PRIME RINGS WITH POLYNOMIAL IDENTITIES

ABSTRACT

AUTHOR: Ney A. Borba

TITLE: Prime Rings with Polynomial Identities

DEPARTMENT: Mathematics

DEGREE: Master of Science

SUMMARY: Let R be a ring with a ring of operators Ω. The ring R is said to be a ring with a polynomial identity (in short: R is a P.I.-ring) over Ω if R satisfies a polynomial identity $f(X_1, \ldots, X_n) = 0$ with coefficients in Ω.

Let R be a prime P.I.-ring. Then R has a right and left quotient ring Q which is a finite dimensional central simple algebra. Moreover, if C denotes the center of Q, then $RC = Q$.

PRIME RINGS WITH POLYNOMIAL IDENTITIES

by

NEY A. BORBA

A thesis submitted to

the Faculty of Graduate Studies and Research

of McGill University

in partial fulfillment of the requirements

for the degree of Master of Science

March 1972

ACKNOWLEDGEMENT

I wish to express to Professor H.Schwerdtfeger, my research supervisor, my great appreciation for the continued encouragement he has given me in my work.

TABLE OF CONTENTS

INTRODUCTION

This thesis arose from the desire of understanding some aspects of the theory of rings. My principal object was to give a self-contained and connected account, without pretense to completeness, of the principal facts about rings which satisfy polynomial identities (in short: P.I.-rings, cf. Definition in p.57.)

By now, most of the work presented here is classical. The theory goes back to 1943 when M.Hall [9, Theorem 6.2], as the result of his studies on projective planes, discovered that if there is a division ring D, for which the identity

$$(XY-YX)^2 Z - Z(XY-YX)^2 = 0$$

holds, then either D is a field or a generalized quaternion algebra over its center C. Moreover D is finite dimensional over C. This result was later extended by Kaplansky [12] to division rings satisfying any polynomial identity and more generally to primitive algebras with polynomial identities. Much has been done since then and the names of Amitsur, Herstein, Kaplansky, Levitzki , Martindale, Posner, Procesi and Small are familiar in the large literature on this subject. From this broad amount of literature I have chosen to prove some of those results which seemed to me most important and representative of the subject, either for their consequences (cf. Kaplansky's Theorem) or for the techniques involved in their proofs (cf. Theorem 5.2 and Theorem 7.4).

The thesis is organized as follows. Chapters I to IV prepare the tools which are needed for the following chapters, so their character is utilitarian. Chapters V to VII are devoted to P.I.-rings, and particularly to prime P.I.-rings. Most of the material included in the first four chapters, though familiar to the experts, was unknown to me when I started to work in this project. Therefore, I decided to include them and tried to give proofs of all relevant results used as an attempt to make this work as self-contained as possible.

Chapter I contains all properties about primitive and prime rings which are needed in this thesis.

Chapter II is a short description of the centroid of a ring and its main properties.

Chapter III is devoted to the study of Goldie rings and related topics. I have not included there but what I needed for the development of my work. For this reason many important results on Goldie theory are missing. They can be found, for example, in Goldie's own paper [7] or in Chapter 7 of the beautiful book by Herstein [10].

Chapter IV deals with the embedding of certain non-commutative rings into a ring of "fractions". Essentially this is an exercise on patience but as a mathematics student I thought I had to do it at least once during my lifetime!

Chapter V introduces us to the heart of the subject: prime P.I.-rings. Most of the results in this chapter are from the papers by Amitsur [4] and Posner [16] although I have adapted them slightly to my purposes and I have supplied a little more detail to the proofs.

Chapter VI contains what perhaps is the most important result on P.I.-rings: Kaplansky's Theorem. This theorem says that every primitive P.I.-ring R is a finite dimensional simple algebra over its center C(R). The approach I follow was suggested to me by Professor G.Michler from Tübingen University during his visit to McGill in the academic year 1970-1971. The main idea is to prove Kaplansky's Theorem for division rings (Theorem 6.7) using some new techniques developped by Martindale [14] and then reduce to this case, the general one, via Lemma 6.3. I take this opportunity to thank my friend and fellow student Kenneth Louden for his helpful suggestions on some of the proofs in this chapter.

Chapter VII, finally, reproduces (with more details) the proof given recently by Goldie [8] about the structure of prime P.I.-rings.

CHAPTER I

GENERAL PROPERTIES OF PRIME AND PRIMITIVE RINGS

Unless mentioned otherwise R will always denote an associative ring not necessarily containing an identity element. By an ideal of R we mean a two-sided ideal. A proper ideal is one which is different from R. Following Lambek [13, p.12] for any two additive subgroups A and B of R we define the residual quotients $A.\cdot B$ (read "A over B") and $B\cdot.A$ (read "B under A") as

$$A.\cdot B = \{x \in R : xB \subset A\}$$

and

$$B\cdot.A = \{x \in R : Bx \subset A\}.$$

A trivial verification shows that both $A.\cdot B$ and $B\cdot.A$ are additive subgroups of R. Moreover if A and B are both left-ideals of R then $A.\cdot B$ is an ideal of R because for all $x \in A.\cdot B$ and for all $r \in R$ we have

$$(xr)B = x(rB) \subset xB \subset A, \quad \text{and}$$

$$(rx)B = r(xB) \subset rA \subset A.$$

Similarly if A and B are right-ideals of R, then $B\cdot.A$ is an ideal.

DEFINITION 1.1. A proper ideal P of R is called (right, left) <u>prime</u> if $IJ \subseteq P$ for (right, left) ideals I and J of R implies that $I \subseteq P$ or $J \subseteq P$.

LEMMA 1.1. If P is a proper ideal of R, then the following statements are equivalent.

(1) If $x, y \in R$ and $xRy \subseteq P$, then $x \in P$ or $y \in P$.

(2) P is right-prime.

(3) P is prime.

(4) P is left-prime.

Proof: (1) ⇒ (2). Assume (1) and let I and J be right-ideals of R with $IJ \subseteq P$. If $I \not\subset P$, then there exists $0 \neq x \in I - P$. Therefore $(xR)J \subseteq IJ \subseteq P$, hence $xRy \subseteq P$ for all y in J. Since $x \notin P$, by (1) we must have $y \in P$ for all y in J. Hence $J \subseteq P$.

(2) ⇒ (3). Obvious because every ideal is a right-ideal.

(3) ⇒ (4). Let I and J be left-ideals of R such that $IJ \subseteq P$. Then IR and JR are ideals of R and $(IR)(JR) = I(RJ)R \subseteq (IJ)R \subseteq PR \subseteq P$, therefore by (3) $IR \subseteq P$ or $JR \subseteq P$. If $IR \subseteq P$, then $I \subseteq \{x \in R : xR \subseteq P\}$ $= P.\cdot R$ and since the ideal $P.\cdot R$ satisfies $(P.\cdot R)(P.\cdot R) \subseteq (P.\cdot R)R \subseteq P$, by (3) we must have $P.\cdot R \subseteq P$, hence $I \subseteq P$. Similarly, if $JR \subseteq P$, then $J \subseteq P$. Thus (4) holds.

(4) ⇒ (1). Suppose (4) holds and let $xRy \subseteq P$ with x and y in R. Then $(Rx)(Ry) \subseteq P$, therefore $Rx \subset P$ or $Ry \subset P$. If $Ry \subset P$, then $y \in \{x \in R : Rx \subset P\} = R^{\cdot}.P$. But $R^{\cdot}.P$ is an ideal of R (hence a left-ideal) satisfying $(R^{\cdot}.P)(R^{\cdot}.P) \subseteq P$, then $R^{\cdot}.P \subseteq P$ by (4), hence $y \in P$. Similarly $Rx \subset P$ implies $x \in P$, so (1) holds.

DEFINITION 1.2. R is a prime ring if 0 is a prime ideal.

For example, every integral domain is a prime ring.

DEFINITION 1.3. Let S be a non-empty subset of R. The set $S_r = \{x \in R : Sx = 0\}$ is called the right-annihilator of S.

One easily verifies that S_r is a right ideal of R. Similarly the left-ideal $S_\ell = \{x \in R : xS = 0\}$ is called the left-annihilator of S.

A right ideal I of R is called a right-annihilator ideal if there exists a subset S of R for which $S_r = I$.

Let $\mathbb{Z}$ denote the ring of integers and for $n \in \mathbb{Z}$ and $x \in R$ write nx for the sum of n terms equal to x. Given a non-empty set $S \subset R$ let (S) denote the subset of R consisting of all finite sums of the type $\Sigma r_i x_i + \Sigma n_i x_i$ where $r_i \in R$, $n_i \in \mathbb{Z}$ and $x_i \in S$. Then (S) is the smallest left-ideal of R containing S and we call it the left-ideal generated by S.

Observe that $(S)_r = S_r$ therefore if I is a right-annihilator ideal of R we may always assume that $I = K_r$ for some left-ideal K of R.

Left-annihilator ideals are defined similarly.

LEMMA 1.2. The following statements are equivalent.

(1) R is a prime ring

(2) $I_r = 0$ for every non-zero right-ideal I of R.

(3) $J_\ell = 0$ for every non-zero left-ideal J of R.

Proof: (1) $\Rightarrow$ (2). For every non-zero right-ideal I of R we have $I \cdot I_r = 0$. Since R is prime and $I \neq 0$ it follows $I_r = 0$.

(2) $\Rightarrow$ (1). Assume $IJ = 0$ where I and J are right-ideals. Then either $I = 0$ or $I \neq 0$. If $I \neq 0$, then $J \subseteq I_r$ and therefore by (2) $J = 0$. Thus 0 is a right-prime ideal, hence a prime ideal.

(1) $\Leftrightarrow$ (3). The proof is similar and we omit it.

The following lemma is sometimes useful.

LEMMA 1.3. P is a prime ideal of R if and only if the factor ring, R/P, is prime.

Proof: For $r \in R$, let $\bar{r} = r+P$. Assume that P is a prime ideal and $\bar{x}(R/P)\bar{y} = \bar{0}$ in R/P. Then $xRy \subseteq P$ and therefore $x \in P$ or $y \in P$. Thus $\bar{x} = \bar{0}$ or $\bar{y} = \bar{0}$, hence R/P is a prime ring. Conversely, if R/P is prime and $xRy \subseteq P$, then $\bar{x}(R/P)\bar{y} = \bar{0}$; therefore $\bar{x} = \bar{0}$ or $\bar{y} = \bar{0}$. Thus $x \in P$ or $y \in P$ and P is a prime ideal.

DEFINITION 1.4. The center of a ring R, denoted by C(R), consists of all elements $c \in R$ such that $cx = xc$ for all x in R.

It is an easy exercise to verify that C(R) is a subring of R.

LEMMA 1.4. The center of a prime ring is an integral domain.

Proof: If $xy = 0$ with x and y in C(R), then $xRy = Rxy = 0$ and therefore $x = 0$ or $y = 0$ by the primeness of R.

If we consider the non-zero two-sided ideals of a prime ring R as rings, then the properties of R carry over to them, namely

LEMMA 1.5. If R is a prime ring and P is a non-zero ideal of R, then P is a prime ring.

Proof: Let $xPy = 0$ with x and y in P. Assume $x \neq 0$. Then xP is a non-zero right-ideal of R (otherwise $x \in P_{\ell}$ contradicting our assumption). Then $(xP)_r = 0$ by Lemma 1.2, therefore $y = 0$ and P is a prime ring.

DEFINITION 1.5. The ring R is called semiprime if for any two-sided ideals I and J of R, $IJ = 0$ implies $I \cap J = 0$.

COROLLARY 1.6. A prime ring is also semiprime.

Proof: If R is prime and $IJ = 0$ for ideals I and J of R, then $I = 0$ or $J = 0$, hence $I \cap J = 0$.

Later on we will need the following porperty of prime rings.

LEMMA 1.7. If R is a prime ring so is R[X], the ring of polynomials in one commuting indeterminate X over R.

Proof: Assume $p(X) R[X] q(X) = 0$ where p(X) and q(X) are in R[X]. If both p(X) and q(X) are different from 0, let a and b denote the leading coefficients of p(X) and q(X) respectively. Since $R \subseteq R[X]$ we have $f(X) = p(X) R q(X) = 0$. But the leading coefficient of the polynomials $f(X)$ is aRb and this is different from 0 because R is prime and both a and b are different from 0. Therefore we must have $p(X) = 0$ or $q(X) = 0$. Hence $R[X]$ is prime.

DEFINITION 1.6. A right (left) ideal I of R is called regular if there exists an element u in R such that $x-ux$ (resp. $x-xu$) belongs to I for all x in R.

If R happens to have a unit element e, then $x-ex = x-xe = 0$ for all x in R, therefore every right (left) ideal is regular.

It is clear from Definition 1.6 that every right (left) ideal J containing a regular right (left) ideal I is itself regular. In particular, since every right (left) ideal is contained in a maximal one we see that every regular right (left) ideal is contained in a maximal regular right (left) ideal.

DEFINITION 1.7. A right R-module A is called irreducible if $AR \neq 0$ and A has no submodules other than 0 and itself.

The following result describes all the irreducible right R-modules of R.

LEMMA 1.8. A is an irreducible right R-module if and only if A is isomorphic as R-module to R/M for some maximal regular right ideal M of R.

Proof: Assume A is irreducible and consider the set $B = \{a \in A : aR = 0\}$. Then B is a submodule of A and since A is irreducible either $B = 0$ or $B = A$. But $AR \neq 0$ by Definition 1.7, so $B = 0$. Therefore for all $a \in A$, $a \neq 0$ we have $aR \neq 0$, hence $aR = A$ because aR is a submodule of A. Fix a non-zero element $a \in A$ and define the map $f : R \to A$ by the rule $f(x) = ax$ for all x in R. Then f is an homomorphism of right-R-modules, moreover f is surjective because $aR = A$. Let $M = \operatorname{Ker} f = \{x \in R : ax = 0\}$. It is well known that M is a right ideal and that $A = \operatorname{Im} f \cong R/M$. Let I be a right-ideal of R such that $M \subset I$ and $M \neq I$. Then $f(I)$ is a non-zero submodule of A, therefore must equal A. Since f is surjective we have $I = f^{-1}f(I) = f^{-1}(A) = R$. Hence M is a maximal right-ideal. Finally because $aR = A$ there is an element u in R with $au = a$. Then for every x in R, $aux = ax$ which implies $a(x-ux) = 0$. Thus $x-ux \in M$ for all x in R, i.e. M is regular.

Conversely, assume M is a maximal regular right-ideal of R. We want to show that R/M is an irreducible right-R-module. By hypothesis, there exists $u \in R$ such that $x-ux \in M$ for all x in R. If $(R/M)x = 0$ with x in R, then $Rx \subset M$. In particular $ux \in M$, therefore $x = (x-ux)+ux$ belongs to M. Thus $(R/M)x = 0$ if and only if $x \in M$. Since $M \neq R$ this implies $(R/M)R \neq 0$. If A is a submodule of R/M then, one easily verifies that A is of the form I/M for some right ideal I with $M \subset I \subset R$. Since M is maximal we must have $I = M$ or $I = R$, therefore $A = 0$ or $A = R/M$, hence R/M is irreducible.

There are many ways of introducing the concept of primitive ideals; we follow Lambek's approach [13, p. 52] although it should be noticed that our rings do not necessarily contain a unit element.

DEFINITION 1.8. An ideal P in R is called right (left) primitive if there is a maximal regular right (left) ideal M such that P is the largest ideal contained in M.

Observe that if P is the largest ideal contained in a maximal regular right-ideal M, then $P = R^{\cdot}.M = \{x \in R : Rx \subset M\}$. Indeed $R^{\cdot}.M$ is an ideal of R contained in M and containing P, hence equal to P. Thus P is right-primitive if and only if $P = R^{\cdot}.M$ for some maximal regular right ideal M of R. Similarly P is left-primitive if and only if $P = N.^{\cdot}R$ for some maximal regular left ideal N of R.

It follows immediately from Definition 1.8 that every maximal ideal is a right and left primitive ideal.

DEFINITION 1.9. R is said to be a right (left) primitive ring if 0 is a right (left) primitive ideal.

REMARK. It has been shown by Bergman [6] by constructing a counter-example that right-primitive does not imply left-primitive.

LEMMA 1.9. P is a right (left) primitive ideal of R if and only if R/P is a right (left) primitive ring.

<u>Proof</u>. Assume P is right-primitive. Then $P = R\cdot.M$ for some maximal regular right ideal M of R. Since M is regular, there exists $u \in R$ such that $x - ux \in M$ for all x in R. Then $\bar{x} - \bar{u}\bar{x} \in M/P$ for all $\bar{x} = x + P$ in R/P, so M/P is a right-regular-ideal in R/P. Moreover M/P is a maximal right ideal because so is M. We claim that $(R/P)\cdot.(M/P) = \bar{0}$ and therefore R/P is right-primitive. Let $\bar{x}$ be in $(R/P)\cdot.(M/P)$. Then for all r in R, $\bar{r}\bar{x} = rx + P \in M/P$ and consequently $rx \in M$. Therefore $x \in R\cdot.M = P$, hence $\bar{x} = \bar{0}$. Thus our claim is proved.

Conversely, if R/P is a right-primitive ring, then $(R/P)\cdot.(M/P) = \bar{0}$ for some maximal regular right ideal M/P of R/P and it follows that M is a maximal regular right ideal of R containing P. Then for all x in P, $Rx \subset P \subset M$ therefore $P \subset R\cdot.M$. To prove the opposite inclusion let $x \in R\cdot.M$ then for all r in R, $\bar{r}\bar{x} = rx + P \in M/P$ so $(R/P)\bar{x} \subset M/P$. Therefore $\bar{x} = \bar{0}$, hence $x \in P$. The proof of Lemma 1.9 is now complete for the case of right-primitive ideals. For left-primitive ideals the argument is similar and we omit it.

A characterization of primitive ideals is given by the following result due to Jacobson. We first recall that if A is a right-R-module, then $\mathrm{Ann}_R(A) = \{x \in R : Ax = 0\}$ is an ideal of R called the <u>annihilator of A in R</u>. The right-R-module A is <u>faithful</u> if $\mathrm{Ann}_R(A) = 0$.

LEMMA 1.10. P is a right-primitive ideal of R if and only if there exists an irreducible right R-module A such that $\mathrm{Ann}_R(A) = P$.

Proof. If P is right-primitive, then $P = R^{\bullet}.M$ for some maximal regular right ideal M of R. Then $A = R/M$ is an irreducible right R-module by Lemma 1.8. Since $P \subset M$ we have $AP = 0$, so $P \subset \mathrm{Ann}_R(A)$ and if $x \in \mathrm{Ann}_R(A)$ then $Rx \subset M$, hence $x \in R^{\bullet}.M = P$. Thus $\mathrm{Ann}_R(A) = P$.

Conversely, assume that $P = \mathrm{Ann}_R(A)$ for some irreducible right-R-module A. By Lemma 1.8 we may assume $A = R/M$ where M is a maximal regular right ideal. Since $AP = 0$ we have $P \subset M$ therefore $P \subset R^{\bullet}.M$. Furthermore if $x \in R^{\bullet}.M$, then $Rx \subset M$, so $Ax = 0$ and $x \in \mathrm{Ann}_R(A) = P$. Hence $P = R^{\bullet}.M$ and so is right-primitive.

COROLLARY 1.11. R is a right-primitive ring if and only if there exists a faithful irreducible right R-module.

Proof. 0 is a right-primitive ideal of R is and only if $0 = \mathrm{Ann}_R(A)$ for some irreducible right R-module A, i.e. if and only if A is faithful and irreducible.

The next result shows that in a ring R the class of right primitive ideals is smaller than the class of prime ideals.

LEMMA 1.12. If P is a right primitive ideal of R then P is prime.

