An analysis of Semisimple Group Rings and Integral Group Rings

David Breadner

April 2018

1 Abstract

This paper outlines the difference between trivial and nontrivial units, and uses Bicyclic units to show when certain types of Group Rings only have trivial units.

2 Introduction

This paper will outline the concept of Group Rings and show some important results for understanding their structure. I will start by outlining general group rings and transition into an analysis of the units of integral group rings.

3 Modules

Definition 3.1. *Let R be a ring. An abelian group M is called a* ***left R-module*** *if for each $a \in R$ and every $m \in M$ we have $am \in M$ such that:*

(i) $(a+b)m = am + bm$

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

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

(iv) $1m = m$

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

Right R-module is defined similarly with multiplication of the ring elements on the right rather than left.

Example 3.2. *For any abelian group A we can show that A is a $\mathbb{Z}$-module with the following calculations.*
For $a, b \in \mathbb{Z}$ and $m, m_1, m_2 \in A$ we can define multiplication by:

$$am = \underbrace{m + \cdots + m}_{a\text{-}times}$$

Then

(i)

$(a+b)m = \underbrace{m + \cdots + m}_{(a+b)\text{-}times}$

$= \underbrace{m + \cdots + m}_{a\text{-}times} + \underbrace{m + \cdots + m}_{b\text{-}times}$

$= am + bm$

(ii) $a(m_1 + m_2) = \underbrace{m_1 + m_2 \cdots m_1 + m_2}_{a\text{-}times}$

$= \underbrace{m_1 + \cdots + m_1}_{a-times} + \underbrace{m_2 + \cdots + m_2}_{a-times}$

$= am_1 + am_2$

(iii) Associativity is carried from Z as a ring.

(iv) $1m = \underbrace{m}_{1-time} = m$

We can easily see that rings are modules over themselves.

Definition 3.3. *Let M be a module over a ring R. A subset $N \subset M$ is an **R-submodule** if*

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

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

A module that contains only itself and the zero ring as submodules is called **simple**

Definition 3.4. *An R-module M is called semisimple if every submodule is a direct summand.*

Proposition 3.5. *Let $N \neq (0)$ be a submodule of a semisimple module M. Then N is semisimple and it contains a simple submodule.*

Proof. Let S be an arbitrary submodule of N. Then S is also a submodule of M, so there exists another submodule S' such that $M = S \oplus S'$. We claim that $N = S \oplus (S' \cap N)$. Since $N \cap S' \subset S'$ it is obvious that $S \cap (S' \cap N) \subset S \cap S' = \{0\}$ Therefore for any $n \in N$ we can write $n = x + y$ with $x \in S$ and $y \in S'$. But $y = n - x \in N$ so $y \in N \cap S'$, as desired. Therefore $N = S \oplus (S' \cap N)$ and N is semisimple.
Choose $x \in N, x \neq 0$. Notice that the family of all submodules of N not containing x is nonempty and every totally ordered family has an upper bound. Then by Zorn's Lemma, there exists a maximal element N_1. Since N is semisimple, there exists another submodule N_2 of N sucht that $N = N_1 \oplus N_2$. It will now suffice to show that N_2 is simple.
If N_2 is not simple, it contains a proper submodule W and there exists W' such

that $N_2 = W \oplus W'$. Notice that $N = N_1 \oplus W \oplus W'$ and $N_1 = (N_1 + W) \cap (N_1 + W')$. Since $x \not\in N_1$. we have that either $x \not\in N_1 + W$ or $x \not\in N_1 + W'$ This contradicts N_1 is maximum.

□

Definition 3.6. *A ring R is called* ***semisimple*** *if the left module of R over R is semisimple.*

Theorem 3.7. *Let R be a ring. Then the following conditions are equivalent*

i) Every R-module is semisimple

ii) R is a semisimple ring.

iii) R is a direct sum of a finite number of minimal left ideals.

We will omit this proof.

This result is useful for observing the structure of rings. In the same way that the fundamental theorem for finite abelian groups is useful for understanding the structure of all groups we can now analyze the structure of any semisimple ring.

