4-21-2009

Primary Decomposition and Secondary Representation of Modules over a Commutative Ring

Muslim Baig

PRIMARY DECOMPOSITION AND SECONDARY REPRESENTATION OF MODULES OVER A COMMUTATIVE RING

by

MUSLIM BAIG

Under the Direction of Dr. Florian Enescu

ABSTRACT

This paper presents the theory of Secondary Representation of modules over a commutative ring and their Attached Primes; introduced in 1973 by I. MacDonald as a dual to the important theory of associated primes and primary decomposition in commutative algebra. The paper explores many of the basic aspects of the theory of primary decomposition and associated primes of modules in the hopes to delineate and motivate the construction of a secondary representation, when possible. The thesis discusses the results of the uniqueness of representable modules and their attached primes, and, in particular, the existence of a secondary representation for Artinian modules. It concludes with some interesting examples of both secondary and representable modules, highlighting the consequences of the results thus established.

INDEX WORDS: Secondary representation, Attached primes, Primary decomposition, Associated primes, Inverse limit, p-adic numbers

PRIMARY DECOMPOSITION AND SECONDARY REPRESENTATION OF MODULES OVER A COMMUTATIVE RING

by

MUSLIM BAIG

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of

Master of Science

in the College of Arts and Sciences

Georgia State University

2009

PRIMARY DECOMPOSITION AND SECONDARY REPRESENTATION OF MODULES OVER A COMMUTATIVE RING

by

MUSLIM BAIG

Committee Chair: Dr. Florian Enescu

Committee: Dr. Yongwei Yao
Dr. Imre Patyi

Electronic Version Approved:

Office of Graduate Studies
College of Arts and Sciences
Georgia State University
May 2009

DEDICATION

In loving memory of my Dad. May you find all the answers you sought.

ACKNOWLEDGEMENTS

I am deeply grateful to all of the people who helped me realize this thesis. Without the dedication and patience of my advisor, Dr. Florian Enescu, this paper would not have come to be. I would also like to thank Drs. Imre Patyi and Yongwei Yao, for their extremely helpful feedback in helping edit this paper. Of course, thanks are due to all the participants of our commutative algebra seminar, for their insightful questions and encouragement.

Finally, my deepest thanks to Irina Nikiforova for being an unflinching source of inspiration and motivation, my role-model.

TABLE OF CONTENTS

Chapter 1

Introduction: Ring and Module Theory Background

The theory of secondary representations can be thought of as a dual of the theory of primary decomposition in a module over a commutative ring. Both theories in some sense go all the way back to the work of Kummer, in the 19^{th} century, on the ring of algebraic integers. Kummer showed, in our setting, that every ideal in a ring of algebraic integers is uniquely (up to order) a product (or intersection) of prime ideals. (Note: α is an algebraic integer if there exists a monic polynomial $p(t)$ with integer coefficients such that $p(\alpha) = 0$. The algebraic integers form a ring.) The next challenge was to try to extend the factorization of ideals due to Kummer to polynomial rings, the natural setting of algebraic geometry. Emmanuel Lasker in 1905, found that every ideal in a polynomial ring is the intersection of primary ideals. The result is the best one can hope for in general. For instance, the ideal in $k[X, Y]$, k a field, generated by X^2 and Y^2 is neither the intersection nor the product of prime ideals. Primary ideals were a sort of generalization of prime ideals. Noether in 1921 simplified and generalized this result.

We begin the first chapter by reviewing the salient aspects of ring and module theory needed to describe the theory of primary decomposition for these objects. Once the fundamentals have been established, in Chapter 2 we define and explore the primary decomposition of these objects, identifying the various consequences of the construction and introducing the very important notion of the associated prime ideals of a ring and module. Finally, in Chapter 3 we "dualize" the theory of primary decomposition, introducing the secondary

representations of modules over a commutative ring and their attached primes. The chapter also studies Artinian modules recognizing them as the raison d'être of the new construction. The chapter concludes with some interesting examples of both secondary and representable modules, highlighting the consequences of the results thus established.

1.1 Primary Submodules and Ideals

Note: all rings throughout this paper will be commutative, with identity element, and all modules will be unital.

Definition 1.1.1. If N is a submodule of the R-module M, and $a \in R$, let $f_a : M/N \to M/N$ be multiplication by a. Then N is a *primary submodule* of M if N is proper and for every a, f_a is either injective or nilpotent.

Injectivity means that for all $x \in M$, we have $ax \in N \Rightarrow x \in N$. Nilpotence means that for some positive integer n, $a^n M \subseteq N$, that is, a^n belongs to the annihilator of M/N, $Ann_R(M/N)$. Equivalently, a belongs to the radical of the annihilator of M/N, $\sqrt{Ann_R(M/N)}$.

Remark 1.1.2. Note that f_a cannot be both injective and nilpotent. If so, then nilpotence gives $a^n M = a(a^{n-1}M) \subseteq N$, and injectivity gives $a^{n-1}M \subseteq N$. Inductively then $M \subseteq N$, so $M = N$, contradicting the assumption that N was proper. Thus, if N is a primary submodule of M, then $\sqrt{Ann_R(M/N)}$ is the set of all $a \in R$ such that f_a is not injective. Since $\sqrt{Ann_R(M/N)}$ is the radical of an ideal, it is an ideal of R, and in fact it is a prime ideal. For if f_a and f_b fail to be injective, then so does $f_{ab} = f_a \circ f_b$. If $P = \sqrt{Ann_R(M/N)}$, then we say that N is *P-primary.*

If I is an ideal of R, then $\sqrt{Ann_R(R/I)} = \sqrt{I}$, because $Ann_R(R/I) = I$. (Note that $a \in Ann_R(R/I)$ iff $aR \subseteq I$ iff $a = a1 \in I$.)

Definition 1.1.3. Let $M = R$, replacing a by y above, we define a *primary ideal* in a ring R as a proper ideal Q such that if $xy \in Q$, then either $x \in Q$ or $y^n \in Q$ for some $n \geq 1$.

Equivalently, $R/Q \neq 0$ and every zero-divisor in R/Q is nilpotent.

Lemma 1.1.4. *Let I be an ideal of R and define $V(I)$ to be the set of prime ideals of R containing I, $V(I) = \{P \in Spec(R) : P \supseteq I\}$. Then $\sqrt{I} = \bigcap_{P \in V(I)} P = \bigcap_{P \in Spec(R)} P$.*

Proof. Let $a \in \sqrt{I}$ and let $P \in V(I)$. Then there exists $n \geq 1$ such that $a^n \in I \subseteq P$, so that, since P is prime, $a \in P$. Hence, $\sqrt{I} \subseteq \bigcap_{P \in V(I)} P$. To get the reverse inclusion, let $b \in \bigcap_{P \in V(I)} P$. Suppose that $b \notin \sqrt{I}$. Which means that $I \cap S = \emptyset$, where $S = \{b^n : n \geq 1\}$, a multiplicatively closed subset of R. Then, by Zorn's Lemma there exists a prime ideal P' of R such that $I \subseteq P'$ and $P' \cap S = \emptyset$. It follows that $P' \in V(I)$, so that $b \in P' \cap S$, a contradiction. □

Lemma 1.1.5. *Let Q be a primary ideal of R. Then $P = \sqrt{Q}$ is a prime ideal of R, and we say Q is P-primary. Furthermore, P is the unique minimal prime ideal of Q.*

Proof. Since $1 \notin Q$ we have that $1 \notin \sqrt{Q} = P$, so that P is proper. Now, suppose $a, b \in R$ with $ab \in \sqrt{Q}$, but $a \notin \sqrt{Q}$. Thus $\exists n \in \mathbb{N}$ such that $(ab)^n = a^n b^n \in Q$; however, no positive power of a belongs to Q, and so $\nexists m > 0$ such that $(a^n)^m \notin Q$. Since Q is primary, we see that $b^n \in Q$, so $b \in \sqrt{Q}$. Hence, $P = \sqrt{Q}$ is prime. Next, if $P' \in Spec(R)$ and $P' \supseteq Q$, then we can take radicals and see that $P' = \sqrt{P} \supseteq \sqrt{Q} = P$. Hence P is the unique minimal prime ideal of Q. □

Lemma 1.1.6. *If P is a prime ideal, then $\sqrt{P^n} = P$ for all $n \geq 1$.*

Proof. By Lemma 1.1.4 the radical of P^n is the intersection of all prime ideals containing P^n, one of which is P. Thus $\sqrt{P^n} \subseteq P$. Conversely, if $x \in P$, then $x^n \in P^n$, so $x \in \sqrt{P^n}$. □

Lemma 1.1.7. *If $\sqrt{I}$ is a maximal ideal M, then I is M-primary.*

Proof. Suppose that $ab \in I$ and $b \notin \sqrt{I} = M$. Then by the maximality of M, it follows that $M + Rb = R$, so for some $m \in M$ and $r \in R$ we have $m + rb = 1$. Now $m \in M = \sqrt{I}$, hence $m^k \in I$ for some $k \geq 1$. Thus $1 = 1^k = (m + rb)^k = m^k + sb$ for some $s \in R$. Multiplying by a gives $a = am^k + sab \in I$, since $ab \in I$. □

Corollary 1.1.8. *If M is a maximal ideal, then M^n is M-primary for every $n \geq 1$.*

Proof. Recalling our observation from Lemma 1.1.6, $\sqrt{M^n} = M$, together with Lemma 1.1.7 the corollary follows. □

Definition 1.1.9. An *integral domain* is a commutative ring with no zero divisors. A *principal ideal domain* (PID) is an integral domain in which every ideal is principal, that is, generated by a single element.