Proof. By hypothesis and Lemma 1.10 we have $P = \mathrm{Ann}_R(A)$ for some irreducible right-R-module A. Assume $xRy \subset P$ for x and y in R. If $x \notin P$, then $Ax \neq 0$ and therefore $ax \neq 0$ for some non-zero element a in A. Since A is irreducible we have $(ax)R = A$ therefore

$$Ay = (ax)Ry = a(xRy) = 0.$$

Then $y \in P$, hence P is prime.

DEFINITION 1.10. The Jacobson radical of a ring R, denoted by Rad(R), is the intersection of all its right-primitive ideals. R is called semi-primitive if $\text{Rad}(R) = 0$. If R has no right-primitive ideals, we write $\text{Rad}(R) = R$ and call R a radical ring.

REMARK. Being the intersection of ideals Rad(R) is itself an ideal of R. Strictly speaking, we should call Rad(R) the right-Jacobson radical but we should see later that the intersection of all left-primitive ideals of R coincides with Rad(R).

DEFINITION 1.11. An element $x \in R$ is called right-quasi-regular if there exists $x' \in R$ such that $x + x' + xx' = 0$. If this is the case x' is called a right-quasi-inverse of x.

A right ideal I of R is said to be right-quasi-regular if all its elements have a right-quasi-inverse.

The definition of Rad(R) does not tell us much about the nature of its elements. This is essentially the content of the following

THEOREM 1.13.

(i) Rad(R) is the intersection of all the maximal regular right ideals of R.

(ii) Rad(R) contains all the right-quasi-regular right-ideals of R (i.e. Rad(R) is the largest right-quasi-regular right-ideal of R).

Proof. (i) By definition $\text{Rad}(R) = \cap P$ where P runs over all the right-primitive ideals of R. Then by the observation made after Definition 1.8, $\text{Rad}(R) = \cap(R \cdot\!. M)$ as M runs over all the maximal regular-right-ideals of R, therefore since $R \cdot\!. M \subset M$ we get $\text{Rad}(R) \subset \cap M$. To prove the reverse inclusion let $M^* = \cap M$ and for each $x \in M^*$ define $I_x = \{xy+y : y \in R\}$. Then I_x is a right-ideal of R, furthermore taking $u = -x$ in Definition 1.6 we see that I_x is regular. If $I_x \neq R$, then I_x is contained in a maximal regular-right-ideal M_x of R. Since $x \in M^* \subset M_x$ for all y in R we have $xy \in M_x$, therefore $y = (xy+y)-xy$ belongs to M_x. Thus $M_x = R$ which is a contradiction. Therefore we must have $I_x = R$ which in particular implies the existence of an element x' in R with $xx'+x' = -x$. Then $x+x'+xx' = 0$. Hence every element in M^* is right-quasi-regular.

Next, if $M^* \neq \text{Rad}(R)$, then since $\text{Rad}(R) \subset M^*$ there must exist a non-zero element $x_0 \in M^*$ and a maximal regular-right-ideal M of R such that x_0 does not belong to the right-primitive ideal $R \cdot\!. M$. Then $(R/M)x_0 \neq 0$, so $(R/M)M^* \neq 0$ hence $\bar{r}M^* \neq 0$ for some $\bar{r} = r+M$ with $r \in R-M$. Since $\bar{r}M^*$ is a non-zero submodule of R/M and R/M is irreducible (Lemma 1.8) we deduce $\bar{r}M^{*} = R/M$. This implies the existence of x_1 in M^{*} satisfying $\bar{r}x_1 = \overline{-r}$. But since $x_1 \in M^{*}$ it has a right-quasi-inverse x_1' therefore

$$0 = \bar{r}(x_1 + x_1' + x_1 x_1') = \bar{r}x_1 + \bar{r}x_1' + \bar{r}x_1 x_1'$$
$$= \overline{-r} + (\bar{r} + \bar{r}x_1)x_1' = \overline{-r} \ .$$

Thus $-r \in M$ which is a contradiction. Hence we must have $M^{*} = \mathrm{Rad}(R)$. This shows that Rad(R) is right-quasi-regular and also proves (i); it remains to show that Rad(R) contains all right-quasi-regular right-ideals of R. The proof is exactly the same as the one given above to show that $M^{*} \subset \mathrm{Rad}(R)$ so we omit it.

As it was pointed out after Definition 1.10 one can introduce the concept of left-radical of R as the intersection of all its left-primitive ideals but fortunately this intersection coincides with Rad(R). Indeed we have the following

THEOREM 1.14.

(1) $\mathrm{Rad}(R) = \cap P'$ as P' runs over all the left-primitive ideals of R.

(2) $\mathrm{Rad}(R) = \cap M'$ as M' runs over all the maximal regular left ideals of R.

(3) Rad(R) contains all the left-quasi-regular left-ideals of R.

Proof. Let $J = \cap P'$ as P' runs over all the left-primitive-ideals of R. Using the left analogue of Definition 1.11 and Theorem 1.13 one shows that (2) and (3) hold with J instead of Rad(R). To prove that $J = \text{Rad}(R)$ we show that Rad(R) is a left-quasi-regular ideal of R, hence $\text{Rad}(R) \subset J$, and similarly that J is a right-quasi-regular ideal of R therefore $J \subset \text{Rad}(R)$.

Let $x \in \text{Rad}(R)$ and let x' be its right-quasi-inverse. Then $x' = x - xx'$ and since $x \in \text{Rad}(R)$ so does x'. Therefore there exists $x'' \in R$ satisfying $x' + x'' + x'x'' = 0$. Then

$$(x' + x + xx')x'' = 0 = x(x' + x'' + x'x'')$$

this implies that $x'x'' = xx'$. From

$$x' + x + xx' = 0 = x' + x'' + x'x''$$

we deduce then that $x = x''$. Thus $x + x' + x'x = 0$ which says that x is left-quasi-regular. Hence $\text{Rad}(R) \subset J$. The other inclusion is proved in the same way.

The Jacobson radical has another important property, namely

LEMMA 1.15. The factor ring R/Rad(R) is semiprimitive.

Proof. Let $J = \text{Rad}(R)$. We must prove that $\text{Rad}(R/J) = 0$. The right-primitive-ideals of R/J are of the form P/J where P is a right-primitive-ideal of R. Indeed any ideal of R/J is of the type I/J where I is an ideal of R containing J. If P/J is right-primitive, then P/J is the largest ideal contained in some maximal regular-right ideal M/J of R/J. By the standard argument already used in the proof of Lemma 1.9, we conclude that M is a maximal regular-right-ideal containing P. Moreover P is the largest ideal contained in M because otherwise we could put an ideal between P/J and M/J which is impossible. Thus P is right-primitive. Therefore

$$\mathrm{Rad}(R/J) = \cap(P/J)$$

as P runs over all right-primitive ideals of R. Then $\bar{x} = x + J \in \mathrm{Rad}(R/J)$ if and only if $\bar{x} \in P$ for all P, i.e. if and only if $x \in J$. Hence $\mathrm{Rad}(R/J) = 0$.

CHAPTER II

THE CENTROID OF R

Following Herstein [10, p.46] and for the purposes of this chapter, it is convenient to write homomorphisms on the right side of their arguments and we do so.

Given a ring R, let R^+ be its additive group and $E(R) = Hom(R^+, R^+)$ the ring of endomorphisms of R^+. For r and s in R define the maps

$$\lambda_r : R^+ \to R^+ \quad \text{and} \quad \rho_s : R^+ \to R^+$$

by the rules $(x)\lambda_r = rx$ and $(x)\rho_s = xs$ respectively for all x in R. The maps λ_r and ρ_s are called respectively <u>left-multiplication</u> by r and <u>right-multiplication</u> by s.

It follows from the distributive law in R that λ_r and ρ_s belong to E(R) for all r and s in R. Denote by B(R) the subring of E(R) generated by all the λ_r and ρ_s for r and s in R. The ring B(R) is called the <u>multiplication ring of R</u>. Under the mapping $R \times B(R) \to R$ defined by sending $(x, \beta) \in R \times B(R)$ into the image $(x)\beta$ of x under β, it is easy to verify that R becomes a B(R)-module.

If M is a B(R)-submodule of R, then $x\beta \in M$ for all $\beta \in B(R)$ and for all $x \in M$. In particular $x\lambda_r = rx$ and $x\rho_r = xr$ are in M for all $x \in M$ and for all $r \in R$. Thus M is a two-sided ideal of R. Conversely if M is a two-sided ideal of R, then M is a B(R)-submodule of R. Recalling that a ring R having no proper ideals other than 0 is said to be simple the above observation establishes the following

LEMMA 2.1. R is an irreducible B(R)-module if and only if R is a simple ring.

DEFINITION 2.1. The centroid of R (denoted by $\Omega(R)$) is the ring of endomorphisms of R considered as a B(R)-module, i.e. $\Omega(R) = \mathrm{Hom}_{B(R)}(R, R)$.

The following result characterizes $\Omega(R)$

LEMMA 2.2. $\Omega(R)$ is the set of all elements in E(R) which commute elementwise with B(R).

Proof. Let $\omega \in \Omega(R)$. Since $B = B(R)$ is generated by all the λ_r and ρ_s for r and s in R, it suffices to show that $\omega\lambda_r = \lambda_r\omega$ and $\omega\rho_s = \rho_s\omega$. Let $x \in R$, then

$$x(\omega\lambda_r) = (x\omega)\lambda_r = (x\lambda_r)\omega$$

because $\omega \in \mathrm{Hom}_B(R, R)$, therefore $x(\omega\lambda_r) = x(\lambda_r\omega)$ and since this holds for all x in R we get $\omega\lambda_r = \lambda_r\omega$. Similarly $\omega\rho_s = \rho_s\omega$ for all s in R.

Conversely, assume that $\omega \in E(R)$ commutes with every element $\beta \in B$. Then for all x in R

$$(x\omega)\beta = x(\omega\beta) = x(\beta\omega) = (x\beta)\omega$$

therefore ω is a B(R)-endomorphism of R, hence $\omega \in \Omega(R)$.

COROLLARY 2.3. $\omega \in \Omega(R)$ if and only if

$$(xy)\omega = (x\omega)y = x(y\omega)$$

for all x, y in R.

Proof. If $\omega \in \Omega(R)$ and x, y are in R, then

$$(xy)\omega = (y\lambda_x)\omega = y(\lambda_x\omega) = y(\omega\lambda_x) = (y\omega)\lambda_x = x(y\omega)$$

and

$$(xy)\omega = (x\rho_y)\omega = x(\rho_y\omega) = x(\omega\rho_y) = (x\omega)\rho_y = (x\omega)y.$$

Conversely, if the condition holds, then $\omega\lambda_r = \lambda_r\omega$ and $\omega\rho_s = \rho_s\omega$ for all r and s in R, hence $\omega \in \Omega(R)$ by Lemma 2.2.

LEMMA 2.4. If $R^2 = R$, then $\Omega(R)$ is commutative.

Proof. Assume that ω and σ are in $\Omega(R)$. For any x and y in R we have

$$(xy)(\omega\sigma) = ((xy)\omega)\sigma = ((x\omega)y)\sigma = (y\lambda_{x\omega})\sigma$$

$$= (y\sigma)\lambda_{x\omega} = (y\sigma)(x\omega).$$

By Corollary 2.3 we have

$$(x\omega)(y\sigma) = (x(y\sigma))\omega = ((xy)\sigma)\omega = (xy)(\sigma\omega)$$

therefore $(xy)(\omega\sigma) = (xy)(\sigma\omega)$ for all $x, y \in R$ and for all $\omega, \sigma \in \Omega(R)$. Since by hypothesis, every $r \in R$ can be expressed as a finite sum $\sum_i x_i y_i$ with x_i and y_i in R we have

$$(r)(\omega\sigma) = (\sum_i x_i y_i)(\omega\sigma) = \sum_i (x_i y_i)(\omega\sigma)$$

$$= \sum_i (x_i y_i)(\sigma\omega) = (\sum_i x_i y_i)\sigma\omega = (r)(\sigma\omega).$$

This holding for all r in R, we conclude $\omega\sigma = \sigma\omega$ hence $\Omega(R)$ is commutative.

Before proving our next result about $\Omega(R)$, for the case in which R is a simple ring, we need the following well known lemma due to Schur and the definition of an algebra.

LEMMA 2.5. If A is an irreducible R-module, then $\mathrm{Hom}_R(A, A)$, the ring of R-endomorphisms of A, is a division ring.

Proof. Let $f \in \mathrm{Hom}_R(A, A)$ and assume $f \neq 0$. Since A is irreducible, $f(A) = A$ and $\mathrm{Ker}\, f = \{a \in A : (a)f = 0\} = 0$. Thus f is an automorphism of A, therefore f^{-1}, the inverse automorphism of f, exists and belongs to $\mathrm{Hom}_R(A, A)$. Since $ff^{-1} = e$ where e is the identity automorphism of A the proof of Schur's Lemma is complete.

DEFINITION 2.2. Let R be a commutative ring. An algebra over R (or R-algebra) is a pair (A, α) where A is an R-module and $\alpha: A \times A \to A$ is a bilinear mapping; i.e. a mapping satisfying

$$\alpha(xa + yb, c) = x\alpha(a, c) + y\alpha(b, c)$$

and

$$\alpha(a, xb + yc) = x\alpha(a, b) + y\alpha(a, c)$$

for all x, y in R and for all a, b, c in R.

A homeomorphism of R-algebras $(A, \alpha) \to (B, \beta)$ is a homeomorphism $f: A \to B$ of R-modules with the additional property:

$$f(\alpha(a, a')) = \beta(f(a), f(a'))$$

for all a, a′ in A.

(A, α) is called an <u>associative R-algebra</u> if

$$\alpha(a_1, \alpha(a_2, a_3)) = \alpha(\alpha(a_1, a_2), a_3)$$

for all a_1, a_2, a_3 in A.

By abuse of language, one often speaks of the "R-algebra A" instead of the "R-algebra (A, α)". Furthermore, in order to simplify the notation, it is customary to write the law of composition α as mulitplication, i.e. $\alpha(a, b) = ab$, for all a, b in A.

It is easy to verify that relative to this multiplication A is a ring and from the bilinearity of the map α it follows that the ring structure and the R-module structure of A are linked by the rule

$$x(ab) = (xa)b = a(xb)$$

for all x in R and for all a and b in A.

If the multiplication in A has a unit element e then Re is contained in the center of A, because for all x in R and for all a in A we have

$$(xe)a = x(ea) = x(ae) = a(xe).$$

A subset S of A is called a <u>sub-algebra of A</u> if S is a submodule of A and S is a subring of A. Similarly I is an ideal of A if I is an ideal of the ring structure of A and I is a submodule of A. With these definitions in mind, it is then clear what do we mean when we talk about algebra ideals, algebra homomorphisms, simple algebras, etc. One can define, for example, the radical of A as an algebra in a similar way as we did for rings in Chapter I. Fortunately the radical of A as an algebra coincides with the radical of A as a ring. We do not need this result in what follows so we mention it only, and refer to Herstein's book [10, p. 15] for a proof of it.

THEOREM 2.6. If R is a simple ring, then

(i) $\Omega(R)$ is a field,

(ii) R is an algebra over $\Omega(R)$,

(iii) if $C(R) \neq 0$, then $C(R) = \Omega(R)$.

<u>Proof</u>. By Lemma 2.1 to say that R is simple is equivalent to saying that R is an irreducible B(R)-module, therefore $\Omega(R)$ is a division ring by Schur's Lemma. Since R simple, $R^2 = R$, hence $\Omega(R)$ is commutative by Lemma 2.4. Thus $\Omega(R)$ is a field.

By mapping (x, ω) into $x\omega$ for all x in R and ω in $\Omega(R)$, it is obvious that R becomes an $\Omega(R)$-module. Moreover, by Corollary 2.3 $(xy)\omega = (x\omega)y = x(y\omega)$ so R is an algebra over $\Omega(R)$. Thus a simple ring is a simple algebra over its centroid.

Next assume that $C(R) \neq 0$ and $0 \neq c \in C(R)$. Then $cR = Rc$ is a non-zero ideal of R therefore coincides with R. Then for all x in R there is an element x' in R such that $cx' = x'c = x$. In particular there is a $c' \in R$ with $cc' = c'c = c$. Then for all x in R

$$c'x = c'(cx') = (c'c)x' = cx' = x$$

and

$$xc' = (x'c)c' = x'(cc') = x'c = x$$

thus $c'x = xc' = x$. If e is any other element with this property, then $e = ec' = c'e = c'$, hence R has a unique unit element e.

From the definition of C(R) it follows that

$$(xy)c = x(yc) = x(cy) = (xc)y$$

for all $x, y \in R$ and for all $c \in C(R)$, therefore $C(R) \subseteq \Omega(R)$.

Conversely, let $\omega \in \Omega(R)$, then since R has a unit element e we have for all x in R

$$x\omega = (xe)\omega = (e\lambda_x)\omega = (e\omega)\lambda_x = x(e\omega)$$

and similarly

$$x\omega = (ex)\omega = (e\rho_x)\omega = (e\omega)\rho_x = (e\omega)x.$$

Thus $x\omega = x(e\omega) = (e\omega)x$ for all $x \in R$, hence $e\omega \in C(R)$. Moreover since

$$0 = x\omega - x(e\omega) = x(\omega - e\omega)$$

for all x in R, we get $R(\omega - e\omega) = 0$.

Being a field, $\Omega(R)$ is simple and since R is an algebra over $\Omega(R)$

we get $\omega - e\omega \in \mathrm{Ann}_{\Omega(R)}(R) = 0$. Therefore $\omega = e\omega \in C(R)$, thus $\Omega(R) \subseteq C(R)$. This completes the proof of Theorem 2.6.

CHAPTER III

GOLDIE RINGS

In this chapter we prove a classical result by Utumi (Theorem 3.6) and introduce the concept of Goldie ring which is fundamental for the development of later chapters. We begin with a

DEFINITION 3.1. A right ideal I of R is called essential (or large) if $I \cap J \neq 0$ for every non-zero right ideal J of R.

LEMMA 3.1. Let R be an arbitrary ring.

(a) If I and J are essential right ideals of R so is $I \cap J$.

(b) If I is an essential right ideal of R so is every right ideal of R containing I.

(c) If I is an essential right ideal of R, then for all x in R

$$x^{-1}I = \{y \in R : xy \in I\}$$

is an essential right ideal of R.

Proof. (a) Let K be a non-zero right ideal of R. If $(I \cap J) \cap K = 0$, then $I \cap (J \cap K) = 0$, therefore $J \cap K = 0$ because I is essential and hence $K = 0$ because J is also essential. This contradicts the assumption $K \neq 0$. Thus $(I \cap J) \cap K \neq 0$ for every non-zero right ideal K.

(b) Trivial.

(c) Let J be a non-zero right ideal of R and x any element in R. Then we consider two cases.

(i) $xJ = 0 \in I$; i.e. $J \subset x^{-1}I$, therefore $x^{-1}I \cap J = J \neq 0$.

(ii) $xJ \neq 0$. Since xJ is a right ideal and I is essential, we have $I \cap xJ \neq 0$, i.e. there exists a non-zero y in J such that $xy \in I$. Hence $0 \neq y \in x^{-1}I \cap J$.

(i) and (ii) imply $x^{-1}I$ is essential.

The concept of essential right ideal as well as the following definition and lemma are due to R.E.Johnson. We remark that for the set $\{x\}$ consisting of a single element $x \in R$ we write $(x)_r$ for the right-annihilator of $\{x\}$.

LEMMA 3.2. For a ring R the set

$$Z_r(R) = \{x \in R : (x)_r \text{ is essential}\}$$

is a two-sided ideal of R and is called the <u>right-singular ideal of R</u>.

<u>Proof</u>. For all x and y in $Z_r(R)$ we have $(x)_r \cap (y)_r \subseteq (x \pm y)_r$ therefore $(x \pm y)_r$ is essential and hence $x \pm y \in Z_r(R)$.

For all a in R and x in $Z_r(R)$ we have

(i) $(x)_r \subseteq (ax)_r$ because $(ax)(x)_r = a[x(x)_r] = a \cdot 0 = 0$ therefore $(ax)_r$ is essential, hence $ax \in Z_r(R)$.

