PRIMITIVITY OF FINITELY PRESENTED MONOMIAL ALGEBRAS

by

Pinar Pekcagliyan
BSc., Bilkent University, 2006

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE
in the Department
of
Mathematics

SIMON FRASER UNIVERSITY
Summer 2008

APPROVAL

Name: Pinar Pekcagliyan

Degree: Master of Science

Title of thesis: Primitivity of Finitely Presented Monomial Algebras

Examining Committee: Dr. Nils Bruin
Chair

Dr. Jason P. Bell
Senior Supervisor

Dr. Norman Reilly
Supervisor

Dr. Luis Goddyn
SFU Examiner

Date Approved:

Abstract

We consider prime monomial algebras and we prove a special case of a conjecture of Jason P. Bell and Agata Smoktunowicz. We show that a prime finitely presented monomial algebra is either primitive or satisfies a polynomial identity and has GK dimension 1. More generally, we show that this result holds for automaton algebras; that is, monomial algebras whose set of nonzero words is recognized by a finite state machine.

Keywords:

monomial algebras; automata; primitivity; GK dimension; polynomial identities

Subject Terms:

Algebra; Noncommutative algebras; PI-algebras

To my family

“I hope I didn’t brain my damage”

— Homer Simpson

Acknowledgments

First of all, I would like to express my sincere gratitude to my supervisor Jason P. Bell for his constant guidance, and for always having time and patience for me. This work would not be possible without his help. I also would like to thank to Norman Reilly and Luis Goddyn for reading and improving my thesis. Finally, I would like to thank my beloved parents Dogan and Cigdem, and my dearest Recep for their constant support and motivation during this study.

Contents

Chapter 1

Introduction

Prime monomial algebras over a field k are the object of this thesis. Given a field k and a finite alphabet $\Sigma = \{x_1, \ldots, x_d\}$, if I is a list of words in Σ, then we can create an algebra

$$k\{x_1, \ldots, x_d\}/(I),$$

where multiplication is defined as follows: If w_1, w_2 are words on the alphabet Σ, then we define $w_1 \cdot w_2$ to be the concatenation of w_1 and w_2 if $w_1 \cdot w_2$ doesn't contain a subword in I and to be 0 otherwise. For a given field k, such a k-algebra A is called a *monomial algebra.* If I is a finite list of words, then we say A is a *finitely presented monomial algebra.* Monomial algebras are useful for many mathematical areas such as algebraic geometry, combinatorial ring theory and representation theory of algebras.

The connection to algebraic geometry and commutative algebra comes via Gröbner bases. Gröbner bases reduce many difficult questions about polynomial ideals to questions about monomial ideals, which are easier to work with. Given a polynomial ring $R = k[x_1, \ldots, x_n]$ and a monomial order, a set of nonzero polynomials $G = \{g_1, \ldots, g_n\}$ contained in an ideal I of R, is called *Gröbner basis* for I, if

$$\mathrm{in}(I) =< \mathrm{in}(g_1), \ldots, \mathrm{in}(g_n) >,$$

where $\mathrm{in}(g_i)$ is the greatest term of g_i with respect to a specified monomial order and $\mathrm{in}(I)$ is the ideal generated by the elements $\mathrm{in}(f)$ for $f \in I$. Gröbner bases associate a monomial algebra to a finitely generated algebra, and for this reason monomial algebras can be used to answer questions about ideal membership and Hilbert series for general algebras. There are two groups of problems that can be attacked with Gröbner bases [10].

1. Construction theory:

   Example 1.0.1. *The ideal description problem: Does every ideal* $I \subset k[x_1, \ldots, x_n]$ *have a finite generating set? In other words, can we write* $I =< f_1, \ldots, f_s >$ *for some* $f_i \in k[x_1, \ldots, x_n]$ *[8]?*

   Example 1.0.2. *The ideal membership problem: Given* $f \in k[x_1, \ldots, x_n]$ *and an ideal* $I =< f_1, \ldots, f_s >$*, determine whether* $f \in I$ *[8].*

2. Elimination theory:

   Example 1.0.3. *Elimination: Compute the intersection* J *of an ideal* $I \subset k[x_1, \ldots, x_n]$ *with a subring* $R' = k[x_1, \ldots, x_s]$ *[10].*

In addition to Gröbner Bases, many difficult problems in algebras can be reduced to combinatorial problems in monomial algebras and can be studied in terms of forbidden subwords. Monomial algebras can be used to answer interesting combinatorial problems. For example, the number of DNA strands of length n on the letters A, C, T, G that avoid GAG and CAT can be computed by finding the Hilbert series of the monomial algebra $k\{A, C, T, G\}/(CAT, GAG)$.

Monomial algebras are a rich area of study. The paper of Belov, Borisenko, and Latyshev [5] is an interesting survey of what is known about monomial algebras.

Our main focus is on primitivity of prime monomial algebras. In algebraic geometry the points of an affine complex variety are parameterized by the maximal ideals of its coordinate ring; that is, we have the correspondence

$$\text{points in variety} \leftrightarrow \text{maximal ideals in coordinate ring.}$$

Roughly speaking, primitive ideals are one possible noncommutative analogue of maximal ideals; and primitive rings are one possible noncommutative analogue of fields. Just as in classical algebraic geometry, for many algebras the primitive ideals are parameterized by points in a variety. In Section 2.1 we give the basic background on primitive rings and ideals.

Bell and Smoktunowicz [4] studied prime monomial algebras of quadratic growth and showed that they are either primitive or have nonzero Jacobson radical. They made the following conjecture about prime monomial algebras in general.

Conjecture 1.0.4. *Let A be a prime monomial algebra over a field k. Then A is either polynomial identity algebra, primitive, or has nonzero Jacobson radical.*

These type of "trichotomies" are very common in ring theory. The theorem by Farkas and Small [12, Theorem 2.2] about just infinite algebras over an uncountable field is an example of an algebra for which such a trichotomy is known to hold:

Theorem 1.0.5. *Assume that k is an uncountable field. If R is a finitely generated, semiprimitive, just infinite dimensional k-algebra then either R is (left) primitive or R satisfies a polynomial identity.*

In fact, Small and Farkas show the Jacobson radical is zero, so the trichotomy reduces to a dichotomy.

Small's conjecture [3, Question 3.2] is another example with the same type of trichotomy:

Conjecture 1.0.6. *A finitely generated Noetherian algebra of quadratic growth is either primitive, satisfies a polynomial identity or has nonzero Jacobson radical.*

We are going to prove Conjecture 1.0.4 in the case that the monomial algebra is finitely presented. In fact, we are able to prove it for a more general case, when A is a automaton algebra; i.e., monomial algebras whose set of nonzero words are recognized by a finite state machine.

Theorem 1.0.7. *Let k be a field and let A be a prime finitely presented monomial k-algebra. Then A is either primitive or A satisfies a polynomial identity.*

A consequence of this theorem is that any finitely generated prime monomial ideal P in a finitely presented monomial algebra A is necessarily primitive, unless A/P has GK dimension at most 1.

We prove our main result by showing that a finitely presented monomial algebra A has a well-behaved free subalgebra. In this case, well-behaved means that the poset of left ideals of the subalgebra embeds in the poset of left ideals of A, and nonzero ideals in our algebra A intersect the subalgebra non-trivially. A free algebra is primitive if it is free on at least two generators; otherwise it is polynomial identity algebra. From this fact and the fact that A has a well-behaved free subalgebra, we are able to deduce that A is either primitive or polynomial identity algebra.

In Chapter 2 we give some useful background information about primitive algebras, polynomial identity algebras and free algebras. First, in Section 2.1 we give some important definitions and theorems about primitive rings and ideals; in Section 2.2 we look at the historical progress in this area, and we prove Jacobson's Density Theorem. Next, we give some basic definitions and examples of Free algebras and modules in Section 2.3. Then in Section 2.4 we define polynomial identity algebras and we prove Kaplansky's Theorem, which characterizes the polynomial identity rings that are primitive. Finally we define Gelfand-Krillov dimension in Section 2.5, which will help us to prove our main Theorem. In Chapter 3 we focus on automata theory and automaton algebras. In Section 3.1, we define finite state machine and we give useful results about automata theory. Then in Section 3.2, we give the relation between monomial algebras and automaton algebras. Last but not least, in Section 3.3 we show how to construct the finite state machine for a few examples of finitely presented monomial algebra. In Chapter 4 we prove Theorem 1.0.7. In Section 4.1 we define nearly free modules, which are essential for our proof. Then in Section 4.2 we give the proof of Theorem 1.0.7, and apply the techniques to some examples to see how the proof works in Section 4.3.

Chapter 2

Ring Theory

In this chapter we give some basic background in ring theory. Throughout this thesis, we assume that all rings and subrings have a multiplicative identity.

2.1 Primitivity

In this section we give the basic facts and definitions for rings that we will use in obtaining our main result. We begin with a few definitions.

Definition 2.1.1. A ring R is *simple* if R has no proper nonzero ideals. A nonzero left module M of a ring R is *simple* if M has no proper nonzero R-submodules.

Example 2.1.2. *$M_2(\mathbb{C})$ is an example of a simple ring.*

Example 2.1.3. *$\mathbb{Z}$ is not a simple ring as $n\mathbb{Z}$ is a nonzero ideal for any nonzero n in $\mathbb{Z}$.*

Example 2.1.4. *Let $R = M_2(\mathbb{C})$. Define*

$$M := \left\{ \begin{bmatrix} a \\ b \end{bmatrix} : a, b \in \mathbb{C} \right\}.$$

Then notice that M is a simple left R-module.

Example 2.1.5. *Consider $\mathbb{Q}$ as $\mathbb{Z}$-module, then $\mathbb{Q}$ is not a simple module as $M := 2\mathbb{Z}$ is a proper $\mathbb{Z}$-submodule.*

Definition 2.1.6. Let R be a ring and M be a left R-module. M is said to be *faithful* if for any nonzero element r of R, there exists $m \in M$ such that $rm \neq 0$.

Example 2.1.7. *Let $R = M_2(\mathbb{C})$, then the left R-module*

$$M := \left\{ \begin{bmatrix} a \\ b \end{bmatrix} : a, b \in \mathbb{C} \right\}$$

is an example of a faithful left module.

Example 2.1.8. *Consider the ring $R = \mathbb{Z}$ and $M = \mathbb{Z}/6\mathbb{Z}$ as a left (and right) R-module. Then notice if we let $r = 12 \in R$, then $rm = 0$ for every $m \in M$. Hence M is not a faithful left module.*

Now we can define a primitive ring.

Definition 2.1.9. A ring R is *left-primitive* if it has a faithful simple left R-module M.

Right-primitivity is defined analogously. Left-primitivity and right-primitivity often coincide; however there are examples of algebras which are left- but not right-primitive [6]. For the purposes of this thesis, we will say that an algebra is *primitive* if it is *both* left- and right-primitive.

Let's give an example.

Example 2.1.10. *Let $R = M_2(\mathbb{C})$. Define*

$$M := \left\{ \begin{bmatrix} a \\ b \end{bmatrix} : a, b \in \mathbb{C} \right\} \text{ and}$$

$$N := \left\{ \begin{bmatrix} a & b \end{bmatrix} : a, b \in \mathbb{C} \right\}.$$

From Examples 2.1.4 and 2.1.7 M is a left simple faithful R-module and similarly N is a right simple faithful R-module. Hence R is both left-primitive and right-primitive. So we say, R is primitive.

Example 2.1.11. *Any simple ring is primitive.*

Proof. Let R be a simple ring and let $\mathcal{I}$ be a maximal left ideal of R. Then $M = R/\mathcal{I}$ is clearly simple. Now by contradiction assume that M is not faithful. So there exists nonzero $r \in R$ such that $rm = 0$ for every $m \in M$. If $rR \subseteq \mathcal{I}$, then $RrR \subseteq R\mathcal{I} = \mathcal{I}$. Since R is simple, and RrR is a two-sided ideal, either RrR is equal to (0) or R. But since $RrR \subseteq \mathcal{I}$, it must be zero, so $r = 0$. The result follows. $\square$

Example 2.1.12. *A commutative ring R is primitive if and only if it is a field.*

Proof. If R is a field than it is primitive by Example 2.1.11. Conversely, if R is primitive, then it has a faithful simple module M. Then note that

$$M \cong R/\mathcal{M}$$

for some maximal ideal $\mathcal{M}$, as M is simple. Then we should have $\mathcal{M} \cdot M = 0$, but M is faithful, so we get $\mathcal{M} = (0)$. Hence R is a field. □

Definition 2.1.13. Let R be a ring and M be a left R-module. Then for $S \subseteq M$ we define the *left annihilator* of S in R, denoted by $\mathrm{Ann}_R S$, to be the set $\{r \in R : rs = 0\}$.

