SEMIPERFECT AND PERFECT GROUP RINGS

A Thesis Submitted to
the Graduate School of Engineering and Sciences of
İzmir Institute of Technology
in Partial Fulfillment of the Requirements for the Degree of

MASTER OF SCIENCE

in Mathematics

by
Tekgül KALAYCI

June 2014
İZMİR

We approve the thesis of **Tekgül KALAYCI**

Examining Committee Members:

Prof. Dr. Dilek PUSAT
Department of Mathematics, İzmir Institute of Technology

Assoc. Prof. Dr. Noyan Fevzi Er
Department of Mathematics Engineering, Yıldız Technical University

---

Assist. Prof. Dr. Başak AY SAYLAM
Department of Mathematics, İzmir Institute of Technology

24 June 2014

Prof. Dr. Dilek PUSAT
Supervisor, Department of Mathematics
İzmir Institute of Technology

Prof. Dr. Oğuz YILMAZ
Head of the Department of
Mathematics

Prof. Dr. R. Tuğrul SENGER
Dean of the Graduate School of
Engineering and Sciences

ACKNOWLEDGMENTS

I would like to thank to my advisor Prof.Dr.Dilek PUSAT for her supervision, advice and guidance. I also thank to my dear friends, especially Gonca KIZILASLAN, Mehmet YEŞİL and Neslihan GİRGİN for motivating me to complete my thesis. I owe the same amount of thanks to my family for their love and being constantly proud of me without any reason. I feel their eternal love, patience and understanding in every second in my lifelong.

ABSTRACT

SEMIPERFECT AND PERFECT GROUP RINGS

In this thesis, we give a survey of necessary and sufficient conditions on a group G and a ring R for the group ring RG to be semiperfect and perfect. A ring R is called semiperfect $R/\operatorname{Rad} R$ is semisimple and idempotents of $R/\operatorname{Rad} R$ can be lifted to R. It is given that if RG is semiperfect, so is R. Necessary conditions on G for RG to be semiperfect are also given for some special type of groups. For the sufficient conditions, several types of rings and groups are considered. If R is commutative and G is abelian, a complete characterization is given in terms of the polynomial ring $R[X]$.

A ring R is called left (respectively, right) perfect if $R/\operatorname{Rad} R$ is semisimple and $\operatorname{Rad} R$ is left (respectively, right) T-nilpotent. Equivalently, a ring is called left (respectively, right) perfect if R satisfies the descending chain condition on principal right (respectively, left) ideals. By using these equivalent definitions of a perfect ring and results from group theory, a complete characterization of a perfect group ring RG is given in terms of R and G.

ÖZET

YARI MÜKEMMEL VE MÜKEMMEL GRUP HALKALARI ÜZERİNE

Bu tezde G grubu ve R halkası ile kurulan RG grup halkasının yarımükemmel ve mükemmel olması için R ve G üzerinde gerek ve yeter koşullar üzerine bir inceleme yapılmıştır. Bir R halkası için $R/\operatorname{Rad} R$ yarıbasit halkaysa ve $R/\operatorname{Rad} R$ halkasının eşgüçlüleri R halkasına yükseltilebiliyorsa R yarımükemmeldir denir. Eğer RG grup halkası yarı mükemmel ise, R halkası da yarımükemmeldir. RG grup halkasının yarımükemmel olması için G üzerinde gerekli olan koşullar da bazı özel gruplar için verilmiştir. Yeter koşullar için bazı özel halka ve gruplar göz önüne alınmıştır. Eğer R değişmeli bir halka, G de değişmeli bir grupsa $R[X]$ polinom halkası kullanılarak tam bir karakterizasyon verilmiştir.

Bir R halkası için $R/\operatorname{Rad} R$ yarıbasit halkaysa ve $\operatorname{Rad}(R)$ sol (sırasıyla, sağ) T-sıfırgüçlüyse R sol (sırasıyla, sağ) mükemmeldir denir. Denk olarak, bir R halkası için asıl sağ (sırasıyla, sol) idealler üzerinde azalan zincir koşulunu sağlıyorsa sol (sırasıyla, sağ) mükemmeldir denir. Bu denk tanımlar ve gruplar teorisinden bazı sonuçlar kullanılarak mükemmel grup halkaları, R ve G'nin özellikleri cinsinden tam olarak karakterize edilmiştir.

TABLE OF CONTENTS

LIST OF SYMBOLS

R	an associative ring with identity element unless otherwise stated
D	a division ring unless otherwise stated
K	a field unless otherwise stated
G	an arbitrary group unless otherwise stated
$\|G\|$	order of the group G
RG	the group ring of the ring R and the group G
p	an arbitrary prime integer
$\mathbb{Z}$	the ring of integers
$\mathbb{Q}$	the field of rational numbers
$\mathbb{R}$	the field of real numbers
$\mathbb{C}$	the field of complex numbers
$R[X]$	the polynomial ring with coefficients from the ring R
$M_n(R)$	the ring of $n \times n$ matrices entries from the ring R
ωG	the fundamental (augmentation) ideal of the group ring RG
R-module	left R-module
$\mathrm{Hom}_R(M, N)$	all R-module homomorphism from M to N
$\mathrm{Rad}(M)$	the Jacobson radical of the R-module M
$\mathrm{rad}(M)$	the prime radical of R-module M
$\mathrm{Ann}_l(I)$	the left annihilator of an ideal I
$\mathrm{Ann}_r(I)$	the right annihilator of an ideal I
$\mathrm{char}(R)$	the characteristic of the ring R
$\subseteq$	subset
$\subset$	proper subset
$\mathrm{Ker}(f)$	the kernel of the map f
$\mathrm{Im}(f)$	the image of the map f
$\mathrm{End}_R(M)$	the endomorphism ring of a module M
$\overline{R}$	the factor ring $R/\operatorname{Rad} R$

CHAPTER 1

INTRODUCTION

Throughout this thesis, R is an associative ring with unity, G is an arbitrary group and RG is the group ring of G over R. Also all modules are unitary left R-modules unless otherwise indicated.

A ring R is called semiperfect if $R/\operatorname{Rad} R$ is semisimple and idempotents of $R/\operatorname{Rad} R$ can be lifted to R. A ring R is called left (respectively, right) perfect if $R/\operatorname{Rad} R$ is semisimple and $\operatorname{Rad} R$ is left (respectively, right) T-nilpotent. If R is both left and right perfect, we call R a perfect ring. In this thesis, semiperfectness and perfectness of an arbitrary group G over an associative ring R is studied.

In Chapter 2 we mention about some well-known results about groups and rings that will be useful for our work. We also give the definition and main properties of a group ring that will be used in the following chapters. For further information and proofs we refer to (Bland, 2010), (Burnside, 1902), (Connell, 1963), (Golod & Shafarevich, 1964), (Herstein, 2002), (Lam, 1990), (Robinson, 1991).

In Chapter 3 we give some necessary and sufficient conditions on a ring R and on a group G for the group ring RG to be semiperfect. For this purpose, a class of groups is given such that RG is not semiperfect for any ring R if G is in that class. If RG is semiperfect, so is R, thus $\overline{R}$ is the direct product of matrix rings over some division rings. It is indicated that characteristics of these division rings give us a plenty of information about the group G. Later we mention about some special types of groups and rings that gives us a semiperfect group ring. When R is commutative and G is abelian, a complete characterization of a semiperfect group ring RG is given in terms of the polynomial ring $R[X]$. Using this characterization, it is shown by examples that the class of groups G for which RG is semiperfect for an arbitrary ring R is not closed under taking subgroups or direct products in the last section of this chapter.

In Chapter 4 a a complete characterization of perfect group rings is given in terms of R and G. A ring R is called left perfect if it satisfies the descending chain condition on principal right ideals. In this part, by using this definition of a left perfect ring, it is shown that for a group ring RG to be semiperfect, G must be torsion. Then in the abelian case, it is shown that G must be finite. With the further results in this chapter, we see that the group ring RG is perfect if and only if R is perfect and G is finite.

CHAPTER 2

PRELIMINARIES

In this chapter of our study we give fundamental properties of groups, rings and group rings that will be used later.

2.1. Groups

Firstly, we give some necessary properties of groups.

Definition 2.1 *A group G is an Ω-group if for any non-empty finite subsets A and B of G, there exists at least one $x \in G$ which has a unique representation in the form $x = ab$ with $a \in A$ and $b \in B$.*

Definition 2.2 *A group G is an ordered group if it has a linear ordering $<$ such that $x < y$ implies $xz < yz$ for all $z \in G$.*

Example 2.1 *All torsion-free abelian groups are ordered groups. In particular, $\mathbb{Z}$ is an ordered group.*

Let G be an ordered group. Let A and B be two finite subsets of G. If a and b are largest elements of A and B, respectively, and $x = ab \in G$, then there is no other representation for $x = a^{'}b^{'}$, where $a^{'} \in A$ and $b^{'} \in B$. So, every ordered group is an Ω-group.

Definition 2.3 *A group G is called p-group if every element of G has an order a power of p, where p is a prime.*

Definition 2.4 *A group G is called $p^{'}$-group if no element of G has an order divisible by p, where p is a prime.*

Theorem 2.1 ***(First Sylow Theorem)*** *(Robinson, 1991) Let G be a finite group and let $|G| = p^n m$, where $n \geq 1$ and p does not divide m. Then*

(i) G contains a subgroup of order p^i for each i, where $1 \leq i \leq n$.

(ii) Every subgroup H of G of order p^i is a normal subgroup of a subgroup of order p^{i+1} for $1 \leq i \leq n$.

Definition 2.5 *A Sylow p-subgroup of a group G is a maximal p-subgroup of G, that is, a p-subgroup contained in no larger subgroup.*

Now, we will mention about some structural properties of finitely generated abelian groups.

Theorem 2.2 *(Robinson, 1991) If G is a finitely generated abelian group, then G satisfies the maximal condition on subgroups.*

Theorem 2.3 *(Robinson, 1991) If G is an abelian torsion group, then G is finitely generated.*

Theorem 2.4 *(Robinson, 1991) An abelian group G is finitely generated if and only if it is a direct sum of finitely many cyclic groups of infinite or prime-power orders.*

For a group G, it is not always the case that finitely generated subgroups of G are finite. So, the class of groups with this property is of special interest.

Definition 2.6 *A group G is called locally finite if every finitely generated subgroup of G is finite.*

Let G be a locally finite group. Then every finitely generated subgroup of G is finite. In particular, cyclic subgroups of G are finite. This means that G is a torsion group. The following proposition states when the converse holds.

Proposition 2.1 *(Dixon, 1994) Let G be a torsion group. If G is solvable, then G is locally finite.*

Since an abelian group is always solvable, a torsion abelian group is always locally finite by Proposition 2.1. But for an arbitrary group, it was a problem named after Burnside, who first raised it in 1902.

Burnside's Problem: Is a torsion group necessarily locally finite?

This question was answered in the negative by Golod and Shafarevicht in 1964.

Theorem 2.5 ***Golod-Shafarevicht Theorem*** *(Herstein, 2002) Let $A = K[x_1, ..., x_n]$ be the free algebra over a field K in $n = d + 1$ non-commuting variables x_i. Let J be the 2-sided ideal of A generated by homogeneous elements f_j of A of degree d_j with $2 \leq d_1 \leq d_2 \leq \ldots$ where d_j tends to infinity. Let r_i be the number of d_j equal to i. Let $B = A/J$, a graded algebra. Let $bj = \dim Bj$. Then*

(i) $b_j \geq nb_{j-1} - \sum_{i=2}^{j} b_{j-i}r_i$.

(ii) *if $r_i \leq \frac{d^2}{4}$ for all i, then B is infinite-dimensional.*

(iii) *if B is finite-dimensional, then $r_i > \frac{d^2}{4}$ for some i.*

Using Theorem 2.5, one can obtain a finitely generated infinite group as the following theorem states.

Theorem 2.6 *(Herstein, 2002) If p is any prime number, then there exists an infinite group G generated by three elements in which every element has finite order, a power of p.*

Theorem 2.6 gives us a finitely generated and infinite group. With this group, one can construct an infinite dimensional nil algebra, as the following theorem states.

Theorem 2.7 *(Herstein, 2002) If K is a field of characteristic p, then there exists an infinite dimensional nil algebra over K generated by three elements.*

2.2. Semisimple Rings and Modules

Since semisimple rings play an important role in our study, we mention about them in this section.

Definition 2.7 *An R-module M is called left semisimple if it can be written as a direct sum of simple left R-submodules of M.*

In particular, a ring R is called left semisimple if it can be written as a direct sum of simple left ideals.

Proposition 2.2 *(Bland, 2010) Let M be an R-module with the property that every submodule of M is a direct summand of M. Then every submodule of M also has this property.*

Proposition 2.3 *(Bland, 2010) An R-module M is semisimple if and only if every submodule of M is a direct summand of M.*

Now, we will give some characterizations of semisimple rings.

Proposition 2.4 *(Bland, 2010) The following hold for each left semisimple ring R.*

(i) There exist minimal left ideals $A_1, \ldots, A_n$ of R such that

$$R = A_1 \oplus \cdots \oplus A_n.$$

(ii) If $A_1, \ldots A_n$ and $B_1, \ldots B_m$ are minimal left ideals of R such that

$$R = A_1 \oplus \cdots \oplus A_n \text{ and } R = B_1 \oplus \cdots \oplus B_m,$$

then $n = m$ and there is a permutation $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ such that $A_i \cong B_{\sigma(i)}$ for $i = 1, \ldots, n$.

(iii) If $A_1, \ldots, A_n$ is a set of minimal left ideals of R such that

$$R = A_1 \oplus \cdots \oplus A_n,$$

then there is a complete set of orthogonal idempotents of R such that

$$R = Re_1 \oplus \cdots \oplus Re_n$$

and $A_i = Re_i$ for some $i = 1, \ldots, n$. Furthermore, the idempotents $e_1, \ldots, e_n$ are unique.

Lemma 2.1 *(Bland, 2010) Let M and S be R-modules, and suppose that S is simple.*

(i) If $f : S \to M$ is a nonzero R-linear mapping, then f is a monomorphism.

(ii) If $f : M \to S$ is a nonzero R-linear mapping, then f is an epimorphism.