Example 1.1.10. Let R be a PID which is not a field. Then the set of all primary ideals of R is $\{0\} \cup \{Rp^n : p \text{ an irreducible element of } R, n \geq 1\}$.

Proof. Since $0 \in Spec(R)$, (as R is a domain), for an irreducible element p of R and $n \geq 1$, the ideal Rp^n is a power of a maximal ideal of R and so is a primary ideal of R. On the other hand, a non-zero primary ideal of R must have the form Ra, for some non-zero $a \in R$, and a cannot be a unit since a primary ideal is proper. We write a as product of irreducible elements of R. If a were divisible by two non-associate irreducible elements p, q of R, then Rp and Rq would be distinct maximal ideals of R and minimal prime ideals of Ra, contradicting Lemma 1.1.5. It follows that Ra is generated by a positive power of some irreducible elements of R. □

Note, however, that not every M-primary ideal, where M is a maximal ideal of a commutative ring R, has to be a power of M, consider the following example.

Example 1.1.11. Let $R = k[x, y]$, the ring of polynomials in indeterminates x, y over the field k. Let $M = Rx + Ry$, a maximal ideal of R. Then, (x, y^2) is an M-primary ideal of R which is not a power of a prime ideal of R.

Proof. We have $M^2 = (x^2, xy, y^2) \subseteq (x, y^2) \subseteq (x, y) = M$, so on taking radical we get, $M = \sqrt{(M^2)} \subseteq \sqrt{(x, y^2)} \subseteq \sqrt{M} = M$. Hence, $\sqrt{(x, y^2)} = M$, a maximal ideal of R, and so it follows from Corollary 1.1.8 that (x, y^2) is M-primary. Now, (x, y^2) is not a positive power of a prime ideal P of R, otherwise, $P = M$ by Lemma 1.1.6 and since the powers of M form

a descending chain $M \supseteq M^2 \supseteq \ldots \supseteq M^i \supseteq M^{i+1} \supseteq \ldots$, we should have that $(x, y^2) = M$ or M^2; both which do not hold since $x \notin M^2$, and $y \notin (x, y^2)$ (since otherwise $y = xf + y^2 g$, for some $f, g \in R$, and evaluation of x, y at $0, y$ leads to a contradiction). □

Definition 1.1.12. Let M be an R-module, and suppose we have an increasing sequence of submodules $M_1 \subseteq M_2 \subseteq M_3 \subseteq \ldots$, or a decreasing sequence $M_1 \supseteq M_2 \supseteq M_3 \supseteq \ldots$. We say that the sequence *stabilizes* if for some t, $M_t = M_{t+1} = M_{t+2} = \ldots$. The module M is said to satisfy the *ascending chain condition (ACC)* if every increasing sequence of submodules stabilizes; M satisfies the *descending chain condition (DCC)* if every decreasing sequence of submodules stabilizes.

Proposition 1.1.13. *The following conditions on a R-submodule M are equivalent, and define a Noetherian module:*

(1) *M satisfies the ACC;*

(2) *Every nonempty collection of submodules has a maximal element (with respect to inclusion).*

The following conditions on M are equivalent, and define an Artinian module:

(1) *M satisfies the DCC;*

(2) *Every nonempty collection of submodules of M has a minimal element.*

Proof. Assume (1) and let S be a nonempty collection of submodules. Choose an $M_1 \in S$. If M_1 is maximal, we are done; otherwise we have $M_1 \subsetneq M_2$ for some $M_2 \in S$. If we continue inductively, the process must terminate at a maximal element; otherwise the ACC condition would be violated.

Conversely, assume (2), and let $M_1 \subseteq M_2 \subseteq M_3 \subseteq \ldots$. The sequence must stabilize; otherwise $\{M_1, M_2, M_3, \ldots\}$ would be a nonempty collection of submodules with no maximal element. The proof for the Artinian case is identical, with all inclusions reversed. □

There is another equivalent condition in the Noetherian case.

Proposition 1.1.14. *M is Noetherian if and only if every submodule of M is finitely generated.*

Proof. If the sequence $M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots$ does not stabilize, let $N = \bigcup_{i=1}^{\infty} M_i$. Then N is a submodule of M, and it cannot be finitely generated. For if $x_1, \dots, x_s$ generate N, then for sufficiently large t, all the x_i belong to M_t. But then $N \subseteq M_t \subseteq M_{t+1} \subseteq \dots \subseteq N$, so $M_t = M_{t+1} = \dots$. Conversely, assume that ACC holds, and let $N \subseteq M$. If $N \neq 0$, choose $x_1 \in N$. If $Rx_1 = N$, then N is finitely generated. Otherwise, there exists $x_2 \notin Rx_1$. If x_1 and x_2 generate N, we are done. Otherwise, there exists $x_3 \notin Rx_1 + Rx_2$. The ACC forces this process to terminate at some stage t, in which case $x_1, \dots, x_t$ generate N. □

Remark 1.1.15. The analogous equivalent condition in the Artinian case is that every quotient module M/N is *finitely cogenerated*, that is, if the intersection of a collection of submodules of M/N is 0, then there is a finite subcollection whose intersection is 0.

Definition 1.1.16. If M is an R-module and S a multiplicative subset of R, then we can essentially repeat the construction of the ring of fractions to form the *localization* $S^{-1}M$ of M by S, and thereby divide elements of M by elements of S. If $x, y \in M$ and $s, t \in S$, we call the ordered pairs (x, s) and (y, t) equivalent if for some $u \in S$, $u(tx - sy) = 0$. The equivalence class of (x, s) is denoted by x/s, and addition is defined by

$$\frac{x}{s} + \frac{y}{t} = \frac{tx + sy}{st}$$

If $a/s \in S^{-1}R$ and $x/s \in S^{-1}M$, we define

$$\frac{a}{s}\frac{x}{t} = \frac{ax}{st}$$

In this way, $S^{-1}M$ becomes an $S^{-1}R$-module.

Chapter 2

Primary Decomposition and Associated Primes

2.1 Primary Decomposition

Definition 2.1.1. A *primary decomposition* of the submodule N of M is given by $N = \bigcap_{i=1}^{r} N_i$, where the N_i are P_i-primary submodules. The decomposition is *reduced* if the P_i are distinct and N cannot be expressed as the intersection of a proper subcollection of the N_i.

Remark 2.1.2. A reduced primary decomposition can always be extracted from an unreduced one, by discarding those N_i that contain $\bigcap_{j \neq i} N_j$ and intersecting those N_i that are P-primary for the same P.

Lemma 2.1.3. *If $N_1, \ldots, N_k$ are P-primary, then $\bigcap_{i=1}^{k} N_i$ is P-primary.*

Proof. Without loss of generality, we may assume that $k = 2$, since an induction argument essentially takes care of larger values of k. Let $N = N_1 \cap N_2$ and $\sqrt{Ann_R(N_1)} = \sqrt{Ann_R(N_2)} = P$. Assume for the moment that $\sqrt{Ann_R(N)} = P$. If $a \in R$, $x \in M$, $ax \in N$, and $a \notin \sqrt{Ann_R(N)}$, then since N_1 and N_2 are P-primary, we have $x \in N_1 \cap N_2 = N$. We next show that $\sqrt{Ann_R(N)} = P$. If $a \in P$, then there are positive integers n_1 and n_2 such that $a^{n_1} M \subseteq N_1$ and $a^{n_2} M \subseteq N_2$. Therefore, $a^{n_1+n_2} M \subseteq N$, so $a \in \sqrt{Ann_R(N)}$. Conversely, if $a \in \sqrt{Ann_R(N)}$ then a belongs to $\sqrt{Ann_R(N_i)}$ for $i = 1, 2$, and therefore $a \in P$. $\square$

We now prove that every submodule of a Noetherian module has a primary decomposition.

Definition 2.1.4. The proper submodule N of M is *irreducible* if N cannot be expressed as $N_1 \cap N_2$ with N properly contained in the submodules $N_i, i = 1, 2$.

