The Fox Calculus and Differentiation in Group Rings

Simon Byeonguk Han

Abstract

In this MTH 501 project, we present results from the article *"Free Differential Calculus I: Derivation in the Free Group Ring"* by Ralph H. Fox [1]. This work introduces a group ring generalization of the classical differential calculus of functions of one or more real variables. Specifically, the calculus of differentiation is generalized to the case where the objects being differentiated are elements of an abstract group ring $\mathbb{Z}G$ over an arbitrary multiplicative group G with respect to the ring $\mathbb{Z}$ of integers. In this more general setting, a number of familiar and basic properties regarding differentiation are established, and the results highlight many similarities with the classical case. Specific results are applied to the case of a free group ring.

A Math 501 Project

Under the direction of
Dr. John Caughman

Second Reader
Dr. Derek Garton

Submitted in partial fulfillment of the requirements for the degree of

Master of Science in Mathematics

Portland State University
Winter and Spring Quarter, 2022

Contents

1 Introduction

In this MTH 501 project, we present results from the article *"Free Differential Calculus I: Derivation in the Free Group Ring"* by Ralph H. Fox [1]. This work introduces a group ring generalization of the classical differential calculus of functions of one or more real variables.

1.1 History and Context

In 1952, Ralph H. Fox was inspired by his research in topological classifications, and specifically by his work with the Alexander polynomial, to formulate a more general theory of differentiation that would be applicable to more general algebraic objects than real-valued functions.

Specifically, in the paper under consideration [1], Fox presented his theory of free differential calculus (now called the *Fox Calculus* in his honor), in which the theory of differentiation is generalized to the case where the objects being differentiated are elements of an abstract group ring $\mathbb{Z}G$ over an arbitrary multiplicative group G with respect to the ring $\mathbb{Z}$ of integers. In this more general setting, a number of familiar and basic properties regarding differentiation are established, and the results highlight many similarities with the classical case. Specific results are applied to the case of a free group ring.

Our aim in this project is to present the results found in the original article of Fox. Specifically, we aim to fill in the many details and calculations of the paper that are left to the reader. Furthermore, we hope to increase the readability by offering a number of running examples to illustrate the results and proof methods wherever possible.

1.2 Organization of Topics

The content of this project is organized as follows. Chapter 1 contains a brief introduction to the topic of group rings, in order to offer a bit of historical and mathematical context for this work. Chapter 2 presents the basic properties of group rings, with an emphasis on homomorphisms and derivations. In Chapter 3, we focus in on the specific case of derivations in a free group ring. Finally, in Chapter 4 we conclude with a number of observations and possible directions for further research.

2 Basic Properties of Group Rings

In this section, we present a number of basic results regarding group rings $\mathbb{Z}G$ for a multiplicative group G with respect to the ring $\mathbb{Z}$ of integers. Many of the concepts will be familiar to students of an introductory course in abstract algebra, but if more context is desired, we refer the interested reader to the classic textbook by Pinter [4]. Other references for algebraic topics that may be a bit more advanced include the textbooks by Fraleigh [2] and Hungerford [3].

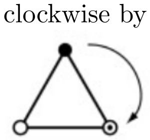
Our first results simply consider the various relationships that exist between the group homomorphisms defined on G and the ring homomorphisms defined on the group ring $\mathbb{Z}G$. After that, we will briefly explore the relationships between normal subgroups of G and two-sided ideals of $\mathbb{Z}G$. At that point, we will discuss a particularly important homomorphism for the group ring known as a retraction. Finally, we will introduce the main topic for consideration in this project, the concept of a derivation in a group ring. Each of these topics will be illustrated with examples.

2.1 Running Example $\mathbb{D}_6$

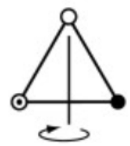
Recall that the dihedral group $\mathbb{D}_6$ denotes the group of all 6 symmetries of an equilateral triangle. This group $\mathbb{D}_6$ belongs to the well-known family of dihedral groups, where D_{2n} denotes the symmetry group of a regular n-sided polygon.

The group $\mathbb{D}_6$ has generators R and F, where R denotes a 120° clockwise rotation and F denotes a reflection through a vertical axis. We can illustrate these group elements visually as symmetries of a triangle as follows.

- The generator R rotates the triangle clockwise by 120°:



- The generator F reflects the triangle across a vertical axis



The full operation table (the Cayley table for composition) for the group $\mathbb{D}_6$ can be easily computed by hand, and the result is given as follows:

$\circ$	I	R	R^2	F	FR	FR^2
I	I	R	R^2	F	FR	FR^2
R	R	R^2	I	FR^2	F	FR
R^2	R^2	I	R	FR	FR^2	F
F	F	FR	FR^2	I	R	R^2
FR	FR	FR^2	F	R^2	I	R
FR^2	FR^2	F	FR	R	R^2	I

Using this example, we will illustrate many of the concepts and results that follow. We begin in the next section with a consideration of homomorphisms.

2.2 Homomorphisms of Groups and Rings

Let G be any multiplicative group. Recall that we can form the associated group ring $\mathbb{Z}G$ with respect to the ring $\mathbb{Z}$ of integers. Each element of $r \in \mathbb{Z}G$ is expressible as a sum

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

where every coefficient a_g is an integer, and these coefficients are zero for all but finitely many $g \in G$. Addition and multiplication in $\mathbb{Z}G$ are defined by

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g \tag{1}$$

and

$$\left(\sum_{g\in G} a_g g\right)\cdot\left(\sum_{h\in G} b_h h\right) = \sum_{g,h\in G}(a_g b_h)gh. \tag{2}$$

Each element $a \in \mathbb{Z}$ is identified with the element $a \cdot 1_g \in \mathbb{Z}G$ and each element $g \in G$ is identified with the element $1 \cdot g \in \mathbb{Z}G$. So, in this way, both $\mathbb{Z}$ and G can easily be regarded as subsets of the group ring $\mathbb{Z}G$.

