2018

GROUP RINGS

Christopher Wrenn
John Carroll University, cwrenn16@jcu.edu

GROUP RINGS

An Essay Submitted to the
Office of Graduate Studies
College of Arts & Sciences of
John Carroll University
in Partial Fulfillment of the Requirements
for the Degree of
Master of Sciences

By
Christopher J. Wrenn
2018

The essay of Christopher J. Wrenn is hereby accepted:

____ ________________

Advisor – Barbara K. D'Ambrosia Date

I certify that this is the original document:

____ ________________

Author – Christopher J. Wrenn Date

Introduction

Group rings are a special class of rings. They are built by combining two of the most important structures in Algebra: groups and commutative rings. Interestingly, the resultant group rings are not necessarily commutative. So group rings provide an additional example of noncommutative rings outside of the usual example of matrix rings. Further, we'll see that group rings can be viewed as modules over the component ring, with an additional way to multiply elements of the module. In particular, if the ring is a field, its group rings can be viewed as vector spaces over the field, with the additional multiplicative operation. This paper will provide an overview of group rings, explore conditions under which group rings have zero divisors, and discuss ways to view group rings in terms of simple components.

Section 1. Basic Definitions and Properties

We begin our exploration of group rings by looking at some useful facts about group rings. These properties will not only provide some support for some of the later theorems, but also show that group rings are different enough from generic rings to make them worth studying. Throughout this paper we assume that all rings are commutative with $1 \neq 0$. We begin with the definition of *group ring*.

Definition 1.1. Let R be a ring, and let $G = \{g_1, \ldots, g_n\}$ be a finite group whose operation is written multiplicatively. Then the *group ring* of G with coefficients in R is the set of all formal sums:

$$RG = \{a_1 g_1 + a_2 g_2 + \cdots + a_n g_n : a_i \in R \text{ for } 1 \leq i \leq n\},$$

with operations as defined below. This definition is extended to group rings of infinite groups by only considering finite sums (i.e., sums in which only finitely many coefficients are nonzero). The ordering of terms in the sum is irrelevant. So two elements of a group ring are considered equal if and only if the coefficients of each group element are equal. That is, if $a_1g_1 + a_2g_2 + \cdots + a_ng_n$ and $b_1g_1 + b_2g_2 + \cdots + b_ng_n$ are elements of RG, then $a_1g_1 + a_2g_2 + \cdots + a_ng_n = b_1g_1 + b_2g_2 + \cdots + b_ng_n$ if and only if $a_i = b_i$ for each i between 1 and n. Based on the context, we will usually write elements of RG as $\sum a_ig_i$, representing the element $\sum_{i=1}^{n} a_ig_i$. Similarly, we may write an element as $\sum_{x\in G} a_x x$, and again without the index as $\sum a_x x$.

Addition is defined componentwise:

$$\begin{aligned}&\left(a_1g_1 + a_2g_2 + \cdots + a_ng_n\right) + \left(b_1g_1 + b_2g_2 + \cdots + b_ng_n\right)\\ &\qquad = \left(a_1 + b_1\right)g_1 + \left(a_2 + b_2\right)g_2 + \cdots + \left(a_n + b_n\right)g_n.\end{aligned}$$

That is, $\left(\sum a_ig_i\right) + \left(\sum b_ig_i\right) = \sum\left(a_i + b_i\right)g_i$.

Multiplication is defined by

$$\left(a_1g_1 + a_2g_2 + \cdots + a_ng_n\right)\left(b_1g_1 + b_2g_2 + \cdots + b_ng_n\right) = c_1g_1 + c_2g_2 + \cdots + c_ng_n,$$

where c_k, the coefficient of g_k, is $\sum_{g_ig_j = g_k} a_ib_j$. That is,

$$\left(\sum a_ig_i\right)\left(\sum b_jg_j\right) = \sum_{k=1}^{n}\left(\sum_{g_ig_j = g_k} a_ib_j\right)g_k .$$

Since elements of RG are finite sums, this characterization of multiplication is valid even in the case that G is an infinite group.

Proposition 1.1. With the operations defined above, RG is a ring with unity.

Proof: First, we show that $(RG,+)$ is an abelian group. It is easy to check that $\sum 0g$ is the additive identity. It is also clear that for an element $\sum a_g g$, the additive inverse is $\sum(-a_g)g$. The remaining group properties for RG are inherited from the ring R. As an example, we check the associativity of addition in RG. Let $\sum_{g\in G} a_g g$, $\sum_{g\in G} b_g g$, and $\sum_{g\in G} c_g g$ be elements of RG. Then, since addition is associative in R,

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

and hence addition is associative in RG.

The associativity of multiplication likewise follows from the corresponding properties in the ring R and the group G.

Note that for any *i* and *k*, there is a unique *j* with $g_i g_j = g_k$. By the definition of addition in RG, and because addition is commutative and associative in RG, for any $\sum a_i g_i$ and $\sum b_j g_j$ in RG,

$$\left(\sum a_i g_i\right)\left(\sum b_j g_j\right) = \sum_{k=1}^{n}\left(\sum_{g_i g_j = g_k} a_i b_j\right) g_k = \sum_{(i,j)} \left(a_i b_j\right) g_i g_j .$$

Notice that for a particular pair (i, j), the definition of multiplication in RG implies that $\left(a_i b_j\right)\left(g_i g_j\right) = \left(a_i g_i\right)\left(b_j g_j\right)$. Therefore,

$$\left(\sum a_i g_i\right)\left(\sum b_j g_j\right) = \sum_{(i,j)} \left(a_i b_j\right) g_i g_j = \sum_{(i,j)} \left(a_i g_i\right)\left(b_j g_j\right).$$

It is now straightforward to check the distributive properties in RG.

The unity element of RG is $1_R 1_G$ since for every $\sum a_x x \in RG$ we have

$$1_R 1_G \left(\sum a_x x\right) = \sum \left(1_R a_x\right)\left(1_G x\right) = \sum a_x x = \sum \left(a_x 1_R\right)\left(x 1_G\right) = \left(\sum a_x x\right) 1_R 1_G . \ \blacksquare$$

Example. If $G = D_8 = \left\langle s, r \mid s^2 = r^4 = 1, rs = sr^3 \right\rangle$ is the dihedral group of order 8, and $R = \mathbb{Z}$, then $\alpha = 3r - 2sr^2$ and $\beta = 2s + sr^2$ are elements of $\mathbb{Z}D_8$. Then

$$\begin{aligned} \alpha + \beta &= 3r + \left(-2 + 1\right) sr^2 + 2s \\ &= 3r - sr^2 + 2s \end{aligned}$$

and

$$\begin{aligned}\alpha\beta &= \left(3r-2sr^2\right)\left(2s+sr^2\right)\\ &= 6rs+3rsr^2-4sr^2s-2sr^2sr^2\\ &= 6sr^3+3sr-4r^2-2\cdot 1_G.\end{aligned}$$

In the case where *F* is a field, an alternate characterization of the group ring FG is as an *F*-vector space with basis *G* and the additional multiplicative operation defined above. As we have already seen, FG is an additive abelian group. The remaining parts of the definition of vector space are straightforward to verify.

There are a few quick facts worth pointing out regarding group rings. Note that we can identify the ring *R* with the subring $\{r1_G : r \in R\}$ of RG using the injective ring homomorphism $\varphi : R \to RG$ by $\varphi(r) = r1_G$. Also, we can identify the group *G* with the subgroup $\{1g : g \in G\}$ of $(RG)^\times$, the multiplicative group of invertible elements in RG, using the injective group homomorphism $\psi : G \to (RG)^\times$ by $\psi(g) = 1_R g$.