Example 2.1.14. *In the Example 2.1.8, note that every integer $r \in R$ which is a multiple of 6 will give us $rm = 0$ for every $m \in M$. Hence $\mathrm{Ann}_R M = (6)$.*

Definition 2.1.15. Let R be a ring and P be an ideal of R. P is called an *left-primitive ideal* if R/P is a left-primitive ring.

Right-primitivity is defined analogously, and we say that ideal P is *primitive* if it R/P is primitive.

The following proposition gives a nice criterion for an ideal to be primitive.

Proposition 2.1.16. *(Rowen [21]) If R is a ring, then P is a left-primitive ideal if and only if P is the annihilator of a simple left R-module M.*

Proof. Let P be a left-primitive ideal. R/P is a left-primitive ring by definition, so R/P has a faithful simple left-module M. We can turn M into an R-module by defining $rm = (r + P)m$. It can be easily showed that this is well-defined and makes M a left R-module. For any nonzero m in M, we have $Rm = (R/P)m = M$, as M is simple as a left R/P-module. Hence M is simple as a left R-module. We also note that $Pm = 0$ for any $m \in M$, so P is the annihilator of M.

Conversely, assume that P is the annihilator of a simple left R-module M. We want to show that P is a left-primitive ideal, that is, R/P is a left-primitive ring. We need to show that M is a simple faithful left R/P-module. M is an R-module, but we can turn it into an R/P-module by defining $(r + P)m = rm$ where $(r + P) \in R/P$ and $m \in M$. It is easy to show that this is well-defined and makes M a left R/P-module. Next note that for any $r + P \in R/P$, we have $(R/P)m$ must be either 0 or M, as M is a simple left R-module.

Hence M is a simple left R/P-module. Now, towards a contradiction, assume that M is not a faithful left R/P-module. Let $r+P$ be a nonzero element in R/P; that is, $r \notin P$. If M is not faithful, then for some element $r+P$, $(r+P)m = 0$ for every $m \in M$. Then $rm = 0$ for every $m \in M$. This implies that $r \in P$, which is a contradiction. Hence M is a faithful left R/P-module. □

Definition 2.1.17. A ring R is a *prime ring* if for any two elements a, b in R, $aRb = 0$ implies either $a = 0$ or $b = 0$. An ideal P of R is *prime* if R/P is a prime ring.

Proposition 2.1.18. *(Rowen [21]) Any left- or right-primitive ring is a prime ring.*

Proof. Let R be a left-primitive ring and M be a simple faithful left R-module. Assume that $aRb = 0$ for some a and b in R. We want to show that either a or b is 0. So if b is 0, then we are done. Hence assume that b is nonzero. Then $Rb \neq 0$, and $bM \neq 0$, as M is faithful. But since M is simple, $RbM = M$. Next we get $aRbM = aM = 0$. M is faithful, so we get that a is 0. □

The converse of Proposition 2.1.18 is not true. Consider the ring $\mathbb{Z}$; it is clearly prime. If we let M be a simple $\mathbb{Z}$-module, then M is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for some prime p. But then M cannot be faithful, as $pm = 0$ for every $m \in M$.

Corollary 2.1.19. *Let R be a ring and let P be a primitive ideal of R. Then P is prime.*

Proof. P is a primitive ideal of R, hence R/P is primitive. Then R/P is prime and hence P is prime. □

Two useful criteria for being primitive are given in the following two propositions.

Proposition 2.1.20. *A ring A is left-primitive if and only if it has a maximal left ideal $\mathcal{I}$ such that $\mathcal{I}$ does not contain a nonzero two sided ideal of A.*

Proof. First assume that A is primitive and M is a faithful simple left-module of A. Let $m \in M$ be nonzero and consider the A-module homomorphism $\phi : A \to M$ defined by $\phi(a) = am$. Note that $Am \neq (0)$, as $m \neq 0$. Also note that $Am \subseteq M$ and M is simple, hence $Am = M$ and this gives that ϕ is onto. Now we can use the first isomorphism theorem:

$$A/\ker(\phi) \cong M \tag{2.1}$$

Note that $\phi(s) = 0$ if and only if $sm = 0$, hence $\ker(\phi)$ is a left ideal of A. Let $I = \ker(\phi)$. Since A/I is isomorphic to M, I must be maximal. Now we need to show that I does not contain a nonzero two sided ideal. Let $J \subseteq I$ be a two sided ideal of A. Then we have $\phi(J) = 0$ and hence $Jm = 0$. Then $JAm = 0$ so $JM = 0$. We get that J is a annihilator of M, but M is faithful so J must be (0).

Conversely, assume A has a maximal left ideal $\mathcal{I}$ which does not contain a nonzero two sided ideal. Since $\mathcal{I}$ is maximal we get that $A/\mathcal{I}$ is simple A-module [14]. We need to show that $A/\mathcal{I}$ is faithful. Now let $L = \mathrm{Ann}_A(A/\mathcal{I})$. For any $r \in L$, we have $r \cdot 1 \in rA \subseteq \mathcal{I}$. Hence $L \subseteq \mathcal{I}$. However, the annihilator of any A-module is a two sided ideal, so $L = (0)$, implying that $A/\mathcal{I}$ is faithful. Therefore $A/\mathcal{I}$ is a simple faithful A-module. □

Proposition 2.1.21. *A ring A is primitive if and only if there is a proper left ideal I such that $I + P = A$ for every nonzero prime ideal P of A.*

Proof. First assume that A is primitive. Then by the previous proposition we get that A has a maximal left ideal $\mathcal{M}$ which does not contain any nonzero two sided ideal. Since $\mathcal{M}$ is maximal we get that if I is a left-ideal and $I \not\subset \mathcal{M}$ then $\mathcal{M} + I = A$. Note that prime ideals are two sided so any nonzero prime ideal P is not a subset of M hence we get $\mathcal{M} + P = A$ for any nonzero prime ideal P.

Conversely, assume that I is a proper left ideal of A such that $I + P = A$ for every nonzero prime ideal of A. By Zorn's lemma there is a maximal proper left ideal $\mathcal{M} \supseteq I$. Hence we get $\mathcal{M} + P = A$ for every nonzero prime ideal. Now note that $A/\mathcal{M}$ is simple since $\mathcal{M}$ is maximal left ideal of A. We also need to show that $A/\mathcal{M}$ is faithful A-module. By contradiction, assume it is not faithful. Hence the annihilator of $A/\mathcal{M}$ is not only zero. By Proposition 2.1.16, $\mathrm{Ann}_A(A/\mathcal{M})$ is a primitive ideal and primitive ideals are prime. Now, let $P := \mathrm{Ann}_A(A/\mathcal{M})$ and note that for every $r \in P$ we get $(r(x + \mathcal{M})) = 0$ for every $x \in A$. Then $rx + r\mathcal{M} = rx + \mathcal{M} = 0$ for every $x \in A$. Therefore $rx \in \mathcal{M}$ for every $x \in A$ and for every $r \in P$. Hence $PA \subseteq \mathcal{M}$. But since $A = \mathcal{M} + P$, we get $PA = P\mathcal{M} + PP = \mathcal{M} + P = A$. Hence we get $\mathcal{M} \subseteq A$ and this is a contradiction as $\mathcal{M}$ is maximal in A. We get that $A/\mathcal{M}$ is a simple faithful A-module, hence A is primitive. □

2.2 Historical Background of Primitivity

In this section we give some historical information about primitive rings and ideals. We begin with structure theoretical approach.

The aim of structure theory is to decompose complicated objects into simpler objects which are easier to work with. In this section we are going to prove the Jacobson density theorem, which is an important result for structure theory, as it is useful for studying primitive rings and has applications throughout ring theory, but first we need to give some basic definitions and facts.

Definition 2.2.1. Let R be a ring, and M and N be R-modules. A mapping $f : M \to N$ is an *R-module homomorphism* if:

1. $f(m+n) = f(m) + f(n)$
2. $f(rm) = rf(m)$

for every $m, n \in M$ and $r \in R$. f is called a *module endomorphism* if f is a homomorphism mapping of M to itself.

For a given ring R and an R-module M, $\mathrm{End}_R(M)$ denotes the ring of al endomorphisms of M with multiplication given by composition of maps.

Simple modules are one of the basic concepts of structure theory, as they are considered as "building blocks" of other modules. As Schur's Lemma states, they have few homomorphisms among them, therefore they are easier to work with [11].

Lemma 2.2.2. *(Schur's Lemma, Farb and Dennis [11]) Let R be a ring. Any homomorphism between two simple R-modules is either an isomorphism or the zero homomorphism. Therefore, if M is simple, then* $\mathrm{End}_R(M)$ *is a division ring.*

Proof. Let M and N be two modules and $f : M \to N$ be a module homomorphism. Then note that $\ker(f)$ is a submodule of M and $\mathrm{im}(f)$ is a submodule of N. If M is simple, then $\ker(f)$ is 0 or M, and if N is simple, then $\mathrm{im}(f)$ is 0 or N. Thus if both of them are simple, then f is either an isomorphism or the zero map. $\square$

Primitive rings are generalization of simple rings. As in the case with simple rings, primitive rings may also be viewed as the basic building blocks of other rings, but in an infinite dimensional context ([11]).

Definition 2.2.3. Let M be a vector space over a division ring D, and let R be an arbitrary subring of $\mathrm{End}_D(M)$. Then R is called *dense* in $\mathrm{End}_D(M)$ if for every finite set $\{v_1, \ldots, v_n\}$

of D-linearly independent vectors in M, and any set $\{w_1, \ldots, w_n\}$ of vectors in M, there exists $\phi \in R$ such that

$$\phi(v_i) = w_i \ \ for \ \ i = 1, \ldots, n.$$

Now we can state and prove the Jacobson density theorem.

Theorem 2.2.4. *(Jacobson Density Theorem) (Rowen [21]) Suppose R has a faithful simple module M and $D = \mathrm{End}_R(M)$. Then R is dense in $\mathrm{End}_D(M)$.*

Proof. We want to show that R is dense; i.e., for a given D-linearly independent set $\{x_1, \ldots, x_n\}$ in M and any set $\{y_1, \ldots, y_n\}$ in M there exists an element r of R such that $rx_i = y_i$ for $1 \leq i \leq n$. We do the proof by induction on n. If $n = 1$, then the result is true as M is simple. Now suppose the claim is true for $n < m$ and consider the case $n = m$. By induction we have $R(x_1, \ldots, x_{m-1}) = M^{m-1}$. If there exists r in R such that $rx_i = 0$ for every $1 \leq i < m$ and $rx_m \neq 0$, then we are done as rx_m generates M as a R-module. Hence assume that there exists no such r; i.e., if $rx_i = 0$ for $1 \leq i < m$, then $rx_m = 0$. Then the map

$$\Phi : R(x_1, \ldots, x_{m-1}) \to M$$

defined by

$$(rx_1, \ldots, rx_{m-1}) \mapsto rx_m$$

is a well-defined surjective module homomorphism. Let

$$f_j : M \to M^{m-1}$$

defined by

$$f_j(x) = (0, \ldots, 0, x, 0, \ldots, 0) \ \text{ for } \ 1 \leq j < m,$$

and where x has the j^{th} position. Note that $\delta_j := \Phi \circ f_j : M \to M$ is in D for $1 \leq j < m$. Then notice that for $j < m$, $\Phi \circ f_j(x_i) = r_j x_m$, where r_j satisfies

$$r_j x_i = \begin{cases} x_j, & \text{if } i = j \\ 0, & \text{otherwise} \end{cases}$$

Hence we get $(r_1 + \ldots r_{m-1} - 1)x_i = 0$ for $i < m$. Now we have $(r_1 + \ldots r_{m-1} - 1)x_m = 0$ by the assumption and we can rewrite this equation as

$$(r_1 + \ldots r_{m-1})x_m = x_m.$$

Note that

$$\begin{aligned}\delta_1 x_1 + \cdots + \delta_{m-1} x_{m-1} &= \Phi \circ f_1(x_1) + \cdots + \Phi \circ f_{m-1}(x_{m-1}) \\ &= r_1 x_m + \cdots + r_{m-1} x_m \\ &= (r_1 + \cdots + r_{m-1}) x_m = x_m.\end{aligned}$$

But this contradicts with $\{x_1, \ldots, x_m\}$ being D-linearly independent subset of M. The result follows. $\square$

Primitive rings also have many applications for representation theory. Representation theory is a branch of mathematics which tries to represent objects using linear mappings of vector spaces.