(iii) $\mathrm{End}_R(S)$ is a division ring.

Lemma 2.2 *(Bland, 2010) If R is a left semisimple ring, then there are only a finite number of isomorphism classes of simple R-modules.*

Proposition 2.5 *(Bland, 2010) If S is a simple R-module, then for any positive integer n, $\mathrm{End}_R(S^{(n)})$ is isomorphic to $M_n(D)$, where D is the division ring $\mathrm{End}_R(S)$.*

Definition 2.8 *Let $R = A_1 \oplus \cdots \oplus A_n$ be a decomposition of R, where the A_i are minimal left ideals of R. Arrange the minimal left ideals A_i into isomorphism classes and renumber with double subscripts such that*

$$R = (A_{11} \oplus \cdots \oplus A_{1n_1}) \oplus \cdots \oplus (A_{m1} \oplus \cdots \oplus A_{mn_m}).$$

If $H_i = A_{i1} \oplus \cdots \oplus A_{in_i}$ for $i = 1, \ldots, m$, then $n = n_1 + \cdots + n_m$ and

$$R = H_1 \oplus \cdots \oplus H_m$$

The H_i are said to be the homogeneous components of R.

Proposition 2.6 *(Bland, 2010) The following hold for any left semisimple ring R with decomposition $R = A_1 \oplus \cdots \oplus A_n$ as a direct sum of minimal left ideals.*

(i) The homogeneous components $\{H_i\}_{i=1}^m$ are ideals of R, and there is a complete orthogonal set $\{e_1, \ldots, e_m\}$ of central idempotents of R such that $R = Re_1 \oplus \cdots \oplus Re_m$ and $H_i = Re_i$ for some $i = 1, \ldots, m$.

(ii) $\mathrm{End}_R(H_i)$ *is isomorphic to an* $n_i \times n_i$ *matrix ring with entries from a division ring* D_i *for* $i = 1, \ldots, m$.

Theorem 2.8 *(**Wedderburn-Artin Theorem**) (Bland, 2010) A ring* R *is left semisimple if and only if there exist division rings* $D_1, \ldots, D_m$ *such that* $R \cong M_{n_1}(D_1) \times \cdots \times M_{n_m}(D_m)$.

Theorem 2.9 *(Bland, 2010) A ring* R *is a simple left Artinian ring if and only if there is a division ring* D *such that* $R \cong M_n(D)$ *for some integer* $n \geq 1$.

Corollary 2.1 *A ring* R *is semisimple if and only if* R *is a ring direct product of a finite number of simple Artinian rings.*

Definition 2.9 *Let* R *be a ring. We say that* R *is Jacobson semisimple (*J*-semisimple) if* $\mathrm{Rad}(R) = 0$.

Clearly, a semisimple ring is Jacobson semisimple. But the converse is not true in general.

Definition 2.10 *A ring* R *is called semiprime if its prime radical is zero.*

2.3. The Theory of Idempotents

Proposition 2.7 *(Lam, 1990) Let* e *and* e' *be idempotents and* M *a left* R*-module. There is a natural additive group isomorphism* $\lambda : \mathrm{Hom}_R(Re, M) \to eM$. *In particular, there is a natural group isomorphism* $\mathrm{Hom}(Re, Re') \cong e'Re$.

Corollary 2.2 *(Lam, 1990) For any idempotent* $e \in R$*, there is a natural ring isomorphism* $\mathrm{End}_R(Re) \cong eRe$.

Proposition 2.8 *(Lam, 1990)For any nonzero idempotent* $e \in R$*, the following statements are equivalent:*

(i) Re *is indecomposable as a left* R*-module,*

(ii) eR *is indecomposable as a right* R*-module,*

(iii) *The ring* eRe *has no nontrivial idempotents,*

(iv) e *has no decomposition into* $\alpha + \beta$*, where* α, β *are nonzero orthogonal idempotents in* R.

Definition 2.11 *If a nonzero idempotent* e *satisfies one of the equivalent conditions in Proposition 2.8, then* e *is said to be a primitive idempotent of* R.

Proposition 2.9 *(Lam, 1990)*

For any idempotent $e \in R$, the following statements are equivalent:

(i) Re *is strongly indecomposable as a left R-module,*

(ii) eR *is strongly indecomposable as a right R-module,*

(iii) eRe *is a local ring.*

Definition 2.12 *If an idempotent e satisfies one of the equivalent conditions in Proposition 2.9, then e is said to be a local idempotent of R.*

Clearly, a local idempotent is always a primitive idempotent.

Theorem 2.10 *(Lam, 1990) Let e be an idempotent in R. Then $\mathrm{Rad}(eRe) = \mathrm{Rad}\, R \cap (eRe) = e(\mathrm{Rad}\, R)e$. Moreover, $eRe/\,\mathrm{Rad}(eRe) \cong \overline{e}\overline{R}\overline{e}$, where $\overline{e}$ is the image of e in $\overline{R}$.*

Theorem 2.11 *(Lam, 1990) Let e be an idempotent in R.*

(i) Let I be any left ideal of eRe. Then $RI \cap eRe = I$. In particular, the map from $I \mapsto RI$ defines an injective (inclusion preserving) map from the left ideals of eRe to those of R.

(ii) Let I be an ideal in eRe. Then $e(RIR)e = I$. In particular, the map $I \mapsto RIR$ defines an injective (inclusion preserving) map from ideals of eRe to those of R. This map respects multiplication of ideals, and is surjective if e is a full idempotent, in the sense that $ReR = R$.

Corollary 2.3 *(Lam, 1990) Let e be a nonzero idempotent in R. If R is Jacobson semisimple (respectively, semisimple, simple, prime, semiprime, Noetherian, Artinian), then the same holds for eRe.*

2.4. Regular Rings

We need the definition and properties of regular rings. So, we mention about them in this part.

Definition 2.13 *A ring R is said to be a (von Neumann) regular ring if for each $r \in R$ there exists $s \in R$ such that $rsr = r$.*

Theorem 2.12 *(Lam, 1990) The following are equivalent for a ring R:*

(i) R *is a regular ring,*

(ii) *Every principal left ideal is generated by an idempotent,*

(iii) *Every principal left ideal is a direct summand of R,*

(iv) *Every finitely generated left ideal is a direct summand of R,*

(v) *Every finitely generated left ideal is generated by an idempotent,*

(vi) *Every finitely generated left ideal is a direct summand of R.*

Since the condition given in Definition 2.13 is left-right symmetric, the last four conditions are still valid if we replace the word 'left' by 'right'.

Corollary 2.4 *(Lam, 1990) If R is a semisimple ring, then R is regular.*

Corollary 2.5 *(Lam, 1990) If R is a regular ring, then R is Jacobson semisimple.*

Theorem 2.13 *(Lam, 1990) Semisimple rings are exactly the left (respectively, right) Noetherian regular rings.*

2.5. Semiperfect Rings

Definition 2.14 *A ring R is called semiperfect if $R/\operatorname{Rad} R$ is semisimple and idempotents of $R/\operatorname{Rad} R$ can be lifted to R.*

Proposition 2.10 *(Lam, 1990) The following are equivalent for a ring R:*

(i) *R is semiperfect,*

(ii) *R has a complete set of orthogonal idempotents $\{e_1, \ldots, e_n\}$ such that e_iRe_i is a local ring for $i = 1, \ldots, n$.*

Theorem 2.14 *(Mueller, 1971) The following are equivalent for a ring R:*

(i) *R is semiperfect,*

(ii) *The unit 1 in R is a sum of orthogonal local idempotents,*

(iii) *Every primitive idempotent is local and there is no set of orthogonal idempotents in R.*

Lemma 2.3 *(Mueller, 1971) Let R be a ring, and let $\{e_1, ..., e_n\}$ a set of orthogonal idempotents in R whose sum is 1. Then R is semiperfect if and only if e_iRe_i is semiperfect for each i.*

Theorem 2.15 *(Kaye, 1967) A ring R is semiperfect if and only if $M_n(R)$ is semiperfect.*

Theorem 2.16 *(Lam, 1990) A commutative ring R is semiperfect if and only if it is a finite direct product of commutative local rings.*

2.6. Perfect Rings

Definition 2.15 *A subset S of a ring R is called left (respectively, right) T-nilpotent if, for any sequence of elements $\{a_1, a_2 \ldots\} \subseteq S$, there exists an integer $n \geq 1$ such that $a_1 a_2 \ldots a_n = 0$ (respectively,$a_n \ldots a_2 a_1 = 0$).*

Definition 2.16 *A ring R is called left (respectively, right) perfect if $R/\operatorname{Rad} R$ is semisimple and $\operatorname{Rad} R$ is left (respectively, right) T-nilpotent. If R is both left and right perfect, we call R a perfect ring.*

Proposition 2.11 *(Lam, 1990) The following are equivalent for a ring R:*

(i) *R is a left perfect ring,*

(ii) *$R/\operatorname{Rad} R$ is semisimple and every non-zero R-module contains a maximal submodule.*

Proposition 2.12 *(Lam, 1990) The following are equivalent for a ring R.*

(i) *R is a left perfect ring,*

(ii) *R satisfies the descending chain condition on principal right ideals,*

(iii) *R contains no infinite set of orthogonal idempotents and every non-zero right R- module contains a simple submodule.*

Theorem 2.17 *(Lam, 1990) A commutative ring R is perfect if and only if it is a finite direct product of (commutative) local rings each of which has a T-nilpotent maximal ideal.*

Proposition 2.13 *(Lam, 1990) If a ring R is perfect, then $M_n(R)$ is also perfect.*

2.7. Group Rings

In this section we give the definition of a group ring and mention about basic properties of a group ring that we will use in the following chapters. We denote group identities by 1, we also use 1 for the unit element of the ring R.

2.7.1. Basic Facts

Let G be a group (not necessarily finite) and R a ring. We wish to construct an R-module, having the elements of G as a basis, and then use the operations in both G and R to define a ring structure on it.
To do so, we denote by RG, the set of all formal linear combinations of the form

$$\alpha = \sum_{g \in G} r_g g,$$

where $r_g \in R$ and $r_g = 0$ almost everywhere, that is, only a finite number of coefficients are different from zero in each of these sums.
It follows from the above consideration that, given two elements

$$\alpha = \sum_{g \in G} r_g g \text{ , } \beta = \sum_{g \in G} s_g g,$$

in RG, we have that $\alpha = \beta$ if and only if $r_g = s_g$, for all g in G.
We define the sum of two elements in RG componentwise:

$$\sum_{g \in G} r_g g + \sum_{g \in G} s_g g = \sum_{g \in G} (r_g + s_g) g$$

Also, given two elements $\alpha = \sum_{g \in G} r_g g$ and $\beta = \sum_{h \in G} s_h h$ we define their product by

$$\alpha\beta = \sum_{g,h \in G} (r_g s_h) gh$$

With the operations defined above, RG becomes a ring, which has an identity; namely the element

$$1 = \sum_{g \in G} u_g g,$$

where the coefficient corresponding to the identity element of the group is equal to 1_R and $u_g = 0$ for every other element g of G.

Definition 2.17 *The set RG, with the operations defined above, is called the group ring of G over R. If R is commutative, then RG is called the group algebra of G over R.*

We can also give another definition of a group ring RG. The set of all functions $f : G \to R$ such that $f(g) \neq 0$ for finitely many $g \in G$ with pointwise addition and convolution as multiplication gives us the group ring RG. We will use both of these equivalent definitions.

We have said that given an element $\alpha = \sum_{g \in G} r_g g$ in RG, only finitely many of the r_g's are different from zero. Thus, elements of G that have nonzero coefficient r_g in the expression of $\alpha = \sum_{g \in G} r_g g$ gives us a finite subset of G. This leads to the following definition.

Definition 2.18 *Let G be a group and R a ring. Given an element $\alpha = \sum_{g\in G} r_g g$ in RG, support of α, denoted by $\mathrm{supp}(\alpha)$, is the subset of elements in G that have nonzero coefficient in the expression of α, that is,*

$$\mathrm{supp}(\alpha) = \{g \in G : r_g \neq 0\}.$$

If we look at the equivalent definition of a group ring, we see that a function $f \in RG$ satisfies $f(g) \neq 0$ for only a finitely many elements of RG. The subset of elements in G such that $f(g) \neq 0$ is called support of the function f.

To say that RG is an R-module, we can also define a product of elements in RG by elements $\lambda \in R$ as

$$\lambda(\sum_{g\in G} r_g g) = \sum_{g\in G} (\lambda r_g) g.$$

With this scalar product, RG becomes an R-module.

We can define an embedding $i : G \to RG$ by assigning to each element $x \in G$ the element

$$i(x) = \sum_{g\in G} r_g g$$

where $r_x = 1$ and $r_g = 0$ if g is different from x. We may, thus, regard G as a subset of RG.

We may also consider the mapping $\nu : R \to RG$ given by

$$\nu(r) = \sum_{g\in G} r_g g,$$

where $r_{1_G} = r$ and $r_g = 0$ if g is different from the identity of the group. It is clear that $\nu(r)$ is a ring monomorphism, and thus we can regard R is a subring of RG.

Now, we give a universal property of group rings.

Proposition 2.14 *(Milies & Sehgal, 2002) Let G be a group and R a ring. Given any ring A such that $R \subseteq A$ and any mapping $f : G \to A$ such that $f(gh) = f(g)f(h)$ for $g, h \in G$, there exists a unique ring homomorphism $f^* : RG \to A$ which is R-linear such that $f^* o i = f$, where $i : G \to RG$ is the inclusion given above. That is, the diagram*

$$\begin{tikzcd} G \arrow[r, "i"] \arrow[d, "f"'] & RG \arrow[dl, dashed, "f*"] \\ A & \end{tikzcd}$$

is commutative.