(ii) $a^{-1}(x)_r \subseteq (xa)_r$, because

$$(xa) \cdot a^{-1}(x)_r = x[a \cdot a^{-1}(x)_r] \subseteq x(x)_r = 0$$

then $(xa)_r$ is essential (by Lemma 3.1 (b) and (c)), hence $xa \in Z_r(R)$. Thus $Z_r(R)$ is an ideal of R.

Let $\mathcal{S}$ be a set of right ideals of R. We say that R satisfies the ascending chain condition on $\mathcal{S}$ if for each ascending sequence

$$I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq I_{n+1} \subseteq \ldots, \qquad I_j \in \mathcal{S}$$

there exists k such that $I_j = I_k$ for all $j \geq k$.

For the special case in which $\mathcal{S}$ consists of all right ideals of R we say that R is right Noetherian if it satisfies the ascending chain condition on $\mathcal{S}$.

LEMMA 3.3. R satisfies the ascending chain condition on a set $\mathcal{S}$ of right ideals if and only if every non-empty subset of $\mathcal{S}$ has a maximal element.

Proof. Assume R satisfies the ascending chain condition on the set $\mathcal{S}$ of right ideals. Let $\mathcal{Q}$ be any non-empty subset of $\mathcal{S}$ and suppose $\mathcal{Q}$ has no maximal element. Take any $I_1 \in \mathcal{Q}$; since I_1 is not a maximal element of $\mathcal{Q}$, there exists an ideal $I_2 \in \mathcal{Q}$ such that $I_1 \subsetneqq I_2$. By repeating this argument we construct an infinite ascending sequence $I_1 \subsetneqq I_2 \subsetneqq I_3 \subsetneqq \ldots$ of ideals in $\mathcal{S}$ contrary to our assumption. Hence $\mathcal{Q}$ must have a maximal element.

Conversely, if every non-empty subset of $\mathcal{S}$ has a maximal element and if $I_1 \subset I_2 \subset \ldots$ is any ascending sequence with $I_j \in \mathcal{S}$ $(j=1, 2, \ldots)$, then the set $\mathcal{Q} = \{I_1, I_2, \ldots\}$ has a maximal element I_k. From

$I_k \subset I_{k+1} \subset \ldots$ and the maximality of I_k we deduce $I_j = I_k$ for all $j \geq k$. Thus R satisfies the ascending chain condition on $\mathcal{S}$.

REMARK. In view of the previous lemma, the ascending chain condition on $\mathcal{S}$ is also referred to as the maximum condition on $\mathcal{S}$.

By considering sequences of the type

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq \ldots \supseteq I_n \supseteq \ldots$$

one defines in a similar fashion as above the concept of descending chain condition on a set $\mathcal{S}$ of right ideals of R. We state without proof the analogue of Lemma 3.3 for future reference.

LEMMA 3.4. R satisfies the descending chain condition on a set $\mathcal{S}$ of right ideals if and only if every non-empty subset of $\mathcal{S}$ has a minimal element, (i.e. if and only if R satisfies the minimum condition on $\mathcal{S}$).

R is said to be right-Artinian if it satisfies the minimum condition on the set of all right ideals.

DEFINITION 3.2. An element x in R is said to be nilpotent if there exists a positive integer n such that $x^n = 0$.

A (right, left) ideal I is said to be nilpotent if there exists a positive integer n such that $I^n = 0$ and I is called a nil (right, left) ideal if every element in I is nilpotent.

In 1.5 we introduced the concept of semi-prime rings. It turns out that such rings have no nilpotent ideals different from 0 and that the intersection of all their prime ideals is zero. In order to prove this we would have to introduce the concepts of prime radical and strongly nilpotent elements. Since we will not be using these ideas in what follows we prefer to prove only part of these results and refer to Lambek's book [13, Proposition 2, p.56] for the complete proof of them.

LEMMA 3.5. If R is a semiprime ring, then 0 is the only nilpotent (right, left) ideal.

Proof. Let I be a nilpotent right ideal of R. Then $I^n = 0$ for some positive integer n, therefore the ideal RI is nilpotent because $(RI)^n \subseteq RI^n = 0$. Let k be the least positive integer for which $(RI)^k = 0$. Since R is semiprime and $0 = (RI)^k = (RI)(RI)^{k-1}$ we have $0 = (RI) \cap (RI)^{k-1} = (RI)^{k-1}$ and this is impossible unless $RI = 0$. If this is the case, then $I \subseteq R_r$. But $R_r \cdot R_r = 0$ so $R_r = 0$ because R is semiprime. Hence $I = 0$. For nilpotent (left) ideals, the proof is similar.

The following theorem due to Utumi will be of use later.

THEOREM 3.6. If R is a semiprime ring which satisfies the maximum condition on right-annihilators, then R has no non-zero nil (right, left) ideals.

Proof. Let I be a non-zero nil right-ideal of R and let $\mathcal{S} = \{(x)_r : 0 \neq x \in I\}$. Since I is nil for every non-zero element x in I, there exists a positive integer k(x) such that $x^{k(x)} = 0$ and $x^{k(x)-1} \neq 0$. This simple remark implies that every $(x)_r \in \mathcal{S}$ is different from zero. Since $I \neq 0$, the set $\mathcal{S}$ is non-empty therefore by hypothesis $\mathcal{S}$ has a maximal element $(x_0)_r$. We observe that $k(x_0) = 2$. Indeed if $k(x_0) = m > 2$, then since $(x_0)_r \subseteq (x_0^{m-1})_r$ and since $0 \neq x_0^{m-1} \in I$, the maximality of $(x_0)_r$ forces $(x_0)_r = (x_0^{m-1})_r$. Then from $(x_0^{m-1})x_0 = x_o^m = 0$ it follows $x_0 \in (x_0^{m-1})_r = (x_0)_r$ hence $x_0 \cdot x_0 = x_0^2 = 0$.

We claim that $x_0 y x_0 = 0$ for all y in R. We may assume that $y \notin (x_0)_r$ otherwise the result is trivial. Since the non-zero element $x_0 y$ is in I we have $(x_0 y)^n = 0$ and $(x_0 y)^{n-1} \neq 0$ where $n = k(x_0 y)$. Now $(x_0 y)^{n-1} x_0 = 0$ because otherwise from $0 = (x_0 y)^n = ((x_0 y)^{n-1} x_0) y$ we deduce $y \in ((x_0 y)^{n-1} x_0)_r \supseteq (x_0)_r$, hence by the maximality of $(x_0)_r$ in $\mathcal{S}$, this last inclusion is an equality, then $y \in (x_0)_r$ contradicting our assumption. Then $(x_0 y)^{n-1} x_0 = 0$, therefore $x_0 y x_0 = 0$ if n=2. If $n > 2$, then from

$$0 = (x_0 y)^{n-1} x_0 = ((x_0 y)^{n-2} x_0) y x_0$$

and the fact that $0 \neq (x_0 y)^{n-2} x_0 \in I$ we get $y x_0 \in ((x_0 y)^{n-2} x_0)_r \supseteq (x_0)_r$. Again using the maximality of $(x_0)_r$ we conclude that $y x_0 \in (x_0)_r$ hence $x y x_0 = 0$. The proof of our claim is now complete, and since it holds for all y in R we obtain in particular that $x_0 R^2 x_0 = 0$ and hence $(Rx_0R)(Rx_0R) = 0$. Thus Rx_0R is a nilpotent ideal of the semiprime ring R, therefore $Rx_0R = 0$, hence $Rx_0 \subseteq R_\ell$. Since $R_\ell \cdot R_\ell = 0$ using Lemma 3.5 again we conclude that $R_\ell = 0$. Therefore $Rx_0 = 0$ so $x_0 \in R_r$ and since R is semiprime $R_r = 0$ forcing $x_0 = 0$. This contradicts the definition of $\mathcal{S}$ and therefore contradicts the hypothesis that I was a non-zero nil right-ideal. Hence 0 is the only nil right-ideal of R.

Next let J be a nil left-ideal. Then for all y in J the left-ideal Ry is nil and therefore for all x in R there is a positive integer $t = t(x)$ satisfying $(xy)^t = 0$. This implies $(yx)^{t+1} = y(xy)^t x = 0$. Thus yR is a nil right-ideal of R so by the first part of the proof $yR = 0$. Then $y \in R_\ell = 0$, therefore $y = 0$. Since y was any element in J we conclude $J = 0$ which completes the proof of Utumi's Theorem.

Rings without non-zero nil ideals have the property that their ring of polynomials in one commuting indeterminate are semiprimitive. This result is due to Amitsur and we follow below his original proof, given in [2]. One other type of proof can be found in Herstein's book [10, pp. 150-152]. As usual R[X] stands for the ring of polynomials over R in one commuting indeterminate X.

LEMMA 3.7. Let I be a non-zero ideal of R[X] and let

$$p(X) = a_0 + a_1 X + \ldots + a_n X^n, \quad (a_j \in R,\ a_n \neq 0)$$

be a non-zero polynomial in I having minimal degree. If there exists $b \in R$ satisfying $a_n^{\mu} b = 0$ for some positive integer μ, then $a_n^{\mu-1} p(X) b = 0$.

Proof. Since I is an ideal of $R[X]$ and $p(X) \in I$ so does $q(X) = a_n^{\mu-1} p(X)b$. But the coefficient of X^n in $q(X)$ is $a_n^{\mu} b = 0$ therefore the minimality of the degree of $p(X)$ implies $q(X) = 0$.

COROLLARY 3.8. Let I be a non-zero ideal in $R[X]$ and $p(X) = a_0 + a_1 X + \ldots + a_n X^n$, $(a_n \neq 0)$ a polynomial of minimal degree contained in I. If there exists $r(X)$ in $R[X]$ such that $a_n^{\mu} r(X) = 0$ for some positive integer μ, then $a_n^{\lambda} p(X) r(X) = 0$ for every integer $\lambda \geq \mu - 1$.

Proof. Let $r(X) = \sum_{j=0}^{m} b_j X^j$, $b_j \in R$. Since $a_n^{\mu} r(X) = 0$ for some positive integer μ, we have $a_n^{\mu} b_j = 0$ for $j = 0, 1, \ldots, m$. Then Lemma 3.7 implies $a_n^{\mu-1} p(X) b_j = 0$ and hence $a_n^{\lambda} p(X) r(X) = 0$ for every integer $\lambda \geq \mu - 1$.

NOTATION. As pointed out in Chapter I our rings do not necessarily have a unit element therefore in general X does not belong to $R[X]$. If $t(X) = b_0 + b_1 X + \ldots + b_n X^n$ we will use the notation $t(X)X$ for the polynomial $b_0 X + b_1 X^2 + \ldots + b_n X^{n+1}$. Similarly $Xt(X) = Xb_0 + X^2 b_1 + \ldots + X^{n+1} b_n$.

We can now prove Amitsur's

THEOREM 3.9. If R is a ring having no non-zero nil ideals, then $R[X]$ is semiprimitive.

Proof. Assume that $J = \mathrm{Rad}(R[X])$ is not zero and let n be the minimal degree of the non-zero polynomials in J. Let L be the set consisting of 0 and the leading coefficients of all the polynomials in J having degree n. Then L is a non-zero ideal of R. If we can show that L is nil, then by hypothesis $L = 0$ which is a contradiction. With this in mind, let $0 \neq a \in L$. By definition of L there exists a polynomial $p(X) = a_0 + a_1 X + \ldots + a_n X^n$ in J with $a_n = a$. In $R[X]$ we have $a_n X = X a_n$ therefore since J is an ideal $p(X) \in J$ implies $p(X) X a_n \in J$. By Propositions 1.13 and 1.14 there exists $\bar{q}(X) \in R[X]$ satisfying

$$p(X)Xa_n + q(X) + p(X)Xa_n q(X) = 0 \qquad (1)$$

and

$$p(X)Xa_n + q(X) + q(X)p(X)Xa_n = 0. \qquad (2)$$

From (1) we get $q(X) = Xt(X)$ where $t(X) = -p(X)Xa_n q(X) - p(X)Xa_n$ belongs to $R[X]$.

Let $s(X) = p(X)a_n$. If $s(X)=0$, then $a_n^2 = 0$, hence $a_n = a$ is nilpotent as required to prove. If $s(X) \neq 0$, then since $s(X)$ belongs to J and has degree at most n its degree must be equal to n because of the minimality of n. Therefore $a_n^2 \neq 0$. From (1) we deduce

$$Xs(X) + Xt(X) + X^2 s(X)t(X) = 0$$

therefore

$$s(X) + t(X) + Xs(X)t(X) = 0 \qquad (3)$$

since in $R[X]$ we have $Xr(X) = 0$ if and only if $r(X) = 0$. By a similar reasoning (2) implies

$$s(X) + t(X) + Xt(X)s(X) = 0 \quad . \qquad (4)$$

Suppose now that for every positive integer μ is $a_n^{\mu}t(X) \neq 0$. We will derive a contradiction. Let ν be the minimal degree of the polynomials $a_n^{\mu}t(X)$ where μ ranges over the positive integers. Express $t(X)$ as

$$t(X) = t_1(X)+X^{\nu+1}t_2(X) \qquad (5)$$

where $t_1(X) = b_0+b_1X+\ldots+b_{\nu}X^{\nu}$.

From the definition of ν we deduce that $a_n^{\mu}b_{\nu} \neq 0$ for every μ and $a_n^{\pi}t_2(X) = 0$ for some fixed positive integer π. Since $s(X)$ is a polynomial of minimal degree in J by Corollary 3.8 we have $a_n^{\mu}s(X)t_2(X) = 0$ for all $\mu \geq \pi-1$. Substitution of (5) into (3) and left-multiplication by $a_n^{2\pi}$ yields

$$0 = a_n^{2\pi}[s(X)+t_1(X)+X^{\nu+1}t_2(X)+Xs(X)(t_1(X)+X^{\nu+1}t_2(X))]$$

$$= a_n^{2\pi}s(X)+a_n^{2\pi}t_1(X)+a_n^{2\pi}Xs(X)t_1(X) \qquad (6)$$

Since the polynomial (6) is zero all its coefficients must vanish. In particular the coefficient of $X^{n+\nu+1}$ which is $a_n^{2\pi+2}b_{\nu}$ must be 0, contradicting our previous remark that $a_n^{\mu}b_{\nu} \neq 0$ for all μ. Therefore the assumption that $a_n^{\mu}t(X) \neq 0$ for all μ is false. Thus $a_n^{\lambda}t(X) = 0$ for some integer $\lambda > 0$. Multiplying (4) on the left by a_n^{λ} we obtain

$$0 = a_n^{\lambda}s(X)+a_n^{\lambda}t(X)+Xa_n^{\lambda}t(X)s(X) = a_n^{\lambda}s(X)$$

therefore $a_n^{\lambda+2} = 0$ and therefore $a = a_n$ is nilpotent as required to prove.

REMARK. The argument in the proof of Amitsur's Theorem shows that if $0 \neq a \in R \cap \mathrm{Rad}(R[X])$, then a is nilpotent because in this case the minimal degree of the non-zero elements in $\mathrm{Rad}(R[X])$ is $n = 0$.

DEFINITION 3.3. The ring R is right-finite dimensional if R has no infinite direct sum of non-zero right-ideals.

It can be shown that if R is right-finite dimensional, then there exists a positive integer n such that R contains a direct sum of n summands and the number of summands of every direct sum of R is at most n. This unique number n is called the right Goldie dimension of R and is denoted by dim R.

DEFINITION 3.4. R is said to be a right-Goldie ring if

(1) R is right-finite dimensional, and

(2) R satisfies the maximum condition on right-annihilators.

Left Goldie rings are defined similarly.

For example, every right Noetherian ring R is a right Goldie ring, because R certainly satisfies the maximum condition on right-annihilators and it has no infinite direct sum since for any ideals I_j the ascending chain $I_1 \subseteq I_1 + I_2 \subseteq I_1 + I_2 + I_3 \subseteq \ldots$ must stop.

A generalization of Fitting's Lemma (cf. Lambek [13, p.23]) is given by the following result due to Lesieur-Croisot.

LEMMA 3.10. If R is a right Goldie ring, then for every $x \in R$ there exists a positive integer $n = n(x)$ such that

(i) $I = x^n R + (x^n)_r$ is a direct sum, and

(ii) I is an essential right ideal.

<u>Proof</u>. For $x = 0$ the assertion is clear because $0_r = R$. If $x \neq 0$, then by the maximum condition for right-annihilator ideals there exists a positive integer $n = n(x)$ such that $(x^n)_r = (x^{2n})_r$. If $y \in x^n R \cap (x^n)_r$, then $y = x^n t$ for some $t \in R$ and since $y \in (x^n)_r$ we have $0 = x^n y = x^n(x^n t) = x^{2n} t$. Thus $t \in (x^{2n})_r = (x^n)_r$ hence $y = x^n t = 0$. Therefore (i) holds and we write $I = x^n R \oplus (x^n)_r$ to indicate that the sum is direct. Next let J be a right-ideal of R. We prove that I is essential by showing that $J \cap I = 0$ implies $J = 0$.

If $J \cap I = 0$ and $J \neq 0$, then

$$J \oplus x^n J \oplus x^{2n} J \oplus \dots \tag{1}$$

is a direct sum of right-ideals of R and $x^{kn} \neq 0$ for all positive integers k. Indeed, if $x^{kn} = 0$ for some k, then $x^{kn} J = 0$ so $J \subseteq (x^{kn})_r = (x^n)_r$. Therefore $J = J \cap (x^n)_r \subseteq J \cap I = 0$, so $J = 0$ contradicting our assumption. Hence $x^{kn} \neq 0$ for all k. Now if (1) is not a direct sum, then there exists a non-trivial representation

$$0 = x^{k_1 n} y_1 + x^{k_2 n} y_2 + \dots + x^{k_t n} y_t \qquad \text{with } y_i \text{ in } J,$$

$$0 < k_1 < k_2 < \ldots < k_t \quad \text{and} \quad x^{k_i n} y_i \neq 0.$$

Then

$$0 = x^{k_1 n}(y_1 + x^n z) \quad \text{with} \quad z \text{ in } R.$$

Therefore

$$y_1 + x^n z \in (x^{k_1 n})_r = (x)_r,$$

hence $y_1 = -x^n z + (y_1 + x^n z)$ belongs to I. But $I \cap J = 0$, therefore $y_1 = 0$, hence $x^{k_1 n} y_1 = 0$ which contradicts our hypothesis.

Then (1) is a direct sum contradicting the finite dimensionality of R. Therefore we must have $J = 0$ and the proof of Lesieur-Croisot's Lemma is then complete.

COROLLARY 3.11. If R is a right-Goldie ring, then $Z_r(R)$ is a nil ideal.

Proof. From Lesieur-Croisot's Lemma, for each $z \in Z_r(R)$ there exists a positive integer $n = n(z)$ such that the sum $z^n R + (z^n)_r$ is direct. Since $z^n \in Z_r(R)$ according to Definition 3.2, $(z^n)_r$ is essential. But $z^n R \cap (z^n)_r = 0$ therefore $z^n R = 0$. In particular $z^{n+1} = 0$. Hence every element in $Z_r(R)$ is nilpotent.

COROLLARY 3.12. If R is a semiprime right Goldie ring then $Z_r(R) = 0$.

Proof. By Corollary 3.11 $Z_r(R)$ is nil and by Theorem 3.6 it must be equal to 0.

DEFINITION 3.4. An element $x \in R$ is said to be right-regular if $(x)_r = 0$ and left-regular if $(x)_\ell = 0$.

If x is both right and left regular we say that x is <u>regular</u>.

LEMMA 3.13. If R is a right Goldie ring and if $c \in R$ is right-regular, then

(i) cR is an essential right-ideal of R

(ii) if R is also semiprime, then c is regular.