Let R be a ring and M be an R-module. Then notice that M is a left $\mathrm{End}_R(M)$-module, as we can define the action $f \cdot x = f(x)$, where $f \in \mathrm{End}_R(M)$ and $x \in M$. Hence for a given R-module M, we can find a homomorphism f of R in $\mathrm{End}_R(M)$. So we have the following definition:

Definition 2.2.5. Let R be a ring and M be an R-module. Then we call ρ a *representation* of R (acting on M) if ρ is a homomorphism of R into $\mathrm{End}(M)$. The map ρ is called an *irreducible representation* of R if M is simple.

Finding irreducible representations is one of the main purposes of representation theory. However, for a given associative algebra A, the set of classes of irreducible representations of A is very large. Often it is easier to find the primitive ideals of A as an intermediate step [9]. Dixmier and Moeglin [13] gave one of the most important results for enveloping algebras of the Lie algebras. We refer the reader to Dixmier [9] for the definitions.

Theorem 2.2.6. *(Dixmier-Moeglin) Let U be the enveloping algebra of a finite dimensional complex Lie algebra, and P be a prime ideal of U. Then the following are equivalent.*

1. *P is primitive,*

2. *The intersection of the prime ideals strictly containing P, strictly contains P,*

3. *The center of the quotient ring of fractions of U/P is equal to $\mathbb{C}$.*

With this famous theorem, there have been numerous attempts to classify primitive ideals in certain settings.

- Quantum Groups: The results in this area are beyond the scope of this thesis, so we refer the reader to Goodearl and Letzter [13].
- Skew Polynomials: The results in this area are beyond the scope of this thesis, so we refer the reader Jøndrup [17].

In this thesis, we look at the problem of determining primitivity in finitely presented monomial algebras.

2.3 Free Algebras and Free Modules

Definition 2.3.1. Let k be a commutative ring. Given a set $X = \{x_\alpha\}_{\alpha \in I}$ we define the *free algebra* on X to be the ring spanned by all linear combinations of finite products of elements in X with the product as the concatenation of the elements of X and with coefficients from k.

When $X = \{x_1, \ldots, x_d\}$, we denote the free algebra by $k\{x_1, \ldots, x_d\}$.

Intuitively, a free algebra can be thought of as being a “noncommutative” ring of polynomials.

Example 2.3.2. *$k[x]$ is a free algebra on one generator.*

Note that $k[x]$ is not primitive by Example 2.1.12, but Jacobson showed that if a free algebra has more than 2 generators, then it is primitive.

Theorem 2.3.3. *A free algebra that is either countably infinitely generated or is generated by d elements for some natural number $d \geq 2$ is primitive.*

For the proof first we need a theorem of Lanski, Resco and Small. The following theorem is used for their main result.

Theorem 2.3.4. *(Lanski, Resco and Small [20]) If R is a prime ring containing a nonzero idempotent e, then R is a primitive ring if and only if eRe is a primitive ring.*

Proof. First assume that R is a primitive ring, so there exists a simple faithful right R-module M. We are going to show that Me is a simple faithful right eRe-module. First let ere be in eRe. If for all elements me of Me we have $0 = (me)(ere) = mere$, then $ere = 0$

as M is faithful right R-module. Thus, Me is a faithful right eRe-module. For any nonzero element me in Me we have

$$me(eRe) = (meR)e = Me,$$

as M is a simple R-module. Then Me is a simple right eRe-module. Hence eRe is a right-primitive ring. Dually, eRe is left-primitive, therefore eRe is primitive.

Conversely, assume that eRe is primitive. Then by Proposition 2.1.20, eRe has a maximal left ideal $\mathcal{M}$ which does not contain nonzero two-sided ideal of eRe. If we let $I := R\mathcal{M} + R(1-e)$, then note that $eIe = \mathcal{M}$. By Zorn's Lemma there exists a left R-ideal $\mathcal{M}'$ containing I and $\mathcal{M}'$ is maximal with respect to the property $e\mathcal{M}'e = \mathcal{M}$. Then $\mathcal{M}'$ is a maximal left ideal of R, as if $\mathcal{M}' + Rx \supsetneq\supseteq\ \mathcal{M}'$, then $e\mathcal{M}'e + eRxe \supsetneq e\mathcal{M}'e = \mathcal{M}$. Also $\mathcal{M}$ is maximal left-ideal of eRe, hence we get $eRe = e\mathcal{M}'e + eRxe = \mathcal{M} + eRe$. Then $e = m + erxe$ for some $m \in \mathcal{M}$ and for some $r \in R$. Notice that $m \in \mathcal{M} \subset eRe$, hence we get $m = me$. Now the equation $e = m + erxe$ becomes $e = me + erxe$ so we have $(1 - m - erx)e = 0$. Hence $1 - m - erx$ is in $R(1-e)$. Then

$$1 \in R\mathcal{M} + R(1-e) + Rx \subseteq \mathcal{M}' + Rx,$$

thus $\mathcal{M}'$ is a maximal left ideal. Suppose $\mathcal{M}'$ contains a nonzero two sided ideal J. Then eJe is a two-sided ideal in $\mathcal{M}$, then by the choice of $\mathcal{M}$ $eJe = 0$. However, this is impossible, as R is prime, e and J are nonzero. Thus $\mathcal{M}'$ does not contain any nonzero two-sided ideal, hence R is left-primitive and, by duality, R is also right-primitive and therefore primitive. □

If R is a ring and S is a nonempty subset of R, then $l(S) := \{x \in R | xS = \{0\}\}$.

Theorem 2.3.5. *([20]) If R is a prime ring and V is a left ideal of R such that $l(V) = \{0\}$, then the following are equivalent:*

1. *V is a primitive ring;*
2. *Every subring of R containing V is primitive;*
3. *Some subring of R containing V is primitive.*

In fact, Lanski, Resco and Small were able to prove a stronger statement [20]. Now we can prove Theorem 2.3.3.

Proof of 2.3.3. Since a free algebra is isomorphic to its opposite ring, it is sufficient to prove left-primitivity. First, if A is the free algebra on two generators, say $A = k\{x, y\}$, then we construct a left A-module M as follows. Let M be the k-vector space spanned by $\{e_0, e_1, \dots\}$ and let A act on M via the rules

$$xe_i \ = \ e_{i-1} \qquad \text{and} \qquad ye_i = e_{i^2+1},$$

where we take $e_{-1} = 0$. We claim M is a faithful simple left A-module and so A is left-primitive.

First let's show that M is simple. We want to show that for any nonzero $m \in M$, we have $Am = M$. Write $m = c_0e_0 + \cdots + c_ne_n$, where c_i's are in A with $c_n \neq 0$. Then observe that $x^n m = c_n e_0$, hence

$$\frac{1}{c_n}x^n m = e_0.$$

We also have $y^k e_0 = e_{n(k)}$ for some integer $n(k)$. Note that $n(k) \to \infty$ as $k \to \infty$, so for every l there exists k such that $n(k) > l$.

$$x^{n(k)-l}y^k e_0 = x^{n(k)-l}e_{n(k)} = e_l.$$

So

$$x^{n(k)-l}y^k \frac{1}{c_n}x^n m = e_l.$$

This proves that M is simple.

Next, we need to show that M is faithful. Before beginning the proof, we are going to define an order on the words of A of length $\leq d$. Let w_1 and w_2 be two words of A with length $\leq d$. Write

$$w_1 = x^{i_d}yx^{i_{d-1}}y \dots yx^{i_2}yx^{i_1},$$

$$w_2 = x^{j_{d'}}yx^{j_{d'-1}}y \dots yx^{j_2}yx^{j_1}$$

with $i_d, \dots, i_1, j_{d'}, \dots, j_1 \geq 0$. We say $w_1 > w_2$ if and only if $d > d'$ or $d = d'$ and $i_k < j_k$ for the first index k with $i_k \neq j_k$.

We can also define an order on the elements of M by $e_0 < e_1 < e_2 < \dots$.

We claim that if w, w' are distinct elements of A, then $we_n \neq w'e_n$ for sufficiently large n. Since $w \neq w'$, assume that $w > w'$. Write w and w' as $w = vv_1$ and $w' = v'v_1$, where $v, v', v_1 \in A$ and the last letter of v is different than the last letter of v'. Then we get $v > v'$. It is sufficient to show that $ve_n > v'e_n$ for n sufficiently large.

Case I: The number of y's in v is more than the number y's in v'. Write

$$v = x^{i_0}yx^{i_1}y \dots yx^{i_d},$$

$$v' = x^{j_0} y x^{j_1} y \dots y x^{j_{d'}}.$$

So we have $d' < d$. For v' we get

$$v' e_n = x^{j_0} y x^{j_1} y \dots y x^{j_{d'}} e_n \le y^{d'} e_n = y^{d'-1} e_{n^2+1} < y^{d'-1} e_{2n^2} < y^{d'-2} e_{8n^4} < \dots < e_{c_{d'} n^{2^{d'}}},$$

where $c_{d'} = 2^{2^{d'}-1}$.

We have $i_1, i_2, \dots, i_d \le m$ for some integer m. Then for v we get

$$v e_n = x^{i_0} y x^{i_1} y \dots y x^{i_d} e_n > (x^m y)^d x^m e_n = (x^m y)^d e_{n-m}.$$

Let $k = n - m$ and note that

$$x^m y e_k = x^m e_{k^2+1} = e_{k^2+1-m} > e_{n^2/2}$$

for sufficiently large n. Hence

$$v e_n > (x^m y)^d e_{n-m} > (x^m y)^d e_{n/2} > (x^m y)^{d-1} e_{n^2/8} > e_{n^{2^d}/c_d},$$

where $c_d = 2^{2^d - 1}$.

Hence we get $v e_n > v' e_n$ for all n sufficiently large.

Case II: Assume that the numbers of y's in v and v' are the same. Then by swapping w_1 and w_2 if necessary, we may write

$$v = x^{i_0} y x^{i_1} y \dots x^{i_{d-1}} y,$$

$$v' = x^{j_0} y x^{j_1} y \dots y x^{j_d},$$

where j_d is nonzero. There exists an integer m such that $i_0, i_1, \dots, i_{d-1} \le m$ For v we get

$$v e_n = x^{i_0} y x^{i_1} y \dots x^{i_{d-1}} y e_n = x^{i_0} y x^{i_1} y \dots x^{i_{d-1}} e_{n^2+1} \ge (x^m y)^{d-1} x^m e_{n^2+1}.$$

For v' we have

$$v' e_n = x^{j_0} y x^{j_1} y \dots y x^{j_d} e_n = x^{j_0} y x^{j_1} y \dots y e_{n-j_d} < y^d e_{n-1}.$$

First notice that

$$x^{i_{d-1}} y e_n = e_{n^2+1-i_{d-1}} > y x^{j_d} e_n = e_{(n-j_d)^2+1},$$

as $j_d > 0$ so $n^2 + 1 - i_{d-1} > (n - j_d)^2 + 1$ for sufficiently large n. Let $k_{i_1} := n^2 + 1 - i_{d-1}$ and $k_{j_1} := (n - j_d)^2 + 1$, hence we have $k_{i_1} > k_{j_1}$. Then the equations become

$$ve_n = x^{i_0} y x^{i_1} y \dots x^{i_{d-2}} y e_{k_{i_1}}$$

and

$$v' e_n = x^{j_0} y x^{j_1} y \dots y x^{j_{d-1}} e_{k_{j_1}}.$$

Next we are going to show that $x^{i_{d-2}} y e_{k_{i_1}} > y x^{j_{d-1}} e_{k_{j_1}}$. The left hand side and the right hand side of the inequality become $x^{i_{d-2}} y e_{k_{i_1}} = e_{k_{i_1}^2 + 1 - i_{d-2}}$ and $y x^{j_{d-1}} e_{k_{j_1}} = e_{(k_{j_1} - j_{d-1})^2 + 1}$ respectively. We check the following inequality

$$k_{i_1}^2 + 1 - i_{d-2} > (k_{j_1} - j_{d-1})^2 + 1,$$

equivalently,

$$k_{i_1}^2 - i_{d-2} > k_{j_1}^2 - 2k_{j_1} j_{d-1} + j_{d-1}^2,$$

equivalently,

$$k_{i_1}^2 - k_{j_1}^2 > i_{d-2} - 2k_{j_1} j_{d-1} + j_{d-1}^2.$$

Since $k_{i_1} > k_{j_1}$, the left hand side is greater than 0. If $j_{d-1} > 0$, then for sufficiently large k_{j_1} and hence sufficiently large n, the right hand side of the inequality will be less than 0. If $j_{d-1} = 0$, then the inequality becomes

$$k_{i_1}^2 - k_{j_1}^2 > i_{d-2}$$

and since $k_{i-1} > k_{j-1}$, the inequality will hold for sufficiently large n. Let $l_2 := k_{i_1}^2 + 1 - i_{d-2}$ and $t_2 := (k_{j_1} - j_{d-1})^2 + 1$, so we get

$$ve_n = x^{i_0} y x^{i_1} y \dots x^{i_{d-3}} y e_{l_2}$$

and

$$v' e_n = x^{j_0} y x^{j_1} y \dots y x^{j_{d-2}} e_{t_2},$$

where $l_2 > t_2$. So we keep doing the same operations until the equations become

$$ve_n = e_{l_d}$$

and

$$v' e_n = x^{j_0} e_{t_d} = e_{t_d - j_0},$$

where $l_d > t_d > t_d - j_0$, hence $ve_n > v'e_n$. Therefore M is faithful and $A = k\{x, y\}$ is left-primitive.

