AMERICAN UNIVERSITY OF BEIRUT

STRUCTURE OF RINGS WITH CONDITIONS ON CERTAIN SUBSETS

by
TALA SAMMAN KAAKAJI

A thesis
submitted in partial fulfillment of the requirements
for the degree of Master of Science
to the Department of Mathematics
of the Faculty of Arts and Sciences
at the American University of Beirut

Beirut, Lebanon
February 2015

AMERICAN UNIVERSITY OF BEIRUT

STRUCTURE OF RINGS WITH CONDITIONS ON CERTAIN SUBSETS

by

TALA SAMMAN KAAKAJI

Approved by:

Dr. Abu-Khuzam Hazar, Professor
Mathematics

Advisor

Dr. Nahlus Nazih, Professor
Mathematics

Member of Committee

Dr. Azar Monique, Assistant Professor
Mathematics

Member of Committee

Date of thesis/dissertation defense: February 2, 2015

AMERICAN UNIVERSITY OF BEIRUT

THESIS, DISSERTATION, PROJECT RELEASE FORM

Student Name: Samman Kaakaji Tala Jamil
Last First Middle

● Master's Thesis ○ Master's Project ○ Doctoral Dissertation

■ I authorize the American University of Beirut to: (a) reproduce hard or electronic copies of my thesis, dissertation, or project; (b) include such copies in the archives and digital repositories of the University; and (c) make freely available such copies to third parties for research or educational purposes.

☐ I authorize the American University of Beirut, **three years after the date of submitting my thesis, dissertation, or project,** to: (a) reproduce hard or electronic copies of it; (b) include such copies in the archives and digital repositories of the University; and (c) make freely available such copies to third parties for research or educational purposes.

Tala Kaakaji 04/02/2015

Signature Date

ACKNOWLEDGMENTS

I would like to start by deeply thanking my thesis advisor Dr. Hazar Abu Khuzam for giving me his time and effort; he was a great advisor as well as an amazing professor who taught me not only mathematics, but also a way of thinking. In addition, I would like to show my gratitude to Dr. Monique Azar and Dr. Abu Khuzam for making Abstract Algebra an interesting topic for me. I would also like to thank the jury on my thesis committee and give them my best regards.

Furthermore, I want to thank the department of Mathematics in AUB for these nourishing undergraduate and graduate university years. The type, level, and the methodology of delivering the education in AUB is definitely first-rate.

On a personal level, I would like to dedicate all my success to my lovely parents, for without their constant provision and encouragement, I wouldn't have reached what I am today. I am forever indebted for my mother and father, for they are the reason of my devotion to work. In addition, I would like to thank my amazing brothers who stood beside me through out every step in my life. Finally, I would like to show my gratitude to my lovely husband who is constantly giving me the encouragement and vitality to continue and pursue my dreams.

AN ABSTRACT OF THE THESIS OF

Tala J. Samman Kaakaji for Master of Sciences

Major: Mathematics

Title: Structure of Rings with Conditions on Certain Subsets

Rings are of different structures, altering some conditions on some subsets of a ring might cause a change in its structure. In this thesis, we study some of these alterations and their effects on the ring and its subsets.

In the first chapter, we introduce some basic definitions, theorems, and lemmas that are crucial for the succeeding chapters.

In the Second chapter, we study the structure of rings with prime centers and how varying some conditions on these rings affects its commutativity. We then conclude this chapter by giving an example showing that a ring with a prime center is not necessarily commutative.

In the third chapter, we show that rings multiplicatively generated by idempotents and nilpotents might undergo a change in its structure and the structure of some of its subsets when it's given some conditions. Furthermore, we show that a ring R which is either finite or has an identity is necessarily Boolean when given some property; we then give an example which shows that the finiteness of R and the existence of its identity along with this property are essential to prove that R is Boolean.

In the final chapter, we show how putting some conditions on subsets that are multiplicatively generated by idempotents and nilpotents of a ring might alter the structure of the ring and its subsets.

CONTENTS

CHAPTER I

INTRODUCTION AND PRELIMINARIES

In this chapter, we will introduce some basic definitions and theorems that will be used throughout the forthcoming chapters.

Definition 1.1. *An element e in a ring R is said to be* ***idempotent*** *if* $e^2 = e$. *A ring R is* ***Boolean*** *if every element of R is idempotent.*

Definition 1.2. *An element a in a ring R is said to be* ***nilpotent*** *if there exists a positive integer n = n (a) such that* $a^n = 0$ *. An ideal I is said to be* ***nil*** *if every element in I is nilpotent. An ideal I is said to be* ***nilpotent*** *if* $I^n = 0$ *for some integer n.*

Definition 1.3. *A nonzero ring R is a* ***prime ring*** *if for any two elements a and b of R, arb = 0 for all r in R implies that either a = 0 or b = 0.*

Definition 1.4. *An element x of a ring R is called* ***periodic*** *if there exist distinct positive integers m, n such that* $x^m = x^n$. *A ring R is called* ***periodic*** *if each of its elements is periodic.*

Definition 1.5. *An element a of a ring R is said to be a* ***central*** *element iff* $ax = xa \ \forall x \in R$. *The set of all central elements is called the* ***center*** *of R and is denoted by Z(R) or C(R).*

Definition 1.6. *A ring R with identity is called a* ***division ring*** *if every nonzero element is a unit. A commutative division ring is called a* ***field.***

Definition 1.7. *A ring R with no zero divisors is called a* ***domain.*** *A commutative domain is called an* ***integral domain****.*

Definition 1.8. *In a ring R, the ideal generated by all commutators [x, y] = xy - yx in R is called the* ***commutator ideal*** *of R.*

Definition 1.9. *A ring R is said to be left (right)* ***Artinian*** *if it satisfies the descending chain condition on left (right) ideals of R. A ring R is Artinian if it is both left and right Artinian.*

Theorem 1.1. *A nonzero ring R is an Artinian ring if and only if every nonempty set of ideals has a minimal element. In particular, R has a nonzero minimal ideal.*

Proof. ($\Rightarrow$)

Let R be an Artinian ring, and let A be a nonempty set of ideals in R. Let $I_1 \in A$. Suppose that A has no minimal element, then there exists $I_2 \in A$ such that $I_1 \supset I_2$.
Similarly, I_2 is not minimal in A, then there exists an ideal $I_3 \in A$ such that $I_2 \supset I_3$. We continue in this manner to get a strictly decreasing chain of ideals in R:

$$I_1 \supset I_2 \supset I_3 \supset I_4 \supset \cdots$$

Since R is Artinian, then there exists k such that $I_i = I_k$ for all $i \geq k$, contradiction.
So, A has a minimal element.

($\Leftarrow$)

Assume that every nonempty set of ideals in R has a minimal element.

Let $I_1 \supseteq I_2 \supseteq I_3 \supseteq I_4 \supseteq \cdots$ be a descending chain of ideals of R. Choose S to be the set consisting of these ideals, then S has a minimal element, let it be I_k. By assumption for any $n \geq k, I_n \subseteq I_k$. But, I_k is the minimal element then $\forall n \geq k, I_n = I_{k.}$ Then R satisfies the descending chain condition and thus is Artinian.

Definition 1.10. *An element $a \in R$ is* ***left quasi-regular*** *if there exists r ∈ R such that $r + a + ra = 0$. Similarly, an element $a \in R$ is* ***right quasi-regular*** *if there exists r ∈ R such that $a + r + ar = 0$. An ideal I is left (right) quasi-regular if every element of I is left (right) quasi- regular.*

Definition 1.11. *A left ideal I in a ring R is said to be* ***regular*** *if there exists $e \in R$ such that $r - re \in I$ for every $r \in R$. Similarly, a right ideal I in a ring R is said to be* ***regular*** *if there exists e ∈ R such that $r - er \in I$ for every $r \in R$.*

Definition 1.12. *A left module A over a ring R is said to be* ***simple*** *iff RA $\neq 0$ and A has no proper submodules. A ring R is simple iff $R^2 \neq 0$ and R has no proper two-sided ideals.*

Definition 1.13. *Let B be a subset of a left R- module A. Then, the left* ***annihilator*** *of B is Ann(B) = $\{r \in R \mid rb = 0$ for all $b \in B\}$. If B is a submodule of A, then Ann(B) is an ideal of R.*

Definition 1.14. *A (left) R-module A is called a* ***faithful*** *module if the (left) annihilator of A, Ann(A), is equal to {0}. A ring R is said to be (left)* ***primitive*** *ring if there exists a simple faithful R – module.*

Theorem 1.2. *If R is a ring, then there is an ideal J(R) such that:*

1. *J(R) is the intersection of all regular maximal left ideals of R;*
2. *J(R) is a left quasi- regular left ideal which contains every left quasi- regular left ideal of R;*
3. *J(R) is the intersection of all left annihilators of simple left R-modules;*
4. *J(R) is the intersection of all the left primitive ideals of R;*

Note: Statements 1-4 are true if “left” is replaced by “right”. These statements are all equivalent and they define the ideal J(R) called the ***Jacobson radical***.