4 Group Rings

Definition 4.1. *Given a group G and a ring R, A* ***group ring of G over R****, denoted RG, is defined by combining the elements of G and R as such*

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

$$\beta = \sum_{g \in G} b_g g$$

where $a_g, b_g \in R$, $g \in G$ and only finitely many a_g or b_g are equal to zero.

Addition in RG is defined by

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

we can define multiplication as

$$\alpha\beta = \sum_{g,h \in G} a_g b_h gh$$

This structure functions as a ring. We can construct left ideals using subgroups of G to further understand their structure.

Definition 4.2. *Let H be a subgroup of G. We denote*

$$\Delta(G,H) = \{\sum_{h\in H} \alpha_h(h-1) : \alpha_h \in RG\}$$

This is an ideal of RG.

We can take the idea of the canonical homomorphism and extend it to group rings. If ω is the cannonical homomorphism from $G \to G/H$ we can define ω^* from $RG \to R(G/H)$ as

$$\omega^*(\alpha) = \sum_{g\in G} a_g g = \sum_{g\in G} a_g \omega(g)$$

Proposition 4.3. *$Ker(\omega^*) = \Delta(G,H)$*

Proof. Define $T = \{q_i\}_{i\in I}$ a complete set of representatives of left cosets of H in G, a transversal of H in G. Assume we choose, as the reprasentative of the coset H in T, precisely the identity element of G. This allows us to write every element $g \in G$ as $g = q_i h_j$ where $q_i \in T$, $h_j \in H$

Thus every element $\alpha \in RG$ can be written as $\sum_{i,j} r_{ij} q_i h_j$
If q_i^* is the image of q_i in G/H. then

$$\omega^*(\alpha) = \sum_i (\sum_j r_{ij}) q_i^*$$

It is easy to see that $\alpha \in Ker(\omega^*)$ if and only if $\sum_j r_{ij} = 0$ for all i. So:

$$\alpha = \sum_{i,j} r_{ij} q_i h_j = \sum_{i,j} r_{ij} q_i h_j - \sum_i (\sum_j r_{ij}) q_i = \sum_{i,j} r_{ij} q_i (h_j - 1) \in \Delta(G,H)$$

The opposite inclusion is trivial. □

Corollary 4.4. *Let H be a normal subgroup of G. Then $\Delta(G,H)$ is a two-sided ideal and, by the first Isomorphism theorem for rings*

$$\frac{RG}{\Delta(G,H)} \simeq R(G/H)$$

Definition 4.5. *Let X be a subset of a group ring RG. The **left annihilator** of X is the set*

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

with right annihilator defined similarly.

Definition 4.6. *Denote $\widehat{X}$ as:*

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

Theorem 4.7. *Let H be a subgroup of G and R be a ring. Then H is finite if and only if $Ann_r(\Delta(G,H)) \neq 0$. and*

$$Ann_r(\Delta(G,H)) = \widehat{H} \cdot RG$$

Also if H is normal in G, then $\widehat{H}$ is is central in RG and the left and right annihilators are equal to each other.

Proof. Assume $Ann_r(\Delta(G,H)) \neq 0$. and choose $\alpha \in Ann_r(\Delta(G,H))$ such that $\alpha \neq 0$ For each $h \in H$ we have, by the definition of right annihilators

$$(h-1)\alpha = 0$$

$$h\alpha = \alpha$$
$$\sum_{g\in G} a_g hg = \sum_{g\in G} a_g g$$

Define supp(α)=$\{g \in G$ such that $a_g \neq 0\}$ Take $g_0 \in supp(\alpha)$ above implies that in α, a_g coinciding with g is the same as a_g coinciding with hg for all $h \in H$. Therefore $hg_0 \in supp(\alpha)$ Since by the definition of group rings only finitely many $a_g \neq 0$ for each α we can conclude that H is a group of finite order.

