \cdot \phi(g) + \sum_{g\in G} b_g \cdot \phi(g) = \sum_{g\in G} (a_g + b_g) \cdot \phi(g) \qquad \textit{and}$$
$$\left(\sum_{g\in G} a_g \cdot \phi(g)\right) \cdot \left(\sum_{g\in G} b_g \cdot \psi(g)\right) = \sum_{g,h\in G} (a_g b_h) \cdot (\phi(g) \cdot \psi(h)).$$

The proof of Proposition 3 is not entirely trivial, however, it is exceedingly tedious and requires little in-depth thought. For this reason it is included in Appendix A rather than the body of the dissertation.

We can now move on to considering derivations on the group algebra. We will begin by considering the most natural type of derivation as discussed in the introduction, that is we will be following Equations (1.1) and (1.2). We denote by $\mathrm{Der}(R[G])$ the set of all such derivations on the group algebra and by $\mathrm{Inn}(R[G])$ the set of all such inner derivations.

We define addition and scalar multiplication of derivations pointwise, that is for any $d, d' \in \mathrm{Der}(R[G])$ and $r \in R$:

$$(d + d')(u) = d(u) + d'(u) \quad \text{and} \quad (rd)(u) = rd(u) \qquad \forall u \in R[G].$$

Proposition 4. *Using the above addition and scalar multiplication,* $\mathrm{Der}(R[G])$ *is an R-module.*

The proof of Proposition 4 is straightforward using the trivial mapping as the additive identity element of $\mathrm{Der}(R[G])$ and with the additive inverse of a derivation d being given by $(-d)(u) = -d(u), \forall u \in R[G]$. Using this additive inverse we introduce the following Lie bracket of derivations d, d':

$$[d, d'] = d \circ d' - d' \circ d.$$

With this Lie bracket in mind, we find the following:

Proposition 5. *If* $\mathbb{F}$ *is a field and* A *is an algebra over* $\mathbb{F}$*, then* $\mathrm{Der}(A)$ *is a Lie algebra over* $\mathbb{F}$*.*

Proposition 6. *If* $\mathbb{F}$ *is a field and* A *is an algebra over* $\mathbb{F}$*, then* $\mathrm{Inn}(A)$ *is an ideal of* $\mathrm{Der}(A)$*.*

Again, the proof of Proposition 5 is very straightforward: using pointwise addition and scalar multiplication, it is trivial to demonstrate that $\mathrm{Der}(A)$ is a vector space over $\mathbb{F}$ and that our Lie bracket functions as in Definition 16. Proposition 6 is not quite so obvious:

Proof of Proposition 6. Firstly, it is easy to see that $d_0 = 0$ and hence that $0 \in \mathrm{Inn}(A)$. Now, for any $d_a, d_b \in \mathrm{Inn}(A)$, we have that for each $u \in A$:

$$\begin{aligned}(d_a + d_b)(u) &= a \cdot u - u \cdot a + b \cdot u - u \cdot b \\ &= (a+b) \cdot u - u \cdot (a+b) \\ &= d_{a+b}(u)\end{aligned}$$

and hence $d_a + d_b = d_{a+b} \in \mathrm{Inn}(A)$.

Now, it remains only to show that for any $d_a \in \mathrm{Inn}(A)$ and $d \in \mathrm{Der}(A)$, $[d_a, d] \in \mathrm{Inn}(A)$. Given such a d_a and d, for each $u \in A$:

$$\begin{aligned}[d_a, d](u) &= (d_a \circ d - d \circ d_a)(u) \\ &= d_a(d(u)) - d(d_a(u)) \\ &= a \cdot d(u) - d(u) \cdot a - d(a \cdot u - u \cdot a) \\ &= a \cdot d(u) - d(u) \cdot a - d(a) \cdot u - a \cdot d(u) + d(u) \cdot a + u \cdot d(a) \\ &= -d(a) \cdot u + u \cdot d(a) \\ &= d_{-d(a)}(u)\end{aligned}$$

and so $[d_a, d] = d_{-d(a)} \in \mathrm{Inn}(\mathbb{F}[G])$. □

Since $\mathbb{F}(G)$ is an algebra over $\mathbb{F}$ for any field $\mathbb{F}$, we obtain the following corollaries to Propositions 5 and 6:

Corollary 1. *If* $\mathbb{F}$ *is a field, then* $\mathrm{Der}(\mathbb{F}[G])$ *is a Lie algebra over* $\mathbb{F}$*.*

Corollary 2. *If* $\mathbb{F}$ *is a field, then* $\mathrm{Inn}(\mathbb{F}[G])$ *is an ideal of* $\mathrm{Der}(\mathbb{F}[G])$*.*

Seeing as the inner derivations form an ideal of the Lie algebra of all derivations in this case, we can introduce the following concept:

Definition 27. *The Lie algebra of* ***outer derivations*** *of the algebra* $\mathbb{F}[G]$ *is given by the quotient algebra* $\mathrm{Out}(\mathbb{F}[G]) := \mathrm{Der}(\mathbb{F}[G])/\mathrm{Inn}(\mathbb{F}[G])$.

Lastly, it is interesting to observe that some properties from the underlying group can be transferred to the group algebra, as is seen in the following result from [7]:

Theorem 2. *If* ϕ *is a group homomorphism from group* G *to group* H*, then for any commutative unital ring* R *we can extend* ϕ *by linearity to an algebra homomorphism* $\tilde{\phi} : R[G] \to R[H]$ *such that* $\tilde{\phi}(1_R g) = \phi(g)$ *for all* $g \in G$.

By "extend ϕ by linearity", we mean $\tilde{\phi}\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g \phi(g)$. With that clarified, the proof of this theorem is trivial.

Note 15. *Given any group homomorphism* $\phi : G \to H$*, the linear extension* $\tilde{\phi} : R[G] \to R[H]$ *leaves all elements of the ring* R *unchanged, that is* $\tilde{\phi}(r) = r$ *for all* $r \in R$.

Note 16. *The map* $\phi \mapsto \tilde{\phi}$ *is an adjunction* $\mathrm{Hom}(F(G), X) \cong \mathrm{Hom}(G, U(X))$ *where* G *is any group,* X *is any* R*-algebra,* F *is the functor mapping any group* G *to the free unital* R*-algebra over* G *preserving multiplication from* G *and any group homomorphism* $f : G \to H$ *to* $\tilde{f} : F(G) \to F(H)$ *and* U *is the functor mapping any* R*-algebra* X *to the group of its invertible elements and any* R*-algebra homomorphism* $f : X \to Y$ *to* $f|_{U(X)} : U(X) \to U(Y)$*. Theorem 2 can be derived from this fact, however, this strays from the focus of this dissertation and we therefore judge it unnecessary to explore this in depth.*

As described in [7], this allows us to associate normal subgroups with ideals of the group algebra as follows: every normal subgroup N of a group G is the kernel of some group homomorphism $\phi : G \to H$. But the kernel of $\tilde{\phi} : R[G] \to R[H]$ is also a two-sided ideal of $R[G]$. This establishes a correspondence between two-sided ideals of the group algebra and normal subgroups of the underlying group. Explicitly, $N \trianglelefteq G$ **corresponds** with the ideal $\ker\left(\tilde{\phi}\right)$ where ϕ is the group homomorphism such that $N = \ker(\phi)$.

Moreover, each two-sided ideal I of $R[G]$ **determines** a normal subgroup of G. This subgroup is identified by way of the ring homomorphism ψ such that $I = \ker(\psi)$. Concretely, this homomorphism is $\psi : R[G] \to R[G]/I$ given by $\psi(u) = u + I$ for all $u \in R[G]$. I determines the normal subgroup:

$$N_\psi = \{g \in G : \psi(g) = 1 + I\}.$$

However, for any $g \in G$:

$$\psi(g) = 1 + I \Leftrightarrow g + I = 1 + I \Leftrightarrow g - 1 \in I$$

and so we equivalently say:

$$N_\psi = \{g \in G : g - 1 \in I\}.$$

It is straightforward to show that this is indeed a normal subgroup using Proposition 1 and the properties of ideals.

Note 17. *This result can also be seen as a consequence of the fact that every ideal is a pullback and the right adjoint functor U from Note 16 preserves pullbacks, meaning that $U(I)$ is normal in $U(R[G])$ for any ideal I.*

2.1 Fox-Derivations

This matter of extending mappings by linearity also leads us to a slightly different notion of derivations than that used above. We will be introducing the Fox-derivation, as seen in [7]. Here we follow the approach seen in Equations (1.3) and (1.4). For our left-action we use the identity mapping as our homomorphism. For our right action we use the trivial mapping on G, denoted by $o : G \to G$, extended by linearity to $R[G]$: $\tilde{o}\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g$ since $o(g) = 1_G$. The derivation induced by these two actions leads us to the following definition:

Definition 28. *A **Fox-derivation** is any linear operator $d : R[G] \to R[G]$ such that:*

$$d(u \cdot v) = d(u) \cdot \tilde{o}(v) + u \cdot d(v). \tag{2.4}$$

Equation (1.4) becomes the following:

Definition 29. *For any $u \in R[G]$, we define the mapping $d_u : R[G] \to R[G]$ as follows:*

$$d_u(v) = u \cdot \tilde{o}(v) - v \cdot u \qquad \forall v \in R[G].$$

*Then d_u is a Fox-derivation. We call the Fox-derivations of this type **inner Fox-derivations**.*

This notion of derivations leads to similar results to Corollaries 1 and 2:

Proposition 7. *The set* $\mathrm{FDer}(R[G])$ *of all Fox-derivations over $R[G]$ is a right*

$R[G]$-module with addition of derivations and scalar multiplication defined by:

$$(d + d')(u) = d(u) + d'(u),$$
$$(dv)(u) = d(u) \cdot v$$

for all $R[G]$, given any $d, d' \in \mathrm{FDer}(R[G])$ and $v \in R[G]$.

Proposition 8. *The set $\mathrm{FInn}(R[G])$ of all inner Fox-derivations over $R[G]$ is a submodule of $\mathrm{FDer}(R[G])$.*

These are similarly easy to verify.

Definition 30. *Given the significance of the trivial mapping o for Fox-derivations, the kernel of its linear extension is known as the **fundamental ideal**. Explicitly, this is given by:*

$$O = \ker(\tilde{o}) = \left\{ \sum_{g \in G} a_g g \in R[G] : \sum_{g \in G} a_g = 0 \right\}.$$

Chapter 3

Fox-Derivations

Here we follow the approach to derivations of the group algebra as set out by Ralph H. Fox. This means that we will here be working with Fox-derivations as described in Section 2.1. Furthermore, we will be focusing not on group algebras generally, but more specifically on group algebras over $\mathbb{Z}$.

Immediately this leads to some useful identities:

Proposition 9. *For any Fox-derivation d of $\mathbb{Z}[G]$:*

(i) $d(x) = 0$ *for all* $x \in \mathbb{Z}$,

(ii) $d\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g d(g)$,

(iii) $d(u_1 \cdot u_2 \cdots u_n) = \sum_{i=1}^{n} \left(\prod_{j=1}^{i-1} u_j\right) \cdot d(u_i) \cdot \left(\prod_{j=i+1}^{n} \tilde{o}(u_j)\right)$,

(iv) $d(g^{-1}) = -g^{-1}d(g)$ *for all* $g \in G$.

Proof. (i) Firstly, $d(0) = d(0+0) = d(0) + d(0)$ and so $d(0) = 0$. Further, $d(1) = d(1 \cdot 1) = d(1) + 1 \cdot d(1) = d(1) + d(1)$ and so $d(1) = 0$. Now consider $x \in \mathbb{Z}$ such that $x > 1$. Then $x = \underbrace{1 + 1 + \cdots + 1}_{x \text{ times}}$ and so:

$$d(x) = \underbrace{d(1) + d(1) + \cdots + d(1)}_{x \text{ times}} = 0 + 0 + \cdots + 0 = 0.$$

Lastly, if $x \in \mathbb{Z}$ and $x < 0$, then $0 = d(0) = d(-x + x) = d(-x) + d(x) = 0 + d(x) = d(x)$.

(ii) This is an immediate consequence of d being a linear operator.

(iii) We use induction here. Firstly, if $n = 1$, then $d(u_1) = d(u_1)$ obviously, satisfying the equation. Now suppose that the claim holds for arbitrary $n \in \mathbb{N}$. Then:

$$\begin{aligned} d(u_1 \cdots u_{n+1}) &= d(u_1 \cdots u_n) \cdot \tilde{o}(u_{n+1}) + u_1 \cdots u_n \cdot d(u_{n+1}) \\ &= \sum_{i=1}^{n} \left(\prod_{j=1}^{i-1} u_j \right) \cdot d(u_i) \cdot \left(\prod_{j=i+1}^{n} \tilde{o}(u_j) \right) \cdot \tilde{o}(u_{n+1}) \\ &\quad + u_1 \cdots u_n \cdot d(u_{n+1}) \\ &= \sum_{i=1}^{n} \left(\prod_{j=1}^{i-1} u_j \right) \cdot d(u_i) \cdot \left(\prod_{j=i+1}^{n+1} \tilde{o}(u_j) \right) + \prod_{j=1}^{n} u_j \cdot d(u_{n+1}) \\ &= \sum_{i=1}^{n+1} \left(\prod_{j=1}^{i-1} u_j \right) \cdot d(u_i) \cdot \left(\prod_{j=i+1}^{n+1} \right). \end{aligned}$$

(iv) For any $g \in G$, $0 = d(1) = d(g^{-1} \cdot g) = d(g^{-1}) + g^{-1} \cdot d(g)$ and so $d(g^{-1}) = -g^{-1}d(g)$. □

Further, we obtain the following result, which will prove important when connecting Fox-derivations to the other notion of derivations we will consider:

Proposition 10. *The Fox-derivations of $\mathbb{Z}[G]$ are in fact simply the crossed homomorphisms from G to $\mathbb{Z}[G]$, i.e. the mappings $d : G \to \mathbb{Z}[G]$ such that $d(gh) = d(g) + g \cdot d(h)$ for all $g, h \in G$, extended by linearity to $\mathbb{Z}[G]$.*

Proof. Given a crossed homomorphism d from G to $\mathbb{Z}[G]$, the linear extension to $\mathbb{Z}[G]$ will have the following properties for any $\sum_{g\in G} a_g g, \sum_{g\in G} b_g g \in R[G]$, using Proposition 3:

$$\begin{aligned} \tilde{d}\left(\sum_{g\in G} a_g g + \sum_{g\in G} b_g g \right) &= \tilde{d}\left(\sum_{g\in G} (a_g + b_g) g \right) \\ &= \sum_{g\in G} (a_g + b_g) d(g) \\ &= \sum_{g\in G} a_g d(g) + \sum_{g\in G} b_g d(g) \\ &= \tilde{d}\left(\sum_{g\in G} a_g g \right) + \tilde{d}\left(\sum_{g\in G} b_g g \right) \end{aligned}$$

and:

$$\begin{aligned}
&\tilde{d}\left(\left(\sum_{g\in G} a_g g\right)\cdot\left(\sum_{g\in G} b_g g\right)\right)\\
&= \tilde{d}\left(\sum_{g,h\in G}(a_g b_h)gh\right)\\
&= \sum_{g,h\in G}(a_g b_h)d(gh)\\
&= \sum_{g,h\in G}(a_g b_h)(d(g)+gd(h))\\
&= \sum_{g,h\in G}(a_g b_h)d(g)+\sum_{g,h\in G}(a_g b_h)gd(h)\\
&= \left(\sum_{g\in G} a_g d(g)\right)\cdot\left(\sum_{g\in G} b_g\right)+\left(\sum_{g\in G} a_g g\right)\cdot\left(\sum_{g\in G} b_g d(g)\right)\\
&= \tilde{d}\left(\sum_{g\in G} a_g g\right)\cdot\tilde{o}\left(\sum_{g\in G} b_g g\right)+\left(\sum_{g\in G} a_g g\right)\cdot\tilde{d}\left(\sum_{g\in G} b_g g\right).
\end{aligned}$$

Therefore, $\tilde{d}$ is a Fox-derivation.

Conversely, consider a Fox-derivation d. Then for any $g, h \in G$, $d(gh) = d(g)\cdot o(h) + g\cdot d(h) = d(g) + g\cdot d(h)$. Thus, $d|_G$ is a crossed homomorphism from G to $\mathbb{Z}[G]$. Furthermore, Proposition 9(ii) tells us that d is the unique linear extension of $d|_G$. □

3.1 Normal Subgroups and Ideals

Recall that two-sided ideals of the group algebra determine normal subgroups of the underlying group. This gives us a connection between the structure of the group algebra and the group regardless of our ring, however, working with $\mathbb{Z}[G]$ gives us a stronger connection:

Proposition 11. *The ideal I of $\mathbb{Z}[G]$ that corresponds to a normal subgroup $N \trianglelefteq G$ determines N and is the smallest ideal of $\mathbb{Z}[G]$ that determines N.*

This result is given without proof in [7]. We find that the proof is not obvious and therefore present it as follows:

Proof. Let $N = \ker(\phi)$, where $\phi : G \to H$ is a group homomorphism. Then $I = \ker\left(\tilde{\phi}\right)$ corresponds to N.

First, we will show that I determines N. Let $g \in N$ and consider $\psi : \mathbb{Z}[G] \to \mathbb{Z}[G]/I$ as defined earlier. Then $\tilde{\phi}(g) = 1$ in $\mathbb{Z}[H]$ and so $\tilde{\phi}(1-g) = \tilde{\phi}(1) - \tilde{\phi}(g) = 1 - 1 = 0$. Thus, $1 - g \in I$, i.e. $g + I = 1 + I$. Therefore, $\psi(g) = 1 + I$. By the same logic, $\psi(h) \neq 1 + I$ for any $h \in G \backslash N$. Thereby, $N = \{g \in G : \psi(g) = 1 + I\} = N_\psi$, meaning that I determines N. This concludes the first part of the proof, meaning that it remains only to show that I is the smallest ideal determining N.

Now consider M, an ideal of $\mathbb{Z}[G]$ that determines N. Then, the canonical map $\varphi : \mathbb{Z}[G] \to \mathbb{Z}[G]/M$ is an algebra homomorphism such that $M = \ker(\varphi)$ and $N = \{g \in G : \varphi(g) = 1 + M\}$. Furthermore, the image $\varphi|_G(G)$ of the restriction $\varphi|_G : G \to \mathbb{Z}[G]/M$ is a multiplicative group, meaning that we can write N as the multiplicative group kernel $N = \ker(\varphi|_G)$. Now, there exists a group homomorphism α such that the following diagram commutes:

$$\begin{array}{ccc} G & \xrightarrow{\phi} & \phi(G) \cong G/N \\ & \searrow^{\varphi|_G} & \downarrow \alpha \\ & & \varphi|_G(G) \cong G/N \end{array}$$

Now let $\sum_{g \in G} a_g g \in I = \ker\left(\tilde{\phi}\right)$. Note here that each a_g is an integer. Therefore, for any $a_g > 0$, $a_g = \underbrace{1 + 1 + \cdots + 1}_{a_g \text{ times}}$ and so $\varphi(a_g) = \varphi(\underbrace{1 + 1 + \cdots + 1}_{a_g \text{ times}}) = \varphi(1) + \varphi(1) + \cdots + \varphi(1) = 1 + 1 + \cdots + 1 = a_g$ since φ is a homomorphism. Similarly, $\varphi(a_g) = a_g$ for any $a_g \leq 0$. Thus:

$$\begin{aligned} \varphi\left(\sum_{g \in G} a_g g\right) &= \sum_{g \in G} \varphi(a_g)\varphi(g) \\ &= \sum_{g \in G} a_g \alpha(\phi(g)) \\ &= \tilde{\alpha}\left(\sum_{g \in G} a_g \phi(g)\right) \\ &= \tilde{\alpha}\left(\tilde{\phi}\left(\sum_{g \in G} a_g g\right)\right) \\ &= \tilde{\alpha}(0) = 0 \end{aligned}$$

since $\tilde{\alpha}$ is a ring homomorphism. Thus, $I = \ker\left(\tilde{\phi}\right) \subseteq \ker(\varphi) = M$. This demonstrates that I is a subset of every ideal that determines N, i.e. it is the

smallest ideal determining N. □

Remembering that we are considering only finitely generated groups, if a normal subgroup $N \trianglelefteq G$ is finitely generated, then the generators determine the correpsonding ideal I as explained in the following result:

Proposition 12. *Consider a normal subgroup $N \trianglelefteq G$ with corresponding ideal $I \subseteq \mathbb{Z}[G]$. If N is finitely generated by $n_1, n_2, ..., n_m \in N \backslash \{1\}$, then I is generated by $n_1 - 1, n_2 - 1, ..., n_m - 1$.*

For the proof of Proposition 12 we will require the following lemma:

Lemma 2. *If $N \trianglelefteq G$ is finitely generated by $n_1, n_2, ..., n_m \in N \backslash \{1\}$, then for every $n \in N$, we can express $n - 1$ as a linear combination of $n_1 - 1, n_2 - 1, ..., n_m - 1$, that is:*

$$n - 1 = \sum_{k=1}^{l} u_k \cdot (n_{j_k} - 1) \cdot v_k$$

where $j_k \in \{1, 2, ..., m\}$ and $u_k, v_k \in \mathbb{Z}[G]$ for each k.

Proof. We will prove the lemma by induction on the length of n. Firstly, if n has length 0, then $n = 1$. Hence, $n - 1 = 0$, which is the empty sum and hence a linear combination of $n_1 - 1, ..., n_m - 1$. Further, if n has length 1, then $n = n_j$ or $n = n_j^{-1}$, where $j \in \{1, 2, ..., m\}$. If $n = n_j$, then $n - 1 = n_j - 1$ is a linear combination as required. Alternatively, if $n = n_j^{-1}$, then:

$$n - 1 = n_j^{-1} - 1 = -n_j^{-1} \cdot (n_j - 1)$$

is a linear combination. Hence, the statement holds for all $n \in N$ of lengths 0 and 1.

Now assume that the lemma holds for all elements of N of length $0, 1, ..., l$ and consider $n \in N$ of length $l + 1$. Then $n = n_j^{\epsilon} n'$ where n_j is a generator of N, $\epsilon \in \{-1, 1\}$ and $n' \in N$ has length l. By assumption, we can express $n' - 1$ as:

$$n' - 1 = \prod_{k=1}^{l} u_k \cdot (n_{j_k} - 1) \cdot v_k.$$

where for each k, $j_k \in \{1, ..., m\}$ and $u_k, v_k \in \mathbb{Z}[G]$. Consequently:

$$n - 1 = n_j^{\epsilon} n' - 1$$

$$= n_j^\epsilon - 1 + n_j^\epsilon \cdot (n' - 1)$$
$$= n_j^\epsilon - 1 + \sum_{k=1}^{l} (n_j^\epsilon u_k) \cdot (n_{j_k} - 1) \cdot v_k$$

which is the sum of two linear combinations as required, i.e. a linear combination itself. □

Proof of Proposition 12. Let $N = \ker(\phi)$ where $\phi : G \to H$ is a group homomorphism, so that $I = \ker\left(\tilde{\phi}\right)$.

Furthermore, we introduce the ideal I_N generated by $n_1 - 1, n_2 - 1, ..., n_m - 1$, namely:

$$I_N = \left\{ \sum_{k=1}^{l} u_k \cdot (n_{j_k} - 1) \cdot v_k : l \in \mathbb{N} \text{ and } j_k \in \{1, 2, ..., m\}, u_k, v_k \in \mathbb{Z}[G] \forall k \right\}.$$

Our proof will be complete when we have shown that $I = I_N$. First, consider $\sum_{k=1}^{l} u_k \cdot (n_{j_k} - 1) \cdot v_k \in I_N$. Then:

$$\tilde{\phi}\left(\sum_{k=1}^{l} u_k \cdot (n_{j_k} - 1) \cdot v_k \right) = \sum_{k=1}^{l} \tilde{\phi}(u_k) \cdot \tilde{\phi}(n_{j_k} - 1) \cdot \tilde{\phi}(v_k)$$

but $\phi(n_{j_k}) = 1$ always since $N = \ker(\phi)$ and so $\tilde{\phi}(n_{j_k} - 1) = 0$. Hence:

$$\tilde{\phi}\left(\sum_{k=1}^{l} u_k \cdot (n_{j_k} - 1) \cdot v_k \right) = \sum_{k=1}^{l} \tilde{\phi}(u_k) \cdot 0 \cdot \tilde{\phi}(v_k)$$
$$= 0.$$

Therefore, $\sum_{k=1}^{l} u_k \cdot (n_{j_k} - 1) \cdot v_k \in \ker\left(\tilde{\phi}\right) = I$. We can conclude from this that $I_N \subseteq I$.

Now consider $\sum_{g \in G} a_g g \in I$. Then $\sum_{g \in G} a_g \phi(g) = 0$. For each $h \in H$ we will consider $\phi^{-1}(h)$, the preimage of h, to be the set of all $g \in G$ such that $\phi(g) = h$. Then for any $h \in H$, $\sum_{g \in \phi^{-1}(h)} a_g \phi(g) = 0$ and so $\sum_{g \in \phi^{-1}(h)} a_g = 0$.

Set $h \in H$ and $g_h \in G$ such that $\phi(g_h) = h$. Then:

$$\sum_{g \in \phi^{-1}(h)} a_g g = \sum_{g \in \phi^{-1}(h)} a_g \left(g g_h^{-1} - 1 \right) g_h + \sum_{g \in \phi^{-1}(h)} a_g g_h$$
$$= \sum_{g \in \phi^{-1}(h)} a_g \left(g g_h^{-1} - 1 \right) g_h.$$

Furthermore, for any $g \in \phi^{-1}(h)$, $\phi\left(gg_h^{-1}\right) = hh^{-1} = 1$, i.e. $gg_h^{-1} \in N$. By Lemma 2, $gg_h^{-1} - 1$ is a linear combination of $n_1 - 1, ..., n_m - 1$. Combining all of this:

$$\begin{aligned}\sum_{g\in G} a_g g &= \sum_{h\in H}\left(\sum_{g\in\phi^{-1}(h)} a_g\left(gg_h^{-1}-1\right)g_h\right)\\ &= \sum_{h\in H}\left(\sum_{g\in\phi^{-1}(h)} a_g\left(\sum_{k_g=1}^{l_g} u_{k_g}\cdot\left(n_{j_{k_g}}-1\right)\cdot v_{k_g}\right)g_h\right)\\ &= \sum_{g\in G}\sum_{k_g=1}^{l_g}\left(a_g u_{k_g}\right)\cdot\left(n_{j_{k_g}}-1\right)\cdot\left(v_{k_g}g_{\phi(g)}\right)\end{aligned}$$

which is clearly a linear combination of $n_1 - 1, n_2 - 1, ..., n_m - 1$. Hence, $\sum_{g\in G} a_g g \in I_N$. We conclude that $I \subseteq I_N$ and consequently $I = I_N$. □

With these structural properties of group algebras over $\mathbb{Z}$ established, we can move to an even more particular type of group algebra, namely the primary focus of Fox's research.

3.2 Fox-Derivations of Free Group Algebras

In the introduction of [7], Fox describes various connections between derivations of free group algebras and other contemporary branches of algebra: Reidemeister homotopy chains, Magnus series expansions and Eilenberg-Mac Lane cohomology. Each of these fields centres on concepts that can be described by way of free differentiation, leading Fox to conclude that "free differentiation is the fundamental tool for the study of groups defined by operators and relations." Free differentiation refers to the operations that emulate traditional differentiation utilising Fox-derivations. Many results with this constructed differentiation are remarkably similar to results from traditional differentiation. We will outline and expand upon his findings on free differentiation and explain its connection to some of the concepts mentioned above. To understand these connections, though, we must first give a brief summary of the relevant elements of these notions.

3.2.1 Magnus Series Expansions

Firstly, it is important to understand what a finitely generated free group is:

Definition 31. *A **finitely generated free group** X has a finite set of generators $(x) = \{x_1, x_2, ..., x_m\}$, from which all elements are constructed. Each element $u \in X$ is a possibly empty word formed from generators and their inverses, that is we can write $u = \prod_{k=1}^{l} x_{j_k}^{\epsilon_k}$, where for all k, $j_k \in \{1, 2, ..., m\}$, $\epsilon_k \in \{-1, 1\}$ and $\epsilon_k \neq \epsilon_{k+1}$ whenever $j_k = j_{k+1}$. The **length** of u is l. For each generator $x_j \in (x)$, we say that the **x_j-length** of u is $l_j(u) = \sum_{j_k=j} |\epsilon_k|$, that is the number of instances of x_j in u.*

It is easy to see that this is indeed a group. The identity element of such a free group X is given by the empty word, which we can denote by 1. Note that neither Fox in [7] nor Magnus in [10] require that all groups be finitely generated and so in these papers the generating set (x) may be infinite. Our choice to consider only finitely generated sets does not make substantial differences to most results, however, it does allow for additional results and for simpler proofs on some occasions.

Note 18. *The introduction of free groups provides some insight into why group algebras over $\mathbb{Z}$ are of such interest: for any group G, $\mathbb{Z}[G]$ is the free abelian group over G. Free abelian groups are defined very similarly to finitely generated free groups, however, without the restriction that the underlying group (in this case G) be finite and using commutative addition to construct our elements rather than multiplication as in Definition 31. With this mind, it is trivial to observe that $\mathbb{Z}[G]$ is the free abelian group over G.*

Note 19. *Throughout the remainder of this chapter we will assume that all group algebras considered have an underlying group which is a finitely generated free group.*

Magnus uses the free group X and wishes to represent all elements of X using a free ring R. This ring is constructed as follows: for each $x_j \in (x)$ we set $s_j = x_j - 1 \in R$. We can apply addition and multiplication akin to that of a group algebra over X for $s_1, s_2, ..., s_m$.

Definition 32. *R consists of all functions $f : P \to \mathbb{Z}$, where $P = \{1, P_1, P_2...\}$ is a fixed set containing 1 and all words formed from $\{s_1, s_2, ..., s_m\}$ and their inverses, as defined in Definition 31. Addition and multiplication of $f_1, f_2 \in R$ are defined as follows:*

$$(f_1 + f_2)(p) = f_1(p) + f_2(p) \qquad \forall p \in P,$$
$$(f_1 \cdot f_2)(p) = \sum_{q \in P} f_1\left(pq^{-1}\right) f_2(q) \qquad \forall p \in P.$$

Similarly to Definition 25, we have defined the elements of the Magnus ring as functions. However, similarly to that case we can also equivalently represent these functions as linear combinations. In [10], Magnus represents the ring R as all linear combinations of the form:

$$n_0 1 + \sum_{k=1}^{\infty} n_k P_k$$

where $n_k \in \mathbb{Z}$ for $k = 0, 1, 2, ...$ and $\{P_1, P_2, ...\}$ is a fixed set containing all words formed from $\{s_1, s_2, ..., s_m\}$ and their inverses. This is essentially a manner of writing a function $f : P \to \mathbb{Z}$ from Definition 32 as $\sum_{p \in P} f(p)p$. Addition and multiplication follow equivalently to those in Definition 32. We will primarily be using the representation of the Magnus ring as linear combinations.

It is immediately obvious that R is extremely similar to the group algebra $\mathbb{Z}[X]$. There are two differences between these rings: firstly, $\mathbb{Z}[X]$ uses words formed from $\{x_1, x_2, ...\}$ and its inverses, whereas R uses $\{s_1, s_2, ...\}$; secondly, R allows for infinite sums.

We can represent each $u \in X$ using elements from R. Firstly, for $x_j \in (x)$, $x_j = 1 + s_j$ obviously and $x_j^{-1} = \sum_{n=0}^{\infty} (-1)^n s_j^n$, since formally:

$$\begin{aligned}(1 + s_j) \cdot \sum_{n=0}^{\infty} (-1)^n s_j^n &= \sum_{n=0}^{\infty} (-1)^n s_j^n + \sum_{n=0}^{\infty} (-1)^n s_j^{n+1} \\ &= (1 - s_j + s_j^2 - s_j^3 + \cdots) + (s_j - s_j^2 + s_j^3 + \cdots) \\ &= 1.\end{aligned}$$

Rather than observing that all non-1 terms are cancelled in the above sum, we can also use the function representation as in Definition 32. Then $x_j = 1 + s_j$ and $\sum_{n=0}^{\infty} (-1)^n s_j^n$ can be respectively represented by the functions $f_1, f_2 : P \to \mathbb{Z}$ with:

$$f_1(p) = \begin{cases} 1 & p = 1 \text{ or } p = s_j \\ 0 & \text{otherwise,} \end{cases}$$

$$f_2(p) = \begin{cases} (-1)^n & p = s_j^n \ \exists n \in \mathbb{N} \\ 0 & \text{otherwise.} \end{cases}$$

Then $(f_1 \cdot f_2)(1) = \sum_{q \in P} f_1(q^{-1}) f_2(q) = f_1(1) f_2(1) = 1$ since $f_1(q^{-1}) = 0$ or

$f_2(q) = 0$ for all $q \neq 1$. If $p = s_j^n$ for some $n > 0$, then:

$$\begin{aligned}(f_1 \cdot f_2)(p) &= \sum_{q \in P} f_1\left(pq^{-1}\right) f_2(q) \\ &= \sum_{m=0}^{\infty} f_1\left(ps_j^{-m}\right) f_2\left(s_j^m\right) \\ &= \sum_{m=0}^{n} (-1)^m f_1\left(s_j^{n-m}\right) \\ &= \sum_{m=n-1}^{n} (-1)^m \\ &= 0.\end{aligned}$$

Clearly, if $p \neq s_j^n$ for any $n \in \mathbb{N}$, then $(f_1 \cdot f_2)(p) = 0$. Thus:

$$(f_1 \cdot f_2)(p) = \begin{cases} 1 & p = 1 \\ 0 & p \neq 1. \end{cases}$$

Translating this back to the formal sum representation of the Magnus Ring, $(1+s_j)\cdot\sum_{n=0}^{\infty}(-1)^n s_j^n = 1$, i.e. $x_j^{-1} = (1+s_j)^{-1} = \sum_{n=0}^{\infty}(-1)^n s_j^n$. This demonstrates that we obtain the same results using functions and linear combinations. We have thus found representations in the Magnus Ring for generators and their inverses. For more involved free elements, we require the binomial coefficients, defined as follows:

Definition 33. *For two integers n and $k \geq 0$, the **binomial coefficient** $\binom{n}{k}$ is given by:*

$$\binom{n}{k} = \begin{cases} \dfrac{n!}{k!(n-k)!} & 0 \leq k \leq n \\ 0 & 0 \leq n < k \\ (-1)^k \dbinom{k-n-1}{k} & n < 0. \end{cases}$$

We will not be considering the case that $k < 0$.

Now consider an arbitrary free element with only one generator, that is $u = x_j^{\alpha}$ for some $\alpha \in \mathbb{Z}$. Then, using well-known combinatorial results, if $\alpha \geq 0$:

$$u = (1 + s_j)^{\alpha} = \sum_{n=0}^{\alpha} \binom{\alpha}{n} s_j^n = \sum_{n=0}^{\infty} \binom{\alpha}{n} s_j^n$$

and if $\alpha < 0$:

$$\begin{aligned}
u &= \left((1+s_j)^{-1}\right)^{|\alpha|} \\
&= \left(\sum_{n=0}^{\infty}(-1)^n s_j^n\right)^{|\alpha|} \\
&= \sum_{n=0}^{\infty}\left(\sum_{\substack{m_1,\ldots,m_{|\alpha|}=0 \\ m_1+\cdots+m_{|\alpha|}=n}} 1\right)(-1)^n s_j^n \\
&= \sum_{n=0}^{\infty}\binom{n+|\alpha|-1}{|\alpha|-1}(-1)^n s_j^n \\
&= \sum_{n=0}^{\infty}(-1)^n\binom{n-\alpha-1}{n}s_j^n \\
&= \sum_{n=0}^{\infty}\binom{\alpha}{n}s_j^n.
\end{aligned}$$

This tells us how to represent a free element with only one generator. We may now generalise to represent an arbitrary free element in this manner. Consider $u = x_i^{\alpha}x_j^{\beta}\cdots x_k^{\gamma}$. Then:

$$u = \left(\sum_{n=0}^{\infty}\binom{\alpha}{n}s_i^n\right)\left(\sum_{n=0}^{\infty}\binom{\beta}{n}s_j^n\right)\cdots\left(\sum_{n=0}^{\infty}\binom{\gamma}{n}s_k^n\right),$$

which can be simplified as:

$$u = \sum_{n_\alpha,n_\beta,\ldots,n_\gamma=0}^{\infty}\binom{\alpha}{n_\alpha}\binom{\beta}{n_\beta}\binom{\gamma}{n_\gamma}s_i^{n_\alpha}s_j^{n_\beta}\cdots s_k^{n_\gamma}. \tag{3.1}$$

3.2.2 First-Order Derivatives

For the remainder of this chapter we will focus squarely on the free group algebra $\mathbb{Z}[X]$, that is the group algebra of the finitely generated free group X over $\mathbb{Z}$. Fox describes the elements of $\mathbb{Z}[X]$ as "free polynomials", representing them as functions $f(x)$ of the generating set (x) in [7]. We judge this as a fairly misleading representation, though, since these elements are not actually functions of (x). This is, however, simply using the formulation from Definition 25, referring to group algebra elements as functions $f : X \to \mathbb{Z}$. As stated in Section 1.2, this is an equivalent formulation and so we may refer to the function f and the linear combination $\sum_{g\in G} f(g)g$ interchangeably. Also note

that, given a "free polynomial" $f(x)$, the paper refers repeatedly to $f(1)$, the function "evaluated at the point $x = 1$." This is also a fairly misleading convention as it is actually an entirely different element to $f(x)$. The precise description of this concept would be that, given a function $f : X \to \mathbb{Z}$, we consider $\tilde{o}\left(\sum_{g\in G} f(g)g\right)$. Clearly, though, this is a very clumsy notation. To avoid clumsiness we will simply refer to elements $f \in \mathbb{Z}[X]$ and we will refer to $\tilde{o}(f)$ as $f(1)$ when convenient.

