2003

A new approach to primary decomposition

Pamela R. Kochman
San Jose State University

A NEW APPROACH TO PRIMARY DECOMPOSITION

A Thesis

Presented to

The Faculty of the Department of Mathematics

San Jose State University

In Partial Fulfillment

of the Requirements of the Degree

Masters of Science

by

Pamela R. Kochman

August 2003

UMI Number: 1417485

APPROVED FOR THE DEPARTMENT OF MATHEMATICS

Dr. Eloise Hamann

Dr. Brian Peterson

Dr. Ho Kuen Ng

APPROVED FOR THE UNIVERSITY

ABSTRACT

A NEW APPROACH TO PRIMARY DECOMPOSITION

By Pamela R. Kochman

The Noether Lasker Decomposition Theorem extends a version of prime factorization from the integers to a much larger class of rings, including polynomials in several variables over a field. In this thesis, decomposition is calculated for Noetherian ideals and modules and also a class of non-Noetherian modules. A generalized version of the Noether Lasker Theorem, authored by Barbara Osofsky, is presented for the non-Noetherian case. The Osofsky theorem is based on fundamental homomorphism theorems. We show this generalized version implies the case for Noetherian modules, while maintaining an irredundant intersection of submodules with their unique set of associated primes. Then in the last section a monomial ideal in a particular local ring is decomposed as an irredundant finite intersection of parameter ideals.

CONTENTS

1. Introduction

A fascinating aspect of primary decomposition is its ubiquitous nature in mathematics. Not only is it a vital element of advanced mathematics included in Commutative Algebra, Algebraic Geometry, and Number Theory, but it is introduced at the earliest stages of math education. Of course it is not presented in the abstract form, but rather in bits and pieces pertaining to a particular subject matter. In the fourth grade the multiplication tables are learned. The following year factor trees or the prime factorization of whole numbers is introduced. The number 36 is no longer 3×12, 4×9, or 6×6, but rather a unique product of primes $2\times2\times3\times3$. Everyone has the same correct prime factorization, up to order. In fifth grade the "numbers" or rather the integers are not viewed as a principal ideal domain with unique factorization. They do not consider the prime ideals $\langle 2\rangle$ or $\langle 3\rangle$. They just find comfort in the uniqueness of prime factorization. In high school algebra much of the time is spent on finding the unique factorization of polynomials. Individual polynomials are not studied as part of the principal ideal domain $\mathbb{Z}[x]$ nor is the factor $(x-2)$ seen as a prime ideal where $\{x^2-4\}\in\langle x-2\rangle$. Students just know that everyone with the correct answer will uniquely factor $(x^2-4)=(x-2)(x+2)$.

In undergraduate algebra, the topic of unique factorization is explored. Unique factorization is not limited to principal ideal domains $\mathbb{Z}$ and $\mathbb{Z}[x]$, but it also occurs in $F[x]$, $F[x_1,\cdots,x_n]$, and $\mathbb{Z}[i]$. So it is no surprise that one might generalize unique factorization to include some rings of algebraic integers.

A great deal of the confusion with unique factorization arose from the assumption that an irreducible number was a prime number. In $\mathbb{Z}$ an irreducible number is a prime number. For $p, m, n \in \mathbb{Z}$, p is ***irreducible*** if $m \mid p$ implies $m = \pm p$ or ± 1 and p is a ***prime*** if $p \mid mn$ implies $p \mid m$ or $p \mid n$. But the equivalence of this relationship is not the case for all rings of algebraic integers.

Consider the ring $\mathbb{Z}\left[\sqrt{-5}\right]$. The element 6 has two distinct factorizations.

$$6 = 2 \cdot 3 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right).$$

2 and 3 are irreducibles. Let $n, m \in \mathbb{Z}$ and $\alpha = n + m\sqrt{-5}$ then $\alpha\bar{\alpha} = n^2 + 5m^2$. There are no integer solutions such that $2 = n^2 + 5m^2$ or $3 = n^2 + 5m^2$. This can be used to show $2, 3, 1+\sqrt{-5}$, and $1+\sqrt{-5}$ are all irreducible in $\mathbb{Z}\left[\sqrt{-5}\right]$. However $2 \mid 6$ but $2 \nmid 1+\sqrt{-5}$ and $2 \nmid 1-\sqrt{-5}$, therefore 2 is not prime. The realization was made that the prime property was a requirement for uniqueness of factorization, and in general an irreducible is not necessarily prime.

It was Ernst Kummer who noticed that primes were the key element to unique factorization. While trying to prove Fermat's Last Theorem, Kummer focused on the ring $\mathbb{Z}[\zeta]$, with ζ a root of unity. It was in one of these rings that he discovered unique factorization did not hold. He resolved this issue by introducing a congruence relationship between "ideal prime factors" and ideal numbers. He introduced numbers from out-side $\mathbb{Z}[\zeta]$ to use as factors when factoring elements within $\mathbb{Z}[\zeta]$. These "ideal factors" restored unique factorization. Using these "ideal factors" Kummer proved

Fermat's Last Theorem for a wide range of prime numbers – the so-called "regular" primes.

It was Dedekind who generalized unique factorization to include the ring of integers of any algebraic number field. He accurately amended the "ideal number" to reflect what it really is, a set of numbers, which he renamed an ideal. An ideal in a Dedekind domain can be expressed as a product of prime ideals. Every ideal of a Dedekind domain is generated by at most two elements. $\langle 6 \rangle$ can be uniquely factored in $\mathbb{Z}\left[\sqrt{-5}\right]$, a Dedekind domain, as follows:

$$\langle 6 \rangle = \left\langle 2, 1+\sqrt{-5} \right\rangle^2 \cdot \left\langle 3, 1+\sqrt{-5} \right\rangle \cdot \left\langle 3, 1-\sqrt{-5} \right\rangle.$$

Kronecker was a firm believer in abstracting theory. He did not want to rely on the real or complex numbers. Instead he only used the existence of integers and indeterminates and introduced a theory equivalent to Dedekind's theory of ideals.

Although there is no way to factor ideals multiplicatively in polynomial rings, Lasker showed how to generalize unique factorization into primary decomposition. His proofs used complicated arguments and were formulated only for affine rings and convergent power series rings. Using only intersections, $\langle 6 \rangle$ can be uniquely factored in $\mathbb{Z}\left[\sqrt{-5}\right]$ as follows:

$$\langle 6 \rangle = \left\langle 2, 1+\sqrt{-5} \right\rangle^2 \cap \left\langle 3, 1+\sqrt{-5} \right\rangle \cap \left\langle 3, 1-\sqrt{-5} \right\rangle.$$

Noether thoroughly reformulated and axiomatized Dedekind and Lasker's theories. She developed the general theory of primary decomposition from the ascending chain condition alone. In this way she enormously simplified the theory. Thus the Noether-Lasker Decomposition Theorem extends a version of prime factorization from the integers to a much larger class of rings, including polynomials in several variables over a field. A unique primary decomposition may involve more than a product of powers of prime numbers. It consists of a finite intersection of primary ideals which are generalized prime powers. These primary ideals may not be unique, but the associated primes will be unique. The form of the Noether-Lasker Primary Decomposition Theorem included in this paper is generalized further to include the primary decomposition of modules.

Noether Lasker Theorem: Let M be a finitely generated module over a commutative Noetherian ring R. Then there exists a finite set $\{ N_i \mid 1 \le i \le l \}$ of submodules of M such that:

a) $\bigcap_{i=1}^{l} N_i = 0$ and $\bigcap_{i \ne i_0} N_i$ is not contained in N_{i_0} for all $1 \le i_0 \le l$.

b) Each quotient M/N_i is primary for some prime P_i.

c) The P_i are all distinct for $1 \le i \le l$.

d) The primary component N_i is unique $\Leftrightarrow$ P_i does not contain P_j for any $j \ne i$.

This theorem does not seem to relate at all to the factoring of $\langle 6 \rangle$ in $\mathbb{Z}\left[\sqrt{-5}\right]$. Instead in part (a) of the Noether Lasker Theorem we are decomposing 0. To see the relationship first replace the ring $\mathbb{Z}\left[\sqrt{-5}\right]$ with the module $\mathbb{Z}\left[\sqrt{-5}\right]/\langle 6 \rangle$ over the ring $\mathbb{Z}$. From above

$$\langle 6\rangle = \langle 2, 1+\sqrt{-5}\rangle^2 \cap \langle 3, 1+\sqrt{-5}\rangle \cap \langle 3, 1-\sqrt{-5}\rangle.$$

To decompose 0, the following quotient factors are formed:

$$\langle 6\rangle / \langle 6\rangle = 0 = \langle 2, 1+\sqrt{-5}\rangle^2 / \langle 6\rangle \cap \langle 3, 1+\sqrt{-5}\rangle / \langle 6\rangle \cap \langle 3, 1-\sqrt{-5}\rangle / \langle 6\rangle.$$

By looking at the submodules $\left\{ \langle 2, 1+\sqrt{-5}\rangle / \langle 6\rangle, \langle 3, 1+\sqrt{-5}\rangle / \langle 6\rangle, \langle 3, 1-\sqrt{-5}\rangle / \langle 6\rangle \right\}$ in $\mathbb{Z}\left[\sqrt{-5}\right] / \langle 6\rangle$ we have an understanding of how to get to zero.

Conversely for a submodule *N* of the module *M*, consider M/N. If $0 = N/N = \bigcap_{p\ prime} N_p/N$, then $N = \bigcap_{p\ prime} N_p$. If *M* is not primary, $N \neq 0$, and $M \neq 0$ then the decomposition is not trivial.

In this paper various presentations of primary decomposition are provided. A connection will be established between the zero divisors of rings and modules and the primary decomposition of ideals and modules.

In section two a brief summary of the traditional approach to primary decomposition of ideals is presented. Some supplementary geometric interpretations of decomposition are given to add another perspective. An experienced reader can skip this section.

Section three contains basic properties of modules, submodules, and homomorphisms. Although modules are seen as a natural generalization of vector spaces, modules are really much more general and complex. Some examples are included to help clarify the properties of modules. The additional lemmas and propositions in section three are needed to either prove the Noether Lasker Theorem for Modules or are used in section five, where the Osofsky Theorem is compared to the Noether Lasker Theorem.

In section four a generalization of primary decomposition for modules, which was originally authored by Osofsky, will be studied. The terminology is not customarily used to study decomposition. Some terms are used in the study of non-commutative algebra. Although the generalized form of decomposition may not be reduced, it can be applied to any Abelian module over a Noetherian ring. Osofsky's proof of the generalized theorem is based on fundamental homomorphism theorems. Numerous proofs were omitted in her paper and left as exercises for the reader. These exercises will be renamed propositions and their proofs are included and found in sections three, four and five.

Section five compares the standard Noether Lasker Theorem with the Osofsky Theorem. It highlights and explains both the similarities and the differences between the two theorems.

Section six is a slight diversion. Two algorithms for finding a different type of decomposition are presented. Although the results apply to more general rings, in keeping within the scope of this paper, we will limit the findings to a local ring $k[x_1, \cdots, x_d]$ localized at $\langle x_1, \cdots, x_d \rangle$. Once the geometry of the dimension two case is explained, the theory follows quite easily. The end result produces a unique reduced decomposition expressed as an intersection of parameter ideals. Although the case is very specific, the process is clever and straightforward.

2. Primary Decomposition for Ideals

In this section traditional background material for ideal primary decomposition will be presented. The study of primary factorization will begin with principal ideal domains, where every primary ideal $\langle p^n \rangle = \langle p \rangle^n$, where p is a prime and $n > 0$, is just a power of a prime ideal. Thus every ideal I can be written uniquely (up to order) in the form

$$I = \langle p_1^{n_1} \rangle \cdot \langle p_2^{n_2} \rangle \cdot \quad \cdots \quad \cdot \langle p_r^{n_r} \rangle = \langle p_1^{n_1} \rangle \cap \langle p_2^{n_2} \rangle \cap \quad \cdots \quad \cap \langle p_r^{n_r} \rangle$$

where each $n_i > 0$ and the p_i are distinct primes. Then the scope broadens to include general commutative rings where the ideals need not be principal and the primary ideals may not be powers of prime ideals. Generalizing to rings comes at a cost, there may not be a unique intersection of the primary ideals, but the associated primes will be unique. In the following section we expand this foundation of ideal theory to include the decomposition of modules.

Definition 2.1: An ideal $\langle x \rangle$ generated by a single element is called a ***principal ideal***. A principal ideal ring is a ring in which every ideal is principal.

A principal ideal ring which is an integral domain is called a principal ideal domain, *PID*.

Definition 2.2: Let R be a ring. An ideal I, is ***irreducible*** in case I is a proper ideal of R and is not the intersection $I = a \cap b$ of ideals $a, b \neq I$.

Definition 2.3: A ***maximal ideal*** of a ring R is an ideal $M \neq R$ such that there is no proper ideal N of R properly containing M.

Definition 2.4: An ideal p, $p \neq R$, of R is called a ***prime ideal*** if $a, b \in R$ and $a \cdot b \in p$, implies $a \in p$ or $b \in p$.

In $\mathbb{Z}[x]$ the set of all polynomials with even coefficients is prime.

Definition 2.5: An ideal $Q\,(\neq R)$ in a commutative ring R is ***primary*** if for any $a, b \in R$

$a \cdot b \in Q$ and $a \notin Q \quad \Rightarrow \quad b^n \in Q$ for some $n \in \mathbb{N}$.

Equivalent to this condition is the following: An ideal q of a ring R is called ***primary*** if any zero divisor of R/q is nilpotent.

By examining a *PID* it is clear a primary ideal, that is a power of a prime ideal, is just a generalization of a prime ideal. In $\mathbb{Z}$, the primary ideals are $\langle p \rangle, \langle p^2 \rangle, \langle p^3 \rangle, \cdots$, where p is a prime. In $k[x, y]$ where k is a field $\langle x^2, y \rangle, \langle x^2, y^2 \rangle, \langle x^2, y^3 \rangle, \langle x, y \rangle^2 = \langle x^2, xy, y^2 \rangle, \cdots$ are primary ideals and $\langle x \rangle, \langle y \rangle$ and $\langle x, y \rangle$ are prime ideals.

Definition 2.6: The ***radical*** of an ideal q, *Rad* q, (or also noted as $\sqrt{q}$), is the intersection of all prime ideals containing q; equivalently, it is the set

$$Rad\ q = \left\{ x \in R \;\middle|\; x^n \in q \text{ for some } n > 0 \right\}$$

Theorem 2.7: The radical of a primary ideal is a prime ideal.

Radical ideals play an important role in preserving a sense of uniqueness when an ideal has multiple primary decompositions.

Consider $I = \langle x^2, y^3 \rangle$ in $k[x, y]$ where k is a field. Although neither x nor y belongs to

I, it is clear that $x \in \sqrt{I}$ and $y \in \sqrt{I}$. Also $(xy)^2 = x^2y^2 \in I$ since $x^2 \in I$, and thus $x \cdot y \in \sqrt{I}$. It is less obvious that $x + y \in \sqrt{I}$.

$$(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4 \in I$$

because $x^4, 4x^3y, 6x^2y^2 \in I$ (since they are all multiples of x^2), $4xy^3, y^4 \in I$ (since they are multiples of y^3). Thus $x + y \in \sqrt{I}$. But notice neither xy nor $x + y \in I$. So every element of the primary ideal I can be written as a power of an element of $\sqrt{I}$. It looks much more apparent when you consider $\sqrt{\langle x^2, y^3 \rangle} = \langle x, y \rangle$, but the core of the issue should not be overlooked.

In $k[x, y]$ the ideals $\langle x^2, y \rangle, \langle x^2, y^2 \rangle, \langle x^2, y^3 \rangle, \cdots$ as well as $\langle x^3, y^3, xy(x+y) \rangle$ are primary ideals each of which has the same radical namely $\langle x, y \rangle$.

Although it is often true for a prime ideal p that p^n is primary, it is not always the case.

Example 2.8: Let $M = k[x, y, z] / \langle xy - z^2 \rangle$ and let $\bar{x}, \bar{y}$, and $\bar{z}$ denote the images of x, y, and z respectively in *M*. Let $p = \langle \bar{x}, \bar{z} \rangle$. We have $\bar{x}\,\bar{y} = \bar{z}^2 \in p^2$ but $\bar{x} \notin p^2$ and $\bar{y} \notin p$, thus $\bar{y} \notin p^2$; hence p^2 is not primary.

However it is always true that $\sqrt{p^n} = p$, when $n \in \mathbb{N}$ and p is maximal.

A monomial ideal is an ideal $I \subset k[x_0, \cdots, x_r]$ generated by monomials in the variables $x_0, \cdots, x_r$. Monomial ideals generated by subsets of the variables are prime,

$\langle x_0 \rangle, \langle x_1, x_5, x_n \rangle, \cdots$. Monomial ideals generated by powers of some of the variables are irreducible, $\langle x_1^2 \rangle, \langle x_2^3, x_5, x_7^2 \rangle, \cdots$. Monomial ideals generated by square-free (that is multilinear) monomials are radical $\sqrt{\langle x_1^2 \rangle} = \langle x_1 \rangle$, $\sqrt{\langle x_2^3 x_5 x_7^2 \rangle} = \langle x_2 x_5 x_7 \rangle$. Monomial ideals containing a power of each of a certain subset of the variables and generated by elements involving no further variables, are primary $\langle x_0^3 \rangle$, $\langle x_0^3, x_1^5, x_0 x_1 \rangle \cdots$.

Lemma 2.9: The intersection of finitely many p-primary ideals is p-primary.

Theorem 2.10: Let R be a commutative ring with unity. Then M is a maximal ideal if and only if R/M is a field.

Corollary 2.11: Every maximal ideal in a commutative ring R with unity is a prime ideal.

Maximal ideals do not have to be finitely generated. Consider $k[x_1, x_2, \cdots]$, where $\langle x_1, x_2, \cdots \rangle$ is a maximal ideal and therefore prime and any power of this prime would be primary. If k is a field, the ideal $\langle x, y \rangle$ is maximal in $k[x, y]$ and therefore prime. $\langle x \rangle$ is also prime in $k[x, y]$ but $\langle x \rangle \subsetneq \langle x, y \rangle$ and therefore is not maximal. In $\mathbb{Z} \times \mathbb{Z}$ $\langle (0,1) \rangle$ is a prime ideal but $\langle (0,1) \rangle \subsetneq \langle (2,1) \rangle$ and therefore is not maximal.

In a *PID* every nonzero prime ideal is maximal, furthermore $\langle p^n \rangle$, where p is a prime ideal and $n \in \mathbb{N}$, is always primary. Generalizing from a *PID*, it is always true that the powers of maximal ideals are primary. In example 2.7 $M = k[x, y, z] / \langle xy - z^2 \rangle$, $p = \langle \overline{x}, \overline{z} \rangle$ is not maximal, and p^2 is not primary.

Definition 2.12: A ring R is called ***Noetherian*** if any ideal of R has a finite system of generators.

Theorem 2.13: The following statements are equivalent.

a) R is Noetherian

b) The ***Ascending Chain Condition (a.c.c.)*** for ideals holds: Any ascending chain of ideals of R, $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$ becomes stationary.

c) The ***maximal element condition*** for ideals holds: Any nonempty set of ideals of R contains a maximal element (with respect to inclusion).

The ring $k[x_1, x_2, \cdots]$, in an infinite number of indeterminates, is not Noetherian and therefore does not satisfy *a.c.c.* $\langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset \langle x_1, x_2, x_3 \rangle \subset \cdots$. This chain has no maximal element.

Hilbert Basis Theorem 2.14: If R is a Noetherian ring then so is $R[x_1, x_2, \cdots x_n]$.

Lemma 2.15: In a Noetherian ring, every irreducible ideal is primary.

Theorem 2.16: In a Noetherian ring, every proper ideal is the intersection of finitely many irreducible ideals.

Definition 2.17: An ideal I in a commutative Noetherian ring has a **primary decomposition** if $I = q_1 \cap q_2 \cap \cdots \cap q_r$ with each q_i primary. If no q_i contains $q_1 \cap \cdots \cap q_{i-1} \cap q_{i+1} \cdots \cap q_r$ and the radicals of q_i are all distinct, then the primary decomposition is said to be **reduced**.