Example 1 (*The group ring $\mathbb{Z}G$ for the dihedral group $G = \mathbb{D}_6$.*) Three examples of the elements of the group ring $\mathbb{Z}\mathbb{D}_6$ are given below:

$$2R + R^2 - 3F,$$

$$3R + 2F - 5FR^2 + 3I, \text{ and}$$

$$-R^2 - F + 2FR + 5FR^2.$$

As an example of addition in the group ring $\mathbb{Z}G$, we have:

$$(2R + R^2 - 3F) + (3R + 2F - 5FR^2 + 3I) = 5R + R^2 - F - 5FR^2 + 3I.$$

As an example of multiplication in the group ring $\mathbb{Z}G$, we have:

$$\begin{aligned}(2R + R^2 - 3F)\cdot(3R + 2F - 5FR^2 + 3I) &= 6R^2 + 4RF - 10RFR^2 + 6R + 3R^3 + 2R^2F - \\ &\quad 5R^2FR^2 + 3R^2 - 9FR - 6F^2 + 15F^2R^2 - 9F \\ &= 6R^2 + 4FR^2 - 10FR + 6R + 3I + 2FR - \\ &\quad 5F + 3R^2 - 9FR - 6I + 15R^2 - 9F \\ &= 24R^2 + 4FR^2 - 17FR + 6R - 3I - 14F.\end{aligned}$$

Notice how, in the calculation above, we simply expanded the product using the distributive property, and we simplified the terms using the Cayley table for the group. Finally, we collected like-terms to simplify the result. □

Now we consider the concept of homomorphisms. Recall these are functions defined on a group or a ring that respect the appropriate operations [4].

Let ψ be a homomorphism from a group G into a group H. We denote by $\psi' : ZG \to ZH$ the **linear extension** of the group homomorphism ψ to elements of the group ring. In other words, ψ' is defined so that

$$\left(\sum_{g \in G} a_g g\right)^{\psi'} = \sum_{g \in G} a_g g^{\psi}. \tag{3}$$

Note that ψ' leaves fixed each element of $\mathbb{Z}$.

Example 2 (*Linear Extensions*) Referring to Example 1, we now consider an example of a homomorphism from $\psi : \mathbb{D}_6 \to \mathbb{Z}_2$. Let $\psi(R) = [0]_2$ and $\psi(F) = [1]_2$. These two values actually determine a unique homomorphism from $\mathbb{D}_6$ to $\mathbb{Z}_2$. Moreover, this homomorphism extends linearly to a unique homomorphism ψ' defined on the group ring $\mathbb{Z}\mathbb{D}_6$. Indeed, to illustrate (3), note that $\psi(FR^2) = [1]_2 + [0]_2 + [0]_2 = [1]_2$. So

$$\begin{aligned}
(3R + 2F - 5FR^2 + 3I)^{\psi'} &= (3R)^{\psi'} + (2F)^{\psi'} - (5FR^2)^{\psi'} + (3I)^{\psi'} \\
&= 3(R)^{\psi} + 2(F)^{\psi} - 5(FR^2)^{\psi} + 3(I)^{\psi} \\
&= 3 \cdot [0]_2 + 2 \cdot [1]_2 - 5 \cdot [1]_2 + 3 \cdot [0]_2 \\
&= 6 \cdot [0]_2 - 3 \cdot [1]_2
\end{aligned}$$

□

In the next lemma, we justify such computations by verifying that this rule of linear extension, given in (3), always gives a ring homomorphism.

Lemma 1 *Let ψ be any homomorphism ψ of a group G into a group H. Then, by linear extension as defined in (3), the map ψ induces a ring-homomorphism ψ' of the group ring $\mathbb{Z}G$ into the group ring $\mathbb{Z}H$.*

Proof Let ψ denote any homomorphism of a group G into a group H.

By (3), we begin with addition and argue as follows.

$$\begin{aligned}
\left(\sum_{g\in G} a_g g + \sum_{g\in G} b_g g\right)^{\psi'} &= \left(\sum_{g\in G}(a_g+b_g)g\right)^{\psi'} \\
&= \sum_{g\in G}(a_g+b_g)g^{\psi} \\
&= \sum_{g\in G}(a_g g^{\psi} + b_g g^{\psi}) \\
&= \sum_{g\in G} a_g g^{\psi} + \sum_{g\in G} b_g g^{\psi} \\
&= \left(\sum_{g\in G} a_g g\right)^{\psi'} + \left(\sum_{g\in G} b_g g\right)^{\psi'}.
\end{aligned}$$

In the above deduction, we see that the map ψ' as defined does indeed respect addition in the group rings. Next we consider multiplication.

$$\begin{aligned}
\left(\sum_{g\in G} a_g g \cdot \sum_{h\in G} b_h h\right)^{\psi'} &= \left(\sum_{g,h\in G}(a_g b_h)gh\right)^{\psi'} \\
&= \sum_{g,h\in G}(a_g b_h)(gh)^{\psi} \\
&= \sum_{g,h\in G}(a_g b_h)g^{\psi}h^{\psi} \\
&= \sum_{g\in G} a_g g^{\psi} \cdot \sum_{h\in G} b_h h^{\psi} \\
&= \left(\sum_{g\in G} a_g g\right)^{\psi'} \cdot \left(\sum_{h\in G} b_h h\right)^{\psi'}.
\end{aligned}$$

As the above deduction shows, the map ψ' as defined does indeed respect multiplication in the group rings. The result follows. □

Remark 1 Each normal subgroup N of a group G can be associated with a both-sided ideal $\Re_N$ in the group ring $\mathbb{Z}G$. Specifically, we let $\Re_N$ be the kernel of the ring homomorphism associated with the natural (group) homomorphism $G \to G/N$. □

In the next section, we will further explore this use of homomorphism kernels.