With this notation in mind, we denote the fundamental ideal $\ker(\tilde{o})$ of $\mathbb{Z}[X]$ by Q. Explicitly:

$$Q = \left\{ \sum_{u\in X} a_u u \in \mathbb{Z}[X] : \sum_{u\in X} a_u = 0 \right\} = \{f \in \mathbb{Z}[X] : f(1) = 0\}.$$

Seeing as group algebra elements can be seen as functions from X to $\mathbb{Z}$, we construct an operation similar to differentiation for these functions:

Theorem 3. *To each generator x_j of X there corresponds a Fox-derivation $\frac{\partial}{\partial x_j}$ of $\mathbb{Z}[X]$, known as the **derivative with respect to x_j**, with the property:*

$$\frac{\partial}{\partial x_j}(x_k) = \delta_{jk}.$$

For any $f \in \mathbb{Z}[X]$, the partial derivative with respect to generator x_j will be $\frac{\partial}{\partial x_j}(f)$. For convenience we will simply write $\frac{\partial f}{\partial x_j}$. We will later introduce higher-order partial derivatives, so we may refer to the mappings described above as first-order derivatives.

Proof. For each $x_j \in (x)$, we define $\frac{\partial}{\partial x_j}$ inductively on $\mathbb{Z}[X]$. Firstly we set $\frac{\partial}{\partial x_j}(1) = 0$. Next, for any $x_k \in (x)$, set $\frac{\partial x_k}{\partial x_j} = \delta_{jk}$ and $\frac{\partial}{\partial x_j}\left(x_k^{-1}\right) = -x_k^{-1}\delta_{jk}$. Then for any $u, v \in X$, define $\frac{\partial}{\partial x_j}(uv) = \frac{\partial u}{\partial x_j} + u\frac{\partial v}{\partial x_j}$. It is obvious that the sum arising from this last equation must be finite and is therefore an element of $\mathbb{Z}[X]$.

We simply extend this $\frac{\partial}{\partial x_j}$ linearly over $\mathbb{Z}[X]$. Clearly, this will be a Fox-derivation as shown in Proposition 10. □

We assumed here that the free group has finitely many generators, unlike Fox in [7]. For that reason, we obtain the following result not present in that paper:

Theorem 4. *The partial derivatives form a basis for the $\mathbb{Z}$-module* $\mathrm{FDer}(\mathbb{Z}[X])$

of all Fox-derivations over the free group algebra.

Proof. We must show that every derivation is a linear combination of partial derivatives, that is for all $d \in \mathrm{FDer}(\mathbb{Z}[X])$:

$$d = \sum_{x_j \in (x)} \frac{\partial}{\partial x_j} u_j$$

where $u_j \in \mathbb{Z}[X]$ for all j.

Let $d \in \mathrm{FDer}(\mathbb{Z}[X])$ and set $D = \sum_{x_j \in (x)} \frac{\partial}{\partial x_j} d(x_j)$. Clearly, D is a finite linear combination of partial derivatives and is hence itself a Fox-derivation. First, we will show by induction on the length of words in X that $d - D = 0$ on X. Firstly, $d(1) = 0$ and $D(1) = 0$ since both are Fox-derivations. Now, for any generator $x_k \in (x)$:

$$\begin{aligned}
(d - D)(x_k) &= d(x_k) - \sum_{x_j \in (x)} \frac{\partial x_k}{\partial x_j} \cdot d(x_j) \\
&= d(x_k) - \sum_{x_j \in (x)} \delta_{jk} d(x_j) \\
&= d(x_k) - d(x_k) \\
&= 0.
\end{aligned}$$

Furthermore, by Proposition 9(iv):

$$(d - D)\left(x_k^{-1}\right) = -x_k^{-1}(d - D)(x_k) = 0.$$

Thus, $(d - D)(u) = 0$ for any $u \in X$ of length 0 or 1.

Now assume that $(d - D)(u) = 0$ for all $u \in X$ of length less than or equal to n for some $n \in \mathbb{N}$. Let $u \in \mathbb{Z}[X]$ have length $n + 1$. Then we can write $u = \prod_{k=1}^{n+1} x_{j_k}^{\epsilon_k}$. Therefore:

$$\begin{aligned}
(d - D)(u) &= (d - D)\left(\left(\prod_{k=1}^{n} x_{j_k}^{\epsilon_k}\right) \cdot x_{j_{n+1}}^{\epsilon_{n+1}}\right) \\
&= (d - D)\left(\prod_{k=1}^{n} x_{j_k}^{\epsilon_k}\right) + \prod_{k=1}^{n} x_{j_k}^{\epsilon_k} \cdot (d - D)\left(x_{j_{n+1}}^{\epsilon_{n+1}}\right) \\
&= 0 + \prod_{k=1}^{n} x_{j_k}^{\epsilon_k} \cdot 0 = 0
\end{aligned}$$

by the induction hypothesis. Thus, $(d-D)(u)=0$ for all $u \in X$ by induction on the length of u.

Now consider $f \in \mathbb{Z}[X]$. Then we can write $f = \sum_{u \in X} a_u u$. Thus, by Proposition 9(ii):

$$(d-D)(f) = \sum_{u \in X} a_u (d-D)(u) = \sum_{u \in X} a_u \cdot 0 = 0.$$

Thus, $(d-D)(f)=0$ for all $f \in \mathbb{Z}[X]$, i.e. $d=D$.

We have shown that every Fox-derivation is a linear combination of partial derivatives, however, we cannot yet conclude that the partial derivatives constitute a basis of the Fox-derivations. We must also show that any two distinct linear combinations result in distinct mappings, i.e.:

$$\sum_{x_j \in (x)} \frac{\partial}{\partial x_j} u_j = \sum_{x_j \in (x)} \frac{\partial}{\partial x_j} v_j \quad \Rightarrow \quad u_j = v_j \quad \forall x_j \in (x).$$

This is very easy to prove: for all $x_k \in (x)$, $\left(\sum_{x_j \in (x)} \frac{\partial}{\partial x_j} \cdot u_j\right)(x_k) = u_k$ and $\left(\sum_{x_j \in (x)} \frac{\partial}{\partial x_j} \cdot v_j\right)(x_k) = v_k$. So, if $\sum_{x_j \in (x)} \frac{\partial}{\partial x_j} \cdot u_j = \sum_{x_j \in (x)} \frac{\partial}{\partial x_j} \cdot v_j$, then $u_k = v_k$ for all $x_k \in (x)$.

Thus, we conclude that the partial derivatives constitute a basis of $\mathrm{FDer}(\mathbb{Z}[X])$. □

This result relies on the finiteness of our generating set (x) since we require that $D = \sum_{x_j \in (x)} \frac{\partial}{\partial x_j} d(x_j)$ is a finite sum in order to assume that it is a Fox-derivation. This is not guaranteed unless (x) is finite.

Having shown how significant the partial derivatives are to the whole set of derivations, it will be useful to describe the partial derivatives of arbitrary elements. Given how well we know the structure of the finitely generated free group X, it will be straightforward to describe the derivatives of free group elements: given any $u \in X$ and $x_j \in (x)$, we can write u in the following manner:

$$u = u_0 x_j^{p_1} u_1 x_j^{p_2} \cdots u_{q-1} x_j^{p_q} u_q$$

where $p_1, ..., p_q \in \mathbb{Z} \backslash \{0\}$ and $u_0, ..., u_q$ do not contain any instances of x_j. If u does not contain any instances of x_j itself, then $q=0$ and we simply have $u = u_0$. If u is simply a power of x_j, then $q=1$ and $u_0 = u_1 = 1$. We can use

Proposition 9 to help us differentiate this product:

$$\frac{\partial u}{\partial x_j} = \sum_{i=1}^{q} u_0 x_j^{p_1} u_1 \cdots \frac{\partial}{\partial x_j}\left(x_j^{p_i} u_i\right). \tag{3.2}$$

Now, $\frac{\partial}{\partial x_j}\left(x_j^{p_i} u_i\right) = \frac{\partial\left(x_j^{p_i}\right)}{\partial x_j} + x_j^{p_i}\frac{\partial u_i}{\partial x_j}$. But $\frac{\partial u_i}{\partial x_j} = 0$ since u does not contain any instances of x_j. So $\frac{\partial}{\partial x_j}\left(x_j^{p_i} u_i\right) = \frac{\partial\left(x_j^{p_i}\right)}{\partial x_j}$. We must now determine the derivative with respect to x_j of a power of x_j. Consider x_j^p where $p > 0$. Then, again using Proposition 9:

$$\begin{aligned}\frac{\partial\left(x_j^p\right)}{\partial x_j} &= \sum_{i=1}^{p} x_j^{i-1}\frac{\partial x_j}{\partial x_j} = \sum_{i=1}^{p} x_j^{i-1} \\ &= 1 + x_j + x_j^2 + \cdots + x_j^{p-1} \\ &= \frac{x_j^p - 1}{x_j - 1}.\end{aligned}$$

This fraction is not necessarily a formal element of $\mathbb{Z}[X]$, since $x_j - 1$ may not be multiplicatively invertible. This expression is an abuse of notation representing $1 + x_j + \cdots + x_j^{p-1}$, utilising the fact that $\left(1 + x_j + \cdots + x_j^{p-1}\right)\cdot(x_j - 1) = x_j^p - 1$. Now consider the case that $p < 0$. Then, by Proposition 9:

$$\begin{aligned}\frac{\partial\left(x_j^p\right)}{\partial x_j} &= -x_j^p \cdot \frac{\partial\left(x_j^{-p}\right)}{\partial x_j} = -x_j^p \cdot \frac{x_j^{-p} - 1}{x_j - 1} \\ &= \frac{x_j^p - 1}{x_j - 1}.\end{aligned}$$

Note that for negative p, $\frac{x_j^p - 1}{x_j - 1} = -x_j^p - x_j^{p+1} - \cdots - x_j^{-1}$. Thus, Equation (3.2) becomes:

$$\frac{\partial u}{\partial x_j} = \sum_{i=1}^{q} u_0 x_j^{p_1} u_1 \cdots u_{i-1}\frac{x_j^{p_i} - 1}{x_j - 1}. \tag{3.3}$$

This offers a very usable equation for determining partial derivatives of free group elements, however, there may be a more instructive description of these derivatives, utilising the initial sections of u:

Definition 34. *The* $\boldsymbol{k^{th}}$ ***initial section*** *of* $u = \prod_{i=1}^{l} x_{j_i}^{\epsilon_i}$*, denoted* $u_{(k)}$*, is given by* $\prod_{i=1}^{k-1} x_{j_i}^{\epsilon_i}$ *if* $\epsilon_k = 1$ *and it is given by* $\prod_{i=1}^{k} x_{j_i}^{\epsilon_i}$ *if* $\epsilon_k = -1$*. Formally:*

$$u_{(k)} = \left(\prod_{i=1}^{k-1} x_{j_i}^{\epsilon_i}\right) x_{j_k}^{\frac{\epsilon_k - 1}{2}}.$$

Now, returning to Proposition 9, we can write $\frac{\partial u}{\partial x_j}$ as follows:

$$\frac{\partial u}{\partial x_j} = \sum_{i=1}^{l} x_{j_1}^{\epsilon_1} \cdots x_{j_{i-1}}^{\epsilon_{i-1}} \frac{\partial \left(x_{j_i}^{\epsilon_i}\right)}{\partial x_j}.$$

Clearly, for any i such that $j_i \neq j$, the term in the sum will go to zero since $\frac{\partial x_{j_i}}{\partial x_j} = \frac{\partial \left(x_{j_i}^{-1}\right)}{\partial x_j} = 0$. Therefore, we need only consider the indices i such that $j_i = j$. So:

$$\frac{\partial u}{\partial x_j} = \sum_{j_i=j} x_{j_1}^{\epsilon_1} \cdots x_{j_{i-1}}^{\epsilon_{i-1}} \frac{\partial \left(x_{j_i}^{\epsilon_i}\right)}{\partial x_j}.$$

Whenever $j_i = j$, $\frac{\partial x_{j_i}}{\partial x_j} = 1$ and $\frac{\partial \left(x_{j_i}^{-1}\right)}{\partial x_j} = -x_{j_i}^{-1}$ by Proposition 9(iv). Thus, irrespective of whether $\epsilon_i = 1$ or $\epsilon_i = -1$, $x_{j_1}^{\epsilon_1} \cdots x_{j_{i-1}}^{\epsilon_{i-1}} \frac{\partial \left(x_{j_i}^{\epsilon_i}\right)}{\partial x_j} = \epsilon_i u_{(i)}$. Hence:

$$\frac{\partial u}{\partial x_j} = \sum_{j_i=j} \epsilon_i u_{(i)}. \tag{3.4}$$

Note that no terms in this sum may cancel each other out: suppose that $\epsilon_i u_{(i)} + \epsilon_{i+k} u_{(i+k)} = 0$ for some i and $k > 0$ with $j_i = j_{i+k} = j$. Then, because of how the initial sections are defined, we must have $u_{(i)} = u_{(i+k)}$ and $k = 1$, implying that $\epsilon_i = -1$ and $\epsilon_{i+1} = 1$. But then $\epsilon_i + \epsilon_{i+1} = 0$ with $j_i = j_{i+1}$, contradicting Definition 31. By this contradiction, there can be no cancelling in the sum of Equation (3.4).

This equation expresses $\frac{\partial u}{\partial x_j}$ as a weighted exponent sum of x_j, in which each exponent of x_j is weighted by some initial section of u. Furthermore, this equation tells us that the x_j-length of u is equal to the number of terms in $\frac{\partial u}{\partial x_j}$. Lastly, this shows that in a first-order derivative of a free group element, all coefficients are either 1 or -1.

Partial differentiation does not only yield useful results for free group elements, though. We also obtain two powerful results for first-order derivatives of any free group algebra elements. Firstly, we have a **Chain Rule of Free Differentiation**:

Theorem 5. *If $\lambda : Y \to X$ is a homomorphism between free groups Y and X with generating sets $(y) = \{y_1, y_2, ..., y_n\}$ and $(x) = \{x_1, x_2, ..., x_m\}$ respectively,*

then for any $f \in \mathbb{Z}[Y]$*:*

$$\frac{\partial}{\partial x_j}\left(\tilde{\lambda}(f)\right) = \sum_{k=1}^{n} \tilde{\lambda}\left(\frac{\partial f}{\partial y_k}\right) \cdot \frac{\partial}{\partial x_j}(\lambda(y_k))$$

for any $x_j \in (x)$*.*

Proof. We will prove this by induction on free group algebra elements. Note that this approach is only sufficient because we are considering finitely generated free groups Y and X. If we allowed for infinitely many generators, then we would have to explicitly show that the sum on the right-hand side of the Chain Rule is still finite. According to [7] this is in fact the case, however, we will not be proving that since we restrict ourselves to finitely generated groups.

We begin by considering $f = 1$. Then:

$$\begin{aligned}
\frac{\partial}{\partial x_j}\left(\tilde{\lambda}(f)\right) &= \frac{\partial}{\partial x_j}(\lambda(1)) = \frac{\partial}{\partial x_j}(1) = 0 \\
&= \sum_{k=1}^{n} 0 \cdot \frac{\partial}{\partial x_j}(\lambda(y_k)) \\
&= \sum_{k=1}^{n} \lambda(0) \cdot \frac{\partial}{\partial x_j}(\lambda(y_k)) \\
&= \sum_{k=1}^{n} \tilde{\lambda}\left(\frac{\partial f}{\partial y_k}\right) \cdot \frac{\partial}{\partial x_j}(\lambda(y_k))
\end{aligned}$$

and so the rule holds when $f = 1$. We now consider $f \in (y)$. Set $f = y_i$. Then:

$$\begin{aligned}
\frac{\partial}{\partial x_j}\left(\tilde{\lambda}(f)\right) &= \frac{\partial}{\partial x_j}\left(\lambda(y_i)\right) = \lambda(1) \cdot \frac{\partial}{\partial x_j}(\lambda(y_i)) \\
&= \lambda\left(\frac{\partial y_i}{\partial y_i}\right) \cdot \frac{\partial}{\partial x_j}(\lambda(y_i)) \\
&= \sum_{k=1}^{n} \lambda\left(\frac{\partial y_i}{\partial y_k}\right) \cdot \frac{\partial}{\partial x_j}(\lambda(y_k)) \\
&= \sum_{k=1}^{n} \tilde{\lambda}\left(\frac{\partial f}{\partial y_k}\right) \cdot \frac{\partial}{\partial x_j}(\lambda(y_k))
\end{aligned}$$

seeing as all the terms disappear when $k \neq i$ since $\lambda\left(\frac{\partial y_i}{\partial y_k}\right) = \lambda(0) = 0$. Now

considering $f = y_i^{-1}$ for some $y_i \in (y)$, we obtain:

$$\begin{aligned}
\frac{\partial}{\partial x_j}\left(\tilde{\lambda}(f)\right) &= \frac{\partial}{\partial x_j}\left(\lambda\left(y_i^{-1}\right)\right) = \frac{\partial}{\partial x_j}\left(\lambda(y_i)^{-1}\right) \\
&= -\lambda(y_i)^{-1} \cdot \frac{\partial}{\partial x_j}(\lambda(y_i)) \\
&= \tilde{\lambda}\left(-y_i^{-1}\right) \cdot \frac{\partial}{\partial x_j}(\lambda(y_i)) \\
&= \tilde{\lambda}\left(\frac{\partial\left(y_i^{-1}\right)}{\partial y_i}\right) \cdot \frac{\partial}{\partial x_j}(\lambda(y_i)) \\
&= \sum_{k=1}^{n} \tilde{\lambda}\left(\frac{\partial\left(y_i^{-1}\right)}{\partial y_k}\right) \cdot \frac{\partial}{\partial x_j}(\lambda(y_k)) \\
&= \sum_{k=1}^{n} \tilde{\lambda}\left(\frac{\partial f}{\partial y_k}\right) \cdot \frac{\partial}{\partial x_j}(\lambda(y_k)).
\end{aligned}$$

Thus, the Chain Rule holds for all generators of Y and all of their inverses. Now assume that the Chain Rule holds for $u, v \in Y$ and consider $f = uv$. Then:

$$\begin{aligned}
\frac{\partial}{\partial x_j}\left(\tilde{\lambda}(f)\right) &= \frac{\partial}{\partial x_j}\left(\lambda(uv)\right) = \frac{\partial}{\partial x_j}\left(\lambda(u)\lambda(v)\right) \\
&= \frac{\partial}{\partial x_j}(\lambda(u)) + \lambda(u) \cdot \frac{\partial}{\partial x_j}(\lambda(v)) \\
&= \sum_{k=1}^{n} \tilde{\lambda}\left(\frac{\partial u}{\partial y_k}\right) \cdot \frac{\partial}{\partial x_j}(\lambda(y_k)) + \lambda(u) \cdot \sum_{k=1}^{n} \tilde{\lambda}\left(\frac{\partial v}{\partial y_k}\right) \cdot \frac{\partial}{\partial x_j}(\lambda(y_k)) \\
&= \sum_{k=1}^{n} \left(\tilde{\lambda}\left(\frac{\partial u}{\partial y_k}\right) + \lambda(u) \cdot \tilde{\lambda}\left(\frac{\partial v}{\partial y_k}\right)\right) \cdot \frac{\partial}{\partial x_j}(\lambda(y_k)) \\
&= \sum_{k=1}^{n} \tilde{\lambda}\left(\frac{\partial u}{\partial y_k} + u \cdot \frac{\partial v}{\partial y_k}\right) \cdot \frac{\partial}{\partial x_j}(\lambda(y_k)) \\
&= \sum_{k=1}^{n} \tilde{\lambda}\left(\frac{\partial (uv)}{\partial y_k}\right) \cdot \frac{\partial}{\partial x_j}(\lambda(y_k)) \\
&= \sum_{k=1}^{n} \tilde{\lambda}\left(\frac{\partial f}{\partial y_k}\right) \cdot \frac{\partial}{\partial x_j}(\lambda(y_k)).
\end{aligned}$$

Thus, we have shown that the Chain Rule holds for all $f \in Y$, using the inductive definition of Y. Now we consider $f \in \mathbb{Z}[Y]$, that is $f = \sum_{u \in Y} a_u u$.

This yields:

$$\begin{aligned}
\frac{\partial}{\partial x_j}\left(\tilde{\lambda}(f)\right) &= \frac{\partial}{\partial x_j}\left(\sum_{u\in Y} a_u \lambda(u)\right) = \sum_{u\in Y} a_u \frac{\partial}{\partial x_j}(\lambda(u)) \\
&= \sum_{u\in Y} a_u \left(\sum_{k=1}^{n} \tilde{\lambda}\left(\frac{\partial u}{\partial y_k}\right)\cdot \frac{\partial}{\partial x_j}(\lambda(y_k))\right) \\
&= \sum_{k=1}^{n}\sum_{u\in Y} a_u \tilde{\lambda}\left(\frac{\partial u}{\partial y_k}\right)\cdot \frac{\partial}{\partial x_j}(\lambda(y_k)) \\
&= \sum_{k=1}^{n}\left(\sum_{u\in Y} a_u \tilde{\lambda}\left(\frac{\partial u}{\partial y_k}\right)\right)\cdot \frac{\partial}{\partial x_j}(\lambda(y_k)) \\
&= \sum_{k=1}^{n}\tilde{\lambda}\left(\sum_{u\in Y} a_u \left(\frac{\partial u}{\partial y_k}\right)\right)\cdot \frac{\partial}{\partial x_j}(\lambda(y_k)) \\
&= \sum_{k=1}^{n}\tilde{\lambda}\left(\frac{\partial}{\partial y_k}\left(\sum_{u\in Y} a_u u\right)\right)\cdot \frac{\partial}{\partial x_j}(\lambda(y_k)) \\
&= \sum_{k=1}^{n}\tilde{\lambda}\left(\frac{\partial f}{\partial y_k}\right)\cdot \frac{\partial}{\partial x_j}(\lambda(y_k)).
\end{aligned}$$

Thereby, the Chain Rule of Free Differentiation holds by induction. □

Lastly, we obtain the following result which will prove imperative in constructing expansions analogous to Taylor and MacLaurin series:

Theorem 6. *Let $h : (x) \to \mathbb{Z}[X]$. Then there exists a unique Fox-derivation d_h of $\mathbb{Z}[X]$ such that $d_h(x_j) = h(x_j)$ for all generators $x_j \in (x)$. This derivation is given by:*

$$d_h(f) = \sum_{j=1}^{m} \frac{\partial f}{\partial x_j}\cdot h(x_j) \qquad \forall f \in \mathbb{Z}[X] \tag{3.5}$$

where the generating set (x) has m elements.

Proof. Remembering the scalar multiplication in $\mathrm{FDer}(\mathbb{Z}[X])$, we can write d_h as $d_h = \sum_{j=1}^{m} \frac{\partial}{\partial x_j} h(x_j)$. Since $\mathrm{FDer}(\mathbb{Z}[X])$ is a right $\mathbb{Z}[X]$-module, this means that $d_h \in \mathrm{FDer}(\mathbb{Z}[X])$, i.e. d_h is indeed a Fox-derivation.

Now for any $x_k \in (x)$:

$$d_h(x_k) = \sum_{j=1}^{m} \frac{\partial x_k}{\partial x_j}\cdot h(x_j) = \sum_{j=1}^{m} \delta_{jk}\cdot h(x_j) = h(x_k),$$

meaning that d_h satisfies Equation (3.5). We must, however, show that it is the

only Fox-derivation satisfying Equation (3.5). Suppose that $d \in \mathrm{FDer}(\mathbb{Z}[X])$ such that $d(x_k) = h(x_k)$ for each $x_k \in (x)$. Then we can define another Fox-derivation $d' = d - d_h$. Clearly $d'(x_k) = 0$ for all k and $d'\left(x_k^{-1}\right) = -x_k^{-1} \cdot 0 = 0$. Then, using Proposition 9, for any $\prod_{k=1}^{l} x_{j_k}^{\epsilon_k} \in X$:

$$\begin{aligned} d'\left(\prod_{k=1}^{l} x_{j_k}^{\epsilon_k}\right) &= \sum_{k=1}^{l} \left(x_{j_1}^{\epsilon_1} x_{j_2}^{\epsilon_2} \cdots x_{j_{k-1}}^{\epsilon_{k-1}} d'\left(x_{j_k}^{\epsilon_k}\right)\right) \\ &= \sum_{k=1}^{l} \left(x_{j_1}^{\epsilon_1} x_{j_2}^{\epsilon_2} \cdots x_{j_{k-1}}^{\epsilon_{k-1}} \cdot 0\right) \\ &= 0, \end{aligned}$$

i.e. d' is trivial on X. So for any $\sum_{u \in X} a_u u \in \mathbb{Z}[X]$:

$$d'\left(\sum_{u \in X} a_u u\right) = \sum_{u \in X} a_u d'(u) = \sum_{u \in X} a_u \cdot 0 = 0.$$

Thus, $0 = d' = d - d_h$, that is $d = d_h$. □

Theorem 6 allows us to construct a Fox-derivation that maps each generator to a prescribed value with no restrictions at all on our choice of prescribed values, knowing that this derivation has the structure as described in Equation (3.5). For example, we can observe that the Fox-derivation d defined by $d(f) = f - f(1)$ maps each x_j to $x_j - 1$. Therefore, by Theorem 6:

$$f - f(1) = \sum_{j=1}^{m} \frac{\partial f}{\partial x_j} \cdot (x_j - 1).$$

This leads directly to the so-called **fundamental formula**:

$$f = f(1) + \sum_{j=1}^{m} \frac{\partial f}{\partial x_j} \cdot (x_j - 1). \tag{3.6}$$

This equation allows us to describe any $f \in \mathbb{Z}[X]$ using only $f(1)$ and its first-order derivatives. In the case of $u \in X$ this is particularly powerful because we already know that $u(1) = 1$ and because of our knowledge of the derivatives of u.

3.2.3 Higher-Order Derivatives

In the previous section we worked only with first-order derivatives, however, we can consider n^{th}-order derivatives for any $n \in \mathbb{N}$. We consider the identity mapping to be the 0^{th}-order derivative and for $n > 1$, we define n^{th}-order derivatives inductively as follows:

$$\frac{\partial^n}{\partial x_{j_n} \partial x_{j_{n-1}} \cdots \partial x_{j_1}} := \frac{\partial}{\partial x_{j_n}} \circ \frac{\partial^{n-1}}{\partial x_{j_{n-1}} \cdots \partial x_{j_1}}. \tag{3.7}$$

For the sake of convenience we may write the simplified symbol $D_{j_n \cdots j_1}$ instead of the full expression $\frac{\partial^n}{\partial x_{j_n} \cdots \partial x_{j_1}}$. It is important to note that the higher-order derivatives are not Fox-derivations. It is straightforward to observe that they satisfy the linearity constraint, however the product rule for arbitrary-order derivatives is more involved than Equation (2.4):

$$\begin{aligned}
D_{j_n \cdots j_1}(f \cdot g) &= D_{j_n}\left(D_{j_{n-1}}\left(\cdots (D_{j_1}(f \cdot g)) \cdots\right)\right) \\
&= D_{j_n}\left(\cdots D_{j_2}\left(D_{j_1}(f) \cdot g(1) + f \cdot D_{j_1}(g)\right) \cdots\right) \\
&= D_{j_n}(\cdots D_{j_2}(D_{j_1}(f) \cdot g(1)) + D_{j_2}(f \cdot D_{j_1}(g)) \cdots) \\
&= D_{j_n}(\cdots D_{j_2 j_1}(f) \cdot g(1) + D_{j_1}(f) \cdot D_{j_2}(g(1)) \\
&\qquad + D_{j_2}(f) \cdot \tilde{o}(D_{j_1}(g)) + f \cdot D_{j_2 j_1}(g) \cdots)
\end{aligned}$$

But $D_{j_2}(g(1)) = 0$ since D_{j_2} is a Fox-derivation and $g(1) \in \mathbb{Z}$. Therefore:

$$\begin{aligned}
&D_{j_n \cdots j_1}(f \cdot g) \\
&= D_{j_n}\left(\cdots D_{j_3}\left(D_{j_2 j_1}(f) \cdot g(1) + D_{j_2}(f) \cdot \tilde{o}(D_{j_1}(g)) + f \cdot D_{j_2 j_1}(g)\right) \cdots\right) \\
&= D_{j_n}(\cdots D_{j_4}(D_{j_3 j_2 j_1}(f) \cdot g(1) + D_{j_3 j_2}(f) \cdot \tilde{o}(D_{j_1}(g)) \\
&\qquad + D_{j_3}(f) \cdot \tilde{o}(D_{j_2 j_1}(g)) + f \cdot D_{j_3 j_2 j_1}(g)) \cdots)
\end{aligned}$$

Following this pattern indefinitely we eventually arrive at the following **Product Rule for higher-order Fox-derivatives**:

$$D_{j_n \cdots j_1}(f \cdot g) = \sum_{i=1}^{n} D_{j_n \cdots j_i}(f) \cdot D_{j_{i-1} \cdots j_1}(g)(1) + f \cdot D_{j_n \cdots j_1}(g) \qquad \forall f, g \in \mathbb{Z}[X]. \tag{3.8}$$

We have used iteration to find an equation for higher-order derivatives analogous to Equation (2.4). Similarly, we can iterate to find an equation for higher-order derivatives of free group elements, analogous to Equation (3.4).

We do this by repeatedly applying that very equation:

$$\begin{aligned} D_{j_n\cdots j_1}(u) &= D_{j_n\cdots j_2}\left(\sum_{j_{\lambda_1}=j_1}\epsilon_{\lambda_1}u_{(\lambda_1)}\right) = D_{j_n\cdots j_3}\left(D_{j_2}\left(\sum_{j_{\lambda_1}=j_1}\epsilon_{\lambda_1}u_{(\lambda_1)}\right)\right) \\ &= D_{j_n\cdots j_3}\left(\sum_{j_{\lambda_1}=j_1}\epsilon_{\lambda_1}D_{j_2}\left(u_{(\lambda_1)}\right)\right). \end{aligned}$$

Now:

$$\begin{aligned} D_{j_2}\left(u_{(\lambda_1)}\right) &= D_{j_2}\left(\left(\prod_{k=1}^{\lambda_1-1}x_{j_k}^{\epsilon_k}\right)x_{j_{\lambda_1}}^{\frac{\epsilon_{\lambda_1}-1}{2}}\right) \\ &= D_{j_2}\left(\prod_{k=1}^{\lambda_1-1}x_{j_k}^{\epsilon_k}\right)+\left(\prod_{k=1}^{\lambda_1-1}x_{j_k}^{\epsilon_k}\right)\cdot D_{j_2}\left(x_{j_{\lambda_1}}^{\frac{\epsilon_{\lambda_1}-1}{2}}\right) \\ &= \sum_{k=1}^{\lambda_1-1}x_{j_1}^{\epsilon_1}\cdots x_{j_{k-1}}^{\epsilon_{k-1}}D_{j_2}\left(x_{j_k}^{\epsilon_k}\right)+\frac{\epsilon_{\lambda_1}-1}{2}\delta_{j_{\lambda_1}j_2}\left(\prod_{k=1}^{\lambda_1-1}x_{j_k}^{\epsilon_k}\right)x_{j_{\lambda_1}}^{\epsilon_{\lambda_1}} \\ &= \sum_{j_{\lambda_2}=j_2,j_{\lambda_2}\leq\lambda_1-1}\epsilon_{\lambda_2}u_{(\lambda_2)}+\frac{\epsilon_{\lambda_1}-1}{2}\delta_{j_{\lambda_1}j_2}u_{(\lambda_1)} \\ &= \sum_{j_{\lambda_2}=j_2}\epsilon_{\lambda_2}u_{(\lambda_2)} \end{aligned}$$

with the restriction to the last sum that $1\leq\lambda_2\leq\lambda_1-\frac{1}{2}(\epsilon_{\lambda_1}+1)$ since we keep going up until λ_1 if $\epsilon_{\lambda_1}=-1$ but we stop just beforehand if $\epsilon_{\lambda_1}=1$. Thereby:

$$D_{j_n\cdots j_1}(u) = D_{j_n\cdots j_3}\left(\sum_{j_{\lambda_2}=j_2,j_{\lambda_1}=j_1}\epsilon_{\lambda_2}\epsilon_{\lambda_1}u_{(\lambda_2)}\right)$$

with the aforementioned restriction on λ_2. Continuing this pattern we obtain:

$$D_{j_n\cdots j_1}(u) = \sum_{j_n=j_{\lambda_n},\ldots,j_{\lambda_1}=j_1}\epsilon_{\lambda_n}\cdots\epsilon_{\lambda_1}u_{(\lambda_n)} \tag{3.9}$$

subject to the restriction: $1\leq\lambda_{i+1}\leq\lambda_i-\frac{1}{2}(\epsilon_{\lambda_i}+1)$ for $i=1,\ldots,n-1$. This equation tells us that $D_{j_n\cdots j_1}(u)$ has the same terms as $D_{j_n}(u)$ but possibly with different coefficients and with some terms removed. We observed from Equation (3.4) that first-order derivatives of free group elements only have coefficients 1 and -1. Equation (3.9) shows that any order of derivative of a free group element can only have coefficients 1 and -1.

While these equations are interesting, we are primarily interested in constructing equations analogous to Taylor series as mentioned previously. We can do this by iterating the fundamental formula:

$$\begin{aligned} f &= f(1) + \sum_{j=1}^{m} D_j(f) \cdot (x_j - 1) \\ &= f(1) + \sum_{j_1=1}^{m} \left(D_{j_1}(f)(1) + \sum_{j=1}^{m} D_{jj_1}(f) \cdot (x_j - 1) \right) \cdot (x_{j_1} - 1) \\ &= f(1) + \sum_{j_1=1}^{m} D_{j_1}(f)(1) \cdot (x_{j_1} - 1) + \sum_{j_2=1, j_1=1}^{m} D_{j_2 j_1}(f) \cdot (x_{j_2} - 1) \cdot (x_{j_1} - 1). \end{aligned}$$

Continuing this pattern for n steps, we get the equation:

$$\begin{aligned} f =& f(1) + \sum_{j_1=1}^{m} D_{j_1}(f)(1) \cdot (x_{j_1} - 1) + \cdots \\ &+ \sum_{j_n=1,\ldots,j_1=1}^{m} D_{j_n \cdots j_1}(f)(1) \cdot (x_{j_n} - 1) \cdots (x_{j_1} - 1). \end{aligned} \tag{3.10}$$

If we formally continue the pattern to infinity, then we obtain a formal Taylor series:

$$f = f(1) + \sum_{j=1}^{m} D_j(f)(1) \cdot (x_j - 1) + \sum_{j=1,k=1}^{m} D_{jk}(f)(1) \cdot (x_j - 1) \cdot (x_k - 1) + \cdots \tag{3.11}$$

This Taylor series is remarkably similar to the well-known Taylor series of complex differentiable functions. Additionally, it has a certain similarity to the Magnus series expansion in Equation (3.1): it makes use of $x_j - 1$ which were set to be s_j in the Magnus approach. We now check whether these two expansions are in fact equivalent. Firstly, applying the Taylor series to a generator x_j, we see that it perfectly matches the Magnus series expansion:

$$\begin{aligned} & x_j = 1 + (x_j - 1) = 1 + s_j \\ \text{and} \qquad & x_j^{-1} = 1 - (x_j - 1) + (x_j - 1)^2 - (x_j - 1)^3 + \cdots = \sum_{n=0}^{\infty} (-1)^n s_j^n. \end{aligned}$$

Now we apply the Taylor series to an element $u \in X$ with two generators. For the sake of simplicity we will consider the simplest version of such an element, namely $u = x_i^{\alpha} x_j^{\beta}$ for some $\alpha, \beta \in \mathbb{N} \backslash \{0\}$ and $i \neq j$. When we differentiate u, it is obvious that only derivatives with respect to x_i and x_j will be non-zero.