Theorem 2.18: Every proper ideal of a commutative Noetherian ring has a reduced primary decomposition.

Theorem 2.19: If $I = q_1 \cap q_2 \cap \cdots \cap q_r = q_1' \cap q_2' \cap \cdots \cap q_s'$ are two reduced primary decompositions of I then $r = s$ and $q_1', \cdots, q_s'$, can be indexed so that $Rad\ q_i = Rad\ q_i'$ for all i.

Together theorems 2.18 and 2.19 are the Noether-Lasker Primary Decomposition Theorem for ideals. Consider the following ideals for decomposition.

Example 2.20: Let $R = \mathbb{R}[x, y, z]$ and $J = \langle xy, yz \rangle$. By examining the polynomials which generate J in R, a primary decomposition can be found. A second way to approach the problem is to consider it geometrically. Let $f(a_1, a_2, a_3) = 0$ for all $f \in J$. In this example every term of a polynomial $f \in J$ will have an xy or yz factor. $f(a_1, a_2, a_3) = 0$ is true when $(a_1, a_2, a_3) \in \{(a_i, 0, a_j), (0, a_m, 0)\}$ and $a_i, a_j, a_m \in \mathbb{R}$. Geometrically this represents the xz plane and the y-axis. Thus the unique primary decomposition for $J = \langle y \rangle \cap \langle x, z \rangle$ and the associated prime ideals respectively are $\langle y \rangle$ and $\langle x, z \rangle$.

Example 2.21: Let $R = \mathbb{R}[x, y, z]$ and $I = \langle xy, xz, yz \rangle$. From the geometric point of view we will look at the zeros of the polynomials generated by I. Zeros will occur when $x = 0$ and $y = 0$. Thus $\{(0, 0, a_m)\}$ is one set of components. $\{(a_j, 0, 0)\}$ and $\{(0, a_i, 0)\}$ are the other sets of components with $a_i, a_j, a_m \in \mathbb{R}$. Pictorially this represents the union of the x, y, and z axis. It is clear the x, y, and z axis are independent prime components of the ideal I. Therefore the primary decomposition is $I = \langle x, y \rangle \cap \langle x, z \rangle \cap \langle y, z \rangle$, where the respective prime ideals are $\langle x,y\rangle, \langle x,z\rangle$, and $\langle y,z\rangle$. The ideals in examples 2.20 and 2.21 have unique primary decompositions. Example 2.21 considers an ideal where the primary decomposition is not unique.

Example 2.22: Let the ring $R = k[x,y,z]$ and the ideal $N = \langle x^2, xz, xy, yz\rangle$.

$N = \langle x,z\rangle \cap \langle x,y\rangle \cap \langle x^2,y,z\rangle = \langle x,z\rangle \cap \langle x,y\rangle \cap \langle x,y,z\rangle^2$ represent two different decompositions. However, $\sqrt{\langle x,z\rangle}$, $\sqrt{\langle x,y\rangle}$, and $\sqrt{\langle x^2,y,z\rangle}$ are respectively, $\langle x,z\rangle$, $\langle x,y\rangle$, and $\langle x,y,z\rangle$ and are equal to $\sqrt{\langle x,z\rangle}$, $\sqrt{\langle x,y\rangle}$ and.. $\sqrt{\langle x,y,z\rangle^2}$. The result of the containment of the associated prime ideals, in this case $\langle x,z\rangle \subsetneq \langle x,y,z\rangle$ and $\langle x,y\rangle \subsetneq \langle x,y,z\rangle$, is multiple primary decompositions.

It seems inconsistent to call $\langle x,y,z\rangle$ an embedded prime while $\langle x,y\rangle$ and $\langle x,z\rangle$ are isolated primes. The names isolated and embedded come from geometry. In this example the geometry is defined by the zeros of $\langle x,y\rangle$ that is when $x = y = 0$ or the z axis and for $\langle x,z\rangle$ the zeros form the y axis. The embedded ideal $\langle x,y,z\rangle$ has zeros that corresponds to the origin $(0,0,0)$. $(0,0,0)$ is embedded in the z axis and the y axis.

3. A Traditional Approach to Primary Decomposition for Modules

The concept of a module is an immediate generalization of that of a vector space. Now, however, instead of the scalars being in a division ring, we allow them to be elements of an arbitrary ring. Modules are much more general and complex than vector spaces. Historically the theory of modules did not develop from an extension of vector spaces. The concept of module made its first appearance in algebraic number theory, and due to Emmy Noether became an important tool in algebra. In this section modules over a ring are viewed as a generalization of Abelian groups.

Definition 3.1: Let R be a ring which has an identity element 1. A ***left R module*** is an Abelian group M together with a left action $R \times M \to M$, $(r,x) \to rx$ of R on M such that

1. $r(sx) = (rs)x$
2. $r(x+y) = rx + ry, \quad (r+s)x = rx + sx$
3. $1 \cdot x = x$

for all $x, y \in M$, $r, s \in R$. Elements of R will be referred to as scalars.

Any Abelian group is a module over the ring $\mathbb{Z}$ of integers, where scalar multiplication of x by a positive integer n means adding x to itself n times. Consider the ring R as an R module and Q a primary ideal as a submodule of R. Indeed, if I is any left ideal of the ring R, then the quotient group R/I is a module over R under the induced scalar multiplication $s \cdot (r + I) = sr + I$. Therefore all of the theorems for modules apply to Abelian groups.

The propositions that are proved in this section will be required in section five for developing the relationship between the Noether Lasker Theorem and the Osofsky Theorem. The proofs of these propositions were left as exercises in the original paper, but have been completed for this paper. The unproved theorems and lemmas are important for the study of traditional module decomposition and the proofs can be found in any standard text such as those listed in the works cited, in particular Kunz, Grillet, and Zariski.

Note special care must be taken when forming submodules. First consider the more familiar example where a subring is not an ideal. $\mathbb{Z}$ is a subset of the rational numbers and a subring of $\mathbb{Q}$. However, $\mathbb{Z}$ is not an ideal of $\mathbb{Q}$. Now consider modules over a ring and their submodules. The module or submodule must be closed under scalar multiplication. For instance let $R = k\left[x^2\right]$ and let $M = k[x]$ where k is a field. M is naturally an R module, but R is not naturally an M module. $x^2 \in R$ and $x \in M$ however $x \cdot x^2 = x^3 \notin R$. If R is expanded where $R = k\left[x^2, x^3\right]$ then R is an M module. Not only is $x^3 \in R$ but any power, x^s, where $s \geq 3$ can be formed from $\left(x^2\right)^n \left(x^3\right)^m$ where $m, n,$ and s are integers and $n \geq 0$, $m \geq 1$

One might wonder about trying to set up a notion of a prime submodule generalizing prime ideal, but this does not turn out to be useful.

Let M and N be R modules. The defining property of a ***module homomorphism*** φ: $M \to N$ is that $(r \cdot x + s \cdot y)\varphi = r \cdot (x)\varphi + s \cdot (y)\varphi$ for all $x, y \in M$ and $r, s \in R$. Notice the function will be written to the right of their arguments, on the side opposite the scalars. In the examples below note the effects the R module scalars have on the homomorphisms, isomorphisms, one to one and onto properties.

Example 3.2: Let $\mathbb{Z}[x]$ be a $\mathbb{Z}$ module and $f(x), g(x) \in \mathbb{Z}[x]$ and $c, d \in \mathbb{Z}$. Let $\varphi : \mathbb{Z}[x] \to \mathbb{Z}[x]$ be defined by $(f(x))(\varphi) = (f(x)) \cdot x$.

φ is a module homomorphism, since $\left(c\left(f(x)\right) + d\left(g(x)\right)\right)\varphi = \left(c\left(f(x)\right) + d\left(g(x)\right)\right)x$ $= c\left(f(x)\right)x + d\left(g(x)\right)x = c\left(f(x)\right)\varphi + d\left(g(x)\right)\varphi$.

Let $\mathbb{Z}[x]$ be a ring and $\varphi : \mathbb{Z}[x] \to \mathbb{Z}[x]$ is defined by $(f(x))(\varphi) = (f(x)) \cdot x$. φ is not a ring homomorphism, since $2x^3 \in \mathbb{Z}[x]$ and $2x^3 = (2x^2)\varphi \neq (2)\varphi \cdot (x^2)\varphi = 2x \cdot x^3 = 2x^4$.

The module homomorphism ϕ is an isomorphism if it is one-to-one and onto. Just as in other algebraic structures such as groups, rings, and vector spaces, an isomorphism is essentially a renaming of the elements of the module M. Again special attention must be given to modules and the scalar multiplication. A ring isomorphism may not be an R module isomorphism.

Let the ring $R = k[x, y]$ where k is a field. $k[x,y]/\langle x\rangle \cong k[y] \cong k[x] \cong$ $k[x,y]/\langle y\rangle$. Thus $k[x,y]/\langle x\rangle \cong k[x,y]/\langle y\rangle$ as rings. Let $M_1 = k[x,y]/\langle x\rangle$ and $M_2 = k[x,y]/\langle y\rangle$ be R modules where $R = k[x,y]$ and the scalar multiplication is the natural choice. There does not exist a ϕ such that $\phi : k[x,y]/\langle x\rangle \to k[x,y]/\langle y\rangle$ is a module isomorphism. If ϕ is an isomorphism then ϕ must be one to one. Let

$0 \neq m \in k[x,y]/\langle x\rangle$ and x the scalar from R. $xm = 0$ in $k[x,y]/\langle x\rangle$ thus $(xm)\phi$ must equal zero in $k[x,y]/\langle y\rangle$. However, $(xm)\phi = x(m)\phi$ and since $m \neq 0$ then $(m)\phi \neq 0$. x will not annihilate a nonzero element in $k[x,y]/\langle y\rangle$. Thus there is no module isomorphism between $k[x,y]/\langle x\rangle$ and $k[x,y]/\langle y\rangle$ which will satisfy the one to one or the onto property.

Definition 3.3: A module M is called ***cyclic*** provided $M = R\cdot x = \{r\cdot x \mid r \in R\}$ for some $x \in M$.

Proposition 3.4: Any cyclic module $R\cdot x$ is isomorphic to the quotient module R/I where $I = \{r \in R \mid r\cdot x = 0\}$.

Proof: Let $\varphi: R \to R\cdot x$ defined by $(r)\varphi = r\cdot x$ where $r \in R$.

Show φ is a module homomorphism.

Let $r_1, r_2 \in R$.

$$(r_1 + r_2)\varphi = (r_1 + r_2)x = r_1x + r_2x = (r_1)\varphi + (r_2)\varphi$$

$$(r_2r_1)\varphi = (r_2r_1)x = r_2(r_1x) = r_2(r_1)\varphi$$

Therefore φ is a module homomorphism.

Let $I = \ker\varphi = \{r \in R \mid r\cdot x = 0\} \subseteq R$. By the first module homomorphism theorem $R\cdot x \cong R/I$.

Definition 3.5: A submodule $Q \subset M$ is called ***irreducible*** (in M) if the following condition is satisfied: If $Q = U_1 \cap U_2$ with two submodules $U_i \subset M\,(i = 1,2)$, then $Q = U_1$ or $Q = U_2$.

Definition 3.6: Let M be any R module. For $x \in M$ we let $(0:x)$ denote the ***annihilator of x*** in R that is, $(0:x) = \{ r \in R \mid r \cdot x = 0 \}$.

The annihilator of x is an ideal of R. If $I = \{ r \in R \mid rm = 0 \text{ for all } m \in M \}$, then I is called the ***annihilator of M*** in R also denoted $Ann(M)$.

Lemma 3.7: If R is commutative, then any ideal P maximal in $\{ (0:x) \mid 0 \neq x \in M \}$ is prime.

Proof: Note that P cannot equal R since $1 \notin P$. Let $0 \neq x_0 \in M$ have $P = (0:x_0)$. If $ab \in P$ and $b \notin P$, then $0 \neq b \cdot x_0$ and $(0:b \cdot x_0) \supseteq R \cdot a + P$. By maximality of P, $P = R \cdot a + P$, so $a \in P$. Thus P is prime.

Definition 3.8: Let R be a ring and let M be an R module. A prime ideal $\boldsymbol{p}$ of R, $\boldsymbol{p} \neq R$ is ***associated to M*** if $\boldsymbol{p}$ is the annihilator of an element of M. The set of all primes associated to M is written $Ass(M)$.

Lemma 3.9: For all prime ideals $\boldsymbol{p}$ of R, $\boldsymbol{p} \neq R$ we have $Ass(R/\boldsymbol{p}) = \{\boldsymbol{p}\}$, and $\boldsymbol{p}$ is the annihilator of any $x \neq 0$ in $R/\boldsymbol{p}$.

Definition 3.10: A submodule $P \subset M$ is called ***primary*** if $Ass(M/P)$ consists of a single element. If $\boldsymbol{p}$ is this prime ideal, then P is also called ***p-primary***. ***M*** **is *p*-primary,** if the prime ideal $\boldsymbol{p}$ is associated with M and no other prime is.

Lemma 3.11: Let M be an R module, Q an irreducible submodule of M, and $Q \neq M$. Then Q is primary.

Lemma 3.12: For any submodule $U \subset M$,

$$Ass(U) \subset Ass(M) \subset Ass(U) \cup Ass(M/U).$$

Definition 3.13: A module M is called ***Noetherian*** provided every submodule of M is finitely generated, that is, if N is a submodule of M, then there exists a finite set $\{a_1, \cdots a_n\} \subseteq N$ such that $N = \left\{ \sum_{j=1}^{n} r_j \cdot a_j \,\middle|\, r_j \in R \right\}$.

Remark: a ring is Noetherian if it is Noetherian as a module over itself.

Definition 3.14: A module K is said to satisfy the ***ascending chain condition (a.c.c.)*** on submodules if for every chain $K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n \subseteq \cdots$ of submodules of K there is an integer n such that $K_i = K_n$ for all $i \geq n$.

Definition 3.15: Let M be an R module ordered by the relation $\subseteq$. M has the **maximum condition** if for any non-empty family $\mathscr{F}$ of submodules of M there is a maximal element of $\mathscr{F}$.

Proposition 3.16: Let M be an R module. M has the maximum condition $\Leftrightarrow$ M is Noetherian.

Proof: Show maximum condition $\Rightarrow$ Noetherian $\Rightarrow$ a.c.c. $\Rightarrow$ maximum condition

(a). Maximum condition $\Rightarrow$ Noetherian.

Let K be a submodule of M. Let $\mathscr{F}$ be the family of all finitely generated submodules of K. M has maximal condition so there exists a maximal element of $\mathscr{F}$ call it N. N is finitely generated. Let $k \in K - N$. Consider the submodule $N + kR$, which is finitely generated by k and the generators of N. Since N is a maximal element among finitely generated submodules of K, and $N \subseteq N + kR$, thus $N = N + kR \Rightarrow k \in N$. Therefore $K = N$ and K is finitely generated. Therefore Maximum condition $\Rightarrow$ Noetherian.

(b). Noetherian $\Rightarrow$ a.c.c.

Suppose M is Noetherian, (i.e. each submodule K_i is finitely generated).

Show for every ascending sequence $K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n \subseteq \cdots$ of submodules of M there exists an i such that $K_i = K_l$ for all $i \geq l$.

Let $K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n \subseteq K_{n+1} \subseteq \cdots$ be an ascending sequence of submodules of M. Let $K = \bigcup_{n>0} K_n$.

Show K is a submodule. Let $m_1, m_2 \in K$, then there exist some i, j, such that $m_1 \in K_i$ and $m_2 \in K_j$. Without loss of generality suppose $i \leq j$, thus $K_i \subseteq \cdots \subseteq K_j \subseteq \cdots$. Then $m_1, m_2 \in K_j$ a submodule. Thus for a scalar $r \in R$,

$$r(m_1 + m_2) \in K_j \subseteq K$$

$$(r_1 + r_2)m \in K_j \subseteq K$$

$$r_1(r_2 m) = (r_1 r_2)m \text{ in } K_j \subseteq K.$$

Therefore K is a submodule.

K is a submodule of M, thus K is finitely generated. Let X be the generating set of K. Since X is finite there exists some K_l which contains X hence $K \subseteq K_l$.

But $K = \bigcup_{n>0} K_n \Rightarrow K_l \subseteq K$. Thus $K_l = K$ for all $l \geq n$.

(c). a.c.c. $\Rightarrow$ maximum condition

Suppose M satisfies the ascending chain condition. Let $\mathscr{F}$ be a non-empty family of submodules of M. Since $\mathscr{F}$ is non-empty there exists a submodule $K_1 \in \mathscr{F}$. If K_1 is not maximal in $\mathscr{F}$, then there exists $K_2 \in \mathscr{F}$ such that $K_1 \subset K_2$. If K_2 is not maximal in $\mathscr{F}$ there is a $K_3 \in \mathscr{F}$ such that $K_1 \subset K_2 \subset K_3$. Since M satisfies the ascending chain condition this process must stop. Thus a maximal element of $\mathscr{F}$ is reached. Therefore $\mathscr{F}$ has maximum condition. □

Proposition 3.17: $\mathbb{Z}$ is Noetherian and has the maximum condition.

Proof: Any submodule of $\mathbb{Z}$ ($\mathbb{Z}$ over $\mathbb{Z}$) is of the form $n\mathbb{Z}$ where $n \in \mathbb{Z}$. $\mathbb{Z}$ is finitely generated by $\langle 1 \rangle$ and any submodule would be finitely generated by $\langle n \rangle$. Thus $\mathbb{Z}$ is Noetherian. By Proposition 3.16 $\mathbb{Z}$ has maximum condition.

$\mathbb{Z}$ is Noetherian and therefore has ascending chain condition. Let $n \in \mathbb{Z}$ then $\langle n \rangle \supset \langle n^2 \rangle \supset \cdots \supset \langle n^m \rangle \cdots$ so $\mathbb{Z}$ does not have descending chain condition. $\mathbb{Z}[x]$ is Noetherian and $0 \subseteq \langle 2 \rangle \subseteq \langle 2, x \rangle$ is an example of a finite ascending chain.

Theorem 3.18: Any homomorphic image of a Noetherian module is a Noetherian module.

Lemma 3.19: If M is a Noetherian R module and N is a submodule of M, then M/N is a Noetherian R module.

Theorem 3.20: Let $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ be a short exact sequence of modules. Then B satisfies the ascending chain condition on submodules if and only if A and C satisfy it.

Theorem 3.21 The Fundamental Theorem of Finitely Generated Modules over a *PID*: If R is a *PID* then M, a finitely generated R module, is a direct sum of cyclic submodules.

Proposition 3.22: If a ring R is Noetherian, then every submodule of a finite direct sum of copies of the finitely generated R module R is also finitely generated.

Proof by induction on k, the number of copies of R.

R is Noetherian so every submodule of R is finitely generated. Thus a finite direct sum of one copy of R has every submodule finitely generated. Therefore it is true for $k=1$. Assume it is true for k copies of R, i.e. $R^k = \underbrace{R \oplus R \oplus \cdots \oplus R}_{k\ copies}$ and every submodule of this is finitely generated. Show it is true for $k+1$ copies of R.

$$R^k \oplus 0 \cong R^k \text{ is Noetherian}$$

$$R^k \oplus R \cong R^{k+1}$$

$$R^k \oplus R \big/ R^k \oplus 0 \;\cong\; \{0\} \oplus R \big/ 0 \cong R \text{ is Noetherian}$$

Furthermore by a one-to-one correspondence homomorphism theorem

$0 \to R^k \oplus 0 \xrightarrow{\subset} R^k \oplus R \to R^k \oplus R \big/ R^k \oplus 0 \to 0$ is a short exact sequence.

Since $R^k \oplus 0$ is Noetherian and $R^k \oplus R \big/ R^k \oplus 0$ is Noetherian, then by Theorem 3.20 R^{k+1} is Noetherian. Thus the hypothesis is true for all k.