Proof Let $f : G \to A$ be a such map, consider $f^* : RG \to A$ defined by:

$$\sum_{g\in G} r_g g \mapsto \sum_{g\in G} r_g f(g).$$

The proof of the statement is a straightforward computation. □

Corollary 2.6 *(Milies & Sehgal, 2002) Let $f : G \to H$ be a group homomorphism. Then there exists a unique ring homomorphism $f^* : RG \to RH$ such that $f^*(g) = f(g)$ for all g in G. If R is commutative, then f^* is a homomorphism of R-algebras. Moreover, if f is an epimorphism (monomorphism), then f^* is also an epimorphism (monomorphism).*

We remark that if H is the trivial subgroup, then Corollary 2.6 shows that the trivial homomorphism $G \to H$ induces a ring homomorphism $\varepsilon : RG \to R$ such that $\varepsilon(\sum_{g\in G} r_g g) = \sum_{g\in G} r_g$. This homomorphism gives rise to an important ideal of a group ring.

Definition 2.19 *The homomorphism $\varepsilon : RG \to R$ given by*

$$\varepsilon(\sum_{g\in G} r_g g) = \sum_{g\in G} r_g$$

is called the augmentation mapping of RG and its kernel, denoted by ωG, is called the augmentation ideal of RG.

It can be shown that

$$\omega G = \{\sum_{g\in G} r_g(g-1) : g \in G, g \neq 1, r_g \in R\}.$$

Let H be a subgroup of G. Then the subset of RG which is generated by the set $\{h-1 : h \in H\}$ is a left ideal of RG and is denoted by ωH.

Proposition 2.15 *(Milies & Sehgal, 2002) If H is a normal subgroup of G, then ωH is a two sided ideal of RG and*

$$RG/\omega H \cong R(G/H).$$

Proof Suppose H is a normal subgroup of G. Then G/H is a group, and the canonical map $\Pi : G \to G/H$ is a group homomorphism. Thus, Corollary 2.6 implies that $\Pi : G \to G/H$ produces a ring homomorphism Π^* from RG to $R(G/H)$. Now we will show that $\mathrm{Ker}(\Pi^*) = \omega H$.

Let $\tau = \{q_i\}_{i\in I}$ be a complete set of representatives of left cosets of H in G. We can assume that the identity element of G is the representative of coset H in τ. Thus, every element g of G can be written in the form $g = q_i h_j$ with $q_i \in \tau, h_j \in H$.

Let $\alpha = \sum_{g\in G} r_g g$ be an element of RG. Then by the above argument, α can be written in the form $\sum_{i,j} r_{ij} q_i h_j$, where $r_{ij} \in R$, $q_i \in \tau$, $h_j \in H$. Now we consider $\Pi^*(\alpha) = \sum_i \sum_j r_{ij} q_i h_j H = \sum_i (\sum_j r_{ij}) q_i H$. Then $\alpha \in \mathrm{Ker}(\Pi^*)$ if and only if $\sum_j r_{ij} = 0$ for each value of i. So, if $\alpha \in \mathrm{Ker}(\Pi^*)$, we can write

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

Thus $\mathrm{Ker}(\Pi^*)\subseteq\omega H$. The other containment is clear. Thus, $\mathrm{Ker}(\Pi^*)=\omega H$. So, ωH is a two sided ideal of RG. Since Π is an epimorphism, so is Π^* by Corollary 2.6. Thus by First Isomorphism Theorem, we have $RG/\omega H\cong R(G/H)$. □

Since a group G is always normal in G, by using Corollary 2.6, we get:

$$RG/\omega G\cong R.$$

Proposition 2.16 *(Milies & Sehgal, 2002) If I is an ideal of R, IG, which consists of the elements of RG with coefficients in I, is an ideal of RG and*

$$RG/IG\cong(R/I)G.$$

Proof Consider the map $f:RG\to(R/I)G$ such that $f(\sum_{g\in G}r_gg)=\sum_{g\in G}(r_g+I)g$. It can be shown that f is an epimorphism with kernel IG, thus by First Isomorphism Theorem, the result follows. □

Proposition 2.17 *(Milies & Sehgal, 2002) Let $f:R\to S$ be a homomorphism of rings and let G be a group. Then the map $f^*:RG\to SG$ such that $f(\sum_{g\in G}r_gg)=\sum_{g\in G}f(r_g)g$ is a ring homomorphism. Furthermore, f is a monomorphism (epimorphism) if and only if f^* is a monomorphism (epimorphism).*

Proposition 2.18 *(Milies & Sehgal, 2002) Let R be a commutative ring and let G,H be groups. Then $R(G\times H)\cong(RG)H$.*

Proof Let $f:(RG)H\to R(G\times H)$ such that

$$f(\sum_{h\in H}(\sum_{g\in G}r_{gh}g)h)=\sum_{(g,h)\in G\times H}r_{gh}(g,h).$$

Then f is an isomorphism. □

Proposition 2.19 *(Milies & Sehgal, 2002) For a ring R and a group G, $M_n(R)G\cong M_n(RG)$.*

Proof Let $f:M_n(R)G\to M_n(RG)$ such that,

$$f(A_1g_1+\cdots+A_sg_s)=(b_{ij}),$$

where $b_{ij}=a^1_{ij}g_1+\cdots+a^s_{ij}g_s$ and a^m_{ij} is the entry in the i^{th} row and j^{th} column of A_m, $m=1,\ldots,s$. Then f is an isomorphism. □

Proposition 2.20 *(Milies & Sehgal, 2002) Let $\{R_i\}_{i\in I}$ be a family of rings and let $R = \bigoplus_{i\in I} R_i$. Then for any group G, $RG \cong \bigoplus_{i\in I} R_iG$.*

Proposition 2.21 *(Milies & Sehgal, 2002) Let G be a group and H a subgroup of G. Let $\{h_i\}_{i\in I}$ be a complete set of representatives of left cosets of H in G. Then for any ring R, the group ring RG is a free left RH-module with the basis $\{h_i\}_{i\in I}$.*

Definition 2.20 *Let X be a subset of a group ring RG. The left annihilator of X is the set*

$$\mathrm{Ann}_l(X) = \{\alpha \in RG : \alpha x = 0 \textit{ for every } x \in X\}.$$

Similarly, we define the right annihilator of X by:

$$\mathrm{Ann}_r(X) = \{\alpha \in RG : x\alpha = 0 \textit{ for every } x \in X\}.$$

Definition 2.21 *Given a group ring RG and a finite subset X of the group G, we shall denote by $\widetilde{X}$ the following element of RG :*

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

Lemma 2.4 *(Milies & Sehgal, 2002) Let H be a subgroup of a group G and let R be a ring. Then $\mathrm{Ann}_r(wH) \neq 0$ if and only if H is finite. In this case, we have*

$$\mathrm{Ann}_r(wH) = \widetilde{H}.RG.$$

Furthermore, if H is a normal subgroup of G, then the element $\widetilde{H}$ is central in RG and we have

$$\mathrm{Ann}_r(wH) = \mathrm{Ann}_l(wH) = RG.\widetilde{H}.$$

Proof Assume that $\mathrm{Ann}_r(wH) \neq 0$, and choose a nonzero $\alpha = \sum_{g\in G} r_g g$ in $\mathrm{Ann}_r(wH)$. For each element $h \in H$, we have that $(h-1)\alpha = 0$, and hence $h\alpha = \alpha$, that is,

$$\alpha = \sum_{g\in G} r_g g = \sum_{g\in G} r_g (hg).$$

Take $g_0 \in \mathrm{supp}(\alpha)$. Then r_{g_0} is nonzero, so, the equation above shows that $hg_0 \in \mathrm{supp}(\alpha)$ for all $h \in H$. Since $\mathrm{supp}(\alpha)$ is finite, this clearly implies that H must be finite.

Notice that the above argument shows that, whenever $g_0 \in \mathrm{supp}(\alpha)$, then the coefficient of every element of the form hg_0 is equal to the coefficient of g_0, so we can write α in the form:

$$\alpha = r_{g_0}\widetilde{H}g_0 + r_{g_1}\widetilde{H}g_1 + \cdots + r_{g_t}\widetilde{H}g_t = \widetilde{H}\beta, \quad \text{where} \beta \in RG$$

This shows that if H is finite, then $\mathrm{Ann}_r(wH) \subseteq \widetilde{H}.RG$.

The reverse inclusion follows trivially, since $h\widetilde{H} = \widetilde{H}$ implies that $(h-1)\widetilde{H} = 0$ for all $h \in H$.

Finally, if H is a normal subgroup of G, for any $g \in G$ we have that $g^{-1}Hg = H$; therefore

$$g^{-1}\widetilde{H}g = \sum_{h\in H} g^{-1}hg = \sum_{h\in H} h = \widetilde{H}.$$

Thus, $\widetilde{H}g = g\widetilde{H}$ for all $g \in G$, which shows $\widetilde{H}$ is central in RG. Consequently, $RG.\widetilde{H} = \widetilde{H}.RG$, and the result follows. ☐

Corollary 2.7 *(Milies & Sehgal, 2002) Let G be a finite group. Then*

(i) $\mathrm{Ann}_l(wG) = \mathrm{Ann}_r(wG) = R\widetilde{G}$*, and*

(ii) $\mathrm{Ann}_r(wG) \cap wG = \{r\widetilde{G} : r \in R,\ r|G| = 0\}$.

Proof Statement (i) follows from Lemma 2.4 taking $H = G$.
For statement (ii) note that $\alpha = r\widetilde{G} \in wG$ if and only if $\varepsilon(\alpha) = r\varepsilon(\widetilde{G}) = r|G| = 0$. ☐

Our next result is an elementary remark from ring theory which will be necessary for the main theorem of this section.

Lemma 2.5 *(Milies & Sehgal, 2002) Let I be a two sided ideal of of a ring R. Suppose that there exists a left ideal J such that $R = I \oplus J$ as left R- modules. Then $J \subseteq \mathrm{Ann}_r(I)$.*

Lemma 2.6 *(Milies & Sehgal, 2002) If the augmentation ideal wG is a direct summand of RG as an RG- module, then G is finite and $|G|$ is invertible in R.*

Proof Assume that wG is a direct summand of RG. Then, Lemma 2.4 shows that $\mathrm{Ann}_r(wG)$ is nonzero, and thus G is finite and $\mathrm{Ann}_r(wG) = \widetilde{G}(RG) = \widetilde{G}R$.
If $RG = wG \oplus J$ and $1 = e_1 + e_2$ with $e_1 \in wG$ and $e_2 \in J$, then $1 = \varepsilon(1) = \varepsilon(e_1) + \varepsilon(e_2)$ since $e_2 = r\widetilde{G}$ for some $r \in R$, we have that $r\varepsilon(\widetilde{G}) = 1$; thus $r|G| = 1$. This shows that $|G|$ is invertible in R and that $|G|^{-1} = r$. ☐

The next result is the main theorem of this chapter since it characterizes semisimple group rings in terms of the properties of R and G.

Theorem 2.18 ***(Maschke's Theorem)*** *(Milies & Sehgal, 2002) Let G be a group. Then the group ring RG is semisimple if and only if the following conditions hold.*

(i) R is a semisimple ring.

(ii) G is finite.

(iii) The order of G is a unit in R.

Proof Assume RG is semisimple. We know that $RG/wG \cong R$. Since homomorphic images of semisimple rings are semisimple, R is semisimple.
Semisimplicity of RG implies that wG is a direct summand. By Lemma 2.6, we can say that G is finite and the order of G is a unit in R.

Conversely, assume these three conditions hold. Let M be an RG-submodule of RG. Since R is semisimple, it follows that RG is semisimple as an R-module. Hence there exists an R-submodule N of RG such that $RG = M \oplus N$. Let $\Pi : RG \to M$ be the canonical projection associated to the direct sum. We define $\Pi^* : RG \to M$ by an averaging process, that is,

$$\Pi^*(x) = \frac{1}{|G|}\sum_{g\in G} g^{-1}\Pi(gx)$$

for all $x \in RG$. If we prove that Π^* is actually an RG homomorphism such that $(\Pi^*)^2 = \Pi^*$ and $\mathrm{Im}(\Pi^*) = M$, then $\mathrm{Ker}(\Pi^*)$ will be an RG-submodule such that $RG = M \oplus \mathrm{Ker}(\Pi^*)$, and the theorem will be proved.

Since Π^* is an R homomorphism, in order to show that it is also an RG homomorphism, it will suffice to show $\Pi^*(ax) = a\Pi^*(x)$, for all $a, x \in G$.

We have

$$\Pi^*(ax) = \frac{1}{|G|}\sum_{g\in G} g^{-1}\Pi(gax) = \frac{a}{|G|}\sum_{g\in G}(ga)^{-1}\Pi((ga)x).$$

When g runs over all elements in G, the product ga also runs over all elements in G, thus

$$\Pi^*(ax) = a\frac{1}{|G|}\sum_{h\in G} h^{-1}\Pi(hx) = a\Pi^*(x).$$

Since Π is a projection on M, we know that $\Pi(m) = m$ for all $m \in M$. Also since M is an RG module, we have that $gm \in M$ for all $g \in G$. Thus,

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

Given an arbitrary element $x \in RG$, we have that $\Pi(gx) \in M$, hence $\Pi^*(x) \in M$. It follows that $\mathrm{Im}(\Pi^*) \subset M$. Consequently, $\Pi^*(\Pi^*(x)) = \Pi^*(x)$ for all $x \in RG$, and therefore $(\Pi^*)^2 = \Pi^*$. Finally, the fact that $\Pi^*(m) = m$ also shows that $M \subset \mathrm{Im}(\Pi^*)$, and the theorem follows. □

The case where $R = K$ is a field is of particular importance.

Corollary 2.8 *(Milies & Sehgal, 2002) Let G be a finite group and K a field. Then KG is semisimple if and only if $\mathrm{char}(K) \nmid |G|$.*

A translation of the Wedderburn-Artin Theorem will give us a plenty information about the structure of a group algebra.

Theorem 2.19 *(Milies & Sehgal, 2002) Let G be a finite group and K a field such that $\mathrm{char}(K) \nmid |G|$. Then*

(i) *KG is a direct sum of finite number of two sided ideals $\{B_i\}_{1 \leq i \leq r}$, the simple components of KG. Each B_i is a simple ring.*

(ii) *Any two sided ideal of KG is a direct sum of some of the members of the family $B_i, 1 \leq i \leq r$.*

(iii) *Each simple component B_i is isomorphic to a full matrix ring of the form $M_{n_i}(D_i)$, where D_i is a division ring containing an isomorphic copy of K in its center, and the isomorphism*

$$KG \cong \bigoplus_{i=1}^{r} M_{n_i}(D_i)$$

is an isomorphism of K algebras.