In addition to the group *G* and the ring *R* both residing within the group ring RG, group rings also inherit some other properties from the group and the ring.

Proposition 1.2. Let *G* be a group and *R* be a ring. Then RG is a commutative ring if and only if *G* is abelian.

Proof: First suppose that RG is a commutative ring. Then *G* is abelian as a corollary to the fact that $G \le (RG)^\times$.

Now, suppose that *G* is abelian, and let $\sum_{g\in G} a_g g, \sum_{h\in G} b_h h \in RG$. Then, since *R* is a commutative ring,

$$
\begin{aligned}
\left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h h\right) &= \sum_{(g,h)} \left(a_g b_h\right)(gh) \\
&= \sum_{(g,h)} \left(b_h a_g\right)(hg) \\
&= \left(\sum_{h\in G} b_h h\right)\left(\sum_{g\in G} a_g g\right)
\end{aligned}
$$

and hence RG is a commutative ring. ■

The next proposition is straightforward to check, but shows that subrings of the ring *R* and subgroups of the group *G* translate into subrings of the group ring RG as one would expect.

Proposition 1.3. Let *G* be a group and let *R* be a ring.

(i) If *S* is a subring of *R*, then SG is a subring of RG; and

(ii) If $H \leq G$, then RH is a subring of RG.

Note that if 1_G is the identity in *G*, then for every $a \in R$ we write $a1_G$ as a. If 1_R is the identity in *R*, we write $1_R g$ as *g* for every $g \in G$. In particular, we simply write $1_R 1_G$ as 1.

The following propositions show that group rings of finite groups truly differ from arbitrary rings in the general sense. In particular, most group rings have nontrivial centers and, in the case that the ring is a field, group rings have maximal ideals.

Proposition 1.4. Let *G* be a group with a nontrivial finite normal subgroup *H*, and let *R* be a ring. Then RG has a nontrivial center; specifically, $\eta = \sum_{h\in H} h$ is in the center of the group ring RG. In particular, if *G* is finite, then *G* is a nontrivial finite normal subgroup of itself, and hence RG has nontrivial center.

Proof: Since $H \lhd G$, $gH = Hg$ for every $g \in G$. Since η is the sum of all of the elements of *H*, for every $g \in G$, $g\eta$ is the sum of all of the elements of gH. Similarly, ηg is the sum of all of the elements of Hg. Since $gH = Hg$, it follows that $g\eta = \eta g$. That is, η commutes with every element of *G*. Now let $\sum a_g g \in RG$. Then

$$\begin{aligned}\left(\sum a_g g\right)(\eta) &= \sum\left(a_g g\eta\right)\\ &= \sum\left(a_g \eta g\right)\\ &= (\eta)\left(\sum a_g g\right).\end{aligned}$$

Thus, $\eta = \sum_{h\in H} h$ is in the center of RG. ■

Definition 1.2. Let *R* be a ring and let $G = \{g_1, \ldots, g_n\}$ be a finite group. Then the map $f : RG \to R$ by $f\left(\sum a_i g_i\right) = \sum a_i$ is called the *augmentation map*. Proposition 1.5 shows that this map is a homomorphism. Its kernel is called the *augmentation ideal* of RG.

Proposition 1.5. Let *R* be a ring and let $G = \{g_1, \ldots, g_n\}$ be a finite group. Then the augmentation map is a homomorphism. Also, the augmentation ideal is generated by $\{g - 1 : g \in G\}$. Further, if *R* is a field then the augmentation ideal is maximal.

Proof: Let $f : RG \to R$ be the augmentation map. Let $x = \sum a_i g_i$ and $y = \sum b_j g_j$ be elements of RG. Then

$$f(x+y) = f\left(\sum (a_i + b_i) g_i\right) = \sum (a_i + b_i) = \sum a_i + \sum b_i = f(x) + f(y).$$

Also, using the fact that *f* preserves sums,

$$f(xy) = f\left(\sum_{(i,j)}(a_i b_i) g_i g_j\right) = \sum_{(i,j)} a_i b_j = \left(\sum a_i\right)\left(\sum b_j\right) = f(x) f(y).$$

The augmentation ideal is $I = \left\{\sum a_i g_i \in RG : \sum a_i = 0\right\}$. Let $I_0 = \langle g - 1 : g \in G \rangle$. Suppose that $x \in I$. If $x = \sum a_i g_i$, then $x = x - \sum a_i = \sum a_i (g_i - 1)$. So $x \in I_0$. On the other hand, note that for every $g \in G$, $f(g-1) = f(1_R g - 1_R 1_G) = 1_R - 1_R = 0$. So $g - 1 \in I$ for every $g \in G$. Thus, $I = I_0$, and the augmentation ideal is generated by $\{g - 1 : g \in G\}$.

The augmentation map is clearly onto, so $RG/I \cong R$. So if *R* is a field, then the quotient RG/I is a field, and thus *I* must be maximal [2, p. 224]. ■

Section 2. Zero Divisors

We've already seen conditions under which a group ring is commutative. Taking our investigation a step further, we can try to decide whether a group ring has zero divisors, which will help in classifying group rings in the hierarchy of ring structures. For example, in the case that the group ring is commutative and has no zero divisors, the group ring is an integral domain.

Recall that a group element is called a *torsion element* when its order is finite.

Proposition 2.1. Let *G* be any group containing a torsion element *g*, and let *R* be a ring. Then the group ring RG has zero divisors. So in particular, if *G* is a finite group, then the group ring RG has zero divisors.

Proof. Set $m = \mathrm{ord}(g)$. Then $1-g$ and $1+g+\cdots+g^{m-1}$ are nonzero elements of RG, and $(1-g)(1+g+\cdots+g^{m-1}) = 1-g^m = 1-1=0$. ■

Whether a group ring *RG* must have zero divisors when *G* is infinite and torsion-free is an open problem. The current conjecture is that *G* is torsion-free if and only if RG has no zero divisors. When *R* is a field, we know the conjecture to be true in the case of abelian groups, free groups, and supersolvable groups [4, p. 174]. Proposition 2.2 shows the conjecture is true in the special case where *G* is an abelian group and *R* is a field.

Proposition 2.2. Let *G* be an abelian group and let *F* be a field. Then *G* is torsion-free if and only if FG has no zero divisors.

Proof. The backwards direction follows from Proposition 2.1.

For the forwards direction, suppose that *G* is torsion-free and let $\alpha, \beta \in FG$ be such that $\alpha\beta = 0$. Since there are only finitely many group elements with nonzero coefficients in each of the group ring elements, there is a finitely generated subgroup *H* of *G* such that FH contains α and β. By the Fundamental Theorem of Finitely Generated Abelian Groups, *H* is the direct product of cyclic groups $\langle x_1\rangle, \ldots, \langle x_m\rangle$. Since *G* is torsion-free, each $\langle x_i\rangle$ is infinite. Then FH is contained in $F(x_1, \ldots, x_m)$, the quotient field of the polynomial ring $F[x_1, \ldots, x_m]$. Since $F(x_1, \ldots, x_m)$ is a field, FH is an integral domain. Hence, $\alpha = 0$ or $\beta = 0$, so FG has no zero divisors. ■

There is a related result that sheds some additional light on the zero divisor problem, but first we need a definition.

Definition 2.1. A ring *R* is said to be *prime* if for all $\alpha, \beta \in R$, $\alpha R \beta = 0$ implies that $\alpha = 0$ or $\beta = 0$.