<u>Proof</u>. (i) By Lemma 3.10 there is a positive integer $n = n(c)$ such that $I = c^n R \oplus (c^n)_r$ is essential. Since c is right-regular $(c^n)_r = (c)_r = 0$ therefore $I = c^n R$ hence cR is essential because $c^n R \subseteq cR$.

(ii) If $xc = 0$ then $cR \subseteq (x)_r$, therefore $(x)_r$ is essential by part (i) and Lemma 3.1(b). Thus $x \in Z_r(R)$. Since R is semiprime $Z_r(R) = 0$ by Corollary 3.12. Then c is also left-regular and hence regular.

The above lemma and the next are crucial in the theory of semiprime Goldie rings (cf. [7, Theorem 3.9]). They give a relation between regular elements and essential right-ideals and guarantee that if R is a semiprime Goldie ring,then the set of regular elements of R is non-empty.

LEMMA 3.14. If R is a semiprime right-Goldie ring, then every essential right ideal I of R contains a regular element.

<u>Proof</u>. Suppose I has no regular elements. We will derive a contradiction. By Lemma 3.13 I does not contain any right-regular element and by Theorem 3.6 I is not nil. The set $\mathcal{S} = \{(x)_r : 0 \neq x \in I\}$ has a maximal element say $(a_1)_r$. Since a_1 is not right-regular $(a_1)_r \neq 0$ therefore $(a_1)_r \cap I \neq 0$

because I is essential. Moreover $(a_1)_r \subseteq (a_1^2)_r$ implies $(a_1)_r = (a_1^2)_r$ by the maximality of $(a_1)_r$ in $\mathcal{S}$.

Suppose now that there exist k-1 elements $a_i \in I$ such that

(A) $$(a_j)_r = (a_j^2)_r \quad \text{for } j=1,2,\ldots,k-1$$

(B) $$a_j \in I_{j-1} = I \cap (a_1)_r \cap \ldots \cap (a_{j-1})_r \quad \text{for } j=1,2,\ldots,k-1$$

(C) $$I_{k-1} \neq 0$$

(D) $$S_{k-1} = \sum_{i=1}^{k-1} a_i R \quad \text{is a direct sum.}$$

Then by (C) and the maximum condition on right annihilators, there exists a non-zero element $a_k \in I_{k-1}$ such that $(a_k)_r = (a_k^2)_r$. We claim that the sum $S_k = S_{k-1} + a_k R$ is direct. Let $x_i \in R$, $i=1,2,\ldots,k$ be such that

$$a_1x_1 + a_2x_2 + \ldots + a_kx_k = 0 \tag{1}$$

Left multiplication by a_1 and the fact that $a_j \in (a_1)_r$ for $j=2,\ldots,k$ yields $a_1^2x_1 = 0$. Thus $x_1 \in (a_1^2)_r$ hence $a_1x_1 = 0$ by (A). Therefore (1) becomes

$$a_2x_2 + \ldots + a_kx_k = 0 \tag{2}$$

Repeating the above argument left-multiplication of (2) by a_2 yields $a_2x_2 = 0$. After k-1 steps of this type we see that all terms in (1) are equal to 0, hence S_k is a direct sum.

Next we show that $I_k = I_{k-1} \cap (a_k)_r \neq 0$. If $0 = I_k = I \cap [(a_1)_r \cap \ldots \cap (a_k)_r]$, then

$$(a_1)_r \cap \ldots \cap (a_k)_r = 0 \qquad (3)$$

Then $a_1+a_2+\ldots+a_k = c$ is a right-regular element in I because if $cx=0$ then $0 = a_1x+a_2x+\ldots+a_kx \in S_k$ and since S_k is a direct sum we have $a_ix = 0$ for $i=1, 2, \ldots, k$. Thus $x \in (a_i)_k$ for $i=1, 2, \ldots, k$, hence $x = 0$ by (3). This is a contradiction because I was proved to have no right-regular elements. Then starting with k-1 elements $a_1, \ldots, a_{k-1}$ satisfying conditions (A), (B), (C) and (D) we can find another element $a_k \neq a_j$ for $j = 1, 2, \ldots, k-1$ such that the elements $a_1, a_2, \ldots, a_k$ still satisfy (A), (B), (C) and (D). Then by induction on k from (D) we deduce that R contains an infinite direct sum of right-ideals which contradicts the finite dimensionality of R. The proof of Lemma 3.14 is then completed.

If R is a prime ring and if I is any non-zero two-sided ideal of R, then $JI \neq 0$ for every non-zero right-ideal J. Since $JI \subset J \cap I$ the above remark shows that in a prime ring every ideal is essential. Since every prime ring is semiprime we get the following corollary to Lemma 3.14.

COROLLARY 3.15. If R is a prime right-Goldie ring then every non-zero ideal of R contains a regular element.

CHAPTER IV

ORE'S THEOREM

The construction of the field of rationals from the ring of integers, as is well-known, can be generalized to any commutative integral domain. Under certain hypotheses it is also possible to imbed a non-commutative ring R in a ring of "fractions" as it was shown first by Ore in a now classical paper [15]. We discuss Ore's construction below. As usual R denotes a non-commutative ring which does not necessarily contain a unit element.

A subset S of R is said to be multiplicatively closed if for all s and t in S their product st is in S. One example of such a set is given by the set of all regular elements of R.

DEFINITION 4.1. Let S be a multiplicatively closed subset of R. We say that R satisfies the left-Ore condition with respect to S if for all (a, s) in $R \times S$ the set $Sa \cap Rs$ is non-empty.

NOTE: For the remainder of this chapter and unless mentioned otherwise S will stand for the set of all regular elements in R and we will always assume that $S \neq \phi$. This is certainly the case if R is a semiprime right-Goldie ring (Lemma 3.15).

DEFINITION 4.2. A ring $Q_\ell(R)$ is said to be a left-quotient ring for R if

(1) $Q_\ell(R)$ has a unit element e

(2) $Q_\ell(R)$ contains R (or an isomorphic image of R)

(3) s is invertible in $Q_\ell(R)$ for all s in S (i.e. there exists $s^{-1} \in Q_\ell(R)$ satisfying $s^{-1}s = ss^{-1} = e$)

(4) every x in $Q_\ell(R)$ can be written as $x = s^{-1}a$ where $(a, s) \in R \times S$.

If $Q_\ell(R)$ is a left-quotient ring for R we also say that R is a left-order in $Q_\ell(R)$.

Next we investigate under which conditions a ring R has a left quotient ring. Extending work of Ore, Asano has proved in [5] that if R satisfies the left-Ore condition with respect to a multiplicatively closed subset T of S then R has a left quotient ring. We will prove this below (Theorem 4.3) for the case $T = S$. If $T \neq S$ the proof is essentially the same with some extra technicalities. Before, we need the following

LEMMA 4.1. If R satisfies the left-Ore condition with respect to S and if s_1 and s_2 belong to S, then there exist u_1 and u_2 in S such that $u_1s_1 = u_2s_2$.

Proof. By Ore's condition $Ss_2 \cap Rs_1 \neq \emptyset$ therefore there exist $u_2 \in S$ and $u_1 \in R$ such that $u_2s_2 = u_1s_1$. Since S is multiplicatively closed u_2s_2 belongs to S. It remains to show that u_1 is regular.

(i) If for $x \in R$ is $xu_1 = 0$, then $x(u_1s_1) = 0$ therefore $x = 0$ since $u_1s_1 = u_2s_2$ is regular.

(ii) By Ore's condition applied to $(s_1, u_1 s_1) \in R \times S$ there exists $(a, s) \in R \times S$ such that $ss_1 = a(u_1 s_1)$. Then $(s - au_1)s_1 = 0$ therefore $s = au_1$ because s_1 is regular. But then $u_1 y = 0$ with y in R implies $sy = au_1 y = 0$ therefore $y = 0$ since $s \in S$. Thus u_1 is right-regular.

(i) and (ii) imply that $u_1 \in S$.

REMARK. From the above proof we extract the following result which for future reference will be recorded as

LEMMA 4.2. If R satisfies the left-Ore condition with respect to S and if $(u, s) \in R \times S$ is such that $us \in S$, then $u \in S$.

We are ready to prove the main result of this section, namely Ore's

THEOREM 4.3. R has a left-quotient ring if and only if R satisfies the left-Ore condition with respect to S.

<u>Proof</u>. If R has a left quotient ring $Q_\ell(R)$, then for all a in R and for all s in S the element as^{-1} is in $Q_\ell(R)$ therefore by (4), Definition 4.2, for some $(a_1, s_1) \in R \times S$ is $as^{-1} = s_1^{-1} a_1$. Multiplying on the left by s_1 and on the right by s we obtain $s_1 ae = ea_1 s$, where e is the unit element in $Q_\ell(R)$. Then $s_1 a = a_1 s$. Thus $Sa \cap Rs \neq \phi$. Hence R satisfies the left-Ore condition with respect to S..

Conversely assume that R satisfies Definition 4.1. We prove the existence of a left-quotient ring for R by establishing a series of lemmas. First define a relation $\sim$ in $R \times S$ by saying that $(a, s) \sim (a', s')$ if there exist $u, u' \in R$ such that $us = u's' \in S$ and $ua = u'a'$. It is clear from Lemma 4.2 that u and u' must then be regular elements.

LEMMA 4.4. $\sim$ is an equivalence relation on $R \times S$.

Proof. Symmetry and reflexivity are obvious. Let $(a, s) \sim (a', s')$ and $(a', s') \sim (a'', s'')$. Then there exist u, u', v and v' in S such that

$$us = u's' = \sigma \in S, \quad vs' = v's'' = \sigma' \in S$$
$$ua = u'a' \quad \text{and} \quad va' = v'a''.$$

By Lemma 4.1 applied to σ and σ' there exist t and t' in S such that $t\sigma = t'\sigma'$. Then $tus = tu's' = t'vs' = t'v's''$.

Now $tu's' = t'vs'$ implies $tu' = t'v$ because s' is regular, therefore

$$tua = tu'a' = t'va' = t'v'a''.$$

Thus there exist tu and $t'v'$ such that $(tu)s = (t'v')s''$ and $(tu)a = (t'v')a''$. Hence $(a, s) \sim (a'', s'')$. Therefore $\sim$ is transitive.

We denote by ${}_S R$ the set of equivalence classes of $R \times S$ with respect to $\sim$ and write $s^{-1}a$ for the equivalence class of $(a, s) \in R \times S$. In order to define an addition and multiplication in ${}_S R$ making it into an associative ring we require the following

LEMMA 4.5.

(A) $s^{-1}a = (us)^{-1}ua$ for all $s^{-1}a \in {}_S R$ and $u \in S$.

(B) Let a, a_1, u, u_1, t and t_1 be in R and s and s_1 be in S. If

(1) $ua = u_1 a_1$

(2) $us = u_1 s_1 = \sigma \in S$

(3) $ts = t_1 s_1 = \sigma_1 \in S$

then $ta = t_1 a_1$.

(Condition (B) is known in the literature as Malcev's property.)

Proof. (A) Since s and us are in S by Lemma 4.1, there exist v and v' in S with $vs = v'us$, therefore $v = v'u$ because s is regular and then $va = v'ua$. Thus $(a, s) \sim (ua, us)$, hence $s^{-1}a = (us)^{-1}ua$.

(B) Conditions (1) and (2) imply $(a, s) \sim (a_1, s_1)$ therefore $s^{-1}a = s_1^{-1}a_1$. Condition (3) and Lemma 4.2 imply $t \in S$, therefore by (A) $s^{-1}a = (ts)^{-1}ta$. A similar argument shows that $s_1^{-1}a_1 = (t_1 s_1)^{-1} t_1 a_1$. Then, $(ts)^{-1}ta = (t_1 s_1)^{-1} t_1 a_1$, i.e. $\sigma_1^{-1} ta = \sigma_1^{-1} t_1 a_1$. Therefore by definition of $\sim$ there exist $u, v \in S$ such that

$$\text{(i) } u\sigma_1 = v\sigma_1, \quad \text{(ii) } uta = vt_1 a_1.$$

Since σ_1 is regular (i) implies $u = v$ hence (ii) entails $ta = t_1 a_1$ proving Malcev's property.

REMARK. If $s^{-1}a$ and $s_1^{-1}a_1$ are in $_S R$ then by Lemma 4.2 there exist u and u_1 in S such that $us = u_1 s_1 = \sigma \in S$. Therefore by Lemma 4.5

$$(*) \qquad s^{-1}a = (us)^{-1}ua = \sigma^{-1}ua \quad \text{and} \quad s_1^{-1}a_1 = (u_1 s_1)^{-1} u_1 a_1 = \sigma^{-1} u_1 a_1.$$

If we think of $s^{-1}a$ as a "fraction" having s as denominator and a as numerator, (*) tells us that for any two fractions we can find a "common denominator".

DEFINITION 4.3. If $s^{-1}a$ and $s_1^{-1}a_1$ are in ${}_SR$ we define $s^{-1}a+s_1^{-1}a_1 = \sigma^{-1}(ua+u_1a_1)$ where u and u_1 are elements in S satisfying $us = u_1s_1 = \sigma$.

Notice that u and u′ exist because of Lemma 4.1.

LEMMA 4.6. Addition in ${}_SR$ is well defined.

Proof. (i) Addition is independent of the representatives of the equivalence classes. Indeed let $s_2^{-1}a_2 = s^{-1}a$ and $v_1, v_2 \in S$ with $v_1s_1 = v_2s_2 = \sigma_1$. Then

$$s_2^{-1}a_2+s_1^{-1}a_1 = \sigma_1^{-1}(v_2a_2+v_1a_1).$$

By Lemma 4.1 there exist t and t_1 in S such that $t\sigma = t_1\sigma_1$, i.e.

$$tus = tu_1s_1 = t_1v_1s_1 = t_1v_2s_2.$$

Since $s^{-1}a = s_2^{-1}a_2$ and $tus = t_1v_2s_2$ it follows from Malcev's property that

$$tua = t_1v_2a_2 \qquad (1)$$

Since s_1 is regular, $tu_1s_1 = t_1v_1s_1$ entails $tu_1 = t_1v_1$ therefore

$$tu_1a_1 = t_1v_1a_1 \qquad (2)$$

Adding (1) and (2) we get

$$t(ua+u_1a_1) = t_1(v_2a_2+v_1a_1)$$

and since also $t\sigma = t_1\sigma_1$ we obtain

$$\begin{aligned} \sigma^{-1}(ua+u_1a_1) &= (t\sigma)^{-1}t(ua+u_1a_1) \\ &= (t_1\sigma_1)^{-1}t_1(v_2a_2+v_1a_1) \\ &= \sigma_1^{-1}(v_2a_2+v_1a_1) \end{aligned}$$

thus

$$s^{-1}a+s_1^{-1}a_1 = s_2^{-1}a_2+s_1^{-1}a_1.$$

The independence of addition with respect to the representative of the second summand $s_1^{-1}a_1$ is proved similarly since addition in R is commutative.

(ii) Addition is independent of the pair u, u_1. In other words if also $u's = u_1's_1 = \tau$, then

$$\sigma^{-1}(ua+u_1a_1) = \tau^{-1}(u'a+u_1'a_1).$$

Indeed by Lemma 4.1 there exist t and t′ in S with $t\sigma = t'\tau$, therefore

$$tus = tu_1s_1 = t'u's = t'u_1's_1 \tag{3}$$

since both s and s_1 are regular (3) implies

$$tu = t'u' \text{ and } tu_1 = t'u_1'.$$

Therefore

$$tua = t'u'a \text{ and } tu_1a_1 = t'u_1'a_1$$

Adding these two equalities we get

$$t(ua+u_1a_1) = t'(u'a+u_1'a_1)$$

therefore since $t\sigma = t'\tau$ we deduce

$$\begin{aligned}\sigma^{-1}(ua+u_1a_1) &= (t\sigma)^{-1}t(ua+u_1a_1)\\ &= (t'\tau)^{-1}t'(u'a+u_1'a_1)\\ &= \tau^{-1}(u'a+u_1'a_1)\end{aligned}$$

as required to prove.

DEFINITION 4.4. If $s^{-1}a$ and $s_1^{-1}a_1$ are in ${}_SR$ and if $(b, t) \in R \times S$ satisfies $ta = bs_1$, then we define the product $s^{-1}a * s_1^{-1}a_1$ by the rule

$$s^{-1}a * s_1^{-1}a_1 = (ts)^{-1}ba_1 .$$

The existence of the pair (b, t) is guaranteed by the left-Ore condition applied to $(a, s_1) \in R \times S$.

LEMMA 4.7. Multiplication in ${}_SR$ is well-defined.

Proof. (i) Multiplication is independent of the pair (b, t) and of the class representative of the first factor. To prove this let $s_2^{-1}a_2 = s^{-1}a$ and $(b', t') \in R \times S$ such that $t'a_2 = b's_1$. We must show that

$$s^{-1}a * s_1^{-1}a_1 = s_2^{-1}a_2 * s_1^{-1}a_1, \text{ i.e. } (ts)^{-1}ba_1 = (t's_2)^{-1}b'a_1 .$$

By Lemma 4.1 there exist $u, u' \in S$ such that $u(ts) = u'(t's_2)$. This and $s^{-1}a = s_2^{-1}a_2$ imply (by Malcev's property) that $uta = u't'a_2$. From this and the relations $uta = ubs_1$ and $u't'a_2 = u'b's_1$ it follows that $ubs_1 = u'b's_1$, therefore $ub = u'b'$ since $s_1 \in S$. Then

$$\begin{aligned}(ts)^{-1}ba_1 &= (uts)^{-1}uba_1 \\ &= (u't's_2)^{-1}u'b'a_1 \\ &= (t's_2)^{-1}b'a_1\end{aligned}$$

as required to prove.

(ii) Multiplication is independent of the class representative of the second factor. Let $s_2^{-1}a_2 = s_1^{-1}a_1$, then there exist $u_1, u_2 \in S$ such that $u_1a_1 = u_2a_2$ and $u_1s_1 = u_2s_2 = \sigma$. Applying Ore's condition to $(a, \sigma) \in R \times S$

we obtain $(b_1, t_1) \in R \times S$ such that $t_1 a = b_1 \sigma$, i.e. $t_1 a = b_1 u_1 s_1 = b_1 u_2 s_2$.

Therefore

$$s^{-1}a * s_1{}^{-1}a_1 = (t_1 s)^{-1} b_1 u_1 a_1 = (t_1 s)^{-1} b_1 u_2 a_2$$

and

$$s^{-1}a * s_2{}^{-1}a_2 = (t_1 s)^{-1} b_1 u_2 a_2$$

hence

$$s^{-1}a * s_1{}^{-1}a_1 = s^{-1}a * s_2{}^{-1}a_2 .$$

LEMMA 4.8. ${}_S R$ with addition and multiplication defined as above is an associative ring with identity.

<u>Proof</u>. (A) $({}_S R, +)$ is an abelian group where $0 = s^{-1}0$ for every $s \in S$ and $-s^{-1}a = s^{-1}(-a)$. Indeed if $u, u_1 \in S$ with $us = u_1 s_1 = \sigma$, then

$$s^{-1}a + s_1{}^{-1}0 = \sigma^{-1}(ua + u_1 0) = (us)^{-1}ua = s^{-1}a$$

and similarly

$$s_1{}^{-1}0 + s^{-1}a = s^{-1}a.$$

Also for every $u \in S$

$$s^{-1}a + s^{-1}(-a) = (us)^{-1}(ua + u(-a)) = (us)^{-1}0 = (us)^{-1}u0 = s^{-1}0.$$

To prove the associative law, given $s_i{}^{-1}a_i$ in ${}_S R$ for i=1, 2, 3 we find a "common denominator" σ, i.e. we can write $s_i{}^{-1}a_i = \sigma^{-1}a_i'$ (i=1, 2, 3) with $\sigma \in S$, then since addition is independent of the class representatives, the associativity in ${}_S R$ follows from the associativity in R.