Proof. [9, p.426]

Theorem 1.3. *The Jacobson radical J(R) of a ring R contains no nonzero idempotent elements.*

Proof. Let a be an idempotent element in $J = J(R)$, we want to show that $a = 0$. Since $a \in J$, then $-a \in J$. Therefore, $-a$ is left quasi-regular and we get $r - a - ra = 0$ for some r in R. Hence, $a = r - ra$. Then, $a^2 = ra - ra^2$ but a is idempotent and thus $a = ra - ra = 0$.

Theorem 1.4. *If R is a left (right) Artinian ring, then the Jacobson radical of R is nilpotent.*

Proof. Let J = J(R). Consider the chain of left ideals in R:

$$J \supseteq J^2 \supseteq J^3 \supseteq \cdots$$

Since R is left Artinian then there exists k such that $J^i = J^k \ \forall\ i \geq k$.

Suppose $J^k \neq 0$. Let $C = \{\ I \neq \{0\} | I$ is a left ideal of $R\ satisfying\ J^k . I \neq \{0\}\ \}$;

$C \neq \phi$ since $J^k.J^k = J^k \neq \{0\}$.

Since R is left Artinian, then C has a minimal element $M \neq \{0\}$ and so $J^k.a \neq \{0\}$ for some $a \neq 0$ in M. So, there exists $r \in J^k$ such that $ra = a$.

Since $r \in J^k$, then $-r \in J^k$ which gives that $-r$ is left quasi-regular (since $J^k \subseteq J$).

Then, $s - r - sr = 0$ for some $s \in R$ and $sa - ra - sra = 0$. But $ra = a$ and hence $a = 0$, contradiction. Therefore, $J^k = \{0\}$ and J is nilpotent.

Lemma 1.1. *Let R be a ring with identity 1. Let J be the Jacobson radical of R, let a be an element of J, then (a+1) is a unit.*

Proof. Since $a \in J$ then a is left quasi-regular. So, there exists b ∈ R such that

$b + a + ba = 0$. Therefore, $(b + 1)(a + 1) = ba + b + a + 1 = 0 + 1 = 1$. Hence, $(b + 1)$ is the inverse of $(a + 1)$.

Lemma 1.2. *Let R be a ring. If r is both idempotent and nilpotent in R, then r = 0.*

Proof. Let r be an element of R which is both nilpotent and idempotent, assume $r \neq 0$.

Since r is nilpotent, let $n \geq 2$ be the least positive integer such that $r^n = 0$; hence, $r^{n-2}.r^2 = 0$ but r is idempotent i.e., $r^2 = r$. Then, $r^{n-1} = 0$, this contradicts the fact that n is the least positive integer satisfying $r^n = 0$. As a consequence, $r = 0$.

Definition 1.15. *A ring R is said to be* ***semisimple*** *if J(R) = 0.*

Theorem 1.5. *(Wedderburn-Artin) The following conditions on a left Artinian ring R are equivalent.*

(i) *R is simple;*

(ii) *R is primitive;*

(iii) *R is isomorphic to the endomorphism ring of a nonzero finite dimensional vector space V over a division ring D.*

(iv) *For some positive integer n, R is isomorphic to the ring $Mat_n D$ of all n×n matrices over a division ring D.*

Proof. [9, p.421].

Theorem 1.6. *(Wedderburn-Artin). The following conditions on a ring R are equivalent.*

(i) *R is a nonzero semisimple left Artinian ring;*

(ii) *R is a direct product of a finite number of simple ideals each of which is isomorphic to the endomorphism ring of a finite dimensional vector space over a division ring;*

(iii) *there exist division rings $D_1, \dots, D_t$ and positive integers $n_1, \dots, n_t$ such that R is isomorphic to the ring $Mat_{n_1} D_1 \times Mat_{n_2} D_2 \times \dots \times Mat_{n_t} D_t$.*

Proof. [9, p.436]

Theorem 1.7. *Let R be a semisimple left Artinian ring, then R has an identity.*

Proof. If R is a semisimple left Artinian ring, then by Theorem 1.6, there exist division rings $D_1, D_2, \dots, D_t$ and positive integers $n_1, n_2, \dots, n_t$ such that:

$$R \cong Mat_{n_1}D_1 \times Mat_{n_2}D_2 \times \dots Mat_{n_t}D_t$$

Where $Mat_{n_i}D_i$ is the complete matrix ring over the division ring D_i. Since each matrix ring has an identity, then R has an identity.

Theorem 1.8. *Let R be a ring. Then, the quotient ring R/J(R) is semisimple.*

Proof. Let J = J(R). We want to show that $J(R/J) = 0$. We consider the canonical epimorphism, $\pi: R \longrightarrow R/J$ defined by $\pi(r) = r + J = \bar{r}$; and let A be the collection of all regular maximal left ideals of R.

By definition of $J(R)$, $J(R) \subseteq I$ for all $I \in A$.

I/J is a maximal left ideal of R/J because I is a maximal ideal in R. Since I is regular, then there exists an element $e \in R$ with $r - re \in I$ for all r in R. We want to show I/J is regular. Let $\bar{r} \in \bar{R}$, then

$$\bar{r} - \bar{r}.\bar{e} = \pi(r - re) \in \pi(I) = I/J \qquad \forall\, \bar{r} \in \bar{R}.$$

So, I/J is a regular maximal left ideal of R/J.

If $\bar{r} \in \bigcap\{\, \pi(I) \mid I \in A \,\}$, then, $\bar{r} \in \bigcap\{\, I/J \mid I \in A \,\}$. Hence, $r \in I$ for each $I \in A$ and $r \in J(R)$. So, $\bar{r} = 0$ in R/J, and thus $J(R/J) = 0$. As a result, R/J is semisimple.

CHAPTER II

RINGS WITH PRIME CENTERS

In this chapter, the structure of certain classes of rings with prime centers and the relation of this structure to commutativity is going to be studied. Additionally, an example of a non-commutative ring with a prime center is going to be demonstrated.

Throughout this chapter, R is an associative ring.

Definition 2.1. *A ring is said to have a* ***prime center C*** *if whenever ab*$\in C, then$ $a \in C \; or \; b \in C.$

Definition 2.2. *A ring is said to have a* ***semiprime center C*** *if whenever* $x^n \in C, then$ $x \in C.$

Lemma 2.1. *If R is a periodic ring, then for each x in R, some power of x is idempotent* $(\, i.e \; \exists \; a \; positive \; integer \; k = k(x) such \; that \; (x^k)^2 = (x^k))$

Proof. If $x \in$ R, then $x^m = x^n$ for some positive integers m = m(x) and n= n(x); without loss of generality consider n > m. Then, $x^m = x^{m+1}.x^{n-m-1}$

(since $n = m + 1 + n - m - 1$)

$$\begin{aligned} x^m &= x^m.x.x^{n-m-1} \\ &= (x^{m+1}.x^{n-m-1}).x.x^{n-m-1} \\ &= x^{m+1}.x^{n-m}.x^{n-m-1} \end{aligned}$$

$$= (x^{m+1}.x).(x^{n-m-1})^2$$

$$= x^{m+2}.x^{2(n-m-1)}$$

Now repeat the same process a second time to gain: $x^m = x^m.x^2.x^{2(n-m-1)}$

$= (x^{m+1}.x^{n-m-1})x^2.x^{2(n-m-1)} = x^{m+3}.x^{3(n-m-1)}$

Repeating the same process until we obtain:

$$x^m = x^{m+m}.x^{m(n-m-1)} = x^{2m}.\left(x^{(n-m-1)}\right)^m$$

Then, $x^m.\left(x^{(n-m-1)}\right)^m = x^{2m}.\left(x^{(n-m-1)}\right)^m.\left(x^{(n-m-1)}\right)^m$

$$= \left(x^m.\left(x^{(n-m-1)}\right)^m\right)^2$$

Therefore, $x^m.\left(x^{(n-m-1)}\right)^m$ is idempotent. Thus, k(x) is a function of n(x) and m(x) and $k = m + m(n-m-1) = m + mn - mm - m = mn - m^2$

Hence, $(x^k)^2 = \left(x^{m+m(n-m-1)}\right)^2 = \left(x^{mn-m^2}\right)^2 = x^{mn-m^2} = x^k$.