(iv) *In each matrix ring $M_{n_i}(D_i)$, the set*

$$I_i = \{ \begin{pmatrix} x_1 & 0 & \dots & 0 \\ x_2 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ x_{n_i} & 0 & \dots & 0 \end{pmatrix} : x_1, x_2, \dots x_{n_i} \} \cong D_i^{n_i}$$

is a minimal left ideal.

(v) *$I_i \ncong I_j$, if $i \neq j$.*

(vi) *Any simple KG- module is isomorphic to some I_i, $1 \leq i \leq r$.*

Corollary 2.9 *(Milies & Sehgal, 2002) Let G be a finite group and let K be an algebraically closed field such that $\mathrm{char}(K) \nmid |G|$. Then*

$$KG \cong \bigoplus_{i=1}^{r} M_{n_i}(K)$$

and $(n_1)^2 + (n_2)^2 + \cdots + (n_r)^2 = |G|$.

Proof Since $\mathrm{char}(K) \nmid |G|$, we have that

$$KG \cong \bigoplus_{i=1}^{r} M_{n_i}(D_i),$$

where D_i is a division ring containing an isomorphic copy of K in its center. If we compute dimensions over K on both sides of the equation we have that

$$|G| = \sum_{i=1}^{r} n_i^2 [D_i : K],$$

and it follows that each division ring is finite dimensional over K. As K is algebraically closed, we have that $D_i = K$, $1 \leq i \leq r$, and the result follows. $\square$

Now we give a complete description of the group ring of a finite abelian group G over a field K such that $\mathrm{char}(K) \nmid |G|$. But first we will state some results from field theory which will be useful for us.

Definition 2.22 *A nonzero polynomial $f(x) \in K[X]$ is called separable when it has distinct roots in a splitting field over K, that is, each root of $f(x)$ has multiplicity 1. If $f(x)$ has a multiple root, then $f(x)$ is called inseparable.*

Definition 2.23 *If α is algebraic over K, it is called separable over K when its minimal polynomial in $K[X]$ is separable, that is, the minimal polynomial of α in $K[X]$ has distinct roots in a splitting field over K. If the minimal polynomial of α in $K[X]$ is inseparable, then α is called inseparable over K.*

Theorem 2.20 *(Lang, 2000) A nonzero polynomial in $K[X]$ is separable if and only if it is relatively prime to its derivative in $K[X]$.*

Theorem 2.21 ***(Primitive Element Theorem)** (Lang, 2000) Let E be a finite separable extension of a field K. Then there exists $\alpha \in E$ such that $K = K(\alpha)$.*

Theorem 2.22 ***(Chinese Remainder Theorem)** (Lang, 2000) Let R be a principal ideal domain. If $u_1, \ldots, u_n$ are elements of R which are pairwise coprime and $u = u_1 u_2 \ldots u_n$ then*

$$R/Ru \cong R/Ru_1 \times \cdots \times R/Ru_n.$$

Definition 2.24 *For any field K, a field $K(\zeta_n)$ where ζ_n is a root of unity of order n is called a cyclotomic extension of K.*

We shall begin with the case where G is cyclic, so we assume $G =< a : a^n = 1 >$ and that K is a field such that $\mathrm{char}(K) \nmid |G|$. Consider the map $\phi : K[X] \to KG$ given by $f \mapsto f(a)$ for all $f \in K[X]$. It is easily seen that ϕ is a ring epimorphism. Hence,

$$KG \cong \frac{K[X]}{\mathrm{Ker}(\phi)}.$$

Since $K[X]$ is a principal ideal domain, $\mathrm{Ker}(\phi)$ is the ideal generated by the monic polynomial f_0 of least degree such that $f_0(a) = 0$. Since $a^n = 1$, it follows that
$x^n - 1 \in \mathrm{Ker}(\phi)$. Note that if $f = \sum_{i=1}^{r} k_i x^i$ is a polynomial of degree $r < n$, we have that $f(a) = \sum_{i=1}^{r} k_i a^i \neq 0$ because the elements $\{1, a, a^2, \ldots, a^r\}$ are linearly independent over K. Thus $\mathrm{Ker}(\phi) =< x^n - 1 >$ so that

$$KG \cong \frac{K[X]}{< x^n - 1 >}.$$

Let $x^n - 1 = f_1 f_2 ... f_t$ be the decomposition of $x^n - 1$ as a product of irreducible polynomials in $K[X]$. Since we assume that $\mathrm{char}(K) \nmid n$, this polynomial is separable by Theorem 2.20 and thus, $f_i \neq f_j$ if $i \neq j$. Using Chinese Remainder Theorem, we can write

$$KG \cong \frac{K[X]}{< f_1 >} \oplus \frac{K[X]}{< f_2 >} \oplus \cdots \oplus \frac{K[X]}{< f_t >}.$$

Under this isomorphism, the generator a is mapped to the element $(x+ < f_1 >, \ldots, x+ < f_t >)$. Then we have that $\dfrac{K[X]}{< f_i >} \cong K(\zeta_i)$. Consequently,

$$KG \cong K(\zeta_1) \oplus K(\zeta_2) \oplus \cdots \oplus K(\zeta_t).$$

Since all the elements ζ_i ($1 \leq i \leq t$), are roots of $x^n - 1$, we have shown that KG is isomorphic to a direct sum of cyclotomic extensions of K. Under this isomorphism, the element a maps to the element $(\zeta_1, \zeta_2, \ldots, \zeta_t.)$

Example 2.2 *Let $G =< a : a^7 = 1 >$ and $K = \mathbb{Q}$. In this case the decomposition of $x^7 - 1$ in $\mathbb{Q}[X]$ is*

$$x^7 - 1 = (x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1).$$

Hence if ζ denotes a primitive root of unity of order 7, we have

$$\mathbb{Q}G \cong \mathbb{Q} \oplus \mathbb{Q}(\zeta).$$

Example 2.3 *Let $G =< a : a^6 = 1 >$ and $K = \mathbb{Q}$. The decomposition of $x^6 - 1$ as a product of irreducible polynomials in $\mathbb{Q}$ is*

$$x^6 - 1 = (x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1)$$

Thus

$$\mathbb{Q}G \cong \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}(\tfrac{-1+i\sqrt{3}}{2}) \oplus \mathbb{Q}(\tfrac{1+i\sqrt{3}}{2}).$$

Here $\frac{-1+i\sqrt{3}}{2}$ is root of $x^2 + x + 1$ and $\frac{1+i\sqrt{3}}{2}$ is a root of $x^2 - x + 1$. Note that the last two summands are equal.

We wish to give a more precise description of KG in the general case. In order to do this we shall try to calculate all the direct summands in the decomposition of KG. We recall that, for a positive integer d, the cyclotomic polynomial of order d, denoted by Φ_d, is the product $\Phi_d = \prod_j (x - \zeta_i)$, where ζ_i runs over all the primitive d^{th} root of unity. Also, we know that $x^n - 1 = \prod_{d|n} \Phi_d$, the product of all cyclotomic polynomials Φ_d in $K[X]$, where d is a divisor of n. For each d, let $\Phi_d = \prod_{i=1}^{a_d} f_{d_i}$ be the decomposition of Φ_d as a product of irreducible polynomials in $K[X]$. Then the decomposition of KG can actually be written in the form:

$$KG \cong \bigoplus_{d|n} \bigoplus_{i=1}^{a_d} \frac{K[X]}{< f_{d_i} >} \cong \bigoplus_{i=1}^{a_d} K(\zeta_{d_i})$$

where ζ_{d_i} denotes a root of f_{d_i}, $1 \leq i \leq a_d$. For a fixed d, all the elements ζ_{d_i} are primitive d^{th} roots of unity. Therefore, all the fields of the form $K(\zeta_{d_i})$, $1 \leq i \leq a_d$ are equal to one another, and we may write

$$KG \cong \bigoplus_{d|n} a_d K(\zeta_d),$$

where ζ_d is a primitive root of unity of order d and $a_d K(\zeta_d)$ denotes the direct sum of a_d different fields, all of which are isomorphic to $K(\zeta_d)$. Also, since $\deg(f_{d_i}) = [K(\zeta_d) : K]$, we see that all the polynomials f_{d_i}, where $1 \leq i \leq a_d$, have the same degree. Thus taking degrees in the decomposition of Φ_d, we get

$$\Phi(d) = a_d[K(\zeta_d) : K],$$

where Φ denotes Euler's totient function, namely

$$\Phi(d) = \{n \in \mathbb{Z} : 1 \geq n \geq d, \gcd(n, d) = 1\}.$$

Since G is a cyclic group of order n, for each divisor d of n, the number of elements of order d in G, which we denote by n_d, is precisely $\Phi(d)$. Hence, we can write
$a_d = \frac{n_d}{[K(\zeta_d):K]}$.

Example 2.4 *Let $G =< a : a^n = 1 >$ be a cyclic group of order n and take $K = \mathbb{Q}$. It is well-known that the polynomial $x^n - 1$ decomposes in $\mathbb{Q}[X]$ as a product of cyclotomic polynomials*

$$x^n - 1 = \prod_{d|n} \Phi_d(x),$$

and these are irreducible. Hence, in this case, the decomposition of $\mathbb{Q} < g >$ is

$$\mathbb{Q} < g > \cong \bigoplus_{d|n} \mathbb{Q}(\zeta_d).$$

Notice that as before in this isomorphism the generator a corresponds to the tuple whose entries are the primitive d^{th} roots of unity, where d runs over all divisors of n.

The description obtained above can be extended to group rings of arbitrary finite abelian groups.

Theorem 2.23 *(Milies & Sehgal, 2002) Let G be a finite abelian group of order n, let K be a field such that $\mathrm{char}(K) \nmid n$. Then*

$$KG \cong \bigoplus_{d|n} a_d K(\zeta_d),$$

where ζ_d denotes a primitive root of unity of order d and $a_d = \frac{n_d}{[K(\zeta_d):K]}$. In this formula, n_d denotes the number of elements of order d in G.

Proof We proceed by induction on n. Suppose the result holds for all abelian groups of order less than n. Let G be a finite group of order n. If G is cyclic, we have already shown that the theorem is valid. Otherwise, we can use the structure theorem of finite abelian groups to write $G \cong G_1 \times H$, where H is cyclic and $|G_1| = n_1 < n$. By the induction hypothesis, we can write $KG_1 \cong \bigoplus_{d_1|n_1} a_{d_1} K(\zeta_{d_1})$, where $a_{d_1} = \frac{n_{d_1}}{[K(\zeta_{d_1}):K]}$ and n_{d_1} denotes the number of elements of order d_1 in G_1. Therefore, we have

$$KG = K(G_1 \times H) \cong (KG_1)H \cong (\bigoplus_{d_1|n_1} a_{d_1} K(\zeta_{d_1}))H \cong \bigoplus_{d_1|n_1} a_{d_1} K(\zeta_{d_1})H.$$

Now, decomposing each direct summand, we get

$$KG \cong \bigoplus_{d_1|n_1} \bigoplus_{d_2||H|} a_{d_1} a_{d_2} K(\zeta_{d_1}, \zeta_{d_2}),$$

where $a_{d_2} = \frac{n_{d_2}}{[K(\zeta_{d_1},\zeta_{d_2}):K(\zeta_{d_1})]}$ and n_{d_2} denotes the number of elements of order d_2 in H. If we set $d = \mathrm{lcm}(d_1, d_2)$, we have that $K(\zeta_{d_1}, \zeta_{d_2}) = K(\zeta_d)$. Thus,

$$KG \cong \bigoplus_{d|n} a_d K(\zeta_d)$$

with $a_d = \sum a_{d_1} a_{d_2}$, where the sum is taken over all pairs d_1, d_2 such that $\mathrm{lcm}(d_1, d_2) = d$. Since $[K(\zeta_d) : K] = [K(\zeta_{d_1}, \zeta_{d_2}) : K(\zeta_{d_1})][K(\zeta_{d_1}) : K]$, we have that

$$a_d[K(\zeta_{d_1}) : K] = \sum_{d_1,d_2} a_{d_1} a_{d_2} [K(\zeta_{d_1}, \zeta_{d_2}) : K(\zeta_{d_1})][K(\zeta_{d_1}) : K] = \sum_{d_1,d_2} n_{d_1} n_{d_2}.$$

Finally, we notice that since $G \cong G_1 \times H$, each element can be written in the form $g = g_1 h$, with $g_1 \in G_1$ and $h \in H$. Also, it is easy to see that $o(g) = \mathrm{lcm}(o(g_1), o(h))$. Hence, $\sum_{d_1,d_2} n_{d_1}, n_{d_2} = n_d$, the number of elements of order d in G, so that we have

$$a_d = \frac{n_d}{[K(\zeta_d) : K]},$$

and the result follows. □

Corollary 2.10 *(Milies & Sehgal, 2002) Let G be an abelian group of order n and K be a field such that $\mathrm{char}(K) \nmid n$. If K contains a primitive root of unity of order n, then KG is isomorphic to direct sum of n copies of K. That is,*

$$KG \cong K \oplus \cdots \oplus K,$$

where the sum occurs $n-1$ times.

Proof If K contains a primitive root of unity of order n, then $K(\zeta_d) = K$, for all $d|n$, and the corollary follows directly from Theorem 2.23 (to see that there must occur exactly n summands it suffices to compute the dimensions over K on both sides of the equation). $\square$

If G and H are isomorphic groups, universal property gives that the group rings RG and RH are isomorphic. However, the converse is not true. We can give a counter example using this Corollary 2.10.

Suppose G and H are non-isomorphic abelian groups of the same order n and K is a field such that $\mathrm{char}(K) \nmid n$ and contains a primitive root of unity of order n. Then Corollary 2.10 shows that

$$KG \cong K \oplus \cdots \oplus K \cong KH,$$

where the sum occurs $n-1$ times.

For example if C_2 and C_4 denote the cyclic groups of order 2 and 4, respectively, then for the complex group algebras we have:

$$\mathbb{C}(C_2 \times C_2) \cong \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \cong \mathbb{C}C_4.$$

Information about the idempotents in a group ring will be helpful for our aim, so we mention about them in the next part of this section.