This also allows us to write α as:

$$\alpha = a_{g0}\widehat{H}g_0 + a_{g1}\widehat{H}g_1 + \cdots + a_{gm}\widehat{H}g_m = \widehat{H}\beta$$

with $\beta \in RG$
This shows that if H is finite, then $Ann_r(\Delta(G,H)) \subset \widehat{H} \cdot RG$ We can show that $\widehat{H} \cdot RG \subset Ann_r(\Delta(G,H))$ by realizing that if H is finite then $h\widehat{H} = \widehat{H}$ for all $h \in H$

$$h\widehat{H} = \widehat{H} \Rightarrow (h-1)\widehat{H} = 0$$

Therefore $\widehat{H} \cdot RG \subset Ann_r(\Delta(G,H))$ We can show similarly that $Ann_l(\Delta(G,H)) = RG \cdot \widehat{H}$

Lastly, if H is normal in G,

$$g^{-1}\widehat{H}g = \sum_{x\in H} g^{-1}xg = \sum_{x\in H} x = \widehat{H}$$

Therefore $\widehat{H}g = g\widehat{H}$ for all $g \in G$, which shows $\widehat{H}$ is central in G. Therefore $RG \cdot \widehat{H} = \widehat{H} \cdot RG$ and $\widehat{H}$ is central in RG. □

For the next result we need the following definition.

Definition 4.8. *The **Augmentation Mapping** $\epsilon : RG \to R$ is given by,*

$$\epsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g$$

Lemma 4.9. *If the ideal $\Delta(G,G)$ is a direct summand of RG as an RG-module then G is finite and $|G|$ is invertible in R.*

Proof. Assume $\Delta(G,G)$ is a direct summand of RG. Then let J be a left ideal such that $RG = \Delta(G,G) \oplus J$ Take $x \in J, y \in \Delta(G,G)$ we can see that $yx \in J \cap \Delta(G,G) = (0)$
Therefore $x \in Ann_r(\Delta(G,G))$ and $Ann_r(\Delta(G,G))$ is nonempty.
This shows that G is finite and $Ann_r(\Delta(G,G)) = \widehat{G}(RG) = \widehat{G}R$ let: $1 = e_1 + e_2$ with $e_1 \in \Delta(G,G)$ and $e_2 \in J$. Consider the augmentation mapping $\epsilon : RG \to R$
$\epsilon(1) = \epsilon(e_1) + \epsilon(e_2)$ Since $e_2 = a\widehat{G}$, for some $a \in R$, we can see that

$$a\epsilon(\widehat{G}) = a\sum_{g\in G} 1 = a|G|$$

Therefore $|G|$ is invertible in R. □

Now we can show when Group Rings are semisimple, in order to more easily understand their structures

Theorem 4.10. ***Mascheke's Theorem**: Let G be a group. Then the group ring RG is semisimple if and only if;*

i) R is a semisimple ring.

ii) G is finite.

iii) $|G|$ is invertible in R.

Proof. $\Rightarrow$ Assume that RG is semisimple. We know that $\dfrac{RG}{\Delta(G,G)} \simeq R(G/G) \simeq R$. Since factor rings of semisimple rings are themselves semisimple R is as stated. RG being semisimple implies that $\Delta(G,G)$ a direct summand, so by above Lemma the second and third conditions hold.
$\Leftarrow$ assume the three conditions hold and let M be an RG-submodule of RG. Since R is semisimple RG is semisimple as an R-module. Hence, there exists an R-submodule N of RG such that

$$RG = M \oplus N.$$

Let $\pi^* : RG \to M$

$$\pi^*(x) = \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi(gx), \forall x \in RG$$

where π is the canonical projection $\pi : RG \to M$

$$\pi(m+n) = m, m \in M, n \in N, (m+n) \in RG.$$

It will suffice to show that π^* is actually an RG-homomorphism such that $(\pi^*)^2 = \pi^*$ and $Im(\pi^*) = M$, then $Ker(\pi)$ will be an RG-submodule such that $RG = M \oplus Ker(\pi^*)$ and the theorem will be proved.
We can show $\pi*$ is an RG homomorphism by showing that

$$\pi^*(ax) = a\pi^*(x), \forall a \in G$$

We can see that

$$\pi^*(ax) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gax)$$

$$\pi^*(ax) = \frac{a}{|G|} \sum_{g \in G} (ga)^{-1}\pi(gx)$$

Let $ga = t \in G$ then

$$\pi^*(ax) = \frac{a}{|G|} \sum_{t \in G} t^{-1}\pi(tx)$$

By definition $\pi(m) = m$, for all $m \in M$. And since M is an RG-module, we have that $gm \in M$, for all $g \in G$. So

$$\pi^*(m) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gm) = \frac{1}{|G|} \sum_{g \in G} g^{-1}gm = m$$