Proposition 3.23: If M is a finitely generated module over a Noetherian ring and $\mathscr{F}$ is a non-empty family of submodules of M, then there is a maximal element of $\mathscr{F}$.

Proof: Let M be a finitely generated module over a Noetherian ring R. By Definition 3.13 M is Noetherian. By assumption $\mathscr{F}$ is a non-empty family of submodules of M. By Proposition 3.16 M has maximum condition and therefore there is a maximal element of $\mathscr{F}$.

Lemma 3.24: If R is Noetherian and $M \neq 0$, then $Ass(M) \neq \varnothing$.

Theorem 3.25: Let M be a finitely generated module over a Noetherian ring R. Then there is a chain of submodules

$$M = M_0 \supset M_1 \supset \cdots \supset M_n = \langle 0 \rangle$$

such that $M_i / M_{i+1} \cong R/\boldsymbol{p}_i$ for some prime ideal $\boldsymbol{p}_i$ of R $(i = 0, \cdots, n-1)$ and $\boldsymbol{p}_i \neq R$.

Corollary 3.26: For a finitely generated module M over a Noetherian ring R, $Ass(M)$ is a finite set. In particular, $Ass(R)$ is finite.

Definition 3.27: A submodule $U \subset M$ has a ***primary decomposition*** if there are primary submodules $P_1, \cdots, P_s$ $(s \geq 1)$ of M such that

(1) $$U = P_1 \cap \cdots \cap P_s.$$

The primary decomposition (1) is called ***reduced*** if the following holds:

a) If P_i is p_i – primary $(i = 1, \cdots, s)$, then $p_i \neq p_j$ for $i \neq j$ $(i, j = 1, \cdots, s)$.

b) $\bigcap_{j \neq i} P_j \not\subset P_i$ for $i = 1, \cdots, s$.

The P_i occurring in a reduced primary decomposition are also called the primary components of U.

Noether Lasker Theorem 3.28: Let M be a finitely generated module over a commutative Noetherian ring R. Then there exists a finite set $\{ N_i \mid 1 \leq i \leq l \}$ of submodules of M such that:

a) $\bigcap_{i=1}^{l} N_i = 0$ and $\bigcap_{i \neq i_0} N_i$ is not contained in N_{i_0} for all $1 \leq i_0 \leq l$.

b) Each quotient M/N_i is primary for some prime P_i.

c) The P_i are all distinct for $1 \le i \le l$.

d) The primary component N_i is unique $\Leftrightarrow$ P_i does not contain P_j for any $j \ne i$.

Example 3.29: Let $R = M = k[x,y,z]/\langle x^2z^2, xyz^2\rangle$ where k is a field. Let M be an R module.

Let $N_1 = \langle z^2\rangle/\langle x^2z^2, xyz^2\rangle$ $N_2 = \langle x\rangle/\langle x^2z^2, xyz^2\rangle$, and $N_3 = \langle x^2, y\rangle/\langle x^2z^2, xyz^2\rangle$.

$0 = N_1 \cap N_2 \cap N_3 = \langle z^2\rangle/\langle x^2z^2, xyz^2\rangle \cap \langle x\rangle/\langle x^2z^2, xyz^2\rangle \cap \langle x^2, y\rangle/\langle x^2z^2, xyz^2\rangle$.

$M/N_1 = k[x,y,z]/\langle z^2\rangle$, $M/N_2 = k[x,y,z]/\langle x\rangle$, and $M/N_3 = k[x,y,z]/\langle x^2, y\rangle$ are primary with the associated primes in $k[x,y,z]$ respectively $\langle z\rangle$, $\langle x\rangle$, $\langle x,y\rangle$.

$\langle x\rangle \subset \langle x,y\rangle$ so the decomposition is not unique.

An alternate decomposition would be

$$0 = \langle z^2\rangle/\langle x^2z^2, xyz^2\rangle \cap \langle x\rangle/\langle x^2z^2, xyz^2\rangle \cap \langle x^2, xy, y^2\rangle/\langle x^2z^2, xyz^2\rangle.$$

4. Osofsky's Primary Decomposition Theorem

Osofsky claims her generalized version of primary decomposition for modules over a commutative Noetherian ring can be studied as a supplementary topic at the conclusion of an introductory undergraduate algebra course. She has reduced the number of definitions and propositions to a minimum only requiring 4.1 through 4.4, 4.6, 4.11, and 4.17 to prove her primary decomposition theorem 4.19. The proof of theorem 4.19 relies on the homomorphism theorems included in a basic algebra course. Zorn's lemma is also needed to prove Proposition 4.14. Proposition 4.21 is a generalization of the Fundamental Theorem of Finitely Generated Modules over a *PID*. The proof of Proposition 4.21 relies on Osofsky Theorem 4.19 as well as Propositions 4.9, 4.10, and 4.17. The remaining propositions and examples in section four are included to help clarify the new definitions and notation.

Definition 4.1: M is ***uniform*** if it is a nonzero module and any two nonzero submodules have nonzero intersection.

Definition 4.2: ***M contains enough uniforms*** provided it is a nonzero module and every nonzero submodule contains a uniform submodule.

Definition 4.3: If U and V are uniform, we say U is ***subisomorphic*** to V and write $U \sim V$ provided U and V contain nonzero isomorphic submodules.

Definition 4.4: M is called ***primary*** if M has enough uniforms and any two uniform submodules of M are subisomorphic.

A nonzero submodule of a uniform module is uniform. If M is a uniform module with nonzero submodules U and V then $U \cap V \neq 0$ is a nonzero uniform submodule. Hence every uniform submodule is primary.

Example 4.5: The module $\mathbb{Z}$ is a uniform module over the ring of integers, $\mathbb{Z}$. Let I and J be two nonzero ideals of $\mathbb{Z}$ and let $0 \neq m \in I$ and $0 \neq n \in J$. Then the nonzero element $mn \in I \cap J$ so $I \cap J \neq 0$. $\mathbb{Z}$ is a uniform module and therefore must be primary.

Proposition 4.6: $\sim$ is an equivalence relation on the class of all uniform modules.

Proof:

Reflexive: Let U be a nonzero uniform module. U is a submodule of U, $U \cong U$, and therefore $U \sim U$.

Symmetric: If U and V are nonzero uniform modules and $U \sim V$ then there exists a nonzero submodule U_1 contained in U and a nonzero submodule V_1 contained in V such that $U_1 \cong V_1$ thus $V_1 \cong U_1$ and therefore $V \sim U$.

Transitive: If U, V, and W are nonzero uniform modules and $U \sim V$ then there exist nonzero submodules U_1 contained in U and V_1 contained in V such that $U_1 \cong V_1$. And if $V \sim W$ then there exist nonzero submodules V_2 contained in V and W_1 contained in W such that and $V_2 \cong W_1$. V is a uniform module therefore $V_1 \cap V_2 \neq 0$. Let V_3 be the nonzero submodule such that $V_3 = V_1 \cap V_2$. $V_3 \subseteq V_1 \cong U_1$ thus U_1 contains a nonzero submodule U_2 such that $V_3 \cong U_2$. Also $V_3 \subseteq V_2 \cong W_1$ thus W_1 contains a nonzero submodule W_2 such that $V_3 \cong W_2$. Thus $U_2 \cong W_2$ and $U \sim W$. Therefore $\sim$ is an equivalence relation on the class of all uniform modules. □

Let $[U]$ denote the equivalence class of the uniform module U.

Proposition 4.7: Any commutative domain is uniform as a module over itself.

Proof: Let D, a commutative domain, be viewed as a module over itself. Let N_1 and N_2 be two nonzero submodules of D where $0 \neq n_1 \in N_1$ and $0 \neq n_2 \in N_2$. n_2 can be viewed as a scalar in the D ring, thus $n_2 n_1 \in N_1$ and $n_2 n_1 \neq 0$ since D is a domain. Similarly, n_1 can be viewed as a scalar in the D ring, thus $0 \neq n_1 n_2 \in N_2$. Since D is commutative $n_2 n_1 = n_1 n_2$. Therefore $0 \neq n_1 n_2 \in N_1 \cap N_2$ and D is uniform.

Proposition 4.8: A vector space over a field is uniform if and only if it is one dimensional. Any nonzero vector space contains enough uniforms and is primary.

Proof: Assume $\mathbf{U} \neq \mathbf{0}$ is a one dimensional vector space over a field K. Let $\mathbf{u}$ be a generator of $\mathbf{U}$. Let $\mathbf{U}_1$ and $\mathbf{U}_2$ be nonzero subspaces of $\mathbf{U}$. Then there exist some nonzero $k_1, k_2 \in K$ such that $\mathbf{U}_1 = \langle k_1\mathbf{u} \rangle$ and $\mathbf{U}_2 = \langle k_2\mathbf{u} \rangle$. Hence $\mathbf{0} \neq k_1 k_2 \mathbf{u} \in \mathbf{U}_1 \cap \mathbf{U}_2$ and $\mathbf{U}$ is uniform. Therefore a one dimensional vector space is uniform.

Conversely, $\mathbf{V} = \mathbf{0}$ cannot be uniform, since $\mathbf{V}$ must be a nonzero module. Let $\mathbf{V}$ be a uniform vector space over a field K with a basis $\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n\}$ where $n > 1$. Let $\mathbf{V}_1 = \text{span}\{\mathbf{v}_i\}$ and $\mathbf{V}_2 = \text{span}\{\mathbf{v}_j\}$ where $\mathbf{v}_i, \mathbf{v}_j \in \{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n\}$ and $\mathbf{v}_i \neq \mathbf{v}_j$. $\mathbf{V}$ is uniform therefore there exists a $\mathbf{0} \neq \mathbf{v} \in \mathbf{V}_1 \cap \mathbf{V}_2$. $\mathbf{v} \in \mathbf{V}$ and since $\mathbf{v} \neq \mathbf{0}$ there exists nonzero $k_i, k_j \in K$ such that $k_i\mathbf{v}_i = \mathbf{v}$ and $k_j\mathbf{v}_j = \mathbf{v}$. Thus $k_i\mathbf{v}_i = k_j\mathbf{v}_j \Rightarrow k_i\mathbf{v}_i - k_j\mathbf{v}_j = \mathbf{0}$. Thus $\mathbf{v}_i$ and $\mathbf{v}_j$ are linearly dependent. Therefore $\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n\}$ is linearly dependent. This is a contradiction since $\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n\}$ is a basis for $\mathbf{V}$. Thus the dimension of $\mathbf{V}$ is one.

We now show any nonzero vector space contains enough uniforms.

Let $\mathbf{W} \neq \mathbf{0}$ be a vector space and $\mathbf{W}_i$ be a nonzero subspace of $\mathbf{W}$. The dimension of $\mathbf{W}_i \geq 1$, so there exists a basis element $\mathbf{0} \neq \mathbf{w}_i \in \mathbf{W}_i$. The subspace $\langle \mathbf{w}_i \rangle$ has dimension one so as proved above $\langle \mathbf{w}_i \rangle$ is uniform. Therefore $\mathbf{W}$ has enough uniforms.

Next we show any nonzero vector space is primary.

Let $\mathbf{S} \neq \mathbf{0}$ be a vector space. By above $\mathbf{S}$ contains enough uniforms. Let $\mathbf{S}_1$ and $\mathbf{S}_2$ be uniform subspaces of $\mathbf{S}$. By part one of Proposition 4.8 $\mathbf{S}_1$ and $\mathbf{S}_2$ are one dimensional. Therefore $\mathbf{S}_1$ is isomorphic to $\mathbf{S}_2$ and $\mathbf{S}$ is primary.

Proposition 4.9: A cyclic $\mathbb{Z}$ module, $\mathbb{Z}/n\mathbb{Z}$ is uniform if and only if n is 0 or a power p^i of a prime where i is an integer and $i > 0$.

Proof: Assume $n = 0$ then $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}$ a commutative domain. By Proposition 4.7 $\mathbb{Z}$ is uniform as a module over itself.

$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. This proposition will be proved for $\mathbb{Z}_n$ and thus it will be true for $\mathbb{Z}/n\mathbb{Z}$.

Consider $\mathbb{Z}_{p^i}$ where p^i is a power of a prime p. If $i = 1$, then $\mathbb{Z}_p$ is a field. There are no proper nonzero submodules of $\mathbb{Z}_p$, thus $\mathbb{Z}_p$ is uniform.

The submodules of $\mathbb{Z}_{p^i}$ for $i > 1$ are generated by powers of p^i.

$\langle p^i \rangle \subset \langle p^{i-1} \rangle \subset \langle p^{i-2} \rangle \subset \cdots \subset \langle p^2 \rangle \subset \langle p^1 \rangle$. Let $m, n \in \mathbb{Z}$ such that $1 \leq m \leq n \leq i$ then $\langle p^n \rangle \cap \langle p^m \rangle = \langle p^n \rangle \neq 0$. Thus any two nonzero submodules have a nonzero intersection. Therefore $\mathbb{Z}_{p^i}$ is uniform.

Proof of converse: Case 1: By Proposition 4.7 $\mathbb{Z}$ is a uniform module, therefore a cyclic

$\mathbb{Z}$ module, $\mathbb{Z}/n\mathbb{Z}$, is uniform when $n = 0$. Case 2 will use proof by contradiction. Let $\mathbb{Z}_n$ be uniform where $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_m^{e_m}$, p_i are all distinct, $e_i > 0$ for $i = 1, \cdots, m$, and $m \geq 2$ where $m \in \mathbb{N}$. Let $r = p_j^{e_j}$ and $s = n/p_j^{e_j}$. $\langle r \rangle$ and $\langle s \rangle$ are submodules of $\mathbb{Z}_n$ and $\langle r \rangle \cap \langle s \rangle = 0$. Thus $\mathbb{Z}_n$ is not uniform. This is a contradiction, thus $m = 1$. Therefore by case 1 and 2 if a cyclic $\mathbb{Z}$ module, $\mathbb{Z}/n\mathbb{Z}$ is uniform then n is 0 or a power p^i of a prime where i is an integer and $i > 0$. □

From this proposition we know $\mathbb{Z}_p$ is uniform. $\mathbb{Z}_{p^n}$ is a uniform module with a uniform submodule isomorphic to $\mathbb{Z}_p$. Therefore $\mathbb{Z}_{p^n} \sim \mathbb{Z}_p$ hence $\left[\mathbb{Z}_{p^n}\right] = \left[\mathbb{Z}_p\right]$ for $n \in \mathbb{N}$. Since uniform implies primary, $\mathbb{Z}_{p^n}$ and $\mathbb{Z}_p$ are primary.

Proposition 4.10: Any $\mathbb{Z}$ module (i.e., any Abelian group as a module over the ring of integers), contains enough uniforms.

Proof: Let $0 \neq M$ be a $\mathbb{Z}$ module. Let H be a nonzero submodule of M and $0 \neq h \in H$. $\mathbb{Z} \cdot h$ is a cyclic submodule of H. By Proposition 3.4 $\mathbb{Z} \cdot h \cong \mathbb{Z}/I$ where $I = \{z \in \mathbb{Z} \mid z \cdot h = 0\}$. $I \neq \varnothing$ since $0 \in I$. If $I = 0$ then $\mathbb{Z} \cdot h \cong \mathbb{Z}$. By Proposition 4.9 $\mathbb{Z} \cdot h$ is uniform. Therefore M has enough uniforms in this case. If $I \neq 0$ then there exists a least $n \in \mathbb{Z}^+$ such that $\underbrace{h + h + \cdots + h}_{n\ times} = 0$. Then $\mathbb{Z} \cdot h \cong \mathbb{Z}/n\mathbb{Z}$. By The Fundamental Theorem of Finitely Generated Modules over a *PID* $\mathbb{Z} \cdot h \cong \mathbb{Z}_{(p_1)^{r_1}} \oplus \mathbb{Z}_{(p_2)^{r_2}} \oplus \cdots \oplus \mathbb{Z}_{(p_n)^{r_n}}$. $\mathbb{Z}_{(p_1)^{r_1}} \oplus 0 \oplus \cdots \oplus 0 \cong \mathbb{Z}_{(p_1)^{r_1}}$ is a submodule of $\mathbb{Z} \cdot h$

so by Proposition 4.9 $\mathbb{Z}\cdot h$ contains a uniform submodule. Thus M contains enough uniforms.

Proposition 4.11: Every nonzero module over a ring R contains enough uniforms if and only if every nonzero cyclic module R/I contains a uniform submodule.

Proof: If every nonzero module over a ring R contains enough uniforms then every nonzero cyclic module contains enough uniforms and hence has a uniform submodule. Proof of the converse, let M be a nonzero module over a ring R. Let K be a nonzero submodule of M and $0 \neq x \in K$. $R\cdot x$ is a cyclic submodule of K. By Proposition 3.4 $R\cdot x \cong R/I$ where $I = \{r \in R \mid r\cdot x = 0\}$. By assumption R/I contains a uniform submodule. Therefore M contains enough uniforms. □

Osofsky Notation: Let the nonzero module M contain enough uniforms. For each class $[U]$ of uniforms, set

$$\mathscr{F}_{[U],M} = \{K \subseteq M \mid K \text{ a submodule which contains no submodule in } [U]\}.$$

Thus writing $K \in \mathscr{F}_{[U],M}$ is a short way of saying that K is a submodule of M which contains no uniform submodule subisomorphic to U. $\mathscr{F}_{[U],M}$ is never empty as the zero submodule is always in it.

Example 4.12: For each class $[U]$ of uniforms find $\mathscr{F}_{[U],M}$ where $M = R = \mathbb{Z}$. The submodules of $\mathbb{Z}$ are of the form $n\mathbb{Z}$, $n \geq 0$ and since $\mathbb{Z} \cong n\mathbb{Z}$ when $n \neq 0$ we have $\mathscr{F}_{[\mathbb{Z}],\mathbb{Z}} = \{0\}$. By Proposition 4.9 $\mathbb{Z}_{p^n}$ is uniform where $n \geq 1$. We have already observed that for any prime p_i and $n > 0$ $\left[\mathbb{Z}_{p_i^n}\right] = \left[\mathbb{Z}_{p_i}\right]$. Let $[U_i] = \left[\mathbb{Z}_{p_i}\right]$, then

$\mathcal{F}_{[\mathbb{Z}_{p_i}],\mathbb{Z}} = \{ n\mathbb{Z} \mid n \geq 0 \}$.

We have accumulated some examples of uniform modules. A commutative domain is uniform as a module over itself. $\mathbb{Z}$ and $\mathbb{Z}_p$, where p is prime, are uniform $\mathbb{Z}$ modules and in addition $[\mathbb{Z}_p] = [\mathbb{Z}_{p^n}]$. A nonzero submodule of a uniform module is uniform, and every uniform module is primary. But how can we find these uniforms in a module with enough uniforms? How do they compare with prime ideals? If P is a prime ideal of R, then R/P is a domain and hence by Proposition 4.7 a uniform R/P module. Since multiplication by an element $r \in R$ gives the same result as multiplication by $r + P \in R/P$, R/P is also a uniform R module. We will make one more observation about prime ideals before we relate uniforms to prime ideals.

Lemma 4.13: Every nonzero cyclic submodule of R/P, for P a prime ideal of R, is isomorphic to R/P.

Proof: Let $x \neq 0$, $x \in R/P$ and $R \cdot x$ is a nonzero cyclic submodule of R/P. By Lemma 3.9, P is the annihilator of any nonzero x in R/P, thus P is the annihilator of every element of $R \cdot x$. By Proposition 3.4 $R \cdot x \cong R/P$ where $P = Ann(x)$. Therefore every nonzero cyclic submodule of R/P, for P a prime ideal of R, is isomorphic to R/P.

Lemma 4.14: Let U be a uniform module over a commutative Noetherian ring R. Then U contains a submodule isomorphic to R/P for precisely one prime ideal P.