Lemma 2.7 *(Milies & Sehgal, 2002) Let R be a ring and H be a subgroup of a group G. If $|H|$ is invertible in R, then $e_H = \dfrac{1}{\widetilde{H}}$ is an idempotent of RG. Moreover, if H is a normal subgroup of G, then e_H is central.*

Proof First we prove e_H is an idempotent.

$$\begin{aligned} e_H e_H = \frac{1}{|H|^2}\widetilde{H}\widetilde{H} &= \frac{1}{|H|^2}(\sum_{h\in H} h)\widetilde{H} \\ &= \frac{1}{|H|^2}\sum_{h\in H}(h\widetilde{H}) \\ &= \frac{1}{|H|^2}\sum_{h\in H}\widetilde{H} \\ &= \frac{1}{|H|^2}|H|\widetilde{H} = e_H. \end{aligned}$$

$\square$

We already know from Lemma 2.4 that if H is a normal subgroup of G, then $\widetilde{H}$ is central. So, centrality of e_H follows immediately. Our next result will tell us what the decomposition obtained from one of these idempotents looks like.

Proposition 2.22 *(Milies & Sehgal, 2002) Let R be a ring, and H a normal subgroup of a group G. If $|H|$ is invertible in R, setting $e_H = \frac{1}{|H|}\widetilde{H}$, we have a direct sum of rings*

$$RG = RGe_H \oplus RG(1 - e_H),$$

where $RGe_H \cong R(G/H)$ and $RG(1 - e_H) = \omega H$.

Proof We have shown that e_H is a central idempotent. Thus,

$$RG = RGe_H \oplus RG(1 - e_H).$$

is a valid decomposition. To see that $R(G/H) \cong RGe_H$, we shall first show that $G/H \cong Ge_H$ as groups. The map $\phi : G \to Ge_H$ such that $g \mapsto ge_H$ is a group epimorphism. Clearly, $\mathrm{Ker}(\phi) = H$. As Ge_H is a basis of RGe_H over R, we already have $RGe_H \cong R(G/H)$.

Finally, it follows from Lemma 2.4 that $RG(1 - e_H)$ is an annihilator of RGe_H and it can be easily shown that $\mathrm{Ann}(RGe_H) = \omega H$. $\square$

Definition 2.25 *Let R be a ring and G a finite group such that $|G|$ is invertible in R. The idempotent $e_G = \frac{1}{|G|}\widetilde{G}$ is called the principal idempotent of RG.*

For a group ring RG, we can use the principal idempotent of RG and obtain a decomposition given in the next theorem by Proposition 2.22.

Corollary 2.11 *(Milies & Sehgal, 2002) Let R be a ring and G a finite group such that $|G|$ is invertible in R. Then we can write RG as a direct sum of rings*

$$RG \cong R \oplus \omega G.$$

2.7.2. Chain Conditions

In this part of our study, we give necessary and sufficient conditions on R and G for the group ring RG to have some chain conditions.

Theorem 2.24 *(Connell, 1963) RG is Artinian if and only if R is Artinian and G is finite.*

Theorem 2.25 *(Connell, 1963) If R is Noetherian and G is finite, then RG is Noetherian.*

Theorem 2.26 *(Connell, 1963) If RG is Noetherian, then R is Noetherian and G has the maximum condition on subgroups.*

2.7.3. Regularity

The following theorem completely characterizes regular group rings.

Theorem 2.27 *(Connell, 1963) RG is regular if and only if*

(i) R is a regular ring.

(ii) G is locally finite.

(iii) The order of every subgroup of G is a unit in R.

2.7.4. On the Radicals

This part of this section contains some special cases about the Jacobson radical and the prime ideal of a group ring RG.

Proposition 2.23 *(Connell, 1963) Let H be a subgroup of G. Then $RH \cap \mathrm{Rad}(RG) \subseteq \mathrm{Rad}(RH)$.*

If we let H to be the trivial subgroup of G, we have the following corollary.

Corollary 2.12 *(Connell, 1963) Let H be the trivial subgroup of G. Then $R \cap \mathrm{Rad}(RG) \subseteq \mathrm{Rad}(R)$ with equality if R is Artinian or G is locally finite.*

Proposition 2.24 *(Connell, 1963) Let R be a commutative ring and and G an abelian group. If $\mathrm{Rad}(R) = 0$ and the order of every element $g \in G$ is regular in R, then $\mathrm{Rad}(RG) = 0$.*

Proposition 2.25 *(Connell, 1963) RG is semiprime if and only if R is semiprime and G has no finite normal subgroups whose orders are zero divisors in R.*

2.7.5. Properties of the Fundamental Ideal

This part of this section contains some special cases about the fundamental ideal of a group ring RG that will be useful.

Proposition 2.26 *(Connell, 1963) If $\omega G \subseteq \mathrm{Rad}(RG)$, then G is a p-group and $p \in \mathrm{Rad}\, R$.*

Proposition 2.27 *(Connell, 1963) If ωG is nil, then G is a p-group and $p \in \mathrm{rad}\, R$.*

Theorem 2.28 *(Connell, 1963) ωG is nilpotent if and only if G is a finite p-group and p is nilpotent in R.*

Corollary 2.13 *(Connell, 1963) ωG is locally nilpotent if and only if G is a locally finite p-group and p is nilpotent in R.*

Proposition 2.28 *(Connell, 1963) If ωG is a nil ideal, then G is a p-group and p is nilpotent in R.*

Proposition 2.29 *(Connell, 1963) If G is a locally finite p-group and p is nilpotent in R, then ωG is a nil ideal.*

Proposition 2.30 *(Connell, 1963) If $\mathrm{Rad}(RG) = \omega G$, then G is a p-group, $\mathrm{Rad}(R) = 0$ and $p = 0$ in R.*

Proposition 2.31 *(Connell, 1963) If G is a locally finite p-group, $\mathrm{Rad}\, R = 0$ and $p = 0$ in R, then $\mathrm{Rad}(RG) = \omega G$.*

CHAPTER 3

SEMIPERFECT GROUP RINGS

In this chapter we give some necessary and sufficient conditions on a ring R and a group G for the group ring RG to be semiperfect.

3.1. Some Necessary Conditions

Proposition 3.1 *(Burgess, 1969) If RG is semiperfect, so is R, and so is DG for each division ring D appearing in the factors of $R/\operatorname{Rad} R$.*

Proof Suppose RG is semiperfect. Then since $RG/\omega G \cong R$, we have R is semiperfect. R is semiperfect means that $R/\operatorname{Rad}(R)$ is semisimple. By Wedderburn-Artin Theorem, $R/\operatorname{Rad}(R)$ is a direct product of matrix rings over division rings. That is,

$$R/\operatorname{Rad}(R) \cong M_n(D_1) \times M_n(D_2) \times \cdots \times M_n(D_k),$$

where $D_1, \ldots, D_k$ are division rings. We know that homomorphic images of semiperfect rings are semiperfect. Thus, here $M_n(D_i)G$ is semiperfect since

$$\frac{\overline{R}G}{(M_n(D_1) \times \cdots \times M_n(D_{i-1}) \times M_n(D_{i+1}) \times \cdots \times M_n(D_k))G} \cong (M_n(D_i))G$$

By Proposition 2.19, $M_n(R)G \cong M_n(RG)$. Thus $M_n(RG)$ is semiperfect for $1 \leq i \leq k$. By Theorem 2.15, DG is semiperfect for $1 \leq i \leq k$. $\square$

The following definition helps us to give an example of a group ring which is not semiperfect.

Definition 3.1 *A group G is called an ID group (integral domain group) if for each ring R with no zero divisors except zero, RG has no zero divisors except zero.*

Proposition 3.2 *(Rudin & Schneider, 1963) Every Ω- group is an ID group.*

Proof Let G be an Ω-group and R a ring with no non-zero zero divisors. Let α, β be non-zero elements of RG. Then $\operatorname{supp}(\alpha)$ and $\operatorname{supp}(\beta)$ are non-empty, and finite subsets of G. Since G is an Ω-group, for an arbitrary $a \in \operatorname{supp}(\alpha)$ and $b \in \operatorname{supp}(\beta)$, there exists $x \in G$ such that $x = ab$ is the unique representation of $x = a^{'}b^{'}$, where $a^{'}$ and $b^{'}$ in $\operatorname{supp}(\beta)$. Let $\alpha\beta = \sum_{x \in G} r_x x$. If r_a and r_b are the coefficients of a and b in the expression of α and β respectively, $r_x = r_a r_b$ if $x = ab$. Since R has no non-zero zero divisors and $r_a \neq 0$ and $r_b \neq 0$, $r_x \neq 0$. Thus, the product $\alpha\beta$ is non-zero as desired. $\square$

Proposition 3.3 *(Rudin & Schneider, 1963) Every ID group is torsion free.*

Proof Let G be an ID group. Suppose for the contrary that G has a finite non-trivial subgroup H. Let $\alpha = \sum_{h \in H} rh$. Here r is a non-zero fixed element of R. Let $0 \neq \beta = \sum_{h \in H} r_h h$ such that $\sum r_h = 0$. Since H is a finite group, $\alpha\beta = 0$. So RH has non-zero zero divisors. That is, RG has non-zero zero divisors. So G is not an ID group, which is a contradiction. This contradiction shows that G does not have a finite non-trivial subgroup H, that is, G is torsion-free. $\square$

Proposition 3.4 *(Burgess, 1969) If G is a non-trivial ID group, then RG is not semiperfect for any ring R.*

Proof If RG is semiperfect, then by Proposition 3.1, DG is semiperfect for some division ring D. Since G is an ID group, $(D/\operatorname{Rad} D)G \cong DG/\operatorname{Rad}(DG)$ has no non-trivial idempotents. Hence, if $e + \operatorname{Rad}(DG)$ is an idempotent of $DG/\operatorname{Rad}(DG)$, either $e \in \operatorname{Rad}(DG)$ or $1 - e \in \operatorname{Rad}(DG)$. Since DG is semiperfect, $DG/\operatorname{Rad}(DG)$ is semisimple. It follows that $DG/\operatorname{Rad}(DG)$ is a division ring. Thus, $\operatorname{Rad}(DG)$ is a maximal ideal. Also, $DG/\omega G \cong D$, so ωG is a maximal ideal, too, that is, $\operatorname{Rad}(DG) = \omega G$. By Proposition 2.30, G is a p-group for some prime p. This contradicts with the fact that an ID group is torsion free. $\square$

Corollary 3.1 *(Burgess, 1969) If G is an extension of a group by a nontrivial ID group, then RG is not semiperfect for any ring R.*

Proof Let G be an extension of a group by a nontrivial ID group. That is, there exists an exact sequence

$$0 \to H \to G \to N \to 0$$

such that N is an ID group. Since the sequence is exact $N \cong G/H$. It is seen that $RG/RH \cong R(G/H) \cong RN$. Since N is an ID group, RN is not semiperfect by Proposition 3.4. Thus, RG can not be semiperfect. $\square$

Now let G be a non-torsion abelian group. Then it is possible to write the exact sequence

$$0 \to \operatorname{Tor}(G) \to G \to G/\operatorname{Tor}(G) \to 0.$$

$G/\operatorname{Tor}(G)$ is nontrivial since G is not a torsion group. It is also torsion-free and abelian. Thus, $G/\operatorname{Tor}(G)$ is a nontrivial ID group. By Corollary 3.1, RG cannot be semiperfect. So, as a special case, if G is abelian and RG is semiperfect, then we can say that G is torsion. Furthermore, a more general statement can be made.

Proposition 3.5 *(Burgess, 1969) If RG is semiperfect and G is abelian, then either G is finite or $G \cong G_p \times H$, where G_p is an infinite p-group, H finite, p does not divide the order of H and* *each of the division rings associated with the semisimple ring $R/\operatorname{Rad} R$ is of characteristic p.*

Proof As we have seen, if RG is semiperfect, so is DG, where D is a division ring associated with the semisimple ring $R/\operatorname{Rad}(R)$. If D has characteristic zero, then DG is regular by Theorem 2.27, hence $\operatorname{Rad}(DG) = 0$. This means that DG is semisimple, and by Maschke's Theorem, G is finite.

Suppose D has characteristic p. Since G is an abelian and must be torsion by the above observation, we can write $G \cong G_p \times H$, where G_p is the Sylow p-subgroup of G, and H has no elements of order p. Then $DH \cong D(G/G_p) \cong DG/\omega G_p$ is semiperfect. DH is regular since H is locally finite and H has no elements of order p. Thus, as above H is finite. $\square$

Corollary 3.1 and Proposition 3.5 lead to a conjecture that RG is semiperfect implies G is torsion. But it is not known whether RG is semiperfect implies that G is locally finite. If K is a field of characteristic $p > 0$ and G is a p-group which is not locally finite, then KG will be local, hence semiperfect if $\operatorname{Rad}(KG) = \omega G$.

Lemma 3.1 *(Woods, 1974) Let R be a ring such that $R/\operatorname{Rad}(R)$ is Artinian, and let $x \in R$. Let $\{x_n\}$ be the sequence $x_0 = x$, $x_{i+1} = x_i - (x_i)^2$ for $i \geq 0$. Then for some n, $1 - x_n$ has a right inverse in R.*

Proof Consider the chain $Rx_1 \supseteq Rx_2 \supseteq \cdots$ of left ideals in R. Using this chain, we can obtain a chain

$$\frac{Rx_1 + \operatorname{Rad} R}{\operatorname{Rad} R} \supseteq \frac{Rx_2 + \operatorname{Rad} R}{\operatorname{Rad} R} \supseteq \cdots$$

of right ideals in $R/\operatorname{Rad} R$. Since $R/\operatorname{Rad} R$ is Artinian, there exists a positive integer n such that $\frac{Rx_n + \operatorname{Rad} R}{\operatorname{Rad} R} = \frac{Rx_{n+1} + \operatorname{Rad} R}{\operatorname{Rad} R}$ and $x_n \in Rx_{n+1} + \operatorname{Rad} R$. For some $r \in R$ and $y \in \operatorname{Rad} R$, $x_n = r(x_n - x_n^2) + y$. Now $1 - y = (1 - x_n)(1 + rx_n)$ has a left inverse in R, and so $1 - x_n$ has a left inverse in R. $\square$

Theorem 3.1 *(Woods, 1974) Let D be a division ring of characteristic $p \geq 0$ and G a group. If DG is semiperfect, then G is a torsion group and there is a positive integer n such that no chain of finite p'-subgroups of G has length greater than n.*

Proof Suppose $x \in G$ has infinite order. Let $\{x_n\}$ be the sequence in DG such that $x_0 = x$, $x_{i+1} = x_i - x_i^2$ for $i \geq 0$. By Lemma 3.1, $1 - x_m$ has a left inverse in DG for some m. Clearly, $1 - x_m \in KH$, where K is the prime subfield of D and H is the subgroup generated by x. Since KH is a direct summand of DG as left KH- modules, $1 - x_m$ has a left inverse in KH, that is $h(x)(1 - x_m) = 1$ for some $h(x) = \sum_{i=-r}^{r'} a_i x^i \in KH$. Multiplying by x^r, we obtain the factorization

$$x^r = x^r h(x)(1 - x^m) = \sum_{i=0}^{r+r'} d_{i-r} x^r (1 - x_m)$$

in the polynomial ring $K[X]$. This is impossible since x^r is a monomial. Thus, G must be a torsion group.