Proposition 2.1.5. *If N is an irreducible submodule of the Noetherian module M, then N is primary.*

Proof. Suppose not, then for some $a \in R$, $f_a : M/N \to M/N$ is neither injective nor nilpotent. The chain $ker(f_a) \subseteq ker(f_a^2) \subseteq ker(f_a^3) \subseteq \ldots$ terminates by the ascending chain condition, say at $ker(f_a^i)$. Let $\varphi = f_a^i$; then $ker(\varphi) = ker(\varphi^2)$ and we claim that $ker(\varphi) \cap im(\varphi) = 0$. Suppose $x \in ker(\varphi) \cap im(\varphi)$, and let $x = \varphi(y)$. Then $0 = \varphi(x) = \varphi^2(y)$, so $y \in ker(\varphi^2) = ker(\varphi)$, so $x = \varphi(y) = 0$.

Now f_a is not injective, so $ker(\varphi) \neq 0$, and f_a is not nilpotent, so f_a^i cannot be 0 (since $a^i M \nsubseteq N$). Consequently, $im(\varphi) \neq 0$.

Let $g : M \to M/N$ be a canonical epimorphism, and set $N_1 = g^{-1}(ker(\varphi))$, $N_2 = g^{-1}(im(\varphi))$. We next show that $N = N_1 \cap N_2$. If $x \in N_1 \cap N_2$, then $g(x)$ belongs to both $ker(\varphi)$ and $im(\varphi)$, so $p(x) = 0$, in other words, $x \in N$. Conversely, if $x \in N$, then $p(x) = 0 \in ker(\varphi) \cap im(\varphi)$, so $x \in N_1 \cap N_2$.

Finally, we show that N is properly contained in both N_1 and N_2, so N is reducible, a contradiction. Pick a nonzero element $y \in ker(\varphi)$. Since g is surjective, there exists $x \in M$ such that $p(x) = y$. Thus, $x \in p^{-1}(ker(\varphi)) = N_1$ (since $y = p(x) \in ker(\varphi)$), but, $x \notin N$ (because $p(x) = y \neq 0$). Similarly, $N \subset N_2$ (with $0 \neq y \in im(\varphi)$), and the result follows. □

Theorem 2.1.6. (Existence Theorem) *Every proper submodule of the Noetherian module M has a primary decomposition, hence a reduced primary decomposition.*

Proof. We show that any proper submodule can be expressed as a finite intersection of irreducible submodules of M, so that Proposition 2.1.5 applies. Let S be the collection of all submodules of M that cannot be expressed in this form. If S is nonempty then S has

a maximal element N (since M is Noetherian). By the definition of S then N must be reducible, so we can write $N = N_1 \cap N_2$, $N \subset N_1$, $N \subset N_2$. By maximality of N, N_1 and N_2 can be expressed as finite intersections of irreducible submodules, hence so can N, contradicting $N \in S$. Thus, S is empty. □

2.2 Associated Primes

Definition 2.2.1. Let M be an R-module, and P a prime ideal of R. We say that P is an *associated prime* of M (or that P is *associated* to M) if P is the annihilator of some nonzero $x \in M$. The set of associated primes of M is denoted by $Ass(M)$.

Proposition 2.2.2. *The prime ideal P is associated to M if and only if there is an injective R-module homomorphism from R/P to M. Therefore, if N is a submodule of M, then $Ass(N) \subseteq Ass(M)$.*

Proof. If P is the annihilator of $x \neq 0$, the required homomorphism is given by $r + P \mapsto rx$. Conversely, if an injective R-homomorphism from R/P to M exists, let x be the image of $1 + P$, which is nonzero in R/P. By injectivity, $x \neq 0$. We show that $P = Ann(x)$, the set of elements $r \in R$ such that $rx = 0$. If $r \in P$, then $r + P = 0$, so $rx = 0$, and therefore $r \in Ann(x)$. If $rx = 0$, then by injectivity, $r + P = 0$, so $r \in P$. □

Associated primes exist under wide conditions, and are sometimes unique.

Proposition 2.2.3. *Let M be an R-module. If $M = 0$, then $Ass(M)$ is empty. The converse is true if R is Noetherian.*

Proof. There are no nonzero elements in the zero module, hence no associated primes. Assuming that $M \neq 0$ and R is Noetherian, there is a maximal element $I = Ann(x)$ in the collection of all annihilators of nonzero elements of M. The ideal I is proper, otherwise, if $I = R$, then $x = 1x = 0$, a contradiction. Let $ab \in I$ with $a \notin I$. Then $abx = 0$ but $ax \neq 0$, so $b \in Ann(ax)$. But, $I = Ann(x) \subseteq Ann(ax)$, and the maximality of I gives $I = Ann(ax)$. Consequently, $b \in I$. Thus, I is prime and we have that $I \in Ass(M)$, as desired. □

Proposition 2.2.4. *For any prime ideal P, $Ass(R/P) = \{P\}$.*

Proof. By (2.2.2), P is an associated prime of R/P because there certainly is an injective R-homomorphism from R/P to itself. If $Q \in Ass(R/P)$, we must show that $Q = P$. Suppose that $Q = Ann(r + P)$ with $r \notin P$. Then $s \in Q$ iff $sr \in P$ iff $s \in P$ (because P is prime). □

The next result gives us information about the elements that belong to associated primes.

Theorem 2.2.5. *Let $Z(M)$ be the set of zero-divisors of M, that is, the set of all $r \in R$ such that $rx = 0$ for some nonzero $x \in M$. Then $\bigcup\{P : P \in Ass(M)\} \subseteq Z(M)$, with equality if R is Noetherian.*

Proof. Inclusion follows from the definition (2.2.1) of associated prime. Thus, we assume $a \in Z(M)$, with $ax = 0$, $x \in M$, $x \neq 0$. Then $Rx \neq 0$, so by (2.2.3), Rx has an associated prime $P = Ann(bx)$. Since $ax = 0$ we have $abx = 0$, so $a \in P$. But $P \in Ass(Rx) \subseteq Ass(M)$ by (2.2.2). Therefore, $a \in \bigcup\{P : P \in Ass(M)\}$. □

Proposition 2.2.6. *If N is a submodule of M, then $Ass(M) \subseteq Ass(N) \cup Ass(M/N)$.*

Proof. Let $P \in Ass(M)$, and let $h : R/P \to M$ be an injective homomorphism. Set $H = h(R/P)$ and $L = H \cap N$. If $L = 0$, then the map from H to M/N given by $h(r + P) \mapsto h(r + P) + N$ is injective. (If $h(r + P)$ belongs to N, it must belong to $H \cap N = 0$.) Thus H is isomorphic to a submodule of M/N, so by definition of H, there is an injective map from R/P to M/N. Thus $P \in Ass(M/N)$. If $L \neq 0$ and if L has a nonzero element x, then x must belong to both H and N, and H is isomorphic to R/P via h. Thus, $x \in N$ and the annihilator of x coincides with the annihilator of some nonzero element of R/P. So $Ann(x) = P$, and $P \in Ass(N)$. □

Corollary 2.2.7. $Ass(\bigoplus_{j\in J} M_j) = \bigcup_{j\in J} Ass(M_j)$

Proof. Proposition 2.2.2 gives $\bigcup_{j\in J} Ass(M_j) \subseteq Ass(\bigoplus_{j\in J} M_j)$. The reserve containment follows from Proposition 2.2.6 when the index set is finite.

$$\begin{aligned} Ass(M_1 \oplus M_2 \oplus M_3) &\subseteq Ass(M_1) \cup Ass(M/M_1) \\ &= Ass(M_1) \cup Ass(M_2 \oplus M_3) \\ &= Ass(M_1) \cup Ass(M_2) \cup Ass(M_3) \end{aligned}$$

In general, if P is an associated prime of the direct sum, then there is an injective homomorphism from R/P to $\bigoplus M_j$. The image of the monomorphism is contained in the direct sum of finitely many components, as R/P is generated as an R-module by the single element $1 + P$. This takes us back to the finite case. □

We now establish the connection between associated primes and primary decomposition, and show that under wide conditions, there are only finitely many associated primes.