Note 2.1. *Every commutative ring has a prime center.*

Proof. Let R be a commutative ring. Let C be the center of R. Then, obviously C = R;

Consequently, $xy \in C$ does imply that $x \in C$ and $y \in C$ since C = R and $x \in R, y \in R$; concluding that C is prime.

Note 2.2. *A prime center is a semi prime center.*

Proof. Let R be a ring with a prime center C. Let $x^n \in C,\ then\ x^{n-1}.x \in C,\ then\ x^{n-1} \in C\ or\ x \in C$ (since C is prime). If $x \notin C$ then $x^{n-1} \in C$ and then repeat the same process to reach $x \in C$.

Lemma 2.2. *Let R be a ring having a semiprime center C. Then the nilpotent and the idempotent elements of R belong to the center.*

Proof. Let a be any nilpotent element of R. Then, $a^n = 0$ for some positive integer n. Consequently, $a^n = 0 \in C$. But R has a semiprime center C, so if $a^n \in C$ then $a \in C$. Thus, all nilpotents of R are in C.

Now, let e be any idempotent element of R, then, $e^2 = e.$ Let x be any element in R. Consider $ex - exe$.

$$\begin{aligned}(ex - exe)^2 &= (ex - exe)(ex - exe)\\ &= exex - exexe - exe^2x + exe^2xe\\ &= exex - exexe - exex + exexe\\ &= 0\end{aligned}$$

Thus, $ex - exe$ is nilpotent and hence belongs to C.

Then,
$$\begin{aligned}e(ex - exe) &= (ex - exe)e\\ e^2x - e^2xe &= exe - exe^2\\ ex - exe &= exe - exe\\ ex &= exe\end{aligned}$$

Similarly, $xe - exe$ is nilpotent and thus belongs to C.

Then, $$e(xe - exe) = (xe - exe)e$$
$$exe - e^2xe = xe^2 - exe^2$$
$$exe - exe = xe - exe$$
$$exe = xe$$

As a result, $ex = xe$, concluding that $e \in C$.

Theorem 2.1. *Let R be a periodic ring. R is commutative iff R has a semiprime center.*

Proof.

($\Longrightarrow$)

If R is commutative, then R has a prime center, but every prime center is semiprime, thus R has a semiprime center.

($\Longleftarrow$)

Suppose that R has a semiprime center, and let x be any element of R. Since R is periodic, then there exists a power of x which is idempotent (Lemma 2.1). Let k be this positive integer power. Therefore, $(x^k)^2 = x^k$ and hence $x^k \in C$ (Lemma 2.2). Thus $x \in C$ since C is semiprime. Then R ⊆ C, but we know that C ⊆ R. We conclude that R = C and thus R is commutative.

Lemma 2.3. *Let R be a ring with identity 1 and having a prime center C. Let U be the set of units of R. Then U ⊆C.*

Proof. Let $u \in U$. Then $u.u^{-1} = 1 \in C$. But R has a prime center C, this implies that $u \in C \; or \; u^{-1} \in C$, and hence $u \in C$. Concluding that $U \subseteq C$.

Lemma 2.4. *Let R be a ring with identity 1 and having a prime center C. Let J be the Jacobson radical of R. Then* $J \subseteq C$.

Proof. Let $a \in J$. So, a is a non-unit, thus $a + 1 \notin J$ implying that $a + 1$ is a unit (Lemma 1.1) and thus central by lemma 2.3. Then $a \in C$ since $a = (a + 1) - 1$ where $(a + 1) \in C$ and $1 \in C$. Consequently, $J \subseteq C$.

Lemma 2.5. *Let R be a prime ring having a semiprime center. If e is an idempotent of R then e = 0 or e = 1 (if R has an identity 1).*

Proof. Let e be an idempotent of R. Then, $e \in C$ (Lemma 2.2). So,

$$eR(ex - x) = Re(ex - x) = R(e^2x - ex) = R(ex - ex) = 0 \;\; \forall \, x \in R$$

This implies, since R is a prime ring, that either $e = 0$ or $ex - x = 0$. So, $e = 0$ or $ex = x, \forall \, x \in R$. If $e \neq 0$, then $ex = x \; \forall x \in R$. But $e \in C$ thus, $ex = xe = x \; \forall \, x \in R$ implying that e is an identity element of R.

Theorem 2.2. *If R is a prime ring with a prime center C, then R is a domain.*

Proof. Let $ab = 0$ where $a \in R \; and \; b \in R$. Then, $ab \in C$, but C is prime, so $a \in C \; or \; b \in C$. Thus, $aRb = 0 \;\; since \; (aR)b = (Ra)b = R(ab) = R.0 = 0$. Now, since R is a prime ring this implies that $a = 0$ or $b = 0$. As a consequence, R has no zero divisors and thus a domain.

Theorem 2.3. *If R is an Artinian ring and I is a nonzero non-nilpotent ideal then I contains a nonzero idempotent element.*

Proof. [8, Theorem 1.5.2]

Theorem 2.4. *Let R be a prime Artinian ring with identity 1. If R has a prime center then R is a field.*

Proof. Let I be a nonzero ideal of R. Then I is non-nilpotent, since if I were nilpotent then for every nonzero $x \in I, \exists\, n$ such that $x^n = 0.$ But $0 \in C$, then $x^n \in C$, thus, $x \in C$ since C is semiprime; consequently, $xRx^{n-1} = Rx^n = 0$, hence, $x = 0 \; or \; x^{n-1} = 0$ for R is a prime ring. If $x \neq 0$, then, $x^{n-1} = 0 \;\; so \; x = 0 \; or \; x^{n-2} = 0$ continuing in this manner we reach $x = 0$, contradicting the fact that I is a nonzero ideal. Thus, since R is Artinian, I contains a nonzero idempotent element (By Theorem 2.3). So, by Lemma 2.5, 1 ∈ I and hence I = R. Subsequently, R has no nonzero proper two sided ideals and thus R is simple. Now, R is a simple Artinian ring and hence is isomorphic to a complete matrix ring $Mat_n D$ over a division ring D (By Theorem 1.5). However, no matrix ring $Mat_n D$ over a division ring D with $n > 1$ can have a prime center. ($E_{11}.E_{22} = 0 \in C$ but, $E_{11} \notin C \; and \; E_{22} \notin C$).

So, n = 1 thus R must be a division ring. By Lemma 2.3, the units of R are central and hence R is commutative. Therefore, R is a commutative division ring and thus a field.

Lemma 2.6. *Let \{ R_i , $i \in \Gamma$ \} be a family of Rings. If the direct product $\prod_{i\in\Gamma} R_i$ has a prime center then R_i has a prime center for each $i \in \Gamma$.*

Proof. Let C be the center of $\prod_{i\in\Gamma} R_i$, C_i be the center of R_i, $\forall\, i \in \Gamma$, let a_j and b_j be two elements of R_j ($j \in \Gamma$) such that $a_j b_j \in C_j$. Let $\{a_i\}$ and $\{b_i\}$ be two elements $\in \prod_{i\in\Gamma} R_i$ such that:

$$a_i = \begin{cases} 0 & if\ i \neq j \\ a_j & if\ i = j \end{cases} \quad \text{and} \quad b_i = \begin{cases} 0 & if\ i \neq j \\ b_j & if\ i = j \end{cases}$$

Thus $\{a_i\}.\{b_i\} = \begin{cases} 0 & if\ i \neq j \\ a_{j.}b_j & if\ i = j \end{cases}$

But $0 \in C_i\ \forall i$ and $a_j.b_j \in C_j$ (the center of R_j). Thus, $\{a_i\}.\{b_i\} \in C$, so $\{a_i\} \in C$ or $\{b_i\} \in C$ since C is prime. Therefore, $a_j \in C_j$ or $b_j \in C_j$. Hence, C_j is prime. So, R_j has a prime center for each $j \in \Gamma$.