Proof: R is Noetherian so by Theorem 2.13 R has maximal element condition. Let $X = \{(0:x) \mid 0 \neq x \in U\}$ be a set of annihilator ideals of R. By Lemma 3.7, a maximal element of X is prime. If $P = (0{:}x_0)$ is such a maximal annihilator, then U contains the submodule $R \cdot x_0$ which is isomorphic to R/P. By lemma 4.13 every nonzero cyclic submodule of R/P, for P a prime ideal of R, is isomorphic to R/P. If I is any ideal distinct from P then there exists an $x \in I$ such that $x \notin P$ or there exists an $x \in P$ such that $x \notin I$. If $x \in I$ and $x \notin P$ then $r \cdot x = 0$ in R/I for all $r \in R$, but $r \cdot x \neq 0$ in R/P if $r \notin P$. If $x \in P$ and $x \notin I$ then $r \cdot x = 0$ in R/P for all $r \in R$, but $1 \cdot x \neq 0$ in R/I. In either case R/I is not R isomorphic to R/P. Hence if U and V are uniform R modules containing submodules isomorphic to R/P and R/Q respectively where P and Q are distinct primes, then $[R/P] = [U] \neq [V] = [R/Q]$. □

Lemma 4.14 shows for each uniform U_i there exists a prime P_i so $[U_i] = [R/P_i]$. Notice in the Osofsky notation each uniform module of R must be considered to calculate $\mathscr{F}_{[U],M}$. By using Lemma 4.15 below we can concentrate on the associated primes of M.

Lemma 4.15: Let M be an R module. Let $S = \{P \mid Ann(m) = P \text{ for some } m \in M \text{ and } P \text{ is a prime}\}$. A prime P is not an element of S if and only if $\mathscr{F}_{[R/P],\,M} = \{K \mid K \subseteq M\}$.

Proof: Let M be an R module, P be a prime ideal of R, and $\mathscr{F}_{[R/P],\,M} = \{K \mid K \subseteq M\}$. Let K be a submodule of M. $K \in \mathscr{F}_{[R/P],\,M}$, thus no uniform submodule of K is isomorphic to R/P. Let $m \in K$ then by Proposition 3.4 $R \cdot m \cong R/I$, where

$Ann(m) = I$. Since $R \cdot m \not\cong R/P$ then $[R/P] \neq [R/I]$ thus $Ann(m) \neq P$. Since K was arbitrary then for all $m \in M$, $Ann(m) \neq P$. Therefore $P \notin S$.

Conversely, let M be an R module and P a prime ideal of R where P is not an element of $S = \{ P \mid Ann(m) = P \text{ for some } m \in M \}$. Let K be a submodule of M and $m \in K$. By Proposition 3.4. $R \cdot m \cong R/I$, where $Ann(m) = I$. Since $P \notin S$ then for any $m \in M$, $Ann(m) \neq P$. Thus $R \cdot m \not\cong R/P$. Since m was arbitrary, K has no uniform submodule isomorphic to R/P, thus $K \in \mathscr{F}_{[R/P],\,M}$. Since K was an arbitrary submodule of M $\mathscr{F}_{[R/P],\,M} = \{ K \mid K \subseteq M \}$.

Example 4.16: For each class $[U]$ of uniforms find $\mathscr{F}_{[U],\,M}$ where

$M = R = k[x,y] / \langle xy, x^2 \rangle$, and k is a field of characteristic 0.

Note that every element of M has a unique representation of $cx + t(y)$ where $c \in k$ and $t(y) \in k[y]$. By abuse of notation we use x, y for cosets of x and y. Find the set S from Lemma 4.15. $Ann(x) = \langle x, y \rangle$ and $R/\langle x, y \rangle$ is isomorphic to a field, therefore $\langle x, y \rangle$ is prime and $\langle x, y \rangle \in S$. $Ann(y) = \langle x \rangle$ and $R/\langle x \rangle$ is isomorphic to a domain, therefore $\langle x \rangle$ is prime and $\langle x \rangle \in S$. These are the only prime annihilators, thus $S = \{ \langle x, y \rangle, \langle x \rangle \}$. If P is a prime ideal and $P \notin S$, then $P = \langle x, q(y) \rangle$ where $q(y)$ is an irreducible polynomial in $k[y]$ and $q(y) \neq y$. To see this note $x \in P$ since $x^2 = 0$. If $P \neq \langle x \rangle$, then there exists a $q(y) \in P$ and therefore there exists an irreducible $q(y) \in P$

and $q(y) \neq 0$. Since $P = \langle x, q(y) \rangle$ is maximal these are the only such P. Thus the prime ideals of R are $\langle x \rangle$, $\langle x, y \rangle$, and $\{\langle x, q(y) \rangle\}$ where $q(y)$ is an irreducible polynomial in $k[y]$. By Lemma 4.15 $\mathscr{F}_{[\langle x, q(y) \rangle],\, M} = \{K \mid K \subseteq M \text{ when } q(y) \neq y\}$.

Let $[U_1] = [R/\langle x \rangle]$. $\mathscr{F}_{[R/\langle x \rangle],\, M}$ contains the submodules of M such that no submodule will have an element whose annihilator is $\langle x \rangle$. $\langle cx + y \cdot p(y) \rangle$ has annihilator $\langle x \rangle$ where $p(y) \neq 0$ and $c \in k$.

$\mathscr{F}_{[R/\langle x \rangle],\, M} = \{K \mid K \cap \langle cx + y \cdot p(y) \rangle = 0, \text{ for all } p(y) \neq 0 \text{ and } c \in k\}$. Thus

$\mathscr{F}_{[R/\langle x \rangle],\, M} = \{0, \langle x \rangle\}$

Let $[U_2] = [R/\langle x, y \rangle]$. $\mathscr{F}_{[R/\langle x, y \rangle],\, M}$ contains the submodules of M such that no submodule will have an element whose annihilator is $\langle x, y \rangle$. $\langle x \rangle$ contains all elements annihilated by $\langle x, y \rangle$. $\mathscr{F}_{[R/\langle x, y \rangle],\, M} = \{K \mid K \cap \langle x \rangle = 0\}$. $K \subseteq \langle x, y \rangle$ and it is not hard to check that if $0 \neq w \in \langle x, y \rangle$ that $Ann(w) = \langle x \rangle$ or $Ann(w) = \langle x, y \rangle$. $Ann(w) = \langle x \rangle$ if and only if $w = cx + y \cdot p(y)$ with $p(y) \neq 0$ and $Ann(w) = \langle x, y \rangle$ if and only if $w = cx \neq 0$. Thus $K \in \mathscr{F}_{[R/\langle x, y \rangle],\, M}$ if and only if K's nonzero elements are of the form $cx + y \cdot p(y)$ for any $c \in k$ and $p(y) \neq 0$. Thus one K submodule is $\langle cx + y \cdot p(y) \rangle$ for any $c \in k$ and $p(y) \neq 0$. $R/\langle x \rangle \cong \langle cx + y \cdot p(y) \rangle$ for any $c \in k$ and $p(y) \neq 0$ thus by Lemma 4.13 every cyclic submodule of $\langle cx + y \cdot p(y) \rangle \in \mathscr{F}_{[R/\langle x, y \rangle],\, M}$. However, if $K \subseteq M$ requires at least two generators of the form $cx+y\cdot p(y)$ with $p(y)\neq 0$ which are not such that one is a scalar multiple of the other, it can be argued that $x\in K$ so $K\notin\mathscr{F}_{[R/\langle x,y\rangle],\,M}$. The argument is tedious so is omitted. Therefore

$\mathscr{F}_{[R/\langle x,y\rangle],\,M}=\left\{0,\left\{\langle cx+y\cdot p(y)\rangle\right\}\text{ where } c\in k \text{ and } p(y)\neq 0\right\}$.

Proposition 4.17: Let M contain enough uniforms. Then for any uniform module U and any $L\in\mathscr{F}_{[U],\,M}$, there is a maximal element of $\mathscr{F}_{[U],\,M}$ which contains L (and which possibly might be 0 or M).

Proof: Let U be a uniform module of M. Let $L\in\mathscr{F}_{[U],\,M}$ and let

$\mathscr{F}=\left\{K_i\subseteq M \,\middle|\, K_i\in\mathscr{F}_{[U],\,M} \text{ and } L\subseteq K_i\right\}$. $L\in\mathscr{F}$ thus $\mathscr{F}\neq\varnothing$. $\mathscr{F}$ is partially ordered by inclusion. Take a chain $\mathscr{C}\subseteq\mathscr{F}$, $\mathscr{C}$ is ordered by inclusion. Let $K=\bigcup_{K_i\in\mathscr{C}}K_i$. Show $K\in\mathscr{F}$. K is a submodule of M was proved in Proposition 3.16 part (b). Suppose $K\notin\mathscr{F}$, then K has a uniform submodule N such $[N]=[U]$. Let $0\neq x\in N\subseteq K$ then $R\cdot x$ is a uniform submodule of N subisomorphic to $[U]$. $x\in K$ so there exists an n such that $x\in\bigcup_{m=1}^{n}K_{i_m}=K_{i_n}$ thus $R\cdot x\subseteq K_{i_n}\in\mathscr{F}_{[U],\,M}$ and this contradicts the definition of $\mathscr{F}_{[U],\,M}$. Therefore $K\in\mathscr{F}$. Clearly K is an upper bound for $\mathscr{C}$. Since each chain has an upper bound, by Zorn's Lemma $\mathscr{F}_{[U],\,M}$ has a maximal element.

Example 4.18: Find a maximal element for each $\mathscr{F}_{[U],\,M}$ in examples 4.12 and 4.16. In Example 4.12 $\mathscr{F}_{[\mathbb{Z}],\,\mathbb{Z}}=\{0\}$ thus the maximal element of $\mathscr{F}_{[\mathbb{Z}],\,\mathbb{Z}}$ is 0. For every prime p_i,

$\mathscr{F}_{[\mathbb{Z}_{p_i}],\mathbb{Z}} = \{ n\mathbb{Z} | n \geq 0 \}$ and for every p_i the maximal element of $\mathscr{F}_{[\mathbb{Z}_{p_i}],\mathbb{Z}}$ is $\mathbb{Z}$. From

Example 4.16 $M = R = {k[x,y]}/{\langle xy, x^2 \rangle}$, and k is a field of characteristic 0. By abuse of notation carried through from Example 4.16, the maximal element of $\mathscr{F}_{[R/\langle x \rangle],M} = \{ 0, \langle x \rangle \}$ is clearly the submodule generated by $\langle x \rangle$. In $\mathscr{F}_{[R/\langle x,y \rangle],M} = \{ 0, \{ \langle cx + y \cdot p(y) \rangle \text{ for all } p(y) \neq 0 \text{ and } c \in k \} \}$ we need to determine a maximal element. $\langle x+y \rangle \in \mathscr{F}_{[R/\langle x,y \rangle],M}$ thus by Proposition 4.17 there is a maximal element of $\mathscr{F}_{[R/\langle x,y \rangle],M}$ which contains $\langle x+y \rangle$. Thus $\langle x+y \rangle \subseteq \langle cx + y \cdot p(y) \rangle$. $y + x = r(cx + y \cdot p(y)) = (dx + q(y))(cx + y \cdot p(y)) = cq_0 x + y \cdot p(y) q(y)$ where q_0 equals the constant term of $q(y)$, and there is a $p(y) \neq 0$ such that $y \cdot p(y) q(y)$ has degree one. This implies the degree of $p(y)$ and $q(y)$ must be zero. Thus $cq_0 x + y \cdot p(y) q(y) = cq_0 x + c_1 y$ where $c_1 \in k$. $(c_1)^{-1} \in k$ and therefore $(c_1)^{-1}(cq_0 x + c_1 y) = c'x + y$ where $(c_1)^{-1}(cq_0) = c'$. Thus $\langle x+y \rangle \subset \langle c'x + y \rangle$. If $c' = 0$ this implies $\langle x+y \rangle \subseteq \langle y \rangle$. $x + y \in \langle x+y \rangle$ but $x + y \notin \langle y \rangle$. Thus $\langle x+y \rangle \not\subseteq \langle y \rangle$. If $c' \neq 0$ then $\langle x+y \rangle \subseteq \langle c'x + y \rangle$. $x + y \in \langle x+y \rangle$ thus $x + y \in \langle c'x + y \rangle$. Thus $c' = 1$, and therefore $\langle x+y \rangle$ is a maximal of $\mathscr{F}_{[R/\langle x,y \rangle],M}$.

$\langle y \rangle \in \mathscr{F}_{[R/\langle x,y \rangle],M}$, thus by Proposition 4.17 there is a maximal element of $\mathscr{F}_{[R/\langle x,y \rangle],M}$ which contains $\langle y \rangle$. If $\langle y \rangle$ is not the maximal element then

$\langle y\rangle \subsetneq \langle cx+y\cdot p(y)\rangle$. By the argument above $\langle y\rangle \subset \langle y+c'x\rangle$. $y\in\langle y\rangle$ thus $y\in\langle y+c'x\rangle$ and this occurs only when $c'=0$. Thus $\langle y\rangle$ is the maximal element containing $\langle y\rangle$ in $\mathscr{F}_{[R/\langle x,y\rangle],M}$. In $\mathscr{F}_{[\langle x,q(y)\rangle],M}$ the maximal element containing an irreducible $q(y)$ in $k[y]$ is M by Theorem 4.15.

We have enough preliminaries to state and prove Osofsky's Theorem 4.19. Proposition 4.17 shows that the module $N_{[U]}$ in Theorem 4.19 must exist. Theorem 4.19 part (b) justifies calling the set of all $N_{[U]}$ which are distinct from M the primary components of 0, and their intersection a primary decomposition of 0 in M.

Theorem 4.19[Osofsky]: Let the nonzero module M contain enough uniforms. For each class $[U]$ of uniforms, let $N_{[U]}$ be any maximal element of $\mathscr{F}_{[U],M}$. Then

a) $\bigcap_{[U]} N_{[U]} = 0$

b) If $0 \neq M/N_{[U]}$ then $M/N_{[U]}$ is primary, that is, it contains enough uniforms and any uniform submodule of $M/N_{[U]}$ is in $[U]$.

c) $\mathscr{F}_{[U],M}$ has more than one maximal element $\Leftrightarrow$ there is a $K \in \mathscr{F}_{[U],M}$ and a nonzero homomorphism φ from K to $V \subseteq M$ where V is a uniform module in $[U]$.

Proof:

(a) Suppose there exists an $0 \neq x \in \bigcap_{[U]} N_{[U]}$. $x \in M$ and $R\cdot x$ is a submodule of M which contains enough uniforms. By definition of enough uniforms $R\cdot x$ contains a uniform submodule V. There exists $0 \neq \langle r \cdot x \rangle \subseteq V$. By definition of $\mathscr{F}_{[V],M}$, $N_{[V]}$ cannot have a nonzero submodule isomorphic to a submodule of V. Thus $V \cap N_{[V]} = 0$ and $x \notin N_{[V]}$ for if $x \in N_{[V]}$ then $r \cdot x \in N_{[V]} \Rightarrow V \cap N_{[V]} \neq 0$, a contradiction. Therefore $x = 0$.

(b) Let K be any nonzero submodule of $M/N_{[U]}$ and W the largest submodule of M mapping onto K modulo $N_{[U]}$. Since W properly contains $N_{[U]}$, by maximality of $N_{[U]}$ in $\mathscr{F}_{[U],M}$, W must contain a uniform submodule V subisomorphic to U. We draw a picture of the situation in Figure 1 and then give the argument.

$$\begin{array}{l} V \\ |\cap \\ W \subseteq M \\ \downarrow^{\nu} \quad \downarrow^{\nu} \\ 0 \neq K \subseteq M/N_{[U]} \end{array}$$

Figure 1

Look at the module $V \cap N_{[U]}$. If it is not zero, then it is a uniform module contained in $N_{[U]}$ and it is subisomorphic to V which is in $[U]$. By definition of $N_{[U]}$, no such nonzero module exists, so $V \cap N_{[U]} = 0$. Restrict the natural quotient map $\nu : M \to M/N_{[U]}$ to V (i.e. look at the left column of Figure 1). This restriction has kernel $V \cap N_{[U]} = 0$ and so is one-to-one. Then K contains a submodule $(V)_\nu$ isomorphic to $V \in [U]$. Thus a submodule K of $M/N_{[U]}$ contains $(V)_\nu$ a uniform submodule and therefore $M/N_{[U]}$ has enough uniforms. Since K was an arbitrary nonzero submodule of $M/N_{[U]}$ and we argued that the uniform in question $(V)_{\nu}$ belonged to $[U]$, $M/N_{[U]}$ is primary.

For $\Rightarrow$ in (c), assume that $K_{[U]}$and $L_{[U]}$ are two distinct maximal elements of $\mathscr{F}_{[U],M}$. Without loss of generality let $0 \neq x \in L_{[U]}$ and $x \notin K_{[U]}$. Since $L_{[U]}$ is not contained in $K_{[U]}$ the natural map ν from M to $M/K_{[U]}$ induces a nonzero map on $L_{[U]}$ where $\nu(x) \neq 0$. We again draw a picture to aid in following the argument.

$$\begin{array}{ccccc} H & \subseteq & L_{[U]} & \subseteq & M \\ \downarrow^{\nu} & & \downarrow^{\nu} & \swarrow & \\ V & \subseteq & M/K_{[U]} & & \end{array}$$

Figure 2

$0 \neq M/K_{[U]}$ so by part (b) $M/K_{[U]}$ is primary, with uniforms in $[U]$. Thus the homomorphic image of ν restricted to $L_{[U]}$ contains enough uniforms, and all of its uniform submodules are in $[U]$. Restrict ν even further to the preimage H in $L_{[U]}$ of a uniform submodule $V \subseteq \left(L_{[U]}\right)\nu$ (i.e. look at the left-hand column of Figure 2). Then ν restricted to H is a nonzero map to V a uniform module in $[U]$.

For the $\Leftarrow$ direction of (c) assume there is a nonzero φ from a submodule $K \in \mathscr{F}_{[U],M}$ to a submodule $V \subseteq M$, $V \in [U]$. Pick $x \in K$ with $0 \neq (x)\varphi$. For the moment we assume that $r \cdot x = 0 \Leftrightarrow r \cdot (x - (x)\varphi) = 0$. By a basic homomorphism theorem and our assumption, both $R \cdot x$ and $R \cdot (x - (x)\varphi)$ are isomorphic to the same quotient module $R/\{r \in R \mid r \cdot x = 0\}$. Since $K_1 = R \cdot x$ is in $\mathscr{F}_{[U],M}$, so is the isomorphic module $K_2 = R\cdot(x-(x)\varphi)$. However, the sum $K_1 + K_2$ contains the module $R\cdot(x)\varphi \in [U]$, so no submodule $L \in \mathscr{F}_{[U],M}$ contains both K_1 and K_2. By Proposition 4.17, each K_1 is contained in a maximal element of $\mathscr{F}_{[U],M}$ so there must be more than one maximal element in $\mathscr{F}_{[U],M}$.

Now we prove our assumption that $r\cdot x = 0 \Leftrightarrow r\cdot(x-(x)\varphi) = 0$. Suppose $r\cdot(x-(x)\varphi)=0$. Since $R\cdot x \in \mathscr{F}_{[U],M}$ and $R\cdot(x)\varphi \in [U]$, $R\cdot x \cap R\cdot(x)\varphi = 0$. Then $0 = r\cdot(x-(x)\varphi)$ implies $0 = r\cdot x - r\cdot(x)\varphi$ by the distributive law for scalar multiplication. Bringing $r\cdot(x)\varphi$ over to the other side shows that $r\cdot(x)\varphi = r\cdot x \in R\cdot x \cap R\cdot(x)\varphi = 0$, so any r with $r\cdot(x-(x)\varphi) = 0$ has $r\cdot x = 0$.

Conversely, if $0 = r\cdot x$, then $0 = (r\cdot x)\varphi = r((x)\varphi)$ so $0 = r\cdot x - r\cdot(x)\varphi = r\cdot(x-(x)\varphi)$. □

Example 4.20: For each class $[U]$ of uniforms, let $N_{[U]}$ be any maximal element of $\mathscr{F}_{[U],M}$ and find $\bigcap_{[U]} N_{[U]} = 0$ for $M = R = \mathbb{Z}$ and for $M = R = k[x,y]/\langle xy, x^2\rangle$.