If $H = \{h_1, \ldots, h_r\}$ is a finite p'-subgroup of G, then $r = r.1$ is a unit in D and by Lemma 2.7, $e_H = \frac{1}{r}(h_1 + \cdots + h_r)$ is an idempotent in DG. Moreover, if $N \leq H$, then $e_H e_N = e_N e_H = e_H$. Since DG is semiperfect, $\overline{DG}$-module $\overline{DG}$ has finite length. Let n be the length of a composition series for the left $\overline{DG}$-module $\overline{DG}$, and suppose

$$\{1\} \subset H_1 \subset \cdots \subset H_{n+1}$$

is a strictly increasing chain of $n+1$ finite p'-subgroups of G. Let $e_i = e_{H_i}$, $i = 1, \ldots, n+1$. Then

$$DG \supseteq DGe_1 \supseteq \cdots \supseteq DGe_{n+1}.$$

Reducing modulo $\operatorname{Rad}(DG)$ we obtain

$$\begin{aligned} DG/\operatorname{Rad}(DG) &\supseteq (e_1 + \operatorname{Rad}(DG))DG/\operatorname{Rad}(DG) \\ &\vdots \\ &\supseteq (e_{n+1} + \operatorname{Rad}(DG))DG/\operatorname{Rad}(DG). \end{aligned}$$

Thus, for some i, $(e_i + \operatorname{Rad}(DG))DG/\operatorname{Rad}(DG) = (e_{i+1} + \operatorname{Rad}(DG))DG/\operatorname{Rad}(DG)$. Then $e_i - e_{i+1}$ is an idempotent in $\operatorname{Rad}(DG)$ and so $e_i = e_{i+1}$. This implies $H_i = H_{i+1}$, a contradiction. □

The following result is a direct consequence of Theorem 3.1.

Corollary 3.2 *(Woods, 1974) Let D be a division ring of characteristic $p \geq 0$ and G a locally finite group. If DG is semiperfect then every p'-subgroup of G is finite.*

3.2. Some Sufficient Conditions

Theorem 3.2 *(Burgess, 1969) If G is an abelian p-group and R is a finite direct product of commutative local rings whose factor fields are of characteristic p, then RG is semiperfect.*

Proof Let $R = L_1 \times \cdots \times L_n$ where L_i is local and $L_i/\operatorname{Rad}(L_i) \cong K_i$, where K_i is a field of characteristic p, $i = 1, \ldots, n$.

Then $RG \cong L_1G \times \cdots \times L_nG$ and for each i,

$$\begin{aligned} L_iG/\operatorname{Rad}(L_iG) &\cong \frac{L_iG/\operatorname{Rad}(L_i)G}{\operatorname{Rad}(L_iG)/\operatorname{Rad}(L_i)G} \\ &\cong \frac{(L_i/\operatorname{Rad}(L_i))G}{\operatorname{Rad}(L_iG/\operatorname{Rad}(L_i)G)} \cong K_iG/\operatorname{Rad}(K_iG). \end{aligned}$$

Here G is an abelian p-group, thus G is locally finite. And each K_i is a field of characteristic p, thus $\operatorname{Rad}(K_iG) = \omega G$ by Proposition 2.31, that is,

$$L_iG/\operatorname{Rad}(L_iG) \cong K_iG/\operatorname{Rad}(K_iG) \cong K_iG/\omega G \cong K_i.$$

Hence, each L_iG is local. Thus, RG is a finite direct product of commutative local rings. By Theorem 2.16, RG is semiperfect. $\square$

Corollary 3.3 *(Burgess, 1969) If R is commutative and $G \cong G_p \times H$, where G_p is a p-group, H is finite and p does not divide the order of H, RG is semiperfect if RH is a finite direct product of local rings whose factor fields are of characteristic p.*

Proof Since $G \cong G_p \times H$, $RG \cong R(G_p \times H) \cong RH(G)$ by Proposition 2.18, the result follows directly from Theorem 3.2. $\square$

Proposition 3.6 *(Woods, 1974) Let R be semiperfect, and let $\{e_1, \ldots, e_n\}$ a set of orthogonal local idempotents in R whose sum is 1. Let G be any group. Then RG is semiperfect if and only if $(e_iRe_i)G$ is semiperfect for each i.*

Proof We have $(e_iRe_i)G \cong e_iRGe_i$, and the result follows from Lemma 2.3. $\square$

Lemma 3.2 *(Woods, 1974) Let R be a ring, G a group, and N a normal subgroup of G such that G/N is locally finite. Then $\operatorname{Rad}(RN) \subseteq \operatorname{Rad}(RG)$.*

Proof Let $x \in \operatorname{Rad}(RN)$, $r \in RG$. To show that $x \in \operatorname{Rad}(RG)$, we will show that $1 - rx$ has a left inverse in RG. Let G' be the subgroup generated by N and $\operatorname{supp}(r)$. We know that $\operatorname{supp}(r)$ is always finite for an arbitrary element of RG. So, the group G'/N is finitely generated. Since G/N is locally finite and G'/N is finitely generated, we have G'/N is finite. Let $G'/N = \{g_1N, g_2N, \ldots, g_nN\}$, where g_1 is the identity element of the group. Then $\{g_1, g_2, \ldots, g_n\}$ is a basis for the free left RN-module RG'. Thus, the endomorphism ring of RG' as a module is the matrix ring $M_n(RN)$. For each $y \in RG'$, let λ_y be the matrix corresponding to left multiplication by y. Then $\lambda : RG' \to M_n(RN)$ is a ring homomorphism. In particular,

$$\lambda_x = \begin{pmatrix} x & 0 & \cdots & 0 \\ 0 & g_2^{-1}xg_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g_n^{-1}xg_n \end{pmatrix}.$$

The entries are in $\mathrm{Rad}(RN)$ because $\mathrm{Rad}(RN)$ is invariant under automorphisms of RN. Thus $\lambda_x \in M_n(\mathrm{Rad}(RN)) = \mathrm{Rad}(M_n(RN))$. This implies that for every $\lambda_x \in M_n(\mathrm{Rad}(RN)) = \mathrm{Rad}(M_n(RN))$, there exists $f \in M_n(RN)$ such that $f(1 - \lambda_r\lambda_x) = 1$. We can regard them as endomorphisms, and if we evaluate them at $1 \in RG'$, we get $f(1)(1 - rx) = 1$. Then $f(1) \in RG' \subseteq RG$ is the left inverse of $1 - rx$. $\square$

Proposition 3.7 *(Woods, 1974) Let R be a local ring with $\mathrm{char}(\overline{R}) = p > 0$ and G a locally finite group. Let N be a normal p-subgroup of G such that $NH = G$. If RH is semiperfect, then so is RG.*

Proof Let $\pi : RG \to \overline{RG}$ be the canonical epimorphism. Let $g \in G$. By assumption, $g = nh$, where $n \in N$ and $h \in H$. Thus we can write $g = nh = (n-1)h + h \in \omega N + RH$. The other containment is clear, so we have $RG = \omega N + RH$. Since $\mathrm{Rad}(R)G \subseteq \mathrm{Rad}(RG)$, π may be factored into

$$RG \xrightarrow{\pi_1} \overline{R}G \xrightarrow{\pi_2} \overline{RG},$$

where $\mathrm{Ker}(\pi_2) = \mathrm{Rad}(\overline{R}G)$. Since N is a p-group and $\mathrm{char}(\overline{R}) = p$, ωN in the group ring $\overline{R}N$ is a nil ideal by Theorem 2.28, hence $\omega_{\overline{R}}N \subseteq \mathrm{Rad}(\overline{R}N)$. Since $G/N \cong H$ is a locally finite group, it follows by Lemma 3.2 that $\mathrm{Rad}(\overline{R}N) \subseteq \mathrm{Rad}(\overline{R}G)$. Thus

$$\omega_{RN}N \subseteq \pi_1^{-1}(\omega_{\overline{R}N}N) \subseteq \pi_1^{-1}(\mathrm{Rad}(\overline{R}G)) = \mathrm{Rad}(RG)$$

and $\omega_{RG}N \subseteq \mathrm{Rad}(RG)$. It follows that $RG = \mathrm{Rad}(RG) + RH$ and $\pi(RH) = \overline{RG}$. By Proposition 2.23 $RH \cap \mathrm{Rad}(RG) \subseteq \mathrm{Rad}(RH)$. Thus,

$$\frac{RH}{\mathrm{Rad}(RH)} \cong \frac{RH/(\mathrm{Rad}(RG) \cap RH)}{\mathrm{Rad}(RH)/(\mathrm{Rad}(RG) \cap RH)}$$

by Third Isomorphism Theorem. Since RH is semiperfect, $\overline{RH}$ is semisimple. This gives us $\frac{RH}{RH \cap \mathrm{Rad}(RG)}$ is semisimple. Thus, $\mathrm{Rad}(RH) = RH \cap \mathrm{Rad}(RG)$. In addition,

$$\frac{RG}{\mathrm{Rad}(RG)} = \frac{RH + \mathrm{Rad}(RG)}{\mathrm{Rad}(RG)} \cong \frac{RH}{RH \cap \mathrm{Rad}(RG)},$$

by Second Isomorphism Theorem. Thus, $\overline{RH} \cong \overline{RG}$ and $\overline{RG}$ is semisimple.

If RH is semiperfect, then $\overline{RG}$ is artinian. Let $\overline{x}^2 = \overline{x} \in \overline{RG}$. Then $\overline{x} = \pi(e)$ for some idempotent e in $RH \subseteq RG$. Thus RG is semiperfect. $\square$

The next result is a consequence of Proposition 3.7.

Corollary 3.4 *(Woods, 1974) Let R be a local perfect ring with $\mathrm{char}(\overline{R}) = p \geq 0$ and G be a locally finite group. If G has a p-subgroup of finite index, then RG is semiperfect.*

Proof By assumption, G has a normal p-subgroup N of finite index and a finite subgroup F such that $NF = G$. Then RF is perfect (See Theorem 4.1), hence semiperfect and so RG is semiperfect. $\square$

Proposition 3.8 *Let R be a local ring with $\mathrm{char}(\overline{R}) = p > 0$. Let G be an abelian group and G_p be the Sylow p-subgroup of G. Then RG is semiperfect if and only if $R(G/G_p)$ is semiperfect, and in this case G/G_p is finite.*

Proof Follows directly from Proposition 3.7 and Corollary 3.4. $\square$

We now show that if G is a finite group of exponent n and if C_n is the cyclic group of order n, then RG is semiperfect if and only if RC_n is semiperfect. Then necessary and sufficient conditions for RC_n to be semiperfect are given when R is commutative, in terms of the polynomial ring $R[X]$.

Without loss of generality, we may assume that R is semiperfect and n is a unit in R. Since G is a finite group, $\mathrm{Rad}(RG) = (\mathrm{Rad}\, R)G$ by Corollary 2.12 and $RG/\mathrm{Rad}(RG) = RG/(\mathrm{Rad}\, R)G \cong (R/\mathrm{Rad}(R))G$ is an Artinian ring by Theorem 2.24. To prove that RG is semiperfect it is sufficient to prove that either idempotents lift from $(R/\mathrm{Rad}\, R)G$ to RG or that every primitive idempotent in RG is local. If e is any idempotent in RG, then ne is a unit in $eRGe$ since we have assumed n is a unit in R. Also $\overline{eRGe} = \overline{e}\overline{RG}\overline{e}$ holds by Theorem 2.10.

Let g be an element of order n in an abelian group G, K an algebraically closed field such that $\mathrm{char}(K) \nmid n$, and z a primitive n^{th} root of unity in K. For $i = 0, \dots, n-1$, let

$$k_j = \frac{1}{n}\sum_{j=0}^{n-1} z^{ij} g^j.$$

We show that k_i are orthogonal idempotents whose sum is 1 and that if z^i is a primitive m^{th} root of unity, then gk_i is a primitive m^{th} root of k_i. Since $z^i g k_i = k_i$, $k_i^2 = k_i$. If $i \neq j$, let $k_i k_j = \frac{1}{n^2}\sum_{t=0}^{n-1} a_t g^t$. Then

$$z^{ij} a_t = \sum_{k=0}^{n-1} z^{ik} z^{j(t-k)} = z^{jt} z^{i-j} \sum_{k=0}^{n-1} z^{(i-j)k} = a_t.$$

Since $z^{i-j} \neq 1$, $a_t = 0$, and hence $k_i k_j = 0$.

Let $\sum_{i=0}^{n-1} k_i = \frac{1}{n}\sum_{t=0}^{n-1} b_t g^t$. Then $z^t b_t = z^t \sum_{i=0}^{n-1} z^{it} = b_t$. If $0 < t < n$, $z^t \neq 1$ and hence $b^t = 0$. Thus,

$$\sum_{i=0}^{n-1} k_i = \frac{1}{n}.n.1 = 1.$$

If z^i is a primitive m^{th} root of 1, then $g^m k_i = g^m z^{im} k_i = k_i$, but if $0 < r < m$, then $k_i = g^r z^{ir} k_i \neq g^r k_i$ since $z^{ir} \neq 1$ and $k_i \neq 0$.