Theorem 2.5. *Let R be a semisimple Artinian ring. If R has a prime center, then R is isomorphic to a direct product of fields.*

Proof. Since R is semisimple Artinian then it is isomorphic to a complete direct product $Mat_{n_1}D_1 \times Mat_{n_2}D_2 \times \ldots \times Mat_{n_t}D_t$ where $n_1, n_2, \ldots, n_t$ are positive integers and each $Mat_{n_i}D_i$ is an $n_i \times n_i$ matrix ring over a division ring D_i. Now, R has a prime center implies that $Mat_{n_1}D_1 \times Mat_{n_2}D_2 \times \ldots \times Mat_{n_t}D_t$ has a prime center, thus, each $Mat_{n_i}D_i$ for $i \in \{1, \ldots, t\}$ has a prime center (by Lemma 2.6). But in the proof of Theorem 2.3, it was shown that this cannot happen unless each $n_i = 1$, thus $n_i = 1\ \forall\ i \in \{1, \ldots, t\}$. Therefore, R is isomorphic to a direct product of division rings with prime centers. But each division ring D_i is a ring with unity and with a prime center; hence, by Lemma 2.3, all the units of D_i are central. As a consequence, all elements of D_i are central, implying that D_i is commutative, hence, D_i is a field. Therefore, R is isomorphic to a direct product of fields.

Theorem 2.6. *Let R be a simple ring with identity 1 and having a prime center. Then R is a domain.*

Proof. Let a be a nonzero element of C (center of R). Then, aR is a nonzero ideal of R $(1 \in R)$. R is simple, so it has no proper two sided ideals implying that $aR = Ra = R$. However, $1 \in R$ thus $\exists\, a^{-1} \in R$ such that $a.a^{-1} = a^{-1}.a = 1 \in R$. Thus, a must be a unit and hence every nonzero element of C must be a unit. Now, assume that R has zero divisors, then, $u.v = 0$ for some $u \neq 0\,, v \neq 0$. But, 0 belongs to the prime center C of R, which implies that $u.v \in C$. As a result, $u \in C$ or $v \in C$; therefore, u is a unit or v is a unit since every non-zero element in C must be a unit. Consequently, $\exists u^{-1}$ such that $u^{-1}.u = u.u^{-1} = 1$.

$$u.v = 0$$

$$u^{-1}.u.v = u^{-1}.0$$

$$1.v = 0$$

$$v = 0$$

Contradiction, since $v \neq 0$. Thus, R can't have zero divisors which makes it a domain.

Theorem 2.7. *Let R be a ring with identity and having a prime center C. If for each $x \in R, \exists$ a monic polynomial $P = P_x$ with integer coefficients such that $P_x(x) \in C$, then R is commutative.*

Proof. We start by proving that if $x \in R$ with $P_x(x) \in C$, then $x \in C$. We will do this by induction on n the degree of P_x.

If n = 1 and $x \in R$ with $P_x(x) \in C$ then $P_x(x) = x + a_n \in C$ where a_n is an integer. So, $x \in C$. Now, assume that for all $x \in R$ with $P_x(x)$ of degree n belongs to C implies x belongs to C is true for n. We want to prove it for n+1.

Let $y \in R$, such that $P_y(y) = y^{n+1} + a_n y^n + \cdots + a_1 y + a_0 \in C$ where $a_0, a_1, \ldots, a_n \in \mathbb{Z}$. Then, $y^{n+1} + a_n y^n + \cdots + a_1 y \in C$. Therefore, $y(y^n + a_n y^{n-1} + \cdots + a_1) \in C$. But C is prime; hence, $y \in C$ or $y^n + a_n y^{n-1} + \cdots + a_1 \in C$. If $y \in C$ we are done, else $y^n + a_n y^{n-1} + \cdots + a_1 \in C$; then, y has a polynomial of degree n which belongs to C, hence, $y \in C$ (by the inductive hypothesis) and thus proved for degree n+1.

Example of a noncommutative ring with a prime center:

Let F be an infinite field, let σ be an automorphism of F with infinite order. Let $F[x, \sigma]$ be the ring of all polynomials $p(x)$ over F such that $x^n a = \sigma^n(a) x^n \ \forall\, a \in F, \forall n \in \mathbb{Z}^+$. $F[x, \sigma]$ can be easily proved a domain.

Now, let R = $F[x, \sigma]x$. We will prove that this R is a noncommutative ring with a prime center.

Let C be the center of R, let $P(x) = a_1 x + a_2 x^2 + \cdots + a_n x^n$ be any nonzero element in the center of R.

$$x.P(x) = x a_1 x + x a_2 x^2 + \cdots + x a_n x^n$$

$$= \sigma(a_1) x.x + \sigma(a_2) x.x^2 + \cdots + \sigma(a_n) x.x^n$$

$$= \sigma(a_1)x^2 + \sigma(a_2)x^3 + \cdots + \sigma(a_n)x^{n+1}$$

$$P(x).x = a_1.x.x + a_2.x^2.x + \cdots + a_n.x^n.x$$

$$= a_1.x^2 + a_2.x^3 + \cdots + a_n.x^{n+1}$$

But $P(x) \in C$, then $x.P(x) = P(x).x$, therefore,

(i) $\sigma(a_1) = a_1 \quad \sigma(a_2) = a_2 \quad \ldots \quad \sigma(a_n) = a_n$.

σ has an infinite order (i.e. σ^i is not the identity automorphism for $i < \infty$). Hence, $\forall i \in \mathbb{Z}^+, \ \exists a \in F$ such that:

(ii) $\sigma^i(a) \neq a$.

$axP(x) = a\sigma(a_1)x^2 + a\sigma(a_2)x^3 + \cdots + a\sigma(a_n)x^{n+1} = aa_1x^2 + aa_2x^3 + \cdots + aa_nx^{n+1}$ (By part (i)). In addition,

$$P(x)ax = a_1xax + a_2x^2.ax + \cdots + a_nx^nax$$

$$= a_1\sigma(a)x^2 + a_2\sigma^2(a)x^3 + \cdots + a_n\sigma^n(a)x^{n+1}$$

But $axP(x) = P(x)ax$ since $P(x) \in C$. Thus:

(iii) $aa_1 = a_1\sigma(a), \ aa_2 = a_2\sigma^2(a), \ldots aa_n = a_n\sigma^n(a)$

F is a field, assume $P(x) \neq 0$. Then $a_i \neq 0$ for some positive integer i. Let a be an element of F satisfying $\sigma^i(a) \neq a$. Thus, $a_i\sigma^i(a) = aa_i$ by (iii). Then, $a_i\sigma^i(a) = a_ia$ (F is a field then it is a commutative ring where the nonzero elements are units, hence, for $a, a_i \in F \quad aa_i = a_ia$ and a, a_i are units)

$$a_i^{-1}a_i\sigma^i(a) = a_i^{-1}a_i a$$

$$\sigma^i(a) = a$$

But this contradicts with (ii). As a result, $P(x) = 0$, then the center C = 0. If $p(x).q(x) \in C$ for $p(x), q(x) \in R$ then $p(x).q(x) = 0$ which implies that $p(x) = 0$ or $q(x) = 0$ (since $C \subset R$ which is a domain thus has no zero divisors); therefore, $p(x) \in C$ or $q(x) \in C$ concluding that C is prime. And so, R has a prime center C. R is non-commutative since $xa = \sigma(a)x \neq ax$. Consequently, R is a non-commutative ring with a prime center.

CHAPTER III

RINGS WHICH ARE MULTIPLICATIVELY GENERATED BY IDEMPOTENTS

A Boolean ring is a ring where every element is idempotent. This motivates the study of the structure of a ring R which is multiplicatively generated by its idempotents and rings which are multiplicatively generated by idempotents and nilpotents. Indeed, we show that if R is finite or has an identity along with this property, then it is necessarily Boolean. Afterwards, we give an example to show that to prove R Boolean, the finiteness of R and the existence of its identity along with the above property cannot be omitted.