2.3 Normal Subgroups and Ideals

The kernel of a group homomorphism $\psi : G \to H$ is, by definition, the normal subgroup N consisting of those elements of G that are mapped by ψ to the identity element 1 of H. The kernel of a ring homomorphism ψ' is the both-sided ideal $\Re$ consisting of those elements of $\mathbb{Z}G$ that are mapped by ψ' to the zero element 0 of $\mathbb{Z}H$. Recall that we have associated a ring homomorphism ϕ' with each group homomorphism ϕ. In this way, a both-sided ideal $\Re$ is made to correspond to each normal subgroup N.

Conversely, Lemma 2 below will show that each both-sided ideal $\Re$ in $\mathbb{Z}G$ determines a normal subgroup of G. Specifically, we can associate with $\Re$ the subgroup consisting of those elements of G that are mapped to 1 by the ring homomorphism $\mathbb{Z}G \to \mathbb{Z}G/\Re$.

Subsequently, in Lemma 3, we will see that the ideal $\Re$ that corresponds to a given normal subgroup N does, in turn, determine N. And in fact, $\Re$ is the smallest ideal of $\mathbb{Z}G$ that determines N.

Lemma 2 *Each both-sided ideal $\Re$ in a group ring $\mathbb{Z}G$ determines a normal subgroup N of the group G such that*

$$N = \{g_i \in G \,|\, \phi(1 \cdot g_i) = 1_{\mathbb{Z}G/\Re}\}$$

where ϕ denotes the natural homomorphism $\mathbb{Z}G \to \mathbb{Z}G/\Re$.

Proof Since the identity of G maps to $1_{\mathbb{Z}G/\Re}$, we know that N is non-empty. It remains to check closure, inverses, and normality.

First we consider closure. Let $g_k, g_l \in N$. Then, $\phi(1 \cdot g_k) = \phi(1 \cdot g_l) = 1_{\mathbb{Z}G/\Re}$. So it follows that

$$
\begin{aligned}
\phi(1 \cdot (g_k \cdot g_l)) &= \phi((1 \cdot g_k) \cdot (1 \cdot g_l)) \\
&= \phi(1 \cdot g_k) \cdot \phi(1 \cdot g_l) \\
&= 1_{\mathbb{Z}G/\Re} \cdot 1_{\mathbb{Z}G/\Re} \\
&= 1_{\mathbb{Z}G/\Re}.
\end{aligned}
$$

Therefore, we can conclude that $g_k \cdot g_l \in N$, and closure holds.

Next we consider inverses. Let $g_k \in N$, so that $\phi(1 \cdot g_k) = 1_{\mathbb{Z}G/\Re}$. Then

$$
\begin{aligned}
1_{\mathbb{Z}G/\Re} &= \phi(1 \cdot 1_g) \\
&= \phi(1 \cdot (g_k \cdot {g_k}^{-1})) \\
&= \phi((1 \cdot g_k) \cdot (1 \cdot {g_k}^{-1})) \\
&= 1_{\mathbb{Z}G/\Re} \cdot \phi(1 \cdot {g_k}^{-1}).
\end{aligned}
$$

It follows that $\phi(1 \cdot {g_k}^{-1}) = 1_{\mathbb{Z}G/\Re}$. Therefore, $g_k^{-1} \in N$, and N has inverses.

Finally we consider normality. Let $g_i \in N$, so that $\phi(1 \cdot g_i) = 1_{\mathbb{Z}G/\Re}$. Then for any $g \in G$, we have

$$
\begin{aligned}
\phi(1 \cdot (g \cdot g_i \cdot g^{-1})) &= \phi(1 \cdot g) \cdot \phi(1 \cdot g_i) \cdot \phi(1 \cdot g^{-1}) \\
&= \phi(1 \cdot g) \cdot 1_{\mathbb{Z}G/\Re} \cdot \phi(1 \cdot g^{-1}) \\
&= \phi(1 \cdot g) \cdot \phi(1 \cdot g^{-1}) \\
&= \phi(1 \cdot (g \cdot g^{-1})) \\
&= \phi(1 \cdot 1_g) \\
&= 1_{\mathbb{Z}G/\Re}.
\end{aligned}
$$

Therefore, $g \cdot N \cdot g^{-1} \subset N$ and N is a normal subgroup of G. □

To illustrate the result above, we return to our example.

Example 3 (*Normal Subgroup from Ideal*) Recall the ring homomorphism $\phi' : \mathbb{Z}\mathbb{D}_6 \to \mathbb{Z}\mathbb{Z}_2$ from Example 2. Then for any integers a, b, c, d, e, f we have

$$(aI + bR + cR^2 + dF + eFR + fFR^2)^{\phi'} = (a + b + c)[0]_2 + (d + e + f)[1]_2.$$

The 0 element in $\mathbb{Z}\mathbb{Z}_2$ is $0 \cdot [0]_2 + 0 \cdot [1]_2$, so the kernel of ϕ' is the both-sided ideal

$$\Re = \{aI + bR + cR^2 + dF + eFR + fFR^2 \mid a + b + c = 0, d + e + f = 0\}.$$

We now consider congruence mod $\Re$. For example, the element below,

$$2I - 3R + 4R^2 - F + 3FR - 2FR^2,$$

which is an element in the group ring $\mathbb{Z}\mathbb{D}_6$, corresponds with any of the expressions below

$$3I + \Re, \quad 3R + \Re, \quad \text{or} \quad 3R^2 + \Re$$

in the quotient ring $\mathbb{Z}\mathbb{D}_6/\Re$. Similarly, since $1_{\mathbb{Z}\mathbb{D}_6/\Re} = I + \Re$, it follows that the multiplicative element of the quotient ring can be represented by any expression of the form

$$aI + bR + cR^2 + dF + eFR + fFR^2 + \Re$$

where

$$a + b + c = 1 \quad \text{and} \quad d + e + f = 0.$$

This implies that $\{I, R, R^2\}$ are the elements of $\mathbb{D}_6$ that are mapped into $1_{\mathbb{Z}\mathbb{D}_6/\Re}$ by the ring homomorphism $\mathbb{Z}\mathbb{D}_6 \to \mathbb{Z}\mathbb{D}_6/\Re$. Therefore, the ideal $\Re$ corresponds to the normal subgroup $\{I, R, R^2\}$ of $\mathbb{D}_6$. □

The subgroup N and the ideal $\Re_n$ are closely related, as we now show.