For each m with $m|n$, let $e_m = \sum k_i$ where the sum is taken over all i such that z^i is a primitive m^{th} root of 1, and let $e_m^{'} = \sum k_i$ where the sum is taken over all i such that $z^{im} = 1$. Then $\{e_m : m|n\}$ is an orthogonal set of idempotents whose sum is 1. Since $e_m k_i = k_i$ whenever z^i is a primitive m^{th} root of unity, ge_m is a primitive m^{th} root of e_m. Clearly $e_m^{'} = \sum_{d|m} e_d$. Since $z^{im} = 1$ if and only if $s|i$, where $s = \frac{n}{m}$, $e_m^{'} = \sum_{j=0}^{m-1} k_{sj}$. Let

$$e_m^{'} = \frac{1}{n} \sum_{t=0}^{n-1} c_t g^t.$$

Then $c_t = \sum_{j=0}^{m-1} z^{sjt}$. If $m|t$, $z^{sjt} = 1$ and $c_t = m$. If $m \nmid t$, then, since $z^{st} c_t = c_t$ and $z^{st} \neq 1$, $c_t = 0$. Thus,

$$e_m^{'} = \frac{m}{n}(1 + g^m + \cdots + g^{n-m}).$$

If $K = \mathbb{C}$, the complex numbers, then for each $m|n$, $ne_m^{'} \in \mathbb{Z}G$, where $\mathbb{Z}$ denotes the integers. Since $e_m = e_m^{'} - \sum e_d$ where the sum is taken over all $d|m$, $d < m$, we see by induction that $ne_m \in \mathbb{Z}G$.

Let R be any ring which n is a unit, and let $R^{'}$ be the subring $\{t.1 : t \in \mathbb{Z}\}$. Then $R^{'} \cong \mathbb{Z}$ or $R^{'} \cong \mathbb{Z}/ < r >$ for some r relatively prime to n. In either case, for some $p \nmid n$ there are homomorphisms

$$\mathbb{Z} \to R^{'} \to \mathbb{Z}/ < p > \to K,$$

where K is the algebraic closure of $\mathbb{Z}/ < p >$, which extend to homomorphisms

$$\mathbb{Z}G \to R^{'}G \to KG.$$

In RG, we may define inductively for each $m|n$, $e_m^{'} = \frac{m}{n}(1+g^m+\cdots+g^{n-m})$ and $e_m = e_m^{'} - \sum e_d$, where the sum is taken over all $d|m$, $d < m$. Then $ne_m \in R^{'}G$ for each $m|n$. Using the homomorphisms defined above, $(ne_m)^2 = n(ne_m)$, $(ne_m)(ne_d) = 0$ if $m \neq d$, $\sum_{m|n} e_m = 1$ and $g^m e_m = e_m$. If $g^r e_m = e_m$ in RG for some r, $0 < r < m$ then $g^r(ne_m) = ne_m$ in $R^{'}G$, hence in KG. Thus $g^r e_m = e_m$ in KG, a contradiction. It follows that ge_m is a primitive m^{th} root of unity in RGe_m.

Lemma 3.3 *(Woods, 1974) Let e be a nonzero primitive idempotent in RG, and let $m|n$. Then ge is a primitive m^{th} root of unity in $eRGe$ if and only if $e = e_m e$. In this case, $\overline{ge}$ is a primitive m^{th} root of unity in $\overline{eRGe}$.*

Proof Since $(ge)^n = g^n e = e$, ge is a primitive d^{th} root of unity in $eRGe$ for a unique $d|n$. Since e is primitive and $e = \sum_{m|n} e_m e$, $e = e_m e$ for a unique $m|n$. We will show that $d = m$.

Since $(ge_m)^m = e_m$, $(ge)^m = (ge_m e)^m = e_m e = e$. Thus $d|m$. Since $g^d e = e$, $e^{'}_d e = e$. If $d < m$, then $e = e^{'}_d e_m e = 0$, a contradiction. Thus, $d = m$.

In this case, $\overline{eRGe} = \overline{e}\overline{R}G\overline{e}$ and $\overline{ge} = g\overline{e}$ in $\overline{R}G$. Then $\overline{e} = \overline{e_m e}$, and the above argument applied in $\overline{R}G$ shows that $g\overline{e}$ is a primitive m^{th} root of unity in $\overline{e}\overline{R}G\overline{e}$. $\square$

Lemma 3.4 *(Woods, 1974) Let R be a local ring, G a group and e an idempotent in RG such that $eRGe \subseteq eR \cap Re$ and $e(1)$ is central and not a zero divisor in R. Let $R^{'} = \{r \in R : er = re\}$. Then $eRGe \cong R^{'}$ as rings and $R^{'}$ is local.*

Proof If $x \in eRGe$, then $x = re$ for a unique $r \in R$. Define $f : eRGe \to R$ by $f(re) = r$. Clearly, f preserves sums, and $\operatorname{Ker} f = 0$. If $re \in eRGe$, then $ere = re$. Thus $f(rese) = f(rse) = rs = f(re)f(rs)$. This proves that $eRGe \cong \operatorname{Im} f$ by First Isomorphism Theorem.

Clearly, $R^{'} \subseteq \operatorname{Im} f$. Let $r \in \operatorname{Im} f$. Then $re \in eRGe \subseteq eR \cap Re$, and so $re = er^{'}$ for some $r^{'} \in R$. Thus, $re(1) = e(1)r^{'} = e(1)r^{'}$, so by assumption $r = r^{'} \in R^{'}$. This completes the proof that $eRGe \cong R^{'}$.

Finally if $r^{'} \in R^{'}$ is a unit in R, then $r^{'}$ is a unit in $R^{'}$. Thus, the set of non-units in $R^{'}$ is precisely $R^{'} \cap \operatorname{Rad} R$, an ideal of $R^{'}$. It follows that $R^{'}$ is local. $\square$

Lemma 3.5 *(Woods, 1974) Let R be a local ring with $\operatorname{char}(\overline{R}) = p \geq 0$, and let $G =< g >$ be a cyclic group of order n, $p \nmid n$. Let $m|n$, and suppose R has a primitive m^{th} root of unity r such that $\overline{r}$ is a primitive m^{th} root of unity in $\overline{R}$. Then RGe_m is semiperfect.*

Proof Since $RGe_{m'} = RGe_m \oplus RG(e^{'}_m - e_m)$, it is sufficient to show that $RGe^{'}_m$ is semiperfect.

For $i = 1, \ldots, m$, let

$$f_i = \frac{1}{m}\sum_{j=0}^{m-1} r^{ij} g^j e^{\prime}_m.$$

Since $r^i g f_i = f_i$, $f_i^2 = f_i$. If $i \neq k$, then $0 < |i - k| < m$. Thus $\overline{r}^{i-k} \neq \overline{1}$ in $\overline{R}$ and $r^{i-k} - 1$ is a unit in R. Now

$$\begin{aligned} f_j f_k &= \frac{1}{m^2}\sum_{j=0}^{m-1}\sum_{t=0}^{m-1} r^{ij} r^{k(t-j)} g^j g^{t-j} e^{'}_m \\ &= \frac{1}{m^2}\sum_{t=0}^{m-1} r^{kt} x g^t e^{'}_m \end{aligned}$$

where $x = \sum_{j=0}^{m-1} r^{(i-k)j}$. But $r^{i-k}x = x$, and so $x = 0$. Thus, $f_i f_k = 0$. Moreover,

$$\sum_{i=1}^{m} f_i = \frac{1}{m}\sum_{j=0}^{m-1}(\sum_{i=1}^{m} r^{ij})g^j e_m^{'} = 1e_m^{'},$$

the unity of $RGe_m^{'}$.

Finally, $f_iRGe_m^{'}f_i = f_iRGf_i$. Since $r^igf_i = f_i$, $gf_i = r^{-i}f_i \in Rf_i$. Thus, $RGf_i = Rf_i$. Similarly, $f_iRG = f_iR$, and so $f_iRGf_i \subseteq f_iR \cap Rf_i$. Moreover, $f_i(1) = \frac{1}{m}\frac{m}{n}r^0 = \frac{1}{n}$, a central unit in R. By Lemma 3.4, f_iRGf_i is local. Thus, $RGe_m^{'}$ is semiperfect. $\square$

Lemma 3.6 *(Woods, 1974) Let g and h be commuting elements in a group G of orders s and t respectively, and $u = \mathrm{lcm}(s,t)$. Then for some integer r, gh^r has order u.*

Proof The group $< g, h >$ is a finite abelian group of exponent u. Hence, $< g, h >= Y \times Z$, where $Y =< y >$ is a cyclic group of order u, and $z^u = 1$ for all $z \in Z$. Let $g = (y^a, z_1)$ and $h = (y^b, z_2)$. Since g and h generate $Y \times Z$, y^a and y^b generate Y. Thus, $\gcd(a, b, u) = 1$. If $u|a$, let $r = 1$. Otherwise, let r be the product of all primes which divide u but not a. A check of possible prime factors gives that $\gcd(a + br, u) = 1$. Thus, $gh^r = (y^{a+br}, z_1z_2^r)$ has order u. $\square$

Lemma 3.7 *(Woods, 1974) Let R be a ring, and let $G = C_n$. If RG is semiperfect, then so is $R(G \times G)$.*

Proof Without loss of generality we may assume R is local and n is a unit in R. Let g generate G, and $H =< h >$ denote the second copy of G. For each m with $m|n$, define $e_m \in RG$ as in the beginning of this section, and define $f_m \in RH$ in a corresponding way using h in place of g.

Let e be a primitive idempotent in $R(G \times H)$. We show that e is local. Now $e = ee_sf_t$ for a unique s with $t|n$. Thus, by Lemma 3.6, in the multiplicative group $< ge, he >$, ge has order s and he has order t. Let $u = \mathrm{lcm}(s, t)$, and let r be an integer such that gh^re has order u. The automorphism of $G \times H$ which sends gh^r to g and h to h extends to an automorphism θ of $R(G \times H)$. Since $\theta(e)R(G \times H)\theta(e) \cong eR(G \times H)e$, it is sufficient to show that $\theta(e)$ is local idempotent.

Since e is a primitive idempotent, so is $\theta(e)$. In $< g\theta(e), h\theta(e) >$, $g\theta(e) = \theta(gh^re)$ has order u, and $h\theta(e) = \theta(he)$ has order t. By Lemma 3.6, $\theta(e) = \theta(e)e_uf_t$. Now $R(G \times H)e_uf_t \cong (RGe_u)Hf_t$ in a natural way. Since RGe_u is semiperfect, the unit element e_u is sum of orthogonal local idempotents. If f is a local idempotent in RGe_u, then $f(RGe_u)Hf_tf \cong (fRGe_uf)Hf_t$ is semiperfect by Lemmas 3.3 and 3.5. Thus, RGe_uHf_t is semiperfect by Lemma 2.3. It follows that

$$\theta(e)R(G \times H)\theta(e) = \theta(e)R(G \times H)e_uf_t\theta(e)$$

is a local ring and $R(G \times H)$ is semiperfect. $\square$

Proposition 3.9 *(Woods, 1974) Let R be a ring and G be a finite group of exponent n. Then RG is semiperfect if and only if RC_n is semiperfect.*

Proof Since RC_n is a homomorphic image of RG, if RG is semiperfect, then so is RC_n. Conversely, suppose RC_n is semiperfect. If $r \geq 2$, then $RC_n^r \cong (RC_n^{r-2})(C_n \times C_n)$ and $RC_n^{r-1} \cong (RC_n^{r-2})C_n$. By Lemma 3.7 and induction, RC_n^r is semiperfect for all $r > 0$. But RG is a homomorphic image of RC_n^r for some r. Thus, RG is semiperfect. $\square$

Before giving the main theorem of this chapter, we need the following definition and theorem.

Definition 3.2 *Let R be a commutative local ring and $f(x) \in R[X]$ a monic polynomial. We say that Hensel Lemma holds for $f(x)$ in $R[X]$ if for every factorization $\overline{f}(x) = g(x)h(x)$ of $\overline{f}(x)$ in $\overline{R}[X]$ such that $g(x)$ is monic and $g(x)$ and $h(x)$ are relatively prime, there exists monic polynomials $g^*(x)$ and $h^*(x)$ in $R[X]$ such that $f(x) = g^*(x)h^*(x)$, $\overline{g^*(x)} = g(x), \overline{h^*(x)} = h(x)$.*

Theorem 3.3 *(Azumaya, 1950) Let K be a commutative local ring and $f(x)$ be a monic polynomial in $K[X]$. Then Hensel Lemma holds for $f(x)$ if and only if idempotents of $\overline{K}[X]/ < \overline{f}(x) >$ can be lifted to an idempotent of $K[X]/ < f(x) >$.*

Theorem 3.4 *(Woods, 1974) Let R be a commutative local ring with $\mathrm{char}(\overline{R}) = p \geq 0$ and G an abelian group with Sylow p-subgroup G_p. Then RG is semiperfect if and only if G/G_p is a finite group of exponent n and every monic factor of $x^n - 1$ in $\overline{R}[X]$ can be lifted to a monic factor of $x^n - 1$ in $R[X]$.*

Proof By Proposition 3.8 and Proposition 3.9, we may assume $G = C_n$ and n is a unit in R. Then $RG \cong R[X]/ < x^n - 1 >$ and since G is a finite group, by Corollary 2.12, $\overline{RG} = \overline{R}G \cong \overline{R}[X]/ < x^n - 1 >$. Since n is a unit in $\overline{R}$, $x^n - 1$ has no multiple roots in any extension of $\overline{R}$ by Theorem 2.20. Thus, if $x^n - 1 = f(x)g(x)$ in $\overline{R}[X]$, then $f(x)$ and $g(x)$ are relatively prime. By Theorem 3.3, idempotents in $\overline{R}[X]/ < x^n - 1 >$ lift to idempotents in $R[X]/ < x^n - 1 >$ if and only if every monic factor of $x^n - 1$ in $\overline{R}[X]$ lifts to a monic factor of $x^n - 1$ in $R[X]$. $\square$

3.3. Examples

In this section it is shown that for a given ring R, the class of groups G for which RG is semiperfect is not closed under taking direct products or subgroups.