Theorem 2.2.8. *Let M be a nonzero finitely generated module over the Noetherian ring R, so that by Theorem 2.1.6, every proper submodule has a reduced primary decomposition. In particular, the zero module can be expressed as $\bigcap_{i=1}^{r} N_i$, where N_i is P_i-primary. Then $Ass(M) = \{P_1, \ldots, P_r\}$, a finite set.*

Proof. Let P be an associated prime of M, so that $P = Ann(x)$, $x \neq 0$, $x \in M$. We renumber the N_i so that $x \notin N_i$ for $1 \leq i \leq j$ and $x \in N_i$ for $j + 1 \leq i \leq r$. Since N_i is P_i-primary, we have $P_i = \sqrt{N_i}$. Since P_i is finitely generated, $P_i^{n_i} M \subseteq N_i$ for some $n_i \geq 1$. Therefore,

$$\left(\bigcap_{i=1}^{j} P_i^{n_i} \right) x \subseteq \bigcap_{i=1}^{r} N_i = (0)$$

so $\bigcap_{i=1}^{j} P_i^{n_i} \subseteq Ann(x) = P$. Since P is prime, $P_i \subseteq P$ for some $i \leq j$. We claim that $P_i = P$, so that every associated prime must be one of the P_i. Let $a \in P$, then $ax = 0$ and $x \notin N_i$, so f_a is not injective and therefore must be nilpotent. Consequently, $a \in \sqrt{N_i} = P_i$, as claimed. Conversely, we now show that each P_i is an associated prime. Without loss of generality, we may take $i = 1$. Since the decomposition is reduced, N_1 does not contain the intersection of the other N_i's, so we can choose $x \in N_2 \cap \ldots \cap N_r$ with $x \notin N_1$. Now N_1 is P_1-primary, so as in the preceding paragraph, for some $n \geq 1$ we have $P_1^n x \subseteq N_1$ but $P_1^{n-1} x \nsubseteq N_1$.

(Consider $P_1^0 x = Rx$ and recall that $x \notin N_1$). Choose $y \in P_1^{n-1} x \setminus N_1$ (hence $y \neq 0$), then $P_1 y \subseteq P_1^n x \subseteq N_1$ and $x \in \bigcap_{i=2}^r N_i$, so $P_1^n x \subseteq \bigcap_{i=2}^r N_i$. Thus $P_1 y \subseteq \bigcap_{i=1}^r N_i = (0)$, so $P_1 \subseteq Ann(y)$. On the other hand, if $a \in R$ and $ay = 0$, then $ay \in N_1$ but $y \notin N_1$, so $f_a : M/N_1 \to M/N_1$ is not injective and is therefore nilpotent. Thus, $a \in \sqrt{N_1} = P_1$. □

We now discuss the uniqueness of primary decompositions.

Theorem 2.2.9. *Let M be a finitely generated module over the Noetherian ring R. If $N = \bigcap_{i=1}^r N_i$ is a reduced primary decomposition of the submodule N, and N_i is P_i-primary, $i = 1, \ldots, r$, then (assuming M and R fixed) the P_i are uniquely determined by N.*

Proof. By the correspondence theorem, a reduced primary decomposition of (0) in M/N is given by $(0) = \bigcap_{i=1}^r N_i/N$, and N_i/N is P_i-primary, $1 \leq i \leq r$. By Theorem 2.2.8, $Ass(M/N) = \{P_1, \ldots, P_r\}$. But (see Definition 2.2.1) the associated primes of M/N are determined by N. □

Remark 2.2.10. Theorems 2.2.8 & 2.2.9 together are sometimes referred to as the First Uniqueness Theorem for Primary Decomposition.

Definition 2.2.11. A subset Σ of $Ass(M)$ is said to be *isolated* if, for each $P \in \Sigma$, every $Q \in Ass(M)$ such that $Q \subset P$ belongs to Σ. Otherwise, we say Σ is *embedded*.

Theorem 2.2.12. (Second Uniqueness Theorem) *If $\{P_{i_1}, \ldots, P_{i_r}\}$ is an isolated subset of $Ass(M)$, then the submodule $Q_{i_1} \cap \ldots \cap Q_{i_r}$ is independent of the decomposition chosen.*

Proof. Let N be a decomposable submodule of M, with reduced primary decomposition $N = \bigcap_{j=1}^r Q_j$. Suppose Σ is an isolated set of prime ideals belonging to N, where $P_i = \sqrt{Ann(Q_i)}$. Define $Q = \bigcap_{P_i \in \Sigma} Q_i$. Clearly, $S = R - \bigcup_{P_i \in \Sigma} Q_i$ is a multiplicatively closed subset of R. Then Q depends only on Σ, and is independent of the minimal primary decomposition of N. In particular, the isolated components of N are uniquely determined. □

Chapter 3

Secondary Representation and Attached Primes

3.1 Secondary Representation

Our presentation and treatment of secondary representation and attached primes closely follows the one in MacDonald [7].

Definition 3.1.1. An R-module M is said to be secondary if $M \neq 0$ and if, for each $x \in R$, the endomorphism $\varphi_{x,M} : M \to M$ defined by multiplication by x, is either *surjective* or *nilpotent*.

Claim 3.1.2. If an R-module M is secondary, then $nilradical(M) = \sqrt{Ann_R(M)}$ is a prime ideal p.

Proof. For $a, b \in R$, let $ab \in \sqrt{Ann_R(M)} \Rightarrow (ab)^n M = 0_M$ for some $n > 0$. If $b \notin \sqrt{Ann_R(M)} \implies b$ is surjective, that is $b^n M = M$. Then, $a^n M = a^n(b^n M) = (ab)^n M = 0_M$ $\implies a$ is nilpotent. Thus, $a \in \sqrt{Ann_R(M)}$ and $nilradical(M)$ is prime. □

Definition 3.1.3. Following Claim 3.1.2, M is said to be *p-secondary*.

To discuss the uniqueness theorems we establish some lemmas.

Lemma 3.1.4. *Finite direct sums and non-zero quotients of p-secondary modules are p-secondary.*

Proof. Let $M = N_1 \oplus N_2$ be a finite direct sum of two p-secondary modules, with $p = \sqrt{Ann_R(N_1)} = \sqrt{Ann_R(N_2)}$. Let $x \in R$, assume x is not surjective. That is, $x(N_1 \oplus N_2) \neq (N_1 \oplus N_2)$ which implies that either $xN_1 \neq N_1$ or $xN_2 \neq N_2$. Suppose $xN_1 \neq N_1$ then $\exists k > 0$ such that $x^k N_1 = 0$, which implies $x^k \in Ann_R(N_1) \Rightarrow x \in p = \sqrt{Ann_R(N_1)}$. But this means that $\exists l > 0$ such that $x^l \in Ann(N_2)$, that is $x^l N_2 = 0$. So taking $n = max\{k, l\}$, then $x^n(N_1 \oplus N_2) = 0$. Thus, M is secondary. To show that M is p-secondary, let $ab \in \sqrt{Ann_R(M)}$, which means that $\exists n > 0$ such that $(ab)^n M = (ab)^n(N_1 \oplus N_2)$. But N_1, N_2 were p-secondary, so either $a \in p = \sqrt{Ann_R(N_i)}$ or $b \notin p$, that is a is nilpotent if b is surjective. From Claim 3.1.2 we have M is p-secondary.

Next let M be p-secondary, so that $p = \sqrt{Ann_R(M)}$. Let $\varphi : M \to M' = \frac{M}{N}$ be the natural projection from M to a non-zero quotient of M. Let $x \in R$, with $\varphi_{x,M}$ surjective, that is $xM = M$ which implies $xM' = M'$ as $xM + N = M$. Otherwise, $\exists k > 0$ such that $x^k M = 0 \implies x^k M' = 0_{M'} \iff x^k M + N = N$ as $x^k M = 0$. This also shows that $x^k \in Ann_R(M/N) \implies x \in \sqrt{Ann_R(M/N)}$. Then, as before $\sqrt{Ann_R(M')} = p$ which implies that M' is p-secondary. □

Remark 3.1.5. The result of Lemma 3.1.4 cannot in general be extended to infinite direct sums of p-secondary modules, see Examples 3.2.19 & 3.2.20.

Lemma 3.1.6. *The annihilator of a p-secondary module is a p-primary ideal.*

Proof. Finally, let $Ann_R(M) = I$ with M p-secondary. Let $ab \in I$ and assume $b^n \notin I$, $\forall n$. Then for $b \in R$ either $bM = M$ or $\exists n > 0$ such that $b^n \in Ann_R(M)$ which we assumed otherwise, so $bM = M$. Thus, $ab \in I \implies abM = 0 \implies aM = 0 \implies a \in I$. Thus, I is primary. Since $p = \sqrt{Ann_R(M)} = \sqrt{I} \implies I$ is p-primary. □

Example 3.1.7. If R is an integral domain, its quotient field K is a (0)-secondary R-module.

If R is a local ring with maximal ideal P and if every element of P is nilpotent, then R itself is a P-secondary R-module.