(B) Multiplication is associative. Let $s_i{}^{-1}a_i$ be in ${}_S R$ for i=1, 2, 3. By Ore's condition applied to $(a_2, s_3) \in R \times S$ there exists $(a, s) \in R \times S$ such that $sa_2 = as_3$. This implies that

$$s_2^{-1}a_2 * s_3^{-1}a_3 = (ss_2)^{-1}aa_3 .$$

Similarly for $(a_1, ss_2) \in R \times S$ there exists $(b, t) \in R \times S$ such that $ta_1 = bss_2$ which then gives

$$s_1^{-1}a_1*(s_2^{-1}a_2*s_3^{-1}a_3) = s_1^{-1}a_1*(ss_2)^{-1}aa_3 = (ts_1)^{-1}baa_3 .$$

Since $ta_1 = bss_2$ we have $s_1^{-1}a_1*s_2^{-1}a_2 = (ts_1)^{-1}bsa_2$ and since $sa_2 = as_3$ we have $s_1^{-1}a_1*s_2^{-1}a_2 = (ts_1)^{-1}bas_3$.

Now apply Ore's condition to $(bas_3, s_3) \in R \times S$ to find $(b_1, t_1) \in R \times S$ satisfying $t_1bas_3 = b_1s_3$. But since s_3 is regular this implies $t_1ba = b_1$. Thus

$$(s_1^{-1}a_1*s_2^{-1}a_2)*s_3^{-1}a_3 = (ts_1)^{-1}bas_3*s_3^{-1}a_3 = (t_1ts_1)^{-1}b_1a_3$$

$$= (t_1ts_1)^{-1}t_1baa_3 = (ts_1)^{-1}baa_3$$

hence

$$(s_1^{-1}a_1*s_2^{-1}a_2)*s_3^{-1}a_3 = s_1^{-1}a_1*(s_2^{-1}a_1*s_3^{-1}a_3).$$

(C) Distributive law. Since for every pair of elements in ${}_SR$ there exists a "common denominator" it suffices to prove

(i) $s^{-1}a*(s_1^{-1}b+s_1^{-1}c) = s^{-1}a*s_1^{-1}b+s^{-1}a*s_1^{-1}c$

(ii) $(s_1^{-1}b+s_1^{-1}c)*s^{-1}a = s_1^{-1}b*s^{-1}a+s_1^{-1}c*s^{-1}a$.

To prove (i) we apply Ore's condition to $(a, s_1) \in R \times S$ and obtain $(p, t) \in R \times S$ such that $ta = ps_1$. Thus

$$s^{-1}a*s_1^{-1}b+s^{-1}a*s_1^{-1}c = (ts)^{-1}pb+(ts)^{-1}pc = (ts)^{-1}(pb+pc)$$
$$= (ts)^{-1}p(b+c) = s^{-1}a*s_1^{-1}(b+c)$$
$$= s^{-1}a*(s_1^{-1}b+s_1^{-1}c)$$

proving (i).

Applying Ore's condition to (b, s) and (c, s) in $R \times S$ we get (p_1, t_1) and (p_2, t_2) in $R \times S$ such that $t_1 b = p_1 s$ and $t_2 c = p_2 s$. Thus

$$s_1^{-1}b*s^{-1}a + s_1^{-1}c*s^{-1}a = (t_1 s_1)^{-1}p_1 a + (t_2 s_1)^{-1}p_2 a.$$

By Lemma 4.1 there exist $u_1, u_2 \in S$ such that $u_1 t_1 = u_2 t_2 = \sigma$ therefore $u_1 t_1 s_1 = u_2 t_2 s_1 = \sigma s_1$. Then

$$s_1^{-1}b*s^{-1}a+s_1^{-1}c*s^{-1}a = (u_1 t_1 s_1)^{-1}u_1 p_1 a + (u_2 t_2 s_1)^{-1}u_2 p_2 a$$
$$= (\sigma s_1)^{-1}(u_1 p_1 + u_2 p_2)a \qquad (1)$$

From $\sigma b = u_1 t_1 b = u_1 p_1 s$ and $\sigma c = u_2 t_2 c = u_2 p_2 s$ follows $\sigma(b+c) = (u_1 p_1 + u_2 p_2)s$, thus

$$s_1^{-1}(b+c)*s^{-1}a = (\sigma s_1)^{-1}(u_1 p_1 + u_2 p_2)a \qquad (2)$$

(1) and (2) imply (ii).

(D) In ${}_SR$, $s^{-1}s$ is the identity for every $u \in S$. By Lemma 4.1 if $s, s_1 \in S$ then there exist $u, u_1 \in S$ such that $us = u_1 s_1$, therefore $(s, s) \sim (s_1, s_1)$ for all $s, s_1 \in S$. Thus $s^{-1}s = s_1^{-1}s_1$ and we write $e = s^{-1}s$. If $s^{-1}a \in {}_SR$, then by Ore's condition applied to $(s, s) \in R \times S$ there exists $(b, t) \in R \times S$ such that $ts = bs$, therefore $b = t \in S$ because s is regular.

Thus

$$e*s^{-1}a = s^{-1}s*s^{-1}a = (ts)^{-1}ta = s^{-1}a \qquad (3)$$

Similarly by Ore's condition applied to $(a,s)\in R\times S$ we get $(b_1,t_1)\in R\times S$ with $t_1a=b_1s$ therefore

$$s^{-1}a*e = s^{-1}a*s^{-1}s = (t_1s)^{-1}b_1s = (t_1s)^{-1}t_1a = s^{-1}a \quad .$$

This and (3) imply that e is the identity element in ${}_SR$.

To complete the proof of Theorem 4.3 we show next that R can be imbedded into ${}_SR$ and that ${}_SR$ satisfies all the conditions in Definition 4.2.

LEMMA 4.9. ${}_SR$ with addition and multiplication defined as above is a left-quotient ring for R.

Proof. We have already seen that ${}_SR$ is an associative ring with identity. Next define a map $f: R \to {}_SR$ by $f(a)=s^{-1}sa$, for every a in R and some s in S. The map is well defined because if $s_1\in S$ and $f(a)= s_1^{-1}s_1a$ then by Lemma 4.1 there exist $u, u_1\in S$ with $us=u_1s_1$, therefore $usa=u_1s_1a$ and hence $s^{-1}sa=s_1^{-1}s_1a$.

The map f is an homomorphism of rings. Indeed

$$f(a+a_1) = s^{-1}s(a+a_1) = s^{-1}(sa+sa_1)=s^{-1}sa+s^{-1}sa_1 = f(a)+f(a_1)$$

for all a and a_1 in R. For the product we have

$$f(a)*f(a_1) = s^{-1}sa*s^{-1}sa_1 = (ts)^{-1}bsa_1$$

where $(b,t)\in R\times S$ and $tsa=bs$.

On the other hand

$$f(aa_1) = s^{-1}saa_1 = (ts)^{-1}tsaa_1 = (ts)^{-1}bsa_1$$

therefore

$$f(aa_1) = f(a)*f(a_1).$$

If $f(a) = f(a_1)$ then $s^{-1}sa = s^{-1}sa_1$ therefore there exist $u, u_1 \in S$ such that $us = u_1 s$ and $usa = u_1 sa_1$. These imply $u = u_1$ and therefore $a = a_1$. Since f is an embedding we can assume without loss of generality that $R \subseteq {}_S R$, thus we identity $f(a) = s^{-1}sa$ with a for all $a \in R$.

To conclude we verify condition (3) and (4) in Definition 4.2. Let $s_1 \in S$ then $s_1 = f(s_1) = s^{-1}ss_1$. Therefore $(ss_1)^{-1}s$ is an inverse of s_1 in ${}_S R$ because there exists $(b, t) \in R \times S$ with $tss_1 = bss_1$, therefore t=b and hence

$$s^{-1}ss_1 * (ss_1)^{-1}s = (ts)^{-1}bs = (ts)^{-1}ts = s^{-1}s = e.$$

Similarly $(ss_1)^{-1}s * s^{-1}ss_1 = e$. Hence every regular element of R is invertible in ${}_S R$. Finally if $s \in S$ and $a \in R$ then in ${}_S R$ we have

$$s^{-1} * a = (s_1 s)^{-1} s_1 * s_1^{-1} s_1 a = (ts_1 s)^{-1} bs_1 a$$

where $(b, t) \in R \times S$ with $ts_1 = bs_1$. Then $(ts_1 s)^{-1}bs_1 a = s^{-1}a$. Hence $s^{-1} * a = s^{-1}a$. Thus every element $s^{-1}a$ in ${}_S R$ can be written as the product of the inverse of a regular element s in R and an element a also in R. This justifies the notation $s^{-1}a$ for the equivalence class of (a, s). The proof of Theorem 4.3 is now complete.

REMARK. The ring ${}_S R$ that we have constructed above is sometimes called in the literature the <u>full left ring of quotients of R</u> or the <u>classical left ring of quotients of R</u>. If R satisfies the <u>right-Ore condition</u> with respect to S (i.e. $aS \cap sR \neq \phi$ for all $(a, s) \in R \times S$) then one defines R_S, the right analogue of ${}_S R$, and all the statements proved so far in this chapter remain valid with obvious modifications for R_S. We must stress though that in R_S the multiplication $*$ is defined by $a_1 s_1^{-1} * as^{-1} = a_1 b(st)^{-1}$ where $(b, t) \in R \times S$ satisfies $at = s_1 b$. With this in mind we can now prove the following

LEMMA 4.10. If R satisfies the left Ore condition as well as the right Ore condition then ${}_S R$ is isomorphic to R_S.

<u>Proof</u>. Define $\varphi: R_S \to {}_S R$ by $\varphi(as^{-1}) = \sigma^{-1}\alpha$ where $(\alpha, \sigma) \in R \times S$ and $\sigma a = \alpha s$. The existence of the pair (α, σ) is guaranteed by the left Ore condition. If also $(\alpha_1, \sigma_1) \in R \times S$ and satisfies $\sigma_1 a = \alpha_1 s$ then by Lemma 4.1 applied to σ, σ_1 we have $u\sigma = u_1\sigma_1$ with $u, u_1 \in S$. Therefore $u\alpha s = u\sigma a = u_1\sigma_1 a = u_1\alpha_1 s$, then $u\alpha = u_1\alpha_1$ since s is regular. Hence $\sigma^{-1}\alpha = \sigma_1^{-1}\alpha_1$ and φ is well defined. Next we prove

(A) $$\varphi(a_1 s_1^{-1} + a_2 s_2^{-1}) = \varphi(a_1 s_1^{-1}) + \varphi(a_2 s_2^{-1}).$$

In R_S we have $a_1 s_1^{-1} + a_2 s_2^{-1} = (a_1 u_1 + a_2 u_2)s^{-1}$ where $u_1, u_2 \in S$ and $s_1 u_1 = s_2 u_2 = s$. Therefore

$$\varphi(a_1 s_1^{-1} + a_2 s_2^{-1}) = \varphi((a_1 u_1 + a_2 u_2)s^{-1}) = \sigma^{-1}\alpha$$

where $(\alpha, \sigma) \in R \times S$ and

$$\sigma(a_1u_1+a_2u_2) = \alpha s = \alpha s_1u_1 = \alpha s_2u_2 .$$

Also $\qquad \varphi(a_is_i^{-1}) = \sigma_i^{-1}\alpha_i$ with $\sigma_ia_i = \alpha_is_i$ for i=1, 2 $\qquad$ (1)

Now in ${}_SR$ we have $\sigma_1^{-1}\alpha_1+\sigma_2^{-1}\alpha_2 = \tau^{-1}(\tau_1\alpha_1+\tau_2\alpha_2)$ where $\tau_1, \tau_2 \in S$ and $\tau_1\sigma_1 = \tau_2\sigma_2 = \tau$.

We must show that in ${}_SR$ is

$$\sigma^{-1}\alpha = \tau^{-1}(\tau_1\alpha_1+\tau_2\alpha_2) . \qquad (2)$$

By Lemma 4.1 there exist $\omega, \omega' \in S$ such that

$$\omega\sigma = \omega'\tau . \qquad (3)$$

Then

$$\begin{aligned} \omega'(\tau_1\alpha_1+\tau_2\alpha_2)s &= \omega'(\tau_1\alpha_1s+\tau_2\alpha_2s) \\ &= \omega'(\tau_1\alpha_1s_1u_1+\tau_2\alpha_2s_2u_2) \\ &= \omega'(\tau_1\sigma_1a_1u_1+\tau_2\sigma_2a_2u_2) \quad \text{(by (1))} \\ &= \omega'\tau(a_1u_1+a_2u_2) \\ &= \omega\sigma(a_1u_1+a_2u_2) \quad \text{(by (3))} \\ &= \omega\alpha s . \end{aligned}$$

Since s is regular the above implies that $\omega'(\tau_1\alpha_1+\tau_2\alpha_2) = \omega\alpha$ which together with (3) entails (2) and hence (A).

Next we show that

(B) $$\varphi(a_1 s_1^{-1} * a_2 s_2^{-1}) = \varphi(a_1 s_1^{-1}) * \varphi(a_2 s_2^{-1})$$

In R_S we have $a_1 s_1^{-1} * a_2 s_2^{-1} = a_1 b(s_2 t)^{-1}$ where

$$(b, t) \in R \times S \quad \text{and} \quad a_2 t = s_1 b. \tag{4}$$

Then $\varphi(a_1 s_1^{-1} * a_2 s_2^{-1}) = \varphi(a_1 b(s_2 t)^{-1}) = \rho^{-1}\beta$ where

$$(\beta, \rho) \in R \times S \quad \text{and} \quad \rho a_1 b = \beta s_2 t \tag{5}$$

On the other hand in ${}_S R$ we have

$$\varphi(a_1 s_1^{-1}) * \varphi(a_2 s_2^{-1}) = \sigma_1^{-1}\alpha_1 * \sigma_2^{-1}\alpha_2 = (\lambda\sigma_1)^{-1}\gamma\alpha_2$$

$$\text{with} \quad (\gamma, \lambda) \in R \times S \quad \text{and} \quad \lambda\alpha_1 = \gamma\sigma_2 . \tag{6}$$

Lemma 4.1 applied to ρ and $\lambda\sigma_1$ gives us $v, v' \in S$ such that

$$v\rho = v'\lambda\sigma_1 . \tag{7}$$

Therefore

$$\begin{aligned} v'\gamma\alpha_2 s_2 t &= v'\gamma\sigma_2 a_2 t && \text{by (1)} \\ &= v'\lambda\alpha_1 s_1 b && \text{by (4) and (6)} \\ &= v'\lambda\sigma_1 a_1 b && \text{by (1)} \\ &= v\rho a_1 b && \text{by (7)} \\ &= v\beta s_2 t && \text{by (5).} \end{aligned}$$

Since $s_2 t$ is regular this equality implies $v\beta = v'\gamma\alpha_2$ which together with (7) yields $\rho^{-1}\beta = (\lambda\sigma_1)^{-1}\gamma\alpha_2$. Hence (B) holds.

Given $\sigma^{-1}\alpha \in {}_S R$ by the right-Ore condition applied to $(\alpha, \sigma) \in R \times S$, we can find $(a, s) \in R \times S$ with $\alpha s = \sigma a$. Therefore $\varphi(as^{-1}) = \sigma^{-1}\alpha$, hence

φ is surjective. Finally, if $\varphi(a_1 s_1^{-1}) = \varphi(a_2 s_2^{-1}) = \sigma^{-1}\alpha$ then

$$\sigma a_i = \alpha s_i \quad \text{for} \quad i=1,2. \tag{8}$$

By the right analogue of Lemma 4.1 there exist $u_1, u_2 \in S$ such that

$$s_1 u_1 = s_2 u_2 = t. \tag{9}$$

Multiplication of (8) on the right by u_i yields

$$\sigma a_i u_i = \alpha s_i u_i = \alpha t \quad \text{for} \quad i=1,2$$

and substracting these two equalities we deduce $\sigma(a_1 u_1 - a_2 u_2) = 0$ which implies $a_1 u_1 = a_2 u_2$ because $\sigma \in S$. Thus $a_1 s_1^{-1} = a_2 s_2^{-1}$ in R_S and hence φ is injective, completing the proof of Lemma 4.10.

CHAPTER V

PRIME P.I.-RINGS HAVE A CLASSICAL RING OF QUOTIENTS

Let R be a ring with a ring of operators Ω. By this we mean that R is a Ω-module and for any $x, y \in R$ and any $\omega \in \Omega$ we have

$$\omega(xy) = (\omega x)y = x(\omega y).$$

Let $X_1, X_2, \ldots, X_n$ be a set of non-commuting indeterminates and consider a polynomial $f(X) = f(X_1, \ldots, X_n)$ with coefficients in Ω. We say that $f(X)$ is a <u>non-trivial identity of R</u> provided

(1) $f(r_1, r_2, \ldots, r_n) = 0$ for all $r_i \in R$, and

(2) $f(X)$ is not identically zero.

If R satisfies a non-trivial polynomial identity we say that R is a <u>P.I.-ring</u>.

We introduce some terminology and notation.

If $f(X)$ is a polynomial over Ω, then $\Omega(f)$ will denote the set of coefficients of $f(X)$. Observe that if $f(X)$ is a non-trivial identity of R, then $\Omega(f) \neq \{0\}$.

If R is a P.I.-ring, an identity of minimal degree will be called a <u>minimal identity</u>, and the corresponding polynomial a <u>minimal polynomial</u>. Finally we say that $f(X)$ is <u>multilinear of degree n</u> if and only if $f(X)$ is of the form

$$f(X) = \sum_{\sigma \in S_n} \omega_\sigma X_{\sigma(1)} \cdots X_{\sigma(n)}$$

where $\omega_\sigma \in \Omega$ and S_n denotes the group of all permutations of the symbols $\{1, 2, \ldots, n\}$.

EXAMPLES OF P.I.-RINGS.

1. Any commutative ring satisfies

$$f(X) = X_1X_2 - X_2X_1 = 0.$$

2. Let Ω be the field of reals and R the ring of quaternions over Ω. Then R is an algebra over Ω with basis $\{1, i, j, k\}$ such that $i^2 = j^2 = k^2 = 1$ and $ij = -ji = k$. Every quaternion x has a unique expression

$$x = x_0 + x_1 i + x_2 j + x_3 k, \quad x_i \in \Omega . \tag{1}$$

An easy verification shows that if in (1) is $x_0 = 0$, then x^2 is real, that is, $x^2 \in \Omega$. One also checks that for any two quaternions x and y the difference $xy - yx$ is of the form

$$xy - yx = a_1 i + a_2 j + a_3 k, \quad a_i \in \Omega$$

therefore $(xy-yx)^2 \in \Omega$. Moreover since for every quaternion z and every $\omega \in \Omega$ is $\omega z = z\omega$, the above remarks show that the ring of quaternions satisfy

$$f(X) = (X_1X_2 - X_2X_1)^2 X_3 - X_3(X_1X_2 - X_2 - X_1)^2 = 0.$$

3. Let $\Omega = \mathbb{Z}$ the ring of integers and let

$$R = \{M = \begin{bmatrix} a & 0 & 0 \\ b & a & 0 \\ c & d & a \end{bmatrix} : a, b, c, d \in \mathbb{Z}\}.$$

A simple but tedious verification shows that R is a ring, a $\mathbb{Z}$-module and that

$$n(M_1M_2) = (nM_1)M_2 = M_1(nM_2)$$

for every $M_1, M_2 \in R$ and $n \in \mathbb{Z}$.