Theorem 2.3. Let F be a field and let G be a group. Then G has a nontrivial finite normal subgroup if and only if FG is not a prime ring.

Proof (part 1). The forward direction is fairly simple, while the reverse direction will require some work.

First, suppose that $H = \{h_1, \ldots, h_n\}$ is a nontrivial finite normal subgroup of G. Let $\alpha = h_1 + \cdots + h_n$. Since multiplication by elements of H is a bijection from H to H, it follows that $h\alpha = \alpha$ for every $h \in H$. So

$$\alpha^2 = (h_1 + \cdots + h_n)\alpha = h_1\alpha + \cdots + h_n\alpha = n\alpha .$$

Now let $\beta = n1 - \alpha$. Then $\alpha\beta = \alpha(n1) - \alpha^2 = n\alpha - n\alpha = 0$.

By Proposition 1.4, we know that α is a central element of FG. Thus for any $u \in FG$, we have $\alpha u \beta = u\alpha\beta = u0 = 0$, and hence $\alpha(FG)\beta = 0$. Since α and β are clearly nonzero, FG is not a prime ring. This concludes the proof of the forwards direction of Theorem 2.3. ■

The reverse direction of the proof will require a bit more work. We start with some definitions and necessary lemmas.

Definition 2.2. Let G be a group. We define

$$\Delta(G) = \{x \in G : x \text{ has only finitely many conjugates in } G\}$$

and

$$\Delta^+(G) = \{x \in G : x \in \Delta(G) \text{ and } x \text{ has finite order}\}.$$

So $\Delta^+(G)$ is the set of torsion elements in $\Delta(G)$. Hence, $\Delta^+(G) \subseteq \Delta(G)$. When there is no ambiguity of the group G, we will abbreviate the notation of these two subsets as simply Δ and Δ^+.

It is well known that the number of conjugates of a group element x is equal to the index of the centralizer of x in the group, $[G:C_G(x)]$. Hence, an alternate characterization of the subgroup Δ is the set of all $x \in G$ such that $[G:C_G(x)] < \infty$.

Recall that the *commutator subgroup* of a group H is $H' = \langle x^{-1}y^{-1}xy : x, y \in H \rangle$. The commutator subgroup is normal in H, and the quotient H/H' is abelian [2, p. 90].

Lemma 2.4. Let G be a group. Then

(i) Δ and Δ^+ are normal subgroups of G;

(ii) Δ/Δ^+ is torsion-free abelian; and

(iii) Δ^+ is nontrivial if and only if G has a nontrivial finite normal subgroup.

Proof. For the proof of (i), it is clear that $1 \in \Delta$. Let $x \in \Delta$ and $g \in G$. Then $gx^{-1}g^{-1} = (gxg^{-1})^{-1}$, and is hence an inverse of one of the finitely many conjugates of x. Thus, there are only finitely many conjugates of x^{-1}, so $x^{-1} \in \Delta$.

Let $y \in \Delta$. Then $gxyg^{-1} = gxg^{-1}gyg^{-1}$, a product of a conjugate of x with a conjugate of y. Since there are only finitely many such conjugates, $xy \in \Delta$ and hence $\Delta \leq G$.

Lastly, gxg^{-1} is one of the finitely many conjugates of x, and so has only finitely many conjugates itself. Hence, $gxg^{-1} \in \Delta$, and Δ is a normal subgroup of G.

Suppose further that *x* and *y* have finite order, so $x, y \in \Delta^+$. We've already shown that x^{-1}, xy, and any conjugate of *x* are elements of Δ. So to complete the proof that Δ^+ is a normal subgroup of *G*, we need only to show that these elements have finite order. Since $\operatorname{ord}(x) = \operatorname{ord}(x^{-1})$, $x^{-1} \in \Delta^+$. Also, since $\operatorname{ord}(gxg^{-1}) = \operatorname{ord}(x)$, $gxg^{-1} \in \Delta^+$.

It remains to show that xy has finite order. Consider $H = \langle x, y \rangle$. Since *H* is a finitely generated subgroup of Δ, we see that the set H_0 of torsion elements of *H* is a finite subgroup of *H* [5, p. 116]. But since H_0 contains the generators of *H*, we have $H_0 = H$, and so xy is a torsion element. Thus we can conclude that Δ^+ is a normal subgroup of *G*, and hence of Δ.

For (ii), since Δ^+ is a normal subgroup of Δ, and Δ^+ consists of those elements of Δ of finite order, Δ/Δ^+ is torsion-free. To show that Δ/Δ^+ is abelian, let $x, y \in \Delta$. Then $\langle x, y \rangle$ is a finitely generated subgroup of Δ, and so $\langle x, y \rangle'$ is finite [5, p. 116]. So $x^{-1}y^{-1}xy = (yx)^{-1}(xy)$ has finite order. That is, $(yx)^{-1}(xy) \in \Delta^+$, which implies that $(xy)\Delta^+ = (yx)\Delta^+$, so that Δ/Δ^+ is abelian.

For (iii), we'll start with the forward direction by supposing that $\Delta^+ \neq \langle 1 \rangle$. So let $\delta \in \Delta^+$ be nontrivial. Consider $D = \langle \delta, \delta_2, \ldots, \delta_n \rangle$, where $\delta, \delta_2, \ldots, \delta_n$ are the finitely many *G*-conjugates of δ. As above, since *D* is a finitely generated subgroup of Δ, we know that $|D'|$ is finite. Also, D/D' is finitely generated by elements of finite order. Since D/D' is abelian, it follows that $|D/D'|$ must be finite. Since $|D| = |D/D'||D'|$, we see that $|D|$ is also finite. So *D* is nontrivial and finite, and it remains to show that *D* is closed under conjugation.

Let $x \in G$ and $d \in D$. For some $m \in \mathbb{N}$, $\alpha_1, \ldots, \alpha_m \in \mathbb{Z}$, and $d_1, \ldots, d_m \in \{\delta, \delta_2, \ldots, \delta_n\}$,

$$\begin{aligned} xdx^{-1} &= xd_1^{\alpha_1} d_2^{\alpha_2} \cdots d_m^{\alpha_m} x^{-1} \\ &= xd_1^{\alpha_1} x^{-1} xd_2^{\alpha_2} x^{-1} \cdots xd_m^{\alpha_m} x^{-1} \\ &= \left(xd_1x^{-1}\right)^{\alpha_1} \left(xd_2x^{-1}\right)^{\alpha_2} \cdots \left(xd_mx^{-1}\right)^{\alpha_m}. \end{aligned}$$

Since each d_i is a conjugate of δ, then each xd_ix^{-1} is a conjugate of δ and thus is one of the generators of *D*. Hence, the entire product is in *D*, so $xdx^{-1} \in D$ and thus $D \triangleleft G$. So *G* has a nontrivial finite normal subgroup.

For the reverse direction of (iii), suppose that $\Delta^+ = \langle 1 \rangle$. Let *H* be a finite normal subgroup of *G* and let $h \in H$. Then for every $x \in G$, $xhx^{-1} \in H$, and since *H* is finite, *h* has only finitely many *G*-conjugates. Also, since *H* is finite, $\mathrm{ord}(h)$ is finite. Hence $h \in \Delta^+$, so $h = 1$ and thus *H* is trivial. ■

Lemma 2.5. Let *G* be a group and let $H_1, \ldots, H_n$ be a finite collection of subgroups of *G*.

(i) If $[G : H_i] < \infty$ for all *i*, then $[G : \cap H_i] < \infty$.

(ii) If *G* is the union of finitely many right cosets of the subgroups H_i, then $[G : H_i] < \infty$ for some *i*.