Lemma 3 *Suppose $\Re_N$ is the ideal associated with a normal subgroup N of a group G (as described in Remark 1). Then $\Re_N$ is the smallest ideal of $\mathbb{Z}G$ that determines N.*

Proof First we observe that if N' and N are any normal subgroups of G with $N' \subseteq N$, then the associated ideals $\Re'$ and $\Re$ also satisfy $\Re' \subseteq \Re$.

So now, let $\Re = \Re_N$ be the ideal associated with N and suppose an ideal $\Re' \subseteq \Re$ determines $N' = N$. Then $N \subseteq N'$, so $\Re \subseteq \Re'$, and therefore $\Re = \Re'$. □

In our next lemma, we consider a relationship between a set of generators of a normal subgroup N of a group G and a set of generators of the associated ideal $\Re_N$ in the group ring $\mathbb{Z}G$.

Lemma 4 *Suppose a normal subgroup N of a group G is generated by the elements of a set $S = \{n_j \,|\, j \in \mathcal{J}\}$. Then the set $\hat{S} = \{n_j - 1 \,|\, j \in \mathcal{J}\}$ generates the associated ideal $\Re_N$ in the group ring $\mathbb{Z}G$.*

Proof Suppose that $N \trianglelefteq G$, and let S be a set of generators as stated above. Let ϕ denote the natural homomorphism, mapping each element $g \in G$ to the coset gN in the quotient group G/N. Recall that the associated ring homomorphism ϕ' maps each element $\sum a_g g \in \mathbb{Z}G$ to the element $\sum a_g g^\phi \in \mathbb{Z}(G/N)$.

Fix any $\sum a_g g \in \Re_N$. Recall that $\Re_N = \ker \phi'$, so $\sum a_g g^\phi = 0$. Notice that, for any $h \in G/N$, we have $\sum' a_g = 0$, where the summation $\sum'$ extends over g such that $g^\phi = h$. Fix any $h \in G/N$ and any $g_0 \in G$ such that $g_0^\phi = h$. Note that if $g^\phi = h$, then $gg_0^{-1} \in N$. Furthermore,

$$\begin{aligned} {\sum}' a_g g &= {\sum}' a_g (gg_0^{-1} - 1) g_0 + {\sum}' a_g g_0 \\ &= {\sum}' a_g (gg_0^{-1} - 1) g_0. \end{aligned}$$

It follows that $\sum' a_g g$ (and thus also $\sum a_g g$) is a linear combination of elements of the form $n - 1$, where $n \in N$. To see that each element of the form $n - 1$, where $n \in N$, is a linear combination of elements of the form $n_j - 1 \in \hat{S}$, we observe the identities below:

$$\begin{aligned} n^{-1} - 1 &= -n^{-1}(n-1) \\ nn' - 1 &= (n-1) + n(n'-1) \\ gng^{-1} - 1 &= g(n-1)g^{-1}, \end{aligned}$$

and the result follows. □

In the next section, we consider a particular homomorphism used in group rings.

2.4 Retractions in Group Rings

We begin with a definition.

Definition 1 (Retraction in a group ring $\mathbb{Z}G$) *Let G denote any (multiplicative) group. The* **retraction $^\circ$ of $\mathbb{Z}G$ upon $\mathbb{Z}$** *is the ring homomorphism induced by the trivial group homomorphism $^o : G \to \{1\}$. In other words:*

$$(\sum a_g g)^\circ = \sum a_g g^\circ = \sum a_g,$$

so that every element $\sum a_g g$ of $\mathbb{Z}G$ is mapped by $^\circ$ into its coefficient sum. □

The kernel of the ring-homomorphism $^\circ$ consists of all elements of coefficient sum zero. This kernel will be called the **fundamental ideal** of $\mathbb{Z}G$.

Example 4 (*Example of retraction*) Let us return to our group $G = \mathbb{D}_6$. Let $^\circ$ denote the retraction of $\mathbb{Z}G$ upon $\mathbb{Z}$. Then

$$\begin{aligned} (3R + 2F - FR + 4FR^2)^\circ &= 3R^\circ + 2F^\circ - (FR)^\circ + 4(FR^2)^\circ \\ &= 3 + 2 - 1 + 4 \\ &= 8. \end{aligned}$$

As this example suggests, it is a trivial matter to verify that $^\circ$ is a ring homomorphism. □

2.5 Derivations in Group Rings

In this section we introduce the central concept of this project, a derivation in a group ring.