Next observe that if $A = k\{x, y\}$ then $k + Ay$ is free on infinitely many generators $y, xy, x^2y, \ldots$. A is primitive and contains $k + Ay$, hence a free algebra on a countably infinite number of generators is primitive by Theorem 2.3.5. It follows that if $d \geq 2$ is a natural number, then $k + Ax_d$ is free on a countably infinite number of generators and is primitive. Then $A = k\{x_1, \ldots, x_d\}$ is primitive, as any subring containing $k + Ax_d$ must be primitive by Theorem 2.3.5. □

It follows that if $d \geq 2$ is a natural number then $A = k\{x_1, \ldots, x_d\}$ is again primitive since $k + Ax_d$ is free on a countably infinite number of generators by Theorem 2.3.5. □

Definition 2.3.6. Let B be a subring of a ring A. We say that A is *free* as a left B-module if there exists some set $E = \{x_\alpha \mid \alpha \in S\} \subseteq A$ such that:

1. $A = \sum_\alpha Bx_\alpha$;
2. if $b_1, \ldots, b_n \in B$ and $b_1x_{\alpha_1} + \cdots + b_nx_{\alpha_n} = 0$ then $b_i = 0$ for $i = 1, \ldots, n$.

The set E in the definition is called a *free basis* of A as a left B-module and is an analog of a basis of a vector space.

Note that not all modules are free.

Example 2.3.7. *$\mathbb{Q}$ is not free as a $\mathbb{Z}$-module: If $E = \{x_\alpha\}$ is a free basis for $\mathbb{Q}$ as a $\mathbb{Z}$-module, then consider $\frac{a}{b}$, $\frac{c}{d}$ in E with b and d nonzero and $\frac{a}{b} \neq \frac{c}{d}$ (We can find two such elements, as $\mathbb{Q}$ is not isomorphic to $\mathbb{Z}$). Note that $bc\frac{a}{b} - da\frac{c}{d} = 0$. By the second condition $bc = 0$ and $da = 0$. $b \neq 0$ and $d \neq 0$, hence $a = 0$ and $c = 0$. But then $\frac{a}{b} = \frac{c}{d} = 0$, so E does not satisfy the first condition, we get a contradiction.*

Example 2.3.8. *For an example where the second condition is not satisfied, consider $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$ as a left $\mathbb{Z}$-module. Then note that $2(1, 0) = (0, 0)$..*

2.4 PI algebras

Definition 2.4.1. We say that a k-algebra A satisfies a *polynomial identity* if there is a nonzero noncommutative polynomial $p(x_1, \ldots, x_n) \in k\{x_1, \ldots, x_n\}$ such that $p(a_1, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in A^n$. If an algebra A satisfies a polynomial identity we will say that A is *PI*.

Example 2.4.2. *Any commutative ring is PI with the polynomial identity* $[x, y] = xy - yx = 0$.

Example 2.4.3. *The ring of* 2×2 *matrices over a field is a PI with the polynomial* $[[x, y]^2, z] = 0$, *where* $[x, y] = xy - yx$ *(This identity is also called the Hall identity).*

Proof. By the Cayley-Hamilton Theorem we get $A^2 - \operatorname{tr}(A)A + \det(A)I = 0$, where A is 2×2 matrix over any field and I is the identity matrix. Hence if $\operatorname{tr}(A) = 0$, then $A^2 = -\det(A)I$. As $\det(A)$ is a scalar, the square of a trace 0 matrix commutes with every other matrix. Since $[x, y]$ gives us a trace 0 matrix, we see $[[x, y]^2, z] = 0$. $\square$

Example 2.4.4. *The free algebra on more than 2 generators does not satisfy any polynomial identity.*

Polynomial identity algebras are a natural generalization of commutative algebras, which, by definition, satisfy the polynomial identity $xy - yx = 0$. An important theorem of Kaplansky [14, 6.3.1 p. 157] shows that an algebra that is *both* primitive and PI is a matrix ring over a division algebra that is finite dimensional over its centre. Kaplansky's theorem shows that being primitive and being PI are in some sense incongruous and this incongruity is expressed in the fact that for many classes of algebras there are either theorems or conjectured dichotomies which state that the algebra must be either primitive or PI [12, 4, 3].

Definition 2.4.5. The n^{th} *standard identity* is defined by

$$S_n(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) x_{\sigma(1)} \ldots x_{\sigma(n)}.$$

Theorem 2.4.6. *(Amitsur-Levitzki) Let* k *be a field. Then* $M_n(k)$ *satisfies the standard identity of degree* $2n$

$$S_{2n}(x_1, \ldots, x_{2n}) = 0.$$

Moreover, $M_n(k)$ *does not satisfy a nonzero polynomial identity of degree less than* $2n$.

Proof. See [7, Theorem 14 p. 20]. $\square$

Theorem 2.4.7. *(Kaplansky's theorem) (Herstein [14]) If* R *is a primitive ring satisfying a polynomial identity of degree* d, *then* $R \cong M_m(D)$, *where* $m \leq \lfloor d/2 \rfloor^2$ *and* $D = \operatorname{End}_R(M)$, *and* D *is finite dimensional over its center.*

Proof. Since R is a primitive ring, it is dense in $\mathrm{End}_D(V)$ for some D-vector space V by Jacobson density theorem. Suppose that V has dimension greater than $\lfloor d/2 \rfloor$ and let $\{x_1, \ldots, x_k\}$, where $k > \lfloor d/2 \rfloor$, be D-linearly independent elements in V. Let

$$S = \{r \in R | rx_i \in Span\{x_1, \ldots, x_k\} \ \ for \ \ 1 \leq i \leq k\}$$

and

$$I = \{r \in R | rx_i = 0 \ \ for \ \ 1 \leq i \leq k\}.$$

Notice that I is an ideal of S and so $S/I \cong M_k(D)$ by density theorem. Let Z be the center of D, then $M_k(Z)$ is a subring of a factor ring of a subring of R. Hence $M_k(Z)$ should satisfy the same polynomial identity as R. But by Amitsur-Levitzki Theorem, $M_k(Z)$ cannot satisfy a polynomial identity of degree less than $2k > d+1$, we have a contradiction. Hence V has dimension $m < \lfloor d/2 \rfloor$. Thus R is a dense subring of $\mathrm{End}_D(V) \cong M_m(D)$, where $m < \lfloor d/2 \rfloor$. Hence

$$R \cong M_m(D).$$

To show that D is finite dimensional over its center, first we let Z denote the center of D and let K be the maximal subfield of D. Then we let $S = D \otimes_Z K$. For the reader who is not familiar with tensor products, $D \otimes_Z K$ can be thought of as extending the ring of scalars from Z to K. Then it can be shown that D is a faithful simple S-module and $\mathrm{End}_S(D) \cong K$, however these proofs are beyond the scope of this thesis, hence we refer the reader to [14] for the details. $\square$

2.5 GK dimension

In this section we give the basic facts about GK-dimension.

Let k be a field. A ring A is called a *finitely generated k-algebra*, if there exists a set $\{a_1, \ldots, a_m\} \subseteq A$ such that any element in A can be expressed as a polynomial in $a_1, \ldots, a_m$ with coefficients from k.

Let V be a finite dimensional k-vector subspace of A. V is called a *generating subspace*, if

1. $1 \in V$,

2. V generates A as a k-algebra.

We define $V^0 = k$ and for $n \geq 1$, let V^n denote the subspace spanned by all monomials $a_1, \ldots, a_m$ of length n, then we get $A = \bigcup_{n=0}^{\infty} V^n$ where $V^n \supseteq V^{n-1}$, since $1 \in V$.

The *Gelfand-Kirillov dimension* of the k-algebra is defined as:

$$\mathrm{GKdim}(A) := \limsup_{n\to\infty} \log(\dim V^n)/\log(n).$$

While it looks as if GK dimension is dependent on the choice of the generating subspace V, it can be shown that it is in fact independent of this choice.

Proposition 2.5.1. *(Krause and Lenagan [18])The GK dimension of a k-algebra A is independent of the choice of the generating subspace V.*

Proof. Let A be a finitely generated k-algebra and let V and W be two generating subspaces of A. Let $\mathrm{GKdim}_V(A)$ and $\mathrm{GKdim}_W(A)$ be the corresponding GK dimensions of A. We want to show $\mathrm{GKdim}_V(A) = \mathrm{GKdim}_W(A)$. Since

$$A = \bigcup_{n=0}^{\infty} V^n = \bigcup_{n=0}^{\infty} W^n,$$

there exists a positive integer s such that $V \subseteq W^s$. Hence $V^n \subseteq W^{sn}$. Then

$$\begin{aligned}\log(\dim V^n)/\log(n) &\leq \log(\dim W^{sn})/\log(n)\\ &= (1 + \log(s)/\log(n))\log(\dim W^{sn})/\log(ns).\end{aligned}$$

Since s is fixed, we have

$$1 + \log(s)/\log(n) \to 1 \ \ as \ \ n \to \infty.$$

Take the limsup of both sides as n goes to infinity, then we get

$$\mathrm{GKdim}_V A \leq \mathrm{GKdim}_W A.$$

By symmetry, we also get

$$\mathrm{GKdim}_V A \geq \mathrm{GKdim}_W A$$

and the result follows. □

Next, we consider an example where A is a polynomial ring with d generators.

Example 2.5.2. *Let $A = \mathbb{C}[x_1, \dots, x_d]$ be a polynomial ring. Then* $\mathrm{GKdim}(A) = d$.

Proof. Let $V = \mathbb{C} + \mathbb{C}x_1 + \cdots + \mathbb{C}x_d$. Then $V^n = \mathrm{Span}\{\mathcal{B}_n\}$, where

$$\mathcal{B}^n = \{{x_1}^{i_1} \dots {x_d}^{i_d} | i_1 + \cdots + i_d \leq n\}.$$

Note that any element of $\mathcal{B}_n$ corresponds to an element in the free algebra $k\{x, y\}$:

$$y^{i_1} x y^{i_2} x \dots y^{i_d} x y^t,$$

where $i_1 + \cdots + i_d + t = n$. There are $n + d$ positions for d many x's, which gives $\binom{n+d}{d}$ many elements in $\mathcal{B}_n$. Hence $\dim V^n = \binom{n+d}{d} \sim \frac{n^d}{d!}$. Thus

$$\lim_{n \to \infty} \frac{\log \dim V^n}{\log n} = \lim_{n \to \infty} \frac{\log \frac{n^d}{d!}}{\log n} = d.$$

Hence $\mathrm{GKdim} A = d$. □

GK dimension is a noncommutative analogue of Krull dimension, which is the notion of dimension used in algebraic geometry.

Definition 2.5.3. Let k be a field. A k-algebra A has *Krull dimension* $\mathrm{Kdim}(A) = m$, if there exists a chain of prime ideals

$$P_0 \supsetneq P_1 \supsetneq \cdots \supsetneq P_{m-1} \supsetneq P_m$$

of length m, and there is no such chain of greater length. If A has chains of prime ideals of arbitrary length, then $\mathrm{Kdim}(A) = \infty$.

GK dimension and Krull dimension coincide if A is finitely generated and commutative.

Proposition 2.5.4. *Let A be a commutative finitely generated k-algebra, where k is a field. Then* $\mathrm{Kdim}(A) = \mathrm{GKdim}(A)$.

The proof uses the following theorem.

Theorem 2.5.5. *(Noether's normalization theorem) Let k be a field and A be a commutative finitely generated k-algebra of Krull dimension n. Then there exists a subalgebra $B \cong k[x_1, \dots, x_n]$ such that A is a finite module over B.*

Proof. See [10] page 283 Theorem 13.3. □

Proof of Theroem 2.5.4. Let A be a commutative finitely generated k-algebra and let $d = \mathrm{Kdim}(A)$. By Theorem 2.5.5, there exists a subalgebra $B \cong k[x_1, \ldots, x_d]$ with A a finite module over B. As one might expect, if A is finite module over a subalgebra B, then they have the same GK dimension [18, 4.3 p. 39]. By Example 2.5.2, we have $d = \mathrm{GKdim}(B)$. Hence

$$\mathrm{Kdim}(A) = d = \mathrm{GKdim}(B) = \mathrm{GKdim}(A).$$

Chapter 3

Automata Theory and Automaton Algebras

3.1 Automata Theory

In this section we give some basic background about finite state automata.