Now:

$$D_i(u) = D_i\left(x_i^\alpha\right) + x_i^\alpha \cdot D_i\left(x_j^\beta\right) = D_i(x_i^\alpha) = \sum_{k=1}^{\alpha} x_i^{k-1}$$

and

$$D_j(u) = D_j\left(x_i^\alpha\right) + x_i^\alpha \cdot D_j\left(x_j^\beta\right) = x_i^\alpha \cdot D_j\left(x_j^\beta\right) = x_i^\alpha \cdot \sum_{k=1}^{\beta} x_j^{k-1}$$

so that $D_i(u)(1) = \alpha$ and $D_j(u)(1) = \beta$. Continuing with second-order derivatives, we find:

$$\begin{aligned}
D_{ii}(u) &= D_i\left(\sum_{k=1}^{\alpha} x_i^{k-1}\right) = \sum_{k=1}^{\alpha} D_i\left(x_i^{k-1}\right) = \sum_{k=1}^{\alpha}\sum_{q=1}^{k-1} x_i^{q-1}, \\
D_{ji}(u) &= 0, \\
D_{ij}(u) &= \sum_{k=1}^{\beta}\sum_{q=1}^{\alpha} x_i^{q-1}
\end{aligned}$$

and

$$D_{jj}(u) = x_i^\alpha \sum_{k=1}^{\beta}\sum_{q=1}^{k-1} x_j^{q-1}$$

so that $D_{ii}(u)(1) = \binom{\alpha}{2}$, $D_{ji}(u)(1) = 0$, $D_{ij}(u)(1) = \alpha\beta$ and $D_{jj}(u)(1) = \binom{\beta}{2}$. Continuing this pattern and applying the Taylor series, we get:

$$\begin{aligned}
u &= 1 + \alpha(x_i - 1) + \beta(x_j - 1) + \binom{\alpha}{2}(x_i - 1)^2 \\
&\qquad + \alpha\beta(x_i - 1)\cdot(x_j - 1) + \binom{\beta}{2}(x_j - 1)^2 + \cdots \\
&= \sum_{v,w=0}^{\infty} \binom{\alpha}{v}\binom{\beta}{w}(x_i - 1)^v \cdot (x_j - 1)^w \\
&= \sum_{v,w=0}^{\infty} \binom{\alpha}{v}\binom{\beta}{w} s_i^v s_j^w
\end{aligned}$$

which is the Magnus series expansion of u. The same process applies for more complex elements, however, with much more intricate computations. Hereby, we see that the Taylor series in Equation (3.11) can be shown to be equivalent to the Magnus series expansion in Equation (3.1). The Taylor series is in Fox's view less cumbersome, a view shared by this dissertation's author.

Subsequent results in [7] concern the coefficient sum of higher-order Fox-derivatives. These equations relate to the coefficients in the Taylor series expansion and are therefore of interest. However, they are exceedingly technical to explain and are not relevant to the later work of the paper. For that reason the proofs are provided in Appendices B, C and D.

The relevant equations are as follows, keeping in mind that we must have $p \in \mathbb{Z}$, $n \geq 0$, $u \in X$ and $x_j \neq x_k$ in Equation (3.14):

$$\tilde{o}\left(\frac{\partial^n x_j^p}{\partial x_j^n}\right) = \binom{p}{n}, \tag{3.12}$$

$$\tilde{o}\left(\frac{\partial^n u}{\partial x_j^n}\right) = \binom{\tilde{o}\left(\frac{\partial u}{\partial x_j}\right)}{n}, \tag{3.13}$$

$$\tilde{o}\left(\frac{\partial^2 u}{\partial x_j \partial x_k}\right) + \tilde{o}\left(\frac{\partial^2 u}{\partial x_k \partial x_j}\right) = \tilde{o}\left(\frac{\partial u}{\partial x_j}\right)\tilde{o}\left(\frac{\partial u}{\partial x_k}\right). \tag{3.14}$$

3.3 The Structure of $\mathbb{Z}[X]$

We will now study the structure of the finitely generated free group algebra $\mathbb{Z}[X]$ by way of its fundamental ideal Q. Recall from Definition 30 that the fundamental ideal is made up of all elements of the group algebra with coefficient sum 0:

$$Q = \left\{ \sum_{u \in X} a_u u \in \mathbb{Z}[X] : \sum_{u \in X} a_u = 0 \right\}.$$

Note that we denote this fundamental ideal by Q to differentiate it from O, which is used more broadly for the fundamental ideal of a general group. More specifically, we are interested in the powers of Q, that is in the chain of ideals $Q \supseteq Q^2 \supseteq Q^3 \cdots$. We say that $Q^0 = \mathbb{Z}[X]$.

Proposition 13. *Given $f \in \mathbb{Z}[X]$ and $n \in \mathbb{N}$, $f \in Q^n$ if and only if all of its partial derivatives of order less than n "vanish at $x = 1$", that is if $f(1) = 0$ and $D_{j_i \cdots j_1}(f)(1) = 0$ for all $i \in \{1, ..., n-1\}$ with any combination of generators $x_{j_1}, ..., x_{j_i}$.*

Proof. Firsly, note that when $n = 0$ the statement is vacuously true. For $n > 0$, we will prove Proposition 13 by induction on n. If $n = 1$, then the statement is obviously true by the definition of Q.

Now consider $n > 1$ and assume that the statement holds for $1, 2, ..., n-1$. Suppose that $f \in Q^n$. We can write f as a finite sum $f = \sum_k f_{1k} \cdot f_{2k} \cdots f_{nk}$,

where $f_{ik}(1) = 0$ for all $i = 1, ..., n$ and all k. From Equation (3.8):

$$\begin{aligned} D_{j_{n-1}\cdots j_1}(f) =& D_{j_{n-1}}\left(\cdots D_{j_1}\left(\sum_k f_{1k}\cdot f_{2k}\cdots f_{nk}\right)\right) \\ =& \sum_k D_{j_{n-1}\cdots j_1}(f_{1k}\cdot f_{2k}\cdots f_{nk}) \\ =& \sum_k \sum_{i=1}^{n-1}(D_{j_{n-1}\cdots j_i}(f_{1k})\cdot D_{j_{i-1}\cdots j_1}(f_{2k}\cdots f_{nk})(1) \\ &+ f_{1k}D_{j_{n-1}\cdots j_1}(f_{2k}\cdots f_{nk})) \\ =& \sum_k \sum_{i=1}^{n-1} f_{1k}\cdot D_{j_{n-1}\cdots j_1}(f_{2k}\cdots f_{nk}) \end{aligned}$$

since $f_{2k}\cdots f_{nk} \in Q^{n-1}$ and so $D_{j_{i-1}\cdots j_1}(f_{2k}\cdots f_{nk})(1) = 0$ for $i \in \{1, ..., n-1\}$ by the induction hypothesis. Thus:

$$D_{j_{n-1}\cdots j_1}(f)(1) = \sum_k \sum_{i=1}^{n-1} f_{1k}(1)D_{j_{n-1}\cdots j_1}(f_{2k}\cdots f_{nk})(1) = 0$$

as $f_{1k}(1) = 0$ for all k. The same ideas apply for any derivative of order less than $n-1$. Thus, the forward implication holds.

Now suppose that all derivatives of f of order up to $n-1$ vanish at $x = 1$. Then by Equation (3.10):

$$\begin{aligned} f =& f(1) + \sum_{j_1=1}^{m} D_{j_1}(f)(1)(x_{j_1} - 1) + \cdots \\ &+ \sum_{j_{n-1},\ldots,j_1=1}^{m} D_{j_{n-1}\cdots j_1}(f)(x_{j_{n-1}} - 1)\cdots(x_{j_1} - 1) \\ =& \sum_{j_{n-1},\ldots,j_1=1}^{m} D_{j_{n-1}\cdots j_1}(f)(x_{j_{n-1}} - 1)\cdots(x_{j_1} - 1) \in Q^n \end{aligned}$$

since $D_{j_{n-1}\cdots j_1}(f), x_{j_{n-1}} - 1, ..., x_{j_1} - 1 \in Q$. Thereby, the backward implication also holds. □

We now move on to a lemma, which itself requires the definition of a new quantity:

Definition 35. *For any $f \in \mathbb{Z}[X]$ we can write f as $f = a_1u_1 + \cdots + a_qu_q$ where $u_i \neq u_k$ whenever $i \neq k$ and $a_i \neq 0$ for all i. With this in mind, the*

length *of f is given by $l(f) = \max_{1\leq i\leq q}\{l(u_i)\}$, where $l(u_i)$ refers to the length of free group elements as defined in Definition 31. We say that $l(0) = 0$.*

It is worth mentioning here that the derivative of an element cannot have greater length than the element itself: $D_j(f) = a_1 D_j(u_1) + \cdots + a_q D_j(u_q)$ and so $l\left(D_j(f)\right) = \max_{1\leq i\leq q}\{l(D_j(u_i))\}$. But for each i, $D_j(u_i) = \sum_{j_k=j} \epsilon_k u_{ik}$ and so $l(D_j(u_i)) \leq l(u_i)$. Therefore, $l(D_j(f)) \leq l(f)$.

Lemma 3. *For any non-zero $f \in Q^n$, $l(f) \geq \frac{n}{2}$.*

Proof. Again, we use induction on n. For any non-zero f, $l(f) \geq 1 \geq \frac{1}{2}$ and so the statement holds for $n = 1$ and $n = 2$.

Now consider $n > 2$ and suppose that the statement holds for $1, 2, ..., n-2$. Assume that there exists some $f \in Q^n \setminus \{0\}$ such that $l(f) < \frac{n}{2}$. Each term in f ends in a generator or its inverse and so we can write $f = \sum_{j=1}^{m}(g^j \cdot x_j + h^j \cdot x_j^{-1})$, where g^j and h^j always have length less than $l(f)$. Hence, for any $x_k \in (x)$:

$$\begin{aligned} D_k(f) &= \sum_{j=1}^{m} \left(D_k\left(g^j \cdot x_j\right) + D_k\left(h^j \cdot x_j^{-1}\right)\right) \\ &= \sum_{j=1}^{m} \left(D_k\left(g^j\right) + \delta_{jk} g^j + D_k\left(h^j\right) - \delta_{jk} h^j \cdot x_j^{-1}\right). \end{aligned}$$

We write this derivative as $D_k(f) = a^k - h^k \cdot x_k^{-1}$, where:

$$a_k = \sum_{j=1}^{m} \left(D_k\left(g^j\right) + \delta_{jk} g^j + D_k\left(h^j\right)\right)$$

has length less than $l(f)$ since g^j and h^j have length less than $l(f)$ for each j. Now, for $i \neq k$, $D_{ik}(f) = D_i\left(a^k\right) - D_i\left(h^k\right)$ and so $D_{ik}(f)$ has length less than $l(f)$.

Now, remember that $f \in Q^n$ and so by Proposition 13, all of its derivatives of order $0, 1, ..., n-1$ vanish at $x = 1$. Thus, all derivatives of $D_{ik}(f)$ of order $0, 1, ..., n-3$ vanish at $x = 1$, meaning that by Proposition 13, $D_{ik}(f) \in Q^{n-2}$. Therefore, using the induction hypothesis, unless $D_{ik}(f) = 0$ we must have that $l\left(D_{ik}(f)\right) \geq \frac{n-2}{2} = \frac{n}{2} - 1 \geq l(f)$. This inequality contradicts our earlier working, meaning that $D_{ik}(f) = 0$. This holds for any $i \neq k$.

Further, $D_{kk}(f) = D_k(a_k) - D_k\left(h^k\right) + h^k \cdot x_k^{-1}$ and so:

$$\begin{aligned} D_k\left(D_k(f) \cdot x_k\right) &= D_{kk}(f) + D_k(f) \\ &= D_k\left(a^k\right) - D_k\left(h^k\right) + a^k \end{aligned}$$

has length less than $l(f)$ seeing as a^k and h^k do. Now, following Equation (3.10), all derivatives of order $0, 1, ..., n-3$ of $D_k\left(D_k(f) \cdot x_k\right)$ vanish at $x = 1$ and so $D_k\left(D_k(f) \cdot x_k\right) \in Q^{n-2}$. Similarly to the last paragraph, we find that $0 = D_k\left(D_k(f) \cdot x_k\right) = D_{kk}(f) + D_k(f)$, i.e. $D_{kk}(f) = -D_k(f)$.

But by the fundamental formula, $D_k(f) = D_k(f)(1) + \sum_{i=1}^{m} D_{ik}(f) \cdot (x_i - 1)$. Since $D_k(f)(1) = 0$ by Proposition 13 and $D_{ik}(f) = 0$ whenever $i \neq k$, this becomes:

$$D_k(f) = D_{kk}(f) \cdot (x_k - 1) = -D_k(f) \cdot (x_k - 1).$$

Therefore:

$$\begin{aligned} D_k(f) &= D_k(f) \cdot x_k^{-1} + D_k(f) - D_k(f) \cdot x_k^{-1} \\ &= \left(D_k(f) + D_k(f) \cdot (x_k - 1)\right) \cdot x_k^{-1} \\ &= \left(-D_k(f) \cdot (x_k - 1) + D_k(f) \cdot (x_k - 1)\right) \cdot x_k^{-1} \\ &= 0. \end{aligned}$$

Seeing as x_k was arbitrary, the fundamental formula tells us that $f = f(1) + \sum_{k=1}^{m} D_k(f) \cdot (x_k - 1) = 0$ since $f(1) = 0$ and $D_k(f) = 0$ for all k. So $f = 0$, contradicting that f is non-zero. Therefore, our assumption that there exists such an $f \in Q^n \setminus \{0\}$ was false, i.e. the statement holds for n.

Thus, the induction is complete. □

Using this lemma we obtain the **Uniqueness Theorem for Formal Power Series Expansions**:

Theorem 7. *Given $f, g \in \mathbb{Z}[X]$, if $f(1) = g(1)$, $D_j(f)(1) = D_j(g)(1)$ for all $x_j \in (x)$, $D_{ij}(f)(1) = D_{ij}(g)(1)$ for all $x_i, x_j \in (x)$ and so on, then $f = g$.*

Proof. Assume that $f \neq g$, i.e. $f - g \neq 0$. By Proposition 13, $f - g \in Q^n$ for all $n \in \mathbb{N}$. Hence, by Lemma 3, $l(f - g) \geq \frac{n}{2}$ for all $n \in \mathbb{N}$. But $l(f - g)$ must be finite since all elements of $\mathbb{Z}[X]$ are finite sums. This is a contradiction, meaning that our assumption was false: $f = g$. □

Proposition 14. $\bigcap_{n\in\mathbb{N}} Q^n = \{0\}$.

Proof. Suppose that $f \in \bigcap_{n\in\mathbb{N}} Q^n$. By Proposition 13, $D_{j_n\cdots j_1}(f)(1) = 0$ for any combination of generators $x_{j_1}, ..., x_{j_n}$ for all $n \in \mathbb{N}$. This can be rephrased as:

$$D_{j_n\cdots j_1}(f)(1) = D_{j_n\cdots j_1}(0)(1)$$

for any combination of generators for all $n \in \mathbb{N}$. Thus, $f = 0$ by Theorem 7. □

With these results, we obtain a generalisation of Proposition 13:

Proposition 15. *For $f \in \mathbb{Z}[X]$, $n \in \mathbb{N}$ and an ideal I of $\mathbb{Z}[X]$, $f \in IQ^n$ if and only if $f \in Q^n$ and all derivatives of f of order n belong to I.*

We note that this is slightly different to Result (4.5) from [7] (and slightly weaker than it): there it is stated as "...if and only if $f \in Q$ and..." We believe this to be a typographical error. Note also that our version of the statement allows for $n = 0$ and that it is a more natural generalisation of Proposition 13.

Proof. This proof is extremely similar to the proof of Proposition 13.

We start with the forward implication. Suppose that $f \in IQ^n$. Obviously $f \in Q^n$. Further, $f = \sum_k g_k \cdot f_{1k} \cdots f_{nk}$ where $g_k \in I$ and $f_{ik}(1) = 0$ for all k and $i = 1, ..., n$. So, using Equation (3.8):

$$\begin{aligned} D_{j_n\cdots j_1}(f) &= \sum_k D_{j_n\cdots j_1}(g_k f_{1k} \cdots f_{nk}) \\ &= \sum_k \left(\sum_{i=1}^{n} D_{j_n\cdots j_i}(g_k) \cdot D_{j_{i-1}\cdots j_1}(f_{1k} \cdots f_{nk})(1) + g_k D_{j_n\cdots j_1}(f_{1k} \cdots f_{nk}) \right) \\ &= \sum_k g_k D_{j_n\cdots j_1}(f_{1k} \cdots f_{nk}) \end{aligned}$$

by Proposition 13 since $f_{1k} \cdots f_{nk} \in Q^n$. Therefore, $D_{j_n\cdots j_1}(f) \in I$, being the sum of right-multiples of elements from I.

Conversely, suppose that $f \in Q^n$ and that all of its derivatives of order n belong to I. Then:

$$f = f(1) + \sum_{j_1=1}^{m} D_{j_1}(f)(1) \cdot (x_{j_1} - 1) + \cdots$$

$$+ \sum_{j_n,\ldots,j_1=1}^{m} D_{j_n\cdots j_1}(f)\cdot(x_{j_n}-1)\cdots(x_{j_1}-1)$$
$$= \sum_{j_n,\ldots,j_1=1}^{m} D_{j_n\cdots j_1}(f)\cdot(x_{j_n}-1)\cdots(x_{j_1}-1) \in IQ^n. \qquad \square$$

The Uniqueness Theorem also leads us to the following:

Proposition 16. *$\mathbb{Z}[X]$ has no zero divisors.*

This is in fact an application of a theorem from [8] which states that if G is a group that is indicable throughout and R has no zero divisors, then the group ring $R[G]$ has no zero divisors. (A group is indicable throughout if there exists a group homomorphism onto $\mathbb{Z}$.) Clearly, this applies to $\mathbb{Z}[X]$, however, we can prove it using only the results we have obtained in this dissertation:

Proof. Let $h = f \cdot g$ where $f, g \neq 0$. By Equation (3.8):

$$D_{j_{n+q}\cdots j_1}(h) = \sum_{i=1}^{n+q} D_{j_{n+q}\cdots j_i}(f)\cdot D_{j_{i-1}\cdots j_1}(g)(1) + f\cdot D_{j_{n+q}\cdots j_1}(g)$$

and so:

$$D_{j_{n+q}\cdots j_1}(h)(1) = \sum_{i=1}^{n+q} D_{j_{n+q}\cdots j_i}(f)(1)D_{j_{i-1}\cdots j_1}(g)(1) + f(1)D_{j_{n+q}\cdots j_1}(g)(1).$$

Since $f, g \neq 0$, there must exist $n, q \in \mathbb{N}$ such that $f \notin Q^{n+1}, f \in Q^n, g \notin Q^{q+1}$ and $g \in Q^q$. This is because $f, g \in Q^0 = \mathbb{Z}[X]$ at least and by Proposition 14 there must be some point in taking powers of Q at which f and g cease belonging to the ideals. Therefore, following Proposition 13, there exists some n^{th}-order derivative of f that does not vanish at $x = 1$ and similarly a q^{th}-order derivative of g. However, all derivatives of order up to n and q of f and g respectively disappear at $x = 1$. Thus, for some choice of indices $j_1, ..., j_{n+q}$:

$$D_{j_{n+q}\cdots j_1}(h)(1) = D_{j_{n+q}\cdots j_{q+1}}(f)(1)D_{j_q\cdots j_1}(g)(1) + f(1)D_{j_{n+q}\cdots j_1}(g)(1)$$

where $D_{j_{n+q}\cdots j_{q+1}}(f)(1)D_{j_q\cdots j_1}(g)(1) \neq 0$. Clearly, if $n > 0$, then $f(1) = 0$ and so this equation tells us that $D_{j_{n+q}\cdots j_1}(h)(1) \neq 0$. However, if $n = 0$, then $f(1) \neq 0$ and this becomes:

$$D_{j_q\cdots j_1}(h)(1) = f(1)D_{j_q\cdots j_1}(g)(1) + f(1)D_{j_q\cdots j_1}(g)(1) \neq 0.$$

Either way, $D_{j_{n+q}\cdots j_1}(h)(1) \neq 0$ and so $h \neq 0$. □

Note that the proof in [7] has errors in its presentation: the bracketing is done incorrectly and the case of $n = 0$ is omitted. (Admittedly, this case is very simple to consider.)

It is now relevant to introduce the lower central series of X:

Definition 36. *The **lower central series** of a group G is a series of normal subgroups $G_1 \supseteq G_2 \supseteq G_3 \supseteq \cdots$ of G known as the **commutator subgroups**, defined inductively as follows: $G_1 = G$ and for any $n \geq 1$, G_{n+1} is the subgroup generated by all of the commutators $[g, h] = ghg^{-1}h^{-1}$ with $g \in G_n$ and $h \in G$. Explicitly:*

$$G_{n+1} = \{[g_1, h_1][g_2, h_2] \cdots [g_k, h_k] : k \in \mathbb{N}, g_1, ..., g_k \in G_n, h_1, ..., h_k \in G\}.$$

Note that each commutator subgroup is indeed a normal subgroup of all preceeding commutator subgroups. It is obvious that they are all subgroups. Now suppose that $u \in G_n$ and $g \in G_{n-1}$. Then:

$$gug^{-1} = u\left(u^{-1}gug^{-1}\right) = u[u^{-1}, g] \in G_n$$

since $u^{-1} \in G_n \subseteq G_{n-1}$ and $g \in G$. Therefore, $G_n \trianglelefteq G_{n-1}$ and continuing this approach yields $G_n \trianglelefteq G_{n-1} \trianglelefteq G_{n-2} \trianglelefteq \cdots \trianglelefteq G_1$.

Note here that for the commutator subgroup G_2 we may also write $[G, G]$, for G_3 we may write $[G_2, G]$, etc. The notation $G_2, G_3, ...$ is more succinct but possibly less clear depending on the context. As implied earlier, we will be interested in the lower central series of X. In fact, it will become clear that the lower central series of X is closely connected to the series of ideals $Q \supseteq Q^2 \supseteq Q^3 \supseteq \cdots$.

For the following work, however, we rely on a result from [15], namely that $u \in X_n$ if and only if all of its derivatives of order $1, 2, ..., n-1$ "vanish at $x = 1$." (In [15] this is phrased as $u \in X_n$ if and only if u has dimension greater than or equal to n.) This claim, combined with Proposition 13, leads directly to:

Lemma 4. *For any $u \in X$ and $n \in \mathbb{N}$, $u \in X_n$ if and only $u - 1 \in Q^n$.*

Equivalently:

Proposition 17. *Q^n determines X_n.*

However, X_n is also determined by the ideal corresponding to it. We denote this ideal by Q_n and call it the ***n^{th}* lower central ideal**. We can describe this ideal completely: based on Proposition 11, it is obvious that $Q_n \subseteq Q^n$. Furthermore, we have $Q_1 = Q$ since X clearly corresponds to Q. It may be interesting to briefly note that for each $n \in \mathbb{N}$, Q_n is generated by the elements of $\{gh - hg : g \in X_{n-1}, h \in X\}$. This is because X_n is generated by $\{ghg^{-1}h^{-1} : g \in X_{n-1}, h \in X\}$ and so from Proposition 12, the generators of Q_n are the elements $ghg^{-1}h^{-1} - 1$. Because of how ideals are generated we may simply right-multiply each generator by hg and obtain the form $gh - hg$. Thereby, we know the precise composition of this ideal.

Moreover, from Proposition 17 we can extrapolate that $\cap_{n\in\mathbb{N}} Q^n$ determines $\cap_{n\in\mathbb{N}} X_n$. But from Proposition 14, we know that $\cap_{n\in\mathbb{N}} Q^n = \{0\}$ and hence $\cap_{n\in\mathbb{N}} X_n = \{1\}$.

Finally, we discuss what implications Proposition 17 has regarding the structure of other group algebras. It allows us to glean results for particular groups, namely those that can be constructed using the same generators of X but possibly with conditions limiting the freeness of the group. Explicitly, this is any group G that is a homomorphic image of X. The fundamental ideal of the group algebra $\mathbb{Z}[G]$ can be denoted by O, allowing for the following result analogous to Proposition 17:

Proposition 18. *Let G be a group such that there exists a surjective homomorphism $\phi : X \to G$. Then for any $n \in \mathbb{N}$, the ideal O^n determines the n^{th} lower central group G_n.*

It should be obvious without proof that in such a case $\tilde{\phi} : \mathbb{Z}[X] \to \mathbb{Z}[G]$ is a surjective ring homomorphism. However, the proof of the above proposition relies upon further results that are somewhat less obvious:

Lemma 5. *If $\phi : X \to G$ is a surjective group homomorphism, then $\phi|_{X_n} : X_n \to G_n$ and $\tilde{\phi}|_{Q^n} : Q^n \to O^n$ are also surjective homomorphisms.*

This result is alluded to in [7], however, it is not proved, presumably because the proof is fairly straightforward and very tedious. Nevertheless, we shall present the proof for the sake of comprehensiveness:

Proof. We can immediately see that these are homomorphisms, however, we must show that they are surjective and that $\phi(X_n) \subseteq G_n$ and $\tilde{\phi}(Q^n) \subseteq O^n$.

We will do this by induction on n.

Firstly let $n = 1$. Then $\phi|_{X_n} = \phi$ and immediately satisfies the desired properties. Now we must consider $\tilde{\phi}|_{Q^n} = \tilde{\phi}|_Q$. If $f \in Q$, then $\tilde{o}(f) = 0$ and so $\tilde{o}\left(\tilde{\phi}(f)\right) = 0$ as well since $\tilde{\phi}$ has no effect on the coefficients in the sum of f. Therefore, $\tilde{\phi}(f) \in O$, meaning that $\tilde{\phi}(Q) \subseteq O$. Now to demonstrate surjectivity we must consider $g \in O$. Recalling that $\tilde{\phi}$ is a surjective homomorphism from $\mathbb{Z}[X]$ to $\mathbb{Z}[G]$, there must exist some $f \in \mathbb{Z}[X]$ such that $\tilde{\phi}(f) = g$. By similar logic to that earlier in this paragraph, we can conclude that $f \in Q$. Thus, $\tilde{\phi}|_Q$ is surjective.

Now assume that the statement holds up to $n-1$. Letting $u \in X_n$, we can write $u = [u_1, v_1] \cdots [u_k, v_k]$ where $u_1, ..., u_k \in X_{n-1}$ and $v_1, ..., v_k \in X$. Then:

$$\phi(u) = \phi\left([u_1, v_1] \cdots [u_k, v_k]\right) = [\phi(u_1), \phi(v_1)] \cdots [\phi(u_k), \phi(v_k)] \in G_n$$

since $\phi(u_1), ..., \phi(u_k) \in G_{n-1}$ and $\phi(v_1), ..., \phi(v_k) \in G$. Thus, $\phi(X_n) \subseteq G_n$. In order to prove surjectivity we let $g \in G_n$. Then $g = [g_1, h_1] \cdots [g_k, h_k]$ for $g_1, ..., g_k \in G_{n-1}$ and $h_1, ..., h_k \in G$. But there must exist $u_1, ..., u_k \in X_{n-1}$ and $v_1, ..., v_k \in X$ such that $\phi(u_1) = g_1, ..., \phi(u_k) = g_k$ and $\phi(v_1) = h_1, ..., \phi(v_k) = h_k$. Hence, $\phi(u) = g$ where $u = [u_1, v_1] \cdots [u_k, v_k] \in X_n$. Thereby, $\phi|_{X_n} : X_n \to G_n$ is indeed a surjective homomorphism.

For $\tilde{\phi}|_{Q^n}$ the process is very similar. Considering $f \in Q^n$, we may express f as $f = \sum_k f_{1k} \cdots f_{nk}$ where each $f_{ik} \in Q$. Then:

$$\tilde{\phi}(f) = \sum_k \tilde{\phi}(f_{1k}) \cdots \tilde{\phi}(f_{nk}) \in O^n$$

since $\tilde{\phi}(f_{ik}) \in O$ always. Thus, $\tilde{\phi}(Q^n) \subseteq O^n$. Lastly, we show that for any $g \in O^n$ there exists $f \in Q^n$ such that $\tilde{\phi}(f) = g$. Any such g can be expressed as $g = \sum_k g_{1k} \cdots g_{nk}$ where $g_{ik} \in O$ for all i, k. Then for each pair i, k there exists some $f_{ik} \in Q$ such that $\tilde{\phi}(f_{ik}) = g_{ik}$ and so:

$$\tilde{\phi}\left(\sum_k f_{1k} \cdots f_{nk}\right) = \sum_k \tilde{\phi}(f_{1k}) \cdots \tilde{\phi}(f_{nk}) = g.$$

Clearly, $\sum_k f_{1k} \cdots f_{nk} \in Q^n$ and thus the proof is completed. □

Proof of Proposition 18. To prove this we must show that:

$$G_n = \{g \in G : g - 1 \in O^n\}.$$

First consider $g \in G_n$. Then by Lemma 5 there must exist $u \in X_n$ such that $\phi(u) = g$. But by Proposition 17, $u - 1 \in Q^n$ and hence Lemma 5 tells us that $g - 1 = \phi(u) - 1 = \tilde{\phi}(u - 1) \in O^n$. Thus:

$$G_n \subseteq \{g \in G : g - 1 \in O^n\}.$$

Conversely, let $g \in G$ such that $g - 1 \in O^n$. Firstly, there exists $u \in X$ such that $\phi(u) = g$ and:

$$\tilde{\phi}(u - 1) = \phi(u) - 1 = g - 1 \in O^n.$$

It seems intuitive at this point that $u - 1 \in X_n$, however, this is not assured based on our working thus far. To this end, let:

$$\tilde{\phi}(u - 1) = \sum_k g_{1k} \cdots g_{nk}$$

where $g_{ik} \in O$ for each pair i, k. But $\tilde{\phi}$ cannot introduce sums and therefore $u - 1$ must have the form $u - 1 = \sum_k f_k$ such that:

$$\tilde{\phi}(f_k) = g_{1k} \cdots g_{nk}.$$

At this point we may express the terms in the above sum as $g_{1k} = \sum_{g \in G} a_{1k_g} g, ...,$ $g_{nk} = \sum_{g \in G} a_{nk_g} g$ where $\sum_{g \in G} a_{1k_g} = \cdots = \sum_{g \in G} a_{nk_g} = 0$. Hence:

$$\tilde{\phi}(f_k) = \sum_{g \in G} \left(\cdots \sum_{h \in G} a_{1k_{g \cdots h^{-1}}} \cdots a_{nk_h} \cdots \right) g.$$

But each $g \in G$ in this sum can be expressed as $\phi(u)$ for some $u \in X$. Thereby, the above sum over G can rewritten as a sum over X:

$$\tilde{\phi}(f_k) = \sum_{u \in X} \left(\cdots \sum_{v \in X} a_{1k_{u \cdots v^{-1}}} \cdots a_{nk_v} \cdots \right) \phi(u).$$

There may not be a unique way of summing over X as each $g \in G$ might be mapped from any number of elements of $u \in X$. However, the relevant fact is that there must be at least one way of expressing $\tilde{\phi}(f_k)$ as above. Again,

since $\tilde{\phi}$ cannot create sums it must be possible to write f_k as:

$$f_k = \sum_{u\in X}\left(\cdots\sum_{v\in X} a_{1k_{u\cdots v-1}}\cdots a_{nk_v}\cdots\right)u = \left(\sum_{u\in X} a_{1k_u}u\right)\cdots\left(\sum_{u\in X} a_{nk_u}u\right)$$

where $\sum_{u\in X} a_{1k_u} = \cdots = \sum_{u\in X} a_{nk_u} = 0$. Since this is true for each k, we can conclude that $u-1 = \sum_k f_k \in Q^n$. Proposition 17 then tells us that $u \in X_n$ and hence $g = \phi(u) \in G_n$. Thus:

$$\{g \in G : g-1 \in O^n\} \subseteq G_n. \qquad \square$$

We now know that Proposition 18 holds which is useful because this means that properties of the lower central groups can be used to describe the ideals $O \supseteq O^2 \supseteq O^3 \cdots$ and vice versa.

Having discussed the subgroups determined by Q^n, it may be interesting to expand this to something broader. Considering the way we generalised Proposition 13 to Proposition 15, it would be interesting to know what subgroups are determined by the ideals IQ^n. We know for $I = Q^q$, but it would be instructive to have answers for the general case. Unfortunately, neither we nor Ralph H. Fox in 1952 had an answer for the completely general case. We do, however, have one result from [7]:

Proposition 19. *The ideal IQ determines the commutator subgroup $[N,N]$ of N, where N is the normal subgroup of X that corresponds to I.*

Proof. We let ϕ be the homomorphism such that $N = \ker(\phi)$ and $I = \ker\left(\tilde{\phi}\right)$. Now, for any $u, v \in N$ and $x_j \in (x)$:

$$\begin{aligned} D_j([u,v]) &= D_j\left(uvu^{-1}v^{-1}\right) \\ &= D_j(u) + u\cdot D_j(v) + uv\cdot D_j\left(u^{-1}\right) + uvu^{-1}\cdot D_j\left(v^{-1}\right) \\ &= D_j(u) + u\cdot D_j(v) - uvu^{-1}\cdot D_j(u) - uvu^{-1}v^{-1}\cdot D_j(v) \\ &= \left(1-uvu^{-1}\right)\cdot D_j(u) + u\cdot\left(1-vu^{-1}v^{-1}\right)\cdot D_j(v). \end{aligned}$$

But $\phi(u) = \phi(v) = 1$ and so $\tilde{\phi}\left(1-uvu^{-1}\right) = \tilde{\phi}\left(1-vu^{-1}v^{-1}\right) = 0$, meaning that $D_j([u,v]) \in \ker\left(\tilde{\phi}\right) = I$. Also, $D_j([u,v]-1) = D_j([u,v])$ and so $D_j([u,v]-1) \in I$. Thus, all derivatives of order 1 of $[u,v]-1$ belong to I. Furthermore, $([u,v]-1)(1) = 0$, i.e. $[u,v]-1 \in Q$. Thus, by Proposition 15, $[u,v]-1 \in IQ$. It is trivial to extend this to the fact that $u-1 \in IQ$ for all

$u \in [N, N]$.

The subgroup determined by IQ is $N_{IQ} = \{u \in X : u - 1 \in IQ\}$. Clearly, $[N, N] \subseteq N_{IQ}$.

Now we must show that $N_{IQ} \subseteq [N, N]$. To that end, consider $w \in X$ such that $w \in N_{IQ}$, i.e. $w - 1 \in IQ$. We will prove by induction on the length of w that $w \in [N, N]$. (For convenience we will denote this length by l instead of writing $l(w)$ every time.)

Firstly, let $l = 0$. Then $w = 1$. But $1 \in N$ and so $w = [1, 1] \in [N, N]$.