By Proposition 4.7 we know $\mathbb{Z}$ is uniform and therefore its decomposition is not interesting. But from example 4.18 we find

$$0 = \bigcap_{[U]} N_{[U]} = N_{[\mathbb{Z}]} \bigcap_{p=\text{prime}} N_{[\mathbb{Z}_p]} = 0 \cap \mathbb{Z} \cap \mathbb{Z} \cap \cdots.$$

From example 4.18 where $M = R = k[x,y]/\langle xy, x^2\rangle$ we have

$0=\bigcap_{[U]}N_{[U]}=\langle x\rangle\cap\langle x+y\rangle\cap M\cap M\cap\cdots$. Since $\mathscr{F}_{[R/\langle x,y\rangle],\,M}$ has more than one maximal element, $0=\bigcap_{[U]}N_{[U]}=\langle x\rangle\cap\langle y\rangle\cap M\cap M\cap\cdots$ is an alternative decomposition of M.

If $R=F$ is a field, there are no proper nonzero ideals. Thus if $M=F$ there is only one nonzero uniform F, hence $N_{[F]}=\{0\}$. This is not an interesting case. But as stated before the theorems for modules apply to Abelian groups. Consider any Abelian group as a module over the ring of integers. Proposition 4.9 proves that the only cyclic uniform modules over $\mathbb{Z}$ are isomorphic either to $\mathbb{Z}$ or to $\mathbb{Z}/p^i\mathbb{Z}$ for some prime p. Osofsky's Theorem decomposes any module containing enough uniforms. Proposition 4.21 specializes the Osofsky Theorem by limiting the module to a $\mathbb{Z}$ module, that is any Abelian group over $\mathbb{Z}$. Proposition 4.21 is a generalization of the Fundamental Theorem of Finitely Generated Modules over a *PID*.

Proposition 4.21: Let the module M be an Abelian group over the ring $\mathbb{Z}$. Let $\tau(M)$ be the set of elements of M of finite order.

a) For each prime p in $\mathbb{Z}$ there exists a submodule $N_p\subseteq M$ such that every element of M/N_p is of order a power of p. Furthermore,

$$\left(\bigcap_{p\ prime} N_p\right)\cap\tau(M)=0$$

b) If $\tau(M)\neq M$ then each N_p contains a submodule K isomorphic to $\mathbb{Z}$. If in addition $M/N_p\neq 0$, then there is a nonzero map from K to a uniform submodule of M

isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

c) If $\tau(M) \neq M$ then for any p with $N_p \neq M$, N_p is not a unique submodule of M.

d) If $\tau(M) = M$ then all the N_p are unique.

Proof (a):

Let M be a $\mathbb{Z}$ module. By Proposition 4.10 M contains enough uniforms. Let $0 \neq x \in M$, $\mathbb{Z} \cdot x$ is a cyclic $\mathbb{Z}$ module which contains a uniform module U. By Proposition 4.9 $[U] \sim [\mathbb{Z}_p]$ where p is a prime in $\mathbb{Z}$ or $[U] \sim [\mathbb{Z}]$. By Proposition 4.17 there is a maximal element of $\mathscr{F}_{[\mathbb{Z}_p],M}$ for every prime p. Let N_p be a maximal element of $\mathscr{F}_{[\mathbb{Z}_p],M}$. Let $\tau(M)$ be the set of elements of M of finite order. If M contains no nonzero elements of finite order then

$\left(\bigcap_{p\text{ prime}} N_p\right) \cap \tau(M) = \left(\bigcap_{p\text{ prime}} N_p\right) \cap 0 = 0$. If $0 \neq x \in \tau(M)$ and $x \in \bigcap_{p\text{ prime}} N_p$ then $x \in N_p$ for every prime p in $\mathbb{Z}$. $\mathbb{Z} \cdot x$ is a finitely generated $\mathbb{Z}$ module thus by The Fundamental Theorem of Finitely Generated Modules over a *PID* $\mathbb{Z} \cdot x \cong \mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$ where the p_i $i = 1, \cdots, k$ may not all be distinct primes and the $n_i \geq 1$. Therefore $\mathbb{Z} \cdot x \notin \mathscr{F}_{[\mathbb{Z}_{pi}],M}$ so $x \notin N_{p_i}$ for $i = 1, \cdots, k$. This implies $x \notin \bigcap_{p\text{ prime}} N_p$.

Thus $\left(\bigcap_{p\text{ prime}} N_p\right) \cap \tau(M) = 0$.

Show that every element of M/N_p is of order a power of p a prime.

Let $0 \neq x \in M/N_p$. $\mathbb{Z} \cdot x$ is a cyclic submodule of M/N_p. By Proposition 4.10 $\mathbb{Z} \cdot x$ has enough uniforms. Therefore $\mathbb{Z}\cdot x$ contains a uniform submodule which is contained in M/N_p. By Theorem 4.19 part (b) any uniform submodule of M/N_p is in $[\mathbb{Z}_p]$. Therefore any uniform submodule of $\mathbb{Z}\cdot x$ is in $[\mathbb{Z}_p]$ where $x \in M/N_p$. Hence every nonzero element of $\mathbb{Z}\cdot x$ is of order a power of p and hence every nonzero element of M/N_p is of order a power of p. If $0 = x \in M/N_p$ then $p \mid x$ and $x = 0$ in $\mathbb{Z}_p$ and $|x| = |0| = 1 = p^0$. Thus every element of M/N_p is of order a power of p.

Proof (b):

M is a $\mathbb{Z}$ module and $\tau(M) \neq M$. Let $x \in M$ such that $x \notin \tau(M)$. $\mathbb{Z}\cdot x$ is a cyclic module isomorphic to $\mathbb{Z}/I$ where $I = \{z \in \mathbb{Z} \mid x \cdot z = 0\}$. Since $x \notin \tau(M)$ this implies $I = 0$. Thus $\mathbb{Z}\cdot x \cong \mathbb{Z}/0 \cong \mathbb{Z}$. $\mathbb{Z}_p \not\cong \mathbb{Z}$ for any prime p thus for any $\mathscr{F}_{[\mathbb{Z}_p],M}$, the associated N_p, will contain a submodule K isomorphic to $\mathbb{Z}$. ($N_p \not\subseteq \tau(M)$ since N_p is maximal.) If in addition $M/N_{p_i} \neq 0$ then $M \notin \mathscr{F}_{[\mathbb{Z}_{p_i}],M}$ and by Lemma 4.15 M contains a submodule L isomorphic to $\mathbb{Z}_{p_i}$. $\mathbb{Z}_{p_i}$ is uniform by Proposition 4.9. Thus there exists a nonzero map φ such that $\varphi : K \to L$, where K is isomorphic to $\mathbb{Z}$ and L is isomorphic to $\mathbb{Z}_{p_i}$.

Proof of (c) by contradiction:

Suppose N_p is unique. For any prime p in $\mathbb{Z}$ if N_p is the maximal element of $\mathscr{F}_{[\mathbb{Z}_p],M}$, then by Theorem 4.19 part (c) for any $K \in \mathscr{F}_{[\mathbb{Z}_p],M}$ the only homomorphism from K to

$V \subseteq M$ where V is a uniform module in $\left[\mathbb{Z}_p\right]$ is the zero homomorphism. By assumption if $\tau(M) \neq M$ then by part (b) above each N_p, which is an element of $\mathcal{F}_{[\mathbb{Z}_p],M}$ contains a submodule L isomorphic to $\mathbb{Z}$. Thus there exists a nonzero map φ such that $\varphi : L \to \mathbb{Z}_p$. $L \subset N_p \in \mathcal{F}_{[\mathbb{Z}_p],M}$ thus $L \in \mathcal{F}_{[\mathbb{Z}_p],M}$. φ is a nonzero map from a submodule of $\mathcal{F}_{[\mathbb{Z}_p],M}$ to $\mathbb{Z}_p$, and this contradicts part (c) of Theorem 4.19. Therefore N_p is not a unique submodule.

Proof (d) by contradiction:

Assume $\tau(M) = M$ and the N_p are not unique. Then some $\mathcal{F}_{[\mathbb{Z}_p],M}$ has more than one maximal element. By Theorem 4.19 (c) there is a $K \in \mathcal{F}_{[\mathbb{Z}_p],M}$ and a nonzero homomorphism ϕ such that $\phi : K \to \mathbb{Z}_p$. Let $x \in K$ such that $(x)\phi \neq 0$. x has finite order, and $p \,\big|\, |\langle x \rangle|$ so $\langle x \rangle$ has a submodule contained in K isomorphic to $\mathbb{Z}_p$. By definition of $\mathcal{F}_{[\mathbb{Z}_p],M}$, K cannot have a submodule isomorphic to $\mathbb{Z}_p$, thus $K \notin \mathcal{F}_{[\mathbb{Z}_p],M}$ is a contradiction. Therefore all the N_p are unique.

Example 4.22: Let $M = \mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_8 \oplus \cdots$

a) Find N_p described in Proposition 4.21 and show that every element of M/N_p is of order a power of p.

One set of choices is:

$N_2 = \mathbb{Z} \oplus 0 \oplus \mathbb{Z}_3 \oplus 0 \oplus \mathbb{Z}_3 \oplus 0 \oplus \cdots$

$N_3 = \mathbb{Z} \oplus \mathbb{Z}_2 \oplus 0 \oplus \mathbb{Z}_4 \oplus 0 \oplus \mathbb{Z}_8 \oplus \cdots$

$N_{p \neq 2,3} = \mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_8 \oplus \cdots$

$$\left(\bigcap_{p \text{ prime}} N_p \right) \cap \tau(M) = 0$$

Every element of

$$\frac{M}{N_2} = \frac{\mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_8 \oplus \cdots}{\mathbb{Z} \oplus 0 \oplus \mathbb{Z}_3 \oplus 0 \oplus \mathbb{Z}_3 \oplus 0 \oplus \cdots} \cong 0 \oplus \mathbb{Z}_2 \oplus 0 \oplus \mathbb{Z}_4 \oplus 0 \oplus \mathbb{Z}_8 \oplus \cdots$$

is of order a power of 2, and the other primes in M/N_p can easily be checked.

b) Since $\tau(M) \neq M$ then each N_p contains a submodule isomorphic to $\mathbb{Z}$ that is

$\mathbb{Z} \cong \mathbb{Z} \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus \cdots$

Let φ be the natural map where

$\varphi : \mathbb{Z} \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus \cdots \rightarrow \mathbb{Z}_2 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus \cdots$. φ

is a nonzero map from K to a submodule of M that is isomorphic to $\mathbb{Z}_2$.

c). Find N_p^* described in Proposition 4.21 such that $N_p^* \neq N_p$ from part (a) above.

$N_2^* = 8\mathbb{Z} \oplus 0 \oplus \mathbb{Z}_3 \oplus 0 \oplus \mathbb{Z}_3 \oplus 0 \oplus \cdots$

$N_3^* = 9\mathbb{Z} \oplus \mathbb{Z}_2 \oplus 0 \oplus \mathbb{Z}_4 \oplus 0 \oplus \mathbb{Z}_8 \oplus \cdots$

$N_{p_i \neq 2,3}^* = p_i^n \mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_8 \oplus \cdots \quad n \geq 1$

$$\frac{M}{N_2^*} = \frac{\mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_8 \oplus \cdots}{8\mathbb{Z} \oplus 0 \oplus \mathbb{Z}_3 \oplus 0 \oplus \mathbb{Z}_3 \oplus 0 \oplus \cdots} \cong \mathbb{Z}_8 \oplus \mathbb{Z}_2 \oplus 0 \oplus \mathbb{Z}_4 \oplus 0 \oplus \mathbb{Z}_8 \oplus \cdots$$

Thus N_p is not unique if $\tau(M) \neq M$

Example 4.23: Find the N_p when $\tau(M) = M$.

Let $M = \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_8 \oplus \cdots$

$N_2 = 0 \oplus \mathbb{Z}_3 \oplus 0 \oplus \mathbb{Z}_3 \oplus 0 \oplus \cdots$

$N_3 = \mathbb{Z}_2 \oplus 0 \oplus \mathbb{Z}_4 \oplus 0 \oplus \mathbb{Z}_8 \oplus \cdots$

$N_{p \neq 2,3} = \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_8 \oplus \cdots$

By part (d) Proposition 4.21 the N_p are unique.

In Proposition 4.21for each prime p the primary component N_p is not required to be the maximal element of $\mathscr{F}_{[U],\,M}$. By parts (b) and (c) of the proposition if $\tau(M) \neq M$ then for any p a prime with $N_p \neq M$, N_p contains a submodule K isomorphic to $\mathbb{Z}$. The nonzero map from K to $\mathbb{Z}_p$ and also the fact that $[\mathbb{Z}_p] = [\mathbb{Z}_{p^n}]$ allows alternative choices for each N_p. Thus the decomposition is unique only if $\tau(M) = M$.

5. How Does the Osofsky Theorem Relate to the Noether Lasker Theorem?

Theorem 4.19 [Osofsky]:

Let the nonzero module M contain enough uniforms. For each class $[U]$ of uniforms, let $N_{[U]}$ be any maximal element of $\mathscr{F}_{[U],M}$. Then

a) $\bigcap_{[U]} N_{[U]} = 0$

b) If $0 \neq M/N_{[U]}$ then $M/N_{[U]}$ is primary, that is, it contains enough uniforms and any uniform submodule of $M/N_{[U]}$ is in $[U]$.

c) $\mathscr{F}_{[U],M}$ has more than one maximal element $\Leftrightarrow$ there is a $K \in \mathscr{F}_{[U],M}$ and a nonzero homomorphism φ from K to $V \subseteq M$ where V is a uniform module in $[U]$.

Theorem 3.28 [Noether-Lasker]:

Let M be a finitely generated module over a commutative Noetherian ring R. Then there exists a finite set $\{\, N_i \mid 1 \leq i \leq l \}$ of submodules of M such that:

a) $\bigcap_{i=1}^{l} N_i = 0$ and $\bigcap_{i \neq i_0} N_i$ is not contained in N_{i_0} for all $1 \leq i_0 \leq l$.

b) Each quotient M/N_i is primary* for some prime P_i, and the P_i's are all distinct for $1 \leq i \leq l$.

c) The primary component N_i is unique $\Leftrightarrow$ P_i does not contain P_j for any $j \neq i$.

* primary refers to the traditional definition

There are a number of inconsistencies between these two theorems. The most noticeable distinction is the Osofsky Theorem is based on modules having enough uniforms, and there is no mention of Noetherian rings. Lemma 5.1 will resolve this issue by finding the relationship between containing enough uniforms and Noetherian rings.

Lemma 5.1: Let M be a Noetherian module or any module over a Noetherian ring. Then M has enough uniforms.

Proof: Let N be a nonzero Noetherian submodule of the module M over the Noetherian ring R. Let $0 \neq x \in N$. N a Noetherian submodule implies $R \cdot x$ is Noetherian and by Proposition 3.17, $R \cdot x$ has maximum condition.

Let $\mathscr{F} = \{K,$ a submodule of $R \cdot x \mid$ there is a submodule $L \neq 0$ of $R \cdot x$ with $L \cap K = 0\}$. $\mathscr{F}$ is not empty since $\{0\} \in \mathscr{F}$. Let K_0 be a maximal element of $\mathscr{F}$, and let U be a nonzero submodule of $R \cdot x$ with $U \cap K_0 = 0$. Assume U is not uniform. Then it contains nonzero submodules H and J such that $H \cap J = 0$. $H + J \subseteq U$, thus $(H + J) \cap K_0 = 0$. Suppose there exists $h \in H$, $j \in J$, and $k \in K_0$ such that $h = j + k \in H \cap (J + K_0)$. Then $h - j = k$ and since $(H + J) \cap K_0 = 0$ thus $h - j = k = 0$. Also $H \cap J = 0$, therefore $h = j = k = 0$. Therefore $H \cap (J + K_0) = 0$, so $J + K_0 \in \mathscr{F}$. $J \not\subseteq K_0$, since $J \neq 0$ and $J \cap K_0 = 0$. Therefore $J + K_0$ properly contains K_0, a contradiction since K_0 was maximal in $\mathscr{F}$. We conclude that U must be uniform. □

In Lemma 5.1 modules did not have to be finitely generated. The Osofsky Theorem is based on a module with enough uniforms, therefore it can decompose an infinitely generated module over a Noetherian ring. On the other hand the Noether Lasker Theorem is limited to a finitely generated module over a commutative Noetherian ring R. The Osofsky Theorem appears to be a generalization of the Noether Lasker

Theorem, but at this point it is not clear if the Osofsky Theorem will reduce to the Noether Lasker Theorem when applied to a finitely generated module.

Lemma 5.2 is an amended version of the Osofsky Theorem.

Lemma 5.2: Let M have enough uniforms, let $\{[U_i]\}$ represent classes of uniforms and let $\{\, N_i \subset M \,|\, 1 \le i \le k < \infty \}$ where k is fixed satisfy

a) $\bigcap_{i=1}^{k} N_i = 0$

b) M/N_i is primary with uniforms all in $[U_i]$.

c) $[U_i] \ne [U_j]$ if $i \ne j$

Then each $N_i \in \mathscr{F}_{[U_i],\,M}$. Moreover, if $\mathscr{F}_{[U_i],\,M}$ has only one maximal element which is distinct from M, then N_i is that maximal element.

Proof: Let U be a uniform submodule of M with $U \in [U_i]$. Then for $j \ne i$, U cannot embed in M/N_j by part (b). Thus $U \cap N_j \ne 0$ for $j \ne i$. Since $U \cap N_j$ is uniform, by finite induction $K_i = \bigcap_{j \ne i}(U \cap N_j) \ne 0$. But $K_i \cap (U \cap N_i)$ is equal to 0, so by the uniformity of U, $U \cap N_i = 0$. Since U was arbitrary, $N_i \in \mathscr{F}_{[U_i],M}$.

Let $\mathscr{F}_{[U_i],M}$ contain a unique maximum element $L_{[U_i]}$ which is not M. Then M contains a uniform $U \in [U_i]$. M/N_i is primary with uniforms in $[U_i]$. If $L_{[U_i]}/N_i \ne 0$, then $L_{[U_i]}/N_i$ is primary with uniforms in $[U_i]$. If $L_{[U_i]}/N_i \ne 0$, the natural map from $L_{[U_i]}$ to $L_{[U_i]}/N_i \ne 0$. Therefore the image contains $V \in [U_i]$ and there would be a nonzero map from the inverse image which is in $\mathscr{F}_{[U_i],M}$. This is a contradiction to the definition of $\mathscr{F}_{[U_i],M}$. Thus N_i must equal $L_{[U_i]}$.

Example 5.3: Find the primary decomposition of the $\mathbb{Z}$ module $\mathbb{Z}_{36}$ using Lemma 5.2.

Let $N_1 = \langle 9 \rangle$ and $N_2 = \langle 4 \rangle$.

(a). $N_1 \cap N_2 = \langle 9 \rangle \cap \langle 4 \rangle = 0$

(b). $\mathbb{Z}_{36}/\langle 9 \rangle$ is uniform and thus primary with all uniforms in $[\langle 4 \rangle] = [\mathbb{Z}_3] = [U_1]$.

$\mathbb{Z}_{36}/\langle 4 \rangle$ is uniform and thus primary with all uniforms in $[\langle 9 \rangle] = [\mathbb{Z}_2] = [U_2]$.

(c). $[\langle 4 \rangle] \neq [\langle 9 \rangle]$

Then by Lemma 5.2 $N_1 = \langle 9 \rangle \in \mathscr{F}_{[\mathbb{Z}_3],\mathbb{Z}_{36}} = \{0, \langle 18 \rangle, \langle 9 \rangle\}$ and since $\mathscr{F}_{[\mathbb{Z}_3],\mathbb{Z}_{36}}$ has a unique maximal element then $\langle 9 \rangle$ is the only choice for N_1. Similarly $N_2 = \langle 4 \rangle \in \mathscr{F}_{[\mathbb{Z}_2],\mathbb{Z}_{36}} = \{0, \langle 12 \rangle, \langle 4 \rangle\}$ and since $\mathscr{F}_{[\mathbb{Z}_2],\mathbb{Z}_{36}}$ has a unique maximal element then $\langle 4 \rangle$ is the only choice for N_2.