For $i=1,2,3$ let

$$M_i = \begin{bmatrix} a_i & 0 & 0 \\ b_i & a_i & 0 \\ c_i & d_i & a_i \end{bmatrix}$$

where the a_i, b_i, c_i, d_i are arbitrary elements in $\mathbb{Z}$. Then one verifies that

$$M_1M_2 - M_2M_1 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ d_1b_2 - b_1d_2 & 0 & 0 \end{bmatrix} \qquad (1)$$

$$(M_1M_2 - M_2M_1)M_3 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ (d_1b_2 - b_1d_2)a_3 & 0 & 0 \end{bmatrix} \qquad (2)$$

and

$$M_3(M_1M_2 - M_2M_1) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ a_3(d_1b_2 - b_1d_2) & 0 & 0 \end{bmatrix}. \qquad (3)$$

(2) and (3) imply that R satisfies the identity

$$f(X) = (X_1X_2 - X_2X_1)X_3 - X_3(X_1X_2 - X_2X_1) = 0.$$

4. Let R be an algebra over a field F and consider $F[X] = F[X_1, X_2, \ldots, X_n]$, the free algebra generated by the non-commuting indeterminates $X_1, X_2, \ldots, X_n$ over F. In other words the elements of F[X] are polynomials in the variables X_i with coefficients in F. Using Kaplansky's terminology, the standard identity of degree n in F[X] is the polynomial

$$S(X_1, X_2, \ldots, X_n) = \sum_{\sigma \in S_n} (-1)^{\sigma} X_{\sigma(1)} \cdots X_{\sigma(n)}$$

where σ ranges over S_n, the set of all permutations of the symbols $\{1, 2, \ldots, n\}$ and $(-1)^{\sigma}$ is 1 for even permutations and -1 for odd permutations. Sometimes we shall use the notation $S_n(X)$ for the standard identity of degree n.

Assume now that R has dimension n over F, and let $\{v_1, v_2, \ldots, v_n\}$ be a basis for R over F. Let $r_1, \ldots, r_{n+1}$ be n+1 elements of R. Then each r_i can be expressed as a linear combination of the v_i's over F. Since $S_{n+1}(X)$ is multilinear it follows that $S(r_1, r_2, \ldots, r_{n+1})$ is a linear combination of terms of the form $S(v_{\sigma(1)}, \ldots, v_{\sigma(n+1)})$ where $\sigma \in S_{n+1}$, the symmetric group of degree n+1, and the $v_{\sigma(i)} \in \{v_1, v_2, \ldots, v_n\}$. But in $S(v_{\sigma(1)}, \ldots, v_{\sigma(n+1)})$ two arguments are equal, therefore $S(v_{\sigma(1)}, \ldots, v_{\sigma(n+1)}) = 0$ because $S_{n+1}(X)$ is multilinear. Then $S(r_1, r_2, \ldots, r_{n+1}) = 0$. Thus we have shown that every n-dimensional algebra over F satisfies the standard identity of degree n+1.

5. Let F be a field and F_n the ring of all nxn matrices with entries in F. Since $[F_n:F] = n^2$ by Example 4 we know that F_n satisfies $S_{n^2+1}(X)$.

However more is true. In a rather involved paper Amitsur and Levitzki [1] have shown that F_n actually satisfies S_{2n} and that this is in fact a minimal identity for F_n. Swan has given in [17] a quite elementary proof of this result as an application of graph theory.

It is not difficult to verify that

$$S(X_1, X_2, \dots, X_{n+1}) = X_1 S(X_2, \dots, X_{n+1}) - X_2 S(X_1 X_3 \dots X_{n+1}) + \dots$$
$$\dots + (-1)^n X_{n+1} S(X_1, \dots, X_n).$$

Therefore if R satisfies the standard identity of degree n, then it satisfies all the standard identities of higher degree. Observe that if the standard identity of degree 2 is satisfied by R, then R is commutative. With this in mind, we may regard a standard identity for R as a generalization of the commutative law.

When working with P.I.-rings it is convenient to be able to find some "nice" polynomial identities satisfied by R. The following provide us with such polynomials.

LEMMA 5.1. If R satisfies a non trivial polynomial identity of degree d, then it satisfies a multilinear identity of degree $\leq d$.

Proof. Assume R satisfies a non-trivial polynomial identity $f(X) = f(X_1, \dots, X_n)$ of degree d. If $f(X)$ is not linear in the variable X_1, then $f(X)$ considered as a polynomial in X_1 has degree $d_1 > 1$. Let X_{n+1} be an indeterminate different from the X_j, $j=1,2,\ldots,n$. Consider the polynomial

$$g(X_1 X_2, \ldots, X_n, X_{n+1}) = f(X_1+X_{n+1}, X_2, \ldots, X_n) - f(X_1, \ldots, X_n)$$

$$- f(X_{n+1}, X_2, \ldots, X_n).$$

By elementary linear algebra considerations one easily checks that

1. $0 \not\equiv g(X)$ is a polynomial identity of R
2. degree of $g(X) \leq$ degree of $f(X)$
3. for $j \neq 1, n+1$ the degree of g as polynomial in X_j is less than or equal to the degree of f as polynomial in X_j.
4. for $j=1, n+1$, the degree of g as polynomial in X_j is less than or equal to $d_1 - 1$.

If $g(X)$ has degree greater than 1 in one of the $n+1$ indeterminates X_j we repeat the argument for that variable. After a finite number of steps of this kind we obtain a polynomial $p(X) = p(X_1, \ldots, X_t)$ of degree $\leq d$ which is of degree ≤ 1 in all its variables. Moreover we may assume that every monomial of $p(X)$ is linear in every variable because if there were terms in $p(X)$ not involving X_j say, we may write

$$p(X) = q_1(X) + q_2(X)$$

where the monomials of q_1 contain X_j and those of $q_2(X)$ don't. Substituting in this X_j by 0 and X_i by $r_1 \in R$ for $i \neq j$ we get $q_2(r_1, \ldots, r_{j-1}, r_{j+1}, \ldots, r_t) = 0$. Therefore $q_2(X) = q_2(X_1, \ldots, X_{j-1}, X_{j+1}, \ldots, X_t)$ is also a polynomial identity of R of degree $\leq d$. Repeating this argument if necessary, we reach a multilinear identity $q(X)$ of degree $\leq d$ involving $m \leq d$ variables. Finally we may assume that

$$q(X) = \sum_{\sigma \in S_m} \omega_\sigma X_{\sigma(1)} \cdots X_{\sigma(m)}, \quad (\omega_\sigma \in \Omega)$$

because if the monomial $X_{\sigma(1)} \cdots X_{\sigma(m)}$ corresponding to the permutation $\sigma \in S_m$ does not appear in $q(X)$ we can always introduce it with coefficient $\omega_\sigma = 0$. This completes the proof of 5.1.

Unless mentioned otherwise, by a prime P.I.-ring we mean a prime ring R which satisfies polynomial identities over its centroid $\Omega(R)$. For this particular class of rings we have the following result due to Posner [16].

THEOREM 5.2. If R is a prime P.I.-ring, then R is a left and right Goldie ring.

Proof. By Lemma 5.1 we may assume that R satisfies

$$f(X) = \sum_{\sigma \in S_n} \omega_\sigma X_{\sigma(1)} \cdots X_{\sigma(n)}, \quad (\omega_\sigma \in \Omega(R)) \tag{1}$$

where $\omega_\sigma \neq 0$ for some $\sigma \in S_n$. Furthermore we may assume that $\omega = \omega_e \neq 0$ where e is the identity in S_n (otherwise relabel the indeterminates X_i so that this is the case).

Claim I. The length of a direct sum of non-zero left-ideals of R is at most n-1.

Assume that

$$I = I_1 \oplus I_2 \oplus \ldots \oplus I_n \qquad (2)$$

is a direct sum of non-zero left ideals of R and pick $y_j \in I_j$ for $j=1, 2, \ldots, n$.

Since $\omega_\sigma y_{\sigma(1)} \cdots y_{\sigma(n)} = (\omega_\sigma y_{\sigma(1)} \cdots y_{\sigma(n-1)}) y_{\sigma(n)}$ we have

$$0 = f(y_1, \ldots, y_n) = \sum_{\sigma \in S_n} \omega_\sigma y_{\sigma(1)} \cdots y_{\sigma(n)}$$

$$= \sum_{k=1}^{n} \Big(\sum_{\substack{\sigma \in S_n \\ \sigma(n)=k}} \omega_\sigma y_{\sigma(1)} \cdots y_{\sigma(n-1)} \Big) y_k . \qquad (3)$$

Then $u_k = \Big(\sum_{\substack{\sigma \in S_n \\ \sigma(n)=k}} \omega_\sigma y_{\sigma(1)} \cdots y_{\sigma(n-1)} \Big) y_k$ belongs to I_k for $k=1, 2, \ldots, n$.

Since the sum (2) is direct, all terms u_k in the sum (3) must be equal to 0. In particular

$$u_n = \Big(\sum_{\substack{\sigma \in S_n \\ \sigma(n)=n}} \omega_\sigma y_{\sigma(1)} \cdots y_{\sigma(n-1)} \Big) y_n = 0$$

and since this holds for arbitrary y_n in I_n we deduce

$$\Big(\sum_{\substack{\sigma \in S_n \\ \sigma(n)=n}} \omega_\sigma y_{\sigma(1)} \cdots y_{\sigma(n-1)} \Big) I_n = 0 \qquad (4)$$

for arbitrary $y_j \in I_j$, $1 \le j \le n-1$.

Since R is prime the left annihilator of the non-zero left-ideal I_n must be zero. Therefore (4) implies

$$\sum_{\substack{\sigma \in S_n \\ \sigma(n)=n}} \omega_\sigma y_{\sigma(1)} \cdots y_{\sigma(n-1)} = 0 \qquad (5)$$

for all y_j in I_j, $1 \le j \le n-1$.

Using (5) we can write

$$0 = \sum_{k=1}^{n-1} \Big(\sum_{\substack{\sigma \in S_n \\ \sigma(n)=n \\ \sigma(n-1)=k}} \omega_\sigma y_{\sigma(1)} \cdots y_{\sigma(n-2)} \Big) y_k$$

and repeat the above argument. Eventually we get $\omega I_1 = 0$. Then

$$0 = (\omega I_1)R = I_1(\omega R). \qquad (6)$$

By hypothesis $\omega \neq 0$ therefore the ideal ωR is not zero, thus (6) implies $I_1 = 0$ since R is prime. But this contradicts our hypothesis about the I_j's. Hence our claim is proved.

Claim II. Every properly ascending chain of left-annihilators has at most length n. Suppose

$$0 \subsetneqq I \subsetneqq I_2 \subsetneqq \cdots \subsetneqq I_n$$

where the I_j's are left annihilators. By the remarks made following Definition 1.3 we may assume that I_j is the left annihilator of a right-ideal H_j of R. By hypothesis $I_{j-1} \subsetneqq I_j$ for $j=2, \ldots, n$ therefore $I_j H_{j-1} \neq 0$.

Let k be the smallest positive integer such that there exists $\{\beta_\sigma \in \Omega(R) : \sigma \in S_k\}$ satisfying

(i) $\beta_e \neq 0$ where e denotes the identity in S_k

(ii) $\sum_{\sigma \in S_k} \beta_\sigma y_{\sigma(1)} \cdots y_{\sigma(k)} = 0$ whenever $y_j \in I_j$, $1 \leq j \leq k$.

Clearly such k exists and $k \leq n$ since R satisfies the multilinear identity (1) for which (i) and (ii) hold. Multiplying (ii) by H_{k-1} on the right we obtain

$$0 = \left(\sum_{\sigma \in S_k} \beta_\sigma y_{\sigma(1)} \cdots y_{\sigma(k)} \right) H_{k-1}$$

$$= \sum_{\sigma \in S_k} \beta_\sigma y_{\sigma(1)} \cdots y_{\sigma(k)} H_{k-1}$$

$$= \sum_{j=1}^{k} \left(\sum_{\substack{\sigma \in S_k \\ \sigma(k)=j}} \beta_\sigma y_{\sigma(1)} \cdots y_{\sigma(k-1)} \right) y_j H_{k-1}$$

$$= \left(\sum_{\substack{\sigma \in S_k \\ \sigma(k)=k}} \beta_\sigma y_{\sigma(1)} \cdots y_{\sigma(k-1)} \right) y_k H_{k-1} \qquad (7)$$

since for $j \leq k-1$ we have

$$\Big(\sum_{\sigma(k)=k} \beta_\sigma y_{\sigma(1)} \cdots y_{\sigma(k-1)}\Big) y_j \in I_j \subseteq I_{k-1} = (H_{k-1})_\ell .$$

Since y_k was arbitrary in I_k, from (7) we get

$$0 = \Big(\sum_{\substack{\sigma \in S_k \\ \sigma(k)=k}} \beta_\sigma y_{\sigma(1)} \cdots y_{\sigma(k-1)}\Big) I_k H_{k-1} \tag{8}$$

for all $y_j \in I_j$, $1 \leq j \leq k-1$. Therefore

$$\sum_{\substack{\sigma \in S_k \\ \sigma(k)=k}} \beta_\sigma y_{\sigma(1)} \cdots y_{\sigma(k-1)} = 0 \tag{9}$$

for all $y_j \in I_j$, $1 \leq j \leq k-1$, because R is prime and $I_k H_{k-1}$ is a non-zero left-ideal. But (9) contradicts the minimality of k and since the contradiction comes from the hypothesis $I_k H_{k-1} \neq 0$ we must have $I_k H_{k-1} = 0$, hence $I_k = I_{k-1}$ which proves Claim II.

I and II imply that R is a left Goldie ring. In a similar way we prove that R is a right Goldie ring completing thus the proof of 5.2.

The following theorem due to Amitsur [4, Theorem 9] plays a fundamental part in most of the theorems about prime rings satisfying polynomial identities over their centroid.

THEOREM 5.3. Let R be a prime P.I.-ring. Then for every $a \in R$ there exist positive integers $k = k(a)$ and $m = m(a)$ such that

(i) the left ideal $Ra^k+(a^k)_\ell$ contains a non-zero two sided ideal

(ii) the right ideal $a^mR+(a^m)_r$ contains a non-zero two sided ideal.

Proof. If $a=0$, then the statement is trivial because in this case for every positive integer i we have

$$Ra^i+(a^i)_\ell = a^iR+(a^i)_r = R.$$

If $a \neq 0$, then by Lemma 5.1 we may assume that R and in particular all its left-ideals of the form Ra^i satisfy a non-trivial multilinear identity. Among all the non-trivial multilinear identities satisfied by left-ideals of the form Ra^i pick one of minimal degree. We may assume that this identity has form

$$q(X_1,\dots,X_n) = \sum_{\sigma\in S_n} \omega_\sigma X_{\sigma(1)}\cdots X_{\sigma(n)}$$

$$= q_1(X_1,\dots,X_{n-1})X_n + q_2(X_1,X_2,\dots,X_n) \qquad (1)$$

where

(A) $\omega_\sigma \in \Omega(R)$ and $\omega_e \neq 0$ where e is the identity in S_n

(B) $q_1(X_1,\dots,X_{n-1}) = \sum_{\substack{\sigma\in S_n\\ \sigma(n)=n}} \omega_\sigma X_{\sigma(1)}\cdots X_{\sigma(n-1)}$

(C) $q_2(X_1,\dots,X_n) = \sum_{\substack{\sigma\in S_n\\ \sigma(n)\neq n}} \omega_\sigma X_{\sigma(1)}\cdots X_{\sigma(n)}$.

Let Ra^k satisfy $q(X)=0$. This means that for all i, Ra^i does not satisfy a non-trivial multilinear identity of degree less than n. Therefore

$q_1(X_1, \ldots, X_{n-1})$, which is not identically zero because of (A), being of degree $n-1$ is not an identity for Ra^{2k}. Then there exist elements $r_1, r_2, \ldots, r_{n-1}$ in R such that $q_1(r_1a^{2k}, \ldots, r_{n-1}a^{2k}) = b \neq 0$.

Moreover since $Ra^{2k} \subset Ra^k$ and Ra^k satisfies $q(X) = 0$ from (1) we deduce that for arbitrary r_n in R is

$$0 = q(r_1a^{2k}, \ldots, r_{n-1}a^{2k}, r_na^k)$$

$$= br_na^k + q_2(r_1a^{2k}, \ldots, r_{n-1}a^{2k}, r_na^k) \ . \qquad (2)$$

From the form of q_2 (see (C)) we have

$$q_2(r_1a^{2k}, \ldots, r_{n-1}a^{2k}, r_na^k) = ta^{2k} \quad \text{with} \quad t \in R$$

therefore from (2) it follows that $(br_n + ta^k)a^k = 0$. Thus $br_n + ta^k \in (a^k)_\ell$, hence

$$-ta^k + (br_n + ta^k) = br_n \in Ra^k + (a^k)_\ell \ .$$

Since this is true for arbitrary r_n in R and fixed b, we get $bR \subseteq Ra^k + (a^k)_\ell$. Furthermore since R is prime and $b \neq 0$ is also $bR \neq 0$, hence the non-zero two-sided ideal RbR is contained in the left-ideal $Ra^k + (a^k)_\ell$, proving 5.3 (i).

The proof of part (ii) is similar and we omit it.

Amitsur's Theorem has an important consequence, namely

COROLLARY 5.4. If R is a prime P.I.-ring, then for every regular element c of R

(i) Rc contains a non-zero two-sided ideal of R

(ii) cR contains a non-zero two-sided ideal of R.

The proof is immediate from Theorem 5.3 by observing that the regularity of c implies $(c^k)_\ell = 0 = (c^m)_r$, hence $Rc^k + (c^k)_\ell = Rc^k \subseteq Rc$ and $c^m R + (c^m)_r = c^m R \subseteq cR$.

We come now to the main theorem in this chapter

THEOREM 5.5. If R is a prime P.I.-ring, then R has a simple right and left quotient ring $Q(R)$.

Proof. Because of Theorem 4.3 and Lemma 4.10 it suffices to show that R satisfies both the left and right Ore conditions with respect to its subset S consisting of all regular elements. We remark that S is non-empty by 3.15 and 5.2.

Let $(a, s) \in R \times S$. By Corollary 5.4 there is a non-zero ideal $P \subseteq Rs$. Therefore $RP \subseteq Rs$. Since RP is a non-zero two-sided ideal in a prime Goldie ring, it contains a regular element s_1. Then $s_1 R \subseteq RP \subseteq Rs$, therefore there exists $a_1 \in R$ satisfying $s_1 a = a_1 s$. Thus R satisfies the left-Ore condition with respect to S. One similarly shows that R satisfies the right Ore condition. Then R has a left and right quotient ring $Q(R)$. We prove next that $Q = Q(R)$ is simple by showing that every non-zero two-sided ideal of Q coincides with Q.

If V is a non-zero two-sided ideal of Q then $Qbt^{-1}Q$ is also a non-zero two-sided ideal for some $0 \neq bt^{-1} \in V$ where $(b, t) \in R \times S$.

Since Q has a unit element e and $R \subseteq Q$ we have $ebt^{-1}t = b \in (Qbt^{-1}Q) \cap R$ therefore $(Qbt^{-1}Q) \cap R$ is a non-zero two-sided ideal of R, hence it contains a regular element u. Thus

$$V \supseteq Qbt^{-1}Q \supseteq Q[(Qbt^{-1}Q) \cap R] \supseteq Qu \supseteq (Qu^{-1})u = Q.$$

Hence $V = Q$ as required to prove ..

REMARK. Theorem 5.5 is a special case of a more general theorem due to Goldie, namely, the ring R has a simple Artinian right quotient ring if and only if R is a prime Goldie ring. A neat account of Goldie's Theorem can be found in Herstein's book [10, Chapter 7].

CHAPTER VI

KAPLANSKY'S THEOREM

This chapter is devoted to the proof of a beautiful result of Kaplansky [12, Theorem 1] about primitive P.I.-rings. Our approach follows essentially Martindale's [14]. We start by recalling some basic definitions and well known facts from the theory of rings which will be stated without proofs; these can be found, for example, in Lambek's book [13, §3.3 and §3.4].

A right ideal I of a ring R is called minimal if I is an irreducible right R-module (cf. Definition 1.7). A theorem due to Brauer asserts that if I is a minimal right ideal of R, then either $I^2 = 0$ or $I = eR$ where $e^2 = e \in I$. Hence every minimal right ideal of a semiprime ring is of the form eR where $e^2 = e \in R$ (i.e. e is idempotent).