Now consider w such that $l > 0$ and assume that $y \in [N, N]$ for all $y \in N_{IQ}$ with $0 \leq l(y) < l$. Since $w - 1 \in IQ$, by Proposition 15, $D_j(w - 1) \in I$ for all $x_j \in (x)$. But $D_j(w) = D_j(w - 1)$ and so $D_j(w) \in I$ for all j. Therefore, $\tilde{\phi}(D_j(w)) = 0$ for every j. Returning to Equation (3.4), though, this becomes:

$$\sum_{j_i = j} \epsilon_i \phi\left(w_{(i)}\right) = 0.$$

But $\phi\left(w_{(i)}\right)$ is always a group element and all the coefficients are either 1 or -1. Therefore, the terms must all cancel each other out pairwise. Hence, it must be possible to pair up all the indices $1, ..., l$ so that for each pair $p < q$ with $j_p = j_q = j$, we have $\epsilon_p + \epsilon_q = 0$ and $\phi\left(w_{(p)}\right) = \phi\left(w_{(q)}\right)$. So:

$$\begin{aligned}
0 &= \epsilon_p \phi\left(w_{(p)}\right) + \epsilon_q \phi\left(w_{(p)}\right) \\
&= \tilde{\phi}\left(\epsilon_p w_{(p)} + \epsilon_q w_{(q)}\right) \\
&= \epsilon_q \tilde{\phi}\left(x_{j_1}^{\epsilon_1} \cdots x_{j_{q-1}}^{\epsilon_{q-1}} x_{j_q}^{\frac{\epsilon_q - 1}{2}} - x_{j_1}^{\epsilon_1} \cdots x_{j_{p-1}}^{\epsilon_{p-1}} x_{j_p}^{\frac{\epsilon_p - 1}{2}}\right) \\
&= \epsilon_q \phi\left(x_{j_1}^{\epsilon_1} \cdots x_{j_{q-1}}^{\epsilon_{q-1}} x_{j_q}^{\frac{\epsilon_q - 1}{2}}\right) - \epsilon_q \phi\left(x_{j_1}^{\epsilon_1} \cdots x_{j_{p-1}}^{\epsilon_{p-1}} x_{j_p}^{\frac{\epsilon_p - 1}{2}}\right)
\end{aligned}$$

From here we get the following string of equations:

$$\begin{aligned}
&\phi\left(x_{j_1}^{\epsilon_1} \cdots x_{j_{q-1}}^{\epsilon_{q-1}} x_{j_q}^{\frac{\epsilon_q - 1}{2}}\right) = \phi\left(x_{j_1}^{\epsilon_1} \cdots x_{j_{p-1}}^{\epsilon_{p-1}} x_{j_p}^{\frac{\epsilon_p - 1}{2}}\right) \\
\Rightarrow\ &\phi\left(x_{j_p}^{\frac{1 - \epsilon_p}{2}} x_{j_{p-1}}^{-\epsilon_{p-1}} \cdots x_{j_1}^{-\epsilon_1}\right) \phi\left(x_{j_1}^{\epsilon_1} \cdots x_{j_{q-1}}^{\epsilon_{q-1}} x_{j_q}^{\frac{\epsilon_q - 1}{2}}\right) = 1 \\
\Rightarrow\ &\phi\left(x_{j_p}^{\frac{\epsilon_p + 1}{2}} x_{j_{p+1}}^{\epsilon_{p+1}} \cdots x_{j_{q-1}}^{\epsilon_{q-1}} x_{j_q}^{\frac{\epsilon_q - 1}{2}}\right) = 1
\end{aligned}$$

since all generators are cancelled from j_1 to j_{p-1} (seeing as $p < q$) and $x_{j_p}^{\frac{1 - \epsilon_p}{2}}$

is multiplied with x_j^p. We can remove the first and last factors on the left to obtain:

$$\phi\left(x_{j_{p+1}}^{\epsilon_{p+1}} \cdots x_{j_{q-1}}^{\epsilon_{q-1}}\right) = \phi\left(x_{j_p}^{-\frac{\epsilon_{p+1}}{2}} x_{j_q}^{\frac{1-\epsilon_q}{2}}\right).$$

But $j_p = j_q$ and $\epsilon_p = -\epsilon_q$, so this becomes:

$$\phi\left(x_{j_{p+1}}^{\epsilon_{p+1}} \cdots x_{j_{q-1}}^{\epsilon_{q-1}}\right) = 1$$

and hence $x_{j_{p+1}}^{\epsilon_{p+1}} \cdots x_{j_{q-1}}^{\epsilon_{q-1}} \in N$. Remember, though, that this holds for any generator at all. So we pair up all generator indices $1, ..., l$ into $p < q$ where $x_{j_p} = x_{j_q}$ and $\epsilon_p + \epsilon_q = 0$, resulting in $x_{j_{p+1}}^{\epsilon_{p+1}} \cdots x_{j_{q-1}}^{\epsilon_{q-1}} \in N$. Note that we must always have $q > p + 1$: if $q = p + 1$, then this would contradict Definition 31.

Of these pairs, there must be one $p' < q'$ that is furthest left, that is $q' \leq q$ for all q. Then $p'' = q' - 1$ must be paired with $q'' > q$. Thus, w has the form:

$$w = ax_j^{\epsilon} b x_k^{\eta} x_j^{-\epsilon} c x_k^{-\eta} d$$

taking $x_j^{-\epsilon} = x_{j_{q'}}^{\epsilon_{q'}}$ and $x_k^{\eta} = x_{j_{p''}}^{\epsilon_{p''}}$. Here $bx_k^{\eta} = x_{j_{p'+1}}^{\epsilon_{p'+1}} \cdots x_{j_{q'-1}}^{\epsilon_{q'-1}}$ and $x_j^{-\epsilon} c = x_{j_{p''+1}}^{\epsilon_{p''+1}} \cdots x_{j_{q''-1}}^{\epsilon_{q''-1}}$, so $bx_k^{\eta}, x_j^{-\epsilon} c \in N$. Remembering that $[N, N]$ is a normal subgroup of G:

$$\begin{aligned}
&\left(bx_k^{\eta}\right)\left(x_j^{-\epsilon} c\right)\left(bx_k^{\eta}\right)^{-1}\left(x_j^{-\epsilon} c\right)^{-1} \in [N, N] \\
\Rightarrow &\left(ax_j^{\epsilon}\right)\left(bx_k^{\eta}\right)\left(x_j^{-\epsilon} c\right)\left(bx_k^{\eta}\right)^{-1}\left(x_j^{-\epsilon} c\right)^{-1}\left(ax_j^{\epsilon}\right)^{-1} \in [N, N] \\
\Rightarrow &\left(ax_j^{\epsilon}\right)\left(bx_k^{\eta}\right)\left(x_j^{-\epsilon} c\right)\left(x_k^{-\eta} d\right)\left(x_k^{-\eta} d\right)^{-1}\left(bx_k^{\eta}\right)^{-1}\left(x_j^{-\epsilon} c\right)^{-1}\left(ax_j^{\epsilon}\right)^{-1} \in [N, N] \\
\Rightarrow &\, w(acbd)^{-1} \in [N, N].
\end{aligned}$$

But $[N, N] \subseteq N_{IQ}$ and so $w(acbd)^{-1} \in N_{IQ}$. Seeing as $w \in N_{IQ}$, we must have that $acbd \in N_{IQ}$. Clearly, $l(acbd) < l$ and so by the inductive hypothesis, $acbd \in [N, N]$. Then $w \in [N, N]$ because $w(acbd)^{-1} \in [N, N]$. This completes the induction. □

We finish this section with one final result relating to the product of ideals with the fundamental ideal:

Proposition 20. *Let $u \in X$ and let I be an ideal of $\mathbb{Z}[X]$ that corresponds to a finitely generated normal subgroup $N \trianglelefteq X$. Then $u - 1 \in I$ if and only if there exists $n \in N$ such that $u - n \in IQ$.*

Proof. Again we let ϕ be the group homomorphism such that $N = \ker(\phi)$ and $I = \ker\left(\tilde{\phi}\right)$.

We begin with the backward implication. Suppose that there exists $n \in N$ such that $u-n \in IQ$. Then $u-n \in I$ and so $\tilde{\phi}(u-n) = 0$, i.e. $\phi(u) = \phi(n) = 1$. Thus, $\tilde{\phi}(u-1) = \phi(u) - \phi(1) = 1 - 1 = 0$ and so $u - 1 \in I$.

Now suppose that $u - 1 \in I$. Then, from Proposition 12:

$$u - 1 = \sum_{i=1}^{l} \epsilon_i c_i (p_i - 1) b_i$$

where $\epsilon = \pm 1$, $c_i, b_i \in X$ and $p_i \in N$ for all i. For each i, set $a_i = c_i p_i^{\frac{1-\epsilon_i}{2}} \in X$ and $n_i = p_i^{\epsilon_i} \in N$ so that:

$$\begin{aligned} a_i(n_i - 1) &= c_i p_i^{\frac{1-\epsilon_i}{2}} (p_i^{\epsilon_i} - 1) = c_i p_i^{\frac{\epsilon_i+1}{2}} - c_i p_i^{\frac{1-\epsilon_i}{2}} \\ &= \epsilon_i c_i p_i - \epsilon_i c_i = \epsilon_i c_i (p_i - 1) \end{aligned}$$

meaning that:

$$u - 1 = \sum_{i=1}^{l} a_i (n_i - 1) b_i.$$

Define $n = \prod_{i=1}^{l} a_i n_i a_i^{-1} \in N$. Then:

$$n - 1 = \sum_{i=1}^{l} a_i (n_i - 1) a_i^{-1} \prod_{k=i+1}^{l} a_k n_k a_k^{-1}$$

and so:

$$\begin{aligned} u - n &= (u - 1) - (n - 1) \\ &= \sum_{i=1}^{l} a_i (n_i - 1) b_i - \sum_{i=1}^{l} a_i (n_i - 1) a_i^{-1} \prod_{k=i+1}^{l} a_k n_k a_k^{-1} \\ &= \sum_{i=1}^{l} a_i (n_i - 1) \left(b_i - a_i^{-1} \prod_{k=i+1}^{l} a_k n_k a_k^{-1} \right). \end{aligned}$$

But for each i, $a_i(n_i - 1) \in I$ since $n_i - 1 \in I$ and $b_i - a_i^{-1} \prod_{k=i+1}^{l} a_k n_k a_k^{-1} \in Q$ since all involved quantities are from the group. Therefore, $u - n \in IQ$. $\square$

3.4 Commutator Results

We end our review of [7] by presenting a selection of results related to the commutators of free group elements. Firstly:

Proposition 21. *For any $n \geq 2$, if $w \in X_n$, then $D_{j_r \cdots j_1}(w)(1) = 0$ for $r = 1, 2, ..., n-1$ and if $u, v \in X_n$, then $D_{j_n \cdots j_1}(uv)(1) = D_{j_n \cdots j_1}(u)(1) + D_{j_n \cdots j_1}(v)(1)$.*

The original paper [7] claims that this statement holds for any $n \geq 1$, however, we believe that the first part of the statement does not hold for $n = 1$. It is not entirely clear what it would even mean in this case, however, we err on the side of caution and so simply restrict the statement to $n \geq 2$.

Proof. We use induction on n. Let $n = 2$. It is sufficient to prove the statement for $w = [u, v]$ for some $u, v \in X$. Then, as stated in the proof of Proposition 19:

$$D_j(w) = \left(1 - uvu^{-1}\right) D_j(u) + \left(u - uvu^{-1}v^{-1}\right) D_j(v)$$

and so $D_j(w)(1) = 0$.

Now, for any $u, v \in X_2$, by Equation (3.8):

$$\begin{aligned} D_{j_2 j_1}(uv) &= D_{j_2 j_1}(u) \cdot v(1) + D_{j_2}(u) \cdot D_{j_1}(v)(1) + u \cdot D_{j_2 j_1}(v) \\ \Rightarrow D_{j_2 j_1}(uv)(1) &= D_{j_2 j_1}(u)(1) + D_{j_2}(u)(1) D_{j_1}(v)(1) + D_{j_2 j_1}(v)(1) \end{aligned}$$

But by the first part which we have already proved, $D_{j_2}(u)(1) = D_{j_1}(v)(1) = 0$, so:

$$D_{j_2 j_1}(uv)(1) = D_{j_2 j_1}(u)(1) + D_{j_2 j_1}(v)(1).$$

Now let $n > 2$ and assume that the statement holds for $2, ..., n-1$. Let $w \in X_n$. Again, it is sufficient to consider only $w = [u, v]$ where $u \in X_{n-1}$ and $v \in X$. Then for any $r = 1, ..., n-1$:

$$\begin{aligned} D_{j_r \cdots j_1}(uv) &= \sum_{i=1}^{r} D_{j_r \cdots j_i}(u) \cdot D_{j_{i-1} \cdots j_1}(v)(1) + u \cdot D_{j_r \cdots j_1}(v) \\ \Rightarrow D_{j_r \cdots j_1}(uv)(1) &= \sum_{i=1}^{r} D_{j_r \cdots j_i}(u)(1) D_{j_{i-1} \cdots j_1}(v)(1) + u(1) D_{j_r \cdots j_1}(v)(1) \\ &= D_{j_r \cdots j_i}(u)(1) + D_{j_r \cdots j_1}(v)(1) \end{aligned}$$

by the inductive hypothesis. Also, $wvu = uv$ and so:

$$D_{j_r \cdots j_1}(wvu)(1) = D_{j_r \cdots j_i}(u)(1) + D_{j_r \cdots j_1}(v)(1).$$

But, again using the inductive hypothesis:

$$\begin{aligned} D_{j_r \cdots j_1}(wvu) &= \sum_{i=1}^{r} D_{j_r \cdots j_i}(wv) \cdot D_{j_{i-1} \cdots j_1}(u)(1) + wv \cdot D_{j_r \cdots j_1}(u) \\ &= D_{j_r \cdots j_1}(wv) \cdot u(1) + wv \cdot D_{j_r \cdots j_1}(u) \end{aligned}$$

and:

$$D_{j_r \cdots j_1}(wv) = \sum_{i=1}^{r} D_{j_r \cdots j_i}(w) \cdot D_{j_{i-1} \cdots j_1}(v)(1) + w \cdot D_{j_r \cdots j_1}(v)$$

meaning that:

$$D_{j_r \cdots j_1}(wvu) = \sum_{i=1}^{r} D_{j_r \cdots j_i}(w) \cdot D_{j_{i-1} \cdots j_1}(v)(1) + w \cdot D_{j_r \cdots j_1}(v) + wv \cdot D_{j_r \cdots j_1}(u).$$

Therefore:

$$\begin{aligned} D_{j_r \cdots j_1}(wvu)(1) =& \sum_{i=1}^{r} D_{j_r \cdots j_i}(w)(1) D_{j_{i-1} \cdots j_1}(v)(1) \\ &+ w(1) D_{j_r \cdots j_1}(v)(1) + w(1)v(1) D_{j_r \cdots j_1}(u)(1) \\ =& D_{j_r \cdots j_1}(w)(1) + D_{j_r \cdots j_1}(v)(1) + D_{j_r \cdots j_1}(u)(1) \end{aligned}$$

since $w \in X_n \subseteq X_{n-1}$ and so from the inductive hypothesis, $D_{j_r \cdots j_i}(w)(1) = 0$ unless perhaps $i = 1$. So, in summary:

$$D_{j_r \cdots j_1}(w)(1) + D_{j_r \cdots j_1}(v)(1) + D_{j_r \cdots j_1}(u)(1) = D_{j_r \cdots j_i}(u)(1) + D_{j_r \cdots j_1}(v)(1)$$

meaning that:

$$D_{j_r \cdots j_1}(w)(1) = 0$$

for any $r = 1, ..., n-1$. Thus, the first part of the proposition is proved. Proving the second part for arbitrary n is extremely similar to proving it for $n = 2$ and so we do not need to do this explicitly. □

The paper then presents the claim that for $u \in X_n$ and $v \in X_q$:

$$D_{j_{n+q}\cdots j_1}([u,v])(1) = D_{j_{n+q}\cdots j_{n+1}}(u)(1)D_{j_q\cdots j_1}(v)(1) - D_{j_{n+q}\cdots j_{q+1}}(v)(1)D_{j_n\cdots j_1}(u)(1).$$

This strikes us as strange, though. There are various equations involving summing over different orders of derivatives and since $u \in X_n$ and $v \in X_q$, all derivatives of order $1, ..., n-1$ and $1, ..., q-1$ of u and v respectively "vanish at $x = 1$." For this reason it would make intuitive sense if the only remaining terms on the right-hand side of the above equation were to involve n^{th}-order and q^{th}-order derivatives of u and v respectively. But it does not. A more intuitive version of the equation would be:

$$D_{j_{n+q}\cdots j_1}([u,v])(1) = D_{j_{n+q}\cdots j_{q+1}}(u)(1)D_{j_q\cdots j_1}(v)(1) - D_{j_{n+q}\cdots j_{n+1}}(v)(1)D_{j_n\cdots j_1}(u)(1).$$

The equation as stated in the paper also does not follow from the equations used in the proof from the paper.

Lastly, we generalise the following equation:

$$[u, vw] = [u, v][u, w]^v. \tag{3.15}$$

This can easily be seen to be true. For the following, we will say $u^{-v} = (u^v)^{-1}$. We generalise Equation 3.15 as:

Proposition 22. *If $u \in X$ and $v = \prod_{i=1}^{l} x_{j_i}^{\epsilon_i}$, then $[u, v] = \prod_{i=1}^{l} [u, x_{j_i}]^{\epsilon_i v_{(i)}}$.*

Proof. If $\epsilon_i = 1$, then $[u, x_{j_i}]^{\epsilon_i v_{(i)}} = [u, x_{j_i}]^{x_{j_1}^{\epsilon_1}\cdots x_{j_{i-1}}^{\epsilon_{i-1}}}$. But if $\epsilon_i = -1$:

$$\begin{aligned}
[u, x_{j_i}]^{\epsilon_i v_{(i)}} &= [u, x_{j_i}]^{-x_{j_1}^{\epsilon_1}\cdots x_{j_i}^{\epsilon_i}} = \left(x_{j_1}^{\epsilon_1}\cdots x_{j_i}^{-1} u x_{j_i} u^{-1} x_{j_i}^{-1} x_{j_i}\cdots x_{j_1}^{-\epsilon_1}\right)^{-1} \\
&= x_{j_1}^{\epsilon_1}\cdots x_{j_{i-1}}^{\epsilon_{i-1}} u x_{j_i}^{-1} u^{-1} x_{j_i} x_{j_{i-1}}^{-\epsilon_{i-1}}\cdots x_{j_1}^{-\epsilon_1} \\
&= \left[u, x_{j_i}^{-1}\right]^{x_{j_1}^{\epsilon_1}\cdots x_{j_{i-1}}^{\epsilon_{i-1}}}.
\end{aligned}$$

So, irrespective of the value of ϵ_i, we find that $[u, x_{j_i}]^{\epsilon_i v_{(i)}} = \left[u, x_{j_i}^{\epsilon_i}\right]^{x_{j_1}^{\epsilon_1}\cdots x_{j_{i-1}}^{\epsilon_{i-1}}}$. Thus:

$$\prod_{i=1}^{l} [u, x_{j_i}]^{\epsilon_i v_{(i)}} = \prod_{i=1}^{l} \left[u, x_{j_i}^{\epsilon_i}\right]^{x_{j_1}^{\epsilon_1}\cdots x_{j_{i-1}}^{\epsilon_{i-1}}}$$

$$
\begin{aligned}
&= \left(u x_{j_1}^{\epsilon_1} u^{-1} x_{j_1}^{-\epsilon_1}\right) \cdot \left(x_{j_1}^{\epsilon_1} u x_{j_2}^{\epsilon_2} u^{-1} x_{j_2}^{-\epsilon_2} x_{j_1}^{-\epsilon_1}\right) \cdots \\
&\quad \left(x_{j_1}^{\epsilon_1} \cdots x_{j_{l-1}}^{\epsilon_{l-1}} u x_{j_l}^{\epsilon_l} u^{-1} x_{j_l}^{-\epsilon_l} x_{j_{l-1}}^{-\epsilon_{l-1}} \cdots x_{j_1}^{-\epsilon_1}\right) \\
&= u x_{j_1}^{\epsilon_1} \cdots x_{j_l}^{\epsilon_l} u^{-1} x_{j_l}^{-\epsilon_l} \cdots x_{j_1}^{-\epsilon_1} \\
&= \left[u, x_{j_1}^{\epsilon_1} \cdots x_{j_l}^{\epsilon_l}\right] = [u, v]. \qquad \square
\end{aligned}
$$

Chapter 4

Review of Category Theory

We now briefly move to category theory, a very general approach to mathematical structures. This will be useful in our discussions of the existing research. We must begin with some necessary definitions.

In our approach we will be using **classes**, a notion similar to sets. Classes are defined as in Von Neumann-Bernays-Gödel set theory. The axiomatic definition is lengthy and will therefore not be given here. Suffice it to say that a class is a collection of objects defined by a property that all its members share. Classes resolve the paradoxes that arise while working with sets by working with "layers" of set theory. We cannot have a set of all sets, but there exists a class of all sets. Furthermore, there is a superclass of all classes and so on. Classes are not more general than sets in the sense that we still cannot have a class of all classes. Note that all sets are classes but some classes are not sets. These are called **proper classes**.

With this notion of classes in mind, we can define categories. For the Definitions 37 to 39 we follow [9]:

Definition 37. *A* ***category*** $\mathbf{C}$ *has a class of objects* $\mathrm{Obj}(\mathbf{C})$ *along with a class of morphisms* $\mathrm{Mor}(\mathbf{C})$ *(also denoted by* $\mathrm{Hom}(\mathbf{C})$*) between these objects. There must exist a well-defined domain function* $\mathrm{dom} : \mathrm{Mor}(\mathbf{C}) \to \mathrm{Obj}(\mathbf{C})$ *and codomain function* $\mathrm{cod} : \mathrm{Mor}(\mathbf{C}) \to \mathrm{Obj}(\mathbf{C})$*. For all* $a, b \in \mathrm{Obj}(\mathbf{C})$*, we require that there exists a set* $\mathrm{Mor}(a, b)$ *of all morphisms* $f \in \mathrm{Mor}(\mathbf{C})$ *with* $\mathrm{dom}(f) = a$ *and* $\mathrm{cod}(f) = b$*. Further, we must have a composition of morphisms in* $\mathbf{C}$ $\circ : \mathrm{Mor}(b, c) \times \mathrm{Mor}(a, b) \to \mathrm{Mor}(a, c)$ *for any* $a, b, c \in \mathrm{Obj}(\mathbf{C})$*.*

Lastly, a category must satisfy associativity of composition and have identity

morphisms in the following sense:

1. *For any objects* $a, b, c, d \in \mathrm{Obj}(\mathbf{C})$*, if* $f \in \mathrm{Mor}(a, b)$*,* $g \in \mathrm{Mor}(b, c)$ *and* $h \in \mathrm{Mor}(c, d)$*, then* $h \circ (g \circ f) = (h \circ g) \circ f$*.*
2. *For every* $x \in \mathrm{Obj}(\mathbf{C})$*, there exists a morphism* $\mathrm{Id}_x \in \mathrm{Mor}(x, x)$ *such that for all* $a, b \in \mathrm{Obj}(\mathbf{C})$*,* $f \circ \mathrm{Id}_x = f$ *for any* $f \in \mathrm{Mor}(x, a)$ *and* $\mathrm{Id}_x \circ g = g$ *for any* $g \in \mathrm{Mor}(b, x)$*.*

One example of a category would be $\mathbf{G}$, the category of all groups with $\mathrm{Obj}(\mathbf{G})$ being the class of all groups and $\mathrm{Mor}(\mathbf{G})$ the class of all group homomorphisms.

With the notion of a category established, we introduce some relevant concepts within category theory, following [14]. Firstly, we define homomorphisms of categories:

Definition 38. *Given two categories* $\mathbf{C_1}$ *and* $\mathbf{C_2}$*, a* ***functor*** *from* $\mathbf{C_1}$ *to* $\mathbf{C_2}$ *is a pair of mappings* $(F, F') : \mathbf{C_1} \to \mathbf{C_2}$ *with* $F : \mathrm{Obj}(\mathbf{C_1}) \to \mathrm{Obj}(\mathbf{C_2})$ *and* $F' : \mathrm{Mor}(\mathbf{C_1}) \to \mathrm{Mor}(\mathbf{C_2})$ *that preserves domain and codomain, identity and composition. That is, for all* $a \in \mathrm{Obj}(\mathbf{C_1})$ *and* $f, g \in \mathrm{Mor}(\mathbf{C_1})$*:*

$$\begin{aligned} F(a) &\in \mathrm{Obj}(\mathbf{C_2}), \\ F'(f) &\in \mathrm{Mor}(\mathbf{C_2}), \\ F'(f) &\in \mathrm{Mor}(F(\mathrm{dom}(f)), F(\mathrm{cod}(f))), \\ F'(\mathrm{Id}_a) &= \mathrm{Id}_{F(a)}, \\ F'(g \circ f) &= F'(g) \circ F'(f), \end{aligned}$$

whenever the composition $g \circ f$ *is admitted.*

It is natural to consider an isomorphism of categories to be a functor which is bijective on objects and morphisms.

Category theory further introduces a generalisation of disjoint unions, known as the **coproduct**. This is denoted by $a \coprod b$ for objects a and b. As noted, this is a generalisation, however, for our purposes the only coproduct we will consider is the disjoint union. Therefore, we will not provide the lengthy formal definition.

4.1 The Groupoid of the Adjoint Action

Definition 39. *A **groupoid** is a category in which every morphism is invertible, that is for every morphism $f : a \to b$ there exists a morphism $f^{-1} : b \to a$ such that $f^{-1} \circ f = \mathrm{Id}_a$ and $f \circ f^{-1} = \mathrm{Id}_b$.*

Many different categories are in fact groupoids, however, we are focusing on groupoids defined by means of group actions:

Definition 40. *Given a group G and a set X, a (left) group action of G on X is an operation $* : G \times X \to X$ such that for all $g, h \in G$ and $x \in X$:*

$$e_G * x = x,$$
$$g * (h * x) = (gh) * x.$$

We can of course consider an action of a group G on itself. We can then construct a groupoid Γ using a finitely generated discrete group G and an action $*$ on itself: we define $\mathrm{Obj}(\Gamma) = G$ and for each $a, b \in G$ we set $\mathrm{Mor}(a, b) = \{g \in G : g * a = b\}$, defining $\mathrm{Mor}(\Gamma) = \coprod_{a,b \in G} \mathrm{Mor}(a, b)$. This means that we are considering morphisms $g \in \mathrm{Mor}(a, b)$ to be arrows $a \xrightarrow{g} b$ where $g * a = b$. The composition of $g \in \mathrm{Mor}(a, b)$ and $h \in \mathrm{Mor}(b, c)$ is $hg \in \mathrm{Mor}(a, c)$. Note that in this case we must have $hg \in \mathrm{Mor}(a, c)$ since $(hg) * a = h * (g * a) = h * b = c$.

Then each morphism in Γ is invertible: for any $g \in \mathrm{Mor}(a, b)$, we have that $g^{-1} \in \mathrm{Mor}(b, a)$ since $g^{-1} * b = g^{-1} * (g * a) = (g^{-1}g) * a = a$. Clearly, $g^{-1}g = e_G = gg^{-1}$ and e_G is the identity morphism for both a and b. Therefore, g^{-1} is the morphism inverse of g.

We focus one particular such groupoid, namely the groupoid of the adjoint action, that is $g * a = gag^{-1}$. In this case, $g * a = b$ if and only if $ga = bg$. Here we provide a rigorous definition of this category as described in [3]:

Definition 41. *The **groupoid of the adjoint action on G** is a category Γ with objects $\mathrm{Obj}(\Gamma) = G$. The set of morphisms with domain $a \in G$ and codomain $b \in G$ is as follows:*

$$\mathrm{Mor}(a, b) = \{g \in G : ga = bg\}.$$

We use the notation $\left(\frac{a \to b}{g}\right)$ to denote a morphism $g \in \mathrm{Mor}(a, b)$. This distin-

guishes between $\left(\frac{a\to b}{g}\right)$ *and* $\left(\frac{c\to d}{g}\right)$ *in a case where* $ga = bg$ *and* $gc = dg$*. Like this, we can define the set of all morphisms on* Γ *as the disjoint union:*

$$\mathrm{Mor}(\Gamma) = \coprod_{a,b\in G} \mathrm{Mor}(a, b).$$

Composition of morphisms is defined by:

$$\left(\frac{b\to c}{h}\right) \circ \left(\frac{a\to b}{g}\right) = \left(\frac{a\to c}{hg}\right)$$

for all $a, b, c, g, h \in G$ *where* $ga = bg$ *and* $hb = ch$.[1] *For each* $a \in \mathrm{Obj}(\mathbf{\Gamma})$*, the identity morphism is given by* $\mathrm{Id}_a = \left(\frac{a\to a}{e}\right)$.

This is indeed a groupoid: for any $\left(\frac{a\to b}{g}\right) \in \mathrm{Mor}(\Gamma)$ the inverse is given by $\left(\frac{b\to a}{g^{-1}}\right)$. Note also that $\mathrm{Mor}(a, b)$ is non-empty if and only if a and b belong to the same conjugacy class.

Definition 42. *A morphism* $\xi \in \mathrm{Mor}(\Gamma)$ *is a* ***loop*** *if its domain and codomain are equal, that is* $\xi \in \mathrm{Mor}(a, a)$ *for some* $a \in G$.

With the above in mind, we can construct subgroupoids of Γ: for any $u \in G$, we define the subgroupoid $\Gamma_{[u]}$ as the category with objects $\mathrm{Obj}\left(\Gamma_{[u]}\right) = [u]$ and morphisms $\mathrm{Mor}\left(\Gamma_{[u]}\right) = \left\{\left(\frac{a\to b}{g}\right) \in \mathrm{Mor}(\Gamma) : a, b \in [u], g \in G\right\}$, where $[u]$ is the conjugacy class of u as in Definition 5.

Note 20. *The groupoid can be decomposed into a disjoint union of subgroupoids as follows:*

$$\mathrm{Obj}\left(\Gamma\right) = \coprod_{[u]\in[G]} \mathrm{Obj}\left(\Gamma_{[u]}\right),$$
$$\mathrm{Mor}\left(\Gamma\right) = \coprod_{[u]\in[G]} \mathrm{Mor}\left(\Gamma_{[u]}\right)$$

where $[G] = \{[u] : u \in G\}$.

This decomposition is fairly straightfoward. The one point to explain explicitly is that the union of all classes $\mathrm{Mor}\left(\Gamma_{[u]}\right)$ indeed covers all of $\mathrm{Mor}(\Gamma)$: we cannot have any morphism $\left(\frac{a\to b}{g}\right)$ that is not a member of some class $\mathrm{Mor}(\Gamma_{[u]})$. This is because $a = eae^{-1}$ and $b = gag^{-1}$, so $a, b \in [a]$, i.e. $\left(\frac{a\to b}{g}\right) \in \mathrm{Mor}(\Gamma_{[a]})$.

Further, for each $u \in G$ we can define a subgroupoid $\mathrm{Mor}(u, u)$ with morphisms $\mathrm{Mor}(u, u)$ and the solitary object u. Note that every morphism in this

[1] This guarantees that $hga = hbg = chg$.

subgroupoid will have the form $\left(\frac{u\to u}{g}\right)$ where g commutes with u. We will denote by $Z(u)$ the set of all group elements that commute with u. Further, we will denote by $Z(G)$, the group of all elements that commute with every element in G, known as the **centre** of G:

$$Z(u) = \{g \in G : gu = ug\}, \tag{4.1}$$

$$Z(G) = \{g \in G : gu = ug, \forall u \in G\}. \tag{4.2}$$

Note that $Z(u)$ and $Z(G)$ are both subgroups of G.

We now introduce a type of function on Γ analogous to a homomorphism:

Definition 43. *A mapping $T : \mathrm{Mor}(\Gamma) \to \mathbb{C}$ is a **character** on Γ if $T(\eta\circ\xi) = T(\eta) + T(\xi)$ for all $\eta, \xi \in \mathrm{Mor}(\Gamma)$ admitting the composition $\eta \circ \xi$.*

Note 21. *If T is a character on Γ, then for any $a \in G$, $T\left(\frac{a\to a}{e}\right) = 0$. This is because $\left(\frac{a\to a}{e}\right) = Id_a$ and so for any morphism ξ admitting the composition $\xi \circ \left(\frac{a\to a}{e}\right)$:*

$$T(\xi) = T\left(\xi \circ \left(\frac{a \to a}{e}\right)\right) = T(\xi) + T\left(\frac{a \to a}{e}\right).$$

Definition 44. *We set $H_g = \left\{\left(\frac{a\to b}{g}\right) \in \mathrm{Mor}(\Gamma) : a \in G, b = gag^{-1}\right\}$ for each $g \in G$. A function $T : \mathrm{Mor}(\Gamma) \to \mathbb{C}$ is said to be **locally finitely supported** if for all $g \in G$, $T|_{H_g} : H_g \to \mathbb{C}$ is finitely supported. A subscript f is used to denote the restriction of any set of functions to locally finitely supported functions.*

The set of all characters on Γ is denoted $T(\Gamma)$. Following Definition 44, $T_f(\Gamma)$ denotes the set of all locally finitely supported characters on Γ. On $T(\Gamma)$ we define addition and scalar multiplication over $\mathbb{C}$ pointwise, just as was done with derivations in Section 2. With these in mind we obtain the following result:

Note 22. *$T(\Gamma)$ is a vector space over $\mathbb{C}$ with pointwise addition and scalar multiplication. Likewise, $T_f(\Gamma)$ is also a vector space over $\mathbb{C}$.*

The proof of this result is very straightforward, defining identity and additive inverses in the same way as was done for derivations.

4.1.1 Characters of Subgroupoids

We can consider the characters of subgroupoids as well, defined in exactly the same way but only taking in morphisms from these subgroupoids. This is useful because of the following:

Proposition 23. *Every character T on a subgroupoid $\Gamma_{[u]}$ or $\mathrm{Mor}(u,u)$ can be extended to a character T' on Γ. Moreover, every locally finitely supported character on $\Gamma_{[u]}$ can be extended to a locally finitely supported character on Γ.*

Proof. In the case of a character T on $\Gamma_{[u]}$ this is done by simply setting $T'(\xi) = 0$ for all morphisms ξ not in $\mathrm{Mor}\left(\Gamma_{[u]}\right)$. To see that this works, consider morphisms $\xi, \eta \in \mathrm{Mor}(\Gamma)$ such that $\eta \circ \xi$ exists. We will let $\xi = \left(\frac{a \to b}{g}\right)$ and $\eta = \left(\frac{b \to c}{h}\right)$. Consider two cases:

Case 1: $\boldsymbol{\xi \in \mathrm{Mor}(\Gamma_{[u]})}$. Then $a, b \in [u]$ and so $b = kuk^{-1}$ for some $k \in G$. Thus, $c = hbh^{-1} = hkuk^{-1}h^{-1} = (hk)u(hk)^{-1}$, i.e. $c \in [u]$. Therefore, $\eta, \eta \circ \xi \in \mathrm{Mor}(\Gamma_{[u]})$ and so:

$$T'(\eta \circ \xi) = T(\eta \circ \xi) = T(\eta) + T(\xi) = T'(\eta) + T'(\xi)$$

by assumption.

Case 2: $\boldsymbol{\xi \notin \mathrm{Mor}(\Gamma_{[u]})}$. Then $\xi \in \mathrm{Mor}(\Gamma_{[v]})$ for some $v \notin [u]$. By the logic used in Case 1, $\eta \in \mathrm{Mor}(\Gamma_{[v]})$ as well and hence $\eta \circ \xi \in \mathrm{Mor}(\Gamma_{[v]})$. So, $\xi, \eta, \eta \circ \xi \notin \mathrm{Mor}(\Gamma_{[u]})$. Thus, $T'(\eta \circ \xi) = 0 = T'(\eta) + T'(\xi)$.

Thereby, this extension of T is a character on Γ. If T is a locally finitely supported character on $\Gamma_{[u]}$, then obviously the extension will also be locally finitely supported on Γ since we set $T'(\xi) = 0$ for all new morphisms ξ, meaning that the support is unchanged.

In the case of a character T of $\mathrm{Mor}(u,u)$ the extension is slightly more involved. First we extend it to $\Gamma_{[u]}$ and then extend further to Γ using the method already described above:

For any $\left(\frac{a \to b}{g}\right) \in \mathrm{Mor}(\Gamma_{[u]})$, we must have that $a = g_a u g_a^{-1}$ and $b = g_b u g_b^{-1}$ for some $g_a, g_b \in G$. Using these elements, we set:

$$T'\left(\frac{a \to b}{g}\right) = T\left(\frac{u \to u}{g_b^{-1} g g_a}\right).$$

To show that this is indeed an extension of T from $\mathrm{Mor}(u,u)$ to $\Gamma_{[u]}$, we must

first determine whether T' is well-defined. For any $\left(\frac{a\to b}{g}\right) \in \mathrm{Mor}(\Gamma_{[u]})$, these g_a, g_b must exist and be unique. Further, $ga = bg$ and so:

$$\begin{aligned} gg_a u g_a^{-1} &= g_b u g_b^{-1} g \\ \text{so that} \quad g_b^{-1} g g_a u &= u g_b^{-1} g g_a. \end{aligned}$$

Thereby, $\left(\frac{u\to u}{g_b^{-1}gg_a}\right)$ exists in $\mathrm{Mor}(u,u)$ and so $T\left(\frac{u\to u}{g_b^{-1}gg_a}\right)$ is defined and unique. Thus, T' is well-defined on $\Gamma_{[u]}$.