Decomposing this same example using the Osofsky Theorem a maximal element, $N_{[U]}$ of $\mathscr{F}_{[U],\mathbb{Z}_{36}}$, for each class of uniforms must be found first. By Proposition 4.9 the uniforms of a $\mathbb{Z}$ module are $\mathbb{Z}$ and $\mathbb{Z}_{p_i^n}$, where p_i^n is a power of a prime.

Let $[U_1] = [\mathbb{Z}_3]$, $[U_2] = [\mathbb{Z}_2]$, $[U_3] = [\mathbb{Z}]$, $[U_i] = [\mathbb{Z}_{p_i}]$ where p_i is a prime not equal to 2 or 3.

$\mathscr{F}_{[\mathbb{Z}_3],\mathbb{Z}_{36}} = \{0, \langle 18 \rangle, \langle 9 \rangle\}$ where $N_1 = \langle 9 \rangle$ is the unique maximal element of $\mathscr{F}_{[\mathbb{Z}_3],\mathbb{Z}_{36}}$.

$\mathscr{F}_{[\mathbb{Z}_2],\mathbb{Z}_{36}} = \{0, \langle 12 \rangle, \langle 4 \rangle\}$ where $N_2 = \langle 4 \rangle$ is the unique maximal element of $\mathscr{F}_{[\mathbb{Z}_2],\mathbb{Z}_{36}}$.

$\mathscr{F}_{[\langle\mathbb{Z}\rangle],\mathbb{Z}_{36}} = \{\langle 1\rangle,\langle 2\rangle,\langle 3\rangle,\langle 4\rangle,\langle 6\rangle,\langle 9\rangle,\langle 12\rangle,\langle 18\rangle,0\}$ where $N_3 = \langle 1\rangle = \mathbb{Z}_{36}$ is the unique maximal element in $\mathscr{F}_{[\langle\mathbb{Z}\rangle],\mathbb{Z}_{36}}$

$\mathscr{F}_{[\langle\mathbb{Z}_{p_i}\rangle],\mathbb{Z}_{36}} = \{\langle 1\rangle,\langle 2\rangle,\langle 3\rangle,\langle 4\rangle,\langle 6\rangle,\langle 9\rangle,\langle 12\rangle,\langle 18\rangle,0\}$ where $N_i = \langle 1\rangle = \mathbb{Z}_{36}$ is the unique maximal element in $\mathscr{F}_{[\langle\mathbb{Z}_{p_i}\rangle],\mathbb{Z}_{36}}$ (where p_i is a prime not equal to 2 or 3).

(a). $N_1 \cap N_2 \cap N_3 \cap N_4 \cap \cdots = \langle 9\rangle \cap \langle 4\rangle \cap \langle 1\rangle \cap \langle 1\rangle \cap \cdots = 0$.

(b). $0 \neq \mathbb{Z}_{36}/\langle 9\rangle$ is uniform and any uniform submodule of $\mathbb{Z}_{36}/\langle 9\rangle$ is in $[\mathbb{Z}_3] = [U_1]$.

$0 \neq \mathbb{Z}_{36}/\langle 4\rangle$ is uniform and any uniform submodule of $\mathbb{Z}_{36}/\langle 4\rangle$ is in $[\mathbb{Z}_2] = [U_2]$.

Lemma 5.2 is the bridge between the Osofsky Theorem and the Noether Lasker Theorem. For a finitely generated module over a Noetherian ring the Noether Lasker Theorem guarantees the existence of a decomposition that is reduced, irredundant, and "unique", that is if the components are not unique then the associated primes are unique. Furthermore in the Noether Lasker Theorem the following restriction, $\bigcap_{i=1}^{l} N_i = 0$ and $\bigcap_{i \neq i_0} N_i$ is not contained in N_{i_0} for all $1 \le i_0 \le l$, ensures no $N_i = M$. Thus the Noether Lasker Theorem requires a reduced decomposition.

The Osofsky Theorem approaches decomposition from a different angle. The focus is not on the existence of primary components that represent a reduced and irredundant decomposition, but rather on an algorithm for finding the components. Each component will be a maximal element of $\mathscr{F}_{[U],M}$. The Osofsky decomposition is not reduced or irredundant, because the components are found for each class $[U]$ of uniforms. By Lemma 4.14 we know for each uniform U_i there exist a prime P_i so $[U_i] = [R/P_i]$. By Lemma 4.15 we know for each prime not associated with M, the component is M. Thus the decomposition may consist of an infinite number of components equal to M, as is the case up above. However by finding a maximal element for each class of uniforms, the Osofsky Theorem is not limited to the decomposition of a finitely generated module over a Noetherian ring. The Osofsky Theorem decomposes any nonzero module that contains enough uniforms.

Lemma 5.2 uses the vocabulary of the Osofsky Theorem. The module under consideration must have enough uniforms and $\{[U_i]\}$ represent classes of uniforms. However, the format of Lemma 5.2 more closely follows the format of the Noether Lasker Theorem. If there exist a finite number of primary components N_i that satisfy the three conditions of the lemma then each component $N_i \in \mathscr{F}_{[U_i],\, M}$. Furthermore if $\mathscr{F}_{[U_i],\, M}$ has only one maximal element distinct from M, then N_i is that maximal element. Thus if N_i is the unique maximal element of $\mathscr{F}_{[U_i],\, M}$ then N_i is a primary component in the Noether Lasker decomposition.

Osofsky states before her theorem that limiting the components to those that are distinct from M, will yield the traditional primary components, and their intersection a primary decomposition of 0 in M. Lemma 5.2 amends the Osofsky Theorem to accomplish the goal of including only the primary components that are reduced irredundant, and with unique associated primes. However, changing the Osofsky

Theorem limits the type of modules that can be decomposed. Lemma 5.2 need not hold if there are an infinite number of submodules where $\bigcap_{i=1}^{\infty} N_i = 0$, as shown below.

Example 5.4: Decompose $\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Q}/\mathbb{Z}$ as a $\mathbb{Z}$ module.

Let H_i be a submodule of $\mathbb{Q}/\mathbb{Z}$.

Let $H_i = \left\langle \left\{\frac{1}{p_1^n}\right\}, \left\{\frac{1}{p_2^n}\right\}, \cdots, \left\{\frac{1}{p_{i-1}^n}\right\}, \left\{\frac{1}{p_{i+1}^n}\right\}, \cdots \right\rangle$ where the p_i's are the prime numbers and $n = 1, 2, \cdots$. Let G_i be the submodule of $\mathbb{Q}/\mathbb{Z}$ consisting of all elements whose order is a power of the prime p_i. Let $N_i = p_i\mathbb{Z} \oplus p_i\mathbb{Z} \oplus H_i$, then $\bigcap_{i=1}^{\infty} N_i = 0$.

$\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Q}/\mathbb{Z} \Big/ p_i\mathbb{Z} \oplus p_i\mathbb{Z} \oplus H_i \cong \mathbb{Z}_{p_i} \oplus \mathbb{Z}_{p_i} \oplus G_i$ which is primary with all submodules in $[\mathbb{Z}_{p_i}]$ and $\left[\mathbb{Z}_{p_j}\right] \not\leq \left[\mathbb{Z}_{p_i}\right]$ for $i \neq j$. $n\mathbb{Z} \oplus m\mathbb{Z} \oplus H_i \in \mathscr{F}_{[\mathbb{Z}_{p_i}], \mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Q}/\mathbb{Z}}$ where $n, m \in \mathbb{Z}$.

The N_i defined for $\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Q}/\mathbb{Z}$ fulfills the requirements for parts a, b, and c of Lemma 5.2. However $\mathscr{F}_{[\mathbb{Z}_{p_i}], \mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Q}/\mathbb{Z}}$ has one maximal element, $\mathbb{Z} \oplus \mathbb{Z} \oplus H_i$, and it is distinct from M. But the maximal element of $\mathscr{F}_{[\mathbb{Z}_{p_i}], \mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Q}/\mathbb{Z}}$ is not equal to N_i. Therefore Lemma 5.2 cannot be generalized to include an infinite number of submodules where $\bigcap_{i=1}^{\infty} N_i = 0$.

In Lemma 5.2 as well as in The Noether Lasker Theorem the number of primary components is finite. The Osofsky Theorem as was seen in Example 5.3 can have an infinite number of repeated submodules. In the case of a finitely generated module over a Noetherian ring can the Osofsky Theorem justify a reduced primary decomposition? In order to limit the number of repeated components first we need a definition which generalizes the concept of linear independence for vector spaces to modules.

Definition 5.5: A set $\mathscr{B}$ of elements in a vector space is called **linearly independent** provided the condition $\sum_{i=1}^{n} r_i \cdot b_i = 0$ where the b_i are distinct elements of $\mathscr{B}$, implies that each $r_i = 0$. By convention, the empty set $\varnothing$ is considered independent and indeed a basis for the 0 vector space.

Definition 5.6: A family $\mathscr{B} = \{U_i \subseteq M \mid i \in \mathscr{I}\}$ of submodules of M is called **independent** if, whenever you have $\sum_{i=1}^{n} u_i = 0$ with the u_i from distinct U_i, then each $u_i = 0$. The empty set of submodules is considered independent.

Proposition 5.7: Let M be a module. Then there exists a maximal (possibly empty) independent set of uniform submodules of M.

Proof: If $M = 0$ then by definition of uniform there are no uniform submodules of M. By definition of independent submodules the empty set is independent. Therefore M has an independent set of uniform submodules. If $M \neq 0$ then let $\mathscr{B} = \{U_i \mid U_i \text{ are uniform submodules of } M\}$. Let $\mathscr{S} = \{S_j \mid S_j \text{ are independent subsets of } \mathscr{B}\}$. Take a chain $\mathscr{C} \subseteq \mathscr{S}$, $\mathscr{C}$ is ordered by inclusion. If $S_1, S_2 \in \mathscr{C}$ then $S_1 \subseteq S_2$ or $S_2 \subseteq S_1$. Let $\mathscr{F} = \bigcup_{S_j \in \mathscr{C}} S_j$. Show $\mathscr{F}$ is an independent family of uniform submodules. Take $\{u_1, u_2, \cdots, u_n\}$. Then if $u_1 \in U_{i_1} \in S_{j_1}, u_2 \in U_{i_2} \in S_{j_2}, \cdots, u_n \in U_{i_n} \in S_{j_n}$ and if $S_{j_1} \subseteq \cdots \subseteq S_{j_2} \subseteq \cdots \subseteq S_{j_n}$ then $\{u_1, u_2, \cdots, u_n\}$ are elements in an independent family S_{j_n}.

Thus if $\sum_{i=1}^{n} u_i = 0$ then $u_i = 0$ since S_{j_n} is independent. Thus $\mathscr{F}$ is an independent family of uniform submodules of M. Clearly the $\bigcup_{S_j \in \mathscr{C}} S_j$ is an upper bound for $\mathscr{C} \subseteq \mathscr{S}$. Therefore by Zorn's Lemma there exists a maximal independent set of uniform submodules.

Lemma 5.8: Let M be a nonzero finitely generated module over a commutative Noetherian ring R. Then there are only a finite number of primes associated with M.

Proof: By Proposition 5.7, there is a maximal independent set $\mathscr{B} = \{U_i \mid i \in \mathscr{I}\}$ of uniform submodules of M. By Lemma 5.1, M contains enough uniforms, and since M is nonzero $\mathscr{B}$ is not empty. Set $K = \sum_{i \in \mathscr{I}} U_i$. Since K is finitely generated, some finite subsum of $\sum_i U_i$ must contain all of the generators. Then K must equal that finite subsum, say $K = \sum_{i=1}^{l} U_i$. By the independence of $\mathscr{B}$, no other U_j can have a nonzero element in common with $\sum_{i=1}^{l} U_i$, so $\mathscr{B} = \{ U_i \mid 1 \le i \le l\}$ is a finite set. Each U_i has a single associated prime P_i such that $[U_i] = [R/P_i]$ by Lemma 4.14. Let $Q = (0 : x_0)$ be an associated prime for M. Then $R \cdot x_0$ is a uniform module by remarks before Lemma 4.13. Just as we have for vector spaces, either $R \cdot x_0 \cap \sum_{i=1}^{l} U_i \neq 0$ or $\{ R \cdot x_0, U_1, U_2, \cdots, U_l\}$ is independent. By maximality of $\mathscr{B}$, $R \cdot x_0 \cap K \neq 0$. Let $0 \neq k = \sum_{i=1}^{l} u_i \in R \cdot x_0 \cap K$. The $0 \neq u_i$ are from distinct U_i then by Lemma 4.13 $Q = (0 : k) = \bigcap_{i=1}^{l} (0 : u_i)$. Let $I_i = Ann(u_i)$ and thus $Q \subseteq I_j$ for each j with $u_j \neq 0$. If for each nonzero u_j, there is an element $p_j \in I_j$, $p_j \notin Q$, then $\prod_{u_j \neq 0} p_j$ must belong to Q so one of the p_j must be in Q, a contradiction. We conclude that $Q \supseteq I_j$ for some such j, and therefore $Q = I_j$ for some j. Q is an associated prime of M and $Q = I_j = Ann(u_j)$ where $u_j \in U_j \in [R/P_j]$.Thus $Q \in \{P_1, \cdots, P_l\}$.□

By Proposition 5.7 a module will have a maximal independent set of uniform submodules. If the module M is a finitely generated module over a Noetherian ring then not only is there a finite set of independent uniform modules which generate M but also a unique associated prime for each uniform module. Thus for a Noetherian module the Osofsky Theorem will decompose zero with a finite number of primary components and each uniform will be associated with a unique prime, if an independent set of uniform modules is used.

There is still one remaining problem in part (b) of the two theorems. The word "primary" occurs in both theorem, but they have different definitions.. A review of Definition 3.10: If R is a commutative Noetherian ring and P is a prime ideal of R, then P is ***associated*** with the module M provided $P = (0:x)$ for some $x \in M$. We will call M, ***P-primary***, if the prime ideal P is associated with M and no other prime is.

Proposition 5.9: If R is a commutative Noetherian ring and P is a prime ideal of R, then an R module M is P-primary in the above sense if and only if M has enough uniforms and every uniform submodule of M is in $[R/P]$.

Proof: Assume R is a commutative Noetherian ring, M is an R module, and M is P-primary. By Lemma 5.1 M has enough uniforms. Let U be a uniform submodule of M.

By Lemma 4.14 U contains a submodule isomorphic to R/P for precisely one prime P. M is P-primary, so by Definition 3.10 P is the only prime ideal associated with M. Therefore every uniform submodule of M is in $[R/P]$.

Conversely, assume R is a commutative Noetherian ring. M has enough uniforms and every uniform submodule of M is in $[U]$. Let U' be a uniform submodule of M. By Lemma 4.14 U' contains a submodule isomorphic to R/P for precisely one prime ideal P. By assumption every uniform submodule of M is in $[U]$. Therefore $[U]=[R/P]$. Thus there exists only one prime ideal P in R such that $x \in U' \subset M$ where $P=(0:x)$. Therefore M is P-primary. □

Thus the two definitions of P-primary are equivalent. In texts that first introduce primary ideals and then generalize the concept to primary modules the definition of P-primary is as follows: M is called ***primary*** provided that, whenever $x \in M$ and $r \in R$ satisfy $r \cdot x = 0$, either $x = 0$ or there is a non-negative integer n such that $r^n \cdot M = 0$. We will show the definitions are equivalent for finitely generated modules over commutative Noetherian rings. Otherwise Osofsky's is more general since it is not dependent on a finitely generated module.

Lemma 5.10: Let R be commutative Noetherian, and let M have the set of associated prime ideals $\{P_i \mid i \in \mathscr{I}\}$. Let $x \in M$ and $p \in \bigcap_{i \in \mathscr{I}} P_i$. Then there is a nonnegative integer n such that $p^n \cdot x = 0$.

Proof: R is Noetherian thus by Proposition 2.13 R has maximal element condition. Let

$x \in M$ and $p \in \bigcap_{i \in \mathscr{I}} P_i$. Let $I = (0{:}p^n \cdot x)$ be a maximal element of $\{(0: p^i \cdot x) \mid i \in \mathbb{N}\}$. If $p^n \cdot x \neq 0$, by Lemma 3.7 applied to the module $R(p^n \cdot x)$ some cyclic submodule, say $Rsp^n \cdot x$ is isomorphic to R/P_i for some $i \in \mathscr{I}$. Then $p^n s \cdot x = sp^n \cdot x \neq 0$, but since $p \in P_i$ we have $p \cdot (p^n s \cdot x) = pp^n s \cdot x = 0$. Then $(0: p^{n+1} \cdot x) \supseteq I + Rs$ which properly contains I, contradicting the maximality of I. Hence our assumption, $p^n \cdot x \neq 0$, for all $n \in \mathbb{N}$, must be wrong, i.e. $p^n \cdot x = 0$ for some $n \in \mathbb{N}$.

Lemma 5.11: Let M be a nonzero finitely generated module over a commutative Noetherian ring R. Then M is a P-primary module for some prime ideal P of R if and only if whenever $0 \neq x \in M$ and $r \in R$, if $r \cdot x = 0$, then there exists an $n \in N$ such that $r^n \cdot y = 0$ for all $y \in M$.

Proof: For the only if direction assume M is P-primary for some prime P. Let $0 \neq x \in M$ and $r \in R$ and $r \cdot x = 0$. By Lemma 3.7 applied to the module $R \cdot x$, there is an $s \in R$ with $(0 : s \cdot x)$ a prime ideal. Since M is P-primary, $(0 : s \cdot x)$ must equal P. $r \cdot (s \cdot x) = s \cdot r \cdot x = 0$, thus $r \in P$. By Lemma 5.10, given any element x of M some power of each element of P annihilates x. Since M is finitely generated, $M = \sum_{j=1}^{k} R \cdot x_j$ for some finite set $\{ x_j \mid 1 \leq j \leq k\}$. Given $m \in M$ there exists $r_i \in R$ such that $m = r_1 x_1 + \cdots + r_k x_k$. Since for every element of M there exists some power of each element of P which annihilates it, let $r^{n_j} \cdot x_j = 0$. Then

$r^{(n_1 + \cdots + n_k)}\left(r_1 x_1 + \cdots + r_k x_k\right) = r_1 (r^{n_1} x_1) r^{(n_2 + \cdots + n_k)} + \cdots + r_k \left(r^{n_k} x_k\right) r^{(n_1 + \cdots + n_{k-1})} = 0$. Therefore

$r^{(n_1 + \cdots + n_k)} \cdot M = 0$.

For the if direction, assume $0 \neq x \in M$ and $r \in R$ if $r \cdot x = 0$, then there exists an $n \in N$ such that $r^n \cdot y = 0$ for all $y \in M$. Set

$$P = \left\{ s \in R \middle| \text{there is an } n \in \mathbb{N} \text{ with } s^n \cdot M = 0 \right\}.$$

Clearly $0 \in P$ so $P \neq \varnothing$. Equally clear, $1 \notin P$. Let s, $\hat{s} \in P$, and $r \in R$. If $s^n \cdot M = 0$ and $\hat{s}^{\hat{n}} \cdot M = 0$, then $(s+\hat{s})^{(n+\hat{n})} \cdot M = 0$, thus $s + \hat{s} \in P$. For any rs, $(rs)^n \cdot M = r^n(s^n \cdot M)$ $= 0$, hence $rs \in P$. Thus P is an ideal not equal to R. Let U be any uniform submodule of M. Let Q be an associated prime of M, that is, $Q = (0{:}x)$ for some nonzero $x \in M$ and Q is prime. By definition of P, every element of Q is in P, that is $Q \subseteq P$. If $s \in P$ some power of s is in $(0:x) = Q$ which is a prime ideal. Thus $s \in Q$, so $P \subseteq Q$. We conclude $P = Q$ is the unique prime associated to M, so M is P-primary. □

Thus by Proposition 5.9 when R is a commutative Noetherian ring a traditional definition of P-primary is equivalent to the Osofsky definition of P-primary or by Lemma 5.11 the definitions of P-primary are equivalent in the finitely generated case. We can now consider the one remaining problem, uniqueness. The Noether Lasker Theorem has unique primary components N_i if and only if there are no embedded associated primes. In the Osofsky Theorem we are limiting the case to a Noetherian module, thus there is a finite independent set of uniform modules. Uniqueness will occur in the Osofsky Theorem when $\mathscr{F}_{[U],\,M}$ has only one maximal element that is the only homomorphism from $K \in \mathscr{F}_{[U],\,M}$ to $V \subseteq M$ where V is a uniform module in $[U]$ is the zero homomorphism. How are these two conditions on uniqueness related?