A finite state automaton (or a finite state machine) is a mathematical model of a machine which performs computations by moving from state to state for a given input, which is a word on a finite alphabet Σ. The transition function, usually denoted by δ, takes the input and determines how to move from one state to another depending on the given input. The finite state machine has a starting state and accepting states. At the end of the computations, if the transition function stops at an accepting state, we say that the finite state machine accepts the given input.

As it can be seen, a finite state machine has 5 parts: Finitely many states, a starting state, accepting states, a finite alphabet (the inputs are words on the alphabet) and a transition function (determines the rules of the machine). We give a more formal definition.

Definition 3.1.1. A *finite state automaton* Γ is a 5-tuple $(Q, \Sigma, \delta, q_0, F)$, where:

1. Q is a finite set of states;

2. Σ is a finite alphabet;

3. $\delta : Q \times \Sigma \to Q$ is a transition function;

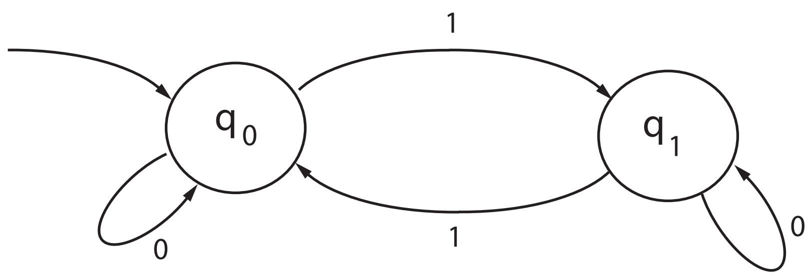

Figure 3.1: A finite state automaton called Γ that has 2 states.

4. $q_0 \in Q$ is the initial state;

5. $F \subseteq Q$ is the set of accepting states.

We give an example.

Example 3.1.2. *Figure 3.1 is called a* state diagram *of* Γ. *It has alphabet* $\Sigma = \{0, 1\}$, *states* $\{q_0, q_1\}$, *accepting state* $\{q_0\}$, *start state* $\{q_0\}$. *The arrows going from one state to another are the transitions. When* Γ *receives an input such as 1001, the transition function* δ *process it one by one from left to right of the string, starting from the starting state. The output is either* accept *or* reject *depending on the state that the process ends on. The processing of* $\delta(q_0, 1001)$ *proceeds as follows:*

1. *Start in state* q_0.

2. *Read 1. Move to state* q_1 *(the transition is from* q_0 *to* q_1*).*

3. *Read 0. Stay at the state* q_1 *(the transition is from* q_1 *to* q_1*).*

4. *Read 0. Stay at the state* q_1 *(the transition is from* q_1 *to* q_1*).*

5. *Read 1. Move to the state* q_0 *(the transition is from* q_1 *to* q_0*).*

6. *The process stops. The output is an* accept *as* q_0 *is an accepting state.*

Note that, in particular, if w *is a word on* $\{0, 1\}$ *then* $\delta(q_0, w)$ *is* q_0 *if and only if the number of ones in* w *is even.*

The next definition is a formal definition for words that the finite state machine accepts.

Definition 3.1.3. Let $\Gamma = (Q, \Sigma, \delta, q_0, F)$ be a finite state machine and let $w = w_1 \dots w_n$ be a string where each w_i is in Σ. Then Γ *accepts* w if there exists a sequence of states $r_0, r_1, \dots, r_n$ in Q such that:

1. $r_0 = q_0$,
2. $\delta(r_i, w_{i+1}) = r_{i+1}$, for $i = 0, 1, \dots n-1$, and
3. $r_n \in F$.

Condition 1 says that the machine starts with the starting state. Condition 2 says that the transition function δ determines how the machine should go from one state to another. Condition 3 says that the machine accepts the input if the computing ends at an accepting state [22].

Definition 3.1.4. A *language* L is a set of strings of symbols from some alphabet Σ. L is a *regular language*, if all strings of L are accepted by some finite state automaton.

We note that we can inductively extend the transition function δ to a function from $Q \times \Sigma^*$ to Q, where Σ^* denotes the collection of finite words of Σ including the empty word.

Notation. *We simply define $\delta(q, \varepsilon) = q$ if ε is the empty word and if we have defined $\delta(q, w)$ and $x \in \Sigma$, we define $\delta(q, wx) := \delta(\delta(q, w), x)$.*

Definition 3.1.5. Let A and B be two languages. The regular operations of *union*, *concatenation*, and *star* are defined as follows.

- Union: $A \cup B = \{x \mid x \in A \;\; or \;\; x \in B\}$
- Concatenation: $A \circ B = \{xy \mid x \in A \;\; and \;\; y \in B\}$
- Star: $A^* = \{x_1 \dots x_k \mid k \geq 0 \;\; and \;\; each \;\; x_i \in A\}$, where $k = 0$ means the empty word.

Example 3.1.6. *Let $A = \{a, b\}$ and $B = \{c, d\}$. Then,*

- $A \cup B = \{a, b, c, d\}$,
- $A \circ B = \{ac, ad, bc, bd\}$,
- $A^* = \{\emptyset, a, b, aa, ab, ba, bb, aaa, aab, aba, baa, abb, bab, \dots\}$.

Definition 3.1.7. The regular operations which are used to build up expressions describing languages are called *regular expressions.*

Example 3.1.8. *Consider the regular expression* $1^*(0 \cup 1)$*.* 1^* *means* $\{1\}^*$*,* $(0 \cup 1)$ *means* $(\{0\} \cup \{1\})$*, and* $1^*(0 \cup 1)$ *means* $1^* \circ (0 \cup 1)$*. Hence the language determined by this regular expression consists of strings starting with any number of* 1*'s followed by either* 1 *or* 0*.*

Theorem 3.1.9. *(Kleene's Theorem [1]) A language is accepted by a finite state automaton if and only if it can be specified by a regular expression.*

Proof. For the proof we refer the reader to Sipser [1, Theorem 4.1.5, page 132]. □

Definition 3.1.10. Let Σ and Δ be alphabets. A *homomorphism* is a map $h : \Sigma^* \to \Delta^*$ such that $h(xy) = h(x)h(y)$ for all words x and y in Σ^*.

We can also define the *inverse homomorphism* of languages. For a given homomorphism $h : \Sigma^* \to \Delta^*$ and a language $L \subseteq \Delta^*$, we define

$$h^{-1}(L) = \{x \in \Sigma^* | h(x) \in L\}.$$

Theorem 3.1.11. *([1]) If* L *is a regular language and* h *is a homomorphism, then* $h^{-1}(L)$ *is regular.*

Proof. $L \subseteq \Delta^*$ is regular, so there exists an automaton $\Gamma = (Q, \Delta, \delta, q_0, F)$ accepting L. Then we define $\Gamma' = (Q, \Sigma, \delta', q_0, F)$ as follows: $\delta'(q, w) = \delta(q, h(w))$. The result follows. □

3.2 Automaton Algebras

We now describe the connection between monomial algebras and finite state automata.

Definition 3.2.1. Let k be a field and let $A = k\{x_1, \ldots, x_n\}/(I)$ be a monomial algebra (See page 1 for the definition). We say that A is an *automaton algebra* if there exists a finite state automaton Γ with alphabet $\Sigma = \{x_1, \ldots, x_n\}$ such that the word w is accepted by Γ if and only if $w \notin (I)$.

Definition 3.2.2. Let u be a word in an algebra A. A word v in A is called an *extension* of u if $uv \neq 0$.

Words u and w in A are called *equivalent*, denoted by $u \sim_A w$ if the set of all extensions of u coincides with the set of all extensions of w.

The number of equivalence classes is called the *index.*

Example 3.2.3. *Consider the monomial algebra $A = \mathbb{C}\{x, y\}/(x^3, yxy)$. Then note that the set of extensions of words x^2 and yx^2 coincide. Thus $x^2 \sim_A yx^2$.*

Proposition 3.2.4. *(Belov, Borisenko and Latyshev [5]) A monomial algebra is an automaton algebra if and only if the set of all its nonzero words has a finite number of equivalency classes.*

Proof. If the monomial algebra is automata, then it has a finite state machine, implying that there are finitely many equivalence classes.

Conversely, let A be a monomial algebra with finite number of equivalence classes. The minimal finite state machine for A can be constructed as following: The equivalence classes of nonzero words give us the accepting states. The equivalence classes of words with zero images give us the rejecting states. The equivalence class of the empty word is the starting state. The generators of A give the transition function. Note that the constructed finite state machine gives all the nonzero words in A. Hence A is an automaton algebra. □

Proposition 3.2.5. *(Belov, Borisenko and Latyshev [5]) Any finitely presented monomial algebra is an automaton algebra.*

Proof. Let A be a finitely presented monomial algebra and let the maximum degree of the defining relations of A be n. The set of extensions of any nonzero word of length $\geq n-1$ is uniquely determined by its end of length $n-1$. Hence the number of equivalence classes of nonzero words of A cannot exceed the number of nonzero words of A of length $\leq n-1$. □

We note that in order for a finite state automaton Γ to give rise to a monomial algebra, the collection of words that are rejected by Γ must generate a two-sided ideal. This need not occur in general (see, for example, Figure 3.1).

In general, an automaton algebra can have many different corresponding finite state automata. We may assume, however, that the corresponding finite state automaton is *minimal*.

Definition 3.2.6. We say that a finite state automaton $\Gamma = (Q, \Sigma, \delta, q_0, F)$ is *minimal* if for $q_1, q_2 \in Q$ with $q_1 \neq q_2$ we have

$$\{w \in \Sigma^* \ : \ \delta(q_1, w) \in F\} \neq \{w \in \Sigma^* \ : \ \delta(q_2, w) \in F\}$$

and for every $q \in Q$ there is a word $w \in \Sigma^*$ such that $\delta(q_0, w) = q$.

We note that this definition of minimality is different from other definitions that appear in the literature. It can, however, be shown to be equivalent [24]. By the Myhill-Nerode theorem [15], if A is an automaton algebra, there is a minimal corresponding automaton Γ; moreover, this automaton Γ is unique up to isomorphism.

Theorem 3.2.7. *(The Myhill-Nerode theorem [15]). The following are equivalent:*

1. *The set $L \subseteq \Sigma^*$ is accepted by some finite automaton.*
2. *L is the union of some of the equivalence classes of a right invariant equivalence relation of finite index.*
3. *Let the equivalence relation $\sim_L$ be defined by : $x \sim_L y$ if and only if for all z in Σ^*, xz is in L exactly when yz is in L. Then $\sim_L$ is of finite index.*

Before proceeding with the proof, recall that we said that two words u and w in a monomial algebra A are equivalent if the set of all extensions of u coincides with the set of all extensions of w. Let's denote the relation by $u \sim_A w$. We can also define a similar relation on the words of a finite state automaton. Let $\Gamma = (Q, \Sigma, \delta, q_0, F)$ be a finite state automaton. For x and y in Σ^*, we say $x \sim_\Gamma y$ if $\delta(q_0, x) = \delta(q_0, y)$. This relation has reflexivity, symmetry and transitivity, as " $=$ " has all three properties.

Definition 3.2.8. Let $\sim$ be an equivalence relation such that $x \sim y$ implies $xz \sim yz$ for every x, y, z, then $\sim$ is called *right invariant.*

Note that the equivalence relation $\sim_\Gamma$ is right invariant: Let x, y, z be in Σ^*, then

$$\delta(q_0, xz) = \delta(\delta(q_0, x), z) = \delta(\delta(q_0, y), z) = \delta(q_0, yz).$$

Now we can prove Theorem 3.2.7

Proof. (1) $\Rightarrow$ (2) Assume that L is accepted by a finite state machine $\Gamma = (Q, \Sigma, \delta, q_0, F)$. Let $\sim_\Gamma$ be the equivalence relation on words of Γ as previously described. The index of $\sim_\Gamma$ is finite, it must be bounded by the number of the states in Q. We already showed that $\sim_\Gamma$ is right invariant. Note that L is the union of words x such that $\delta(q_0, x) \in F$, so (2) follows.