Now we show that T' is indeed an extension of T, i.e. that $T'(\xi) = T(\xi)$ for all $\xi \in \mathrm{Mor}(u,u)$. Let $\xi = \left(\frac{u\to u}{g}\right) \in \mathrm{Mor}(u,u)$. Then $gu = ug$ and so $u = gug^{-1}$. Therefore, $g_u = g$ and consequently:

$$T'(\xi) = T\left(\frac{u\to u}{g_u^{-1}gg_u}\right) = T\left(\frac{u\to u}{g}\right) = T(\xi).$$

Lastly, we must prove that T' is a character on $\mathrm{Mor}(\Gamma_{[u]})$. Let $\xi, \eta \in \mathrm{Mor}(\Gamma_{[u]})$ such that $\eta \circ \xi$ exists. We can let $\xi = \left(\frac{a\to b}{g}\right)$ and $\eta = \left(\frac{b\to c}{h}\right)$. Then:

$$\begin{aligned} T'(\eta\circ\xi) &= T'\left(\frac{a\to c}{hg}\right) \\ &= T\left(\frac{u\to u}{g_c^{-1}hgg_a}\right) \\ &= T\left(\left(\frac{u\to u}{g_c^{-1}hg_b}\right)\circ\left(\frac{u\to u}{g_b^{-1}gg_a}\right)\right) \\ &= T\left(\frac{u\to u}{g_c^{-1}hg_b}\right) + T\left(\frac{u\to u}{g_b^{-1}gg_a}\right) \\ &= T'(\eta) + T'(\xi). \end{aligned}$$

Thus, T' is indeed an extension of T which is a character on $\Gamma_{[u]}$. Setting $T'(\xi) = 0$ for all $\xi \in \mathrm{Mor}(\Gamma)\setminus \mathrm{Mor}(\Gamma_{[u]})$, we will have an extension of T which is a character on all of Γ. □

Note 23. *For each $u \in G$ we have that $T_f(\mathrm{Mor}(u,u)) = T(\mathrm{Mor}(u,u))$ since every character of $\mathrm{Mor}(u,u)$ is trivially locally finitely supported based on Definition 44.*

Note 24. *For any $X \in T(\Gamma)$, X can be written as a sum of characters as follows:*

$$X = \sum_{[u]\in[G]} \left(X|_{\mathrm{Mor}\left(\Gamma_{[u]}\right)}\right)'$$

using the notation from above for extending a character from $\Gamma_{[u]}$ *to* Γ.

Proposition 23 means that we could equivalently consider $T\left(\Gamma_{[u]}\right)$ as the set of all characters of Γ whose support is contained entirely within $\mathrm{Mor}\left(\Gamma_{[u]}\right)$:

$$T\left(\Gamma_{[u]}\right) = \left\{X \in T(\Gamma) : X(\xi) = 0, \quad \forall \xi \notin \mathrm{Mor}\left(\Gamma_{[u]}\right)\right\}, \tag{4.3}$$

$$T_f\left(\Gamma_{[u]}\right) = \left\{X \in T_f(\Gamma) : X(\xi) = 0, \quad \forall \xi \notin \mathrm{Mor}\left(\Gamma_{[u]}\right)\right\}. \tag{4.4}$$

This formulation identifies each character of $\Gamma_{[u]}$ with its extension to Γ. Within this formulation, Note 24 tells us that every character on Γ can be written as the sum of characters from subgroupoids of Γ. Furthermore, it is obvious that any sum of characters on subgroupoids must be a character on Γ. Thus, following Equation (4.3) we obtain:

$$T(\Gamma) = \bigoplus_{[u]\in[G]} T\left(\Gamma_{[u]}\right). \tag{4.5}$$

as in [2]. We can make a similar but weaker statement for $T_f(\Gamma)$:

$$T_f(\Gamma) \subseteq \bigoplus_{[u]\in[G]} T_f\left(\Gamma_{[u]}\right). \tag{4.6}$$

This is because every locally finitely supported character can be written as the sum of locally finitely supported characters of subgroupoids as in Note 24, however, such a sum is not guaranteed to be locally finitely supported. Note that Inequality (4.6) will become an equation if $[G]$ is finite.

4.1.2 Different Representation of Groupoid

It is worth noting that a different presentation of Γ is used in [2]. We will denote this groupoid by Γ'. Here the objects are still simply the elements of G, however, the morphisms are given by $\mathrm{Mor}(\Gamma') = \{(g,h) : g,h \in G\}$ with $\mathrm{dom}(g,h) = h^{-1}g$ and $\mathrm{cod}(g,h) = gh^{-1}$. So:

$$\mathrm{Hom}(a,b) = \{(g,h) \in \mathrm{Mor}(\Gamma') : \mathrm{dom}(g,h) = a, \mathrm{cod}(g,h) = b\}$$

for all $a, b \in G$. Composition of morphisms is given by:

$$(g_2,h_2) \circ (g_1,h_1) = (h_2g_1, h_2h_1)$$

whenever $g_1 h_1^{-1} = h_2^{-1} g_2$. Based on this, $\mathrm{Id}_g = (g, e)$ for each $g \in G$. Subgroupoids can be constructed in the same way as in the previous formulation.

This formulation of the groupoid appears different, but it is in fact equivalent: $\Gamma' \cong \Gamma$ by way of the isomorphism (i.e. bijective functor) $(F, F') : \Gamma' \to \Gamma$ given by:

$$\begin{aligned} F(g) &= g && \forall g \in \mathrm{Obj}(\Gamma'), \\ F'(g,h) &= \left(\frac{h^{-1} g \to g h^{-1}}{h} \right) && \forall (g,h) \in \mathrm{Mor}(\Gamma'). \end{aligned}$$

First we will show that F and F' are both bijections. It is obvious that F is bijective, being the identity mapping. It is also obvious that F' is well-defined. Now suppose that $F'(g_1, h_1) = F'(g_2, h_2)$ for some $(g_1, h_1), (g_2, h_2) \in \mathrm{Mor}(\Gamma')$. Then:

$$\left(\frac{h_1^{-1} g_1 \to g_1 h_1^{-1}}{h_1} \right) = \left(\frac{h_2^{-1} g_2 \to g_2 h_2^{-1}}{h_2} \right),$$

meaning that $h_1^{-1} g_1 = h_2^{-1} g_2$, $g_1 h_1^{-1} = g_2 h_2^{-1}$ and $h_1 = h_2$. We can substitute the last of these three equations into the first to find that $g_1 = g_2$. Therefore, $(g_1, h_1) = (g_2, h_2)$. Thus, F' is injective.

Lastly, suppose that $\left(\frac{a \to b}{g} \right) \in \mathrm{Mor}(\Gamma)$. Then $(ga, g) \in \mathrm{Mor}(\Gamma')$ and:

$$F'(ga, g) = \left(\frac{g^{-1} g a \to g a g^{-1}}{g} \right) = \left(\frac{a \to b g g^{-1}}{g} \right) = \left(\frac{a \to b}{g} \right).$$

Thus, F' is surjective. We have hence shown that F' is indeed a bijection.

We can now show that (F, F') is a functor. First, let $(g, h) \in \mathrm{Mor}(\Gamma')$. Then $\mathrm{dom}(g, h) = h^{-1} g$ and $\mathrm{cod}(g, h) = g h^{-1}$. Obviously, $\mathrm{dom}(F'(g, h)) = h^{-1} g$ and $\mathrm{cod}(F'(g, h)) = g h^{-1}$ and so (F, F') preserves domain and codomain. Now let $k \in \mathrm{Obj}(\Gamma')$. Then $F'(\mathrm{Id}_k) = F'(k, e) = \left(\frac{k \to k}{e} \right) = \mathrm{Id}_k = \mathrm{Id}_{F(k)}$. Hence, (F, F') preserves identity. It now remains only to show that (F, F') preserves composition. To this end, let $(g_1, h_1), (g_2, h_2) \in \mathrm{Mor}(\Gamma')$ such that $(g_2, h_2) \circ (g_1, h_1)$ exists. Then $g_1 h_1^{-1} = h_2^{-1} g_2$ and so:

$$\begin{aligned} F((g_2, h_2) \circ (g_1, h_1)) &= F(h_2 g_1, h_2 h_1) \\ &= \left(\frac{(h_2 h_1)^{-1} h_2 g_1 \to h_2 g_1 (h_2 h_1)^{-1}}{h_2 h_1} \right) \end{aligned}$$

$$
\begin{aligned}
&= \left(\frac{h_1^{-1} g_1 \to h_2 g_1 h_1^{-1} h_2^{-1}}{h_2 h_1} \right) \\
&= \left(\frac{h_1^{-1} g_1 \to g_2 h_2^{-1}}{h_2 h_1} \right) \\
&= \left(\frac{h_2^{-1} g_2 \to g_2 h_2^{-1}}{h_2} \right) \circ \left(\frac{h_1^{-1} g_1 \to g_1 h_1^{-1}}{h_1} \right) \\
&= F(g_2, h_2) \circ F(g_1, h_1).
\end{aligned}
$$

Thus, (F, F') is a functor and consequently an isomorphism.

This second representation of the groupoid is arguably more elegant because we only require two elements from G to describe a morphism, however, the clunky calculations needed to determine the domain and codomain of a morphism make this the far less intuitive representation.

Chapter 5

Derivations of $\mathbb{C}[G]$

Having introduced the groupoid of the adjoint action of G and the notion of characters, we can now show how this connects surprisingly well to the derivations of the group algebra $\mathbb{C}[G]$. In this chapter we will follow the approach from [3], also presenting some ideas from [2]. Our review of these papers will be less thorough than the review of [7] in Chapter 3: we will be particularly orientated around the goal of understanding the derivations and determining non-inner derivations and so will not consider every single result from these papers. Particularly in the case of [2] much of the paper considers specific examples of groups or types of group, whereas we are more interested in the general case. We will not consider the vast majority of these examples.

Here we consider derivations in the simplest way, i.e. following Equations (1.1) and (1.2). We will be more general than in Chapter 3 in terms of which groups we consider: there most of our working used the free group X, whereas here we will consider G to be any finitely generated discrete group. Note also that our group algebra is taken over $\mathbb{C}$ rather than $\mathbb{Z}$, although this makes surprisingly little impact on the results we can attain. Remember from Corollaries 1 and 2 that within this framework, $\mathrm{Der}(\mathbb{C}[G])$ is a Lie algebra over $\mathbb{C}$, of which $\mathrm{Inn}(\mathbb{C}[G])$ is an ideal.

The intention here is primarily to research the nature of these derivations, however, with particular interest in the question of inner derivations: the question automatically arises as to whether all derivations are inner. To this end we will investigate the quotient algebra of outer derivations in particular and attempt to construct non-inner derivations (that is, show that $\mathrm{Out}(\mathbb{C}[G])$ is non-trivial).

Before diving into the meat of this topic we should note the following result:

Proposition 24. *The derivations of* $\mathbb{C}[G]$ *are the mappings* $d : G \to \mathbb{C}[G]$ *such that* $d(gh) = d(g) \cdot h + g \cdot d(h)$ *for all* $g, h \in G$*, extended by linearity to* $\mathbb{C}[G]$*.*

This is analogous to Proposition 10 and its proof is almost identical.

5.1 Describing Derivations as Characters of Γ

Consider a derivation $d \in \mathrm{Der}(\mathbb{C}[G])$. Explicitly, this means that d is a linear mapping on $\mathbb{C}[G]$ such that $d(uv) = d(u)v + ud(v)$ for all $u, v \in \mathbb{C}[G]$. Seeing as d is a linear transformation of an algebra over $\mathbb{C}$, it can be written in terms of a matrix over $\mathbb{C}$. Recall from Note 12 that G is a basis of $\mathbb{C}[G]$. Therefore, the matrix representation of d will consist of rows and columns corresponding to the elements of G: we write this matrix as $\left(d_g^h\right)_{g,h\in G}$, where $d_g^h \in \mathbb{C}$ for all $g, h \in G$.

Recalling from Note 12 that we can enumerate $G = \{g_1, g_2, ...\}$, we can write all elements of $\mathbb{C}[G]$ as vectors with components corresponding to elements of G as follows:

$$\sum_{g_i \in G} a_i g_i = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \end{pmatrix}.$$

We only do this temporarily to clarify the nature of the matrix of d. So, let $u \in \mathbb{C}[G]$. Then we write u as $u = \sum_{g_i \in G} a_i g_i$ so that:

$$d(u) = \begin{pmatrix} d_{g_1}^{g_1} & d_{g_2}^{g_1} & \cdots \\ d_{g_1}^{g_2} & d_{g_2}^{g_2} & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \end{pmatrix} = \begin{pmatrix} \sum_{g_i \in G} d_{g_i}^{g_1} a_i \\ \sum_{g_i \in G} d_{g_i}^{g_2} a_i \\ \vdots \end{pmatrix}.$$

Returning to the traditional notation for group algebra elements, this gives us the following expression, where $u = \sum_{g \in G} a_g g$:

$$d(u) = \sum_{h \in G} \left(\sum_{g \in G} d_g^h a_g \right) h. \tag{5.1}$$

For each $g \in G$ this equation can be written in a simpler form:

$$d(g) = \sum_{h \in G} d_g^h h. \tag{5.2}$$

We now have a practical description of the matrix $\left(d_g^h\right)_{g,h\in G}$ and we can use it to determine properties of d. Firstly, we obtain the following result:

Lemma 6. *A mapping $d : \mathbb{C}[G] \to \mathbb{C}[G]$ is a linear transformation if and only if it is defined by:*

$$d(u) = \sum_{h\in G} \left(\sum_{g\in G} d_g^h a_g \right) h$$

where $\left(d_g^h\right)_{g,h\in G}$ is a complex-valued matrix such that for each $g \in G$ there are finitely many $h \in G$ such that $d_g^h \neq 0$.

Proof. We have already seen that if d is linear, this leads to Equations (5.1) and (5.2). Therefore, d is indeed defined by a complex-valued matrix as stated. Furthermore, Equation (5.2) is only defined if the right-hand side is a finite sum for each $g \in G$: otherwise, this would not yield an element of $\mathbb{C}[G]$, seeing as we are working within a discrete topology where this infinite sum cannot converge. Thus, for each $g \in G$ there are finitely many $h \in G$ such that $d_g^h \neq 0$.

Conversely, suppose that $d : \mathbb{C}[G] \to \mathbb{C}[G]$ is defined by Equation (5.1) and that for each $g \in G$ there are finitely many $h \in G$ such that $d_g^h \neq 0$. Then for any $u \in \mathbb{C}[G]$ the sum in Equation (5.1) must be finite: there are only finitely many $g \in G$ such that $a_g \neq 0$ and for each such g, only finitely many $d_g^h \neq 0$. Therefore, the right-hand side of Equation (5.1) is a finite sum of finite sums. This tells us that $d(u) \in \mathbb{C}[G]$ for each $u \in \mathbb{C}[G]$. Thus, $d\left(\mathbb{C}[G]\right) \subseteq \mathbb{C}[G]$. Moreover, it is defined by a matrix with rows and columns corresponding to the basis of $\mathbb{C}[G]$, meaning that it is linear. □

We now introduce the link with the characters of the groupoid of the adjoint action Γ. For each $d \in \mathrm{Der}(\mathbb{C}[G])$, we define a mapping $T^d : \mathrm{Mor}(\Gamma) \to \mathbb{C}$ as follows:

$$T^d\left(\frac{a \to b}{g}\right) = d_g^{ga} \tag{5.3}$$

for all $\left(\frac{a\to b}{g}\right) \in \mathrm{Mor}(\Gamma)$. This could equivalently be written as $T^d\left(\frac{a\to b}{g}\right) = d_g^{bg}$. Following this method of defining mappings:

Theorem 8. *A function $X : \mathrm{Mor}(\Gamma) \to \mathbb{C}$ is defined by some derivation d of $\mathbb{C}[G]$ such that $X\left(\frac{a\to b}{g}\right) = d_g^{ga}$ for all $\left(\frac{a\to b}{g}\right) \in \mathrm{Mor}(\Gamma)$ if and only if it is a locally finitely supported character.*

Proof. Firstly, to prove the forward implication we suppose that X is defined by some derivation $d \in \mathrm{Der}(\mathbb{C}[G])$ as in Equation (5.3), that is $X = T^d$. By

Lemma 6, for each $g \in G$ there are only finitely many $ga \in G$ such that $d_g^{ga} \neq 0$. Therefore, for each $g \in G$, there are finitely many $\left(\frac{a\to b}{g}\right) \in \mathrm{Mor}(\Gamma)$ such that $X\left(\frac{a\to b}{g}\right) \neq 0$, i.e. X is locally finitely supported.

Now let $\xi, \eta \in \mathrm{Mor}(\Gamma)$ such that $\eta \circ \xi$ exists. Set $\xi = \left(\frac{a\to b}{g_1}\right)$ and $\eta = \left(\frac{b\to c}{g_2}\right)$ so that:

$$T^d(\eta \circ \xi) = T^d\left(\frac{a \to c}{g_2 g_1}\right) = d^{g_2 g_1 a}_{g_2 g_1}.$$

For convenience we set $h = g_2 g_1 a$, leading to:

$$\begin{aligned} T^d(\xi) &= d^{g_1 a}_{g_1} = d^{g_2^{-1} h}_{g_1}, \\ T^d(\eta) &= d^{c g_2}_{g_2} = d^{h g_1^{-1}}_{g_2}. \end{aligned}$$

But d is a derivation and so $d(g_2 g_1) = d(g_2) g_1 + g_2 d(g_1)$. Putting this in terms of Equation (5.2), we find:

$$\begin{aligned} \sum_{h\in G} d^h_{g_2 g_1} h &= \sum_{h\in G} d^h_{g_2} h g_1 + \sum_{h\in G} d^h_{g_1} g_2 h \\ &= \sum_{h\in G} d^{h g_1^{-1}}_{g_2} h + \sum_{h\in G} d^{g_2^{-1} h}_{g_1} h \\ &= \sum_{h\in G} \left(d^{h g_1^{-1}}_{g_2} + d^{g_2^{-1} h}_{g_1} \right) h. \end{aligned}$$

Thus, we can conclude that $d^h_{g_2 g_1} = d^{h g_1^{-1}}_{g_2} + d^{g_2^{-1} h}_{g_1}$ and hence that:

$$T^d(\eta \circ \xi) = T^d(\eta) + T^d(\xi).$$

Therefore, X is a character.

Moving on to the backward implication, suppose that X is a locally finitely supported character. Then we define a mapping $d : \mathbb{C}[G] \to \mathbb{C}[G]$ by Equation (5.1) where the entries of the matrix $\left(d^h_g\right)_{g,h\in G}$ are given by:

$$d^h_g = X\left(\frac{g^{-1} h \to h g^{-1}}{g}\right).$$

Since X is locally finitely supported, for each $g \in G$ there are finitely many $h \in G$ such that $d^h_g \neq 0$ and so $\left(d^h_g\right)_{g,h\in G}$ defines a linear operator by Lemma

6. Now let $g_1, g_2 \in G$. Then, since X is a character:

$$\begin{aligned}
d(g_2g_1) &= \sum_{h\in G} d^h_{g_2g_1}h = \sum_{h\in G} X\left(\frac{g_1^{-1}g_2^{-1}h \to hg_1^{-1}g_2^{-1}}{g_2g_1}\right)h \\
&= \sum_{h\in G} X\left(\left(\frac{g_2^{-1}hg_1^{-1} \to hg_1^{-1}g_2^{-1}}{g_2}\right)\circ\left(\frac{g_1^{-1}g_2^{-1}h \to g_2^{-1}hg_1^{-1}}{g_1}\right)\right)h \\
&= \sum_{h\in G} X\left(\frac{g_2^{-1}hg_1^{-1} \to hg_1^{-1}g_2^{-1}}{g_2}\right)h + \sum_{h\in G} X\left(\frac{g_1^{-1}g_2^{-1}h \to g_2^{-1}hg_1^{-1}}{g_1}\right)h \\
&= \sum_{h\in G} d^{hg_1^{-1}}_{g_2}h + \sum_{h\in G} d^{g_2^{-1}h}_{g_1}h \\
&= \sum_{h\in G} d^h_{g_2}hg_1 + \sum_{h\in G} d^h_{g_1}g_2h \\
&= d(g_2)g_1 + g_2d(g_1)
\end{aligned}$$

and so by Proposition 24, d is a derivation of $\mathbb{C}[G]$. Lastly, for any morphism $\left(\frac{a\to b}{g}\right) \in \mathrm{Mor}(\Gamma)$:

$$T^d\left(\frac{a\to b}{g}\right) = d^{ga}_g = X\left(\frac{a\to gag^{-1}}{g}\right) = X\left(\frac{a\to b}{g}\right)$$

and thus $X = T^d$, meaning that X is defined by a derivation as in Equation 5.3. □

This theorem tells us that there is a one-to-one correspondence between the derivations of $\mathbb{C}[G]$ and the locally finitely supported characters of Γ. In fact, this relationship is even stronger:

Theorem 9. *The vector space of derivations of the group algebra is isomorphic to the space of locally finitely supported characters of the groupoid of the adjoint action:*

$$\mathrm{Der}(\mathbb{C}[G]) \cong T_f(\Gamma).$$

Proof. Define the mapping $T : \mathrm{Der}(\mathbb{C}[G]) \to T_f(\Gamma)$ as follows:

$$T(d) = T^d.$$

If $d_1, d_2 \in \mathrm{Der}(\mathbb{C}[G])$, then for all $\left(\frac{a\to b}{g}\right) \in \mathrm{Mor}(\Gamma)$:

$$T^{d_1+d_2}\left(\frac{a\to b}{g}\right) = (d_1+d_2)^{ga}_g = {d_1}^{ga}_g + {d_2}^{ga}_g$$

$$= T^{d_1}\left(\frac{a \to b}{g}\right) + T^{d_2}\left(\frac{a \to b}{g}\right)$$
$$= \left(T^{d_1} + T^{d_2}\right)\left(\frac{a \to b}{g}\right)$$

since the matrix corresponding to $d_1 + d_2$ must obviously be the sum of the matrices corresponding to d_1 and d_2. Therefore, $T^{d_1+d_2} = T^{d_1} + T^{d_2}$. Similarly, we find that $T^{\alpha d} = \alpha T^d$ for all $\alpha \in \mathbb{C}$ and $d \in \mathrm{Der}(\mathbb{C}[G])$. Therefore, T is a vector space homomorphism.

We can easily see from Theorem 8 that T is well-defined and surjective. Furthermore, if $T^d = 0$ for some $d \in \mathrm{Der}(\mathbb{C}[G])$, then $d_g^h = 0$ for all $g, h \in G$, meaning that $d = 0$. Therefore, $\ker(T) = \{0\}$, i.e. T is injective. We can conclude that T is a bijection and hence an isomorphism. □

This result is extremely useful because it tells us that each derivation can equivalently be considered a locally finitely supported character. Therefore, we can freely use the corresponding characters to describe derivations.

5.1.1 Characters of Inner Derivations

For this reason it will be useful to understand the nature of the characters corresponding to inner derivations. Results are obtained in this direction in [3] and [2], however, the results stated there stop short of a full description: only inner derivations with respect to group elements are considered, i.e. d_g for $g \in G$. We will consider all inner derivations.

Proposition 25. *Let $d_u \in \mathrm{Inn}(\mathbb{C}[G])$ where $u = \sum_{g\in G} u_g g \in \mathbb{C}[G]$. Then for all $\left(\frac{a\to b}{g}\right) \in \mathrm{Mor}(a, b)$:*

$$T^{d_u}\left(\frac{a \to b}{g}\right) = u_b - u_a. \tag{5.4}$$

Proof. For any $g \in G$:

$$d_u(g) = ug - gu = \sum_{h\in G} u_h hg - \sum_{h\in G} u_h gh$$
$$= \sum_{h\in G} u_{hg^{-1}} h - \sum_{h\in G} u_{g^{-1}h} h.$$

Combining this with Equation (5.2) yields:

$$\sum_{h\in G} (d_u)_g^h \, h = \sum_{h\in G} (u_{hg^{-1}} - u_{g^{-1}h}) \, h$$

and so $(d_u)_g^h = u_{hg^{-1}} - u_{g^{-1}h}$ for all $g, h \in G$. Now that we have determined the matrix of d_u, we can express it as a character:

$$T^{d_u}\left(\frac{a \to b}{g}\right) = (d_u)_g^{ga} = u_{gag^{-1}} - u_{g^{-1}ga} = u_b - u_a$$

for any morphism $\left(\frac{a\to b}{g}\right)$. □

This is a strikingly simple expression. It is somewhat surprising that inner derivations can be described so easily within $T_f(\Gamma)$, however, very convenient. Furthermore, since the relationship between $\mathrm{Der}(\mathbb{C}[G])$ and $T_f(\Gamma)$ is one-to-one, every locally finitely supported character satisfying Equation (5.4) for some $\sum_{g\in G} u_g g \in \mathbb{C}[G]$ corresponds to an inner derivation. Thus:

Theorem 10. *A character $T^d \in T_f(\Gamma)$ corresponds to an inner derivation of $\mathbb{C}[G]$ if and only if for all $\left(\frac{a\to b}{g}\right) \in \mathrm{Mor}(\Gamma)$, $T^d\left(\frac{a\to b}{g}\right) = u_b - u_a$ for some $u = \sum_{g\in G} u_g g \in \mathbb{C}[G]$. In this case $d = d_u$.*

Corollary 3. *For any $d_u \in \mathrm{Inn}(\mathbb{C}[G])$, the character T^{d_u} is zero on all loops in $\mathrm{Mor}(\Gamma)$.*

This corollary is a very simple consequence of the preceding theorem. More broadly it is interesting to observe that the characters of inner derivations depend only on the domain and codomain of morphisms.

5.2 Structural Connections Between Derivations and Characters

Here we demonstrate the structural similarities between the derivations and characters, going beyond the isomorphism between $\mathrm{Der}(\mathbb{C}[G])$ and $T_f(\Gamma)$. This is encapsulated in the following diagram, taken from [3]:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Inn}(\mathbb{C}[G]) & \xrightarrow{\mathrm{Id}} & \mathrm{Der}(\mathbb{C}[G]) & \xrightarrow{/} & \mathrm{Out}(\mathbb{C}[G]) & \longrightarrow & 0 \\ & & \downarrow T & & \downarrow T & & \downarrow f & & \\ 0 & \longrightarrow & \ker_f(p_u) & \xrightarrow{\mathrm{Id}} & T_f(\Gamma) & \xrightarrow{p_u} & T(\mathrm{Mor}(u,u)) & \longrightarrow & 0 \end{array}$$

Figure 5.1: Commutative Diagram of $\mathrm{Der}(\mathbb{C}[G])$ and $T_f(\Gamma)$

where for each $u \in G$ we define $p_u : T(\Gamma) \to T(\mathrm{Mor}(u,u))$ by:

$$p_u(X) = X|_{\mathrm{Mor}(u,u)}$$

and $f : \mathrm{Out}(\mathbb{C}[G]) \to T(\mathrm{Mor}(u,u))$ by:

$$f(d + \mathrm{Inn}(\mathbb{C}[G])) = T^d|_{\mathrm{Mor}(u,u)}.$$

Furthermore, recall our convention that the subscript f denotes the restriction of a set of mappings to its locally finitely supported members. Thereby, $\ker_f(p_u)$ is the set of all locally finitely supported characters in $\ker(p_u)$.

It is necessary to demonstrate that all the arrows in the diagram are in fact well-defined. This is obvious for most of them. It is only necessary to clarify this for $\mathrm{Inn}(\mathbb{C}[G]) \xrightarrow{T} \ker_f(p_u)$ and $\mathrm{Out}(\mathbb{C}[G]) \xrightarrow{f} T(\mathrm{Mor}(u,u))$.

Starting with $\mathrm{Inn}(\mathbb{C}[G]) \xrightarrow{T} \ker_f(p_u)$, it is a clear consequence of Corollary 3 that for any $d_v \in \mathrm{Inn}(\mathbb{C}[G])$, $p_u\left(T^{d_v}\right) = 0$ and hence $T^{d_v} \in \ker(p_u)$. Seeing as T^{d_v} must be locally finitely supported, we can conclude that $T^{d_v} \in \ker_f(p_u)$. Therefore, this arrow is corestricted.

Now we show that f is well-defined. It is obvious that $f(d + \mathrm{Inn}(\mathbb{C}[G])) \in T(\mathrm{Mor}(u,u))$ for all $d + \mathrm{Inn}(\mathbb{C}[G]) \in \mathrm{Out}(\mathbb{C}[G])$, however, we must show that f produces a unique output for each coset. To that end, suppose that $d_1 + \mathrm{Inn}(\mathbb{C}[G]) = d_2 + \mathrm{Inn}(\mathbb{C}[G])$. Then $d_1 - d_2 \in \mathrm{Inn}(\mathbb{C}[G])$ and so by Corollary 3, $T^{d_1-d_2}|_{\mathrm{Mor}(u,u)} = 0$, i.e. $T^{d_1}|_{\mathrm{Mor}(u,u)} = T^{d_2}|_{\mathrm{Mor}(u,u)}$. Hence:

$$f(d_1 + \mathrm{Inn}(\mathbb{C}[G])) = f(d_2 + \mathrm{Inn}(\mathbb{C}[G])).$$

We can conclude that f does indeed produce a unique output for each coset and so it is well-defined.

Having established that all the arrows are well-defined, we can now consider the properties of the diagram. It is obvious that it is commutative and nearly exact.

Exactness fails only at $T_f(\Gamma) \xrightarrow{p_u} T(\mathrm{Mor}(u,u)) \longrightarrow 0$. For this segment to be exact would require that every character of $\mathrm{Mor}(u,u)$ is the restriction of some locally finitely supported character. This would be wonderful as it would mean that every character of $\mathrm{Mor}(u,u)$ corresponds to a derivation of $\mathbb{C}[G]$. It appears, however, not to be the case. $T(\mathrm{Mor}(u,u))$ further weakens this diagram in the sense that the vertical arrow from $\mathrm{Out}(\mathbb{C}[G])$ to $T(\mathrm{Mor}(u,u))$ is the weakest of the vertical arrows: the other two vertical arrows are injective homomorphisms (in fact the middle arrow is an isomorphism) whereas f is merely a homomorphism.

We can conclude that the relevant diagram demonstrates a fairly strong structural connection between the world of derivations and that of the locally finitely supported characters. In addition to the established isomorphism from Theorem 9, it shows a strong link between the inner derivations and $\ker_f(p_u)$ as well as the outer derivations and $T(\mathrm{Mor}(u,u))$, along with structural similarities in terms of the connections within these worlds. However, it is somewhat frustrating that it is not exact and that the right-most vertical arrow is not injective. These properties would demonstrate a substantially stronger structural connection.

The absence of exactness can be solved by removing the requirement of local finite support as follows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Inn}(\mathbb{C}[G]) & \xrightarrow{\mathrm{Id}} & \mathrm{Der}(\mathbb{C}[G]) & \xrightarrow{/} & \mathrm{Out}(\mathbb{C}[G]) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle T} & & \downarrow{\scriptstyle T} & & \downarrow{\scriptstyle f} & & \\
0 & \longrightarrow & \ker(p_u) & \xrightarrow{\mathrm{Id}} & T(\Gamma) & \xrightarrow{p_u} & T(\mathrm{Mor}(u,u)) & \longrightarrow & 0
\end{array}$$

Figure 5.2: Exact Commutative Diagram of $\mathrm{Der}(\mathbb{C}[G])$ and $T(\Gamma)$

This is an exact commutative diagram as suggested (although not directly stated) by Theorem 3 from [3] as every character of $T(\mathrm{Mor}(u,u))$ is indeed the restriction of some character of Γ, a consequence of Proposition 23. In that sense this diagram is an improvement over the previous one and shows a stronger structural connection, this time between the derivations and all characters. However, this is something of a trade-off: we have lost the surjectivity of the middle vertical arrow, meaning it is no longer an isomorphism. We have also done nothing to introduce injectivity to the right-most vertical arrow.

5.3 $\mathbf{Der}_{[u]}(\mathbb{C}[G])$

We therefore introduce the following structure in order to construct a more satisfying diagram:

Definition 45. *We define the space* $\mathrm{Der}_{[u]}(\mathbb{C}[G])$ *to be the derivations corresponding to the characters of* $\Gamma_{[u]}$*, that is:*

$$\mathrm{Der}_{[u]}(\mathbb{C}[G]) = \left\{ d \in \mathrm{Der}(\mathbb{C}[G] : T^d \in T_f\left(\Gamma_{[u]}\right) \right\}$$

using the notion of $T_f\left(\Gamma_{[u]}\right)$ *from Equation* (4.4)*. Similarly we define:*

$$\mathrm{Inn}_{[u]}(\mathbb{C}[G]) = \left\{ d \in \mathrm{Inn}(\mathbb{C}[G] : T^d \in T_f\left(\Gamma_{[u]}\right) \right\}.$$

Lastly we can construct a space of outer derivations with respect to $[u]$ *in the obvious way:* $\mathrm{Out}_{[u]}(\mathbb{C}[G]) = \mathrm{Der}_{[u]}(\mathbb{C}[G])/\,\mathrm{Inn}_{[u]}(\mathbb{C}[G])$.

Note here that we can obtain results analogous to Inequality (4.6):

$$\mathrm{Der}(\mathbb{C}[G]) \subseteq \bigoplus_{[u]\in[G]} \mathrm{Der}_{[u]}(\mathbb{C}[G]), \tag{5.5}$$

$$\mathrm{Inn}(\mathbb{C}[G]) \subseteq \bigoplus_{[u]\in[G]} \mathrm{Inn}_{[u]}(\mathbb{C}[G]). \tag{5.6}$$

Inequality (5.5) is fairly simple to see. We can decompose any $d \in \mathrm{Der}(\mathbb{C}[G])$ as follows:

$$d = \sum_{[u]\in[G]} T^{-1}\left(\left(T^d|_{\Gamma_{[u]}}\right)'\right).$$

For inner derivations this is slightly more involved. Consider $d \in \mathrm{Inn}_{[u]}(\mathbb{C}[G])$. Then $d \in \mathrm{Inn}(\mathbb{C}[G])$ and $T^d\left(\frac{a\to b}{g}\right) = 0$ unless $\left(\frac{a\to b}{g}\right) \in \mathrm{Mor}\left(\Gamma_{[u]}\right)$. Using Theorem 10, this tells us that $d = d_v$ for some $v = \sum_{g\in G} v_g g \in \mathbb{C}[G]$ such that $v_b - v_a = 0$ for all conjugate pairs $a, b \notin [u]$. Therefore, without loss of generality we can assume that $v_g = 0$ whenever $g \notin [u]$ and we can write v as $v = \sum_{g\in[u]} v_g g$. Conversely, for any finite $v = \sum_{g\in[u]} v_g g$, $d_v \in \mathrm{Inn}_{[u]}(\mathbb{C}[G])$.

This leads to Inequality (5.6): letting $d = d_w$ be an arbitrary inner derivation, we decompose $w = \sum_{g\in G} w_g g$ as follows:

$$w = \sum_{[u]\in[G]} \sum_{g\in[u]} w_g g = \sum_{[u]\in[G]} w_{[u]}$$

where $w_{[u]} = \sum_{g\in[u]} w_g g$ for each conjugacy class $[u]$. Then by the working

above, $d_{w_{[u]}} \in \mathrm{Inn}_{[u]}(\mathbb{C}[G])$ for each $[u]$. Obviously $d_w = \sum_{[u]\in[G]} d_{w_{[u]}}$, thus demonstrating Inequality (5.6).

These inequalities mean that every (inner) derivation can be constructed out of independent (inner) derivations from each subgroupoid $\Gamma_{[u]}$. Note that these are inequalities because we cannot necessarily construct a derivation out of any arbitrary combination of derivations from subgroupoids: local finite support would not always be guaranteed for the corresponding characters. If there were, however, a finite number of conjugacy classes in the underlying group, then this problem would disappear.

Having established the subspaces $\mathrm{Der}_{[u]}(\mathbb{C}[G])$ and $\mathrm{Inn}_{[u]}(\mathbb{C}[G])$, we can use them to construct a diagram extremely similar to that in Figure 5.2, again suggested by [3]:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Inn}_{[u]}(\mathbb{C}[G]) & \xrightarrow{\mathrm{Id}} & \mathrm{Der}_{[u]}(\mathbb{C}[G]) & \xrightarrow{/} & \mathrm{Out}_{[u]}(\mathbb{C}[G]) & \longrightarrow & 0 \\
 & & \downarrow T & & \downarrow T & & \downarrow f & & \\
0 & \longrightarrow & \ker(p_u) & \xrightarrow{\mathrm{Id}} & T(\Gamma_{[u]}) & \xrightarrow{p_u} & T(\mathrm{Mor}(u,u)) & \longrightarrow & 0
\end{array}$$

Figure 5.3: Exact Commutative Diagram of $\mathrm{Der}_{[u]}(\mathbb{C}[G])$ and $T\left(\Gamma_{[u]}\right)$

where the domain of p_u is here taken to be $T\left(\Gamma_{[u]}\right)$. This is most similar to Figure 5.2 since it also ignores local finite support. It is possibly an improvement over that diagram, though, as it may introduce injectivity to the right-most vertical diagram. Unfortunately, we must still do without surjectivity in the middle vertical arrow so as to maintain exactness.