Lemma 5.12: For R commutative Noetherian, let the set of primes $\{P_1, \cdots, P_k\}$

associated with M be finite, and let Q be any prime which does not contain any of the P_i. Then the only homomorphism from M to R/Q is the zero homomorphism.

Proof: For each i with $1 \le i \le k$ let $p_i \in P_i$ and $p_i \notin Q$. Then $s = \prod_{i=1}^{k} p_i \notin Q$. Let φ be a homomorphism from M to R/Q, $x \in M$. By Lemma 5.10 there is an n such that $s^n \cdot x = 0$. Then $0 = (0)\varphi = (s^n \cdot x)\varphi = s^n \cdot ((x)\varphi)$. But Q is a prime ideal and $s^n \notin Q$, so $s^n \cdot ((x)\varphi) = (0 + Q)$ in R/Q implies $(x)\varphi = (0 + Q)$ in R/Q. □

Assume M satisfies a), b), and c) of the Noether Lasker Theorem below. We want to prove d). PART I is needed for both directions of the proof.

M is a finitely generated module over a commutative Noetherian ring R. There exists a finite set $\{ N_i \mid 1 \le i \le l \}$ of submodules of M such that:

a) $\bigcap_{i=1}^{l} N_i = 0$ and $\bigcap_{i \ne i_0} N_i$ is not contained in N_{i_0} for all $1 \le i_0 \le l$.

b) Each quotient M/N_i is primary for some prime P_i.

c) The P_i are all distinct for $1 \le i \le l$.

d) The primary component N_i is unique $\Leftrightarrow$ P_i does not contain P_j for any $j \ne i$.

PART I

M is a module over a commutative Noetherian ring, therefore by Lemma 5.1 M has enough uniforms. Let $\{[U_k]\}$ represent classes of uniforms of M. By Lemma 4.14 U_k contains a submodule isomorphic to R/P for precisely one prime ideal P. Let $[R/P_k] = [U_k]$ where we have chosen indices so that $[R/P_i] = [U_i]$ for $1 \le i \le l$ and the P_i are the P_i described in a), b), and c) above. By c) above the P_i are all distinct for

$1 \le i \le l$, and $[R/P_i] = [U_i]$, and thus **(i)** $[U_i] \ne [U_j]$ if $i \ne j$ for $1 \le i, j \le l$, furthermore by Lemma 5.8 these are the only associated primes of M. By Proposition 5.9 the Noether Lasker definition of P-primary is equivalent to the Osofsky definition of P-primary. By b) above M/N_i is P_i primary and therefore **(ii)** M/N_i is primary with uniforms all in $[U_i]$. By a) above **(iii)** $\bigcap_{i=1}^{l} N_i = 0$. By the Noether Lasker condition, $\bigcap_{i \ne i_0} N_i$ is not contained in N_{i_0} for all $1 \le i_0 \le l$, thus **(iv)** $N_i \ne M$. Therefore by **(i)**, **(ii)**, **(iii)**, **(iv)**, and Lemma 5.2 each $N_i \in \mathscr{F}_{[U_i],\,M}$.

Using the Osofsky theorem for the nonzero module M where $\{[U_k]\}$ are the classes of uniforms, and $S_{[U_k]}$ is any maximal element of $\mathscr{F}_{[U_k],M}$, then $\bigcap_{[U_k]} S_{[U_k]} = 0$. By Proposition 5.7 there is a maximal independent set of uniform submodules of M. It was shown above for $1 \le i \le l$, $[R/P_i] = [U_i]$ and by Lemma 5.8 these are the only primes associated with M. By Lemma 4.15 if P_x is not associated with M then $S_{[U_x]} = M$, thus $\bigcap_{i=1}^{l} S_{[U_i]} = 0$. $0 \ne M/S_{[U_k]}$ when $1 \le k \le l$ thus by the Osofsky Theorem $M/S_{[U_k]}$ is primary for $1 \le k \le l$.

Now we prove that if P_i does not contain P_j for any $j \ne i$, then the primary component N_i is unique.

Follow PART I and assume no $P_i \supsetneq P_j$ for any $j \ne i$. By definition of $\mathscr{F}_{[R/P_i],M}$ if $K \in \mathscr{F}_{[R/P_i],M}$ then $Ass\{K\} \subseteq \{P_1, \cdots, P_{i-1}, P_{i+1}, \cdots P_l\}$. By Lemma 5.12 there does not exist a nonzero homomorphism from K in $\mathscr{F}_{[R/P_i],M}$ to R/P_i for any K. By Osofsky

Theorem $\mathscr{F}_{[U],M}$ has one maximal element. By Lemma 5.2 $N_i = S_i$ that is N_i is the unique maximal element.

Proof of converse:

Follow PART I and assume **(v),** N_i is a unique primary component. Therefore by **(i), (ii), (iii), (iv), (v)** and Lemma 5.2 $N_i \in \mathscr{F}_{[U_i],M}$ and N_i is the unique maximal element. Thus $N_i = S_i$. By the Osofsky Theorem the only homomorphism from any $K \in \mathscr{F}_{[R/P_i],M}$ to $V \subseteq M$ where V is a uniform module in R/P_i is the zero homomorphism. Suppose $P_i \supsetneq P_j$. By the Osofsky Theorem part b) M/N_j is primary and contains a uniform submodule in $\left[U_j\right] = \left[R/P_j\right]$. Let $K_j \subseteq M$ be the uniform submodule isomorphic to R/P_j. By c) above P_i and P_j are distinct, therefore $K_j \in \mathscr{F}_{[R/P_i],M}$. However $P_i \supsetneq P_j$ so by the third isomorphism theorem there exists a nonzero homomorphism φ from K_j, which is isomorphic to R/P_j , to R/P_i where the kernel of φ is P_i/P_j. This contradicts the Osofsky Theorem. Thus P_i does not contain P_j for any $j \neq i$.

Therefore for a finitely generated module over a Noetherian Ring the Noether Lasker uniqueness follows from Osofsky uniqueness. □

In modern textbooks, details for primary decomposition of ideals are usually included, while the generalization to modules is given cursory coverage. The logic is sensible; it is easier to comprehend the basic theories of a topic when the scope is limited. Then the flow to a more generalized version can be absorbed more readily. The Osofsky presentation opposes this trend.

The basic background information needed for studying the Noether Lasker Theorem or the Osofsky theorem would include a knowledge of the homomorphism theorems for groups and rings, some study of prime factorization for Euclidean domains such as the integers or polynomials over a field, and at least the definition of a prime ideal in a commutative ring. If module decomposition was the only presentation a student was exposed to, the student would not only have to be familiar with the definition of vector space over a field, but also spend time expanding her knowledge to a generalized module. In addition the following would be an absolute minimum representation of items to be included for the Noether Lasker Theorem: 3.5, 3.6, 3.8, 3.9, 3.10, 3.11 3.12, 3.13, 3.16, 3.24, 3.25 3.26, 3.27 and 3.28 or 14 items. On the other hand the minimum requirements for the Osofsky presentation would be 3.3, 3.4, 4.1-4.4, 4.6, 4.11, and 4.19 for a total of 9 items. That is a substantial difference in numbers.

The Osofsky process introduces less new material. The proof of her theorem depends on fundamental theorems of homomorphisms, which certainly reinforces the material taught in a beginning undergraduate algebra class. Proposition 4.21 relates her theorem to Abelian groups. At a minimum this requires at least an introduction to The Fundamental Theorem of Finitely Generated Modules over a *PID* or $\mathbb{Z}$, that is a direct sum of cyclic modules. This theorem reinforces the learning of The Fundamental Theorem of Finitely Generated Abelian Groups, a direct product of cyclic groups. At this stage it must be pointed out that a finite direct product can be written as a finite direct sum. However, being finite is not a condition of Proposition 4.21 and thus the direct sum must be used. Although an introductory algebra course may contain a paragraph about the relationship between direct products and direct sum, this is really not a topic of the course. Additional supplementary material would need to be added to the presentation.

In addition the $\mathscr{F}_{[U],\,M}$ notation is cumbersome. However, once the notation is understood the Osofsky Theorem states how to find the components. Providing an algorithm offers a great advantage to the Osofsky Theorem. Osofsky purposely limits the scope of the topic, and certainly by limiting the types of examples a student could easily grasp the idea. Often a subject matter is better understood, if different presentations are given over a period of time. So after a quick exposure to the Osofsky Theorem, an undergraduate student may find the concepts much easier to grasp in a more advanced course.

However, having said that, a student appreciates the theorem after the comparisons are completed in section five. Osofsky does not intend for an undergraduate student to be exposed to section five, because the student is not yet familiar with the Noether Lasker Theorem. The topic would appear to be a better supplementary subject to a graduate algebra class. In this way, instead of rehashing primary decomposition for modules, Osofsky expands and adds interest to the generalized version.

6. Parametric Decomposition of Monomial Ideals

In this final section two algorithms are given for finding a unique decomposition of an ideal for a very specific family of rings. Although the results in this section apply to more general rings, we will stay within the framework of this paper and limit the discussion to the ring of power series over the ring k denoted by $k[[x_1,\cdots,x_d]]$ or local rings R_M, where $R = k[x_1,\cdots,x_d]$and $M = \langle x_1,\cdots,x_d \rangle$, and R is the smallest subring of $k(x_1,\cdots,x_d)$ where every element in $k[x_1,\cdots,x_d] - \langle x_1,\cdots,x_d \rangle$ has an multiplicative inverse in the ring.

Notation: Where k is a field R_M is the localization of R at M where $R = k[x_1,\cdots,x_d]$ and the maximal ideal $M = \langle x_1,\cdots,x_d \rangle$

Definition 6.1: A ***monomial*** (in $x_1,\cdots,x_d$) is a power product $x_1^{e_1}\cdots x_d^{e_d}$, where $e_1,\cdots,e_d$ are nonnegative integers and a ***monomial ideal*** is a proper ideal generated by monomials.

Definition 6.2: ***Minimal basis*** is a basis such that no proper subset is a generating set of the ideal.

Definition 6.3: An ***open monomial*** in R_M is an ideal that contains a power of the ideal generated by the monomials of degree one.

A topological space is Noetherian in case its open sets satisfy the ascending chain condition. For this paper an example of an open ideal of a local ring R_M, where $R = k[x_1,\cdots,x_d]$ and $M = \langle x_1,\cdots,x_d \rangle$, and $\{x_1,\cdots,x_d\}$ a minimal basis of *M*, is a monomial ideal. This is an example that contains a power of each x_i, $i = 1, \cdots, d$, and that has a basis consisting of power-products of the x_i.

Definition 6.4: A ***parameter ideal*** $(\text{in } x_1, \cdots, x_d)$ is an ideal of the form $\langle x_1^{a_1}, \cdots, x_d^{a_d} \rangle$ where $a_1, \cdots, a_d$ are positive integers.

Example 6.5: If $f = x_1^{e_1} \cdots x_d^{e_d}$ is a monomial, then we let $P(f)$ denote the parameter ideal $\langle x_1^{e_1+1}, \cdots, x_d^{e_d+1} \rangle$. If $f = 1$, then $P(f) = M$. If $a_1, \cdots, a_d$ are positive integers then we let $P(a_1, \cdots, a_d)$ denote the parameter ideal $\langle x_1^{a_1}, \cdots, x_d^{a_d} \rangle$, so $P(a_1, \cdots, a_d) = P(f)$ where $f = x_1^{a_1 - 1} \cdots x_d^{a_d - 1}$.

Definition 6.6: The ***spectrum*** of a Noetherian ring R is the set of all the prime ideals of R, partially ordered by inclusion.

Definition 6.7: The ***Krull dimension*** or dimension of R is finite in case there is an integer $n > 0$ such that every chain of its spectrum has length at most n (equivalently, in case every prime ideal of R has height at most n); then the dimension dim R of R is the smallest such integer n. If no such n exists, then R has infinite dimension.

For example, a field has dimension 0. *PID*s have dimension one, since all their nonzero prime ideals are maximal. In this section where k is a field, $k[x_1, \cdots, x_d]$ has dimension d.

Remark 6.8: Let f be monomial. $f_1, \cdots, f_n$ are monomials then $f \in \langle f_1, \cdots, f_n \rangle$ if and only if $f \in \langle f_i \rangle$ for some $i = 1, \cdots, n$.

Definition 6.9: Let $Q = \langle f_1, \cdots, f_n \rangle \subseteq R = k[x, y]$ and **lexicographically order** the (x, y) in f_i, by saying that $f_i < f_j$ (for $f_i = x^a y^b$ and $f_j = x^c y^e$) if either $a < c$ or $a = c$ and $b < e$

The following conditions pertain to the remaining section of this paper. R_M is a commutative local ring where $R = k[x_1, \cdots, x_d]$, the maximal ideal $M = \langle x_1, \cdots, x_d \rangle$, with the identity $1 \neq 0$, and I is a monomial ideal (that is, a proper ideal generated by monomials $x_1^{e_1}, \cdots, x_d^{e_d}$) such that $Rad\ \langle I \rangle = Rad \langle M \rangle$.

Definition 6.10: Let J be a monomial ideal. Then a ***J corner-element*** is a monomial z such that $z \notin J$ and $zx_i \in J$ for $i = 1, \cdots, d$.

The name corner-element is suggested by the geometric interpretation below, where a corner-element is an element $z = x^a y^b$ in case $d = 2$ with coordinates (a, b) such that $(a, b+1)$, $(a+1, b)$, and $(a+1, b+1)$ are the coordinates of points in I and $z \notin I$.

Note that 1 is the unique M corner-element (since each non-unit monomial is in M).
Also if J is a monomial ideal and 1 is a J corner-element, then $1x_i \in J$ for $i = 1, \cdots, d$ so, $J = M$.

With those definitions we will now find the Q-corner-elements for a monomial ideal Q in R_M.

Geometric Interpretation 6.11: Assume that $d = 2$, let $x = x_1$ and $y = x_2$, let $f_1, \cdots, f_n$ be a minimal basis of I (where the f_l are monomials in *x* and *y*, say $f_l = x^{i_l} y^{j_l}$) and assume $Rad\ \langle I \rangle = Rad\langle x, y\rangle$. First lexicographically order the f_l and assume that $f_1 < \cdots < f_n$. Plot the n points (i_l, j_l) (corresponding to the f_l) in the first quadrant of the xy-plane. Then for each of these n points draw the horizontal line segment connecting (i_l, j_l), $(i_l + 1, j_l)$, $(i_l + 2, j_l), \cdots$ and draw the vertical line segment connecting (i_l, j_l), $(i_l, j_l + 1)$, $(i_l, j_l + 2), \cdots$. It is clear that there is a one-to one correspondence from the set $D = \{(a,b) \mid a \geq i_l \text{ and } b \geq j_l \text{ for some } l = 1, \cdots, n\}$ to a subset **W** of the set of monomials in I, and it follows from Remark 6.8 that, in fact, every monomial in I is in **W**. Since $(i_l, j_l) < (i_{l+1}, j_{l+1})$, the point (i_{l+1}, j_l), are the coordinates of the intersection of the rightward extending horizontal line segment through (i_l, j_l) with the ascending vertical line segment through (i_{l+1}, j_{l+1}), thus $z_l = x^{i_{l+1}-1}y^{j_l-1} \notin I$. $z_l y$ has coordinates on the rightward extending horizontal line segment through (i_l, j_l) so $z_l y \in I$. $z_l x$ has coordinates on the ascending vertical line segment (i_{l+1}, j_{l+1}) so $z_l x \in I$. Hence z_l is an I corner-element. And since an I corner-element must correspond to some (a,b) with $0 \leq a \leq i_n$ and $0 \leq b \leq j_l$, it is readily checked that all I corner-elements are obtained in this way, so there are exactly $n-1$ of them (Heinzer 39).

Example 6.12: For an open monomial ideal Q find the Q-corner-elements for R_M $R = k[x, y]$ and $M = \langle x, y\rangle$ of height two, where $x_1 = x$ and $x_2 = y$, and let $Q = \langle y^9, xy^7, x^3y^4, x^5y^2, x^{11}\rangle$. $Rad\ \langle Q\rangle = Rad\langle x, y\rangle$.

Q is lexicographically ordered with $f_1 = y^9$, $f_2 = xy^7$, $f_3 = x^3y^4$, $f_4 = x^5y^2$, and

$f_5 = x^{11}$. The points (0,9), (1,7), (3,4), (5,2), and (11,0) correspond to $f_1, \cdots, f_5$. Consider $f_i = f_1 = y^9$ with coordinates $(0,9)$. The horizontal line from $(0,9)$ connecting points $(1,9),(2,9),\cdots$ intersects with the vertical line connecting points $(0,9)$ $(0,10),(0,11)$. Then all the monomial $x^a y^b$ with coordinates (a,b) where $a \geq 0$ and $b \geq 9$ such as $x^{10}y^{15}$ are elements of Q. In Figure 3 the horizontal line from $(0,9)$ connecting points $(1,9),(2,9),\cdots$ intersects with the ascending vertical line from $(1,7)$, $(1,8)$ $(1,9),\cdots$ at $(1,9)$.

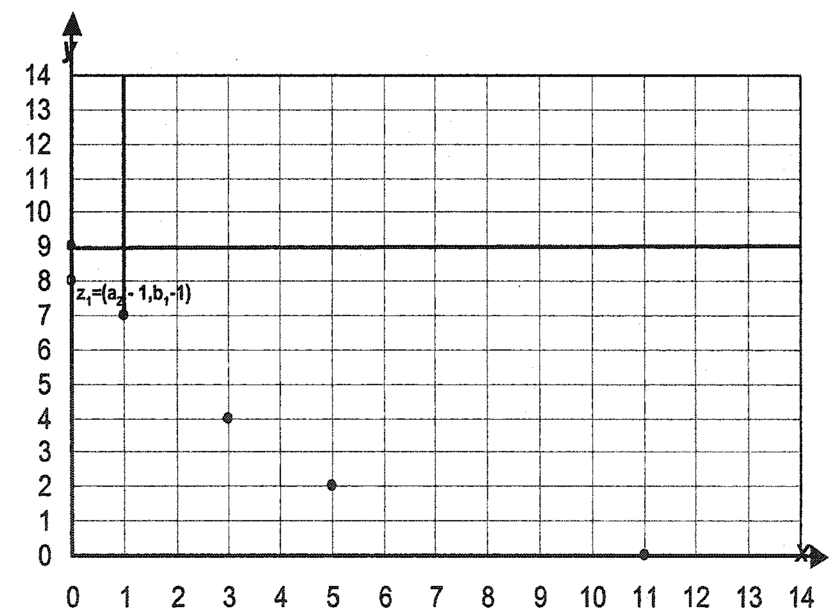

Figure 3

The points that surround the corner element $(0,8)$ are $(0,9)$, $(1,9)$, and $(1,8)$. $(1,9)$

represents (xy^9) and is an element of Q either through the minimal basis element $\langle y^9 \rangle$ or $\langle xy^7 \rangle$. $(1,8)$ represents (xy^8) and is an element of Q through the minimal basis element $\langle xy^7 \rangle$. $(0,8)$ represents $(y^8) \notin Q$. (y^8) is a corner-element by definition so $z_1 = (y^8)$. In Figure 3 z_1 is the open dot. We find the remaining corner-elements by repeating the process for each $l = 2,3,4,5$ where the Q corner-elements are $z_l = x^{i_{l+1}-1} y^{j_l - 1}$, with $z_1 = y^8$, $z_2 = x^2 y^6$, $z_3 = x^4 y^3$, and $z_4 = x^{10} y$, where $z_l \notin Q$

Below in Figure 4 the four corner-elements, $z_1, z_2, z_3,$ and z_4 are labeled as open points. Every closed point represents an element contained in the ideal Q. This set of points is called **W**. It is easy to see by multiplying any corner-element by x or y, the corner-element becomes a member of **W**.