(2) $\Rightarrow$ (3) Let $\sim$ be an equivalence relation satisfying (2). Assume that $x \sim y$. As $\sim$ is right invariant, for any $z \in \Sigma^*$ we have $xz \sim yz$. This implies that yz is in L if and only if xz is in L. Therefore we get $x \sim_L y$, and we see that the equivalence class of x in $\sim$ is

contained in the equivalence class of x in $\sim_L$. Since the choice of x was arbitrary, we see that every equivalence class of $\sim$ is contained in some equivalence class of $\sim_L$. Thus $\sim_L$ has index number less than the index number of $\sim$. The result follows.

(3) $\Rightarrow$ (1) First let's show that $\sim_L$ is right invariant. Assume $x \sim_L y$. We want to show $xw \sim_L yw$ for any w; that is, for any z, xwz is in L if and only if ywz is in L. $x \sim_L y$ implies that for any v, xv is in L if and only if yv is in L. Let $v = wz$. Hence xwz is in L if and only if ywz is in L, so $\sim_L$ is right invariant.

Now let Q' be the set of equivalence classes of $\sim_L$. Let $[x]$ be the equivalence class of Q containing x. Define $\delta'([x], a) = [xa]$ for any word a in L. Let's show that δ' is well-defined. If we use y in $[x]$ instead of x, then we get $\delta'([x], a) = [ya]$. We have $x \sim_L y$, and recall $\sim_L$ is right invariant, hence $xa \sim_L ya$ for any a, implying $[xa] = ya$. Define $q'_0 = [\varepsilon]$ and $F' = \{[x] | x \in L\}$. The finite automaton $\Gamma' = (Q', \Sigma, \delta', q'_0, F')$ accepts L. □

Theorem 3.2.9. *([15]) The minimal state automaton accepting a set L is unique up to an isomorphism (i.e., a renaming of the states) and is given by Γ' in the proof of Theorem 3.2.7.*

Proof. Let L be a language and $\Gamma' = (Q', \Sigma, \delta', q'_0, F')$ be the finite state automaton of L in Theorem 3.2.7. Let $\Gamma = (Q, \Sigma, \delta, q_0, F)$ be another finite state machine accepting L. Then the number of states of Γ is greater than or equal to the number of states of Γ'. Now let q be a state in Γ. There must be some $x \in \Sigma^*$ such that $\delta(q_0, x) = q$, otherwise q can be removed and we will get a smaller automaton. Now identify q with the state q' of Γ' such that $\delta'(q'_0, x) = q'$. If $\delta(q_0, x) = \delta(q_0, y) = q$ for $x \neq y$, then by the proof of Theorem 3.2.7, x and y are in the same equivalence class of $\sim_L$, hence $\delta'(q'_0, x) = \delta'(q'_0, y)$. The result follows. □

3.3 Examples

Recall from Proposition 3.2.5 that any finitely generated monomial algebra is an automaton algebra; i.e., there is a finite state automaton algebra which accepts the words of the monomial algebra. In this section, we will show how to construct the corresponding minimal finite state automaton for a given finitely generated monomial algebra.

Example 3.3.1. *Let $A = k\{x, y\}/(xy)$. The words in $\{x, y\}$ with nonzero image in A are precisely those words which do not contain xy as a subword. To check whether a word* *contains xy or not, we first ignore all occurrences of y before the first appearance of x, since we need an x to have xy as a subword. If we come to an x, then it might be the first letter of xy. We read the next letter, if it is another x, we are in the same position as we were before; if it is a y, then we have a subword xy. Hence there are 3 possibilities:*

1. *We have only seen the letter y.*
2. *We have seen x without a y appearing after it.*
3. *We have seen xy.*

Now we can construct the automaton (See Figure 3.3.1).

- *Step 1: Start with a starting state, say q_0.*
- *Step 2: We ignore all the y's, meaning y's keep us at the starting state. If we see an x, then we move to another state, say q_1.*
- *Step 3: At state q_1, the letter x keeps us in this state; if we see a y, then we move to another state, say q_2.*

In this case q_0 and q_1 are the accepting states. Once the automaton enters q_2, it should stay at that state, as the word contains xy, and cannot be in nonzero anymore.

Note that A is not prime, as $xAy = 0$.

Example 3.3.2. *Let $A = k\{x, y\}/(x^2)$. The words in $\{x, y\}$ with nonzero image in A are precisely those words which do not contain x^2 as a subword. To check whether a given word contains x^2, we ignore all occurrences of y before the first appearance of x, as we need an x to have x^2 as a subword. If we come to an x, then it might be the first letter of x^2. We read the next letter, if it is a y, then we go back ignoring y's. But if we see another x, then that word contains x^2, hence we need to move another state.*

Now we can construct the automaton (See Figure 3.3.2).

- *Step 1: Start with a starting state, say q_0.*
- *Step 2: We ignore all the y's, meaning y's keep us at the starting state. If we see an x, then we move to another state, say q_1.*
- *Step 3: At state q_1, if we see a y, then we go back to ignoring y's; i.e., we go back to the state q_0. If we see an x at state q_1, then we go another state, say q_2.*

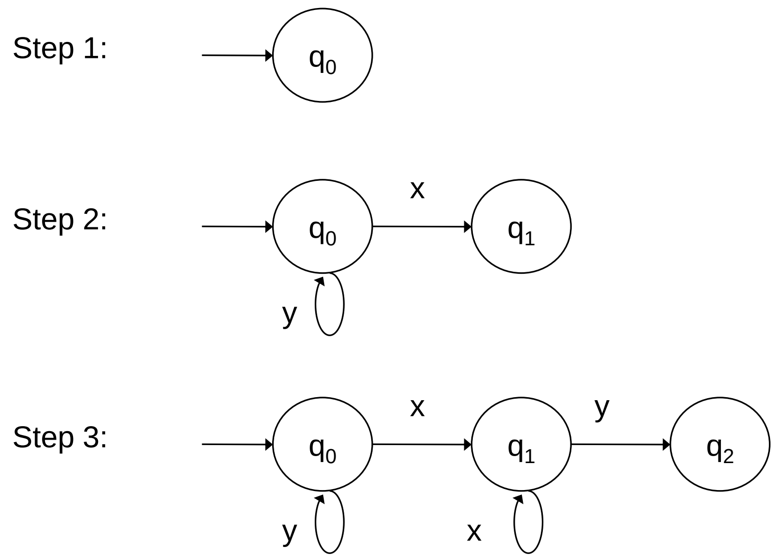

Figure 3.2: The construction of the automaton for $k\{x,y\}/(xy)$

In this example, q_0 and q_1 are the accepting states. Once the automaton enters q_2, then it should stay at that state, as the word contains x^2 and cannot be in A anymore. This is an example of a prime automaton algebra, as there exist no nonzero a and b in A such that $aAb = 0$.

Example 3.3.3. *Let $A = k\{x,y\}/(x^3, y^2)$. The words in $\{x,y\}$ with nonzero image in A are precisely those words which do not contain x^3 or y^2 as a subword. As in the previous examples, we just track the occurrences of the patterns x^3 and y^2. We can construct the automaton as follows (See Figure 3.3.3).*

- *Step 1: Start with a starting state, say q_0.*
- *Step 2: At state q_0: If we see an x, it might be the first letter of the pattern x^3, so we move to another state, say q_1. If we see a y, it might be the first letter of the pattern y^2, so we move to another state q_2.*
- *Step 3: At state q_1: If we see another x, then we have seen the two letters of the*

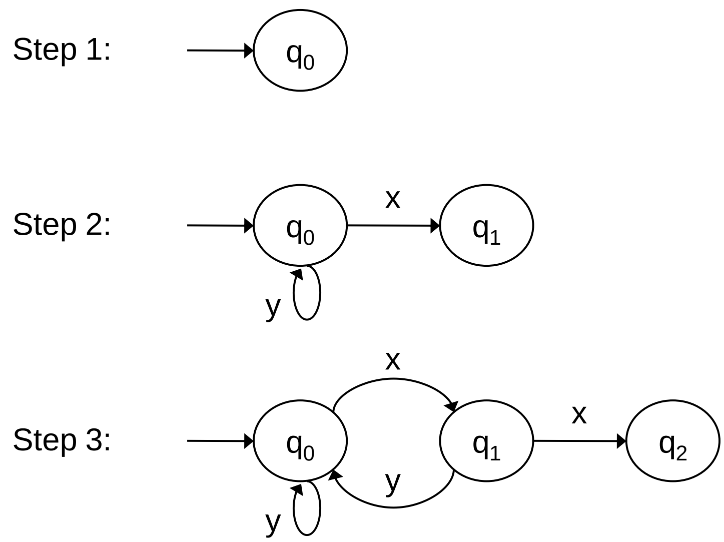

Figure 3.3: The construction of the automaton for $k\{x, y\}/(x^2)$

pattern x^3*, so we move to another state, say* q_3*. If we see a* y*, then it might be the first letter of* y^2*, so we should go to state* q_2*. At state* q_2*: If we see an* x*, then it might be the first letter of* x^3*, so we go to the state* q_1*. If we see a* y*, then we have seen* y^2*, so we move to another state, say* q_4*.*

- *Step 4: At state* q_3*: If we see an* x*, then we completed the pattern* x^3*, so we move to another state, say* q_5*. If we see a* y*, then that* y *might be the first letter of* y^2*, so we go the state* q_2*.*

In this automaton, the accepting states are q_0, q_1, q_2 *and* q_3*. Once the automaton enters* q_4 *or* q_5*, it should stay at that state, as the word contains* x^3 *or* y^2*, and cannot be in* A *anymore.*

This is also an example of a prime automaton algebra, as there exist no nonzero a *and*

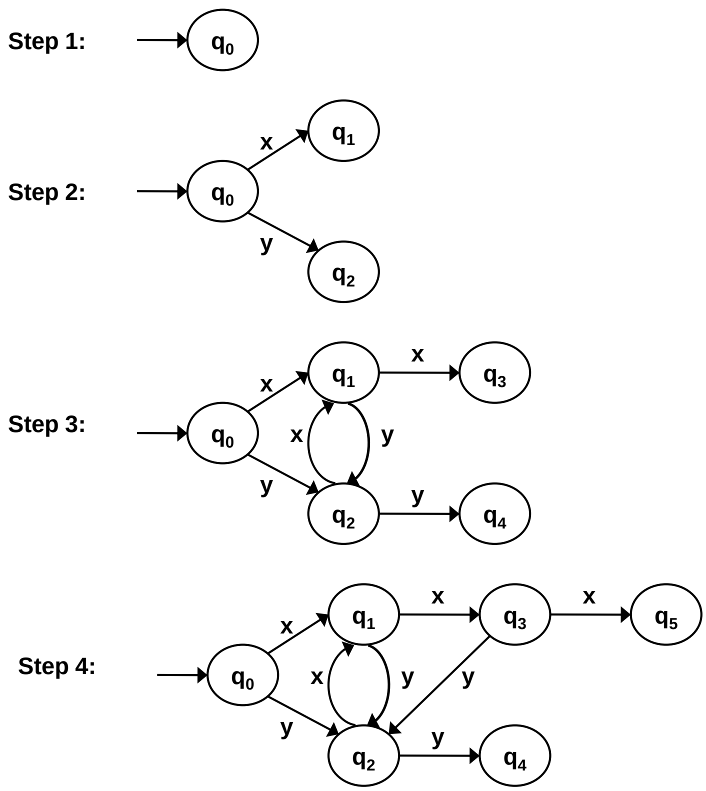

Figure 3.4: The construction of the automaton for $k\{x, y\}/(x^3, y^2)$

b in A such that $aAb = 0$.

Chapter 4

Proofs

4.1 Nearly Free Modules

Definition 4.1.1. Let B be a subring of a ring A. We say that A is *nearly free* as a left B-module if there exists some set $E = \{x_\alpha \mid \alpha \in S\} \subseteq A$ such that:

1. $x_{\alpha_0} = 1$ for some $\alpha_0 \in S$;
2. $A = \sum_\alpha Bx_\alpha$;
3. if $b_1, \ldots, b_n \in B$ and $b_1 x_{\alpha_1} + \cdots + b_n x_{\alpha_n} = 0$ then $b_i x_{\alpha_i} = 0$ for $i = 1, \ldots, n$.

We note that it is possible to be nearly free over a subalgebra without being free.

Example 4.1.2. *Let $A = \mathbb{C}[x]/(x^3)$ and let B be the subalgebra of A generated by the image of x^2 in A. Then A is 3-dimensional as a $\mathbb{C}$-vector space while B is 2-dimensional. Hence A cannot be free as a left B-module. Let $\overline{x}$ denote the image of x in A. Then*

$$A \;=\; B + B\overline{x}.$$

Moreover A is $\mathbb{N}$-graded and B is the graded-subalgebra generated by homogeneous elements of even degree. Hence if $b_1 + b_2\overline{x} = 0$ then $b_1 = b_2\overline{x} = 0$. Hence A is nearly free as a B-module.