Lemma 3.1.8. *Let M be an R-module, p a prime ideal of R and let $M_1, \ldots, M_r$ be p-secondary submodules of M. Then $S = M_1 + \ldots + M_r$ is p-secondary.*

Proof. Each M_i is non-zero. Hence, S is non-zero. Since there exists a natural surjection of $M_1 \oplus \ldots \oplus M_r$ onto S, given by $(m_1, \ldots, m_r) \mapsto m_1 + \ldots + m_r$, S is a quotient of $M_1 \oplus \ldots \oplus M_r$. Hence, S is p-secondary. □

Definition 3.1.9. Let M be an R-module. Then a *secondary representation* of M is an expression of M as a sum of secondary submodules,

$$M = \sum_{i=1}^{n} N_i \tag{3.1}$$

By Lemma 3.1.8 we may assume that the prime ideals $p_i = \sqrt{Ann_R(N_i)}$ are all distinct, and then, by omitting redundant summands, that the representation is *minimal.* If M has a secondary representation then we say that M is *representable.*

3.2 Existence and Uniqueness of a Secondary Representation

3.2.1 First Uniqueness Theorem

Theorem 3.2.1. (First Uniqueness Theorem) *The set of prime ideals $\{p_1, \ldots p_n\}$ depends only on M and not on the minimal secondary representation. More precisely, the following conditions on a prime ideal p are equivalent:*

(1) *p is one of p_i.*

(2) *M has a p-secondary quotient module.*

(3) *M has a quotient Q such that $\sqrt{Ann_R(Q)} = p$.*

(4) *M has a quotient Q such that p is minimal in the set of prime ideals containing $Ann(Q)$.*

Proof. We first prove that (1), (2), (3) are equivalent.

(1)⇒(2). Let $P_i = \sum_{j \neq i} N_j$. Then since the representation is assumed to be minimal, we have $M/P_i \neq 0$, and, by the 2nd Isomorphism Theorem for Modules,

$$M/P_i = (P_i + N_i)/P_i \cong N_i/(N_i \cap P_i),$$

which in turn is p_i-secondary by Lemma 3.1.4.

(2)⇒(3). Clear from earlier comments.

(3)⇒(1). Let $Q = M/P$. We renumber the N_i so that $N_i \nsubseteq P$ for $1 \leq i \leq r$ and $N_i \subset P$ for $r+1 \leq i \leq n$. Then,

$$M/P = \sum_{i=1}^{n} (N_i + P)/P = \sum_{i=1}^{r} (N_i + P)/P,$$

and $(N_i + P)/P \cong N_i/(N_i \cap P)$ is p_i-secondary for $1 \leq i \leq r$ by Lemma 3.1.6. Hence, $p = \sqrt{Ann_R(M/P)} = \bigcap_{i=1}^{r} \sqrt{Ann_R((N_i + P)/P)} = \bigcap_{i=1}^{r} p_i$ and therefore p is one of $p_i, \ldots, p_r$. □

Definition 3.2.2. The prime ideals $p_i, \ldots, p_r$ are called the *attached primes* of the representable R-module M, denoted $Att(M) = \{p_i, \ldots, p_n\}$. The minimal elements of $Att(M)$ are described as *isolated,* the others *embedded*. To complete the proof of Theorem 3.2.1 we establish the following two lemmas.

Lemma 3.2.3. *The annihilator a of M is a decomposable ideal in R, and*

$$Ass(R/a) \subset Att(M).$$

Proof. In the minimal secondary representation 3.1, let $q_i = Ann(N_i)$. Then by Lemma 3.1.6 q_i is a p_i-primary ideal and $a = \bigcap q_i$. □

Lemma 3.2.4. *Let Q be a quotient of M. Then Q is representable and*

$$Att(Q) \subset Att(M).$$

Proof. Let $Q = M/P$. Then $Q = \sum_{i=1}^{n}(N_i + P)/P$ and $(N_i + P)/P \cong N_i/(N_i \cap P)$ is either p_i-secondary or zero, by Lemma 3.1.4. □

We now complete the proof of the first uniqueness theorem for secondary representations.

Proof. (3)⇒(4). If Q is a quotient module of M then $p = \sqrt{Ann_R(Q)}$ and hence is the unique minimal element of the set of prime ideals containing $Ann_R(Q)$.

(4)⇒(1). By Lemma 3.2.4 Q is representable, hence $a = Ann_R(Q)$ is decomposable by Lemma 3.2.3, and we have $p \in Ass(R/a) \subset Att(Q) \subset Att(M)$. □

Similar to the case of primary decomposition the next result gives us information about the elements that belong to the attached primes of a representable R-module.

Theorem 3.2.5. *Let $x \in R$. Then*

(1) *$\varphi_{x,M}$ is surjective if and only if $x \notin \bigcup_{i=1}^{n} p_i$.*

(2) *$\varphi_{x,M}$ is nilpotent if and only if $x \in \bigcap_{i=1}^{n} p_i$.*

Proof. (1). If $x \notin \bigcup_{i=1}^{n} p_i$, then $xN_i = N_i$ for $1 \leq i \leq n$, hence $xM = M$. Conversely, if $x \in p_i$ for some i, then $x^r N_i = 0$ for some $r > 0$, hence $x^r M = \sum_{j=1}^{n} x^r N_j \subset \sum_{j \neq i} N_j \neq M$, and therefore, $xM \neq M$, that is, $\varphi_{x,M}$ is not surjective.

(2). $\varphi_{x,M}$ is nilpotent if and only if each φ_{x,N_i} is nilpotent, that is, if and only if $x \in p_i$ for $1 \leq i \leq n$. □

This result also provides an Artinian analogue of the fact that if N is a Noetherian R-module and $r \in R$, the r is a non-zerodivisor on N if and only if r lies outside all the associated prime ideals of N, recall if N is a Noetherian R-module then $\bigcup p_i = z(N)$ where $z(N)$ is the set of zerodivisors of N.

3.2.2 Second Uniqueness Theorem

Lemma 3.2.6. *Let S be a multiplicatively closed subset of R. Suppose that the attached primes p_i are indexed so that $p_i \cap S = 0$ for $1 \leq i \leq r$ and $p_i \cap S \neq 0$ for $r+1 \leq i \leq n$. Then the following submodules of M are equal:*

(1) $\bigcap_{x \in S} xM$,

(2) $\sum_{i=1}^{r} N_i$, and

(3) *the sum of all p-secondary submodules N of M such that $p \cap S = 0$.*

Proof. Let L_1, L_2, L_3 denote these three modules, respectively. We show $L_1 \subset L_2 \subset L_3 \subset L_1$. Choose $x_i \in p_i \cap S$ for $r+1 \leq i \leq n$, then for some sufficiently large integer k we have $x_i^k N_i = 0$ for $r+1 \leq i \leq n$. Let $x = \prod_{i>r} x_i^k \in S$. Then, $\bigcap_{x \in S} xM = L_1 \subset xM = \sum_{i=1}^{n} N_i = \sum_{i=1}^{r} N_i \subset L_2$. Next, $L_2 \subset L_3$ is clear from the definition. Now let N be a p-secondary submodule of M such that $p \cap S = 0$. For each $x \in S$ we have $N = xN \subset xM$, hence $N \subset L_1$, and therefore, $L_3 \subset L_1$. □

Let $S(M) = \bigcap_{x \in S} xM$, the submodule defined in Theorem 3.2.6. Then $S(M)$ is the analog of the "isolated component" in the theory of primary decomposition.

Theorem 3.2.7. (Second Uniqueness Theorem) *Let Σ be an isolated subset of $Att(M)$ and reindex the p_i so that $\Sigma = \{p_1, \ldots, p_r\}$. Then the submodule $\sum_{i=1}^{r} N_i$ is independent of the choice of of minimal secondary decomposition.*

Proof. Let $S = A - \bigcup_{i=1}^{r} p_i$. Then S satisfies the hypotheses of the Lemma 3.2.6 and therefore $\sum_{i=1}^{r} N_i = S(M)$ depends only on M and Σ. In particular, the isolated secondary components (those N_i such that p_i are isolated) are uniquely determine. N_i is then the unique largest p_i-secondary submodule of M. □

3.2.3 Existence Theorem

Definition 3.2.8. An R-module M is said to be *sum-irreducible* if $M \neq 0$ and the sum of any two proper submodules of M is always a proper submodule.