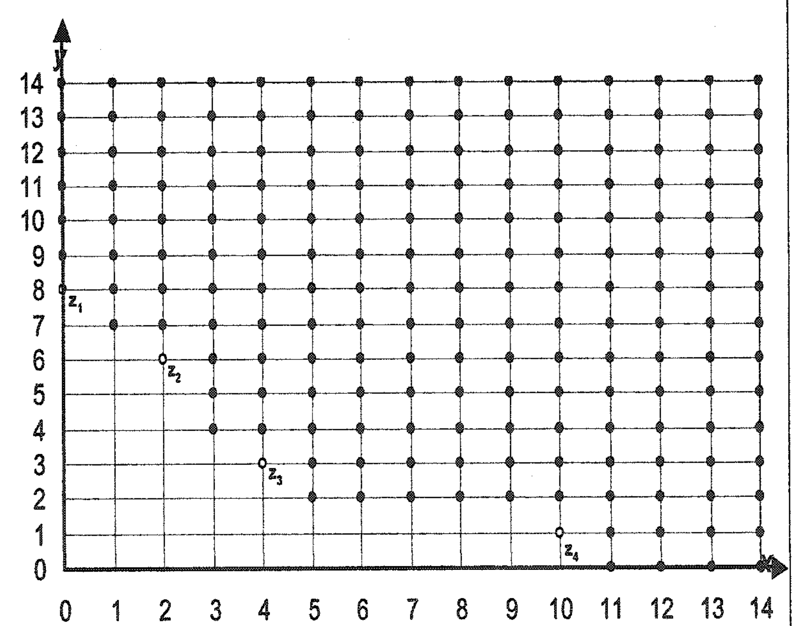

Figure 4

Understanding and visualizing the two space case allows an easier transition to the algebraic construction where $d = n$ and the subsequent associated ideas and properties.

Algebraic Construction Solution 6.13: Let R_M be the local ring where $R = k[x_1, \cdots, x_d]$ and $M = \langle x_1, \cdots, x_d \rangle$ and let I be a monomial ideal such that $Rad\ \langle I \rangle = Rad \langle M \rangle$. The following is an algebraic construction of the I corner-elements. For ease of description it will be said that $\deg(f) = n$ if $f = x_1^{e_1} \cdots x_d^{e_d}$ and $e_1 + \cdots + e_d = n$. Let S be the set of monomials (in $x_1, \cdots, x_d$) that are not in I. S is a finite set, since $Rad\ \langle I \rangle = Rad \langle M \rangle$ implies for $i = 1, \cdots, d$ there exists a positive integer n_i such that $x_i^{n_i} \in I$. Let $w = \max\{n \mid n = \deg(f) \text{ for some } f \in S\}$. For $j = 1, \cdots, w$ let $D_j = \{f \in S \mid \deg(f) = j\}$. Let $C_w = D_w$ and for $j = 1, \cdots, w-1$ let $C_j = \{f \in D_j \mid fx_i \notin D_{j+1} \text{ for } i = 1, \cdots, d\}$. Possibly some of the sets C_j are empty for $j < w$. Then $C_1 \cup \cdots \cup C_w$ is the set of I corner-elements and this union is disjoint.

Example 6.14: Let R_M be the local ring where $R = k[x, y, z]$, $M = \langle x, y, z \rangle$, and height equals three. Let $x_1 = x$, $x_2 = y$, $x_3 = z$ and let the open monomial $Q = \langle z^4, y^2z^3, y^3, xyz, xy^2, x^2 \rangle$. $Rad\ \langle Q \rangle = Rad \langle x, y, z \rangle$. Find the Q-corner-elements.

S is the set of monomials that are not in Q. Thus $S = (z, z^2, z^3, y, yz, yz^2, yz^3, y^2, y^2z, y^2z^2, x, xz, xz^2, xz^3, xy)$. Four is the maximum degree of S therefore $w = 4$. D_4 contains the monomials in S that have degree four, thus $D_4 = \{yz^3, y^2z^2, xz^3\}$. Similarly $D_3 = \{z^3, yz^2, y^2z, xz^2\}$, $D_2 = \{z^2, yz, y^2, xz, xy\}$, and

$D_1 = \{z, y, x\}$. $C_4 = D_4 = \{yz^3, y^2z^2, xz^3\}$. To find C_3, $fx_i \notin D_3$ for $i = 1, 2, 3$. $z^3 \in D_3$ but $yz^3 \in D_4$; $yz^2 \in D_3$ but $y \cdot yz^2 = y^2z^2 \in D_4$; $y^2z \in D_3$, but $z \cdot y^2z = y^2z^2 \in D_4$ and finally $xz^2 \in D_3$ but $z \cdot xz^2 = xz^3 \in D_4$. Hence $C_3 = \varnothing$. Similarly for C_2 we have $z \cdot z^2$, $z \cdot yz$, $z \cdot y^2$, and $z \cdot xz \in D_3$ thus $\{z^2, yz, y^2, xz\} \not\subseteq C_2$ but $x \cdot (xy)$, $y \cdot (xy)$, and and $z \cdot (xy) \notin D_3$ thus $C_2 = \{xy\}$. For C_1 $z \cdot z$, $z \cdot y$, and $z \cdot x \in D_2$ thus $C_1 = \varnothing$. $C_1 \cup \cdots \cup C_w = \{yz^3, y^2z^2, xz^3, xy\}$ are the Q corner-elements

Proof of Algebraic Construction 6.15: Let $f \in C_j$ for some $j = 1, \cdots, w$ Then $f \notin I$ (since $f \in C_j \subseteq S$) and for $i = 1, \cdots, d$ it holds that $\deg(fx_i) = j + 1$. If $j = w$, then $fx_i \notin S$, for no element in S has degree greater than $w = j$. If $j < w$, then $fx_i \notin D_{j+1} = \{g \in S \mid \deg(g) = j + 1\}$ by definition of C_j. Therefore in either case ($j = w$ or $j < w$) $fx_i \notin S$ for $i = 1, \cdots, d$, so $fx_i \in I$, hence f is an I corner-element. Therefore $C_1 \cup \cdots \cup C_w \subseteq \mathbf{C} = \{f \mid f \text{ is an } I \text{ corner-element}\}$.

If $g \in \mathbf{C}$ then $g \notin I$, so $g \in S$, so $g \in D_j$ where $j = \deg(g)$. Also $\deg(gx_i) = j + 1$ and $gx_i \in I$ for $i = 1, \cdots, d$, so $gx_i \notin D_{j+1}$. Therefore $g \in C_j$ so $\mathbf{C} \subseteq C_1 \cup \cdots \cup C_w$ (Heinzer 39-40).

Remark 6.16: With the notation of the algebraic construction in 6.15 let f be a monomial that is not in I, a monomial ideal, such that $Rad\ \langle I \rangle = Rad\ \langle M \rangle$. Then there exists a monomial g (possibly $g = 1$) such that fg is an I corner-element.

Proof: It may be assumed that f is not an I corner-element, so $fx_i \notin I$ for some $i = 1, \cdots, d$. Let $T = \{g \mid g$ is a monomial in $x_1, \cdots, x_d$ and $fg \notin I\}$. Since T is a finite set (T is contained in the finite set S of 6.15 and I is a monomial ideal such that $Rad\ \langle I \rangle = Rad \langle M \rangle$), so let $g \in T$ such that the $\deg(g)$ is greater than or equal to the degree of the other monomials in T. Then $fgx_i \in I$ for $i = 1, \cdots, d$, by maximality of the sum of the exponents of g, so fg is an I corner-element.

Remark 6.17: Let f and g be monomials. If $f \in \langle g \rangle$ then there exists a monomial k (Possibly $k = 1$) such that $f = gk$.

Lemma 6.18: Let f and g be monomials. Then $g \in P(f)$ if and only if $f \notin \langle g \rangle$

Proof: Let $f = x_1^{e_1} \cdots x_d^{e_d}$. Then $f \notin \langle x_i^{e_i+1} \rangle$ for $i = 1, \cdots, d$, since $e_i < e_i + 1$ for $i = 1, \cdots, d$ so Remark 6.8 shows that $f \notin P(f)$. Therefore if $g \in P(f)$ then $f \notin \langle g \rangle$.

For the converse assume that $g \notin P(f)$ and let $g = x_1^{a_1} \cdots x_d^{a_d}$. Then $a_i < e_i + 1$ for $i = 1, \cdots, d$, so $e_i \geq a_i$ for $i = 1, \cdots, d$, hence $f \in \langle g \rangle$.

Proposition 6.19: If J is a monomial ideal with $Rad\ \langle J \rangle = Rad \langle M \rangle$, then the J corner-elements are the monomials in $(J : M) - J$ where $J : M = \{r \in R \mid rx \in J$ for all $x \in M\}$. Also, if z and z' are distinct J corner-elements, then $\langle z \rangle \not\subseteq \langle z' \rangle$ and $\langle z' \rangle \not\subseteq \langle z \rangle$, so there exists only finitely many J corner-elements. Finiteness was observed in the proof of algebraic construction 6.15.

Proof: Let **C** be the set of J corner-elements. Each element in **C** is a monomial. Then it is clear from the definition of corner-element that $\mathbf{C} \subseteq (J:M) - J$. If z is a monomial in $(J:M) - J$ then $z \notin J$ and $zx_i \in J$ for $i = 1, \cdots, d$, so z is a J corner-element, hence $z \in \mathbf{C}$. Therefore **C** is the set of monomials in $(J:M) - J$.

Now let z and z' be distinct J corner-elements and suppose $\langle z \rangle \subseteq \langle z' \rangle$. Then Remark 6.17 shows that $z = z'f$ for some monomial f where $f \neq 1$ since $z \neq z'$. But this implies that $z = z'f \in J$, since z' is a J corner-element, and this is a contradiction. Therefore $\langle z \rangle \not\subseteq \langle z' \rangle$ and similarly, $\langle z' \rangle \not\subseteq \langle z \rangle$. There exists only finitely many J corner-elements.

Corollary 6.20: Let J be a monomial ideal and let $z_1, \cdots, z_m$ be the J corner-elements. Then for $j = 1, \cdots, m$, one has $\langle z_1, \cdots, z_{j-1}, z_{j+1}, \cdots, z_m \rangle \subseteq P(z_j)$ and $z_j \notin P(z_j)$. Therefore $\bigcap \{ P(z_j) \mid j = 1, \cdots, m \}$ is an irredundant intersection of parameter ideals.

Proof: (It follows from Proposition 6.19 that there are only finitely many J corner-elements. If $m = 1$ and $z_1 = 1$ then $P(z_1) = M$. $\langle 0 \rangle$, the ideal generated by the empty set, is contained in M and $1 \notin P(1) = M$, so the conclusion holds in this case.)

Fix $j \in \{1, \cdots, m\}$. It follows from Proposition 6.19 that if $i \in \{1, \cdots, j-1, j+1, \cdots, m\}$) then (1) $z_j \notin \langle z_i \rangle$. By Lemma 6.18 $z_i \in P(z_j)$, hence (2) $\langle z_1, \cdots, z_{j-1}, z_{j+1}, \cdots, z_m \rangle \subseteq P(z_j)$ and $z_j \notin P(z_j)$. (1) and (2) show that $\bigcap \{ P(z_j) \mid j = 1, \cdots, m \}$ is an irredundant intersection and Definition 6.4 shows that the ideals $P(z_j)$ are parameter ideals.

Theorem 6.21: Let I be a monomial ideal such that $Rad\langle I\rangle = Rad\langle M\rangle$ and let $z_1,\cdots,z_m$ be the I corner-elements. Then $I=\bigcap\{P(z_j)|\ j=1,\cdots,m\}$ is a decomposition of I as an irredundant intersection of parameter ideals.

Proof: Let $J=\bigcap\{P(z_j)|\ j=1,\cdots,m\}$. Then Corollary 6.20 shows that J is the irredundant intersection of the m parameter ideals $P(z_j)$.

Let f be a monomial in I and suppose that $f\notin P(z_j)$ for some $j\in\{1,\cdots,m\}$. Then $z_j\in\langle f\rangle\subseteq I$ by Lemma 6.18, and this contradicts the fact that $z_j\notin I$ (since z_j is an I corner-element). Therefore $I\subseteq J$.

Finally (Taylor 17) shows that J is a monomial ideal (since $Rad\langle P(z_j)\rangle = Rad\langle M\rangle$ for $j=\{1,\cdots,m\}$), so it suffices to show that each monomial that is not in I is not in J. For this, let f be a monomial that is not in I. Then Remark 6.16 shows that there exists a monomial g (possibly $g=1$) such that fg is an I corner-element. $fg=z_j$ for some $j=\{1,\cdots,m\}$, since Proposition 6.19 shows that the I corner-elements are finite in number and uniquely determined by I. Then $f\notin P(z_j)$, by Lemma 6.18 so it follow that $I\supseteq J$, hence $I=J$ by the preceding paragraph.

Proposition 6.22: For $j=1,\cdots,m$ let $a_j=(a_{j,1},\cdots,a_{j,d})$ be a d-tuple of positive integers and let $I=\bigcap\{P(a_j)|\ j=1,\cdots,m\}$ be a decomposition of I as an irredundant intersection of parameter ideals. Then the I corner-elements are the m elements

$x_1^{a_{j,1}-1} \cdots x_d^{a_{j,d}-1}$.

Proof: (Note $Rad\langle I\rangle = Rad\langle M\rangle$, since $Rad\langle P(a_j)\rangle = Rad\langle M\rangle$ for $j=1,\cdots,m$).

It will first be shown that each of the m elements $z_j = x_1^{a_{j,1}-1} \cdots x_d^{a_{j,d}-1}$ is an I corner-element.

Note first that $P(z_j) = P(a_j)$ for $j=1,\cdots,m$. Then $z_i \notin \langle z_j\rangle$ for all $i \neq j \in \{1,\cdots,m\}$. To see this, if $z_i \in \langle z_j\rangle$ then $P(a_i) = P(z_i) \subseteq P(z_j) = P(a_j)$, and this is a contradiction since the intersection is irredundant. Lemma 6.18 shows that $z_j \notin P(z_j) = P(a_j)$ (so $z_j \notin I$) and that $z_j \in P(z_k) = P(a_k)$ for $k \in \{1,\cdots,j-1,j+1,\cdots,m\}$. Also $z_j x_i \in \left\langle x_i^{(a_{j,i}-1)+1}\right\rangle \subseteq P(a_j)$ for $i=1,\cdots,d$, so $z_j x_i \in \bigcap\{P(a_h) \mid h=1,\cdots,m\} = I$. Therefore z_j is an I corner-element, so it follow that $z_1,\cdots,z_m$ are among the I corner-elements.

Now let w be an I corner-element. Then $w \notin I$, so $w \notin P(z_j) = P(a_j)$ for some $j=1,\cdots,m$. Therefore $z_j \in \langle w\rangle$ by Lemma 6.18 so $z_j = wg$ for some monomial g by Remark 6.17. If $g \neq 1$, then $wg \in I$, since w is an I corner-element. But this implies that $z_j \in I$, and this contradicts the fact that z_j is an I corner-element. Thus $g=1$ and this implies $w = z_j$. Therefore $z_1,\cdots,z_m$ are all I corner-elements (Heinzer 42).

Theorem 6.23 (Unique Factorization): Let $z_1,\cdots,z_m$ and $w_1,\cdots,w_n$ be monomials such that $\bigcap\{P(z_j) \mid j=1,\cdots,m\} = \bigcap\{P(w_i) \mid i=1,\cdots,n\}$ are irredundant intersections of parameter ideals. Then $n=m$ and $\{z_1,\cdots,z_m\}=\{w_1,\cdots,w_n\}$.

Proof: Let $I=\bigcap\{P(z_j)|\ j=1,\cdots,m\}$. Then it follows from Proposition 6.22 that $z_1,\cdots,z_m$ are the I corner-elements, so they are the monomials in $(I:M)-I$ by Proposition 6.19. However, $I=\bigcap\{P(w_i)|\ i=1,\cdots,n\}$ by hypothesis, so similar statements hold for $w_1,\cdots,w_n$ in place of $z_1,\cdots,z_m$, hence it follows that $n=m$ and that $\{z_1,\cdots,z_m\}=\{w_1,\cdots,w_n\}$ (Heinzer 45).

In Example 6.12 where $Q=\langle y^9,xy^7,x^3y^4,x^5y^2,x^{11}\rangle$, the Q corner-elements are $z_1=y^8$, $z_2=x^2y^6$, $z_3=x^4y^3$, and $z_4=x^{10}y$. By Theorem 6.21 the decomposition of Q is an irredundant intersection of parameter ideals where $Q=\langle x,y^9\rangle\cap\langle x^3,y^7\rangle\cap\langle x^5,y^4\rangle\cap\langle x^{11},y^2\rangle$. It is easy to see every parameter ideal equals $P(f)$ for some f. Therefore, by Theorem 6.23 it is a unique factorization.

In Example 6.14 where $Q=\langle z^4,y^2z^3,y^3,xyz,xy^2,x^2\rangle$, the Q corner-elements are $\{yz^3,\ y^2z^2,\ xz^3,\text{and }xy\}$. By Theorem 6.21 the decomposition of Q is an irredundant intersection of parameter ideals where $Q=\langle y^2,z^4\rangle\cap\langle y^3,z^3\rangle\cap\langle x^2,z^4\rangle\cap\langle x^2,y^2\rangle$. By Theorem 6.23 it is a unique factorization.

Thus for the local ring R_M where $R=k[x_1,\cdots,x_d]$ and $M=\langle x_1,\cdots,x_d\rangle$ containing a monomial ideal I where $Rad\langle I\rangle=Rad\langle M\rangle$, we have shown two algorithms for finding a unique decomposition of the ideal I as an irredundant finite intersection of parameter ideals.

Works Cited

Anderson, Frank W, and Kent R. Fuller. Ring and Categories of Modules. New York: Springer, 1992.

Atiyah, M. F. and I.G. MacDonald. Introduction to Commutative Algebra. Reading: Perseus, 1969.

Anton, Howard. Elementary Linear Algebra. New York: Wiley, 1991.

Cox, David. John Little, and Conal O'Shea. Ideals, Varieties, and Algorithms. New York: Springer, 1997.

Eisenbud, David. Commutative Algebra with a View Toward Algebraic Geometry. New York: Springer, 1995.

Fraleigh, John B. A First Course in Abstract Algebra. Reading: Addison-Wesley, 1989.

Greuel, Gert-Martin, and Gerhard Pfister. A Singular Introduction to Commutative Algebra. Berlin: Springer, 2002.

Grillet, Pierre. Algebra. New York: Wiley, 1999.

Heinzer, William, L. J. Ratliff, Jr., and Kishor Shah. "Parametric Decomposition of Monomial Ideals." Houston Journal of Mathematics 21 (1995): 29-52.

Hungerford, Thomas W. Algebra. New York: Springer, 1974.

Kunz, Ernst. Introduction to Commutative Algebra and Algebraic Geometry. Boston: Birhauser, 1985.

Matsumura, Hideyki. Commutative Ring Theory. Cambridge: Cambridge UP, 1992.

Osofsky, Barbara L. "Noether Lasker Primary Decomposition Revisited." The American Mathematical Monthly 101 (October 1994): 759-768.

Shapiro, Louis. Introduction to Abstract Algebra. New York: McGraw-Hill, 1975.

Stewart, Hall, and David Tall. Algebraic Number Theory. London: Chapman, 1979.

Taylor, Diana. "Ideals Generated By Monomials in an R-Sequence." Ph.D. diss., U. Chicago, 1966.

Zariski, Oscar, and Pierre Samuel, Commutative Algebra. Princeton: Van Nostrand Co., 1958.