Definition 3.1. *A ring R is called an **I-ring** if it is multiplicatively generated by its idempotent elements.*

Lemma 3.1. *Let R be a Boolean ring. Then char(R) = 2.*

Proof. Let $x \in R$. Then $x^2 = x$ and $(x+x)^2 = (x+x)$ which implies that $x^2 + 2x + x^2 = x + x$ and hence $2x = 0$. Thus, $char(R) = 2$. Then, $x = -x\ \forall x \in R$.

Theorem 3.1. *If a ring R is Boolean, then R is commutative.*

Proof. Let $x, y \in R$; we want to show that $xy = yx$. Since R is Boolean, then $x^2 = x$ and $y^2 = y$. Now,

$$x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y.$$

Then, $xy = -yx$. But by Lemma 3.1, $-y = y$; therefore, $xy = yx$.

Lemma 3.2. *Let R be an I-ring, let* $b \in R$. *If the idempotents of R are central then b is idempotent.*

Proof. Since R is an I-ring, and $\mathrm{b} \in \mathrm{R}$, then $\mathrm{b} = \mathrm{e}_1\mathrm{e}_2 \ldots \mathrm{e}_\mathrm{n}$ where e_i is idempotent for every $\mathrm{i} \in \{1, \ldots \mathrm{n}\}$. Hence,

$b^2 = (e_1e_2 \ldots e_n)(e_1e_2 \ldots e_n) = (e_1)^2(e_2)^2 \ldots (e_n)^2 = e_1e_2 \ldots e_n =$ b. Thus, b is idempotent.

Theorem 3.2. *Let R be an I-ring with identity 1. Then R is Boolean.*

Proof. Let $b \in R$ then $b = e_1e_2 \ldots e_n$ where e_i is idempotent for every $i \in \{1, \ldots n\}$.To prove R is Boolean, we need to show that b is idempotent; so, it is enough to show that the idempotents are central (Lemma 3.2). Thus, assume that $e^2 = e \in R, x \in R$ and let $a = ex - exe$, then, $a^2 = 0$ as seen before (p.10-11) and hence $1 + a$ has an inverse in $R \ since \ (1 + a)(1 - a) = 1 - a + a - a^2 = 1$.

By hypothesis, $1 + a = e_1e_2 \ldots e_n$ where e_i is idempotent $\forall i \in \{1, \ldots, n\}$; hence, $e_1(1 + a) = e_1e_1e_2 \ldots e_n = e_1^2e_2 \ldots e_n = e_1e_2 \ldots e_n = 1 + a$. However, $(1 + a)^{-1}$ exists, thus, $e_1(1 + a)(1 + a)^{-1}$ =$(1 + a)(1 + a)^{-1} = 1$. So, $e_1 = 1$. Similarly, $e_i = 1 \ \forall i$ thus $1 + a = 1$ and hence $a = 0$. Therefore, $ex = exe$.

In a similar manner taking $a = xe - exe,$ we can show that $a = 0,$ thus $xe = exe$ which implies that $ex = exe = xe$ and hence e is central. Therefore, R is Boolean.

At the end of this chapter, example 3.1 will show why the condition $1 \in R$ *cannot be dropped from Theorem 3.2.*

Theorem 3.3. *Let R be a finite I-ring. Then R is Boolean.*

Proof. We will proceed by proving this theorem by contradiction. So, suppose that R is a finite I-ring which is not Boolean. Since R is finite, we can consider R not Boolean with least number of elements. That is, any I-ring with fewer elements than R must be Boolean. It is obvious that $R \neq \{0\}$ else R would be Boolean contradicting our assumption. Let J be the Jacobson Radical of R. If J = {0}, then R is semisimple and thus has an identity by Theorem 1.7. Thus, by Theorem 3.2, R is Boolean, contradicting our hypothesis, so $J \neq \{0\}$. Now, since R is Artinian then R has a minimal ideal M_0 by Theorem 1.1. Let $x + M_0$ be an element of R/M_0. Since R is an I-ring then:

$x + M_0 = e_1 e_2 \dots e_n + M_0 = (e_1 + M_0)(e_2 + M_0) \dots (e_n + M_0)$ where e_i is idempotent $\forall i \in \{1, \dots, n\}$. Note that $(e_i + M_0)^2 = (e_i + M_0)(e_i + M_0) = (e_i)^2 + M_0 = (e_i + M_0)$ thus $(e_i + M_0)$ is idempotent $\forall i$, and hence any element in R/M_0 is a product of idempotents, thus R/M_0 is an I- ring with fewer elements than R(since $M_0 \neq 0$). Therefore, since by assumption R is the smallest non-Boolean I-ring then R/M_0 is Boolean. R/M_0 Boolean implies that J/M_0 is Boolean since J/M_0 is a subring of R/M_0, but J is nilpotent (Theorem 1.4) and hence J/M_0 is nilpotent. Hence, every element in J/M_0 is nilpotent and idempotent thus every element of J/M_0 is zero (Lemma 1.2) and hence $M_0 =$ J. Thus, J is the (unique) minimal ideal of R. Since R is finite, J is nilpotent, so ∃ a positive integer $k > 1$ such that $\mathrm{J}^{\mathrm{k}} = 0$. Hence, $\mathrm{J}^2 \neq \mathrm{J}$ since if $\mathrm{J}^2 = \mathrm{J}$, then, by a simple inductive proof it can be shown that $\mathrm{J}^{\mathrm{k}} = \mathrm{J}$. This implies that $\mathrm{J} = \mathrm{J}^{\mathrm{k}} = 0$, contradiction. It follows then that $\mathrm{J}^2 = \{0\}$ since $\mathrm{J}^2 \subset \mathrm{J}$ and J is minimal. Since, as shown above R/J is Boolean, then R/J is commutative (Theorem 3.1) and thus

$$xy - yx \in J, \forall\, x, y \text{ } in\ R. \tag{1}$$

Furthermore, if J = R, then R has no nonzero idempotent elements (Theorem 1.3), but R is an I-ring thus R = {0}, a contradiction. Hence, J ≠ R, thus R/J has an identity since it is semisimple and finite (Theorem 1.7). Let $\bar{u} = u + \mathrm{J}$ be the identity element of $\mathrm{R/J}$. Since R is finite, then, for every $x \in R$, there exists m and n such that $x^m = x^n$, for $m > n$. Then,

$$x^n = x^{n+1}.x^{m-n-1}$$

$$= x^n.x.x^{m-n-1}$$

$$= x^m.x.x^{m-n-1}$$

$$= x^{n+1}.x^{m-n-1}.x.x^{m-n-1}$$

$$= x^n.x^2.(x^{m-n-1})^2.$$

Repeating the above procedure, we get $x^n = x^{2n}(x^{m-n-1})^n$. Now, let

$e = x^n(x^{m-n-1})^n$. Then,

$$e^2 = x^n(x^{m-n-1})^n.x^n.(x^{m-n-1})^n$$

$$= x^{2n}(x^{m-n-1})^n(x^{m-n-1})^n$$

$$= x^n(x^{m-n-1})^n$$

$$= e.$$

So, e is an idempotent element. But $e = x^n(x^{m-n-1})^n$. Then $x^k = e$ for some integer $k \geq 1$. Thus, there exists a positive integer b such that

$$u^b = e \tag{2}$$

where e is an idempotent element of R. Since R/J is Boolean then $\bar{e} = \bar{u}^b = \bar{u}$= identity element of R/J. Therefore,

$$ex - x \in \text{J} \; \forall \, x \in R \tag{3}$$

since $\forall x \in R, \overline{ex - x} = \overline{ex} - \bar{x} = \bar{e}.\bar{x} - \bar{x} = \bar{u}.\bar{x} - \bar{x} = \bar{x} - \bar{x} = \bar{0}$. Similarly,

$$xe - x \in \text{J} \; \forall \, x \in R \tag{4}$$

Now, let x be an arbitrary but fixed element of R and let $r \in R$, then by (1), we have that $xr = rx + j$ for some $j \in$ J. Therefore, J$xr \subseteq$ J$rx +$ J$j \subseteq$ Jx since $\text{J}^2 = \{0\}$. It follows then, for any $x \in R$, Jx is an ideal in R. But J is a minimal ideal of R, and hence

$$Jx = \{0\} \text{ or J}x = \text{J for any given } x \in R\,. \tag{5}$$

Similarly,

$$x\text{J} = \{0\} \text{ or } x\text{J} = \text{J for any given } x \in R\,. \tag{6}$$