Lemma 3.2.9. *If M is Artinian and sum-irreducible, the M is secondary.*

Proof. Suppose M is not secondary. Then $\exists x \in R$, such that $M \neq xM$ and $x^n M \neq 0$ for all $n > 0$. Consider the following sequence of submodules $(x^n M)_{n\geq 0}$ of M, since M is Artinian, the sequence stabilizes, so that for some $p > 0$ we have $x^p M = x^{p+1} M = \ldots$. Let $M_1 = Ker(\varphi_{x^p,M})$ and $M_2 = x^p M$. Then, M_1 and M_2 are proper submodules of M. Note, $M_1 \neq 0$, otherwise, $x^p m = 0 \implies m = 0$, contradicting our earlier assumption. Similarly, $M_2 \neq M$, otherwise, since $x^p M = x^{p+1} M \implies \forall m$, $x^p m = x^{p+1} m'$ for some m'. Then, $x^p(m - xm') = 0$ which implies that $m = xm'$, that is, $M = xM$, again a contradiction. Let $u \in M$. Then $x^p u = x^{2p} v$ for some $v \in M$, hence, $x^p u - x^{2p} v = x^p(u - x^p v) = 0$ and $u - x^p v \in M_1 = Ker(\varphi_{x^p,M})$ since $x^p M \neq 0$, $\forall p > 0$. Therefore, $u \in M_1 + M_2$. Hence, $M = M_1 + M_2$, and therefore M is not sum-irreducible, a contradiction. □

Theorem 3.2.10. (Existence Theorem) *Every Artinian R-module has a secondary representation.*

Proof. Suppose M is an Artinian R-module which is not representable. Consider the set of nonzero submodules of M which is not representable. Since M is Artinian, this set has minimal element element N. By assumption, N is not secondary and $N \neq 0$, hence by Lemma 3.2.9, N is the sum of two strictly smaller submodules N_1, N_2. By the minimality of N, each N_i, $i = 1, 2$, is representable, and therefore so also is N, a contradiction. □

Remark 3.2.11. The proof in fact furnishes us with a representation of an Artinian module M as a sum of sum-irreducible submodules, $M = \sum_{i=1}^{m} S_i$ with S_i sum-irreducible submodules of M. If the S_i summands also happen to be irredundant $\forall i = 1, \ldots, m$, then the representation is *minimal.*

Theorem 3.2.12. *Let N be a representable submodule of M. Then*

$$Att(M/N) \subset Att(M) \subset Att(N) \cup Att(M/N).$$

Proof. The left-hand inclusion was shown in Lemma 3.2.4. To show the reverse inclusion, let $p \in Att(M)$ and let M/P be a p-secondary quotient of M. Consider $Q = P + N$. If $Q = M$, then $M/P = (P + N)/P \cong N/(N \cap P)$, hence N has a p-secondary quotient and therefore $p \in Att(N)$ by Theorem 3.2.1. If on the other hand $Q \neq M$, then M/Q is a quotient of M/P and is therefore p-secondary by Lemma 3.1.4; however, it is also a quotient of M/N, so that $p \in Att(M/N)$. □

Theorem 3.2.13. *Let $M_1, \ldots, M_r$ be representable R-modules. Then $M_1 \oplus \ldots \oplus M_r$ is representable and*

$$Att(M_1 \oplus \ldots \oplus M_r) = \bigcup_{i=1}^{r} Att(M_i).$$

Proof. It is clear that the direct sum is representable. The second assertion follows from Theorem 3.2.12, by induction on r. □

3.2.4 Examples of Representable and Secondary R-modules

We now explore some interesting examples of both secondary and representable R-modules stimulated by a remark in [7], highlighting consequences of the results established thus far. In what follows, unless otherwise noted, p will denote a prime integer.

Proposition 3.2.14. *Every representable module over a PID is a finite direct sum of secondary submodules.*

Proof. Let R be a PID, M a representable R-module and $M = M_1 + M_2 + \ldots + M_r$ a minimal secondary representation of M, where M_i are P_i-secondary submodules of M with $P_i = \sqrt{Ann_R(M_i)} = p_i\mathbb{Z}$. Then $M = M_1 \oplus M_2 \oplus \ldots \oplus M_r$ if and only if, for each i, $M_i \cap (M_1 + \ldots + \hat{M}_i + \ldots + M_r) = 0$, where $\hat{M}_i$ means that the term M_i is omitted from the

sum. Suppose not. Let $x = x_i \in M_i$ such that $x = \sum_{j\neq i}^{r} x_j$, where $x_j \in M_j$. Then, there exist integers $n_j \geq 1$, for $j \neq i$ such that $p_j^{n_j} x_j = 0 \implies \left(\prod_{j\neq i}^{r} p_j^{n_j}\right)\left(\sum_{j\neq i}^{r} x_j\right) = 0$. Let $d = \prod_{j\neq i}^{r} p_j^{n_j}$, then $dx = 0$. Since $p_i^{n_i} x = 0$ and $(d, p_i) = 1$, we have that $1 = ud + vp_i^{n_i}$ for some u, v. Thus, $x = 1x = udx + vp_i^{n_i} x = 0 + 0 = 0 \implies x = 0$. □

Proposition 3.2.15. *If R is an integral domain, then its quotient field K is a 0-secondary R-module.*

Proof. Let $\frac{a}{b} \in K$ with $a, b \in R$ and $b \neq 0$. Without loss of generality, suppose also $a \neq 0$, then for any $x \in R$, $x\frac{a}{b} = 0 \iff x = 0 \implies \sqrt{Ann_R(K)} = 0$. Next, $x\frac{a}{xb} = \frac{a}{b} \implies xK = K$ for all $x \in R$. Thus, K is 0-secondary. □

Example 3.2.16. $\mathbb{Q}$ is a 0-secondary $\mathbb{Z}$-module, and hence so is $\mathbb{Q}/\mathbb{Z}$.

Proof. Follows from Proposition 3.2.15, but we can also prove it explicitly. Let $n \in \mathbb{Z}$, $n \neq 0$ and $\frac{a}{b} \in \mathbb{Q}$, $b \neq 0$. Then, $n\frac{a}{nb} = \frac{a}{b} \implies n\mathbb{Q} = \mathbb{Q}$. Without loss of generality, we may also assume $a \neq 0$, then $n\frac{a}{b} = 0 \iff n = 0 \iff \sqrt{Ann(\mathbb{Q})} = 0$. Thus, $\mathbb{Q}$ is a 0-secondary. Finally, by Lemma 3.1.4 since $\mathbb{Q}/\mathbb{Z}$ is a non-zero quotient of $\mathbb{Q}$, $\mathbb{Q}/\mathbb{Z}$ is also a 0-secondary $\mathbb{Z}$-module. □

Proposition 3.2.17. *If P is a maximal ideal of R, then R/P^n is a P-secondary R-module for every $n > 0$.*

Proof. Let $x \in R$. If $x \in P$, then for any $\bar{r} \in R/P^n$ $\exists n > 0$ such that $x^n\bar{r} = x^n(r + P^n) = x^n r + P^n = P^n = \bar{0}$, where $r \in R$. Otherwise, if $x \notin P \implies (x) + P = R \iff \exists u, v \in R$ such that $ux + vp = 1$ for some $p \in P$, and moreover $ux + vp^n = 1$. Then for any $\bar{r} \in R/P^n$ we need to find an $\bar{s} \in R/P^n$ such that $x\bar{s} = \bar{r}$. Since $\bar{r} = \bar{r}\bar{1} = r1 + P^n = r(ux + vp^n) + P^n = xur + P^n$, so let $\bar{s} = \overline{ur}$. Thus, R/P^n is secondary. Finally, note that $\sqrt{Ann(R/P^n)} = P$ which gives R/P^n is P-secondary. □

Example 3.2.18. Let $R = \mathbb{Z}$ and $M = \mathbb{Z}/p^n\mathbb{Z}$. If $x \in \mathbb{Z}$ and $(x, p) = 1$ then $xM = M$. Otherwise, if $p \mid x$ then $x^n M = 0$. That is, M is a p-secondary $\mathbb{Z}$-module.

Proof. Follows from Proposition 3.2.17, but we prove it explicitly. Let $x \in \mathbb{Z}$. If $p \mid x \implies x = pk$. Let $\bar{m} \in M$, then $x^n\bar{m} = (pk)^n\bar{m} = p^nk^n\bar{m} = p^nk^nm + p^n\mathbb{Z} = p^n\mathbb{Z} \implies x^nM = 0$. If $(x,p) = 1 \implies p \nmid x$ and $(x,p^n) = 1$. Given $m \in M$ we need to find $m' \in M$ such that $xm' = m$. Now, $(x,p^n) = 1 \implies 1 = xa + p^nb \implies m = m1 = xma + p^nbm$, so let $m' = ma$, then $m = xm' + kp^n \iff m - xm' = kp^n \iff p^n \mid m - xm' \iff xm' = m$. Thus, M is p-secondary. □

Example 3.2.19. Let $R = \mathbb{Z}$ and $M = \bigoplus_p \mathbb{Z}/p\mathbb{Z}$. M is not representable as a $\mathbb{Z}$-module.

Proof. Suppose to the contrary. Let M is representable and $M = \sum_{i=1}^{n} N_i$ be a minimal secondary representation of M, then $Att(M) = \{p_1, \ldots, p_n\}$ where $p_i = \sqrt{Ann(N_i)}$. By the First Uniqueness Theorem (3.2.1) if M has quotient Q such that $\sqrt{Ann(Q)} = p$ then $p \in Att(M)$, that is, p is one of the p_i. So for any $Q = M/(\mathbb{Z}/p\mathbb{Z})$ p a prime, $\mathbb{Z}/p\mathbb{Z}$ from Example 3.2.18 is p-secondary and, thus, $\sqrt{Ann(Q)} = p \in Att(M)$, but, this is impossible as the $Att(M) \subsetneqq \bigcup_{p\, prime} Att(M/(\mathbb{Z}/p\mathbb{Z})) = \{2, 3, 5, \ldots\}$ as there are infinitely many p-secondary submodules $\mathbb{Z}/p\mathbb{Z}$ for each of which $\sqrt{Ann(M/(\mathbb{Z}/p\mathbb{Z}))} = p$ is a distinct prime. □

Example 3.2.20. Let $R = \mathbb{Z}$ and $M = \bigoplus_{n>0} \mathbb{Z}/p^n\mathbb{Z}$. M is not secondary as a $\mathbb{Z}$-module, further, M is not representable.