Proposition 4.1.3. *Let A be a prime algebra and suppose that B is a primitive subalgebra of A such that:*

1. *A is an nearly free as a right and left B-module;*

2. *every nonzero two-sided ideal I of A has the property that $I \cap B$ is nonzero.*

Then A is primitive.

Proof. It is sufficient to show that A is right primitive. By Proposition 2.1.20, there exists a maximal right ideal I of B that does not contain a nonzero two-sided ideal of B. Let $E = \{x_\alpha : \alpha \in S\}$ be a subset of A satisfying:

1. $A = \sum_{x_\alpha \in E} Bx_\alpha$;

2. if $b_1 x_{\alpha_1} + \cdots + b_d x_{\alpha_d} = 0$, then $b_i x_{\alpha_i} = 0$ for every i;

3. $x_\beta = 1$ for some $\beta \in S$.

Then

$$IA \;=\; \sum_{\alpha \in S} I x_\alpha.$$

We claim that IA is proper right ideal of A. If not then

$$1 = x_\beta = \sum a_k x_{\alpha_k},$$

for some $a_k \in I$. Since A is nearly free as a left B-module, $x_\beta - ax_\beta = 0$ for some $a \in I$, so that $1 = x_\beta = ax_\beta \in I$ contradicting the fact that I is a proper ideal of B. Thus IA is a proper right ideal of A. The proper ideals of A can be partially ordered by using the subset inclusion, and since IA is a proper right ideal of A, by Zorn's lemma we can find a maximal right ideal L of A containing IA. We claim that A/L is a faithful simple right A-module. To see this, first we show that $L \cap B = I$. Note that $L \cap B \supseteq IA \cap B = I$. If $L \cap B = B$, then $L \subseteq BA = A$, which is a contradiction. Hence $L \cap B = I$. Now suppose that L contains a nonzero primitive ideal P of A. By assumption, $P \cap B = Q$ is a nonzero ideal of B and is contained in $L \cap B = I$, a contradiction. The result follows. $\square$

4.2 Proof of Theorem 1.0.7

In this section we prove the following generalization of Theorem 1.0.7.

Theorem 4.2.1. *Let k be a field and let A be a prime automaton algebra over k. Then A is either primitive or A satisfies a polynomial identity.*

To prove this we need a few definitions.

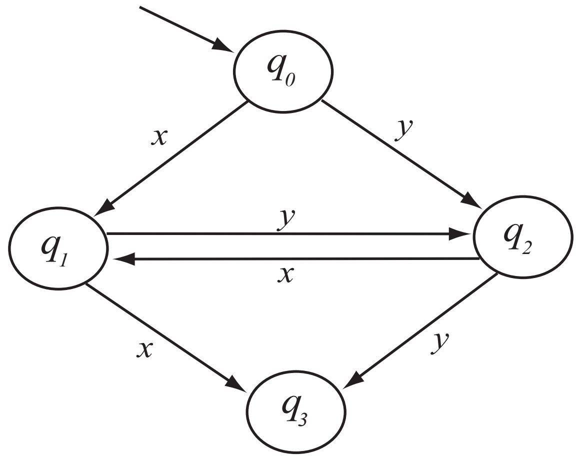

Figure 4.1: A finite state automaton in which the only q_0-revisiting word is the empty word.

Definition 4.2.2. Let $\Gamma = (Q, \Sigma, \delta, q_0, F)$ be a minimal finite state automaton. Given a state $q \in Q$, we say a word $w \in \Sigma^*$ is *q-revisiting* if $w = w'w''$ for some $w', w'' \in \Sigma^*$ with w' non-trivial such that $\delta(q, w') = q$. Otherwise, we say w is *q-avoiding*.

A key obstruction in this proof is that there exist examples of prime automaton algebras for which there are no non-trivial words in Σ^* that are q_0-revisiting in the corresponding minimal automaton $\Gamma = (Q, \Sigma, \delta, q_0, F)$. For example, if $A = k\{x, y\}/(x^2, y^2)$. Then the automaton corresponding to the algebra A is given in Figure 4.2. We note that it is impossible to revisit the initial state q_0 in this case.

Before proceeding with the generalization of Theorem 1.0.7, we define an equivalence relation on the accepting states of a minimal finite state automaton $\Gamma = (Q, \Sigma, \delta, q_0, F)$. We say that $q_i \sim q_j$ if there exists words w and w' such that $\delta(q_i, w) = q_j$ and $\delta(q_j, w') = q_i$.

Given a minimal finite state automaton $\Gamma = (Q, \Sigma, \delta, q_0, F)$, we can put a partial order between the equivalence classes of accepting states in the following way. Let q and q' be two accepting states and let $[q]$ and $[q']$ denote their equivalence classes. We say that $[q] \leq [q']$ if there is a word w such that $\delta(q, w) = q'$ (Note that if $[q] \leq [q']$ and $[q'] \leq [q]$ then $q \sim q'$ and so the two classes are the same.). Figure 4.2 gives an example of a finite state automaton in which the set accepting of states has been partitioned into equivalence classes.

To obtain the proof of Theorem 1.0.7, we show that A has a well-behaved free subalgebra.

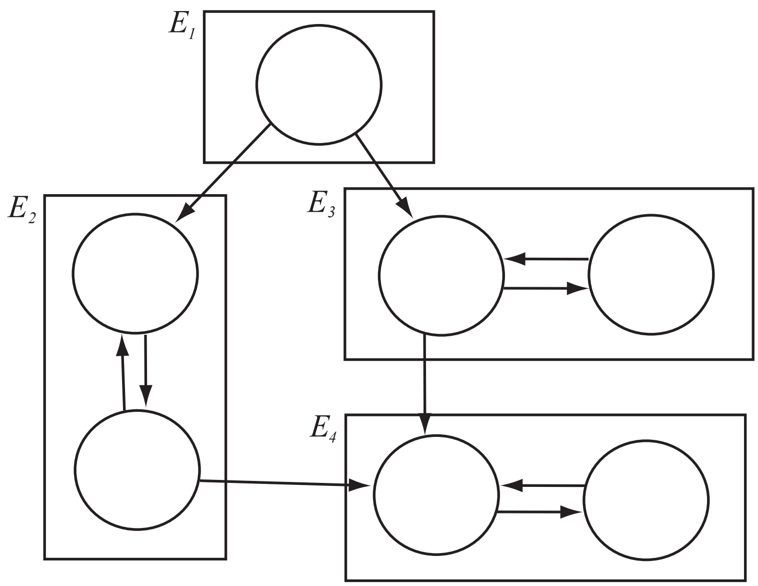

Figure 4.2: A finite state machine with four equivalence classes.

We call the subalgebras we construct *state subalgebras.*

Definition 4.2.3. Let A be an automaton algebra and let $\Gamma = (Q, \Sigma, \delta, q_0, F)$ be its corresponding minimal finite state automaton. Given a state $q \in F$, we define the *state subalgebra of A corresponding to q* to be the subalgebra generated by all words $w \in \Sigma^*$ such that $\delta(q, w) = q$.

Lemma 4.2.4. *Let A be an automaton algebra and let $\Gamma = (Q, \Sigma, \delta, q_0, F)$ be its corresponding minimal finite state automaton. A state subalgebra B of A corresponding to some state q in F is a free algebra.*

Proof. We claim that B is free on

$$E \ := \ \{w \in \Sigma^* \mid \delta(q, w) = q, \text{ every nonempty proper initial subword of } w \text{ is } q\text{-avoiding}\}.$$

Since B is generated by words w such that $\delta(q, w) = q$ and every such word w can be decomposed into a product of words $w = w_1 \cdots w_d$ with $\delta(q, w_i) = q$ and for which every nonempty proper initial subword of w_i is q-revisiting, we see that B is generated by E. Suppose that B is not free on E. Then we have a non-trivial relation of the form

$$\sum c_{i_1,\ldots,i_d} w_{i_1} \ldots w_{i_d} \ = \ 0,$$

in which only finitely many of the $c_{i_1,\ldots,i_d}$ are nonzero and each $w_{i_1}, \ldots, w_{i_d} \in E$. Since A is a monomial algebra, we infer that we must have a relation of the form

$$w_{i_1} \ldots w_{i_d} \ = \ w_{j_1} \ldots w_{j_e}$$

with

$$(w_{i_1}, \ldots, w_{i_d}) \neq (w_{j_1}, \ldots, w_{j_e}).$$

Pick such a relation with d minimal. Then note that $w_{i_1} \neq w_{j_1}$ for otherwise, we could remove w_{i_1} from both sides and have a smaller relation:

$$w_{i_2} \ldots w_{i_d} \ = \ w_{j_2} \ldots w_{j_e}.$$

But then either w_{i_1} is a proper q-revisiting initial subword of w_{j_1} or vice versa, which is impossible by the definition of the set E. The result follows. □

Lemma 4.2.5. *Let A be an automaton algebra and let $\Gamma = (Q, \Sigma, \delta, q_0, F)$ be its corresponding minimal finite state automaton. If B is a state subalgebra of A corresponding to some state q in F then A is nearly free as a left B-module.*

Proof. Let

$$E = \{1\} \cup \{w \in \Sigma^* \mid \delta(q_0, w) \in F \text{ and } w \text{ is } q\text{-avoiding}\}.$$

Let w be in E. The condition that $\delta(q_0, w) \in F$ is just saying that w has nonzero image in A. We claim first that

$$A \; = \; \sum_{x \in E} Bx.$$

Since A is spanned by words, it is sufficient to show that every word w with nonzero image in A is of the form bx for some $b \in B$ and $x \in E$. If w is in B, then we are done. Otherwise $\delta(q, w) \neq q$. Hence there is some proper initial subword b of w such that $w = bx$, $\delta(q, b) = q$ and x is either q-avoiding of $x = 1$. Thus we obtain the first claim.

Next observe that if

$$\sum_{i=1}^{d} b_i x_i \; = \; 0,$$

with $x_i \in E$, $b_i \in B$, then we must have $b_1 x_1 = \cdots = b_d x_d = 0$. To see this, observe by the argument above, every word u has a unique expression as bx for some word $b \in B$ and $x \in E$. Suppose that

$$\sum_{i=1}^{d} b_i x_i \; = \; 0$$

and $b_1 x_1 \neq 0$. Then there is some word u which appears with a nonzero coefficient in $b_1 x_1$. But by the preceding remarks, u cannot appear with nonzero coefficient in any of $b_2 x_2, \ldots, b_d x_d$. Since A is a monomial algebra, we obtain a contradiction. Thus A is nearly free as a left B-module. $\square$

We have now shown that an automaton algebra A has a free subalgebra B such that A is nearly free as a left B-module. To complete the proof that A is primitive or PI, we must show that nonzero ideals of A intersect certain state subalgebras non-trivially.

Proposition 4.2.6. *Let A be a prime automaton algebra with corresponding minimal finite state automaton $\Gamma = (Q, \Sigma, \delta, q_0, F)$. Suppose $q \in F$ is in a maximal equivalence class of F under the order described above and B is the state subalgebra corresponding to q. If I is a nonzero two sided ideal of A then $I \cap B$ is a nonzero two sided ideal of B.*

Proof. Every element $x \in I$ can be written as

$$\sum c_w w,$$

where $w \in \Sigma^*$. Among all nonzero $x \in I$, pick an element

$$x = c_1 w_1 + \cdots + c_d w_d$$

with d minimal. Then $c_1, \ldots, c_d$ are all nonzero. Pick u such that $\delta(q_0, u) = q$. Since A is prime, there is some word v such that $uvx \neq 0$. Then $uvx = c_1 uvw_1 + \cdots + c_d uvw_d$ is a nonzero element of I. By minimality of d, uvw_i has a nonzero image in A for every i. Consequently, $\delta(q_0, uvw_i) \in F$ for all i. Since q is in a maximal equivalence class of F, $\delta(q_0, uvw_i) \in [q]$ for $1 \leq i \leq d$.