To explain what we mean when we say that f is possibly injective here, consider $d_1, d_2 \in \mathrm{Der}_{[u]}(\mathbb{C}[G])$ such that $f\left(d_1 + \mathrm{Inn}_{[u]}(\mathbb{C}[G])\right) = f\left(d_2 + \mathrm{Inn}_{[u]}(\mathbb{C}[G])\right)$. If we can show that this implies $d_1 + \mathrm{Inn}_{[u]}(\mathbb{C}[G]) = d_2 + \mathrm{Inn}_{[u]}(\mathbb{C}[G])$, then we will have proved injectivity of f.

Firstly, our hypothesis is equivalent to saying that $T^{d_1}|_{\mathrm{Mor}(u,u)} = T^{d_2}|_{\mathrm{Mor}(u,u)}$, i.e. that $T^{d_1-d_2}(\xi) = 0$ for all $\xi \in \mathrm{Mor}(u,u)$. We will let $d = d_1 - d_2$ for convenience's sake with the aim of showing that $d \in \mathrm{Inn}_{[u]}(\mathbb{C}[G])$. It is immediately obvious that $d \in \mathrm{Der}_{[u]}(\mathbb{C}[G])$. We will now show that T^d depends only on the domain and codomain of morphisms, a property which it shares with all inner derivations. Consider arbitrary $a, b \in [u]$ and let $\xi, \eta \in \mathrm{Mor}(a,b)$. We will let

$a = xux^{-1}$ and $b = yuy^{-1}$ with $\xi = \left(\frac{a \to b}{g}\right)$ and $\eta = \left(\frac{a \to b}{h}\right)$. Then:

$$\begin{aligned}
T^d(\xi) - T^d(\eta) &= T^d\left(\frac{a \to b}{g}\right) + T^d\left(\frac{b \to a}{h^{-1}}\right) \\
&= T^d\left(\left(\frac{a \to b}{g}\right) \circ \left(\frac{b \to a}{h^{-1}}\right)\right) \\
&= T^d\left(\frac{b \to b}{gh^{-1}}\right) \\
&= T^d\left(\left(\frac{u \to b}{y}\right) \circ \left(\frac{b \to u}{y^{-1}gh^{-1}}\right)\right) \\
&= T^d\left(\frac{b \to u}{y^{-1}gh^{-1}}\right) + T^d\left(\frac{u \to b}{y}\right) \\
&= T^d\left(\left(\frac{b \to u}{y^{-1}gh^{-1}}\right) \circ \left(\frac{u \to b}{y}\right)\right) \\
&= T^d\left(\frac{u \to u}{y^{-1}gh^{-1}y}\right) \\
&= 0
\end{aligned}$$

since T^d is trivial on $\mathrm{Mor}(u, u)$. Observe that every morphism used in the above calculations is indeed an existing morphism in Γ. Thus, $T^d(\xi) = T^d(\eta)$. From this we can conclude that T^d depends only on domain and codomain in $\Gamma_{[u]}$. Further, $T^d(\xi) = 0$ for any $\xi \notin \mathrm{Mor}\left(\Gamma_{[u]}\right)$. These are properties consistent with derivations in $\mathrm{Inn}_{[u]}(\mathbb{C}[G])$. However, to show conclusively that d is inner with respect to $[u]$, we must find some $v = \sum_{g \in [u]} v_g g \in \mathbb{C}[G]$ such that $d = d_v$.

As an attempt to determine such a v, we set $v_g = T^d\left(\frac{u \to g}{x}\right)$ for each $g \in [u]$ where x is a group element such that $g = xux^{-1}$. Then v_g is well-defined since such an x must exist and if more than one exists, i.e. $x_1 u x_1^{-1} = x_2 u x_2^{-1}$, then $T^d\left(\frac{u \to g}{x_1}\right) = T^d\left(\frac{u \to g}{x_2}\right)$ by our previous working. Having set this up, we find that for any $\left(\frac{a \to b}{g}\right) \in \mathrm{Mor}\left(\Gamma_{[u]}\right)$, where $a = xux^{-1}$ and $b = yuy^{-1}$:

$$\begin{aligned}
T^d\left(\frac{a \to b}{g}\right) &= T^d\left(\left(\frac{u \to b}{y}\right) \circ \left(\frac{a \to u}{y^{-1}g}\right)\right) \\
&= T^d\left(\frac{u \to b}{y}\right) + T^d\left(\frac{a \to u}{y^{-1}g}\right) \\
&= T^d\left(\frac{u \to b}{y}\right) + T^d\left(\frac{a \to u}{x^{-1}}\right) \\
&= T^d\left(\frac{u \to b}{y}\right) - T^d\left(\frac{u \to a}{x}\right) \\
&= v_b - v_a.
\end{aligned}$$

It would appear that we have shown that $d = d_v$, following Theorem 10. Unfortunately, there is no guarantee that $\sum_{g\in[u]} v_g g$ is a finite sum since infinitely many $T^d\left(\frac{u\to g}{x}\right)$ could be non-zero. Hence, there is no guarantee that this construction of v is an element of the group algebra.

However, in the case that $[u]$ is a finite conjugacy class we can guarantee finiteness and hence that d is an inner derivation. Then $d_1 - d_2 \in \mathrm{Inn}_{[u]}(\mathbb{C}[G])$ and so $d_1 + \mathrm{Inn}_{[u]}(\mathbb{C}[G]) = d_2 + \mathrm{Inn}_{[u]}(\mathbb{C}[G])$. Thereby, f is indeed injective in this case. Still, this is a very specific case and so this result remains fairly unsatisfactory.

5.3.1 $\mathbf{Der}_{[e]}(\mathbb{C}[G])$

Let us briefly consider the special case of the identity element e of G. Clearly, e is the only element conjugate with itself and so $[e] = \{e\}$. Therefore, $\Gamma_{[e]} = \mathrm{Mor}(e, e)$. From our previous results, T is an injective homomorphism from $\mathrm{Inn}_{[e]}(\mathbb{C}[G])$ to $\ker(p_e)$, taking $p_e : T\left(\Gamma_{[e]}\right) \to T(\mathrm{Mor}(e, e))$. But within this context p_e is simply the identity mapping and so $\ker(p_e) = \{0\}$. From this we find that for any $d \in \mathrm{Inn}_{[e]}(\mathbb{C}[G])$, $T^d = 0 = T^0$ and hence $d = 0$. Thus, $\mathrm{Inn}_{[e]}(\mathbb{C}[G]) = \{0\}$. This result can also be obtained in other ways, as seen in [3]. Consequently, remembering that $T(\mathrm{Mor}(e, e)) = T_f(\mathrm{Mor}(e, e))$ and hence $T\left(\Gamma_{[e]}\right) = T_f\left(\Gamma_{[e]}\right)$, the diagram from Figure 5.3 for $u = e$:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Inn}_{[e]}(\mathbb{C}[G]) & \xrightarrow{\mathrm{Id}} & \mathrm{Der}_{[e]}(\mathbb{C}[G]) & \xrightarrow{/} & \mathrm{Out}_{[e]}(\mathbb{C}[G]) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle T} & & \downarrow{\scriptstyle T} & & \downarrow{\scriptstyle f} & & \\
0 & \longrightarrow & \ker(p_e) & \xrightarrow{\mathrm{Id}} & T(\Gamma_{[e]}) & \xrightarrow{p_e} & T(\mathrm{Mor}(e, e)) & \longrightarrow & 0
\end{array}$$

is an exact commutative diagram where every vertical arrow is an isomorphism, which makes for a very satisfying structural link. Most importantly, though, this tells us that any non-zero character on $\Gamma_{[e]}$ (i.e. $\mathrm{Mor}(e, e)$) corresponds to a non-inner derivation. This is an interesting result in our quest to determine the existence or non-existence of non-inner derivations of $\mathbb{C}[G]$. To establish whether or not such characters exist, though, we must investigate them more closely.

Consider a character $T^d \in T\left(\Gamma_{[e]}\right)$. Then looking at the matrix of the corre-

sponding derivation d we see that for any $g, h \in G$:

$$d_g^h = T^d\left(\frac{g^{-1}h \to hg^{-1}}{g}\right) = 0 \qquad \text{unless } g = h.$$

Therefore, Equation (5.2) yields the following for any $g \in G$:

$$d(g) = \sum_{h \in G} d_g^h h = d_g^g g. \tag{5.7}$$

Furthermore, we have that for any $g, h \in G$:

$$d_{gh}^{gh} = T^d\left(\frac{e \to e}{gh}\right) = T^d\left(\frac{e \to e}{g}\right) + T^d\left(\frac{e \to e}{h}\right) = d_g^g + d_h^h. \tag{5.8}$$

Combining Equations (5.7) and (5.8), we can say that d is defined by a function $\tau : G \to \mathbb{C}$ such that $\tau(gh) = \tau(g) + \tau(h)$ in the sense that:

$$d(g) = \tau(g)g \qquad \forall g \in G.$$

Conversely, any additive homomorphism $\tau : G \to \mathbb{C}$ defines a derivation as above. It is obvious that this derivation is non-zero if and only if τ is non-trivial. Therefore, we can guarantee the existence of a non-inner derivation of $\mathbb{C}[G]$ if there exists a non-trivial additive homomorphism from G to $\mathbb{C}$.

The non-inner derivations we have constructed here, are as it turns out, simply examples of a broader type of derivation, namely the central derivations as introduced in [2]. They will be the focus of the next section.

5.4 Central Derivations

Before defining the central derivations, we must first establish the results from [2] which allow us to prove non-innerness.

Lemma 7. *If $d \in \mathrm{Der}_{[u]}(\mathbb{C}[G])$, then the value of d for any $g \in G$ is given by:*

$$d(g) = g \sum_{a \in [u]} T^d\left(\frac{a \to gag^{-1}}{g}\right) a.$$

Proof. Fix $g \in G$. Then:

$$d(g) = \sum_{h \in G} d_g^h h = \sum_{h \in G} T^d\left(\frac{g^{-1}h \to hg^{-1}}{g}\right) h.$$

Since $d \in \mathrm{Der}_{[u]}(\mathbb{C}[G])$, $d(\xi) = 0$ whenever $\xi \notin \mathrm{Mor}\left(\Gamma_{[u]}\right)$. This means that the terms in the above sum will be zero unless $\left(\frac{g^{-1}h \to hg^{-1}}{g}\right) \in \mathrm{Mor}\left(\Gamma_{[u]}\right)$. In this case $g^{-1}h \in [u]$, i.e. $h = ga$ for some $a \in [u]$. Therefore:

$$\begin{aligned} d(g) &= \sum_{a \in [u]} T^d \left(\frac{a \to gag^{-1}}{g}\right) ga \\ &= g \sum_{a \in [u]} T^d \left(\frac{a \to gag^{-1}}{g}\right) a. \end{aligned}$$ □

Note also that since T^d is locally finitely supported, the number of non-zero terms on the right-hand side in Lemma 7 is finite. This lemma can be stated in a general form as follows:

Lemma 8. *If $d \in Der(\mathbb{C}[G])$, then the value of d for any $g \in G$ is given by:*

$$d(g) = g \sum_{a \in G} T^d \left(\frac{a \to gag^{-1}}{g}\right) a.$$

Proof. Again we fix $g \in G$. We know $T^d \in T_f(\Gamma)$ and so by Inequality (4.6) we can write T^d as $T^d = \sum_{[u] \in [G]} T^d_{[u]}$, where $T^d_{[u]} \in T_f\left(\Gamma_{[u]}\right)$ for each conjugacy class $[u]$. Applying Lemma 7 to each conjugacy class yields:

$$\begin{aligned} d(g) = \sum_{h \in G} d^h_g h &= \sum_{h \in G} T^d \left(\frac{g^{-1}h \to hg^{-1}}{g}\right) h \\ &= \sum_{h \in G} \sum_{[u] \in [G]} T^d_{[u]} \left(\frac{g^{-1}h \to hg^{-1}}{g}\right) h \\ &= \sum_{[u] \in [G]} \sum_{h \in G} T^d_{[u]} \left(\frac{g^{-1}h \to hg^{-1}}{g}\right) h \\ &= \sum_{[u] \in [G]} \sum_{a \in [u]} T^d_{[u]} \left(\frac{a \to gag^{-1}}{g}\right) ga \\ &= \sum_{[u] \in [G]} \sum_{a \in [u]} T^d \left(\frac{a \to gag^{-1}}{g}\right) ga \end{aligned}$$

since $T^d = T^d_{[u]}$ on $\mathrm{Mor}\left(\Gamma_{[u]}\right)$. Continuing the above chain of equalities:

$$d(g) = \sum_{a \in G} T^d \left(\frac{a \to gag^{-1}}{g}\right) ga$$

$$= g \sum_{a \in G} T^d \left(\frac{a \to gag^{-1}}{g} \right) a. \qquad \square$$

These lemmata along with the following definition will prove necessary for showing that a particular type of derivation is non-inner.

Definition 46. *We call a mapping $\tau : G \to \mathbb{C}$ a **group character** if it is an additive group homomorphism. Explicitly this means that $\tau(gh) = \tau(g) + \tau(h)$ for all $g, h \in G$.*

Definition 47. *Given a group character $\tau : G \to \mathbb{C}$ and a central element $z \in Z(G)$, as defined in Equation (4.2), we define the mapping $d_z^\tau : \mathbb{C}[G] \to \mathbb{C}[G]$ by:*

$$d_z^\tau(g) = \tau(g)gz \qquad \forall g \in G$$

*and then extend this linearly over $\mathbb{C}[G]$. Any mapping defined in this way is a derivation. We call these **central derivations**.*

It is not immediately obvious that the central derivations are in fact derivations, but it is the case. By Proposition 24, we need only show that for all $g, h \in G$, $d_z^\tau(gh) = d_z^\tau(g)h + gd_z^\tau(h)$ in order to show that d_z^τ is a derivation:

$$\begin{aligned} d_z^\tau(gh) &= \tau(gh)ghz \\ &= \tau(g)ghz + \tau(h)ghz \\ &= \tau(g)gzh + g\tau(h)hz \\ &= d_z^\tau(g)h + gd_z^\tau(h) \end{aligned}$$

using the fact that $z, \tau(g), \tau(h) \in Z(G)$, since $\tau(g), \tau(h) \in \mathbb{C}$ and by hypothesis for z. We can conclude from this that the central derivations are indeed derivations.

Note 25. *A central derivation d_z^τ is trivial, that is $d_z^\tau = 0$, if and only if $\tau = 0$. The trivial group character is guaranteed to exist in any group and so we will always have the trivial central derivation.*

Theorem 11. *Every non-trivial central derivation d_z^τ is non-inner.*

Proof. Let d_z^τ be a non-trivial central derivation. Then $\tau \neq 0$ and so we can

choose $g \in G$ so that $\tau(g) \neq 0$. Then by Lemma 8:

$$\tau(g)gz = d_z^\tau(g) = g\sum_{a\in G} T^{d_z^\tau}\left(\frac{a \to gag^{-1}}{g}\right)a$$

and canceling g on both sides:

$$\tau(g)z = \sum_{a\in G} T^{d_z^\tau}\left(\frac{a \to gag^{-1}}{g}\right)a.$$

The left-hand side has only one term, namely a scalar multiple of z. This means that every term on the right-hand side is zero except when $a = z$. Hence:

$$T^{d_z^\tau}\left(\frac{a \to gag^{-1}}{g}\right) = \begin{cases}\tau(g) & a = z,\\ 0 & a \neq z.\end{cases} \tag{5.9}$$

But z commutes with all elements of G and so $gzg^{-1} = z$. Therefore:

$$T^{d_z^\tau}\left(\frac{z \to z}{g}\right) = \tau(g) \neq 0.$$

Thus, the character corresponding to d_z^τ is not trivial on all loops of $\mathrm{Mor}(\Gamma)$. Taking the contrapositive of Corollary 3, this tells us that d_z^τ is non-inner. □

We have successfully constructed a class of non-inner derivations of $\mathbb{C}[G]$. This in itself is a powerful result, however, we can continue by using the central derivations to construct more non-inner derivations with useful properties towards describing the algebra of outer derivations:

Definition 48. *By* $\mathrm{ZDer}(\mathbb{C}[G])$ *we denote the vector space generated by the central derivations of* $\mathbb{C}[G]$*, that is the space of all linear combinations of central derivations.*

Proposition 26. $\mathrm{ZDer}(\mathbb{C}[G])$ *is a Lie subalgebra of* $\mathrm{Der}(\mathbb{C}[G])$.

Proof. It should be clear that $\mathrm{ZDer}(\mathbb{C}[G])$ is a subspace of $\mathrm{Der}(\mathbb{C}[G])$. For this reason we need only show that $\mathrm{ZDer}(\mathbb{C}[G])$ is closed under the Lie product of $\mathrm{Der}(\mathbb{C}[G])$. To that end let $d_{z_1}^{\tau_1}$ and $d_{z_2}^{\tau_2}$ be central derivations. Then for any $g \in G$:

$$\begin{aligned}\left(d_{z_1}^{\tau_1} \circ d_{z_2}^{\tau_2}\right)(g) &= d_{z_1}^{\tau_1}(\tau_2(g)gz_2) = \tau_2(g)d_{z_1}^{\tau_1}(gz_2)\\ &= \tau_2(g)\tau_1(gz_2)gz_2z_1\end{aligned}$$

$$= \tau_2(g)\left(\tau_1(g) + \tau_1(z_2)\right) g z_1 z_2$$

and similarly $\left(d^{\tau_2}_{z_2} \circ d^{\tau_1}_{z_1}\right)(g) = \tau_1(g)(\tau_2(g) + \tau_2(z_1))g z_1 z_2$. Therefore:

$$\begin{aligned}\left[d^{\tau_1}_{z_1}, d^{\tau_2}_{z_2}\right](g) &= \left(d^{\tau_1}_{z_1} \circ d^{\tau_2}_{z_2} - d^{\tau_2}_{z_2} \circ d^{\tau_1}_{z_1}\right)(g) \\ &= \tau_2(g)\left(\tau_1(g) + \tau_1(z_2)\right) g z_1 z_2 - \tau_1(g)(\tau_2(g) + \tau_2(z_1))g z_1 z_2 \\ &= (\tau_2(g)\tau_1(z_2) - \tau_1(g)\tau_2(z_1))g z_1 z_2.\end{aligned}$$

To show that the above is itself a central derivation, we define a function $\tau : G \to \mathbb{C}$ by $\tau(g) = \tau_2(g)\tau_1(z_2) - \tau_1(g)\tau_2(z_1)$. Then τ is a group character as for any $g, h \in G$:

$$\begin{aligned}\tau(gh) &= \tau_2(gh)\tau_1(z_2) - \tau_1(gh)\tau_2(z_1) \\ &= (\tau_2(g) + \tau_2(h))\tau_1(z_2) - (\tau_1(g) + \tau_1(h))\tau_2(z_1) \\ &= \tau(g) + \tau(h).\end{aligned}$$

Thus, we can conclude that $\left[d^{\tau_1}_{z_1}, d^{\tau_2}_{z_2}\right] = d^{\tau}_{z_1 z_2}$ where τ is a group character and $z_1 z_2$ is of course a central element, meaning that it is a central derivation. Therefore, the Lie product of any two central derivations is a central derivation. Letting $d_1 = \alpha_1 d^{\tau_1}_{z_1} + \cdots + \alpha_n d^{\tau_n}_{z_n}$ and $d_2 = \beta_1 d^{\phi_1}_{y_1} + \cdots + \beta_m d^{\phi_m}_{y_m}$, bilinearity and antisymmetry of the Lie product yield:

$$\begin{aligned}[d_1, d_2] &= \left[\alpha_1 d^{\tau_1}_{z_1} + \cdots + \alpha_n d^{\tau_n}_{z_n}, \beta_1 d^{\phi_1}_{y_1} + \cdots + \beta_m d^{\phi_m}_{y_m}\right] \\ &= \sum_{i=1}^{n}\sum_{j=1}^{m} \alpha_i \beta_j \left[d^{\tau_i}_{z_i}, d^{\phi_j}_{y_j}\right] \in \mathrm{ZDer}(\mathbb{C}[G]).\end{aligned}$$ □

Theorem 12. *The Lie subalgebra* $\mathrm{ZDer}(\mathbb{C}[G])$ *can be embedded in the the outer derivations* $\mathrm{Out}(\mathbb{C}[G])$.

Proof. By this we mean that each derivation in $\mathrm{ZDer}(\mathbb{C}[G])$ belongs to a distinct coset in $\mathrm{Out}(\mathbb{C}[G]) = \mathrm{Der}(\mathbb{C}[G])/\mathrm{Inn}(\mathbb{C}[G])$. To prove this, we must show only that if $d_1, d_2 \in \mathrm{ZDer}(\mathbb{C}[G])$ and $d_1 - d_2 \in \mathrm{Inn}(\mathbb{C}[G])$, then $d_1 = d_2$.

Before proving this fact, we first show that any non-trivial $d \in \mathrm{ZDer}(\mathbb{C}[G])$ is non-inner. We can write such d as $d = \sum_{i=1}^{n} \alpha_i d^{\tau_i}_{z_i}$ where $\alpha_i \neq 0$ for all i and

$d_{z_i}^{\tau_i} \neq d_{z_j}^{\tau_j}$ whenever $i \neq j$. Then for all $j = 1, 2, ..., n$ and $g \in G$:

$$\begin{aligned} T^d\left(\frac{z_j \to z_j}{g}\right) &= \sum_{i=1}^{n} \alpha_i T^{d_{z_i}^{\tau_i}}\left(\frac{z_j \to z_j}{g}\right) \\ &= \sum_{i=1}^{n} \alpha_i T^{d_{z_i}^{\tau_i}}\left(\frac{z_j \to g z_j g^{-1}}{g}\right) \\ &= \sum_{i=1}^{n} \delta_{z_i}^{z_j} \alpha_i \tau_i(g) \end{aligned}$$

using Equation (5.9). Now assume that d is inner. Then $T^d\left(\frac{z \to z}{g}\right) = 0$ for all $g \in G$ and $z \in Z(G)$. Then for all $j = 1, 2, ..., n$ and $g \in G$:

$$\sum_{i=1}^{n} \delta_{z_i}^{z_j} \alpha_i \tau_i(g) = 0.$$

So for all $g \in G$:

$$d(g) = \sum_{i=1}^{n} \alpha_i \tau(g) g z_i = 0$$

meaning that $d = 0$. This contradicts that d is non-trivial and so our assumption that d is inner was false. Thus, we can conclude by contradiction that every non-trivial derivation in $\mathrm{ZDer}(\mathbb{C}[G])$ is non-inner.

It is now obvious that if $d_1, d_2 \in \mathrm{ZDer}(\mathbb{C}[G])$ such that $d_1 - d_2 \in \mathrm{Inn}(\mathbb{C}[G])$, then $d_1 - d_2 = 0$, i.e. $d_1 = d_2$. □

This last theorem is very significant in our desire to determine the prevalence of inner derivations within the broader space of all derivations. We have established an entire subspace of non-inner derivations, which moreover correspond to more non-inner derivations (usually). Firstly, each $d \in \mathrm{ZDer}(\mathbb{C}[G]) \setminus \{0\}$ is non-inner. Moreover, each d' such that $d' + \mathrm{Inn}(\mathbb{C}[G]) = d + \mathrm{Inn}(\mathbb{C}[G])$ is also non-inner (seeing as $d' + \mathrm{Inn}(\mathbb{C}[G]) \neq \mathrm{Inn}(\mathbb{C}[G])$). Since the cardinality of every coset must be equal, there will always be as many such d' as there are inner derivations. Seeing as each $d \in \mathrm{ZDer}(\mathbb{C}[G]) \setminus \{0\}$ belongs to a distinct coset, this means that there must be at least $|\,\mathrm{ZDer}(\mathbb{C}[G])| - 1$ times as many non-inner derivations as there are inner derivations. This appears to tell us that the derivations of $\mathbb{C}[G]$ are overwhelmingly non-inner.

There is, however, an issue with this conclusion. So far in this section we have

simply repeated and proved the results from [2], however, there is a caveat regarding the central derivations that is not mentioned there, namely that there are not guaranteed to be any non-trivial central derivations of the group algebra. To construct such a derivation we require an element of the centre of G and a non-trivial group character. We can always use the identity element as our element of $Z(G)$ – in fact the central derivations using the identity element are precisely the non-inner derivations described at the end of Section 5.3.1 – but the non-trivial group character is a more difficult matter: its existence depends on the group G.

Let us consider the example of the free group X as used extensively in Chapter 3. Each $u \in X$ can be written as $u = \prod_{j=1}^{l} x_{j_k}^{\epsilon_k}$ and so we define a mapping $\tau : X \to \mathbb{C}$ by:

$$\tau\left(\prod_{j=1}^{l} x_{j_k}^{\epsilon_k}\right) = \sum_{k=1}^{l} \epsilon_k.$$

It is obvious that τ is a non-trivial group character of X and so d_e^τ is a non-trivial central derivation. Thus, we have constructed a non-inner derivation of $\mathbb{C}[X]$.

However, other finitely generated groups are less straightforward. Let us construct the group Y, which is also generated by $(x) = \{x_1, x_2, ..., x_n\}$ but with the sole restriction that each generator is self-inverse, i.e. $x_j^2 = 1$ for all $x_j \in (x)$. This means that Y consists of words of the form $\prod_{k=1}^{l} x_{j_k}$ where $j_{k+1} \neq j_k$ for all k. Then every group character $\tau : Y \to \mathbb{C}$ has the property that for all $x_j \in (x)$:

$$0 = \tau(1) = \tau\left(x_j^2\right) = \tau(x_j) + \tau(x_j)$$

and so τ is trivial on all generators of Y. Thus, for any $u \in Y$:

$$\tau(u) = \tau\left(\prod_{k=1}^{l} x_{j_k}\right) = \sum_{k=1}^{l} \tau\left(x_{j_k}\right) = 0.$$

Hence, the only group character of Y is trivial, meaning that we cannot construct any non-trivial central derivations of $\mathbb{C}[Y]$. Therefore, we cannot guarantee the existence of non-inner derivations using this approach.

Above are two particularly simple examples to illustrate that non-trivial group characters are sometimes guaranteed to exist and sometimes guaranteed not to. There are several more examples for both cases. We might weaken the

restriction for Y to be that for each $x_j \in (x)$ there exists a positive integer m such that $x_j^m = 0$. We would reach the same conclusion regarding the group characters. There are countless groups we could construct to reach this result and indeed countless groups we could construct for which there exist non-trivial group characters. This is to say that the approach laid forth in this chapter sometimes works to construct non-inner derivations of the group algebra and sometimes does not.

This seems to motivate work with broader group algebras, rather than merely those over $\mathbb{C}$. The examples above of groups Y such that there exist no non-trivial group characters rely on the fact that $\mathbb{C}$ has characteristic 0. Perhaps if we considered a group algebra $R[Y]$ over a ring R with $\text{char}(R) > 0$, this would complicate the search for such groups. In particular, if $\text{char}(R) = 2$, then even our most basic example – Y such that $x_i^2 = 1$ for all $x_i \in (x)$ – would fail. In this case, there does exist a non-trivial group character $\tau : Y \to R$, defined as follows:

$$\tau\left(\prod_{k=1}^{l} x_{j_k}\right) = \begin{cases} 1 & l \text{ is odd,} \\ 0 & l \text{ is even.} \end{cases}$$

This seems to imply that the characteristic of our underlying ring R has a significant impact upon the existence of non-inner derivations of group algebras over R. However, the underlying ring $\mathbb{C}$ has been present throughout this chapter, meaning that we cannot jump to conclusions here: the construction of central derivations relied upon work done using the structure of $\mathbb{C}$ and we cannot assume that an analogous notion of central derivations would be constructable for an arbitrary ring R. Nevertheless, research regarding the effect of $\text{char}(R)$ upon the existence of non-inner derivations of group algebras over R may be worthwhile.

Chapter 6

Links to Cohomology

Here we introduce a concept that links our two approaches to derivations. While the working diverged dramatically between the two different versions of derivations, they both lead to the same concept, namely cochains and further cohomology classes. Firstly, we must provide the definition of a cochain complex, following [12] and [13]:

Definition 49. *A **cochain complex** consists of a sequence of abelian groups or modules ..., $C^{-1}, C^0, C^1, ...$ along with a sequence of homomorphisms ..., d^{-1}, $d^0, d^1, ...$ as follows:*

$$\cdots \xrightarrow{d^{-2}} C^{-1} \xrightarrow{d^{-1}} C^0 \xrightarrow{d^0} C^1 \xrightarrow{d^1} C^2 \xrightarrow{d^2} \cdots$$

Figure 6.1: Cochain Complex

*such that $d^{n+1} \circ d^n = 0$ for all $n \in \mathbb{Z}$. The elements of C^n are the **cochains** of dimension n. We denote:*

$$Z^n = \ker\left(d^n\right),$$
$$B^n = \operatorname{im}\left(d^{n-1}\right).$$

*We call the elements of Z^n the **cocycles** of dimension n and the elements of B^n the **coboundaries** of dimension n. The **n^{th} cohomology group** H^n is given by:*

$$H^n = Z^n / B^n.$$

*The elements of H^n are called **cohomology classes** and we say that two cocycles are **cohomologous** if they belong to the same cohomology class.*

Since the groups C^n are abelian, the coboundaries of dimension n form a normal subgroup of the cocycles of dimension n and so the cohomology groups are all well-defined.

Although Definition 49 defines a cochain complex with cochains of all integer-valued dimensions, we may also consider cochain complexes with only a subset of these dimensions, as we will do in the proceeding sections. We may, for example, consider a complex with only non-negative dimensions:

$$C^0 \xrightarrow{d^0} C^1 \xrightarrow{d^1} C^2 \xrightarrow{d^2} \cdots$$

Figure 6.2: Cochain Complex with only non-negative dimensions

or even a cochain complex with a finite number of dimensions.

6.1 Eilenberg-Mac Lane Cohomology

Here we introduce a particular type of cochain complex, as defined in [5]. For this example, we begin with two groups, namely a multiplicative group Π and additive abelian group G, where Π acts on G. Explicitly, this means that for each $x \in \Pi$ and $g \in G$, $x \cdot g \in G$ and this action is such that:

$$\begin{aligned} x \cdot (g + h) &= x \cdot g + x \cdot h, \\ y \cdot (x \cdot g) &= (yx) \cdot g, \\ 1_\Pi \cdot g &= g \end{aligned}$$

for all $x, y \in \Pi$ and $g, h \in G$. Given this set-up, we define the cochains for $n \in \mathbb{N}$ as follows:

Definition 50. *A mapping $f : \Pi^{n+1} \to G$ is an n-dimensional **cochain** of Π over G if:*

$$f(xx_0, ..., xx_n) = x \cdot f(x_0, ..., x_n) \qquad \forall x, x_0, ..., x_n \in \Pi.$$

The set of n-dimensional cochains is denoted by $C^n(\Pi, G)$.

We define addition on cochains pointwise. Under this addition, $C^n(\Pi, G)$ is an abelian group. A crucial concept for this section is the **coboundary operator**

δ on cochains, which we define as the family of operators given by:

$$(\delta^n f)(x_0, ..., x_{n+1}) = \sum_{i=0}^{n+1} (-1)^i f(x_0, ..., x_{i-1}, x_{i+1}, ..., x_n)$$

for each $n \in \mathbb{N}$. We can also write $(x_0, ..., \hat{x_i}, ..., x_{n+1})$ to denote that x_i is omitted from the $n+1$-tuple.

It is very straightforward to see that $\delta^n f$ is an $n+1$-cochain for each n-dimensional cochain f and that $\delta^n(f+g) = \delta^n f + \delta^n g$ for all $f, g \in C^n(\Pi, G)$. Also, for any $f \in C^n(\Pi, G)$:

$$\begin{aligned}(\delta^{n+1}(\delta^n f))(x_0, ..., x_{n+2}) &= \sum_{i=0}^{n+2} (-1)^i (\delta f)(x_0, ..., \hat{x_i}, ..., x_{n+2}) \\ &= \sum_{i=0}^{n+2} (-1)^i \sum_{j=0}^{i-1} (-1)^j f(x_0, ..., \hat{x_j}, ..., \hat{x_i}, ..., x_{n+2}) \\ &\quad + \sum_{i=0}^{n+2} (-1)^i \sum_{j=i+1}^{n+2} (-1)^{j-1} f(x_0, ..., \hat{x_i}, ..., \hat{x_j}, ..., x_{n+2}).\end{aligned}$$

For each pair of indices i, j, the terms involving $f(x_0, ..., \hat{x_i}, ..., \hat{x_j}, ..., x_{n+2})$ will cancel each other out since the coefficient will be 1 for one and -1 for the other. Therefore:

$$(\delta^{n+1}(\delta^n f))(x_0, ..., x_{n+2}) = 0.$$

By the above working, for each $n \in \mathbb{N}$, δ^n is a homomorphism and $\delta^{n+1} \circ \delta^n = 0$. With this established we have that the following is a cochain complex:

$$C^0(\Pi, G) \xrightarrow{\delta^0} C^1(\Pi, G) \xrightarrow{\delta^1} C^2(\Pi, G) \xrightarrow{\delta^2} \cdots$$

Figure 6.3: Eilenberg-Mac Lane Cochain Complex

Explicitly, the cocyles and coboundaries within this framework are defined as follows:

Definition 51. *If $f \in C^n(\Pi, G)$ and $\delta^n f = 0$, then f is an n-dimensional **cocycle**. The set of such mappings is denoted by $Z^n(\Pi, G)$.*

Definition 52. *An n-cochain f such that $f = \delta^{n-1} g$ for some $g \in C^{n-1}(\Pi, G)$ is an n-dimensional **coboundary**. The set of these mappings is $B^n(\Pi, G)$. Formally, we set $B^0(\Pi, G) = \{0\}$.*

Fox claims in [7] that the Fox-derivations are simply the 1-dimensional cocyles. However, there is no explicit explanation of this fact. We independently constructed a cochain complex within the Eilenberg-Mac Lane approach to match this claim. We apply the Eilenberg-Mac Lane approach to X and $\mathbb{Z}[X]$, using X in the place of Π and $\mathbb{Z}[X]$ in the place of G. The action of X on $\mathbb{Z}[X]$ is simply the multiplication operation native to the group algebra. Clearly, X and $\mathbb{Z}[X]$ satisfy all of the required properties set up at the beginning of this section. Note that in this case each $C^n(X, \mathbb{Z}[X])$ is not just an abelian group but a right $\mathbb{Z}[X]$-module.

Theorem 13. *The module of all Fox-derivations of* $\mathbb{Z}[X]$ *is isomorphic to the* 1*-dimensional cocycles of* X *over* $\mathbb{Z}[X]$.

Proof. We will use the mapping $F : \mathrm{FDer}(\mathbb{Z}[X]) \to Z^1(X, \mathbb{Z}[X])$ defined as follows:

$$F(d)(x, y) = d(x) - d(y) \qquad \forall x, y \in X.$$

Firstly, for any Fox-derivation d we will denote $F(d) = d'$ for convenience's sake. Clearly, d' will be well-defined on X^2 and further:

$$\begin{aligned} d'(xu, xv) &= d(xu) - d(xv) \\ &= d(x) + x \cdot d(u) - d(x) - x \cdot d(v) \\ &= x \cdot (d(u) - d(v)) \\ &= x \cdot d'(u, v) \end{aligned}$$

for any $u, v, x \in X$, meaning that d' is a 1-dimensional cochain. Furthermore, for any $u, v, w \in X$:

$$\begin{aligned} \left(\delta^1 d'\right)(u, v, w) &= d'(v, w) - d'(u, w) + d'(u, v) \\ &= d(v) - d(w) - d(u) + d(w) + d(u) - d(v) \\ &= 0. \end{aligned}$$

Thus, $\delta^1 d' = 0$, i.e. d' is a 1-dimensional cocycle. Hence, we can conclude that $F\left(\mathrm{FDer}(X, \mathbb{Z}[X])\right) \subseteq Z^1(X, \mathbb{Z}[X])$.

Now let $d_1, d_2 \in \mathrm{FDer}(\mathbb{Z}[X])$ such that $F(d_1) = F(d_2)$. Then for any $u \in X$:

$$d_1'(u, 1) = d_2'(u, 1) \Rightarrow d_1(u) - d_1(1) = d_2(u) - d_2(1) \Rightarrow d_1(u) = d_2(u)$$

and so $d_1 = d_2$. Therefore, F is injective.