Proof. Let $\bar{1}_i$ denote the identity element of $\mathbb{Z}/p^i\mathbb{Z}$. Then, $x(0, \ldots 0, \bar{1}_n, 0, \ldots, 0) = 0 \iff \bar{x} = 0$ is in $\mathbb{Z}/p^n\mathbb{Z}$, that is, $p^n \mid x$, $\forall n > 0$ which implies that $x = 0$. Thus, $Ann_R(M) = 0$. Let $x \neq 0$. If $x = p$ then $pM \subseteq 0 \bigoplus_{n\geq 2} \mathbb{Z}/p\mathbb{Z} \subsetneqq M$. Thus, M is not secondary.

We show next that there does not exist a Q-secondary submodule N of M, where $Q \neq p\mathbb{Z}$. Let $N \leqslant M$, Q-secondary with $Q \neq p\mathbb{Z}$. Then, $p \notin Q = \sqrt{Ann_R(N)}$ so p is not nilpotent on $N \implies pN = N \implies p^rN = N$, $\forall r \geq 1$. Let $n \in N$ such that $n = (0, \ldots, n_{i_1}, \ldots, n_{i_s}, \ldots)$ where $n_{i_j} \in \mathbb{Z}/p^{i_j}\mathbb{Z}$, $0 \leq j \leq s$. But, $n = p^rn'$ for some $n' \in N$, and for $r = i_s \implies n_{i_j} = 0 \implies n = 0 \implies N = 0$ as 0-secondary is not p-secondary. □

Definition 3.2.21. Let p be a fixed prime. A *p-adic integer* is then a series

$$x = a_0 + a_1 p + a_2 p^2 + \ldots, \ a_i \in [0, p^i - 1]$$

(ignoring convergence issues). Consider the partial sums of x,

$$\begin{aligned} x_0 &= a_0 \\ x_1 &= a_0 + a_1 p \\ x_2 &= a_0 + a_1 p + a_2 p^2 \\ \vdots &\quad \vdots \\ x_n &= a_0 + a_1 p + \ldots + a_n p^n. \end{aligned}$$

We see that $x_n - x_{n-1} = a_n p^n \iff x_n \equiv x_{n-1} (\text{mod } p^n)$, $n \in \mathbb{N}$. Thus, we could also determine x by the sequence (x_n) of integers satisfying $x_n \equiv x_{n-1} (\text{mod } p^n)$. That is, given (x_n) we can recover the coefficients of x expanded in p: $a_0 = x_0$, $a_1 = \frac{x_1 - x_0}{p}$, $a_2 = \frac{x_2 - x_1}{p^2}$,..., $a_n = \frac{x_n - x_{n-1}}{p^n}$. Sums and products of p-adic integers can be defined by taking $x+y = (x_n + y_n)$ and $xy = (x_n y_n)$, taking care to "carry" when the a_i coefficients may be larger than p^i.

With addition and multiplication defined in this way, we get the ring of p-adic integers, denoted $\mathbb{Z}_{\hat{p}}$.

Definition 3.2.22. If a sequence of sets X_n $(n = 1, 2, 3, \ldots)$ and maps $f_n : X_{n+1} \to X_n$ $(n = 1, 2, 3, \ldots)$

$$\ldots \xrightarrow{f_4} X_4 \xrightarrow{f_3} X_3 \xrightarrow{f_2} X_2 \xrightarrow{f_1} X_1$$

are given, the subset of $\prod_{n \geq 1} X_n$ defined by

$$\{(a_n)_{n \geq 1} = (\ldots, a_4, a_3, a_2, a_1) \in \prod_{n \geq 1} X_n \mid f_n(a_{n+1}) = a_n \in X_n \text{ for all } n \geq 1\}$$

is called the *inverse limit* and is denoted $\varprojlim_n X_n$.

In Definition 3.2.22 we let $X_n = \mathbb{Z}/p^n\mathbb{Z}$, the ring of classes of integers $(\text{mod } p^n)$ and $f_n = \pi_n$, the natural projection homomorphism from $\mathbb{Z}/p^{n+1}\mathbb{Z}$ to $\mathbb{Z}/p^n\mathbb{Z}$ with kernel $p^n\mathbb{Z}$, and consider the (projective) inverse limit, $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$, of the sequence

$$\ldots \to \mathbb{Z}/p^4\mathbb{Z} \to \mathbb{Z}/p^3\mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}.$$

Letting n tend to infinity in $\mathbb{Z}/p^n\mathbb{Z}$ we obtain $\mathbb{Z}_{\hat{p}}$, more precisely, $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ is the completion $\mathbb{Z}_{\hat{p}}$ of the ring $\mathbb{Z}$. By definition, an element of $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ is a sequence $x = (\ldots, x_n, \ldots, x_3, x_2, x_1)$ with $x_{n+1} \equiv x_n \,(\text{mod } p^n)$ for all $n \geq 1$. Thus, we can define the structure of a ring on $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$, defining the addition and multiplication of elements $r = (\bar{r}_n)_{n\geq 1}$ and $s = (\bar{s}_n)_{n\geq 1}$ of $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ by $(\overline{r_n + s_n})_{n\geq 1}$ and $(\overline{r_n s_n})_{n\geq 1}$, respectively. In fact, we show that $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_{\hat{p}}$.

Lemma 3.2.23. *The map $\varprojlim \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}_{\hat{p}}$ is a bijection, moreover, $\varprojlim \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_{\hat{p}}$.*

Proof. Note that the map $\mathbb{Z}_{\hat{p}} \to \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ sending $a \mapsto (\bar{a}_n)_{n\geq 1}$ has been thoroughly treated in [1]. Instead, we concentrate here on $\varprojlim \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}_{\hat{p}}$. Let $\pi_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ be the natural projection map for all $n \geq 1$. Let $r = (\bar{r}_n)_{n\geq 1} \in \varprojlim \mathbb{Z}/p^n\mathbb{Z}$, where $\bar{r}_n \in \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ subject to the condition $\pi_n(\bar{r}_{n+1}) = \bar{r}_n$, that is, $p^n \mid \bar{r}_{n+1} - \bar{r}_n$. Set r_n equal to the reduced residue of $\bar{r}_n(\text{mod}\, p^n)$. Then, define $\varphi : \varprojlim \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}_{\hat{p}}$ by $r = (\bar{r}_n)_{n\geq 1} \overset{\varphi}{\longmapsto} \sum_{i=0}^{\infty} a_i p^i$ where $a_i = \dfrac{r_{i+1} - r_i}{p^i}$ for all $i \geq 0$ and such that $r_n = \sum_{i=0}^{n-1} a_i p^i$. We claim that the $\dfrac{r_{i+1} - r_i}{p^i} = a_i \in [0, p-1]$ for all $i \geq 0$. First, for $i = 0$, $a_0 = r_1 \leq p - 1$ since $r_1 \in \mathbb{Z}/p\mathbb{Z}$. Then, for $i = 1$, $a_1 = \dfrac{r_2 - r_1}{p}$ which implies that $r_2 = r_1 + pa_1$, and $r_2 \geq r_1$ if and only if $a_1 \geq 0$. Note that $a_1 \not\geq p$, otherwise, $r_2 \geq p^2$, a contradiction, since by definition $0 \leq r_2 < p^2$. Thus, $0 \leq a_1 < p$. Continuing the argument by induction on i, we have that $a_i \in [0, p-1]$ for all $i \geq 0$ as required.

Now two sequences $(\bar{x}_n)_{n\geq 1}$ and $(\bar{y}_n)_{n\geq 1}$ are equivalent if $x_n \equiv y_n(\text{mod}\, p^{n+1})$, that is, $(\bar{x}_n)_{n\geq 1}$ and $(\bar{y}_n)_{n\geq 1}$ define the same p-adic integer. Thus, every element of $\mathbb{Z}_{\hat{p}}$ can be uniquely written as an infinite formal sum $\sum_{i=0}^{\infty} a_i p^i$.