Definition 2 (Derivations in a group ring $\mathbb{Z}G$) *A* **derivation** *in a group ring $\mathbb{Z}G$ is any mapping $D : \mathbb{Z}G \to \mathbb{Z}G$ that satisfies the following:*

$$D(u+v) = Du + Dv \tag{4}$$

$$D(u \cdot v) = Du \cdot v^\circ + u \cdot Dv, \tag{5}$$

for all $u, v \in \mathbb{Z}G$, where $^\circ$ denotes the retraction of $\mathbb{Z}G$ upon $\mathbb{Z}$. □

Example 5 (*Examples of derivations*) Each of the five maps defined below is an example of a derivation on $\mathbb{Z}\mathbb{D}_6$:

$$\begin{aligned}
D_1(R) &= I - R^2 + FR - FR^2, & D_1(F) &= 0 \\
D_2(R) &= R - R^2 - F + FR, & D_2(F) &= 0 \\
D_3(R) &= -F + FR^2, & D_3(F) &= I - F \\
D_4(R) &= F - FR, & D_4(F) &= R - FR \\
D_5(R) &= FR - FR^2, & D_5(F) &= R^2 - FR^2.
\end{aligned}$$

Indeed, using (4) and (5) above, it is not difficult to show that any derivation of $\mathbb{Z}\mathbb{D}_6$ must be a linear combination of these. □

We will use the derivation D_3 from above to illustrate several results, so it will be convenient to determine its action on all six elements of $\mathbb{D}_6$.

Example 6 (*Complete action of derivation D_3 on $\mathbb{D}_6$*) Using equations (4) and (5) from above, we find that:

$$\begin{aligned}
D_3(I) &= 0, \\
D_3(R) &= -F + FR^2, \\
D_3(R^2) &= D_3(R) + RD_3(R) \\
&= F + FR^2 + R \cdot (-F + FR^2) \\
&= -F + FR, \\
D_3(F) &= I - F, \\
D_3(FR) &= D_3(F) + FD_3(R) \\
&= I - F + F \cdot (-F + FR^2) \\
&= -F + R^2, \\
D_3(FR^2) &= D_3(F) + FD_3(R^2) \\
&= I - F + F \cdot (-F + FR) \\
&= -F + R.
\end{aligned}$$

The action on any element of the group ring is now easily found by linearity. □

We now list a number of consequences of our definition of derivation.

Lemma 5 *The following properties of any derivation D on a group ring $\mathbb{Z}G$ are implied by equations (4) and (5):*

$$D(gh) = Dg + gDh \qquad (g, h \in G), \tag{6}$$

$$Da = 0 \qquad (a \in \mathbb{Z}), \tag{7}$$

$$D(g^{-1}) = -g^{-1}Dg \qquad (g \in G). \tag{8}$$

Proof To see (6), we begin by observing that $h^\circ = 1$. Now we argue that

$$D(gh) = Dg \cdot h^\circ + gDh = Dg + gDh.$$

Next we consider (7). Note that $a \in \mathbb{Z}$ is identified with the element $a \cdot 1_g \in \mathbb{Z}G$. Then $D(1) = 0$, since

$$\begin{aligned} D(1) &= D(1 \cdot 1) \\ &= D(1 \cdot 1_g) \cdot (1 \cdot 1_g)^\circ + (1 \cdot 1_g) \cdot D(1 \cdot 1_g) \\ &= D(1 \cdot 1_g) + D(1 \cdot 1_g) \\ &= D(1) + D(1). \end{aligned}$$

It now follows, by a simple induction, that $Da = 0$.

Finally, we consider (8). By the result above,

$$\begin{aligned} 0 &= D(1) \\ &= D(g^{-1} \cdot g) \\ &= D(g^{-1}) + g^{-1} Dg. \end{aligned}$$

It now follows that $D(g^{-1}) = -g^{-1} Dg$. □

Next we return to our running example of $\mathbb{Z}\mathbb{D}_6$ and we use it to illustrate the rule for applying a derivation to the inverse of a group element.

Example 7 (*Applying rule (8) with D_3 in $\mathbb{Z}\mathbb{D}_6$.*) When we apply (8) to some elements of $\mathbb{D}_6$, we see that

$$\begin{aligned} D_3(R^{-1}) &= -R^{-1} D_3(R) \\ &= -R^2(-F + FR^2) \\ &= R^2 F - R^2 F R^2 \\ &= FR - F \\ &= D_3(R^2). \end{aligned}$$

This agrees with our earlier result in Example 6. Similarly,

$$\begin{aligned} D_3(F^{-1}) &= -F^{-1}D_3(F) \\ &= -F(I-F) \\ &= -F+I \\ &= D_3(F). \end{aligned}$$

Again, the above calculation confirms our earlier results in Example 6. □

In our next lemma, we extend the derivation rules to arbitrary sums and products.

Lemma 6 *Let D be any derivation of a group ring $\mathbb{Z}G$. Then for any $\sum a_g g \in \mathbb{Z}G$, we have*

$$D\left(\sum a_g g\right) = \sum a_g Dg. \tag{9}$$

Furthermore, for any $u_1, u_2, \ldots, u_l \in \mathbb{Z}G$, we have

$$D(u_1 \cdot u_2 \cdots u_l) = \sum_{i=1}^{l} u_1 \cdots u_{i-1} \cdot Du_i \cdot u_{i+1}^{\circ} \cdots u_l^{\circ}. \tag{10}$$

Proof To see (9), we simply note that, by (4), we have

$$D(\sum a_g g) = \sum D(a_g g) = \sum a_g Dg,$$

as desired. To prove (10), we proceed by induction on l. Note that

$$D(u_1 \cdot u_2) = Du_1 \cdot u_2^{\circ} + u_1 \cdot Du_2,$$

so the base case holds. Now assume that

$$D(u_1 \cdot u_2 \cdots u_{l-1}) = \sum_{i=1}^{l-1} u_1 \cdots u_{i-1} \cdot Du_i \cdot u_{i+1}^{\circ} \cdots u_{l-1}^{\circ}.$$

Then we argue that

$$\begin{aligned} D(u_1 \cdot u_2 \cdots u_l) &= D(u_1 \cdot u_2 \cdots u_{l-1}) \cdot u_l + (u_1 \cdot u_2 \cdots u_{l-1}) \cdot Du_l \\ &= (\sum_{i=1}^{l-1} u_1 \cdots u_{i-1} \cdot Du_i \cdot u_{i+1}^\circ \cdots u_{l-1}^\circ) \cdot u_l + (u_1 \cdot u_2 \cdots u_{l-1}) \cdot Du_l \\ &= \sum_{i=1}^{l} u_1 \cdots u_{i-1} \cdot Du_i \cdot u_{i+1}^\circ \cdots u_l^\circ . \end{aligned}$$

The result follows. □

Based on the results described above, the set of derivations in a group ring $\mathbb{Z}G$ form a right $\mathbb{Z}G$-module, where addition is defined by

$$(D_1 + D_2)u = D_1 u + D_2 u$$

and where right-multiplication by an element v of $\mathbb{Z}G$ is defined by

$$(D \cdot v)(u) = Du \cdot v.$$

In the next section, we apply these results to the special case of a free group ring.