Next let $f \in Z^1(X, \mathbb{Z}[X])$. Then we define $d : X \to \mathbb{Z}[X]$ by $d(u) = f(u, 1)$ for all $u \in X$. Clearly, d is well-defined. Furthermore, since $\delta^1 f = 0$, we have that for any $u, v \in X$:

$$\begin{aligned} 0 &= \left(\delta^1 f\right)(uv, u, 1) \\ &= f(u, 1) - f(uv, 1) + f(uv, u) \\ &= f(u, 1) - f(uv, 1) + u \cdot f(v, 1) \end{aligned}$$

and so $f(uv, 1) = f(u, 1) + u \cdot f(v, 1)$. Thus:

$$\begin{aligned} d(uv) &= f(uv, 1) \\ &= f(u, 1) + u \cdot f(v, 1) \\ &= d(u) + u \cdot d(v). \end{aligned}$$

Therefore, following Proposition 10, the linear extension of d to $\mathbb{Z}[X]$ is a Fox-derivation. Moving forward, when we refer to d, we will mean this extension.

Now, we apply the fact that $\delta^1 f = 0$ repeatedly to find that:

$$\begin{aligned} 0 &= \left(\delta^1 f\right)(u, u, u) \\ &= f(u, u) - f(u, u) + f(u, u) \\ &= f(u, u) \end{aligned}$$

and:

$$\begin{aligned} 0 &= \left(\delta^1 f\right)(u, v, u) \\ &= f(v, u) - f(u, u) + f(u, v). \end{aligned}$$

Combining these two equations tells us that $f(v, u) = -f(u, v)$. Now, we again apply the cocycle property to obtain:

$$\begin{aligned} 0 &= \left(\delta^1 f\right)(v, 1, u) \\ &= f(1, u) - f(v, u) + f(v, 1) \\ \Rightarrow f(v, 1) &= f(v, u) - f(1, u). \end{aligned}$$

Thus, for any $u, v \in X$:

$$\begin{aligned} d'(u,v) &= d(u) - d(v) \\ &= f(u,1) - f(v,1) \\ &= f(u,1) - f(v,u) + f(1,u) \\ &= f(u,v). \end{aligned}$$

This is to say that $f = F(d)$. So F is surjective and hence bijective. It remains only to show that F is a homomorphism. Let $d_1, d_2 \in \mathrm{FDer}(\mathbb{Z}[X])$. Then for any $u, v \in X$:

$$\begin{aligned} F(d_1 + d_2)(u,v) &= (d_1 + d_2)(u) - (d_1 + d_2)(v) \\ &= d_1(u) + d_2(u) - d_1(v) - d_2(v) \\ &= F(d_1)(u,v) + F(d_2)(u,v) \end{aligned}$$

and so $F(d_1 + d_2) = F(d_1) + F(d_2)$. Lastly, let $d \in \mathrm{FDer}(\mathbb{Z}[X])$ and $w \in \mathbb{Z}[X]$. Then for any $u, v \in X$:

$$\begin{aligned} F(d \cdot w)(u,v) &= (d \cdot w)(u) - (d \cdot w)(v) \\ &= d(u) \cdot w - d(v) \cdot w \\ &= F(d)(u,v) \cdot w \end{aligned}$$

and so $F(d \cdot w) = F(d) \cdot w$. Therefore, F is homomorphic and we can conclude that F is an isomorphism. Thus:

$$\mathrm{FDer}(\mathbb{Z}[X]) \cong Z^1(X, \mathbb{Z}[X]). \qquad \square$$

This shows that the Fox-derivations are indeed precisely the 1-dimensional cocycles within the Eilenberg-Mac Lane cohomology. However, we also obtain the following result regarding the inner Fox-derivations, not mentioned at all in the literature:

Theorem 14. *The module of all inner Fox-derivations over $\mathbb{Z}[X]$ is isomorphic to the 1-dimensional coboundaries of X over $\mathbb{Z}[X]$.*

Proof. We again use the same mapping F as in the previous proof, except that now we restrict the map to $\mathrm{FInn}(\mathbb{Z}[X])$ and establish that its image is now $B^1(X, \mathbb{Z}[X])$. Much of the working from the previous proof carries over

here: only the corestrictedness and surjectivity of F within this context must be shown.

Suppose that $d_f \in \mathrm{FInn}(\mathbb{Z}[X])$ where $f \in \mathbb{Z}[X]$. Then $F(d_f)$ is a cocycle by the previous proof. Now we construct a 0-dimensional cochain ϕ given by $\phi(u) = u \cdot f$ for $u \in X$. ϕ is indeed a cochain as for any $u, x \in X$:

$$\phi(xu) = xu \cdot f = x \cdot u \cdot f = x \cdot \phi(u).$$

Further, for any $u, v \in X$:

$$\begin{aligned}\left(\delta^0\phi\right)(u,v) &= \phi(v) - \phi(u) \\ &= v \cdot f - u \cdot f \\ &= (f - u \cdot f) - (f - v \cdot f) \\ &= d_f(u) - d_f(v) \\ &= d'_f(u,v)\end{aligned}$$

and so $F(d_f) = \delta^0\phi$, i.e. it is a coboundary. Therefore, F is corestricted: $F\left(\mathrm{FInn}(\mathbb{Z}[X])\right) \subseteq B^1(X, \mathbb{Z}[X])$.

Now let $\varphi \in B^1(X, \mathbb{Z}[X])$. Then φ is a cochain such that $\varphi = \delta^0\psi$ for some 0-dimensional cochain ψ. So, for all $u, v \in X$:

$$\varphi(u,v) = \psi(v) - \psi(u) = v \cdot \psi(1) - u \cdot \psi(1) = (v - u) \cdot \psi(1).$$

Hence:

$$\begin{aligned}d'_{\psi(1)}(u,v) &= d_{\psi(1)}(u) - d_{\psi(1)}(v) \\ &= \psi(1) - u \cdot \psi(1) - \psi(1) + v \cdot \psi(1) \\ &= (v - u) \cdot \psi(1) \\ &= \varphi(u,v).\end{aligned}$$

Thus, $\varphi = F\left(d_{\psi(1)}\right)$, meaning that F is surjective. We conclude:

$$\mathrm{FInn}(\mathbb{Z}[X]) \cong B^1(X, \mathbb{Z}[X]). \qquad \square$$

From these two theorems, we can extrapolate a further result. If we were to

define the outer Fox-derivations in the natural way:

$$\mathrm{FOut}(\mathbb{Z}[X]) = \mathrm{FDer}(\mathbb{Z}[X])/\,\mathrm{FInn}(\mathbb{Z}[X]),$$

then:

Corollary 4.

$$\mathrm{FOut}(\mathbb{Z}[X]) \cong H^1(X, \mathbb{Z}[X]).$$

This corollary is an obvious consequence of Theorems 13 and 14.

6.2 Cayley Complex Cohomology

We now show how the derivations of $\mathbb{C}[G]$ also connect to cohomology, but in rather a different way. This follows the approach taken in [11], although expanding significantly at some crucial points and omitting the many examples which make up the latter portion of the paper. This is in a sense a continuation of Chapter 5 and so we will be using all of the same notation.

Thus far we have only demanded that the underlying group G be discrete and finitely generated, however, here we demand that G be a discrete finitely presentable group. To explain what this means we must introduce some new notation for defining groups: we write $G = \langle X : R \rangle$ to express that X is the set of **generators** of G and R is the set of **relations**. This means that G is the group of all words composed of elements from X and their inverses under the restriction that each word in R is equal to identity in G. This notation $\langle X : R \rangle$ is the **presentation** of G. Having explained this:

Definition 53. *A group G is **finitely presentable** if it can be written in the form $G = \langle X : R \rangle$ where the sets X of generators and R of relations are both finite.*

It is obvious that every finitely presentable group is finitely generated. A free group is the simplest type of finitely presentable group: its set of relations is empty. We already discussed some other examples of finitely generated groups at the end of Chapter 5.4: the group Y defined there can be written as $Y = \left\langle (x) : \left\{ x_j^2 : x_j \in (x) \right\} \right\rangle$.

6.2.1 Presentation of the Groupoid of the Adjoint Action

Given a finitely presentable group $G = \langle X : R \rangle$, we want to find the presentation of Γ. This presentation will be slightly different to the presentations of groups we refer to above since Γ is a category and not a group. The class of objects $\mathrm{Obj}(\Gamma)$ gives no issues since $\mathrm{Obj}(\Gamma) = G$ and so we can present it in exactly the same way. However, $\mathrm{Mor}(\Gamma)$ must be presented in an analogous way for morphisms which we will describe in detail when the time comes.

Since both X and R are assumed to be finite, we can write $X = \{x_1, x_2, ..., x_n\}$ and $R = \{r_1, r_2, ..., r_m\}$. Firstly, we set:

$$\chi = \left\{ \left(\frac{a \to b}{x} \right) \in \mathrm{Mor}(\Gamma) : x \in X \right\}.$$

Further, we set $Y = \chi \cup \chi^{-1}$, the set of every morphism whose denominator is either a generator or the inverse of a generator. Now we introduce the system Q derived from the set of relations R. Every relation $r_i \in R$ is a word:

$$r_i = y_{i_1} y_{i_2} \cdots y_{i_{l_i}}$$

where $y_{i_1}, y_{i_2}, ..., y_{i_{l_i}} \in X \cup X^{-1}$. Then for each $a \in \mathrm{Obj}(\Gamma)$, r_i generates the following word $\rho_{i,a}$:

$$\rho_{i,a} = \left(\frac{a_2 \to a_1}{y_{i_1}} \right) \left(\frac{a_3 \to a_2}{y_{i_2}} \right) \cdots \left(\frac{a_1 \to a_{l_i}}{y_{i_{l_i}}} \right) \tag{6.1}$$

where $a_1 = a$ and $a_{j+1} = y_{i_j}^{-1} a_j y_{i_j}$ for each $j = 1, 2, ..., l_i$. Note that using this inductive definition:

$$\begin{aligned} a_{l_i+1} &= y_{i_{l_i}}^{-1} a_{l_i} y_{i_{l_i}} \\ &= y_{i_{l_i}}^{-1} y_{i_{l_i-1}}^{-1} a_{l_i-1} y_{i_{l_i-1}} y_{i_{l_i}} \\ &= \cdots \\ &= r_i^{-1} a_1 r_i \\ &= a_1 \end{aligned}$$

since r_i is equal to the group identity by definition. This is why the final morphism in the word $\rho_{i,a}$ has domain a_1. Thus, the composition corresponding

to $\rho_{i,a}$ is:

$$\left(\frac{a_2 \to a_1}{y_{i_1}}\right) \circ \left(\frac{a_3 \to a_2}{y_{i_2}}\right) \circ \cdots \circ \left(\frac{a_1 \to a_{l_i}}{y_{i_{l_i}}}\right) = \left(\frac{a_1 \to a_1}{r_i}\right) = \left(\frac{a \to a}{e}\right) \tag{6.2}$$

which is a compositional identity in $\mathrm{Mor}(\Gamma)$: $\left(\frac{a \to a}{e}\right) = \mathrm{Id}_a$. We define:

$$Q = \{\rho_{i,a} : 1 \leq i \leq m, a \in \mathrm{Obj}(\Gamma)\}.$$

It is important to note at some point that the construction of $\rho_{i,a}$ is different to that in [11]. This is because the construction in [11] does not yield the desired results, whereas this one does. We believe this to be the result of a very minor error on the part of the author since our construction required only a very slight adjustment.

Having established all of this we are ready to give the presentation of the class of morphisms:

$$\mathrm{Mor}(\Gamma) = \langle \chi : Q \rangle . \tag{6.3}$$

By this we mean that $\mathrm{Mor}(\Gamma)$ is the class of all compositions of elements from χ and their inverses under the restriction that every composition corresponding to a word in Q is an identity morphism. Before moving on, we must show the legitimacy of this presentation. Firstly, it is obvious that any composition formed from $\chi \cup \chi^{-1}$ is a morphism in $\mathrm{Mor}(\Gamma)$ and likewise that all the compositions corresponding to words in Q are identity morphisms, as per Equation (6.2). However, we must show that every morphism is generated from elements of χ and their inverses and that Q generates every composition equal to an identity morphism:

Suppose that $\xi \in \mathrm{Mor}(\Gamma)$. We let $\xi = \left(\frac{a \to b}{g}\right)$. Then g must be presentable as:

$$g = y_1 y_2 \cdots y_k$$

where $y_1, y_2, ..., y_k \in X \cup X^{-1}$. Thus:

$$\left(\frac{a \to b}{g}\right) = \left(\frac{c_2 \to c_1}{y_1}\right) \circ \left(\frac{c_3 \to c_2}{y_2}\right) \circ \cdots \circ \left(\frac{c_{k+1} \to c_k}{y_k}\right) \tag{6.4}$$

where $c_1 = b$ and $c_{j+1} = y_j^{-1} c_j y_j$ for $j = 1, 2, ..., k$. This works because, similarly to above with a_{l_i+1}, $c_{k+1} = g^{-1} b g = a$. It is obvious that for each

$j = 1, ..., k$, $\left(\frac{c_{j+1} \to c_j}{y_j}\right) \in \chi \cup \chi^{-1}$, and so we have written ξ in the desired form.

Next suppose that we have a composition $\xi_1 \circ \xi_2 \circ \cdots \circ \xi_q = \mathrm{Id}_a$ for some object $a \in \mathrm{Obj}(\Gamma)$. For each $j = 1, .., q$ we can write $\xi_j = \left(\frac{a_{j+1} \to a_j}{g_j}\right)$ where $a_1 = a = a_{q+1}$ and $g_1 g_2 \cdots g_q = e$:

$$\xi_1 \circ \xi_2 \circ \cdots \circ \xi_q = \left(\frac{a_2 \to a_1}{g_1}\right) \circ \left(\frac{a_3 \to a_2}{g_2}\right) \circ \cdots \circ \left(\frac{a_1 \to a_q}{g_q}\right).$$

However, every ξ_j can itself be decomposed as above:

$$\xi_j = \left(\frac{a_{j+1} \to a_j}{g_j}\right) = \left(\frac{c_{j_2} \to c_{j_1}}{y_{j_1}}\right) \circ \left(\frac{c_{j_3} \to c_{j_2}}{y_{j_2}}\right) \circ \cdots \circ \left(\frac{c_{j_{k_j+1}} \to c_{j_{k_j}}}{y_{j_{k_j}}}\right)$$

following the exact same approach to decomposition as in Equation (6.4). Thus, $g_1 g_2 \cdots g_q = y_{1_1} y_{1_2} \cdots y_{1_{k_1}} y_{2_1} \cdots y_{2_{k_2}} \cdots y_{q_1} \cdots y_{q_{k_q}} = e$. But then this word must have the form:

$$y_{1_1} y_{1_2} \cdots y_{1_{k_1}} y_{2_1} \cdots y_{2_{k_2}} \cdots y_{q_1} \cdots y_{q_{k_q}} = s_1 s_2 \cdots s_t$$

where $s_p \in R \cup R^{-1}$ for each p. To be clear, this is not simply saying that both sides of the equation are equal in G but that each s_p appears within the word $y_{1_1} y_{1_2} \cdots y_{1_{k_1}} y_{2_1} \cdots y_{2_{k_2}} \cdots y_{q_1} \cdots y_{q_{k_q}}$ in order. Therefore, the composition can be split up into compositions of the form:

$$\left(\frac{c_{j_{h+1}} \to c_{j_h}}{y_{j_h}}\right) \circ \left(\frac{c_{j_{h+2}} \to c_{j_{h+1}}}{y_{j_{h+1}}}\right) \circ \cdots \circ \left(\frac{c_{j_h} \to c_{j_d}}{y_{j_d}}\right)$$

where $y_{j_h} y_{j_{h+1}} \cdots y_{j_d} = s_p$ for some $p = 1, 2, ..., t$. If $s_p = r_i$ for some $r_i \in R$, then:

$$\left(\frac{c_{j_{h+1}} \to c_{j_h}}{y_{j_h}}\right) \left(\frac{c_{j_{h+2}} \to c_{j_{h+1}}}{y_{j_{h+1}}}\right) \cdots \left(\frac{c_{j_h} \to c_{j_d}}{y_{j_d}}\right) = \rho_{i, c_{j_h}}$$

and if $s_p = r_i^{-1}$, then:

$$\left(\frac{c_{j_{h+1}} \to c_{j_h}}{y_{j_h}}\right) \left(\frac{c_{j_{h+2}} \to c_{j_{h+1}}}{y_{j_{h+1}}}\right) \cdots \left(\frac{c_{j_h} \to c_{j_d}}{y_{j_d}}\right) = \left(\rho_{i, c_{j_h}^{-1}}\right)^{-1}.$$

Thus, the composition $\xi_1 \circ \xi_2 \circ \cdots \circ \xi_j$ can be decomposed so that its corresponding word consists of words from $Q \cup Q^{-1}$.

Therefore, Equation (6.3) is indeed a presentation of $\mathrm{Mor}(\Gamma)$.

6.2.2 Cayley Complex of a Group

For any finitely presentable group, we can construct its Cayley complex. This builds upon the simpler notion of the Cayley graph:

Definition 54. *If G is a group generated by X, then the Cayley graph of G with respect to X is a directed graph, where each element of G is assigned a vertex and for each generator $x \in X$ there is a directed edge going from g to gx.*

Here is a visualisation of a portion of a Cayley graph:

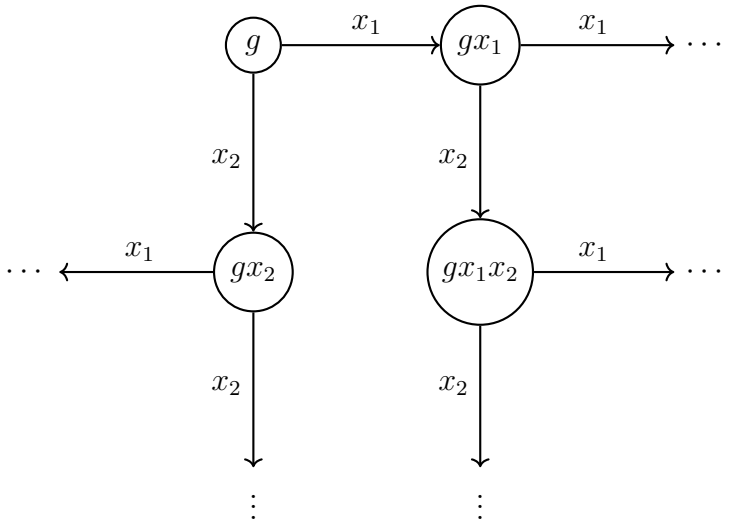
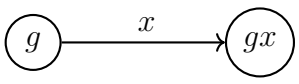


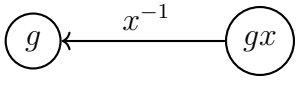
Figure 6.4: Cayley Graph of a Group

where x_1 and x_2 are generators and g is simply some group element. Note that there will also be edges pointing into g, for instance there will be an edge labelled x_1 going from gx_1^{-1} to g. For the sake of comprehensibility we have chosen not to make the above graph exhaustive.

We may also consider edges corresponding to generators' inverses. By convention, though, an edge



is considered to be the same edge as



but with opposite direction. By this approach, Figure 6.4 could equivalently be represented as:

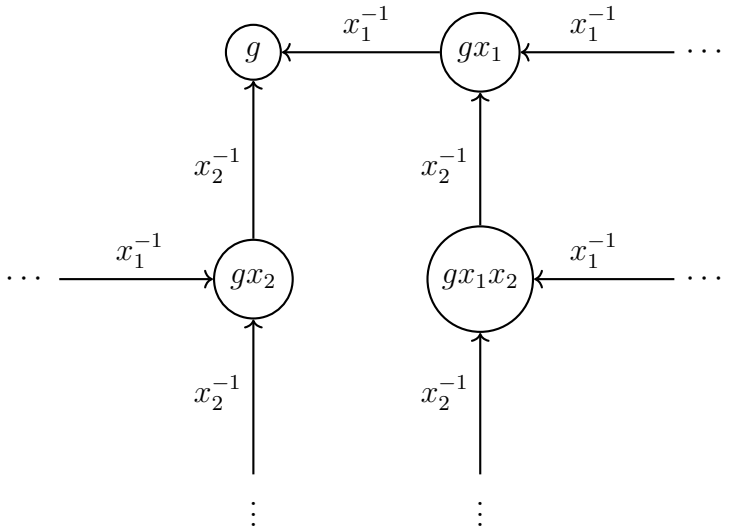


Figure 6.5: Inverted Representation of Figure 6.4

The **Cayley complex** furthers the idea of representing a group by means of a graph by not only capturing the elements and generators of G but also incorporating the relations. Moving forward we will say that $G = \langle X : R \rangle$. We will denote the Cayley complex of G by $\mathrm{Ca}(G)$. In the strictest sense, $\mathrm{Ca}(G)$ is a two-dimensional cell-complex, however, we will not entirely explain what this means since it is outside of the scope of this work. For our purposes we can simply say that the Cayley complex consists of zero-dimensional components (or cells), namely vertices representing the group elements, one-dimensional cells, namely edges representing the generators, and two-dimensional cells, namely polygons representing the relations. The set of zero-dimensional cells is denoted $\mathrm{Ca}_0(G)$ and similar notation is used for the higher dimensions. This is a similar idea to the Cayley graph but now the cycles formed by relations are considered. We will visualise what we mean by this below. Here we will consider a relation $r = y_1 y_2 \cdots y_l$:

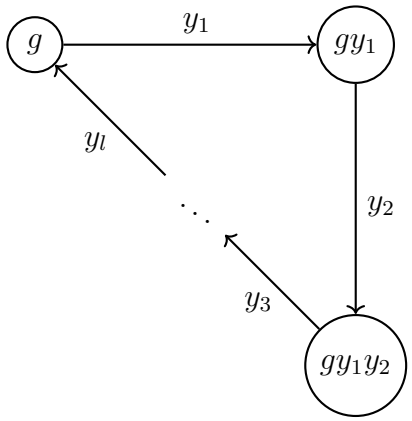


Figure 6.6: Relation in the Cayley Complex of a Group

The polygon formed by the edges $y_1, y_2, ..., y_l$ is a two-dimensional cell in the Cayley complex. The polygon formed by r^{-1} can be considered equivalent but with opposite orientation. It should be clear that every relation will form a polygon in this way around every vertex. Note, however, that not every edge will form part of such a polygon. If we have some $x \in X$ such that x is not present in any relations in R, then any edge labeled x will not form a part of any two-dimensional cell. If G were a free group, then R would be empty and the Cayley complex would have no two-dimensional cells whatsoever.

6.2.3 Cayley Complex of Γ

Having set up the Cayley complex for a group $G = \langle X : R \rangle$, we can now move on to the Cayley complex of the groupoid of its adjoint action. Remembering that $\mathrm{Mor}(\Gamma) = \langle \chi : Q \rangle$, we will use this presentation to construct the Cayley complex just as we used the presentation of G in the previous section. In [11], the Cayley complex of the groupoid of right multiplication is first constructed, however, we judge this to be unnecessary. We will therefore immediately proceed to $\mathrm{Ca}(\Gamma)$.

The zero-dimensional cells are simply vertices given by $\mathrm{Ca}_0(\Gamma) = \mathrm{Obj}(\Gamma)$. Similar to the construction with groups, the one-dimensional cells are directed edges, this time represented by morphisms: $\mathrm{Ca}_1(\Gamma) = \chi \cup \chi^{-1}$. Each morphism $\left(\frac{a \to b}{x}\right) \in \chi$ is directed from vertex a to b. Here is a visualisation of this Cayley complex's zero- and one-dimensional cells:

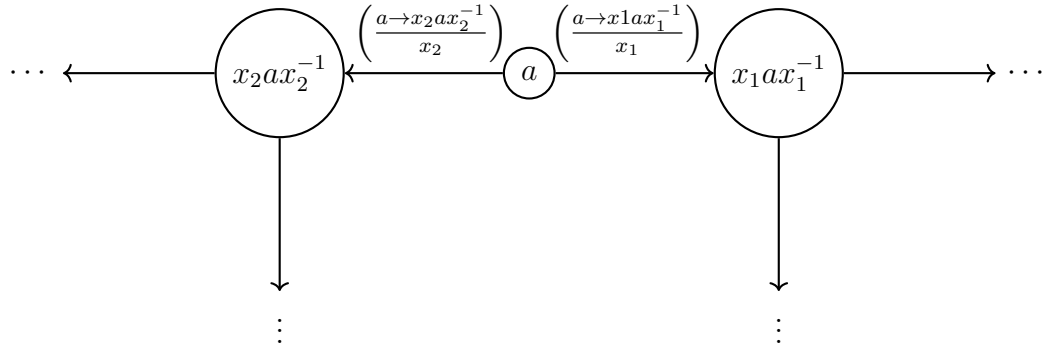


Figure 6.7: Cayley Complex of Γ

where x_1 and x_2 are generators. Similarly to the case of $\mathrm{Ca}(G)$, we consider the edges $\left(\frac{a\to b}{x}\right)$ and $\left(\frac{b\to a}{x^{-1}}\right)$ to be the same edge with opposite direction. The two-dimensional cells $\mathrm{Ca}_2(\Gamma)$ are polygons representing the words in Q (or indeed in Q^{-1}). So for any word $\rho_{i,a} = \left(\frac{a_2\to a_1}{y_{i_1}}\right)\left(\frac{a_3\to a_2}{y_{i_2}}\right)\cdots\left(\frac{a_1\to a_{l_i}}{y_{i_{l_i}}}\right)$ we obtain a polygon as follows:

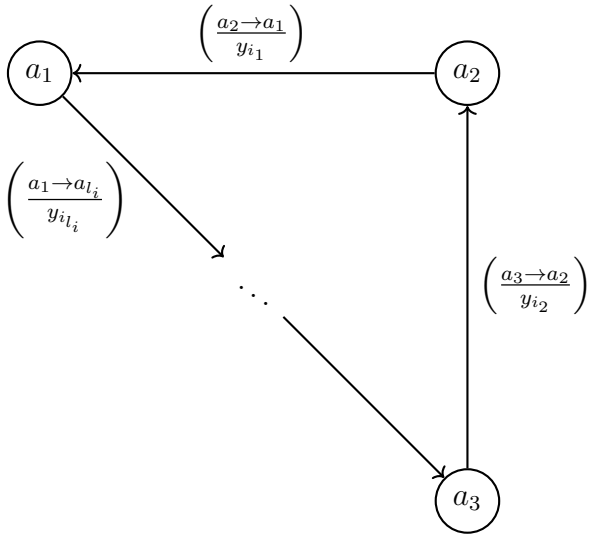


Figure 6.8: Relation in the Cayley Complex of Γ

The cells for $\rho_{i,a}$ and $(\rho_{i,a})^{-1}$ are considered to be the same cell with opposite orientation.

It should be obvious that two vertices a and b can only be connected by a series of edges if they belong to the same conjugacy class. Therefore, the Cayley complex for Γ will be made up of disconnected Cayley complexes, each corresponding to a different conjugacy class. In this sense $\mathrm{Ca}(\Gamma)$ consists of

distinct complexes $\mathrm{Ca}\left(\Gamma_{[u]}\right)$, one for each $[u] \in [G]$.

6.2.4 Cochain Complex of Ca(Γ)

After establishing this Cayley complex, [11] claims that this generates the cochain complex:

$$C^0(\mathrm{Ca}(\Gamma)) \xrightarrow{d^0} C^1(\mathrm{Ca}(\Gamma)) \xrightarrow{d^1} C^2(\mathrm{Ca}(\Gamma)$$

Figure 6.9: Cochain Complex of $Ca(\Gamma)$

However, there is no explanation as to the precise nature of this cochain complex. For this reason we have decided to construct our own which we believe matches what they intended, similar to how we constructed our own Eilenberg-Mac Lane cochain complex in Section 6.1:

$C^0(\mathrm{Ca}(\Gamma)) = \mathbb{C}^{\mathrm{Ca}_0(\Gamma)}$, the set of all mappings from $\mathrm{Ca}_0(\Gamma)$ to $\mathbb{C}$. Similarly, $C^1(\mathrm{Ca}(\Gamma))$ is the set of mappings from $\mathrm{Ca}_1(\Gamma)$ to $\mathbb{C}$ and $C^2(\mathrm{Ca}(\Gamma))$ is the set of mappings from $\mathrm{Ca}_2(\Gamma)$ to $\mathbb{C}$. Clearly these are all vector spaces over $\mathbb{C}$, defining addition and scalar multiplication pointwise on each. For each $\phi \in C^0(\mathrm{Ca}(\Gamma))$ we define:

$$d^0(\phi)\left(\frac{a \to b}{x}\right) = \phi(b) - \phi(a)$$

for all $\left(\frac{a \to b}{x}\right) \in \mathrm{Ca}_1(\Gamma)$. For each $\psi \in C^1(\mathrm{Ca}(\Gamma))$ we define:

$$d^1(\psi)\left(\left(\frac{a_2 \to a_1}{y_1}\right) \cdots \left(\frac{a_1 \to a_l}{y_l}\right)\right) = \sum_{i=1}^{l} \psi\left(\frac{a_{i+1} \to a_i}{y_i}\right)$$

for all $\left(\frac{a_2 \to a_1}{y_1}\right) \cdots \left(\frac{a_1 \to a_l}{y_l}\right) \in \mathrm{Ca}_2(\Gamma)$. In order for this to indeed be a cochain complex we require that d^0 and d^1 be homomorphisms such that $d^1 \circ d^0 = 0$. It should be immediately obvious that they are vector space homomorphisms. Now, for any $\phi \in C^0(\mathrm{Ca}(\Gamma))$ we find that for all $\left(\frac{a_2 \to a_1}{y_1}\right) \cdots \left(\frac{a_1 \to a_l}{y_l}\right) \in \mathrm{Ca}_2(\Gamma)$:

$$\begin{aligned}
&\left(d^1 \circ d^0\right)(\phi)\left(\left(\frac{a_2 \to a_1}{y_1}\right) \cdots \left(\frac{a_1 \to a_l}{y_l}\right)\right) \\
&= d^1\left(d^0(\phi)\right)\left(\left(\frac{a_2 \to a_1}{y_1}\right) \cdots \left(\frac{a_1 \to a_l}{y_l}\right)\right) \\
&= \sum_{i=1}^{l} d^0(\phi)\left(\frac{a_{i+1} \to a_i}{y_i}\right)
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{i=1}^{l} \left(\phi\left(a_{i+1}\right) - \phi\left(a_i\right)\right) \\
&= \phi(a_{l+1}) - \phi(a_1) \\
&= \phi(a_1) - \phi(a_1) \\
&= 0
\end{aligned}
$$

and so $d^1 \circ d^0 = 0$ as desired. Therefore, Figure 6.9 shows a cochain complex. Having now constructed this cochain complex, we now return to following [11] closely, but in considerably more detail.

Our main interest lies in a subcomplex:

$$C_f^0(\mathrm{Ca}(\Gamma)) \xrightarrow{d_f^0} C_f^1(\mathrm{Ca}(\Gamma)) \xrightarrow{d_f^1} C_f^2(\mathrm{Ca}(\Gamma)$$

Figure 6.10: Finitely Supported Subcomplex

Here we consider only finitely supported cochains, that is $C_f^0(\mathrm{Ca}(\Gamma))$ consists of all mappings $\phi : \mathrm{Ca}_0(\Gamma) \to \mathbb{C}$ such that $\phi(g) \neq 0$ for only finitely many $g \in \mathrm{Ca}_0(\Gamma)$. $C_f^1(\mathrm{Ca}(\Gamma))$ and $C_f^2(\mathrm{Ca}(\Gamma))$ differ from their counterparts in Figure 6.9 in the same manner. The mappings d_f^0 and d_f^1 are simply the restrictions of d^0 and d^1 to mappings with finite support.

Is it guaranteed that Figure 6.10 is a cochain complex? All the properties of a cochain complex from Definition 49 are easily seen to be satisfied except for the corestrictedness of d_f^0 and d_f^1: is it certain that every finitely supported mapping will be mapped to another finitely supported mapping? We will show that it is:

Let $\phi \in C_f^0(\mathrm{Ca}(\Gamma))$. Then there exist finitely many $g \in \mathrm{Ca}_0(\Gamma)$ such that $\phi(g) \neq 0$. For each such object, let us consider all the morphisms $\phi \in \mathrm{Ca}_1(\Gamma)$ with domain or codomain g. These morphisms all have a denominator from $X \cup X^{-1}$, remembering that X is the set of generators for the underlying group G. Since G is assumed to be finitely presentable, X is finite. There can be only one morphism with domain g (or codomain g) and denominator y for each $y \in X \cup X^{-1}$. Therefore, the total number of morphisms in $\mathrm{Ca}_1(\Gamma)$ with domain or codomain g is at most twice the cardinality of $X \cup X^{-1}$ and hence at most four times the cardinality of X, a finite number. Now consider all the morphisms $\left(\frac{a \to b}{x}\right) \in \mathrm{Ca}_1(\Gamma)$ such that $d_f^0(\phi)\left(\frac{a \to b}{x}\right) \neq 0$. For this to be the case, we must have $\phi(b) \neq 0$ or $\phi(a) \neq 0$. But there are only finitely many objects

b or a satisfying this, each of which is the domain or codomain of only finitely many morphisms in $\mathrm{Ca}_1(\Gamma)$. Hence, there are only finitely many such $\left(\frac{a\to b}{x}\right)$. Thus, $d_f^0(\phi)$ is finitely supported, proving that d_f^0 is corestricted as desired.

Now let $\psi \in C_f^1(\mathrm{Ca}(\Gamma))$. Then there are finitely many $\xi \in \mathrm{Ca}_1(\Gamma)$ such that $\psi(\xi) \neq 0$. For every such morphism, let us consider all the words $\rho_{i,a} \in \mathrm{Ca}_2(\Gamma)$ in which ξ appears. Let $\xi = \left(\frac{b\to c}{y}\right)$. Remember that the index i corresponds to the relations $r_i \in R$, meaning that it indexes over a finite set. For each i such that ξ appears in some $\rho_{i,a}$, this requires that $y = y_{i_j}$ for some $j = 1, ..., l_i$. Returning to the definition of $\rho_{i,a}$ in Equation (6.1), we can therefore rewrite ξ as $\xi = \left(\frac{y_{i_j}^{-1} c y_{i_j} \to c}{y_{i_j}}\right)$. This identification of ξ with the indices i and j is unique, by which we mean that for distinct words the resulting indices will be distinct. But i indexes over a finite set and for each i, j also indexes over a finite set. Therefore, the total number of such words containing ξ is finite. The same applies when we consider $(\rho_{i,a})^{-1}$. We can conclude that the total number of words $\rho \in \mathrm{Ca}_2(\Gamma)$ containing ξ is finite. Using similar logic to that at the end of the previous paragraph, we can extrapolate that there are finitely many $\rho \in \mathrm{Ca}_2(\Gamma)$ such that $d_f^1(\psi)(\rho) \neq 0$ and hence that d_f^1 is corestricted.

Thus, Figure 6.10 does in fact show a cochain complex. This cochain complex is of paramount importance to us because we will use it to obtain analogous results to Theorems 13 and 14 from Section 6.1:

Theorem 15. *The Lie algebra* $\mathrm{Der}(\mathbb{C}[G])$ *of derivations of* $\mathbb{C}[G]$ *is isomorphic to the 1-dimensional cocycles* $Z_f^1(\mathrm{Ca}(\Gamma))$.

Proof. First we must recall from Definition 49 that $Z_f^1(\mathrm{Ca}(\Gamma)) = \ker\left(d_f^1\right)$.