The proof of this lemma is not difficult, and the details can be found in [5, p. 115, 120].

For an element $\alpha \in FG$, we define the *support of* α, denoted $\mathrm{Supp}\,\alpha$, as the set of all group elements whose coefficients are nonzero in the expression $\alpha = \sum a_x x$. By definition of FG, there can only be finitely many such group elements, and hence $\mathrm{Supp}\,\alpha$ is a finite subset of *G*. Also, note that this subset is empty if and only if $\alpha = 0$.

We now proceed with the remainder of the proof of Theorem 2.3.

Proof of Theorem 2.3 (part 2). Suppose that FG is not a prime ring, and let $\alpha, \beta \in FG$ be nonzero such that $\alpha(FG)\beta = 0$. We begin by separating α and β into Δ components and $G-\Delta$ components. That is, $\alpha = \alpha_0 + \alpha_1$ and $\beta = \beta_0 + \beta_1$, where $\operatorname{Supp}\alpha_0$ and $\operatorname{Supp}\beta_0$ are subsets of Δ and $\operatorname{Supp}\alpha_1$ and $\operatorname{Supp}\beta_1$ are subsets of $G-\Delta$. Let $x \in \operatorname{Supp}\alpha$ and $y \in \operatorname{Supp}\beta$. Note that $(x^{-1}\alpha)(FG)(\beta y^{-1}) = 0$, so $1 \in \operatorname{Supp}(x^{-1}\alpha)$ and $1 \in \operatorname{Supp}(\beta y^{-1})$. Thus, without loss of generality, we can assume that $1 \in \operatorname{Supp}\alpha$ and $1 \in \operatorname{Supp}\beta$. In particular, since $1 \in \Delta$, we know that α_0 and β_0 are nonzero. We now show that $\alpha_0\beta_0 = 0$.

Suppose that $\alpha_0\beta_0 \neq 0$. Recall that for any $x, y \in G$, conjugates of xy are products of conjugates of *x* and *y*. So since $\operatorname{Supp}\alpha_0$ and $\operatorname{Supp}\beta_0$ are subsets of Δ, it follows that $\operatorname{Supp}(\alpha_0\beta_0) \subseteq \Delta$, and since $\operatorname{Supp}\beta_1 \subseteq G-\Delta$, it follows that $\operatorname{Supp}(\alpha_0\beta_1) \subseteq G-\Delta$. Then $\alpha_0\beta = \alpha_0\beta_0 + \alpha_0\beta_1$ is not zero since $\alpha_0\beta_0 \neq 0$ and there is no overlap in the group elements in the expressions for $\alpha_0\beta_0$ and $\alpha_0\beta_1$.

Fix $z \in \operatorname{Supp}(\alpha_0\beta)$. For any $a \in \operatorname{Supp}\alpha_0$ we know that $a \in \Delta$ and hence $[G : C_G(a)]$ is finite. Let

$$H = \bigcap_{a \in \operatorname{Supp}\alpha_0} C_G(a).$$

By Lemma 2.5, $[G : H] < \infty$. Let $h \in H$. Then for every $a \in \operatorname{Supp}\alpha_0$, $h^{-1}ah = a$. Hence, $h^{-1}\alpha_0 h = \alpha_0$. Then, since $\alpha(FG)\beta = 0$ and thus $\alpha h\beta = 0$,

$$0 = h^{-1}\alpha h\beta = h^{-1}(\alpha_0 + \alpha_1)h\beta = h^{-1}\alpha_0 h\beta + h^{-1}\alpha_1 h\beta = \alpha_0\beta + h^{-1}\alpha_1 h\beta.$$

In particular, $-\alpha_0\beta = h^{-1}\alpha_1 h\beta$. Since $z \in \operatorname{Supp}(\alpha_0\beta)$, it is clear that $z \in \operatorname{Supp}(-\alpha_0\beta)$, so that $z \in \operatorname{Supp}\left(h^{-1}\alpha_1 h\beta\right)$. So if $\operatorname{Supp}\alpha_1 = \{x_1, \ldots, x_n\}$ and $\operatorname{Supp}\beta = \{y_1, \ldots, y_m\}$, then $z = h^{-1}x_i h y_j$ for some $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, m\}$. In other words, $zy_j^{-1} = h^{-1}x_i h$, and thus x_i is conjugate to zy_j^{-1} in *G*.

Although *H* may be infinite, there are only finitely many pairs (x_i, y_j), and thus only finitely many (i, j), such that x_i is conjugate to zy_j^{-1}. So we can choose (finitely many) $g_{ij} \in G$ such that $g_{ij}^{-1}x_i g_{ij} = zy_j^{-1}$. So for each $h \in H$, there exist (i, j) such that $h^{-1}x_i h = g_{ij}^{-1}x_i g_{ij}$, so $\left(hg_{ij}^{-1}\right)^{-1} x_i \left(hg_{ij}^{-1}\right) = x_i$. That is, $hg_{ij}^{-1} \in C_G(x_i)$. Thus for every $h \in H$ there exists (i, j) such that $h \in C_G(x_i)g_{ij}$, so that $H \subseteq \bigcup_{i,j} C_G(x_i)g_{ij}$. But $[G:H] < \infty$, so the number of (right) cosets of *H* is finite. So *G* is a finite union of cosets of *H*, with representatives $w_1, \ldots, w_k$: $G = \bigcup_k Hw_k$. Thus, $G = \bigcup_{i,j,k} C_G(x_i)g_{ij}w_k$ is a finite union of cosets of the subgroups $C_G(x_i)$, and Lemma 2.5 allows us to conclude that for some *i*, $\left[G : C_G(x_i)\right] < \infty$. But this implies that $x_i \in \Delta$, which contradicts the fact that $x_i \in \operatorname{Supp}\alpha_1$. Thus, $\alpha_0\beta_0 = 0$.

So we have $\alpha_0\beta_0 = 0$ with α_0 and β_0 nonzero elements of $F\Delta$. That is, $F\Delta$ has nontrivial zero divisors, so that Δ cannot be a torsion-free abelian group by Proposition 2.2. By Lemma 2.4(ii), however, Δ/Δ^+ is a torsion-free abelian group. It follows that Δ^+ is nontrivial, and so by Lemma 2.4(iii), *G* has a nontrivial finite normal subgroup. ■

The relation of Theorem 2.3 to the zero divisor problem is further shown in a corollary.

Corollary 2.6. Let *G* be a torsion-free group and *F* be a field. Then FG has zero divisors if and only if FG has nonzero elements whose squares are zero.

Proof. The backward direction is simple, for if $a \in FG$ is nonzero such that $a^2 = 0$, then a is a zero divisor.

The forward direction isn't much harder. Let $a, b \in FG$ be nonzero such that $ab = 0$. Since G is torsion-free, G cannot have a nontrivial finite normal subgroup, so Theorem 2.3 implies that FG is prime. So $b(FG)a \neq 0$. However, since $ab = 0$, for every $\alpha \in FG$, $(b\alpha a)(b\alpha a) = b\alpha(ab)\alpha b = 0$. This implies that every element of $b(FG)a$ has square zero. ■

Section 3. Semisimplicity

The question of semisimplicity in group rings is also an important area of interest. Much of our focus will be on group rings where the ring is the field $\mathbb{C}$ of complex numbers. First, we present a more general result pertaining to group rings where the ring is any field of characteristic 0. Some of the following proofs will require not only the tools of Algebra, but also the tools of Analysis. Again, we need some definitions.