3 Derivations in a free group ring

We begin with some terminology.

3.1 Definitions for Free Group Rings

To define a **free group** X, we begin by fixing a given set of **generators** $S = \{x_j \mid j \in \mathcal{J}\}$. Note that the set S of generators need not be enumerable. An **element** of X is an equivalence class u of words from S, represented by a unique **reduced word**, which is an expression of the form $\prod_{k=1}^{l} x_{j_k}^{\epsilon_k}$ such that $\epsilon_k = \pm 1$ and $\epsilon_k + \epsilon_{k+1} \neq 0$ if $j_k = j_{k+1}$. The **length** of u means the length of the representative reduced word. The **identity** element 1 is represented by the empty word and is said to be of length 0. The **inverse** u^{-1} of u is represented by the reduced word $\prod_{k=1}^{l} x_{j_{l+1-k}}^{-\epsilon_{l+1-k}}$.

An element of the **free group ring** $\mathbb{Z}X$, defined over the free group X, is called a **free polynomial** $f(x)$ and has the form

$$f(x) = \sum a_u u, \qquad (u \in X, a_u \in \mathbb{Z})$$

where almost all a_u are equal to zero. For any group G, a homomorphism $\phi : X \to G$ that maps $(x_1, x_2, \cdots)$ into $(x_1^\phi, x_2^\phi, \cdots)$ gives rise to an induced ring homomorphism $\phi' : \mathbb{Z}X \to \mathbb{Z}G$ that maps a free polynomial $f(x) = \sum a_u u$ into

$$f(x)^{\phi'} = f(x^\phi) = \sum a_u u^\phi.$$

The associated retraction homomorphism $^\circ : \mathbb{Z}X \to \mathbb{Z}$ maps a free polynomial $f(x)$ to the corresponding coefficient sum. In other words, $f(x)^\circ = \sum a_u = f(1)$. Recall that the fundamental ideal of $\mathbb{Z}X$ consists of those polynomials $f(x)$ for which $f(1) = 0$.

3.2 Derivatives with Respect to Generators

The next theorem shows that any derivation can be realized as a linear combination of the spanning set – namely, the derivatives with respect to the generators.

Theorem 1 *Assume $\{x_j \mid j \in \mathcal{J}\}$ is the set of generators for a free group X. To each generator x_j, there corresponds a derivation $f(x) \to \partial f(x)/\partial x_j$, called the* **derivative with respect to** *x_j, which has the property*

$$\frac{\partial x_k}{\partial x_j} = \delta_{j,k}. \tag{11}$$

Furthermore, for any given elements $h_1(x), h_2(x), \cdots$ of $\mathbb{Z}X$, there is exactly one derivation $f(x) \to f'(x)$ that respectively maps the generators $x_1, x_2, \cdots$ into these elements

$h_1(x), h_2(x), \cdots$ *of* $\mathbb{Z}X$. *It is given by the formula*

$$f'(x) = \sum \frac{\partial f(x)}{\partial x_j} \cdot h_j(x) \tag{12}$$

Proof. For each index j and element u of X, define $\langle j, u\rangle = 1$ if x_j is an initial segment of the reduced word representing u, and $\langle j, u\rangle = 0$ otherwise. Extend this definition linearly to $\mathbb{Z}X$ such that

$$\langle j, f(x)\rangle = \langle j, \sum a_u u\rangle = \sum a_u \langle j, u\rangle.$$

For each index j, each element w of X, and each free polynomial $f(x)$, define

$$\langle j, w, f(x)\rangle = \langle j, w^{-1} f(x)\rangle - \langle j, w^{-1}\rangle f(1).$$

Then for any $u \in X$, we have

$$\langle j, w, u\rangle = \langle j, w^{-1}u\rangle - \langle j, w^{-1}\rangle = 0$$

if w is not an initial segment of u, since x_j is an initial segment of $w^{-1}u$ if and only if x_j is an initial segment of w^{-1}. It follows that, for given j and $f(x)$, the integer

$$\langle j, w, f(x)\rangle = \langle j, w, \sum a_u u\rangle = \sum a_u \langle j, w, u\rangle = 0$$

for all but a finite number of elements w of X. The derivative of $f(x)$ with respect to x_j is now defined to be the finite sum

$$\frac{\partial f(x)}{\partial x_j} = \sum_{w \in X} \langle j, w, f(x)\rangle w.$$

By linearity, it is clear that (4) is satisfied, and it is sufficient to prove the special case (6) of (5). Let $u, v \in X$. Then

$$\begin{aligned}\frac{\partial(uv)}{\partial x_j} &= \sum_w (\langle j, w^{-1}uv\rangle - \langle j, w^{-1}\rangle)w \\ &= \sum_w (\langle j, w^{-1}u\rangle - \langle j, w^{-1}\rangle)w + \sum_w (\langle j, w^{-1}uv\rangle - \langle j, w^{-1}u\rangle)w \\ &= \sum_w (\langle j, w^{-1}u\rangle - \langle j, w^{-1}\rangle)w + u\sum_t (\langle j, t^{-1}v\rangle - \langle j, t^{-1}\rangle)t \\ &= \frac{\partial u}{\partial x_j} + u\frac{\partial v}{\partial x_j}.\end{aligned}$$