We already know that $\mathrm{Der}(\mathbb{C}[G])$ is isomorphic to the space of locally finitely supported characters $T_f(\Gamma)$. We can therefore prove the theorem by showing that $T_f(\Gamma)$ is isomorphic to $Z_f^1(\mathrm{Ca}(\Gamma))$, following Note 7. We will use the mapping $\varphi : T_f(\Gamma) \to Z_f^1(\mathrm{Ca}(\Gamma))$ defined by:

$$\varphi\left(T^d\right) = T^d|_{\mathrm{Ca}_1(\Gamma)} \qquad \forall T^d \in T_f(\Gamma).$$

First we must show that $\varphi\left(T_f(\Gamma)\right) \subseteq Z_f^1(\mathrm{Ca}(\Gamma))$: let $T^d \in T_f(\Gamma)$. Clearly $\varphi\left(T^d\right)$ is a mapping from $\mathrm{Ca}_1(\Gamma)$ to $\mathbb{C}$, but is it finitely supported? T^d is locally finitely supported and so for each $g \in G$ there are only finitely many $\left(\frac{a\to b}{g}\right)$ such that $T^d\left(\frac{a\to b}{g}\right) \neq 0$. But there are finitely many denominators in $\mathrm{Ca}_1(\Gamma)$, since we only allow denominators from $X \cup X^{-1}$. Therefore, there are finitely

many $\xi \in \mathrm{Ca}_1(\Gamma)$ such that $T^d(\xi) \neq 0$, i.e. $T^d|_{\mathrm{Ca}_1(\Gamma)}$ is finitely supported. Thus, $\varphi\left(T^d\right) \in C_f^1(\mathrm{Ca}(\Gamma))$. Furthermore, for any $\rho = \left(\frac{a_2 \to a_1}{y_1}\right) \cdots \left(\frac{a_1 \to a_l}{y_l}\right) \in \mathrm{Ca}_2(\Gamma)$:

$$\begin{aligned} d_f^1\left(\varphi\left(T^d\right)\right)(\rho) &= \sum_{i=1}^{l} \varphi\left(T^d\right)\left(\frac{a_{i+1} \to a_i}{y_i}\right) \\ &= \sum_{i=1}^{l} T^d\left(\frac{a_{i+1} \to a_i}{y_i}\right) \\ &= T^d\left(\left(\frac{a_2 \to a_1}{y_1}\right) \circ \cdots \circ \left(\frac{a_1 \to a_l}{y_l}\right)\right) \\ &= T^d\left(\frac{a_1 \to a_1}{e}\right) \\ &= 0 \end{aligned}$$

since T^d is a character and because of how $\mathrm{Ca}_2(\Gamma)$ is defined. Thus, we obtain $d_f^1(\varphi\left(T^d\right)) = 0$ and hence $\varphi\left(T^d\right) \in Z_f^1(\mathrm{Ca}(\Gamma))$.

Having just shown that φ is corestricted, we will now show that it is injective. We will do this by showing that $\ker(\varphi) = \{0\}$: suppose that $\varphi\left(T^d\right) = 0$ for $T^d \in T_f(\Gamma)$. Then $T^d(\xi) = 0$ for all $\xi \in \mathrm{Ca}_1(\Gamma)$. Let $\xi = \left(\frac{a \to b}{g}\right) \in \mathrm{Mor}(\Gamma)$. But as per Equation (6.3), every morphism can be decomposed into the composition of morphisms from χ and inverses, i.e. morphisms in $\mathrm{Ca}_1(\Gamma)$. So:

$$\xi = \xi_1 \circ \cdots \circ \xi_k$$

for some $\xi_1, ..., \xi_k \in \mathrm{Ca}_1(\Gamma)$. Therefore:

$$T^d(\xi) = T^d(\xi_1) + \cdots + T^d(\xi_k) = 0 + \cdots + 0 = 0$$

meaning that $T^d = 0$. Thus, $\ker(\varphi) = \{0\}$.

It remains only to show that φ is surjective. Let $\phi \in Z_f^1(\mathrm{Ca}(\Gamma))$. Then $\phi : \mathrm{Ca}_1(\Gamma) \to \mathbb{C}$ is finitely supported and $\sum_{i=1}^{l} \phi\left(\frac{a_{i+1} \to a_i}{y_i}\right) = 0$ for any $\left(\frac{a_2 \to a_1}{y_1}\right) \cdots \left(\frac{a_1 \to a_l}{y_l}\right) \in \mathrm{Ca}_2(\Gamma)$.

Now, for every $\xi = \left(\frac{a \to b}{g}\right) \in \mathrm{Mor}(\Gamma)$, we will decompose ξ into morphisms from $\mathrm{Ca}_1(\Gamma)$ just as we did earlier while showing that φ is injective. Here we must be more explicit, though. First we decompose g into $g = y_1 \cdots y_k$ where $y_1, ..., y_k \in X \cup X^{-1}$. Then:

$$\xi = \xi_1 \circ \cdots \circ \xi_k$$

where $\xi_i = \left(\frac{a_{i+1} \to a_i}{y_i}\right)$ for each $i = 1, ..., k$, defining $a_1 = b$ and $a_{i+1} = y_i^{-1} a_i y_i$. We define:

$$T^d(\xi) = \sum_{i=1}^{k} \phi\left(\frac{a_{i+1} \to a_i}{y_i}\right).$$

Note that this T^d is well-defined: it does not depend on the choice of expansion for g. Any distinct expansions of g can differ only in that one contains relations of G not present in the other. But when translating these relations into morphisms as above, we will obtain compositions of morphisms corresponding to words in $\mathrm{Ca}_2(\Gamma)$. By hypothesis, these will disappear in T^d.

Obviously T^d is a character. Its local finite support is not as obvious: let us fix $g \in G$ and consider all $\xi = \left(\frac{a \to b}{g}\right) \in \mathrm{Mor}(\Gamma)$ such that $T^d(\xi) \neq 0$. This means that there exists $\xi_i = \left(\frac{a_{i+1} \to a_i}{y_i}\right)$ in the decomposition $\xi = \xi_1 \circ \cdots \circ \xi_k$ such that $\phi(\xi_i) \neq 0$. This can only be true for finitely many morphisms in $\mathrm{Ca}_1(\Gamma)$. However, this same ξ_i may appear in the decomposition of multiple morphisms over g: consider $\left(\frac{c \to d}{g}\right) \neq \left(\frac{a \to b}{g}\right)$ such that $\left(\frac{c_{j+1} \to c_j}{y_j}\right) = \left(\frac{a_{i+1} \to a_i}{y_i}\right)$ for some j. Then $y_i = y_j$ but $i \neq j$ since $i = j$ would imply that $a = c$ and hence that $\left(\frac{c \to d}{g}\right) = \left(\frac{a \to b}{g}\right)$. Therefore, we must have that the same $y_i \in X \cup X^{-1}$ appears more than once in the decomposition $g = y_1 \cdots y_k$. But the composition is finite, so it can only appear a finite number of times. Therefore, the number of morphisms over g whose decompositions contain this same morphism must be finite. We can thus conclude that there are finitely many morphisms $\eta \in \mathrm{Ca}_1(\Gamma)$ such that $\phi(\eta) \neq 0$, each of which can only appear in the decomposition of finitely many $\xi = \left(\frac{a \to b}{g}\right) \in \mathrm{Mor}(\Gamma)$, meaning that the number of $\xi \in H_g$ such that $T^d(\xi) \neq 0$ is finite. This is to say that T^d is locally finitely supported.

Lastly, for any $\xi \in \mathrm{Ca}_1(\Gamma)$:

$$\varphi\left(T^d\right)(\xi) = T^d(\xi) = \phi(\xi)$$

and so $\varphi\left(T^d\right) = \phi$. Thereby, φ is surjective and consequently bijective. It is also obvious that φ is a vector space homomorphism and so we can conclude that φ is a vector space isomorphism. □

Theorem 15 is analogous to Theorem 13, using traditional derivations rather than Fox-derivations and using a completely different cochain complex. Furthermore, we can also produce the analogous result to Theorem 14:

Theorem 16. *The Lie algebra* $\mathrm{Inn}(\mathbb{C}[G])$ *of inner derivations of* $\mathbb{C}[G]$ *is isomorphic to the 1-dimensional coboundaries* $B^1_f(\mathrm{Ca}(\Gamma))$.

Proof. Here we must recall that $B^1_f(\mathrm{Ca}(\Gamma)) = \mathrm{im}\left(d^0_f\right)$. We will use the same mapping φ, but this time restricting the domain to the characters of Γ corresponding to inner derivations. In order to prove that φ is an isomorphism in this setting, we need only show two things:

1. For every $d_u \in \mathrm{Inn}(\mathbb{C}[G])$, $\varphi\left(T^{d_u}\right) \in B^1_f(\mathrm{Ca}(\Gamma))$.
2. For all $\phi \in B^1_f(\mathrm{Ca}(\Gamma))$ there exists $d_u \in \mathrm{Inn}(\mathbb{C}[G])$ such that $\varphi\left(T^{d_u}\right) = \phi$.

For the first point let $d_u \in \mathrm{Inn}(\mathbb{C}[G])$. We can set $u = \sum_{g\in G} u_g g$. Now we define a mapping $t_u : \mathrm{Ca}_0(\Gamma) \to \mathbb{C}$ by $t_u(g) = u_g$ for each $g \in G$. Since there must be a finite number of non-zero coefficients in the sum defining u, $t_u \in C^0_f(\mathrm{Ca}(\Gamma))$. Moreover:

$$\begin{aligned} d^0_f(t_u)\left(\frac{a\to b}{y}\right) &= t_u(b) - t_u(a) \\ &= u_b - u_a \\ &= T^{d_u}\left(\frac{a\to b}{y}\right) \\ &= \varphi\left(T^{d_u}\right)\left(\frac{a\to b}{y}\right) \end{aligned}$$

for all $\left(\frac{a\to b}{y}\right) \in \mathrm{Ca}_1(\Gamma)$, remembering the nature of T^{d_u} from Theorem 10. Thus, $\varphi\left(T^{d_u}\right) = d^0_f(t_u)$ and hence $\varphi\left(T^{d_u}\right) \in \mathrm{im}\left(d^0_f\right) = B^1_f(\mathrm{Ca}(\Gamma))$.

Now for the second point let $\phi \in B^1_f(\mathrm{Ca}(\Gamma))$. Then there exists $\psi \in C^0_f(\mathrm{Ca}(\Gamma))$ such that $\phi\left(\frac{a\to b}{y}\right) = \psi(b) - \psi(a)$ for all $\left(\frac{a\to b}{y}\right) \in \mathrm{Ca}_1(\Gamma)$. Set $u = \sum_{g\in G} \psi(g) g$. Then $u \in \mathbb{C}[G]$ since ψ is finitely supported. For any $\left(\frac{a\to b}{y}\right) \in \mathrm{Ca}_1(\Gamma)$:

$$\varphi\left(T^{d_u}\right)\left(\frac{a\to b}{y}\right) = T^{d_u}\left(\frac{a\to b}{y}\right) = \psi(b) - \psi(a) = \phi\left(\frac{a\to b}{y}\right)$$

and so $\varphi\left(T^{d_u}\right) = \phi$. □

We have found that $\mathrm{Der}(\mathbb{C}[G]) \cong Z^1_f(\mathrm{Ca}(\Gamma))$ and $\mathrm{Inn}(\mathbb{C}[G]) \cong B^1_f(\mathbb{C}[G])$, which are worthwhile results and lead directly into the central result of [11]:

Corollary 5.

$$\mathrm{Out}(\mathbb{C}[G]) \cong H^1_f(\mathrm{Ca}(\Gamma))$$

since $H^1_f(\mathrm{Ca}(\Gamma)) = Z^1_f(\mathrm{Ca}(\Gamma))/B^1_f(\mathrm{Ca}(\Gamma))$.

These results display a curious similarity between the Fox-derivations and traditional derivations. Both connect in exactly the same ways to a cochain complex, albeit using completely different cochain complexes. This is especially curious considering that the sources from which these ideas are taken do not seem to connect in any other way and have entirely different approaches in all other respects. Furthermore, Fox made no mention whatsoever of inner Fox-derivations and yet we still obtain the desired result involving them.

However, this demonstrates a unity between these very different approaches and points to a broader unity between all approaches to defining derivations: returning to the broadest definition of derivations (Definitions 23 and 24), the introductions of [3] and [11] state that the space of derivations from an algebra A to an A-bimodule E will always satisfy the equation:

$$\mathrm{Out}(A, E) \cong H^1(A, E),$$

a more general version of the results found in both Sections 6.1 and 6.2.

Chapter 7

Conclusion

Having discussed two different formulations of derivations and linked them in Chapter 6, we should briefly discuss why these two formulations were used within their respective contexts. Considering that the formulation used in Chapter 5 is the usual way of defining derivations, that is by Equations (1.1) and (1.2), it is somewhat interesting that Fox defined them differently. Is there a particular reason not to use the usual definition? In attempting to answer this question we must remember that one of the primary goals of [7] was to use Fox-derivations to construct something analogous to traditional differentiation along with results analogous to well-known results around differentiation – such as Taylor series. Is this possible with different notions of derivation?

As it turns out, we can construct partial differentiation on $\mathbb{Z}[X]$ using derivations as defined by Equation (1.1). In fact, this is not only possible for $\mathbb{Z}[X]$ but also for $\mathbb{C}[X]$ and indeed for any $\mathbb{F}[X]$ where $\mathbb{F}$ is a field. The focus can remain on $\mathbb{Z}[X]$, though, since that was chosen for being the free abelian group over X, a choice which does not appear to be related to the type of derivation being used. This construction is almost identical to that in Chapter 3.2.2. We can refer back to that construction exactly with the only changes being that we now define:

$$\frac{\partial x_k^{-1}}{\partial x_j} = -x_k^{-2}\delta_{jk},$$
$$\frac{\partial (uv)}{\partial x_j} = \frac{\partial u}{\partial x_j} \cdot v + u \cdot \frac{\partial v}{\partial x_j}.$$

Despite the existence of partial derivatives here, though, there are several differences that arise. Firstly, it is relevant that $\mathrm{Der}(\mathbb{Z}[X])$ is not a $\mathbb{Z}[X]$-

module while $\mathrm{FDer}(\mathbb{Z}[X])$ is. This is because right-multiplication of derivations by group algebra elements fails to produce further derivations:

$$\begin{aligned}(d \cdot u)(f \cdot g) &= d(f \cdot g) \cdot u = d(f) \cdot g \cdot u + f \cdot d(g) \cdot u \\ &= d(f) \cdot g \cdot u + f \cdot (d \cdot u)(g) \\ &\neq (d \cdot u)(f) \cdot g + f \cdot (d \cdot u)(g)\end{aligned}$$

for $d \in \mathrm{Der}(\mathbb{Z}[X])$ and $u \in \mathbb{Z}[X]$. Similar problems arise for left-multiplication. Therefore, we must view $\mathrm{Der}(\mathbb{Z}[X])$ only as a vector space over $\mathbb{Z}$ and hence the partial derivatives do not form a basis for the space of all derivations. This means that we cannot produce a result analogous to Theorem 4. To prove this claim, consider a derivation d such that $d(x_j) \notin \mathbb{Z}$ for some $x_j \in (x)$. Such derivations definitely exist, for example d_{x_k} where $x_k \neq x_j$. Now assume that d can be written as a linear combination of partial derivatives $\sum_{x_k \in (x)} \alpha_k \frac{\partial}{\partial x_k}$. Then $d(x_j) = \alpha_j \in \mathbb{Z}$, contradicting that $d(x_j) \notin \mathbb{Z}$. Thus, d cannot be written as a linear combination of partial derivatives.

Similarly we cannot produce a result analogous to Theorem 6 as the mapping given in Equation (3.5) is not guaranteed to be a derivation. This theorem was imperative for the fundamental formula, which in turn does not hold:

$$\begin{aligned}\sum_j \frac{\partial x_k^{-1}}{\partial x_j} \cdot (x_j - 1) &= \frac{\partial x_k^{-1}}{\partial x_k} \cdot (x_k - 1) \\ &= -x_k^{-2} \cdot (x_k - 1) \\ &= x_k^{-2} - x_k^{-1} \\ &\neq x_k^{-1} - 1,\end{aligned}$$

demonstrating that the fundamental formula fails for $f = x_k^{-1}$. We can take a similar approach to showing that the Chain Rule from Theorem 5 fails:

$$\frac{\partial\left(\lambda\left(y_i^{-1}\right)\right)}{\partial x_j} = \frac{\partial\left(\lambda(y_i)^{-1}\right)}{\partial x_j} = -\lambda(y_i)^{-1} \cdot \frac{\partial(\lambda(y_i))}{\partial x_j} \cdot \lambda(y_i)^{-1}$$

whereas:

$$\begin{aligned}\sum_{k=1}^{n} \tilde{\lambda}\left(\frac{\partial y_i^{-1}}{\partial y_k}\right) \cdot \frac{\partial(\lambda(y_k))}{\partial x_j} &= \tilde{\lambda}\left(\frac{\partial y_i^{-1}}{\partial y_i}\right) \cdot \frac{\partial(\lambda(y_i))}{\partial x_j} \\ &= \tilde{\lambda}\left(-y_i^{-2}\right) \cdot \frac{\partial(\lambda(y_i))}{\partial x_j}\end{aligned}$$

$$= -\lambda(y_i)^{-2} \cdot \frac{\partial(\lambda(y_i))}{\partial x_j}$$

showing that the Chain Rule fails when $f = y_i^{-1}$.

We cannot obtain any results analogous to Theorems 4, 5 and 6 or Equation (3.6) nor can we for the later results in Chapter 3.2.3 as they largely rely on Equation (3.6). This goes some way to showing why Fox chose his particular type of derivation rather than the more usual formulation that we used here. The main reason that Fox-derivations work where these do not is that Fox introduces a commutative component into derivations: the term $\tilde{o}(v)$ in Equation (2.4) – a defining equation for Fox-derivations – commutes with all elements of $\mathbb{Z}[X]$. This is the factor that causes $\mathrm{FDer}(\mathbb{Z}[X])$ to be a $\mathbb{Z}[X]$-module and consequently leads to Theorems 4 and 6 and hence to Equation (3.6). The presence of this commutative term is also what allows for the Chain Rule. It would appear that Fox managed to introduce just enough commutativity to allow for these results without operating in a completely commutative world.

Bibliography

[1] M. Artin. *Algebra*. Prentice Hall, Boston, 2nd edition, 2010.

[2] A.A. Arutyunov. Derivation algebra in noncommutative group algebras. *Proceedings of the Steklov Institute of Mathematics*, 308(1):22–34, 2020.

[3] A.A. Arutyunov, A.S. Mishchenko, and A.I. Shtern. Derivations of group algebras. *Journal of Mathematical Sciences*, 248:709–718, 2020.

[4] L. Creedon and K. Hughes. Derivations on group algebras with coding theory applications. *Finite Fields and Their Applications*, 56:247–265, 2019.

[5] S. Eilenberg and S. Mac Lane. Cohomology theory in abstract groups. I. *Annals of mathematics*, 48(1):51–78, 1947.

[6] K. Erdmann and M.J. Wildon. *Introduction to Lie algebras*, volume 122. Springer, 2006.

[7] R.H. Fox. Free differential calculus I. Derivation in the free group ring. *Annals of Mathematics*, 57(2):547–560, 1953.

[8] G. Higman. The units of group-rings. *Proceedings of the London Mathematical Society*, 2(1):231–248, 1940.

[9] S. Mac Lane. *Categories for the working mathematician*, volume 5. Springer-Verlag, New York, 1971.

[10] W. Magnus. Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring. *Mathematische Annalen*, 111(1):259–280, 1935.

[11] A.S. Mishchenko. Description of outer derivations of the group algebras. *Topology and its Applications*, 275:107013, 2020.

[12] nLab. cochain complex. `https://ncatlab.org/nlab/show/cochain+complex`, 2021. Accessed: 26 March 2025.

[13] nLab. chain complex. `https://ncatlab.org/nlab/show/chain+complex`, 2023. Accessed: 26 March 2025.

[14] Encyclopedia of Mathematics. Category. `https://encyclopediaofmath.org/index.php?title=Category`, 2023. Accessed: 1 July 2024.

[15] E. Witt. Treue darstellung liescher ringe. In *Collected Papers-Gesammelte Abhandlungen*, pages 195–203. Springer, 1998.

Appendix A

Proof of Prosition 3. Since $\phi(g), \psi(g) \in R[G]$ for any $g \in G$ and G is a basis for $R[G]$, we can define the following expansions for the functions ϕ and ψ: $\phi(g) = \sum_{h \in G} \phi_h^g h$ and $\psi(g) = \sum_{h \in G} \psi_h^g h$, where $(\phi_h^g)_{h \in G}$ and $(\psi_h^g)_{h \in G}$ are sequences in R defined for each $g \in G$. Thus:

$$
\begin{aligned}
&\sum_{g \in G} a_g \cdot \phi(g) + \sum_{g \in G} b_g \cdot \phi(g) \\
&= \sum_{g \in G} a_g \cdot \sum_{h \in G} \phi_h^g h + \sum_{g \in G} b_g \cdot \sum_{h \in G} \phi_h^g h \\
&= \sum_{g \in G} \sum_{h \in G} (a_g \phi_h^g) h + \sum_{g \in G} \sum_{h \in G} (b_g \phi_h^g) h && \text{by Lemma 1} \\
&= \sum_{h \in G} \sum_{g \in G} (a_g \phi_h^g) h + \sum_{h \in G} \sum_{g \in G} (b_g \phi_h^g) h && \text{by commutativity} \\
&= \sum_{h \in G} \left(\sum_{g \in G} a_g \phi_h^g \right) h + \sum_{h \in G} \left(\sum_{g \in G} b_g \phi_h^g \right) h && \text{by distributivity} \\
&= \sum_{h \in G} \left(\sum_{g \in G} a_g \phi_h^g + \sum_{g \in G} b_g \phi_h^g \right) h \\
&= \sum_{h \in G} \left(\sum_{g \in G} (a_g \phi_h^g + b_g \phi_h^g) \right) h \\
&= \sum_{h \in G} \sum_{g \in G} (a_g \phi_h^g + b_g \phi_h^g)\, h && \text{by distributivity} \\
&= \sum_{h \in G} \sum_{g \in G} ((a_g + b_g)\, \phi_h^g) h \\
&= \sum_{h \in G} \sum_{g \in G} (a_g + b_g) \cdot (\phi_h^g h) && \text{by associativity} \\
&= \sum_{g \in G} \sum_{h \in G} (a_g + b_g) \cdot (\phi_h^g h) && \text{by commutativity} \\
&= \sum_{g \in G} (a_g + b_g) \cdot \sum_{h \in G} \phi_h^g h && \text{by distributivity}
\end{aligned}
$$

$$= \sum_{g \in G} (a_g + b_g) \cdot \phi(g).$$

We will now prove the second equation, being less rigorous with the explanations of each step:

$$\begin{aligned}
&\left(\sum_{g \in G} a_g \cdot \phi(g) \right) \cdot \left(\sum_{g \in G} b_g \cdot \psi(g) \right) \\
&= \left(\sum_{g \in G} a_g \cdot \sum_{h \in G} \phi_h^g h \right) \cdot \left(\sum_{g \in G} b_g \cdot \sum_{h \in G} \psi_h^g h \right) \\
&= \left(\sum_{g \in G} \sum_{h \in G} (a_g \phi_h^g) h \right) \cdot \left(\sum_{g \in G} \sum_{h \in G} (b_g \psi_h^g) h \right) \\
&= \left(\sum_{h \in G} \left(\sum_{g \in G} a_g \phi_h^g \right) h \right) \cdot \left(\sum_{h \in G} \left(\sum_{g \in G} b_g \psi_h^g \right) h \right) \\
&= \sum_{h,k \in G} \left(\left(\sum_{g \in G} a_g \phi_h^g \right) \left(\sum_{g \in G} b_g \psi_k^g \right) \right) hk \\
&= \sum_{h,k \in G} \left(\sum_{l \in G} \sum_{g \in G} a_g \phi_h^g b_l \psi_k^l \right) hk \\
&= \sum_{h \in G} \sum_{k \in G} \sum_{l \in G} \sum_{g \in G} (a_g \phi_h^g b_l \psi_k^l) hk \\
&= \sum_{g \in G} \sum_{l \in G} \sum_{h \in G} \sum_{k \in G} (a_g b_l) \cdot ((\phi_h^g \psi_k^l) hk) \\
&= \sum_{g \in G} \sum_{l \in G} (a_g b_l) \cdot \sum_{h \in G} \sum_{k \in G} (\phi_h^g \psi_k^l) hk \\
&= \sum_{g \in G} \sum_{l \in G} (a_g b_l) \cdot \left(\sum_{h \in G} \phi_h^g h \right) \cdot \left(\sum_{k \in G} \psi_k^l k \right) \\
&= \sum_{g,l \in G} (a_g b_l) \cdot (\phi(g) \cdot \psi(l)) \\
&= \sum_{g,h \in G} (a_g b_h) \cdot (\phi(g) \cdot \psi(h)).
\end{aligned}$$

□

Now we move on to proving the results at the end of Section 3.2.3.

Appendix B

Proof of Equation (3.12). We start off by proving Equation (3.12) by applying the Product Rule for n^{th}-order differentiation to x_j^p with $p \in \mathbb{Z}$ and $n > 1$:

$$\begin{aligned}\frac{\partial^n x_j^p}{\partial x_j^n} &= \sum_{i=1}^{n} \frac{\partial^{n-i+1} x_j^{p-1}}{\partial x_j^{n-i+1}} \cdot \tilde{o}\left(\frac{\partial^{i-1} x_j}{\partial x_j^{i-1}}\right) + x_j^{p-1}\frac{\partial^n x_j}{\partial x_j^n} \\ &= \frac{\partial^n x_j^{p-1}}{\partial x_j^n} + \frac{\partial^{n-1} x_j^{p-1}}{\partial x_j^{n-1}}\end{aligned}$$

since $\tilde{o}\left(\frac{\partial^{i-1} x_j}{\partial x_j^{i-1}}\right) = 0$ for all $i > 2$ and $\frac{\partial^n x_j}{\partial x_j^n} = 0$. If $n = 1$, then we obtain the same result since $i = 1$ is the only term i the sum and $x_j^{p-1}\frac{\partial x_j}{\partial x_j} = \frac{\partial^0 x_j^{p-1}}{\partial x_j^0}$. So whenever $n \geq 1$:

$$\frac{\partial^n x_j^p}{\partial x_j^n} = \frac{\partial^n x_j^{p-1}}{\partial x_j^n} + \frac{\partial^{n-1} x_j^{p-1}}{\partial x_j^{n-1}}.$$

Furthermore:

$$\begin{aligned}&\frac{\partial^n x_j^p}{\partial x_j^n} = 1 \qquad \text{if } n = 0 \\ \text{and} \qquad &\frac{\partial^n x_j^p}{\partial x_j^n} = 0 \qquad \text{if } p = 0 \text{ and } n > 0.\end{aligned}$$

From this we can conclude that:

$$\tilde{o}\left(\frac{\partial^n x_j^p}{\partial x_j^n}\right) = \binom{p}{n}.$$

Thus, Equation (3.12) has been derived. □

Appendix C

Proof of Equation (3.13). Equation (3.13), however, requires a more lengthy process. To begin with, we prove another result regarding $\frac{\partial^n x_j^p}{\partial x_j^n}$:

$$\frac{\partial^n x_j^p}{\partial x_j^n} = \sum_{i=0}^{p-n} \binom{p-i-1}{n-1} x_j^i \qquad \text{if } p \geq 0,\ n \geq 1 \qquad \text{(C.1)}$$

$$\text{and} \qquad \frac{\partial^n x_j^p}{\partial x_j^n} = (-1)^n \sum_{i=0}^{-p-1} \binom{n+i-1}{n-1} x_j^{i+p} \qquad \text{if } p < 0,\ n \geq 1. \qquad \text{(C.2)}$$

We prove this by induction on n. Firstly, we consider $p \geq 0$. If $n = 1$, then:

$$\frac{\partial^n x_j^p}{\partial x_j^n} = \frac{\partial x_j^p}{\partial x_j} = \sum_{i=1}^{p} x_j^{i-1} = \sum_{i=0}^{p-1} x_j^i = \sum_{i=0}^{p-1} \binom{p-i-1}{0} x_j^i = \sum_{i=0}^{p-n} \binom{p-i-1}{n-1} x_j^i.$$

Now consider $n \geq 1$ and assume that Equation (C.1) holds for order $1, 2, ..., n$. Then:

$$\begin{aligned}
\frac{\partial^{n+1} x_j^p}{\partial x_j^{n+1}} &= \frac{\partial}{\partial x_j} \left(\sum_{i=0}^{p-n} \binom{p-i-1}{n-1} x_j^i \right) \\
&= \sum_{i=0}^{p-n} \binom{p-i-1}{n-1} \frac{\partial x_j^i}{\partial x_j} \\
&= \sum_{i=0}^{p-n} \binom{p-i-1}{n-1} \sum_{k=0}^{i-1} x_j^k \\
&= \sum_{k=0}^{p-n-1} \binom{p-i-1}{n} x_j^k
\end{aligned}$$

and so Equation (C.1) is true by induction. Now consider the case that $p < 0$. For $n = 1$:

$$\frac{\partial^n x_j^p}{\partial x_j^n} = \frac{\partial x_j^p}{\partial x_j}$$

$$
\begin{aligned}
&= \sum_{i=1}^{-p} x_j^{1-i} \frac{\partial x_j^{-1}}{\partial x_j} \\
&= \sum_{i=1}^{-p} x_j^{1-i} \left(-x_j^{-1}\right) \\
&= -\sum_{i=1}^{-p} x_j^{-i} \\
&= -\sum_{i=0}^{-p-1} x_j^{-i-1} \\
&= -\sum_{i=0}^{-p-1} x_j^{i+p} \\
&= (-1)^1 \sum_{i=0}^{-p-1} \binom{i}{0} x_j^{i+p} \\
&= (-1)^n \sum_{i=0}^{-p-1} \binom{n+i-1}{n-1} x_j^{i+p}.
\end{aligned}
$$

Now we consider $n \geq 1$ and assume that Equation (C.2) holds for order $1, 2, ..., n$. Then:

$$
\begin{aligned}
\frac{\partial^{n+1} x_j^p}{\partial x_j^{n+1}} &= \frac{\partial}{\partial x_j} \left((-1)^n \sum_{i=0}^{-p-1} \binom{n+i-1}{n-1} x_j^{i+p} \right) \\
&= (-1)^n \sum_{i=0}^{-p-1} \binom{n+i-1}{n-1} \frac{\partial x_j^{i+p}}{\partial x_j} \\
&= (-1)^n \sum_{i=0}^{-p-1} \binom{n+i-1}{n-1} \sum_{k=1}^{-i-p} \left(-x_j^{-k}\right) \\
&= (-1)^{n+1} \sum_{i=0}^{-p-1} \binom{n+i-1}{n-1} \sum_{k=0}^{-i-p-1} x_j^{k+i+p} \\
&= (-1)^{n+1} \sum_{k=0}^{-p-1} \binom{n+i}{n} x_j^{i+p}
\end{aligned}
$$

and so Equation (C.2) also holds by induction.

With this result proved, we move on to something seemingly unrelated: consider the homomorphism $\lambda : X \to \langle x_j \rangle$, where $\langle x_j \rangle = \{1, x_j, x_j^2, ...\}$, defined by $\lambda(x_j) = x_j$ and $\lambda(x_k) = 1$ for all $k \neq j$. Applying the Chain Rule of free differentiation, for any $f \in \mathbb{Z}[X]$:

$$
\frac{\partial \left(\tilde{\lambda}(f) \right)}{\partial x_j} = \sum_{k=1}^{m} \tilde{\lambda} \left(\frac{\partial f}{\partial x_k} \right) \cdot \frac{\partial (\lambda(x_k))}{\partial x_j} = \tilde{\lambda} \left(\frac{\partial f}{\partial x_j} \right).
$$

We can write $\frac{\partial f}{\partial x_j}$ as $\sum_{u\in X} a_u u$ so that $\tilde{\lambda}\left(\frac{\partial f}{\partial x_j}\right) = \sum_{u\in X} a_u \lambda(u)$. But because of how we defined λ, $\lambda(u) = x_j^p$ where $p = \sum_{j_k=j} \epsilon_k$. Therefore $\tilde{o}(\lambda(u)) = 1$ for all $u \in X$ and hence $\tilde{o}\left(\tilde{\lambda}\left(\frac{\partial f}{\partial x_j}\right)\right) = \sum_{u\in X} a_u = \tilde{o}\left(\frac{\partial f}{\partial x_j}\right)$. So:

$$\tilde{o}\left(\frac{\partial f}{\partial x_j}\right) = \tilde{o}\left(\frac{\partial\left(\tilde{\lambda}(f)\right)}{\partial x_j}\right).$$

Similarly to the working above, we find $\frac{\partial^2\left(\tilde{\lambda}(f)\right)}{\partial x_j^2} = \frac{\partial}{\partial x_j}\left(\tilde{\lambda}\left(\frac{\partial f}{\partial x_j}\right)\right) = \tilde{\lambda}\left(\frac{\partial^2 f}{\partial x_j^2}\right)$ and consequently $\tilde{o}\left(\frac{\partial^2 f}{\partial x_j^2}\right) = \tilde{o}\left(\frac{\partial^2\left(\tilde{\lambda}(f)\right)}{\partial x_j^2}\right)$. The same principles will apply irrespective of how many times we differentiate with respect to x_j:

$$\tilde{o}\left(\frac{\partial^n f}{\partial x_j^n}\right) = \tilde{o}\left(\frac{\partial^n\left(\tilde{\lambda}(f)\right)}{\partial x_j^n}\right). \tag{C.3}$$

Now, as stated earlier, for any $u \in X$, $\lambda(u) = x_j^p$ where $p = \sum_{j_k=j} \epsilon_k$. Therefore, using Equations (C.1) and (C.2):

$$\tilde{o}\left(\frac{\partial^n(\lambda(u))}{\partial x_j^n}\right) = \sum_{i=0}^{p-n} \binom{p-i-1}{n-1} \qquad \text{if } p \geq 0,$$

$$\tilde{o}\left(\frac{\partial^n(\lambda(u))}{\partial x_j^n}\right) = (-1)^n \sum_{i=0}^{-p-1} \binom{n+i-1}{n-1} \qquad \text{if } p < 0.$$

Either way, $\tilde{o}\left(\frac{\partial^n(\lambda(u))}{\partial x_j^n}\right) = \binom{p}{n}$. So by Equation (C.3), $\tilde{o}\left(\frac{\partial^n u}{\partial x_j^n}\right) = \binom{p}{n}$. But $\tilde{o}\left(\frac{\partial u}{\partial x_j}\right) = \tilde{o}\left(\sum_{j_k=j} \epsilon_k u_{(k)}\right) = \sum_{j_k=j} \epsilon_k = p$. Thus:

$$\tilde{o}\left(\frac{\partial^n u}{\partial x_j^n}\right) = \binom{\tilde{o}\left(\frac{\partial u}{\partial x_j}\right)}{n}. \qquad \square$$

Appendix D

Proof of Equation (3.14). For this equation we consider second-order derivatives of free group elements $u \in X$. First, though, we note that $\tilde{o}\left(\frac{\partial u}{\partial x_j}\right) = p_j$ where $p_j = \sum_{j_i=j} \epsilon_i$ and similarly $\tilde{o}\left(\frac{\partial u}{\partial x_k}\right) = p_k$. Now, if $j \neq k$, then by Equation (3.9):

$$\frac{\partial^2 u}{\partial x_j \partial x_k} = \sum_{j_{\lambda_1}=j, j_{\lambda_2}=k} \epsilon_{j_{\lambda_1}} \epsilon_{j_{\lambda_2}} u_{(j_{\lambda_1})} \qquad \text{where } 1 \leq \lambda_1 < \lambda_2$$

and:

$$\frac{\partial^2 u}{\partial x_k \partial x_j} = \sum_{j_{\lambda_1}=j, j_{\lambda_2}=k} \epsilon_{j_{\lambda_2}} \epsilon_{j_{\lambda_1}} u_{(j_{\lambda_2})} \qquad \text{where } 1 \leq \lambda_2 < \lambda_1.$$

The restrictions on λ_1 and λ_2 are simpler here than in Section 3.2.3 since $j \neq k$ and so we cannot have $\lambda_1 = \lambda_2$, meaning that we need not worry about whether we stop iterating at $\lambda_{1/2}$ or just beforehand. So:

$$\begin{aligned}
\tilde{o}\left(\frac{\partial^2 u}{\partial x_j \partial x_k}\right) &= \sum_{j_{\lambda_1}=j, j_{\lambda_2}=k} \epsilon_{j_{\lambda_1}} \epsilon_{j_{\lambda_2}} \\
&= \sum_{j_{\lambda_2}=k} \left(\sum_{j_{\lambda_1}=j, \lambda_1<\lambda_2} \epsilon_{j_{\lambda_1}} \right) \epsilon_{j_{\lambda_2}} \\
&= \sum_{j_{\lambda_2}=k} p_{j \leq \lambda_2} \epsilon_{j_{\lambda_2}}
\end{aligned}$$

where $p_{j \leq \lambda_2} = \sum_{j_i=j, j_i \leq \lambda_2} \epsilon_i$. Similarly:

$$\tilde{o}\left(\frac{\partial^2 u}{\partial x_k \partial x_j}\right) = \sum_{j_{\lambda_1}=j} p_{k \leq \lambda_1} \epsilon_{j_{\lambda_1}}.$$

Therefore:

$$\tilde{o}\left(\frac{\partial^2 u}{\partial x_j \partial x_k}\right) + \tilde{o}\left(\frac{\partial^2 u}{\partial x_k \partial x_j}\right) = p_j p_k = \tilde{o}\left(\frac{\partial u}{\partial x_j}\right)\tilde{o}\left(\frac{\partial u}{\partial x_k}\right). \qquad \square$$