Let g generate C_2, the 2-element group. If R is a local ring and $\mathrm{char}(\overline{R}) \neq 2$, then $\frac{1+g}{2}$ and $\frac{1-g}{2}$ are local idempotents in RC_2 whose sum is 1. Thus, RC_2 is semiperfect. If $\mathrm{char}(\overline{R}) = 2$, then RC_2 is semiperfect by Proposition 3.7.

Lemma 3.8 *If R is semiperfect and S_3 is the symmetric group of degree 3, then RS_3 is semiperfect.*

Proof We may assume R is local. If $\mathrm{char}(\overline{R}) = 3$, let N be the subgroup of order 3, and let H be a subgroup of order 2 in S_3. Then $S_3 = NH$ and RS_3 is semiperfect by Proposition 3.6.

If $\mathrm{char}(\overline{R}) \neq 3$, let g generate N and h generate H, and let $e = \frac{1+g+g^2}{3}$, a central idempotent. Then

$$RS_3 = RS_3e \oplus RS_3(1-e).$$

Since $RS_3(1-e) = \omega N$ by Proposition 2.22, $RS_3e \cong RS_3/\omega N \cong R(S_3/N) = RC_2$. Thus, RS_3e is semiperfect.

Let $f_1 = \frac{(1-g)(1+h)}{3}$, and let $f_2 = (1-e) - f_1$. Then f_1 and f_2 are orthogonal idempotents whose sum is $1-e$. Also, for $i = 1, 2$, $f_iRS_3(1-e)f_i = f_iRS_3f_i \subseteq f_iR \cap Rf_i$ and $f_i = \frac{1}{3}$. By Lemma 3.4, $f_iRS_3f_i$ is local. Thus, $RS_3(1-e)$ is semiperfect. $\square$

Now we exhibit a local ring R such that RC_3 is not semiperfect. Let $R = \{\frac{a}{b} : a, b \in \mathbb{Z} \text{ and } \gcd(7, b) = 1\}$, a subring of the rationals. Then $\overline{R}$ is a field with 7 elements. In $\overline{R}[X]$,

$$x^3 - 1 = (x - \overline{1})(x - \overline{2})(x - \overline{4}).$$

But in $R[X]$,

$$x^3 - 1 = (x - 1)(x^2 + x + 1).$$

Since $x^2 + x + 1$ is irreducible over R, RC_3 is not semiperfect.

For our second example, we let

$$R = \{\tfrac{x}{y} : x, y \in \mathbb{Z}[i] \text{ and } (2+i) \nmid y \text{ in } \mathbb{Z}[i]\},$$

a subring of the complex numbers. Then $\overline{R}$ is a field with 5 elements. In $\overline{R}[X]$,

$$x^3 - 1 = (x - \overline{1})(x^2 + \overline{1}x + \overline{1})$$

and

$$x^8 - 1 = (x - \overline{1})(x + \overline{1})(x - \overline{i})(x + \overline{i})(x^2 - \overline{i})(x^2 + \overline{i}),$$

and the quadratic factors are irreducible. Since these factorizations can be lifted to $R[X]$, RC_3 and RC_8 are semiperfect.

Now $C_3 \times C_8 = C_{24}$. In $R[X]$, $x^{24} - 1$ has the irreducible factor $x^4 - ix^2 - 1$, but in $\overline{R}[X]$,

$$x^4 - \overline{i}x^2 - \overline{1} = x^4 + \overline{2}x^2 + \overline{9} = (x^2 + \overline{2}x + \overline{3})(x^2 - \overline{2}x + \overline{3}).$$

Thus RC_{24} is not semiperfect.

CHAPTER 4

PERFECT GROUP RINGS

4.1. Sufficiency

In this section we assume that R is perfect and G is finite and show that $\operatorname{Rad}(RG)$ is left T- nilpotent and $RG/\operatorname{Rad}(RG)$ is Artinian.

Lemma 4.1 *(Woods, 1971) If G is a finite group of order n, then there is a ring embedding of RG into $M_n(R)$ which sends $\operatorname{Rad}(R)G$ into $\operatorname{Rad}(M_n(R))$.*

Proof Since $RG \cong R^{(n)}$ as left R-modules, the endomorphism ring $\operatorname{End}_R(RG) \cong M_n(R)$. Right multiplication by an element of RG is a left R-homomorphism of RG into itself, and this correspondence is clearly an embedding of the ring RG into the ring $\operatorname{End}_R(RG)$.

Since elements of R commute with elements of G, an element r of R is mapped onto the matrix with r's on the diagonal and 0's elsewhere. Thus, $\operatorname{Rad}(R)$ is mapped into $M_n(\operatorname{Rad}(R)) = \operatorname{Rad}(M_n(R))$, an ideal. The result follows. $\square$

Proposition 4.1 *(Woods, 1971) If R is perfect and G is finite, then RG is perfect.*

Proof Since R is perfect, $R\big/\operatorname{Rad} R$ is Artinian. Thus $\overline{R}G$ is Artinian by Theorem 2.24. We know that $\operatorname{Rad}(R)G \subseteq \operatorname{Rad}(RG)$ by Corollary 2.12. Then $\overline{R}G \cong RG/\operatorname{Rad}(R)G$ maps onto $RG/\operatorname{Rad}(RG)$ and $RG/\operatorname{Rad}(RG)$ is Artinian.

The canonical epimorphism of RG onto $\overline{R}G$ takes $\operatorname{Rad}(RG)$ into $\operatorname{Rad}(\overline{R}G)$, that is, $\operatorname{Rad}(RG)/\operatorname{Rad}(R)G \subseteq \operatorname{Rad}(\overline{R})G$. Since $\overline{R}G$ is Artinian, $\operatorname{Rad}(\overline{R}G)$ is nilpotent. But, by Lemma 4.1, $\operatorname{Rad}(R)G \subseteq \operatorname{Rad}(M_n(R))$, which is left T-nilpotent since $M_n(R)$ is perfect. Thus, $\operatorname{Rad}(RG)$ is left T-nilpotent. $\square$

4.2. Necessity when G is Abelian

Lemma 4.2 *(Woods, 1971) If RG is perfect, then G is a torsion group.*

Proof If $g \in G$ does not have finite order, then the cyclic subgroups generated by g^{2^n} for $n \geq 0$ form an infinite descending chain. Applying ω yields an infinite descending chain of right ideals of RG, which are principal. $\square$

Proposition 4.2 *(Woods, 1971) If RG is perfect, then so is R. If in addition, G is abelian, then G is finite.*

Proof If RG is perfect then so is $RG/\omega G \cong R$. To show that G is finite, we may assume without loss of generality that $R = M_n(D)$, where D is a division ring, since $R/\operatorname{Rad}(R)$ is a direct sum of rings of this type. Since G is an abelian torsion group, G may be written as $G_p \times H$, where p is the characteristic of D, G_p is a p-group, and the order of every element of H is prime to p, and H must be finite.

Suppose that G_p is infinite. Then $RG_p \cong RG/\omega H$ is perfect. If $g \in G_p$, then $(1-g)^{p^n} = 0$, where p^n is the order of g. Since $1-g$ is in the center, $1 - g \in \operatorname{Rad}(RG_p)$. Construct a sequence $\{g_i\}$ in G_p so that $g_1 \neq 1$ and g_n is not in the (finite) subgroup generated by $\{g_1, \ldots, g_{n-1}\}$. The product is never 0 since the term $\prod_{i=1}^{n}(1-g_i)$ does not cancel. This contradicts to the T-nilpotence of $\operatorname{Rad}(RG_p)$. □

4.3. Reduction to the Abelian Case

In this section it is shown that if RG is perfect and G is infinite then G has an infinite abelian subgroup H and RH is perfect, a contradiction. Without loss of generality, we continue our assumption that $R = M_n(D)$, where D is a division ring.

Lemma 4.3 *(Woods, 1971) If RG is perfect and H is a subgroup of G, then RH is perfect.*

Proof By Proposition 2.21, $RG = \bigoplus_i RHg_i$, where the g_i run over a set of coset representatives for G/H. If I is a principal right ideal of RH, then $IG = \bigoplus_i Ig_i$ is a principal right ideal of RG. Thus, a descending chain of principal right ideals in RH gives rise to a similar chain in RG. □

Lemma 4.4 *(Woods, 1971) If I is a left T-nilpotent ideal of a ring R, then $I \subseteq \operatorname{rad}(R)$. Hence, if R is perfect, then $\operatorname{Rad}(R) = \operatorname{rad}(R)$.*

Lemma 4.5 *(Woods, 1971) A group G, which has infinitely many normal subgroups, has an infinite abelian subgroup.*

Proof Without loss of generality, we may assume that G is the union of a countable chain of finite normal subgroups H_i. It is clear that an infinite set of commuting elements generates an infinite abelian subgroup. Thus if G does not contain an infinite abelian subgroup, then there exists a finite set $\{g_1, \ldots, g_m\}$ of commuting elements which cannot be enlarged. Since $G = \bigcup_{i=1}^{\infty} H_i$, $S \subseteq \bigcup_{i=1}^{n} H_i = H_n$ for some n. Since H_n is finite, the index of its centralizer C in G is finite. Since G is infinite, C is infinite, and so there exists $g \in C$ such that g is not in S. Since g commutes with every element of S, g may be added to S and we have reached a contradiction. $\square$

Proposition 4.3 *(Woods, 1971) If RG is perfect, then either G is finite or G has an infinite abelian subgroup.*

Proof Let $R = M_n(D)$. If D has characteristic 0, then RG is semiprime by Proposition 2.25 hence Jacobson semisimple by Lemma 4.4. Thus, $RG \cong RG/\operatorname{Rad}(RG)$ is Artinian and G is finite.

Suppose D has characteristic $p > 0$. Let

$$S = \{n : G \text{ has a normal subgroup of order } p^n m \text{ for some } m\}.$$

If S is finite, let n be maximal, and let H_n be a normal subgroup whose order is divisible by p^n. By the maximality of n, G/H_n has no finite normal subgroup whose order is divisible by p. Therefore, $R(G/H_n)$ is semiprime. Since $R(G/H_n)$ is perfect, G/H_n is finite. Since H_n is finite, so is G.

If S is infinite, then G has infinitely many finite normal subgroups. By Lemma 4.5, G contains an infinite abelian subgroup. This completes the proof of the following theorem. $\square$

Theorem 4.1 *(Woods, 1971) The group ring RG is perfect if and only if R is perfect and G is finite.*

CHAPTER 5

CONCLUSION

In this thesis, we gave a survey of some properties of group rings, and some characterization of semiperfect and perfect group rings. For this purpose, firstly we mentioned about some properties of groups, rings and group rings. We concentrated on which conditions on R and G are necessary and sufficient on R and G for the group ring RG to be semiperfect and perfect.

We studied the papers (Burgess, 1969) and (Woods, 1974). We saw that semiperfectness of RG implies semiperfectness of R. Thus, R is the direct product product of matrix rings over some division rings. When we look at the necessary conditions on G for RG to be semiperfect, we saw that, if G is an ID group, then RG cannot be semiperfect for any ring R. Since a non-torsion abelian group is an extension of a group by a non-trivial ID group, this gave us that G must be torsion if RG is semiperfect and G is abelian. For an arbitrary group G, it is not known whether RG is semiperfect implies G is locally finite. Again for an arbitrary group, it is seen that that the characteristic of division rings which are related to the semisimple ring $R/\operatorname{Rad} R$ gives some characteristic properties about the group G. For the sufficient conditions, firstly commutative semiperfect rings are considered. Commutative semiperfect rings are exactly finite direct products of commutative local rings. By these characterization, it is seen that when we have a finite direct product of commutative local rings whose factor fields are of characteristic p, we get a semiperfect group ring if G is an abelian p-group. Later, the results that are obtained by considering locally finite groups are reviewed. For semiperfectness of RG, there is not a full characterization for an arbitrary ring R and an arbitrary group G. If we have a commutative ring R and an abelian group G, a characterization is given in terms of the polynomial ring $R[X]$.

For perfectness, we studied the paper (Woods, 1971). Firstly the sufficient conditions on R and G are obtained. Then it is observed that if G is abelian, then G is finite. Later it is seen that we can reduce all cases to the abelian case. Finally, we see that RG is semiperfect if and only if R is perfect and G is finite.

REFERENCES

Azumaya, Gorô (1950) *On Maximally Central Algebras* Mathematical Institute, Nagoya University

Bland, Paul E. (2010) *Rings and Their Modules* De Gruyter

Burgess, W.D. (1969) *On Semiperfect Group Rings* Canadian Mathematical Bulletin, 12: 645-652.

Burnside, W. (1902) *On an Unsettled Question in the Theory of Discontinuous Groups* Quart. J. Pure Appl. Math. 33: 230-238

Connell, I. (1962) *On the Group Ring* Canadian Journal of Mathematics, 15: 650-685.

Dixon, M. R. (1994) *Sylow Theory, Formations and Fitting Classes in Locally Finite Groups* Series in Algebra 2, River Edge, NJ: World Scientific Publishing Co. Inc.

Golod, E.S. & Shafarevich, I.R. (1964) *On the Class Field Tower* Izv. Akad. Nauk SSSSR 28:261-272

Herstein, I.N. (1968) *Noncommutative Rings* The Mathematical Association of America

Kaye, S.M. (1967) *Ring Theoretic Properties of Matrix Rings* Illionis Journal of Mathematics, 10: 365-374

Lam, T.Y. 199O *A First Course in Noncommutative Rings* Springer

Lang, S. (2000) *Undergraduate Algebra* Springer

Milies, C.P. & Sehgal, S.K. (2002) *An Introduction to Group Rings* Kluwer Academic Publishers, Dordrecht

Mueller, B.J. (1970) *On Semi-perfect Rings* Illionis Journal of Mathematics, 14: 464-467

Robinson, D.J.S. (1991) *A Course in the Theory of Groups* Springer

Rudin W., Schneider H. (1963) *Idempotents in Group Rings* Mathematics Research Center, University of Wisconsin

Woods, S.M. (1974)*Some Results on Semiperfect Group Rings* Canadian Journal of Mathematics, 16: 121-129.

Woods, S.M. (1971)*On Perfect Group Rings* Proceedings of the American Mathematical Society, 27: 49-52