Returning to the idempotent element e in (2), we now prove that

$$e\mathrm{J} \neq \{0\} \tag{7}$$

Assume $e\mathrm{J} = \{0\}$, and let $x \in R$. Then, by (4), $x = xe + j$ for some $j \in \mathrm{J}$, and hence,

$$x\mathrm{J} \subseteq xe\mathrm{J} + j\mathrm{J} = \{0\}$$

Since $e\mathrm{J} = \{0\}$ and $\mathrm{J}^2 = \{0\}$. We have thus shown that

$$x\mathrm{J} = \{0\} \text{ for all } x \in R\,. \tag{8}$$

Now, we consider two idempotent elements of R, g and h. Using (1), we have $gh - hg \in \mathrm{J}$ and using (8), we get $g(gh - hg) = 0$. Therefore, $g^2h - ghg = 0$ and $gh = ghg$. Then,

$$(gh)^2 = (gh)(gh) = (ghg)h = (gh)h = gh^2 = gh.$$

In other words, the product of any two idempotent elements is idempotent. But R is an I-ring, which implies that every element in R is a product of idempotents, thus R is Boolean and we get a contradiction. Therefore, $e\mathrm{J} \neq \{0\}$ and similarly we can show that $\mathrm{J}e \neq \{0\}$. Combining (5) and (6) with the above result, we get:

$$\mathrm{J}e = e\mathrm{J} = \mathrm{J} \tag{9}$$

Let $x \in R$, using (4) we have:

$$x = xe + j \text{ for some } j \in \mathrm{J} \tag{10}$$

Now, using (9) we have

$$j = j'e \text{ for some } j' \in \mathrm{J} \tag{11}$$

Combining (10) and (11), we get $xe = (xe + j'e)e = xe + j'e = xe + j$. So, $j = 0$ and by (10), we get $x = xe$. Similarly, we show that $x = ex$ by using J $= e$J.

Hence,

$$xe = ex = x\,, \qquad \forall x \in R.$$

Thus, e is an identity element of R and by using Theorem 3.2, we get that R is Boolean, which contradicts the hypothesis and by this contradiction we end the proof.

Example 3.1. This example shows that Theorem 3.2 might have not been true if R didn't have an identity, and Theorem 3.3 need not be true if R were not finite.

Let R_o be a ring with identity, and let R be the ring of all $\infty \times \infty$ matrices over R_o in which at most a finite number of entries are nonzero. For every $X \in R, \exists$ a finite $n \times n$ matrix A over R_o such that:

$$X = \begin{pmatrix} A & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{where the } 0's \text{ are zero matrices.}$$

Let L, M, and N be the matrices defined by:

$$L = \begin{pmatrix} I_n & I_n & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \qquad M = \begin{pmatrix} 0_n & 0_n & 0 \\ A & I_n & 0 \\ 0 & 0 & 0 \end{pmatrix} \qquad N = \begin{pmatrix} I_n & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

where 0_n is the $n \times n$ zero matrix and I_n is the $n \times n$ identity matrix.

$$L^2 = \begin{pmatrix} I_n & I_n & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} I_n & I_n & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} I_n^2 & I_n^2 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} I_n & I_n & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = L$$

$$M^2 = \begin{pmatrix} 0_n & 0_n & 0 \\ A & I_n & 0 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} 0_n & 0_n & 0 \\ A & I_n & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0_n & 0_n & 0 \\ I_n . A & I_n^2 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0_n & 0_n & 0 \\ A & I_n & 0 \\ 0 & 0 & 0 \end{pmatrix} = M$$

$$N^2 = \begin{pmatrix} I_n & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} I_n & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} I_n^2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} I_n & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = N$$

Thus $L, M,$ and N are idempotents and

$$LMN = \begin{pmatrix} A & I_n & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} I_n & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} A & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = X$$

Then every X in R can be expressed as a product of idempotents. However, the set of nilpotents N' is not an ideal, since: Let $S = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in R$

$T = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in N'$, since $T^2 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

$ST = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \notin N'$, since $(ST)^n = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ $\forall n$ and thus never equal to zero.

Moreover, R is an I- ring which is not commutative and thus not Boolean. This example shows that we cannot drop the hypothesis that $1 \in R$ in Theorem 3.2, or the hypothesis that R is finite in Theorem 3.3.

Lemma 3.2. *Let R be a ring such that the set of nilpotents N is commutative. Then* $ae \in N$ *and* $ea \in N$ *for every* $a \in N$ *and every nonzero idempotent element e in R.*

Proof. Let e be a nonzero idempotent element in R and let $a \in N$. We have that

$(ea - eae)^2 = 0$ as seen before (p.10).

Thus $ea - eae \in N$ but $a \in N$ and N is commutative then

$$a(ea - eae) = (ea - eae)a.$$

Multiplying by e from the left and the right, we get

$$ea(ea - eae)e = e(ea - eae)ae,$$

or

$$eaeae - eaeae = ea^2e - eaeae.$$

Then, $ea^2e - (eae)^2 = 0$ which implies that $ea^2e = (eae)^2$. Now, using induction on n we will prove that $(eae)^{2^n} = ea^{2^n} e$ $\forall$ positive integer n.

For $n = 1$, we already proved that $ea^2e = (eae)^2$ so we are done.

Now, assume the property is true for n i.e. $(eae)^{2^n} = ea^{2^n}e$. We want to prove it true for $n + 1$. We already have that: $(eae)^{2^n} = ea^{2^n}e$ then

$$((eae)^{2^n})^2 = (ea^{2^n}e)^2$$

But we proved that $ea^2e = (eae)^2$ then

$$e(a^{2^n})^2e = \left(ea^{2^n}e\right)^2$$

$$((eae)^{2^n})^2 = e(a^{2^n})^2e$$

$$(eae)^{2^{n+1}} \quad = e(a^{2^{n+1}})e$$

Hence proved for $n + 1$. Now, since a is nilpotent, then, there exists k such that $a^k = 0$. Choose $2^n > k$ to get $(eae)^{2^n} = e(a^{2^n})e = e\left(a^k . a^{2^n - k}\right)e = e. 0. e = 0$, thus $eae \in N$. Since N is commutative, then N is a subring of R. We have $ea - eae \in N$ and $eae \in N,$ then $ea \in N$. Similarly, we can show that $ae \in N$.

Theorem 3.4. *Let R be a ring in which every element is either idempotent or nilpotent and where the set of nilpotent elements N is commutative. Then N is an ideal of R and R/N is Boolean.*

Proof. Let $a \in N$ and let e be a nonzero idempotent element in R. Since N is commutative, then N is a subring and by Lemma 3.2, $ea \in N$ and $ae \in N$. Now, let $r \in R$ then r is either idempotent or nilpotent. If r is idempotent, then $ra \in N$ and $ar \in N, \forall\, a \in N$. If r is nilpotent, then $ra \in N$ and $ar \in N$ since N is a subring. Therefore, N is an ideal of R.

Now, it remains to show that R/N is Boolean. Let $\bar{x} = x + N \in R/N$ for $x \in R$. By hypothesis, $x = e$ where e is idempotent or $x = a$ where a is nilpotent. Then, either $x + N = e + N$ wich is idempotent in R/N, or $x + N = N$ which is the zero element of R/N. Hence, R/N is Boolean.

CHAPTER IV

RINGS WHERE CERTAIN SUBSETS ARE MULTIPLICATIVELY GENERATED BY IDEMPOTENTS

In this chapter, we study the structure of certain rings with certain subsets that are multiplicatively generated by idempotents motivated by the fact that in a Boolean ring every element is trivially the product of idempotents.

Throughout this chapter, R is a ring, N is the set of nilpotents, C is the center of R, J is the Jacobson radical of R, C(R) is the commutator ideal of R, Z is the ring of integers, and $[x, y]$ denotes the commutator $xy - yx$.

Theorem 4.1. *Let R be a finite ring such that:*

(i) The set R\N is multiplicatively generated by idempotents.