Definition 3.1. Let R be a ring and let U be an R-module. Then:

- U is *simple* if $U \neq 0$ and U has no proper nonzero submodules;
- U is *semisimple* if it is a direct sum of simple modules; and
- U is *injective* if whenever U is a submodule of an R-module V, then V has a submodule W such that $V = U \oplus W$.

We will be working with left modules. The results, however, are analogous for right modules. If G is a finite group and F is a field, the following theorem provides the condition under which every FG-module is injective.

Theorem 3.1 (Maschke). Let *G* be a finite group and let *F* be a field with $\operatorname{char}(F) \nmid |G|$. If *V* is any *FG*-module and *U* is any submodule of *V*, then *V* has a submodule *W* such that $V = U \oplus W$.

Proof. Let *V* be an *FG*-module and let *U* be a submodule of *V*. We will construct an *FG*-module homomorphism $\pi : V \to U$ satisfying the following:

(i) $\pi(u) = u$ for every $u \in U$; and

(ii) $\pi(\pi(v)) = \pi(v)$ for every $v \in V$ (so that $\pi^2 = \pi$).

Assuming we have such a homomorphism, set $W = \ker \pi$. Then *W* is a submodule of *V*. If $v \in U \cap W$, then $v = \pi(v)$ since $v \in U$ and $\pi(v) = 0$ since $v \in W$. So $U \cap W = 0$. If $v \in V$, write $v = \pi(v) + (v - \pi(v))$. We have $\pi(v) \in U$ and $v - \pi(v) \in W$, since $\pi(v - \pi(v)) = \pi(v) - \pi^2(v) = \pi(v) - \pi(v) = 0$. Hence $v \in U + W$, and thus $V = U \oplus W$.

We now show the existence of such a function π. First note that *V* is an *F*-vector space, and *U* is an *F*-vector subspace of *V*. Start with an *F*-basis $\mathcal{B}_1$ of *U*. Extend this to a basis $\mathcal{B}$ of *V* containing $\mathcal{B}_1$. Then $W_0 = \operatorname{span}(\mathcal{B} \setminus \mathcal{B}_1)$ is the *F*-complement of *U* in *V*. But W_0 is not necessarily an *FG*-submodule in its own right.

Nonetheless, every element of *V* can be expressed uniquely as the sum of an element in *U* and an element in W_0. So we can define $\pi_0 : V \to U$ by $\pi_0(u + w) = u$ for every $u \in U$ and $w \in W_0$. For each $a \in G$, define $\lambda_a : V \to V$ by $\lambda_a(v) = a \cdot v$. Note that each λ_a is *F*-linear and that for every $a \in G$, $\lambda_{a^{-1}} = \lambda_a^{-1}$. Then for each *a*, $\lambda_a \circ \pi_0 \circ \lambda_{a^{-1}} : V \to V$ is a map given by $(\lambda_a \circ \pi_0 \circ \lambda_{a^{-1}})(v) = a\pi_0(a^{-1}v)$. Since π_0 maps *V* to *U*, and *U* is stable under the action of *G*, the image of $\lambda_a \circ \pi_0 \circ \lambda_{a^{-1}}$ is in *U*. Since λ_a, π_0, and $\lambda_{a^{-1}}$ are *F*-linear, $\lambda_a \circ \pi_0 \circ \lambda_{a^{-1}}$ is an *F*-linear transformation. Further, if $u \in U$, then $a^{-1}u \in U$, so

$\pi_0\left(a^{-1}u\right)=a^{-1}u$. That is, for every $u\in U$,

$$\left(\lambda_a\circ\pi_0\circ\lambda_{a^{-1}}\right)(u)=a\pi_0\left(a^{-1}u\right)=aa^{-1}u=u.$$

Now let $n=|G|=|G|\cdot 1_F$ as an element of *F*. Since $\operatorname{char}(F)\nmid n$, we know *n* is nonzero, and hence *n* has an inverse in *F*. We now define the map $\pi:V\to U$ by

$$\pi(v)=\frac{1}{n}\sum_{a\in G}\left(\lambda_a\circ\pi_0\circ\lambda_{a^{-1}}\right)(v).$$

Then π is a linear combination of *F*-linear transformations, and so is *F*-linear. If $u\in U$, then

$$\pi(u)=\frac{1}{n}\sum_{a\in G}\left(\lambda_a\circ\pi_0\circ\lambda_{a^{-1}}\right)(u)=\frac{1}{n}nu=u.$$

Also, if $v\in V$, then $\pi(v)\in U$, and so $\pi^2(v)=\pi\left(\pi(v)\right)=\pi(v)$.

All that is left to show is that π is in fact an *FG*-module homomorphism. We note that for every $h\in G$ and $v\in V$,

$$\begin{aligned}\pi(hv)&=\frac{1}{n}\sum_{a\in G}\lambda_a\circ\left(\pi_0\circ\lambda_{a^{-1}}\right)(hv)\\&=\frac{1}{n}\sum_{a\in G}h\left(h^{-1}a\right)\pi_0\left(\left(a^{-1}h\right)v\right)\\&=\frac{1}{n}\sum_{\substack{k=h^{-1}a\\a\in G}}h\lambda_k\circ\left(\pi_0\circ\lambda_{k^{-1}}\right)(v)\\&=h\frac{1}{n}\sum_{\substack{k=h^{-1}a\\a\in G}}\lambda_k\circ\left(\pi_0\circ\lambda_{k^{-1}}\right)(v)\\&=h\pi(v).\end{aligned}$$

The additive aspect of the homomorphism follows from the fact that π is *F*-linear, and thus π is an *FG*-module homomorphism. ■

Note that if $\operatorname{char}(F)=0$, then Theorem 3.1 applies to any finite group. Also, by Wedderburn's Theorem, *FG* is semisimple since Theorem 3.1 implies that every *FG*-module is injective [2, p. 820].

The remainder of our focus will be on group rings with coefficients in $\mathbb{C}$. Complex group rings are relatively accessible while remaining interesting. The tools of Analysis will finally come into play as we explore a slightly different, yet closely related, version of semisimplicity known as *Jacobson semisimplicity*.

Definition 3.2. Let *R* be a ring. Then the *Jacobson radical* of *R*, denoted $J(R)$, is the intersection of all maximal ideals of *R*. The ring *R* is called *Jacobson semisimple* when $J(R)=0$.

Jacobson semisimplicity is closely related to the usual semisimplicity through a theorem that says a ring *R* is (left) semisimple if and only if it is (left) artinian and $J(R)=0$ [6, p. 555]. Recall that a ring *R* is *(left) artinian* if every descending chain of (left) ideals $I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$ terminates—so there is some $n \geq 1$ such that for all $m \geq n$, $I_m = I_n$.

Before looking at results that are specific for group rings, there is an alternate characterization of $J(R)$ for any ring with unity, which we will find useful.

Lemma 3.2. Let *R* be a ring with unity. Then

$$J(R)=\{x \in R : 1-rx \text{ is invertible for all } r \in R\}.$$

Proof: Let $x \in R$ such that $1-rx$ is not a unit for some $r \in R$. Let M be a maximal ideal of R with $1-rx \in M$. Since $1 \notin M$, we have $rx \notin M$. Since $J(R) \subseteq M$, $rx \notin J(R)$, and hence $x \notin J(R)$.

Now, let $x \in R \setminus J(R)$. So there is a maximal ideal M of R with $x \notin M$. So $R = (M, x)$. So $1 = y + rx$ for some $y \in M$. Since $1-rx = y$, $1-rx \in M$. Thus $1-rx$ is not a unit. That is, $x \in R$ such that $1-rx$ is not a unit for some $r \in R$.