Given an arbitrary element $x \in RG$, we have that $\pi(gx) \in M$, hence $\pi^*(x) \in M$ and therefore $Im(\pi^*) \subset M$. Consequently, $\pi^*(\pi^*(x)) = \pi^*(x) \forall x \in RG$ and therefore $(\pi^*)^2 = \pi^*$.
Lastly $\pi^*(m) = m, \forall m \in M \Rightarrow M \subset Im(\pi^*)$ □

That covers Mascheke's Theorem. Mascheke's Theorem can be used to analyze the properties of various semisimple group rings. We will however transition into analyzing Integral group rings, which are not semisimple.

5 Integral Group Rings and their Units

Definition 5.1. *An **integral group ring** $RG = \mathbb{Z}G$ is any group ring where the ring is the integers.*

As stated above these groups are not semisimple. We can analyze their structures in other ways. Specifically we can look at units in the group ring. While $\mathbb{Z}$ has only two units, ± 1, $\mathbb{Z}G$ will have more.

Definition 5.2. *Define $U(R)$ as the multiplicative group of units generated by a ring R*

Definition 5.3. ***Trivial Units*** *are units in a group ring of the form rg such that $r \in U(R)$*
Thus in RG $rg \cdot r^{-1}g^{-1} = rr^{-1}gg^{-1} = 1$

Definition 5.4. *Define $U(RG)_1$ as*

$$U(RG)_1 = \{u \in U(RG) : \epsilon(u) = 1\}$$

Proposition 5.5. *Trivial units of $\mathbb{Z}G$ are of the form $\pm g$*

Proof. $r \in U(\mathbb{Z}) = \pm 1$

□

Therefore $U_1(\mathbb{Z}G) = G$ is equivalent to all units of $\mathbb{Z}G$ are trivial.

Definition 5.6. ***Bicyclic Units***
Take a finite order element $a \in G, a \neq 0, |a| = n > 1$, we can construct in $\mathbb{Z}G$ the following zero divisors,
$(a-1)(1 + a + \cdots + a^{n-1}) = 0$,
Denote $\hat{a} = 1 + a + \cdots + a^{n-1}$

Taking any other element $b \in G$ a ***bicyclic unit*** *of $\mathbb{Z}G$ is constructed by $\mu_{a,b} = 1 + (a-1)b\hat{a}$ Notice that*

$$\begin{aligned}(1 + (a-1)b\hat{a})(1 - (a-1)b\hat{a}) \\ = 1 + (a-1)b\hat{a}(a-1)b\hat{a} \\ 1 + (a-1)b0b\hat{a} \\ = 1\end{aligned}$$

Definition 5.7. *Denote B_2 as the subgroup of $U(\mathbb{Z}G)$ generated by all the bicyclic units*

Keep in mind these units aren't always exciting. If a and b commute then $\mu_{a,b} = 1$
We do have to consider the possibility that these units are trivial.