The (right)-socle of R, denoted by SocR, is the sum of all the minimal right-ideals of R. If R has no minimal right ideals, then SocR = 0. The socle of R is a two-sided ideal. If R = SocR, then R is called completely reducible.

The left socle of R is defined similarly. For semiprime rings the left and right socle coincide.

LEMMA 6.1. If R is a prime right-Artinian ring, then R is simple.

Proof. Assume I is a non-zero ideal of R. Since I is right-Artinian, there is a minimal non-zero right ideal K contained in I and since R is prime K is generated by a non-zero idempotent. Thus I contains a non-zero idempotent. Therefore the set $\{(e)_r \cap I : 0 \neq e^2 = e \in I\}$ is non-empty, hence it has a minimal element $E = (e)_r \cap I$.

If $E \neq 0$, then the set of non-zero right ideals of R contained in E is non-empty, so it contains a minimal element M because R is right-Artinian. Clearly M is a minimal right ideal of R, therefore $M = fR$ where $f^2 = f \neq 0$. Since $f \in M \subset E$ we have $ef = 0$. Let $\epsilon = e+f-fe$. Then $\epsilon \in I$ and a short computation shows that $\epsilon^2 = \epsilon$. Also

$$\epsilon f = (e+f-fe)f = f^2 = f \neq 0,$$

therefore $\epsilon \neq 0$. Moreover $(\epsilon)_r \subset (e)_r$ because if $\epsilon x = 0$, then

$$0 = e(\epsilon x) = e(e+f-fe)x = e^2 x = ex.$$

Therefore $(\epsilon)_r \cap I \subset (e)_r \cap I = E$ and the inclusion is strict since $f \in E$ but $f \notin (\epsilon)_r \cap I$. This contradicts the minimality of E. Then we cannot have $E \neq 0$. But then since I is a non-zero two-sided ideal in a prime ring, I is essential so $(e)_r \cap I = E = 0$ forces $(e)_r = 0$. Thus I contains a right regular idempotent e. Since for all x in R is $e(x-ex) = 0$ we conclude $R = eR \subset I$, thus $R = I$. Hence R contains no proper ideals different from 0.

The same argument given above proves the following

LEMMA 6.2. If R is a prime right Goldie ring with a non-zero minimal ideal, then R is simple Artinian.

Proof. By hypothesis R has a non-zero minimal right ideal P so $P = e_1 R$ where $0 \neq e_1 = e_1^2$. Then $\mathrm{Soc}R = S \neq 0$ and S contains idempotents. Since R is right finite dimensional and S is the direct sum of all minimal right ideals of R we must have $S = P_1 \oplus P_2 \oplus \ldots \oplus P_n$ for some integer n and where the P_i's are minimal right ideals. Since the P_i are minimal they are Artinian as right R-modules, hence S is an Artinian right R-module (cf. Lambek [13, page 22]).

If we can prove that R = S, we will have shown that R is right Artinian, hence simple by Lemma 6.1. To show that R = S it suffices to prove that S contains a right regular idempotent e. Actually, the same proof given in Lemma 6.1 holds for Lemma 6.2 with I replaced by S because if we analyse the argument in 6.1 we see that all we needed was the minimum condition on right ideals contained in a two-sided ideal I which contains a non-zero idempotent. S was proved to satisfy all these conditions, so the proof of Lemma 6.2 is completed.

A classical result by Artin and Wedderburn states that if R is simple Artinian, then there exists a unique integer n and a division ring D, unique up to isomorphism, such that R is isomorphic to D_n, the ring of all n×n matrices over D. Conversely for every integer n and every division ring D, the ring D_n is simple Artinian, (cf. Herstein [10, page 48]). In view of the Artin-Wedderburn Theorem, Lemma 6.2 asserts that every prime right-Goldie ring with a non-zero minimal ideal is isomorphic to D_n for some integer n and some division ring D. This observation permits us to prove the following Lemma which is crucial in our approach to Kaplansky's Theorem. In what follows , by a primitive P.I.-ring we mean a primitive ring satisfying polynomial identities over its centroid $\Omega(R)$.

LEMMA 6.3. If R is a right-primitive P.I.-ring then there exists a unique integer n and a unique division ring D such that R is isomorphic to D_n. Moreover D is also a P.I.-ring.

Proof. Since R is right-primitive there exists a faithful irreducible right-R-module A and we may assume that $A = R/M$ where M is a maximal right-ideal of R (cf. Lemma 1.10). We claim that M is not essential. Since R is primitive is semiprime, therefore if M is essential, by Lemma 3.14 M must contain a regular element c. But then by Corollary 5.4 there is a non-zero ideal $I \subset cR \subset M$. Since S is faithful and $AI = 0$, we get a contradiction. Then M is not essential therefore there exists a non-zero right ideal P such that $M \cap P = 0$. Since M is maximal, we get $R = M \oplus P$, hence P is a non-zero minimal right ideal. By Lemma 6.2 and the Artin-Wedderburn Theorem, we conclude that $R \cong D_n$ for some integer n and division ring D. Moreover since D_n is simple, by 2.6 we have $\Omega(D_n) = C(D_n)$, so D_n satisfies polynomial identities over its center $C(D_n)$. Now observe that $C(D_n)$ consists of all $n \times n$ matrices having all entries in the main diagonal equal to $c \in C(D)$ and the remaining entries equal to 0. So $C(D_n) \cong C(D)$. Since D is imbedded in D_n and D_n is a P.I.-ring, we conclude that D satisfies polynomial identities over its center $C(D)$.

LEMMA 6.4. Let D be a division ring with center C and $a, b \in D$, $b \neq 0$. Then $ab^{-1} \in C$ if and only if $axb = bxa$ for all x in D.

Proof.
$$ab^{-1} \in C \Rightarrow ab^{-1}(bxb) = (bxb)ab^{-1}$$
$$\Rightarrow axb = (bx)[b(ab)^{-1}] = bx[(ab^{-1})b] = bxa$$

for all $x \in D$.

Conversely if $axb = bxa$ for all x in D, then

$$b^{-1}ax = xab^{-1} \qquad \text{for all } x \in D. \qquad (1)$$

But $a(b^{-1}b^{-1})b = b(b^{-1}b^{-1})a$ by hypothesis so $ab^{-1} = b^{-1}a$, hence (1) implies $ab^{-1} \in C$.

COROLLARY 6.5. Let D be a division ring with center C. Let $a, b \in D$. If $axb = bxa$ for all $x \in D$, then a and b are linearly dependent over C.

Proof. If $a = 0$ or $b = 0$ the result is trivial. If a and b are different from 0, then $ab^{-1} \in C$, hence $a = (ab^{-1})b$.

We now adapt Martindale's ideas to our particular case (cf. Herstein [11, Theorem 1.2, page 2]).

THEOREM 6.6. (MARTINDALE). Let D be a division ring with center C. Let $a_1, \ldots, a_n \in D$ be linearly independent over C and let $b_1, \ldots, b_n \in D$,

$b_1 \neq 0$. Then, if $B = \{\sum_{i=1}^{n} a_i x b_i : x \in D\}$ is a finite dimensional vector space over C, then D is a finite dimensional algebra over C.

Proof. The proof is by induction on n. If $n = 1$, the hypothesis says that $B = a_1 D b_1$ is a finite dimensional vector space over C. But since D is a division ring and $a_1 \neq 0$, $b_1 \neq 0$, we have $a_1 D b_1 = D$. This proves the result for $n = 1$.

Assume now that Theorem 6.6 holds for all $m < n$, and suppose $B = \{\sum_{i=1}^{n} a_i x b_i : x \in D\}$ is a finite dimensional vector space over C, where the a_i are linearly independent over C and $b_1 \neq 0$. Let $t \in D$. Then $B' = \{\sum_{i=1}^{n} a_i x b_i t b_1 : x \in D\} \subset B t b_1$ so B' is finite dimensional over C.

We also have $\{\sum_{i=1}^{n} a_i (x b_1 t) b_i : x \in D\} \subset B$ therefore

$$B^{*} = \{\sum_{i=1}^{n} a_i x (b_i t b_1 - b_1 t b_i) : x \in D\} \subset B + B t b_1$$

so B^{*} is finite dimensional over C. For i=1, we have $b_1 t b_1 - b_1 t b_1 = 0$; thus at most n-1 of the elements $b_i t b_1 - b_1 t b_i$ are not 0. If for $i = 1, 2, \ldots, n$ and for all $t \in D$ is $b_i t b_1 = b_1 t b_i$; then by Corollary 6.5 we can write $b_i = q_i b_1$ with $q_i \in C$, $i = 1, 2, \ldots, n$, which gives

$$\sum_{i=1}^{n} a_i x b_i = \sum_{i=1}^{n} a_i x q_i b_1 = \sum_{i=1}^{n} (a_i q_i) x b_1 = (\sum_{i=1}^{n} a_i q_i) x b_1$$

and since

$$\sum_{i=1}^{n} q_i a_i = \sum_{i=1}^{n} a_i q_i = a_1' \neq 0$$

(because the a_i are linearly independent over C) we obtain $B^* = a_1'Db_1$, i.e. we are back in the case $n=1$. Now if for some $i \neq 1$ and some $t_0 \in D$ is $b_i t_0 b_1 - b_1 t_0 \neq 0$ then we have in B^* the hypothesis of our theorem applied to a situation of $m \leq n-1$ elements, which by induction concludes the proof.

Amitsur in [3] studied rings which satisfy a more general type of polynomial relation. One considers a ring R which is an algebra over a field F and forms the free product $R\langle X\rangle$ of the ring R and the free associative ring $F[X_1, X_2, \ldots]$ in the non-commuting indeterminates $X_1, X_2, \ldots$. The elements of $R\langle X\rangle$ are of the form

$$f(X) = \Sigma \beta_k a_{i_1} \pi_{j_1} a_{i_2} \pi_{j_2} \ldots a_{i_k} \pi_{j_k} a_{i_{k+1}}$$

where $\beta_k \in F$, the π_j are monomials in the indeterminates X_j and the elements $a_i \in R$ appear both as coefficients and between the monomials π_j.

DEFINITION 6.1. We say that <u>R satisfies a non-trivial generalized polynomial identity</u> (in short R is a G.P.I.-ring) if there exists a non-zero element $f(X_1, \ldots, X_n)$ in $R\langle X\rangle$ which vanishes identically on R.

We remark that, as it was done for P.I.-rings (cf. Lemma 5.1), if R is a G.P.I.-ring, then one can easily show that R satisfies a generalized polynomial identity which is both homogeneous and multilinear. A complete account of the more important properties of $R\langle X\rangle$ can be found in section 4 of the above mentioned paper by Amitsur.

The following result is also due to Martindale [14, Theorem 3].

THEOREM 6.7. Let D be a division ring satisfying a non-trivial polynomial identity over its center C. Then D is a finite dimensional vector space over C.

Proof. Since D is a P.I.-ring, it is also a G.P.I.-ring. Consider a generalized polynomial identity of minimal degree n. We may assume this identity is homogeneous and multilinear of degree n so that it has the form

$$f(X) = \sum_{i=1}^{m} a_i X_1 f_i + \sum_{i=1}^{k} g_i X_1 b_i + \Sigma p_i X_1 q_i \qquad (1)$$

where

1. $a_1, \ldots, a_m \in D$ are linearly independent over C
2. $b_1, \ldots, b_k \in D$
3. the f_i and g_i are generalized multilinear polynomials of degree n-1
4. the p_i and q_i are generalized polynomials of positive degree.

In other words we have broken f up into those monomials where X_1 is the first variable on the left in each monomial, where X_1 is the last variable on the right in each monomial, and finally, where X_1 appears in the middle of each monomial.

For $u(X_1, \ldots, X_n) \in D\langle X\rangle$ and $s_1, \ldots, s_n \in D$, let $\bar{u}$ denote the element $u(s_1, \ldots, s_n)$ in D. Since (1) vanishes identically in D we have for arbitrary $s_1, \ldots, s_n \in D$:

$$\sum_{i=1}^{m} a_i s_1 \bar{f}_i + \sum_{i=1}^{k} \bar{g}_i s_1 b_i + \Sigma \bar{p}_i s_1 \bar{q}_i = 0 \tag{2}$$

For $t \in D$ multiplying (2) on the right by tb_1 we obtain

$$\sum_{i=1}^{m} a_i s_1 \bar{f}_i t b_1 + \sum_{i=1}^{k} \bar{g}_i s_1 b_i t b_1 + \Sigma\, \bar{p}_i s_1 \bar{q}_i t b_1 = 0 \tag{3}$$

Recalling that the generalized polynomials f_i, g_i, p_i and q_i do not involve the variable X_1, if we replace in (1) X_1 by $s_1 b_1 t$ and X_j by s_j for $j=2, 3, \ldots, n$ we get

$$\sum_{i=1}^{m} a_i s_1 b_1 t \bar{f}_i + \sum_{i=1}^{k} \bar{g}_i s_1 b_1 t b_i + \Sigma\, \bar{p}_i s_1 b_1 t \bar{q}_i = 0 \tag{4}$$

Subtracting (4) from (3) we obtain

$$\sum_{i=1}^{m} a_i s_1 (\bar{f}_i t b_1 - b_1 t \bar{f}_i) + \sum_{i=2}^{k} \bar{g}_i s_1 (b_i t b_1 - b_1 t b_i) + \tag{5}$$

$$+ \Sigma\, \bar{p}_i s_1 (\bar{q}_i t b_1 - b_1 t \bar{q}_i) = 0$$

and this holds for all $s_1, \ldots, s_n, t \in D$.

We remark that in passing from (1) to (5) we have shortened in length by one the middle sum in (5).

We claim that if

$$\bar{f}_1 t b_1 - b_1 t \bar{f}_1 = 0 \qquad \text{for all } s_2, s_3, \ldots, s_n, t \in D \qquad (6)$$

then the theorem is proved. Indeed, since f_1 is of degree n-1, we may choose $r_2, r_3, \ldots, r_n \in D$ such that $f_1(r_2, \ldots, r_n) \neq 0$ so the generalized polynomial of degree 1 defined by $h(X_2) = f_1(X_2, r_3, \ldots, r_n)$ is non-trivial. Then $h(X_2)$ can be expressed as

$$h(X_2) = \sum_{i=1}^{j} c_i X_2 d_i$$

where the c_i are linearly independent over C and the d_i are non-zero elements of D. Moreover (6) and Corollary 6.5 imply that $\bar{f}_1 = f_1(s_2, \ldots, s_n) = \lambda(s_2, \ldots, s_n) b_1$ where $\lambda(s_2, \ldots, s_n) \in C$.

In particular this implies that

$$B = \{h(x) = \sum_{i=1}^{j} c_i x d_i : x \in D\} \subset C b_1 .$$

Therefore B is a finite dimensional vector space over C, hence Theorem 6.7 follows from 6.6.

If (6) does not hold, we may choose $s_2', \ldots, s_n', t_0 \in D$ such that $\bar{f}_1 t_0 b_1 - b_1 t_0 \bar{f}_1 \neq 0$. Now set

$$f_i' = f_i t_0 b_1 - b_1 t_0 f_i, \quad b_i' = b_i t_0 b_1 - b_1 t_0 b_i, \quad \text{and} \quad q_i' = q_i t_0 b_1 - b_1 t_0 q_i .$$

Then because of (5) we have shown that D satisfies the new generalized polynomial identity

$$\sum_{i=1}^{m} a_i X_1 f_i' + \sum_{i=2}^{k} q_i X_1 b_i' + \Sigma p_i X_1 q_i' = 0 \qquad (7)$$

where $c_1 = f_1'(s_2', \ldots, s_n') \neq 0$. (7) is not a trivial identity, since this would imply that $\sum_{i=1}^{m} a_i X_1 f_i'$ were trivial. Setting $c_i = f_i'(s_2', \ldots, s_n')$ we would then have that $\sum_{i=1}^{m} a_i x c_i = 0$ for all $x \in D$. Since D is a division ring and $c_1 \neq 0$ we therefore know that $a_1 = 0$, therefore $a_1, \ldots, a_m$ are not linearly independent over C contradicting our assumption. The most important fact about the identity (7) is that the variable X_1 now occurs at least one fewer time as a last variable than in (1). Moreover the a_i's have remained unchanged, and the order in which the variables appear in (7) is the same as in (1). Repeating this argument at most k times, we then transform our original identity (1) into a new one of the form

$$\sum_{i=1}^{m} a_i X_1 f_i(X_2, \ldots, X_n) + g(X_1, \ldots, X_n) = 0 \qquad (8)$$

in which X_1 never appears as the last variable in any monomial of g(X). Assume without loss of generality that $X_1, X_2, \ldots, X_r$, $r \leq n$, are those variables which occured first in some monomial of the original identity (1). Applying the above process to each of these X_i we obtain a new identity satisfied by D of the form

$$\Sigma a_i^{(1)} X_1 f_i^{(1)} + \Sigma a_i^{(2)} X_2 f_i^{(2)} + \ldots + \Sigma a_i^{(r)} X_r f_i^{(r)} = 0 \quad (9)$$

where

(i) the set $\{a_i^{(j)}\}$ is linearly independent over C for each $j \in \{1, 2, \ldots, r\}$.

(ii) the $f_i^{(j)}$ are non-zero generalized polynomials of degree n-1, in which none of the $X_1, \ldots, X_r$ ever appear as the last variable in any monomial.

But some variable has to occur last in each monomial, therefore we must have $r < n$. My the minimality of n we must then have $f_1^{(1)}(r_2, \ldots, r_n) \neq 0$ for some $r_2, \ldots, r_n \in D$. Let

$$\varphi_i^{(1)}(X_2, \ldots, X_{n-1}) = f_i^{(1)}(X_2, \ldots, X_{n-1}, r_n)$$

$$\varphi_i^{(2)}(X_1, X_3, \ldots, X_{n-1}) = f_i^{(2)}(X_1, X_3, \ldots, X_{n-1}, r_n)$$

$$\vdots$$

$$\varphi_i^{(r)}(X_1, \ldots, X_{r-1}, X_{r+1}, \ldots, X_{n-1}) = f_i^{(r)}(X_1, \ldots, X_{r-1}, X_{r+1}, \ldots, X_{n-1}, r_n)$$

Then from (9) we get that

$$\Sigma a_i^{(1)} X_1 \varphi_i^{(1)} + \ldots + \Sigma a_i^{(r)} X_r \varphi_i^{(r)} = 0 \qquad (10)$$

is a generalized polynomial identity for D of degree n-1. If (10) is trivial then, it would follow that $\Sigma a_i^{(1)} X_1 \varphi_i^{(1)}$ is trivial. Letting $c_i = \varphi_i^{(1)}(r_2, \ldots, r_n)$, we would then have that $\Sigma a_i^{(1)} x c_i = 0$ for all $x \in D$. Since D is a division ring and $c_1 \neq 0$ this would imply that $a_1^{(1)} = 0$, which contradicts the linear indepedence of the set $\{a_i^{(1)}\}$. Then (10) is a non-trivial generalized polynomial identity and this contradicts the minimality of n. Martindale's Theorem has thus been proved.

As a consequence of Martindale's Theorem we obtain a classical result due to Kaplansky [12, Theorem 1].

THEOREM 6.8. Let R be a primitive ring satisfying a non-trivial polynomial identity over its centroid. Then R is a finite dimensional central simple algebra.

Proof. The theorem follows from Lemma 6.3, Theorem 6.7 and the fact that D_n is finite dimensional over D. Therefore

$$[R:C(R)] = [D_n : C(D_n)] = [D_n:D][D:C(D_n)]$$

is finite.

Before concluding this chapter, we must remark that Amitsur [4, Theorem 1] has shown that if d is the minimal degree of the identities satisfied by the right-primitive ring R, then $[R:C(R)] = m^2$ and $d = 2m$.

CHAPTER VII

STRUCTURE THEOREM OF PRIME P.I.-RINGS

Using the method of ultra products Amitsur [4] has generalized an earlier theorem due to Posner [16]. The theorem under consideration says that every prime ring with polynomial identities over its centroid has a left and right quotient ring which is a finite dimensional simple algebra over its center. Goldie in [8] has simplified Amitsur's proof by avoiding the method of ultra products. We follow here Goldie's approach. Before proving the main theorem we need some preliminary results.