Then N is an ideal of R and R/N is Boolean.

In proving this theorem, Lemmas 4.1, 4.2, and Theorem 4.2 are required:

Lemma 4.1. *If a ring satisfies (i),*

then any homomorphic image of this ring must satisfy (i).

Proof. Let $\phi: R \to R'$ be a surjective homomorphism. We want to prove that if R satisfies (i) then so does R'. Assume that R satisfies (i) and let $x' = \phi(x)$ be any element of R' for some $x \in R$, then $x \in N$ or $x \in R\backslash N$ i.e. $x \in N$ or $x = e_1.e_2 \dots e_n$ where e_i is an idempotent element $\forall i \in \{1, \dots, n\}$ (By (i)). Therefore, $x^m = 0$ for some positive integer m or $x = e_1.e_2 \dots e_n$. Then, $\phi(x^m) = \phi(x)^m = (x')^m = 0$ and hence x' is nilpotent or $x' = \phi(x) = \phi(e_1.e_2 \dots e_n) = \phi(e_1)\phi(e_2) \dots \phi(e_n)$. But, $\phi(e_i)^2 = \phi(e_i^2) = \phi(e_i)$ $\forall\, i \in \{1, \dots, n\}$ concluding that $\phi(e_i)$ is idempotent $\forall i$. Thus, if $x' \in R'\backslash N'$ where N' is the set of nilpotents of R' then x' is a product of idempotents. Hence, R' satisfies (i).

Lemma 4.2. *If the commutator ideal C(R) of a ring R is nil,*

then the set N of nilpotents forms an ideal of R.

Proof. Let $C(R)$ the commutator ideal of R be nil thus $C(R) \subset N$. Consider $R/C(R)$, this is a commutative ring (let $\bar{x}, \bar{y} \in R/C(R)$ then $\bar{x} = x + C(R)$ and $\bar{y} = y + C(R)$ thus $\bar{x}\bar{y} - \bar{y}\bar{x} = xy + C(R) - \left(yx + C(R)\right) = xy - yx + C(R) = C(R)$ since $xy - yx \in C(R)$. Consequently, $\bar{x}\bar{y} - \bar{y}\bar{x} = 0$, then, $\bar{x}\bar{y} = \bar{y}\bar{x}$ which proves that $R/C(R)$is commutative). Now, let $a, b \in N$ then $a^i = 0$ and $b^j = 0$ for some integers i and j. We want to prove that $a + b \in N$. So, we consider $\left(\bar{a} + \bar{b}\right)^n = \sum_{k=0}^{n} \binom{n}{k} (\bar{a})^k (\bar{b})^{n-k}$ since $R/C(R)$ is commutative. We choose n big enough such that for each $k \in \{0,1, \dots, n\}$, either $k \geq i$ or $n - k \geq j$. Then, $(\bar{a})^k \left(\bar{b}\right)^{n-k} = a^k b^{n-k} + C(R) = 0 + C(R) = C(R)$ and thus $\left(\bar{a} + \bar{b}\right)^n =$ 0, hence, $\bar{a} + \bar{b} \in N,$ but $\bar{a} + \bar{b} = a + b + C(R)$ and $C(R) \subset N$, therefore, $a + b \in N.$ It remains to show that $c.a \in N$ for $a \in N$ and $c \in R$. Now, $a \in N$ implies that there exists an integer m such that $a^m = 0$. Consider $\bar{c}.\bar{a}$ where $\bar{c} = c + C(R)$ and $\bar{a} = a + C(R)$, then $(\bar{c}.\bar{a})^m = \bar{c}^m.\bar{a}^m = \bar{c}^m.\left(a^m + C(R)\right) = \bar{c}^m\left(C(R)\right) = C(R)$ since $C(R)$ is an ideal, thus, $\bar{c}.\bar{a} \in N$ and thus $c.a \in N$. We then conclude that N is an ideal.

Theorem 4.2. *Let R be a ring with identity such that R satisfies (i).*

Then R is Boolean.

Proof. Let $a \in N$. Then, $1 + a$ is invertible and $1 + a \notin N$. Thus, by (i), $1 + a = e_1 e_2 \ldots e_k$ where e_i is idempotent $\forall i \in \{1,2, \ldots, k\}$. Multiply both sides from the left by e_1 to get

$$e_1(1 + a) = e_1 e_1 e_2 \ldots e_k$$

$$e_1(1 + a) = e_1^2 e_2 \ldots e_k$$

$$e_1(1 + a) = e_1 e_2 \ldots e_k = 1 + a$$

Multiply both sides from the right by the inverse of $1 + a$ to get

$e_1(1 + a)(1 + a)^{-1} = (1 + a)(1 + a)^{-1}$, hence, $e_1 = 1$.

Similarly, we can show that each $e_i = 1 \; \forall \; i \in \{1, \ldots, k\}$; consequently, $1 + a = 1$ and $a = 0$, this implies that $N = 0$. Thus, R is multiplicatively generated by idempotents. As a consequence, R is Boolean by theorem 3.2.

Proof of Theorem 4.1. Let R be a finite ring satisfying (i)

<u>Case 1:</u>

If J = 0, then R has an identity since it is a finite semisimple Artinian ring (Theorem 1.7). Furthermore, R satisfies (i). Thus, R is Boolean by Theorem 4.2.

Case2:

If J $\neq 0$ and R satisfies (i), then, by Theorem 1.8, R/J is semisimple; in addition, R/J is Artinian (since finite) and thus has an identity (Theorem 1.7). Since R/J is a homomorphic image of R, then, R/J satisfies (i) (Lemma 4.1). As a result, R/J is Boolean (Theorem 4.2). Hence, R/J is commutative and thus $xy - yx \in J\ \forall x, y \in R$. R is Artinian since it is finite, then, J is nil (Theorem 1.4) which implies that $xy - yx$ is in N for every $x, y \in R$. Now, since C(R) is generated by all commutators $xy - yx \in J\ \forall\ x, y \in R$, then C(R) $\subseteq J \subseteq N\ \forall\ x, y \in R$, thus, the commutator ideal is nil and hence N is an ideal by Lemma 4.2.

Now, by (i) for all $x \in R$, $x \in N$ or $x = e_1 \dots e_k$ where $e_i^2 = e_i$, $\forall i \in \{1, \dots, k\}$.

If $x \notin N$ then $x + N = e_1 e_2 \dots e_k + N = (e_1 + N)(e_2 + N) \dots (e_k + N)$. But $(e_i + N)^2 = (e_i + N)(e_i + N) = e_i^2 + N = e_i + N$, therefore, every element $x + N$ in R/N is multiplicatively generated by idempotents, which implies that R/N is Boolean since R/N is finite (Theorem 3.3).

Theorem 4.3. *Let R be a finite ring such that*

(ii) The set R\J is multiplicatively generated by idempotents

then N is an ideal of R and R/N is Boolean.

To prove theorem 4.3, the following Lemmas are needed:

Lemma 4.3. *If a ring satisfies (ii)*

then any homomorphic image of this ring must satisfy (ii)

Proof. Let $\phi: R \to R'$ be a surjective homomorphism, we want to prove that if R satisfies (ii) so does R'. Assume that R satisfies (ii), let $x' = \phi(x)$ be any element of R' for some $x \in R$.

By (ii) either $x \in J$ or $x = e_1 e_2 \dots e_n$ where e_i is an idempotent of R $\forall\, i \in \{1, \dots, n\}$. Let J' denote the Jacobson radical of R', it can be easily proved that $\phi(J) \subseteq J'$, and thus, for all $x' = \phi(x) \in R' = \phi(R)$, either $x \in J$ then $x' = \phi(x) \in \phi(J) \subseteq J'$; or $x = e_1 \dots e_n$, then, $x' = \phi(x) = \phi(e_1 \dots e_n) = \phi(e_1)\phi(e_2) \dots \phi(e_n)$ $\forall i \in \{1, \dots, n\}$. Hence, each $\phi(e_i)$ is idempotent and thus x' is written as a product of idempotents in R'. As a conclusion, R' satisfies (ii).