To prove (11), note that the only initial segments of x_k are 1 and x_k, thus

$$\begin{aligned}\frac{\partial x_k}{\partial x_j} &= \langle j, 1, x_k\rangle + \langle j, x_k, x_k\rangle x_k \\ &= (\langle j, x_k\rangle - \langle j, 1\rangle) + (\langle j, 1\rangle - \langle j, x_k^{-1}\rangle)x_k \\ &= (\delta_{jk} - 0) + (0 - 0)x_k.\end{aligned}$$

To prove (12), note that $\partial f(x)/\partial x_j$ vanishes for all but a finite number of indices j. Thus, the sum

$$\sum_j \frac{\partial f(x)}{\partial x_j} \cdot h_j(x)$$

is a finite sum. Since the derivations in $\mathbb{Z}X$ form a right $\mathbb{Z}X$-module, a map that sends $f(x)$ to $\sum(\partial f(x)/\partial x_j) \cdot h_j(x)$ is a derivation and, by construction, it sends x_j to $h_j(x)$ for each index j. Conversely, if $f(x) \to f'(x)$ is any derivation that respectively maps $x_1, x_2, \cdots$ into $h_1(x), h_2(x), \cdots$, then

$$f(x) \to f'(x) - \sum_j (\partial f(x)/\partial x_j) \cdot h_j(x)$$

is a derivation mapping each x_j into 0. It therefore also maps each x_j^{-1} into $-x_j^{-1} \cdot 0$, which is 0. From (4) and (5) we conclude that every element of $\mathbb{Z}X$ is mapped into 0. Thus, $f'(x) = \sum_j (\partial f(x)/\partial x_j) \cdot h_j(x)$, as desired. □

In the next lemma, we highlight a derivation that possesses a particularly simple form.

Lemma 7 *Assume $\{x_j \mid j \in \mathcal{J}\}$ is the set of generators for a free group X. The function D, that maps $f(x) \mapsto f(x) - f(1)$, is a derivation on the free group ring $\mathbb{Z}X$ that respectively maps x_j into $x_j - 1$ for each $j \in \mathcal{J}$.*

Proof. Let us show that the given map D satisfies (4) and (5). First, for any free polynomials $f(x)$ and $g(x)$, we have

$$\begin{aligned} D(f(x) + g(x)) &= f(x) + g(x) - f(1) - g(1) \\ &= f(x) - f(1) + g(x) - g(1) \\ &= D(f(x)) + D(g(x)), \end{aligned}$$

so (4) clearly holds. And similarly,

$$\begin{aligned} D(f(x) \cdot g(x)) &= f(x)g(x) - f(1)g(1) \\ &= f(x) \cdot g(1) - f(1) \cdot g(1) + f(x) \cdot g(x) - f(x) \cdot g(1) \\ &= (f(x) - f(1)) \cdot g(1) + f(x) \cdot (g(x) - g(1)) \\ &= D(f(x)) \cdot g(1) + f(x) \cdot D(g(x)). \end{aligned}$$

So the condition (5) holds, as desired. □

To illustrate the spanning property of the set of derivations given in Example 5, we consider the case of the derivation given in Lemma 7.

Example 8 (*The derivation D for the case of $\mathbb{Z}\mathbb{D}_6$.*) The derivation D given in Lemma 7, when applied to case of the group ring $\mathbb{Z}\mathbb{D}_6$, satisfies

$$D(R) = R - I, \quad \text{and} \quad D(F) = F - I.$$

As a result, the derivation D can be represented as $-D_1 + D_2 - D_3$, a linear combination of the derivations in Example 5. To see why, note that $(-D_1 + D_2 - D_3)(R)$ evaluates to

$$-(I - R^2 + FR - FR^2) + (R - R^2 - F + FR) - (-F + FR^2),$$

which simplifies to $R - I$. And $(-D_1 + D_2 - D_3)(F) = -0 + 0 - (I - F) = F - I$. $\square$

3.3 Calculating Derivatives with the Fundamental Formula

Using the result (12) from the previous section, we obtain a useful fact, known as the **fundamental formula**:

$$f(x) = f(1) + \sum_j \frac{\partial f(x)}{\partial x_j} \cdot (x_j - 1). \tag{13}$$

This formula shows that any element $f(x)$ of $\mathbb{Z}X$ can be explicitly recovered from $f(1)$ and from its derivatives $\partial f(x)/\partial x_j$ for $j \in \mathcal{J}$. In particular, any element u of the free group X can be explicitly recovered from its derivatives $\partial u/\partial x_j$ for $j \in \mathcal{J}$.

Example 9 (*The derivation D for the case of $\mathbb{Z}\mathbb{D}_6$.*) Let X be a free group generated by $\{x_1, x_2, x_3\}$ and consider the free polynomial $f(x) \in \mathbb{Z}X$ given by

$$f(x) = 3x_2^{-1}x_1x_2 + 5x_3x_2x_1^{-1}.$$

If we let $\hat{D}_1$ denote $\partial/\partial x_1$, then

$$\begin{aligned}
\partial f(x)/\partial x_1 &= 3(\hat{D}_1 x_2^{-1} + x_2^{-1}\hat{D}_1(x_1x_2)) + 5(\hat{D}_1 x_3 + x_3 D\hat{D}_1(x_2x_1^{-1})) \\
&= 3(0 + x_2^{-1}\hat{D}_1(x_1x_2)) + 5(0 + x_3\hat{D}_1(x_2x_1^{-1})) \\
&= 3x_2^{-1}(\hat{D}_1x_1 + x_1\hat{D}_1x_2) + 5x_3(\hat{D}_1x_2 + x_2\hat{D}_1x_1^{-1}) \\
&= 3x_2^{-1} + 5x_3x_2(-x_1^{-1}) \\
&= 3x_2^{-1} - 5x_3x_2x_1^{-1}.
\end{aligned}$$