LEMMA 7.1. If a ring R (not necessarily prime) is a P.I.-ring, then the polynomial ring R[Y] in a commutative indeterminate Y is also a P.I.-ring. Moreover, R and R[Y] have the same multilinear identities.

Proof. By Lemma 5.1, if R is a P.I.-ring, then R satisfies multilinear identities. We assume that the ring of operators Ω of R, which contains the coefficients of the identities of R, is extended to operate on R[Y] by defining

$$\omega(\sum_i a_i Y^i) = \sum_i (\omega a_i) Y^i$$

for every ω in Ω and $\sum_i a_i Y^i$ in R[Y]. Now let $f_j(Y) = \sum_i a_{ji} Y^i$, $(j=1, 2, \ldots, n)$ be arbitrary polynomials in R[Y] and

$$f(X_1, \ldots, X_n) = \sum_{\sigma \in S_n} \omega_\sigma X_{\sigma(1)} \cdots X_{\sigma(n)}$$

a multilinear identity of R. Since for every permutation σ of $(1, 2, \ldots, n)$ we have

$$f_{\sigma(1)} \cdots f_{\sigma(n)} = \sum_k b_{\sigma, k} Y^k$$

where

$$b_{\sigma, k} = \sum_{i_1 + \ldots + i_n = k} a_{\sigma(1), i_1} \cdots a_{\sigma(n), i_n}$$

we get

$$f(f_1, \ldots, f_n) = \sum_\sigma \omega_\sigma (\sum_k b_{\sigma, k} Y^k) = \sum_\sigma \sum_k (\omega_\sigma b_{\sigma, k}) Y^k$$

$$= \sum_k (\sum_\sigma \omega_\sigma b_{\sigma, k}) Y^k . \qquad (1)$$

But

$$\sum_\sigma \omega_\sigma b_{\sigma, k} = \sum_\sigma \omega_\sigma \sum_{i_1 + \ldots + i_n = k} a_{\sigma(1), i_1} \cdots a_{\sigma(n), i_n}$$

$$= \sum_{i_1 + \ldots + i_n = k} \sum_\sigma \omega_\sigma a_{\sigma(1), i_1} \cdots a_{\sigma(n), i_n} = 0$$

because the $a_{j, i} \in R$ and R satisfies $f(X) = 0$. Therefore from (1) we get that $R[Y]$ also satisfies $f(X) = 0$.

The converse result is trivial because if $R[Y]$ satisfies a multilinear identity so does R since it is contained in $R[Y]$.

The next result also holds for arbitrary P.I.-rings and is due to Amitsur [4, Lemma 5].

LEMMA 7.2. If a ring R (not necessarily prime) satisfies a non-trivial identity $f(X_1, \ldots, X_n)$ with set of coefficients $\Omega(f) \subseteq \Omega(R)$ and if P is a proper prime ideal of R, then

(1) $\omega P \subseteq P$ for all $\omega \in \Omega(f)$, and either

(2) $\Omega(f)R \subseteq P$ or

(2′) f is also a non-trivial identity of R/P and if $\omega R \not\subseteq P$ and $\omega r \in P$, then $r \in P$.

Proof. (1) For all $\omega \in \Omega(f)$ we have

$$R(\omega P) \subseteq (\omega R)P \subseteq RP \subseteq P .$$

Since P is prime and $R \neq P$ it follows that $\omega P \subseteq P$.

(2) If $\omega \in \Omega(R)$, then ω induces an element $\bar{\omega}$ in $\Omega(R/P)$, namely $\bar{\omega}$ is defined by $\bar{\omega}(r+P) = \omega r + P$ for all $r \in R$.

Let $f(X_1, \ldots, X_n)$ be a polynomial identity of R. As we know we may assume that

$$f(X_1, X_2, \ldots, X_n) = \sum_{\sigma \in S_n} \omega_\sigma X_{\sigma(1)} \cdots X_{\sigma(n)} .$$

Then by the above remark one easily verifies that

$$\sum_{\sigma \in S_n} \bar{\omega}_\sigma X_{\sigma(1)} \cdots X_{\sigma(n)}$$

is an identity of R/P. It is clear that this identity is non-trivial if and only if $\Omega(f)R \not\subseteq P$.

Finally, if $\Omega(f)R \not\subseteq P$, then there exists $\omega \in \Omega(f)$ with $\omega R \not\subseteq P$. Let

$T = \{r \in R : \omega r \in P\}$. Then T is a two-sided ideal of R and since $\omega R \not\subset P$ we have $T \neq R$. Then $(\omega R)T = R(\omega T) \subseteq RP \subseteq P$. Since P is prime and $\omega R \not\subset T$ we conclude that $T \subseteq P$. But also $P \subseteq T$ by (1) and the definition of T. Hence $P = T$, which proves (2′).

REMARK. In what follows we assume that R is a semiprimitive prime ring satisfying a non-trivial multilinear identity

$$f(X) = \sum_{\sigma \in S_n} \omega_\sigma X_{\sigma(1)} \cdots X_{\sigma(n)} \qquad \text{where } \omega_\sigma \in \Omega(R).$$

Let $\{P_\alpha : \alpha \in A\}$ be the set of all right-primitive ideals of R. Write $A = \Lambda \cup \Lambda'$ where

$$\Lambda = \{\alpha \in A : \Omega(f)R \not\subseteq P_\alpha\} \text{ and } \Lambda' = \{\alpha \in A : \Omega(f)R \subseteq P_\alpha\}.$$

Following Goldie [8] we say that the right-primitive ideal P_α is <u>trivial</u> (with respect to f(X)) if $\alpha \in \Lambda'$ and <u>non-trivial</u> if $\alpha \in \Lambda$. Since f(X) is a non-trivial identity there exists $\omega \in \Omega(f)$ such that $\omega R \neq 0$, therefore $\Omega(f)R \neq 0$. Then

$$0 \neq \Omega(f)R \subseteq \bigcap_{\alpha \in \Lambda'} P_\alpha . \tag{1}$$

Since R is semiprimitive we have $\bigcap_{\alpha \in A} P_\alpha = 0$ and since

$$\Big(\bigcap_{\alpha \in \Lambda} P_\alpha\Big)\Big(\bigcap_{\alpha \in \Lambda'} P_\alpha\Big) \subseteq \bigcap_{\alpha \in A} P_\alpha = 0$$

we deduce $\bigcap_{\alpha \in \Lambda} P_\alpha = 0$ because of (1) and the primeness of R. We know

(Theorem 5.2) that R is a Goldie ring, therefore it contains regular elements (cf. Corollary 3.15). Let c be a regular element of R. Then there exists a non-zero two-sided ideal $T \subseteq cR$ (Corollary 5.4). Define $\Lambda(T) = \{\alpha \in \Lambda : T \not\subset P_\alpha\}$. Observe that $\Lambda(T)$ is non-empty since $\bigcap_{\alpha \in \Lambda} P_\alpha = 0$. Also if $\alpha \in \Lambda(T)$, then $c \notin P_\alpha$ because otherwise $T \subseteq cR \subseteq P_\alpha$ contradicting the definition of $\Lambda(T)$. Therefore $c+P_\alpha = \bar{c} \neq 0$ in R/P_α for all $\alpha \in \Lambda(T)$. Moreover since $\Lambda(T) \subset \Lambda$ is $\Omega(f)R \notin P_\alpha$ and since P_α is prime (because is primitive) by Lemma 7.2 we conclude that f(X) is also a non-trivial identity of R/P_α for all $\alpha \in \Lambda(T)$. But then R/P_α is simple by Kaplansky's Theorem, therefore since T/P_α is a non-zero ideal of R/P_α we deduce $T/P_\alpha = R/P_\alpha$ so that $0 \neq \bar{c}$ is a unit of the ring R/P_α, for all $\alpha \in \Lambda(T)$.

Next we observe that since $T \neq 0$ then $I = \bigcap\{P_\alpha : \alpha \in \Lambda,\ T \subset P_\alpha\} \neq 0$. Therefore $J = \bigcap\{P_\alpha : \alpha \in \Lambda(T)\} = 0$ because R is prime and $IJ \subseteq \bigcap_{\alpha \in \Lambda} P_\alpha = 0$. We summarize these facts in the following

LEMMA 7.3. Let R be a prime and semiprimitive ring satisfying a non-trivial multilinear identity over $\Omega(R)$. Let c be a regular element in R and T a non-zero ideal contained in cR. Then for all α in $\Lambda(T) = \{\alpha \in \Lambda : T \not\subset P_\alpha\}$

(i) $c+P_\alpha = \bar{c}$ is a unit in the ring R/P_α

(ii) $\bigcap_{\alpha \in \Lambda(T)} P_\alpha = 0$.

We can prove

THEOREM 7.4. Let R be a prime ring satisfying a non-trivial identity of minimal degree d with coefficients in the centroid of R. Then R has a left and right quotient ring Q, which is a simple algebra over its center $C = C(Q)$. Moreover $Q = RC$.

Proof. Case 1. R is prime and semiprimitive with a non-trivial multilinear identity $f(X) = \sum_{\sigma \in S_d} \omega_\sigma X_{\sigma(1)} \ldots X_{\sigma(d)}$ of minimal degree d.

Let $\{P_\alpha : \alpha \in \Lambda\}$ be the class of all non-trivial primitive ideals of R as defined in the proof of 7.3. Set $S = \Pi(R/P_\alpha : \alpha \in \Lambda)$. Then the elements of S are of the form $x = (x_\alpha)_{\alpha \in \Lambda}$ where $x_\alpha = x_\alpha{}' + P_\alpha$ and $x_\alpha{}' \in R$. For each $x \in S$ let $\Lambda(x) = \{\alpha \in \Lambda : x_\alpha \neq 0\}$ and consider the subset V of S consisting of all those $x \in S$ such that $\cap(P_\alpha : \alpha \in \Lambda(x)) \neq 0$. If $x, y \in V$, then $\Lambda(x+y) = \{\alpha \in \Lambda : x_\alpha + y_\alpha \neq 0\} \subseteq \Lambda(x) \cup \Lambda(y)$ therefore

$$\cap(P_\alpha : \alpha \in \Lambda(x+y)) \supseteq \cap(P_\alpha : \alpha \in \Lambda(x) \cup \Lambda(y)) \supseteq [\cap(P_\alpha : \alpha \in \Lambda(x))][\cap(P_\alpha : \alpha \in \Lambda(y))] \quad (1)$$

But R is prime and each of the factors in the right hand side of (1) is a right-ideal different from zero, therefore their product is different from zero, hence $\cap(P_\alpha : \alpha \in \Lambda(x+y)) \neq 0$. This means that $x+y \in V$.

If $x \in V$ and $s \in S$, then $\Lambda(xs) = \{\alpha \in \Lambda : x_\alpha s_\alpha \neq 0\} \subseteq \Lambda(x)$ and also $\Lambda(sx) \subseteq \Lambda(x)$ therefore by a similar argument as for the sum, we conclude that xs and sx belong to V. Since clearly $x \in V$ implies $-x \in V$ we have shown that V is a two-sided ideal of S. Define a map $\varphi : R \to S$ by the rule $\varphi r = (r + P_\alpha)_{\alpha \in \Lambda}$. It is easy to see that φ is a homomorphism of rings, moreover φ is injective because $\cap(P_\alpha : \alpha \in \Lambda) = 0$, therefore we have $\varphi r = 0$ if and only if $r \in P_\alpha$ for all $\alpha \in \Lambda$, i.e. if and only if $r = 0$. Hence φR is a subring of S isomorphic to R. Observe that $\varphi R \cap V = 0$ because if $\varphi r \neq 0$, then $\Lambda(\varphi r) = \Lambda$ therefore $\cap(P_\alpha : \alpha \in \Lambda(\varphi r)) = 0$ hence $\varphi r \notin V$. Then by the well known isomorphism theorem we obtain

$$(V+\varphi R)/V \cong \varphi R/(V \cap \varphi R) \cong \varphi R \cong R \tag{2}$$

so we may consider R to be embedded in the ring S/V. Next pick a regular element $c \in R$ and a non-zero two sided ideal T contained in cR. We know this is possible by previous results. By Lemma 7.3 $c+P_\alpha$ is a unit in R/P_α for all α in $\Lambda(T)$. Let $s = (s_\alpha)_{\alpha \in \Lambda}$ and $v = (v_\alpha)_{\alpha \in \Lambda}$ where

$$s_\alpha = \begin{cases} (c+P_\alpha)^{-1} & \text{if } \alpha \in \Lambda(T) \\ 0+P_\alpha = 0_\alpha & \text{if } \alpha \in \Lambda - \Lambda(T) \end{cases}$$

and

$$v_\alpha = \begin{cases} 0_\alpha & \text{if } \alpha \in \Lambda(T) \\ 1+P_\alpha = 1_\alpha & \text{if } \alpha \in \Lambda - \Lambda(T) \end{cases}.$$

Then $v \in V$ because $\Lambda(v) = \Lambda - \Lambda(T)$ and $0 \neq T \subseteq \cap(P_\alpha : \alpha \in \Lambda - \Lambda(T))$. Moreover by (2) identifying $r \in R$ with $(r_\alpha)_{\alpha \in \Lambda}$ where $r_\alpha = r + P_\alpha$ for all $\alpha \in \Lambda$, we see that for the regular element $c \in R$

$$c_\alpha s_\alpha = \begin{cases} (c+P_\alpha)(c+P_\alpha)^{-1} = 1_\alpha & \text{if } \alpha \in \Lambda(T) \\ (c+P_\alpha) \cdot 0_\alpha = 0_\alpha & \text{if } \alpha \in \Lambda - \Lambda(T). \end{cases}$$

Thus $\quad cs = (c_\alpha s_\alpha)_{\alpha \in \Lambda} = (1_\alpha - v_\alpha)_{\alpha \in \Lambda} = 1-v,$

in other words, $cs \equiv 1 \pmod V$.

Hence every regular element $c \in R$ is invertible in S/V. By Theorem 5.5 R has a simple right and left quotient ring $Q(R)$ whose elements are products of the form ac^{-1} with $a, c \in R$ and c regular. Since R is embedded in S/V and every regular element of R is invertible in S/V, we conclude that $Q(R)$ is isomorphic to a subring of S/V. It is not difficult to see that if $\omega \in \Omega(R)$ then in a natural way it induces an element in $\Omega(S)$, hence an element in $\Omega(S/V)$. We denote this element also by ω.

Letting $y_i = (y_{i,\alpha} + P_\alpha)_{\alpha \in \Lambda} + V$ where $y_{i,\alpha} \in \mathbf{R}$ for $i=1,2,\ldots,d$ we get

$$\begin{aligned}
\sum_{\sigma \in S_d} \omega_\sigma y_{\sigma(1)} \cdots y_{\sigma(d)} &= \sum_{\sigma \in S_d} \omega_\sigma [(y_{\sigma(1),\alpha} \cdots y_{\sigma(d),\alpha} + P_\alpha)_{\alpha \in \Lambda} + V] \\
&= \sum_{\sigma \in S_d} [(\omega_\sigma y_{\sigma(1),\alpha} \cdots y_{\sigma(d),\alpha} + P_\alpha)_{\alpha \in \Lambda} + V] \\
&= \sum_{\sigma \in S_d} (\omega_\sigma y_{\sigma(1),\alpha} \cdots y_{\sigma(d),\alpha} + P_\alpha)_{\alpha \in \Lambda} + V \\
&= (\sum_{\sigma \in S_d} \omega_\sigma y_{\sigma(1),\alpha} \cdots y_{\sigma(d),\alpha} + P_\alpha)_{\alpha \in \Lambda} + V \\
&= (0 + P_\alpha)_{\alpha \in \Lambda} + V \\
&= 0 \pmod V.
\end{aligned}$$

Then S/V and therefore $Q(R)$ satisfy $f(X)=0$, moreover $Q(R)$ is primitive (because is simple) so we conclude from Kaplansky's Theorem that $Q=Q(R)$ is a simple finite dimensional algebra over its center $C(Q)$. This proves the theorem for the case in which R is prime and semiprimitive.

Case 2. R is prime but not semiprimitive.

Then we know R is a Goldie ring (Theorem 5.2), therefore it contains no non-zero nil ideals (Theorem 3.6) and this implies that $R[Y]$ is semiprimitive (Theorem 3.9). Thus the ring of polynomials $R[Y]$ is prime (Lemma 1.7), semiprimitive and with the same multilinear identities as R (Lemma 7.1). We then apply the argument of Case 1 to the ring $R[Y]$. Therefore $Q(R[Y])$ satisfies $f(X)=0$ hence so does $Q(R)\subseteq Q(R[Y])$. But then again Kaplansky's Theorem tells us that $Q=Q(R)$ is a finite dimensional simple algebra over its center $C(Q)$. Finally let $m=[Q:C]$ and let $\{q_1,\ldots,q_m\}$ be a basis of Q over C. Then $q_i=a_is_i^{-1}$ with $a_i, s_i\in R$ and s_i regular. As it was seen in Chapter IV we can always find a "common denominator" s, therefore we may write $q_i=b_is^{-1}$ for $i=1,2,\ldots,m$ where $b_i, s\in R$ and s is regular. Since Q is simple we have

$$Q = Qs = (Cb_1s^{-1}+\ldots+Cb_ms^{-1})s$$

$$= Cb_1+\ldots+Cb_m = b_1C+\ldots+b_mC \subseteq RC.$$

But also $RC\subseteq QC\subseteq Q$, hence $Q=RC$ and Theorem 7.4 is proved.

BIBLIOGRAPHY

1. S.A.AMITSUR-J.LEVITZKI, Minimal identities for algebras. Proc.Amer.Math.Soc. 1 (1950), 449-463.

2. S.A.AMITSUR, An embedding of P.I.-rings. Proc.Amer.Math. Soc. 3 (1952), 3-9.

3. S.A.AMITSUR, Generalized polynomial identities and pivotal monomials. Trans.Amer.Math.Soc. 114 (1965), 210-226.

4. S.A.AMITSUR, Prime rings having polynomial identities with arbitrary coefficients. Proc.London Math.Soc.(3), 17 (1967), 470-486.

5. K.ASANO, Uber die Quotientenbildung von Schiefringen. J.Math. Soc.Japan, 1 (1949), 73-78.

6. G.M.BERGMAN, A ring primitive on the right but not on the left. Proc.Amer.Math.Soc. 15 (1964), 473-475.

7. A.W.GOLDIE, Semi-prime rings with maximum conditions. Proc. London Math.Soc.(3) 10 (1960), 201-220.

8. A.W.GOLDIE, A note on prime rings with polynomial identities, J.London Math.Soc.(2) 1 (1969), 606-608.

9. M.HALL, Projective planes. Trans.Amer.Math.Soc. 54 (1943), 229-277.

10. I.N.HERSTEIN, Non commutative rings. The Carus Math.Monographs, no.15, Publ.Math.Assoc.Amer.; distributed by Wiley, New York, 1968.

11. I.N.HERSTEIN, Notes from a ring theory conference. CBMS Reg. Conf.Math., no 9, Amer.Math.Soc. (1971).

12. I.KAPLANSKY, Rings with a polynomial identity, Bull.Amer.Math. Soc. 54 (1948), 575-580.

13. J.LAMBEK, Lectures on rings and modules. Blaisdell, Waltham, Mass. 1966.

14. W.MARTINDALE, 3rd, Prime rings satisfying a generalized polynomial identity. J. Algebra 12 (1969), 576-584.

15. O.ORE, Linear equations in non-commutative fields. Ann.of Math. 32 (1931), 463-477.

16. E.C.POSNER, Prime rings satisfying a polynomial identity. Proc. Amer.Math.Soc. 11 (1960), 180-184.

17. R.G.SWAN, An application of graph theory to algebra. Proc. Amer. Math.Soc. 14 (1963), 367-373.