By double inclusion, $J(R) = \{x \in R : 1-rx \text{ is invertible for all } r \in R\}$. ■

We'll need a few more definitions and lemmas before we can discuss semisimplicity of complex group rings.

Definition 3.3. Let G be a group, and let $\delta = \sum d_x x$ be in $\mathbb{C}G$. Define $|\delta|$ by

$$|\delta| = \sum |d_x|,$$

where $|d_x| = \sqrt{d_x \bar{d}_x}$ is the usual absolute value (modulus) on $\mathbb{C}$.

Lemma 3.3. Let G be a group. Then for all $\alpha, \beta \in \mathbb{C}G$,

(i) $|\alpha + \beta| \leq |\alpha| + |\beta|$;

(ii) $|\alpha\beta| \leq |\alpha||\beta|$; and

(iii) $|\alpha^n| \leq |\alpha|^n$ for every $n \in \mathbb{N}$.

Proof. Let G be a group, and let $\alpha, \beta \in \mathbb{C}G$. Write $\alpha = \sum a_x x$ and $\beta = \sum b_y y$. Then:

(i) $|\alpha+\beta| = \left|\sum a_x x + \sum b_y y\right| = \left|\sum_{x=y}(a_x + b_y)x\right| = \sum_{x=y}|a_x + b_y| \le \sum_x |a_x| + \sum_y |b_y| = |\alpha| + |\beta|$.

(ii) Using part (i), we see that

$$|\alpha\beta| = \left|\left(\sum a_x x\right)\left(\sum b_y y\right)\right| = \left|\sum_{(x,y)}(a_x b_y)xy\right| \le \sum_{(x,y)}\left|(a_x b_y)xy\right| = \sum_{(x,y)}|a_x b_y|.$$

But since the modulus operator is multiplicative in $\mathbb{C}$,

$$\sum_{(x,y)}|a_x b_y| = \sum_{(x,y)}|a_x||b_y| = \left(\sum |a_x|\right)\left(\sum |b_y|\right) = |\alpha||\beta|,$$

and hence $|\alpha\beta| \le |\alpha||\beta|$.

(iii) Because $|\alpha^n| = |\alpha^{n-1}\alpha| \le |\alpha^{n-1}||\alpha|$ by (ii), an inductive argument shows that $|\alpha^n| \le |\alpha|^n$. ■

Definition 3.4. For an element $\alpha \in \mathbb{C}G$ where $\alpha = \sum a_x x$, define the * operator by

$$\alpha^* = \sum \bar{a}_x x^{-1},$$

where $\bar{a}_x$ denotes the complex conjugate of a_x.

Example. Let $G = Z_8 = \langle x \rangle$ be the cyclic group of order 8, and consider the element $\alpha = ix^2 + (2+3i)x^5$ in $\mathbb{C}G$. Then $\alpha^* = (-i)x^6 + (2-3i)x^3$.

Proposition 3.4. Let G be a group. The * operator defined above has the following properties for every $\alpha = \sum a_x x$ and $\beta = \sum b_y y$ in $\mathbb{C}G$, and for every $z \in \mathbb{C}$:

(i) $(\alpha + \beta)^* = \alpha^* + \beta^*$;

(ii) $(z\alpha)^* = \overline{z}(\alpha^*)$;

(iii) $(\alpha\beta)^* = \beta^*\alpha^*$; and

(iv) $(\alpha^n)^* = (\alpha^*)^n$ for every $n \in \mathbb{N}$.

Proof. Property (i) follows readily from the fact that complex conjugation respects addition. Property (ii) follows from the fact that complex conjugation respects multiplication. Property (iii) also follows from the fact that complex conjugation respects multiplication, along with the fact that for group elements x and y, $(xy)^{-1} = y^{-1}x^{-1}$. Property (iv) is an immediate consequence of property (iii) using an induction argument, since $(\alpha^n)^* = (\alpha^{n-1}\alpha)^* = \alpha^*(\alpha^{n-1})^*$. ■

Definition 3.5. Let G be a group. Let $\sum a_x x \in \mathbb{C}G$. Define the *trace map* $\mathrm{tr} : \mathbb{C}G \to \mathbb{C}$ such that $\mathrm{tr}\left(\sum a_x x\right) = a_1$, where a_1 is the coefficient of the identity element in G. Note that the trace map is $\mathbb{C}$-linear, since for any $\sum a_x x, \sum b_x x \in \mathbb{C}G$ and $z, w \in \mathbb{C}$,

$$\mathrm{tr}\left(z\sum a_x x + w\sum b_x x\right) = \mathrm{tr}\left(\sum (za_x + wb_x)x\right) = za_1 + wb_1 = z\cdot\mathrm{tr}\left(\sum a_x x\right) + w\cdot\mathrm{tr}\left(\sum b_x x\right).$$

Slowly but surely we're getting closer to our big result. We only need one more definition and three more lemmas.

Definition 3.6. Let G be a group. Let $\alpha = \sum a_x x$ and $\beta = \sum b_x x$ be in $\mathbb{C}G$. Define a Hermitian inner product on $\mathbb{C}G$ by

$$\left(\alpha,\beta\right)=\sum_x a_x\overline{b}_x .$$

The norm associated with this inner product is

$$\|\alpha\|=\left(\alpha,\alpha\right)^{1/2}=\left(\sum_x a_x\overline{a}_x\right)^{1/2}=\left(\sum_x |a_x|^2\right)^{1/2}.$$

Lemma 3.5. The inner product defined above is, in fact, a Hermitian inner product.

Proof. Let G be a group, and let $\sum a_x x$, $\sum b_x x$, and $\sum c_x x$ be in $\mathbb{C}G$. Let $z\in\mathbb{C}$.

Note that

$$\begin{aligned}\left(\sum a_x x+\sum c_x x,\sum b_x x\right)&=\left(\sum\left(a_x+c_x\right)x,\sum b_x x\right)\\&=\sum\left(a_x+c_x\right)\overline{b}_x\\&=\sum a_x\overline{b}+\sum c_x\overline{b}\\&=\left(\sum a_x x,\sum b_x x\right)+\left(\sum c_x x,\sum b_x x\right),\end{aligned}$$

and

$$\begin{aligned}\left(\sum a_x x,\sum b_x x+\sum c_x x\right)&=\left(\sum a_x x,\sum\left(b_x+c_x\right)x\right)\\&=\sum a_x\overline{\left(b_x+c_x\right)}\\&=\sum a_x\left(\overline{b}_x+\overline{c}_x\right)\\&=\sum a_x\overline{b}+\sum a_x\overline{c}_x\\&=\left(\sum a_x x,\sum b_x x\right)+\left(\sum a_x x,\sum c_x x\right).\end{aligned}$$

Also,

$$\begin{aligned}\left(z\sum a_x x,\sum b_x x\right)&=\left(\sum za_x x,\sum b_x x\right)\\&=\sum za_x\overline{b}_x\\&=z\sum a_x\overline{b}_x\\&=z\left(\sum a_x x,\sum b_x x\right),\end{aligned}$$

and

$$
\begin{aligned}
\left(\sum a_x x, z\sum b_x x\right) &= \left(\sum a_x x, \sum z b_x x\right) \\
&= \sum a_x \overline{z b_x} \\
&= \bar{z} \sum a_x \bar{b}_x \\
&= \bar{z}\left(\sum a_x x, \sum b_x x\right).
\end{aligned}
$$

Additionally,

$$
\begin{aligned}
\left(\sum a_x x, \sum b_x x\right) &= \left(\sum a_x x, \sum b_x x\right) \\
&= \sum a_x \bar{b}_x \\
&= \sum \overline{b_x \bar{a}_x} \\
&= \overline{\left(\sum b_x x, \sum a_x x\right)}.
\end{aligned}
$$

Finally, $\left(\sum a_x x, \sum a_x x\right) = \sum a_x \bar{a}_x = \sum |a_x|^2$. Thus, $\left(\sum a_x x, \sum a_x x\right)$ is a nonnegative real number, and $\left(\sum a_x x, \sum a_x x\right) = 0$ if and only if $a_x = 0$ for every $x \in G$. ■

The relationships among the * operator, the inner product, the norm, and the trace map are explored in the following lemmas.