Likewise, if we let $\hat{D}_2$ denote $\partial/\partial x_2$, then

$$\begin{aligned}\partial f(x)/\partial x_2 &= 3(\hat{D}_2 x_2^{-1} + x_2^{-1}\hat{D}_2(x_1x_2)) + 5(\hat{D}_2 x_3 + x_3\hat{D}_2(x_2x_1^{-1})) \\ &= 3(-x_2^{-1}\hat{D}_2 x_2 + x_2^{-1}\hat{D}_2(x_1x_2)) + 5(0 + x_3\hat{D}_2(x_2x_1^{-1})) \\ &= 3x_2^{-1}(-1 + \hat{D}_2 x_1 + x_1\hat{D}_2 x_2) + 5x_3(\hat{D}_2 x_2 + x_2\hat{D}_2 x_1^{-1}) \\ &= -3x_2^{-1} + 3x_2^{-1}x_1 + 5x_3.\end{aligned}$$

Finally, if we let $\hat{D}_3$ denote $\partial/\partial x_3$, then

$$\begin{aligned}\partial f(x)/\partial x_3 &= 3(\hat{D}_3 x_2^{-1} + x_2^{-1}\hat{D}_3(x_1x_2)) + 5(\hat{D}_3 x_3 + x_3\hat{D}_3(x_2x_1^{-1})) \\ &= 3(0) + 5(1+0) = 5.\end{aligned}$$

It now follows from (13) that

$$f(x) = (3x_2^{-1} - 5x_3x_2x_1^{-1})(x_1 - 1) + (-3x_2^{-1} + 3x_2^{-1}x_1 + 5x_3)(x_2 - 1) + 5(x_3 - 1),$$

which indeed is easily verified, as desired. □

Another use for the fundamental formula (13) is that it allows us to easily calculate the derivatives of a power of generator.

$$\partial x_j^p/\partial x_j = (x_j^p - 1)/(x_j - 1) = \begin{cases} 1 + x_j + \cdots + x_j^{p-1} & \text{if } p \geq 1 \\ 0 & \text{if } p = 0 \\ -x_j^p - x_j^{p+1} - \cdots - x_j^{-1} & \text{if } p \leq -1. \end{cases} \tag{14}$$

This formula (14) and (10) combine to give us another practical rule. Write any $u \in X$ in the form $u = u_0 x_j^{p_1} u_1 x_j^{p_2} \cdots u_{q-1} x_j^{p_q} u_q$ where $p_1, \cdots, p_q$ are non-zero integers and where the reduced words represented by $u_0, u_1, \cdots, u_q$ do not involve the generator x_j. Then we get

$$\frac{\partial u}{\partial x_j} = \sum_{j=1}^{q} u_0 x_j^{p_1} u_1 x_j^{p_2} \cdots u_{i-1} \frac{x_j^{p_i} - 1}{x_j - 1}. \tag{15}$$

We conclude by considering an example to illustrate the use of this rule.

Example 10 (*Derivation using the fundamental formula*) For any integers $m, n > 0$ we find that:

$$\begin{aligned} \frac{\partial}{\partial x_1}(x_1^m x_2^n x_1^{-m} x_2^{-n}) &= (1 + x_1 + \cdots + x_1^{m-1}) + x_1^m x_2^n(-x_1^{-m} - x_1^{-m+1} - \cdots - x_1^{-1}) \\ &= (1 - x_1^m x_2^n x_1^{-m})(1 + x_1 + \cdots + x_1^{m-1}). \end{aligned}$$

In a similar manner, we can compute the derivative with respect to x_2:

$$\begin{aligned} \frac{\partial}{\partial x_2}(x_1^m x_2^n x_1^{-m} x_2^{-n}) &= x_1^m(1 + x_2 \cdots + x_2^{n-1}) + x_1^m x_2^n x_1^{-m}(-x_2^{-n} - x_2^{-n+1} \cdots - x_2^{-1}) \\ &= (x_1^m - x_1^m x_2^n x_1^{-m} x_2^{-n})(1 + x_2 + \cdots + x_2^{n-1}). \end{aligned}$$

Generally, using this approach is the easiest way to compute derivatives by hand.

4 Conclusion

In this paper, we demonstrated a group ring generalization of the classical differential calculus of functions of one or more real variables.

Of particular interest to me was the interplay between homomorphisms and derivatives. In the classical differential calculus of functions of one or more real variables, derivative is defined at a point of its domain and not explicitly viewed as structural relation between the function and its derivative function. However, in the Fox calculus, derivative is defined as a homomorphism, a structure preserving mapping.

Further results beyond the scope of this project include chain rule of differentiation, derivatives in a free group ring of higher order, and how derivatives in a free group ring shows structures of the free group ring.

Another interesting thing to pursue further might be to explore the associated theory of anti-derivatives. How can we define the anti-derivation in a group ring or free group ring? What are the computational properties of anti-derivation? Can we also have various anti-derivation methods similar to the various methods of anti-derivation in the classical integral calculus of functions of real variables?

For more information on these topics and more, the motivated reader may be interested in exploring the resources listed in the references below.

References

[1] R. H. Fox. Free Differential Calculus. I: Derivation in the Free Group Ring. *Annals of Mathematics*, Second Series, Vol. 57, No. 3 (May, 1953), pp. 547-560

[2] J. B. Fraleigh. *A First Course in Abstract Algebra*, Addison-Wesley. Boston, 2003.

[3] T. Hungerford. *Abstract Algebra: An Introduction*, 3rd edition. (Graduate Texts in Mathematics 73). Springer Verlag, 1997.

[4] C. C. Pinter. *A Book of Abstract Algebra*, Dover Publications. Mineola, N.Y, 2013.