Lemma 4.4. *Let R be a ring with identity such that R satisfies (ii), then R is Boolean.*

Proof. Let $a \in J$. Then, $a + 1 \notin J$, i.e. $a + 1 \in$ R\J. Therefore, by (ii), $a + 1 = e_1 e_2 \dots e_n$ where e_i is an idempotent for $1 \leq i \leq n$. So, $e_1(a + 1) = e_1^2 e_2 \dots e_n = e_1 e_2 \dots e_n = (a + 1)$ which implies that $e_1 = 1$ since $a + 1$ is invertible. Continuing in this manner, we show that $e_1 = e_2 = \cdots e_n = 1$. Therefore, $a + 1 = 1$ and hence $a = 0$. So, J=0, thus, R/J satisfying (ii) and J being 0 implies that R is multiplicatively generated by idempotents. As a result, R is Boolean by Theorem 3.2.

*Proof of Theorem 4.*3:

Let R be a finite ring satisfying (ii).

Case 1: If J = 0, then R is a semisimple Artinian ring and thus has an identity element (Theorem 1.7). Therefore, R is Boolean by Lemma 4.4 and the theorem follows.

Case 2: Suppose J$\neq 0$. Then by theorem 1.8, R/J is semisimple; in addition, R/J is Artinian and thus has an identity (Theorem 1.7). Furthermore, by Lemma 4.3, R/J satisfies (ii). Therefore, R/J is Boolean by Lemma 4.4. So, R/J is commutative, thus, $xy - yx \in J \; \forall \; x, y \in R$. Now, since C(R) is generated by all commutators $xy - yx \in J \; \forall \; x, y \in R$, then $C(R) \subseteq J \subseteq N$. This implies that C(R) is nil and henceforth N is an ideal of R (by Lemma 4.2).

Since $J \subseteq N$, then, $x \notin N$ implies $x \notin J$ but by (ii) $x = e_1 e_2 \ldots . e_n$ where e_i is idempotent $\forall i$; therefore, $x \notin N$ implies that $x + N = e_1 e_2 \ldots . e_n + N = (e_1 + N)(e_2 + N) \ldots (e_n + N)$ where $(e_i + N)^2 = e_i + N, \; \forall i \in \{1, \ldots, n\}$. Consequently, R/N is multiplicatively generated by idempotents, and since R/N is finite, R/N is Boolean, by Theorem 3.3.

Theorem 4.4. *Let R be a ring with identity 1 satisfying:*

(iii) The set R\C is multiplicatively generated by idempotents.

Then R is commutative.

Proof. Let $x \in R, e \in R$ such that $e^2 = e$, then $a = ex - exe \in N$ (since $a^2 = 0$ (as seen before (p.10) thus a is nilpotent).

Assume $a \notin C$, then $1 + a \notin C$, hence, $1 + a \in R \backslash C$.

So by (iii), $1 + a = e_1 e_2 \ldots . e_n$ where each e_i is an idempotent. Therefore,

$$e_1(1+a) = e_1^2 e_2 \ldots . e_n = e_1 e_2 \ldots . e_n = (1+a)$$

But $1 + a$ is a unit thus $e_1 = 1$. Likewise, $e_1 = e_2 = \cdots = e_n$=1, then, $1 + a = 1$ which implies that $a = 0$ and $ex = exe$. Similarly, letting b = $xe - exe$ where $x \in R$ and e an idempotent of R, we get $b = 0$ and $xe = exe$. Therefore, $ex = exe = xe$ concluding that $e \in C$.

On the other hand, if $a \in C$ then $ea = ae$

$$ea = e^2x - e^2xe = ex - exe$$

$$ae = exe - exe^2 = exe - exe = 0$$

Since $ae = ea$ then $ex - exe = 0$ and hence $ex = exe$. Similarly, if $b \in C$, then, $xe = exe$ and hence $ex = xe$ showing that e is central. So, in all cases the idempotents are central; but by (iii) R\C is multiplicatively generated by idempotents then R$\backslash C \subset C$, contradiction. Hence, R = C and thus R is commutative.

Theorem 4.5. *Let R be a ring satisfying:*

(iv) The set R\J is multiplicatively generated by idempotents and nilpotents.

If R satisfies the polynomial identity $x^m = x^{m+1}f$ for some positive integer m, where f is a polynomial with integer coefficients, and if the set N of nilpotent elements is commutative, then N is an ideal of R and R/N is Boolean.

Proof. First, we prove that $x^m = x^{2m}f(x)^m$ by induction. R satisfies the polynomial identity $x^m = x^{m+1}f(x)$ then for $m = 1$, $x = x^{1+1}f(x) = x^2f(x)$ so the inductive hypothesis is true for $m = 1$.

Now, assume $x^m = x^{2m}f(x)^m$ is true for m then:

$$x.x^m = x.x^{2m}\, f(x)^m$$

$$x^{m+1} = x^2f(x)x^{2m}f(x)^m$$

$$x^{m+1} = x^2x^{2m}f(x)f(x)^m$$

$$x^{m+1} = x^{2+2m}f(x)^{m+1}$$

$$x^{m+1} = x^{2(1+m)}f(x)^{m+1}$$

Thus proved for m+1.

$x^m = x^{2m}f(x)^m$ implies that $e = x^mf(x)^m$ is idempotent for each $x \in R$ since

$$e^2 = x^{2m}f(x)^{2m} = x^{2m}f(x)^mf(x)^m = x^mf(x)^m = e.$$

Let $x \in J$. Since J is an ideal then $e = x^mf(x)^m$ is an idempotent element in J.

$(x \in J,\ x^{m-1}f(x)^m \in R\ , then\ x.x^{m-1}f(x)^m \in J\ since\ J\ is\ an\ ideal\ thus\ e = x^mf(x)^m \in J)$

But J contains no nonzero idempotent elements (Theorem 1.3) and hence e= 0. So, $x^mf(x)^m = 0$. Therefore, $x^m = x^{2m}f(x)^m = x^m.x^m.f(x)^m = x^m.0 = 0$, thus, every element in J is nilpotent. Hence, using (iv) every element in R is multiplicatively generated by idempotents and nilpotents. As a result, using Theorem 3.4, N is an ideal and R/N is Boolean.

The importance of the finiteness of R in Theorems 4.1 and 4.3, and essentiality of the existence of an identity element of R in Theorem 4.2 and Lemma 4.4 is demonstrated in example 3.1.

BIBLIOGRAPHY

[1] Abu-Khuzam H., Tominaga H., and Yaqub A., *Equational definability of addition in rings satisfying polynomial identities*, Mathematical Journal of Okayama University. Vol. **22(1)**, 1980.

[2] Abu-Khuzam H., *A note on rings which are multiplicatively generated by idempotents and nilpotents*, Internat. J. Math & Math Sci. Vol. **11(1)**, pp.5-8, 1988.

[3] Abu-Khuzam H. and Yaqub A., *On rings with prime centers*, Internat. J. Math & Math. Sci. Vol. **17(4)**, pp.667-670,1994.

[4] Abu-Khuzam H. and Bell H., *Structure of rings with a condition on nonperiodic elements*, Result. Math. 43, pp. 198-201, 2003.

[5] Abu-Khuzam H. and Yaqub A., *Rings where certain subsets are multiplicatively generated by idempotents*,(Submitted).

[6] Bell H., *Some commutativity results for periodic rings*, Acta Math. Acad. Sci. Hungar.Vol.**28**, pp.279-283, 1976.

[7] Fraleigh J., *A first course in abstract algebra*, Pearson; 7 edition, 2002.

[8] Herstein I. N., *Noncommutative rings,* The Carus Math. Monographs, John-Wiley and Sons, Inc., 1968.

[9] Hungerford T. *Algebra, Graduate texts in mathematics*, Vol. **73**, Springer-Verl New York, 1980.

[10] Jacabson N., *Structure of Rings*. Amer. Math. Soc. Colloq. Publ., vol. 37, 1964.

[11] Kaplansky, I., *Fields and Rings* (2d ed). Chicago: University of Chicago Press, 1972.

[12] McCoy, N., *Theory of Rings.* NewYork: The Macmillan Company, 1964.

[13] Putcha M.S. and Yaqub A., *Rings which are multiplicatively generated by idempotents*, Communication in Algebra Vol. **8(2)**, pp.153-159, 1980.

[14] Stone M. H., *The theory of representations of boolean algebras*, Trans. Amer. Math. Soc.,Vol. **40**, pp. 37-111, 1936.