Lemma 3.6. Let *G* be a group. For all elements $\alpha \in \mathbb{C}G$, $(\alpha, \alpha) = \operatorname{tr}\left(\alpha\alpha^*\right)$.

Proof. Let $\alpha = \sum a_x x$ be an element of $\mathbb{C}G$. Then $\alpha^* = \sum \bar{a}_x x^{-1}$, so

$$
\operatorname{tr}\left(\alpha\alpha^*\right) = \operatorname{tr}\left(\left(\sum a_x x\right)\left(\sum \bar{a}_x x^{-1}\right)\right).
$$

But the trace map produces the coefficient of the group identity element. In the product, we get the group identity element exactly when each *x* multiplies its inverse. So for each *x*, since $\bar{a}_x$ is the coefficient of x^{-1} in α^* we get $a_x \bar{a}_x = |a_x|^2$ attached to the group identity. Summing all of these gives us $\sum|a_x|^2$ as the coefficient of the group identity of the product $\alpha\alpha^*$ as a whole. Hence, $\operatorname{tr}(\alpha\alpha^*) = \sum|a_x|^2 = (\alpha,\alpha)$. ■

Lemma 3.7. Let G be a group. For all elements $\alpha \in \mathbb{C}G$, $|\operatorname{tr}\alpha| \le \|\alpha\|$ and $|\operatorname{tr}\alpha| \le |\alpha|$.

Proof. Let $\alpha = \sum a_x x$ be an element of $\mathbb{C}G$. Then $|\operatorname{tr}\alpha| = |a_1|$. Also,

$$\|\alpha\| = \left(\sum|a_x|^2\right)^{1/2} = \left(|a_1|^2 + \sum_{x\ne 1}|a_x|^2\right)^{1/2}.$$

But the square root function is an increasing function. So since $|a_1|^2 \le |a_1|^2 + \sum_{x\ne 1}|a_x|^2$, we have

$$|\operatorname{tr}\alpha| = |a_1| = \left(|a_1|^2\right)^{1/2} \le \left(|a_1|^2 + \sum_{x\ne 1}|a_x|^2\right)^{1/2} = \|\alpha\|$$

and

$$|\operatorname{tr}\alpha| = |a_1| \le |a_1| + \sum_{x\ne 1}|a_x| = |\alpha|. \ ■$$

Finally, we can put all of these definitions and lemmas together in order to help prove that complex group rings have Jacobson radical 0.

Theorem 3.8. For all groups G, $J(\mathbb{C}G) = 0$.

Proof: Let G be a group. Fix $\alpha \in J(\mathbb{C}G)$. By Lemma 3.2, $1 - z\alpha$ is invertible for every $z \in \mathbb{C}$.

Define $h : \mathbb{C} \to \mathbb{C}G$ by $h(z) = (1 - z\alpha)^{-1}$, and define $f : \mathbb{C} \to \mathbb{C}$ by $f(z) = \operatorname{tr}(h(z))$.

Note that elements of $h(\mathbb{C})$ commute: Let $y, w \in \mathbb{C}$. Then

$$\begin{aligned}(1-y\alpha)(1-w\alpha) &= 1-w\alpha-y\alpha-(yw\alpha\alpha)\\ &= 1-y\alpha-w\alpha-(wy\alpha\alpha)\\ &= (1-w\alpha)(1-y\alpha),\end{aligned}$$

and so

$$\begin{aligned}(1-y\alpha)^{-1}(1-w\alpha)^{-1} &= \left[(1-w\alpha)(1-y\alpha)\right]^{-1}\\ &= \left[(1-y\alpha)(1-w\alpha)\right]^{-1}\\ &= (1-w\alpha)^{-1}(1-y\alpha)^{-1}.\end{aligned}$$

So for $z, z_0 \in \mathbb{C}$, we have

$$\begin{aligned}h(z)-h(z_0) &= (1-z\alpha)^{-1}-(1-z_0\alpha)^{-1}\\ &= \left[(1-z_0\alpha)-(1-z\alpha)\right](1-z\alpha)^{-1}(1-z_0\alpha)^{-1}\\ &= (z-z_0)\alpha h(z)h(z_0).\end{aligned}$$

So $h(z_0)=h(z)-(z-z_0)\alpha h(z)h(z_0)$, and by Lemma 3.3 we have

$$|h(z_0)| \le |h(z)| + |z-z_0||\alpha h(z)||h(z_0)|.$$

Thus,

$$|h(z_0)|\left[1-|z-z_0||\alpha h(z)|\right] \le |h(z)|.$$

For a fixed z, if z_0 is close to z, then $|z-z_0|$ is small. So we can make z_0 sufficiently close to z, so that $0 \le |z-z_0||\alpha h(z)| \le 0.5$. Then $0.5 \le 1-|z-z_0||\alpha h(z)|$, so

$$|h(z_0)|(0.5) \le |h(z_0)|\left[1 - |z - z_0||\alpha h(z)|\right] \le |h(z)|.$$

That is, $h(z_0)$ is bounded in a neighborhood of z.

Next, we show that f is an entire function. Recall from Complex Analysis that a function *f* is *entire* if it is analytic at every point of the complex plane; a function *f* is *analytic* at a point *z* if its derivative $f'(z)$ exists at every point in some neighborhood of *z*. We have

$$h(z) - h(z_0) = (z - z_0)\alpha h(z) h(z_0) = (z - z_0)\alpha h(z)\left[h(z) - (z - z_0)\alpha h(z) h(z_0)\right],$$

and thus

$$\begin{aligned} \frac{h(z) - h(z_0)}{z - z_0} &= \alpha h(z)\left[h(z) - (z - z_0)\alpha h(z) h(z_0)\right] \\ &= \alpha h(z)^2 - (z - z_0)(\alpha h(z))^2 h(z_0). \end{aligned}$$

Recall that the trace map is $\mathbb{C}$-linear, so

$$\frac{f(z) - f(z_0)}{z - z_0} = \operatorname{tr}\left(\frac{h(z) - h(z_0)}{z - z_0}\right) = \operatorname{tr}\left(\alpha h(z)^2\right) - (z - z_0)\operatorname{tr}\left((\alpha h(z))^2 h(z_0)\right).$$

Since $|\operatorname{tr}(\beta)| \le |\beta|$ for all $\beta \in \mathbb{C}G$ and $|h(z_0)|$ is bounded near z,

$$\lim_{z_0 \to z} \frac{f(z) - f(z_0)}{z - z_0} = \operatorname{tr}\left(\alpha h(z)^2\right).$$

So f is an entire function with $f'(z) = \operatorname{tr}\left(\alpha h(z)^2\right)$.