Proposition 5.8. *Let g, h be elements of a group G with $|g|$ is finite. Then, the bicyclic unit $\mu_{g,h}$ is trivial if and only if h normalizes $\langle g \rangle$ In this case we have $\mu_{g,h} = 1$*

Proof. $\Rightarrow$ Assume h is normal in $\langle g \rangle$
then $h^{-1}gh = g^i$, $i \in \mathbb{Z}$.
notice since $g^i\hat{g} = \hat{g}$ we have $gh\hat{g} = hg^i\hat{g} = h\hat{g}$ We can see
$\mu_{g,h} = 1 + (1-g)h\hat{g} = 1 + h\hat{g} - gh\hat{g} = 1 + h\hat{g} - h\hat{g} = 1$
$\Leftarrow$ Assume $\mu_{g,h}$ is trivial.
then $\mu_{g,h} = 1x$ with $x \in G$ so,

$$1 + (1-g)h\hat{g} = x$$

and as a result

$$1 + h(1 + g + g^2 + \cdots g^{n-1}) = x + gh(1 + g + g^2 + \cdots g^{n-1})$$

Case 1: $x = 1$
$\Rightarrow h(1 + g + g^2 + \cdots g^{n-1}) = gh(1 + g + g^2 + \cdots g^{n-1}) \Rightarrow h = ghg^i$
$h^{-1}gh = g^{-i}$
Therefore h normalizes $\langle g \rangle$
Case 2: $x \neq 1$
Then $h \notin \langle g \rangle$. Since 1 is on one side of the equation it must appear on the other side as well.
$\rightarrow \exists i \in \mathbb{Z}$ such that $1 = ghg^i$
$\rightarrow h = g^{-(i+1)}$
$\rightarrow h^{-1}gh = g$
$\rightarrow 1 + (1 - g)h\hat{g} = x = 1$ This is a contradiction. □

Corollary 5.9. *Let G be a finite group. $B_2 = \{1\}$ if and only if every subgroup of G is normal.*

Proposition 5.10. *Every non trivial bicyclic unit of $\mathbb{Z}G$ is of infinite order.*

Proof. Take $\mu_{g,h}$ as above.

$$\mu_{g,h}^s = 1 + s(g - 1)h\hat{g}$$

$$\mu_{g,h}^s - 1 = 1 - 1 + s(g - 1)h\hat{g}$$

If $\mu_{g,h}^s = 1$

$$0 = s(g - 1)h\hat{g}$$

$\Longrightarrow \mu_{g,h} = 1$ □

We will now analyze groups in which every unit is trivial.

Definition 5.11. *A torsion group is a group such that $g \in G \rightarrow |g| < \infty$*

Proposition 5.12. *Let G be a torsion group such that $U_1(\mathbb{Z}G) = G$ Then every subgroup of G is normal.*

Proof. It will suffice to show that every cyclic subgroup of G is normal.
Assume $\exists \langle g \rangle$ which is not normal.
$\rightarrow \exists h \in G$ such that $hgh^{-1} \notin \langle g \rangle$
but then $\mu_{g,h} \neq 1$ and is not trivial. This is a contradiction. □

Therefore every torsion group such that $U_1(\mathbb{Z}G) = G$ is either abelian or Hamiltonian. The question becomes which groups specifically.

Theorem 5.13 (**Higman**). *Let G be a torsion group then $U_1(\mathbb{Z}G) = G$ if and only if G is either an abelian group of exponent equal to 1, 2, 3, 4, or 6. or a Hamiltonian 2-group.*

We will not go into the details of the proof of this result.

Theorem 5.14. *Let $G = \langle g \rangle$ be an infinite cyclic group and let R be a ring with no zero divisors. Then, the units of RG are trivial.*

Proof. Take RG as specified. Suppose u_1 is an invertible element of RG. multiplying u_1 by an appropriate power of g then

$$u = \sum_{i=0}^{s} a_i x^i$$

Let $v \in \langle g \rangle$ be such that $uv = 1$

$$v = \sum_{i=l}^{t} b_i x^i$$

The highest term in uv is $a_s b_t x^{s+t}$ the lowest term is $a_0 b_l x^l$. Since the product is equal to a single term, 1, and R contains no zero divisors, we must have $s + t = 0 = l$ Thus $u = a_0$. We can therefore see that u is trivial, and by extension so is u_1. □

Corollary 5.15. *If G is an infinite cyclic group, then $U_1(\mathbb{Z}G) = G$*

This concludes my analysis of trivial and non-trivial units of Group Rings.

6 Bibliography

- C.P. Milies and S.K. Sehgal, An Introduction to Group Rings. (2002)