Note that if $\delta(q_0, uvw_i) \neq \delta(q_0, uvw_j)$ for some i, j then by minimality of Γ, there is some word $w \in \Sigma^*$ such that $\delta(q_0, uvw_i w) \in F$ and $\delta(q_0, uvw_j w) \notin F$ (or vice versa). Consequently, $uvw_i w$ has nonzero image in A and $uvw_j w = 0$ has a nonzero image in A. Thus $uvxw$ is a nonzero element of I with a shorter expression than that of x, contradicting the minimality of d. It follows that

$$\delta(q_0, uvw_1) = \cdots = \delta(q_0, uvw_d).$$

Since $\delta(q_0, uvw_1) \in [q]$, there is some word u' such that $\delta(q_0, uvw_1 u') = q$. Consequently,

$$\delta(q_0, uvw_1 u') \;=\; \cdots \;=\; \delta(q_0, uvw_d u') \;=\; q.$$

Thus $vw_i u' \in B$ for $1 \leq i \leq d$ and so $vxu' \in B \cap I$ is nonzero. The result follows. □

By Kleene's Theorem 3.1.9, the collection of words accepted by a finite state automaton forms a regular language; by symmetry in the definition of a regular language, the reverse language obtained by reversing all strings in a given regular language is again regular. At the level of algebras, string reversal corresponds to multiplication of words in the opposite ring. [1]

Proof of Theorem 4.2.1. It is sufficient to show that A is right primitive since the opposite ring of A is again an automaton algebra. Let $\Gamma = (Q, \Sigma, \delta, q_0, F)$ be the minimal finite state automaton corresponding to A. We pick a state $q \in F$ that is in an equivalence class $[q]$ that is maximal with respect to the order described above. We let B be the state subalgebra of A corresponding to q. By Lemma 4.2.4, B is a free algebra. We now have two cases.

[1] If R is a ring, then R^{op}, the opposite ring of R, is equal to R as a set but is endowed with multiplication $r * s = s \cdot r$, where $\cdot$ is multiplication in R.

Case I: B is free on at most one generator.

In this case, we claim that A satisfies a polynomial identity. Let u be a word satisfying $\delta(q_0, u) = q$. Let v be a word with nonzero image in A. Since A is prime, there is some word w such that uwv has nonzero image in A. Thus $\delta(q_0, uwv) \in F$. Since $\delta(q_0, u) = q$, and $[q]$ is a maximal equivalence class, $\delta(q, wv) \in [q]$. In particular, there is some word t such that $\delta(q_0, uwvt) = q$. Thus $wvt \in B$. But B is free on at most one generator. In particular every word in B must be a power of some (possibly empty word) b. Thus v is a subword of b^m for some m. It follows that every word with nonzero image in A is a subword of b^m for some m. In particular, the number of words in Σ^* of length n that have nonzero image in A is bounded by the length of b. Hence A has GK dimension one (cf. Krause and Lenagan [18, Chapter 1]. Thus A is PI [23].

Case II: B is free on two or more generators.

In this case, B is primitive by Theorem 2.3.3. By Lemma 4.2.5, A is nearly free as a left B-module. By Proposition 4.2.6, nonzero ideals of A intersect B non-trivially. Hence A is right primitive by Proposition 4.1.3. The result follows.

4.3 Examples

In this section we are going the apply the idea of the proof to the previous examples to actually construct a faithful simple right module for the algebras.

Example 4.3.1. *Consider Example 3.3.2, where $A = k\{x, y\}/(x^2)$. Let B be the state subalgebra of A corresponding to the state q_0. Note that B is a free algebra on the generators y and xy, hence B is primitive by Jacobson's Theorem 2.3.3. We let $M = \sum_{i \geq 0} ke_i$ and let B act on M via the rules*

$$e_i y \;=\; e_{i-1} \qquad \text{and} \qquad e_i xy = e_{i^2+1},$$

where we take $e_{-1} = 0$. Then, as in the proof of Theorem 2.3.3, but dually, M is a faithful simple right B-module. Next, we define a module homomorphism

$$\phi : B \to M \;\; by \;\; \phi(b) = e_1 b.$$

We let I be the kernel of ϕ. Then I is a right ideal of B. Note that $A = B + Bx$ is a nearly free right B-module. We let $J = I + Ix$. Then J is a right ideal of A. Then

$N \cong A/J = A/(I + Ix)$ can be thought of as a direct sum of two copies of M. We write N as

$$N = M \oplus M' = \sum ke_i \oplus \sum ke_i{}'$$

with $e_iy = e_{i-1}$, $e_i{}'y = e_{i^2+1}{}'$, $e_ix = e_i{}'$, $e_i{}'x = 0$. We claim that N is a simple faithful right A-module.

Let $m_1 + m_2$ be an element of N, where $m_1 \in M$ and $m_2 \in M'$.

$$(m_1 + m_2)(b_1 + b_2x) = (m_1b_1 + m_2b_1 + m_1b_2x + m_2b_2x).$$

M and M' are both left B-modules, hence $(m_1 + m_2)(b_1 + b_2x) \in N$. We claim that N is a simple faithful right A-module. By contradiction assume that N is not faithful; i.e., there exists a nonzero element $b_1 + b_2x \in A$ such that $(m_1 + m_2)(b_1 + b_2x) = 0$ for any $(m_1 + m_2) \in N$. Consider

$$0 = (m_1)(b_1 + b_2x) = m_1b_1 + m_1b_2x.$$

A is a nearly free right B-module, so we should have $m_1b_1 = m_2b_2x = 0$. Note that $m_1b_1 = 0$ if and only if $b_1 = 0$, as M is a faithful right B-module. Similarly, $m_1b_2x = 0$ if and only if $b_2x = 0$. Then $b_1 + b_2x = 0$, we have a contradiction an M is a faithful simple A-module.

In order to show that N is a simple right A-module, we need to show that $(m_1+m_2)A = N$ for any element $(m_1 + m_2)$ in N. We have

$$(m_1 + m_2)A = (m_1 + m_2)(B + Bx) = (m_1B + m_2B + m_1Bx + m_2Bx) = M + M',$$

as $Bx \subseteq B$ and M and M' are simple B-modules.

N is a simple faithful right A-module, hence A is primitive.

Example 4.3.2. *Consider the Example 3.3.3 with Figure 3.3.3, where $A = k\{x, y\}/(x^3, y^2)$. Let B be the state subalgebra corresponding to q_2. Note that B is a free algebra on the generators xy and x^2y. Hence B is primitive by Jacobson's Theorem 2.3.3.*

We let $M = \sum_{i\geq 0} ke_i$ and let B act on M via the rules

$$e_ixy \;=\; e_{i-1} \qquad \text{and} \qquad e_ix^2y = e_{i^2+1},$$

where we take $e_{-1} = 0$. Next, we define a module homomorphism

$$\phi : B \to M \;\text{ by }\; \phi(b) = be_1.$$

We let I be the kernel of ϕ. Note that $A = B+Bx+Bx^2+By$ is a nearly free right B-module. We let $J = I + Ix + Ix^2 + Iy$ be an ideal of A. Then $N \cong A/J = A/(I + Ix + Ix^2 + Iy)$ can be thought of a a direct sum of four copies of M. We write N as

$$N = M \oplus M' \oplus M'' \oplus M''' = \sum ke_i \oplus \sum ke_i{}' \oplus \sum ke_i'' \oplus \sum ke_i{}'''$$

with $e_ix = e_i{}'$, $e_iy = e_i{}'''$, $e_i{}'x = e_i{}''$, $e_i{}'y = e_{i-1}{}'$, $e_i{}''x = 0$, $e_i{}''y = e_{i^2+1}{}''$, $e_i{}'''x = e_i{}'$, $e_i{}'''y = 0$. We claim that N is a simple faithful right A-module.

Let $m_1 + m_2 + m_3 + m_4$ be an element of N, where $m_1 \in M$, $m_2 \in M'$, $m_3 \in M''$ and $m_4 \in M'''$. We have

$$\begin{aligned}(m_1 + m_2 + m_3 + m_4)&(b_1 + b_2x + b_3x^2 + b_4y)\\ &= (m_1 + m_2 + m_3 + m_4)b_1 + (m_1 + m_2 + m_3 + m_4)b_2x\\ &+ (m_1 + m_2 + m_3 + m_4)b_3x^2 + (m_1 + m_2 + m_3 + m_4)b_4y.\end{aligned}$$

As M, M', M'', M''' are right B-modules, the product is in $M + M' + M'' + M''' = N$.

We need to show that N is a faithful right A-module. Towards a contradiction assume that N is not faithful; i.e., there exists a nonzero element $b = b_1 + b_2x + b_3x^2 + b_4y \in A$ such that $mb = 0$ for any $m \in N$. Let $m = m_1$. Then

$$0 = m_1(b_1 + b_2x + b_3x^2 + b_4y) = m_1b_1 + m_1b_2x + m_1b_3x^2 + m_1b_4y.$$

A is a nearly free left B-module, so we should have

$$m_1b_1 = m_1b_2x = m_1b_3x^2 = m_1b_4y = 0.$$

M is a faithful right B-module, hence we have $b_1 = b_2x = b_3x^2 = b_4y = 0$, implying $b_1 = b_2 = b_3 = b_4$. But then $b = 0$, so we have a contradiction.

In order to show that N is a simple right A-module, we need to show that $mA = N$ for any element m in N. Here

$$\begin{aligned}mA &= (m_1 + m_2 + m_3 + m_4)(B + Bx + Bx^2 + By)\\ &= (m_1 + m_2 + m_3 + m_4)B + (m_1 + m_2 + m_3 + m_4)Bx\\ &+ (m_1 + m_2 + m_3 + m_4)Bx^2 + (m_1 + m_2 + m_3 + m_4)By.\end{aligned}$$

We know that M, M', M'', M''' *are simple left* B*-modules. Hence the equation becomes*

$$mA = M + M' + M'' + M''' = N.$$

N *is a simple faithful right* A*-module, hence* A *is primitive.*

Bibliography

[1] J.-P. Allouche and J. Shallit, *Automatic Sequences. Theory, Applications, Generalizations*, Cambridge University Press: Cambridge, 2003.

[2] J. P. Bell, *Affine rings of low GK dimension*, Ph.D. thesis, University of California, San Diego, 2002.

[3] ______, *Examples in finite Gelfand-Kirillov dimension*, J. Algebra **263** (2003), 159–175.

[4] J. P. Bell and A. Smoktunowicz, *The prime spectrum of algebras of quadratic growth*, J. Algebra **319** (2008), 414–431.

[5] A. Y. Belov, V. V. Borisenko, and V. N. Latyshev, *Monomial algebras*, J. Math. Sci. **87** (1997), 3463–3575.

[6] G. M. Bergman, *A ring primitive on the right but not on the left*, Proc. Amer. Math. Soc. **15** (1964), 473–475.

[7] B. Bollobás, *Garph Theory, An introductory course*, Springer Verlag: New York, 1979.

[8] D. A. Cox, J. B. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms*, third ed., Undergrad. Texts in Math., Springer: New York, 2007.

[9] J. Dixmier, *Enveloping Algebras*, vol. 14, North-Holland Publishing Company: New York, 1977.

[10] D. Eisenbud, *Commutative Algebra with a View toward Algebraic Geometry*, Grad. Texts in Math., vol. 150, Springer-Verlag: New York, 1995.

[11] B. Farb and R. K. Dennis, *Noncommutative Algebra*, Grad. Texts in Math., no. 144, Springer-Verlag: New York, 1993.

[12] D. Farkas and L. W. Small, *Algebras which are nearly finite dimensional and their identities*, Israel J. Math. **127** (2001), 245–251.

[13] K. R. Goodearl and E. S. Letzter, *The Dixmier-Moeglin equivalence in quantum coordinate rings and quantized Weyl algebras*, **352** (2000), 1381–1403.

[14] I. N. Herstein, *Noncommutative Rings*, Carus Math. Monogr., John Wiley and Sons: New York, 1968.

[15] J. E. Hopcroft and J. D. Ullman, *Introduction to Automata Theory, Languages, and Computation*, Adison-Wesley, Reading: MA, 1979.

[16] N. Jacobson, *Structure of Rings*, no. 37, American Math. Soc. Colloquium Publications, 1964.

[17] S. Jøndrup, *Representations of skew polynomial algebras*, Proc. Amer. Math. Soc. **128** (2000), no. 5, 1301–1305.

[18] G. R. Krause and T. H. Lenagan, *Growth of Algebras and Gelfand-Kirillov Dimension.*, second ed., Graduate Studies in Mathematics, vol. 22, RI: American Mathematical Society, 2000.

[19] T.Y. Lam, *A First Course in Noncommutative Rings. 2nd edn.*, Grad. Texts in Math., vol. 131, Springer: New York, 2001.

[20] C. Lanski, R. Resco, and L. Small, *On the primitivity of prime rings*, J. Algebra **59** (1979), no. 2, 395–398.

[21] L. H. Rowen, *Ring Theory, Vol. I*, Pure and Applied Mathematics, no. 127, Academic Press: Boston, MA, 1988.

[22] M. Sipser, *Introduction to the Theory of Computation*, second ed., Thomson Course Technology: Boston, 2006.

[23] L.W. Small and R.B. Warfield Jr., *Prime affine algebras of Gelfand- Kirillov dimension one*, J. Algebra **91** (1984), no. 2, 386–389.

[24] B .W. Watson, *A taxonomy of finite automata minimization algorithms*, (1993), no. 93.