We now need to find the Taylor series for *f* about the origin. Recall that for any function *k* that is analytic at all points within a circle *C* centered at w_0, its Taylor series centered at w_0 converges to *k* at each point *w* in *C*. That is,

$$k(w) = \sum_{n=0}^{\infty} \frac{k^{(n)}(w_0)}{n!}(w - w_0)^n ,$$

where $k^{(n)}$ denotes the n^{th} derivative of *k*, with the 0^{th} derivative denoting the function *k* itself. We will apply a Complex Analysis result that says that if a series of the form $\sum_{n=0}^{\infty} a_n (w - w_0)^n$ converges to $k(w)$ in some circle centered at w_0, then the series is the Taylor series of the function *k* [1, p.130].

For $n \in \mathbb{N} \cup \{0\}$, set $s_n(z) = \sum_{i=0}^{n} z^i \operatorname{tr}(\alpha^i)$. Then

$$\begin{aligned}
f(z) - s_n(z) &= \operatorname{tr}(h(z) - s_n(z)) \\
&= \operatorname{tr}\left(h(z) - \sum_{i=0}^{n} z^i \alpha^i \right) \\
&= \operatorname{tr}\left((1 - z\alpha)^{-1} - \sum_{i=0}^{n} z^i \alpha^i \right) \\
&= \operatorname{tr}\left((1 - z\alpha)^{-1} \left[1 - (1 - z\alpha) \sum_{i=0}^{n} z^i \alpha^i \right] \right) \\
&= \operatorname{tr}\left(h(z) \left[1 - \sum_{i=0}^{n} z^i \alpha^i + z\alpha \sum_{i=0}^{n} z^i \alpha^i \right] \right) \\
&= \operatorname{tr}\left(h(z) \left[1 - \sum_{i=0}^{n} z^i \alpha^i + \sum_{i=0}^{n} z^{i+1} \alpha^{i+1} \right] \right) \\
&= \operatorname{tr}\left(h(z) z^{n+1} \alpha^{n+1} \right).
\end{aligned}$$

So by Lemmas 3.7 and 3.3,

$$\left| f(z) - s_n(z) \right| = \left| \operatorname{tr}\left(h(z) z^{n+1} \alpha^{n+1} \right) \right| \le \left| h(z) \right| \left| z \right|^{n+1} \left| \alpha \right|^{n+1}.$$

Earlier we saw that $h(z_0)$ is bounded in a neighborhood of z. Specifically, $\left| h(z_0) \right|$ is bounded in a neighborhood of 0. So for z_0 sufficiently close to 0, say $\left| z_0 \right| < \frac{1}{2\left|\alpha\right|}$, then

$$\begin{aligned}
\lim_{n\to\infty} \left| f(z_0) - s_n(z_0) \right| &\le \lim_{n\to\infty} \left| h(z_0) \right| \left| z_0 \right|^{n+1} \left| \alpha \right|^{n+1} \\
&< \lim_{n\to\infty} \left| h(z_0) \right| \left(\frac{1}{2\left|\alpha\right|} \right)^{n+1} \left| \alpha \right|^{n+1} \\
&= \left| h(z_0) \right| \lim_{n\to\infty} \frac{1}{2^n} \\
&= 0.
\end{aligned}$$

Thus, $f(z_0) = \lim_{n\to\infty} s_n(z_0) = \sum_{i=0}^{\infty} z_0^i \operatorname{tr}\left(\alpha^i\right)$, where $\sum_{i=0}^{\infty} z_0^i \operatorname{tr}\left(\alpha^i\right)$ is the Taylor series expansion for $f(z_0)$ in a neighborhood around the origin. Since *f* is an entire function, the Taylor series converges for all z. This shows that for all $\alpha \in J(\mathbb{C}G)$,

$$\lim_{n\to\infty} \operatorname{tr}\left(\alpha^n\right) = 0.$$

But suppose that β is a nonzero element of $J(\mathbb{C}G)$, and let $\alpha = \beta\beta^* / \left\|\beta\right\|^2$. We will show that $\operatorname{tr}\left(\alpha^{2^m}\right) \ge 1$ for all $m \ge 0$, contradicting that $\lim_{n\to\infty} \operatorname{tr}\left(\alpha^n\right) = 0$. This will show that there can be no nonzero elements of $J(\mathbb{C}G)$.

Since $J(\mathbb{C}G)$ is an ideal of $\mathbb{C}G$ and $\beta \in J(\mathbb{C}G)$, then $\alpha \in J(\mathbb{C}G)$. Also, $\alpha = \alpha^*$ since

$$\alpha^* = \left(\frac{\beta\beta^*}{\|\beta\|^2}\right)^* = \frac{(\beta\beta^*)^*}{\|\beta\|^2} = \frac{(\beta^*)^*\beta^*}{\|\beta\|^2} = \frac{\beta\beta^*}{\|\beta\|^2} = \alpha .$$

So by Proposition 3.4, $(\alpha^n)^* = (\alpha^*)^n = \alpha^n$ for all $n \in \mathbb{N}$.

Then by Lemma 3.6,

$$\operatorname{tr}\alpha = \frac{\operatorname{tr}(\beta\beta^*)}{\|\beta\|^2} = \frac{(\beta,\beta)}{\|\beta\|^2} = \frac{\|\beta\|^2}{\|\beta\|^2} = 1.$$

Suppose that for some $k \geq 0$, $\operatorname{tr}\left(\alpha^{2^k}\right) \geq 1$. Then

$$\operatorname{tr}\left(\alpha^{2^{k+1}}\right) = \operatorname{tr}\left(\alpha^{2^k}\alpha^{2^k}\right) = \operatorname{tr}\left(\alpha^{2^k}\left(\alpha^{2^k}\right)^*\right) = \left(\alpha^{2^k}, \alpha^{2^k}\right) = \left\|\alpha^{2^k}\right\|^2 \geq \left|\operatorname{tr}\left(\alpha^{2^k}\right)\right|^2 \geq 1^2 = 1.$$

So by induction, $\operatorname{tr}\left(\alpha^{2^m}\right) \geq 1$ for all $m \geq 0$, which contradicts that $\lim_{n\to\infty} \operatorname{tr}(\alpha^n) = 0$. Hence, there are no nonzero elements of $J(\mathbb{C}G)$, and thus $J(\mathbb{C}G) = 0$. ■

Passman shows that when *F* is a field, the group ring FG is artinian if and only if *G* is finite [3, p. 7]. This, together with Theorem 3.9, allows us to conclude that $\mathbb{C}G$ is semisimple if and only if *G* is finite.

Conclusion

There are many further avenues to explore when it comes to group rings. As we mentioned earlier, one could investigate the zero divisor problem as it applies to free groups and supersolvable groups, as well as searching for an resolution to the general conjecture. We barely scratched the surface in this paper when it comes to semisimplicity. General conditions under which a group ring is semisimple (or even Jacobson semisimple) are highly sought after. The interested reader can investigate the final chapter of [3] for a more detailed list of open problems. Although [3] was first published in (1971), many of these questions appear to still be unresolved.

References

[1] Churchill, R. V. (1960). *Complex Variables and Applications*. York, PA: The Maple Press Company.

[2] Dummit, D. S., & R. M. Foote. (1999). *Abstract Algebra*. 2nd edition. New York: Wiley.

[3] Passman, D. S. (1971). *Infinite Group Rings*. New York: Marcel Dekker, Inc.

[4] Passman, D. S. (1976). "What is a group ring?," *The American Mathematical Monthly*, *83*(3), 173-185.

[5] Passman, D. S. (2011). *The Algebraic Structure of Group Rings*. Mineola, NY: Dover Publications.

[6] Rotman, J. J. (2002). *Advanced Modern Algebra*. Upper Saddle River, NJ: Pearson Education, Inc.