Next we show that φ is a ring homomorphism from $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ to $\mathbb{Z}_{\hat{p}}$, that is, $\varphi(r+s) = \varphi(r)+\varphi(s)$ and $\varphi(rs) = \varphi(r)\varphi(s)$ for $r, s \in \varprojlim \mathbb{Z}/p^n\mathbb{Z}$. Note, that addition and multiplication in $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ are defined "coordinate-wise", that is, the i^{th} coordinates of r, s are added or multiplied then reduced $(\mathrm{mod}\, p^i)$. As a result, consider first the case of the addition of p-adic integers: $(r+s) = (\bar{r}_n + \bar{s}_n)_{n\geq 1} = (\overline{r_n + s_n})_{n\geq 1} = (\bar{t}_n)_{n\geq 1} \overset{\varphi}{\longmapsto} \sum_{i=0}^{\infty} d_i p^i$, where $d_i = \dfrac{t_{i+1} - t_i}{p^i}$ and $r_n + s_n = \varepsilon_n' p^n + t_n$, $\varepsilon_n' \in \{0,1\}$; and $\varphi(r) + \varphi(s) = \sum_{i=0}^{\infty} a_i p^i + \sum_{i=0}^{\infty} b_i p^i = \sum_{i=0}^{\infty} c_i p^i$, where, the sum of the coefficients a_i, b_i is defined by induction by a sequence $(c_i)_{i\geq 1}$ of p-adic digits and a sequence $(\varepsilon_i)_{i\geq 1}$ of elements of $\{0,1\}$ (the "carries"),

$$\begin{aligned} a_0 + b_0 &= \varepsilon_0 p + c_0, & \varepsilon_0 \in \{0,1\} \\ a_1 + b_1 + \varepsilon_0 &= \varepsilon_1 p + c_1, & \varepsilon_1 \in \{0,1\} \\ \vdots \quad & \quad \vdots & \quad \vdots \\ a_n + b_n + \varepsilon_{n-1} &= \varepsilon_n p + c_n, & \varepsilon_n \in \{0,1\} \end{aligned}$$

We prove by induction: $\varepsilon_i' = \varepsilon_{i-1}$ and $d_i = c_i$ for all $i \geq 1$.

P_0: let $n = 0$, then $a_0 + b_0 = \varepsilon_0 p + c_0$ and $d_0 = t_1 = r_1 + s_1 - \varepsilon_1' p = a_0 + b_0 - \varepsilon_1' p$, which gives that $d_0 + \varepsilon_1' p = a_0 + b_0 = \varepsilon_0 p + c_0$.

P_{n-1}: assume $\varepsilon_n' = \varepsilon_{n-1}$, $d_{n-1} = c_{n-1}$.

$$\begin{aligned} P_n: \quad d_n = \frac{t_{n+1} - t_n}{p^n} &= \frac{r_{n+1} + s_{n+1} - \varepsilon_{n+1}' p^{n+1} - (r_n + s_n - \varepsilon_n' p^n)}{p^n} \\ &= a_n + b_n - \varepsilon_{n+1}' p + \varepsilon_n' \\ &= a_n + b_n + \varepsilon_{n-1} - (\varepsilon_{n+1}' p - \varepsilon_n' + \varepsilon_{n-1}) \\ &= \varepsilon_n p + c_n - \varepsilon_{n+1}' p \\ &= p(\varepsilon_n - \varepsilon_{n+1}') + c_n \Rightarrow \varepsilon_n = \varepsilon_{n+1}',\ d_n = c_n \end{aligned}$$

Thus, we have that $\varphi(r+s) = \varphi(r) + \varphi(s)$.

Consider next the multiplication of p-adic integers: $\varphi(rs) = \varphi(r)\varphi(s)$ implies that $\sum_{i=0}^{\infty} d_i p^i = (\sum_{i=0}^{\infty} a_i p^i)(\sum_{i=0}^{\infty} b_i p^i) = \sum_{i=0}^{\infty} c_i p^i$. To show that the two sums are equal it suffices to

show $(\mathrm{mod}\, p^{n+1})$ that $\sum_{i=0}^{n} d_i p^i = \sum_{i=0}^{n} c_i p^i$, that is,

$$t_{n+1}\,(\mathrm{mod}\, p^{n+1}) = (r_{n+1}\,(\mathrm{mod}\, p^{n+1}))(s_{n+1}\,(\mathrm{mod}\, p^{n+1})) = (r_{n+1}s_{n+1}\,(\mathrm{mod}\, p^{n+1})).$$

Notice, that for n sufficiently large, the product of the two sums $(\sum_{i=0}^{n} a_i p^i)(\sum_{i=0}^{n} b_i p^i) = (r_{n+1} + p^{n+1}A)(s_{n+1} + p^{n+1}B) = (w_{n+1} + p^{n+1}C)$, where A,B,C are the sum of the higher order terms, $w_{n+1} = \sum_{i=0}^{n} c_i p^i$ and coincides with the product of r_{n+1} and s_{n+1} terms. Thus, $t_{n+1}\,(\mathrm{mod}\, p^{n+1}) = r_{n+1}s_{n+1}\,(\mathrm{mod}\, p^{n+1}) = w_{n+1}\,(\mathrm{mod}\, p^{n+1})$, that is, the same rule for the product of the terms applies for the finite as well as the infinite sums. □

Proposition 3.2.24. *$x = \sum_{i=0}^{\infty} b_i p^i$ is a unit in $\mathbb{Z}_{\hat{p}}$, if and only if $b_0 \neq 0$.*

Proof. Suppose $b_0 \not\equiv 0\,(\mathrm{mod}\, p)$. Then, by the condition, $x_n \equiv x_{n-1}\,(\mathrm{mod}\, p^{n-1})$, $x_n \equiv x_{n-1} \equiv x_{n-2} \equiv \ldots \equiv x_1\,(\mathrm{mod}\, p)$, so $x_n \not\equiv 0\,(\mathrm{mod}\, p)$. Therefore, $(x_n, p^n) = 1$, so $\exists y_n$ such that $x_n y_n \equiv 1\,(\mathrm{mod}\, p^n)$, hence, also $(\mathrm{mod}\, p^{n-1})$. Since, $x_n \equiv x_{n-1}\,(\mathrm{mod}\, p^{n-1})$, so $x_n y_n \equiv x_{n-1}y_{n-1}\,(\mathrm{mod}\, p^{n-1})$. Thus, $x_n y_n \equiv x_n y_{n-1}\,(\mathrm{mod}\, p^{n-1})$, so $y_n \equiv y_{n-1}\,(\mathrm{mod}\, p^{n-1})$. The sequence $y = (y_n)_{n\geq 1}$ is a p-adic integer, and thus, $xy = 1$. Conversely, if $(\sum_{i=0}^{\infty} a_i p^i)(\sum_{i=0}^{\infty} b_i p^i) = 1$, then $a_0 b_0 = 1$, so $b_0 \not\equiv 0\,(\mathrm{mod}\, p)$. □

Proposition 3.2.25. *$\mathbb{Z}_{\hat{p}}$ is an integral domain, with a $\mathbb{Z}$ subring of $\mathbb{Z}_{\hat{p}}$.*

Proof. Let $x \in \mathbb{Z}_{\hat{p}}$. If $x = \sum_{i=r}^{\infty} a_i p^i$, $a_r \neq 0$, then $x = \sum_{i=r}^{\infty} a_i p^i = p^r(\sum_{i=r}^{\infty} a_i p^{i-r}) = p^r(\sum_{j=0}^{\infty} a_j p^j)$, thus, every non-zero p-adic integer can be represented in the form $x = p^r u$ where $r \geq 0$ and u is a unit. Consequently, $\mathbb{Z}_{\hat{p}}$ is an integral domain. Furthermore, the map $\varphi : \mathbb{Z} \to \mathbb{Z}_{\hat{p}}$ given by $n \mapsto (\ldots, n, \ldots, n, n, n)$, the p-adic representation of n given by the constant sequence, is an isomorphism of $\mathbb{Z}$ with a subring of $\mathbb{Z}_{\hat{p}}$. □

Proposition 3.2.26. *Every ideal of $\mathbb{Z}_{\hat{p}}$ is of the form $p^n\mathbb{Z}_{\hat{p}}$ for some $n \geq 0$. $p\mathbb{Z}_{\hat{p}}$ is the unique maximal ideal of $\mathbb{Z}_{\hat{p}}$ and $\mathbb{Z}_{\hat{p}}/p\mathbb{Z}_{\hat{p}} \cong \mathbb{Z}/p\mathbb{Z}$.*

Proof. Let I be a proper ideal of $\mathbb{Z}_{\hat{p}}$. Suppose $x \in \mathbb{Z}_{\hat{p}}$ belongs to I but not $p\mathbb{Z}_{\hat{p}}$, and let $x = a_0 + a_1 p + a_2 p^2 + \ldots$. Then $a_0 \neq 0$ and by the Proposition 3.2.24, x is a unit in $\mathbb{Z}_{\hat{p}}$, that

is, $\exists y \in \mathbb{Z}_{\hat{p}}$ such that $xy = 1$. But then $1 \in I$, contradicting the assumption that I is proper. Thus, $I \subseteq p\mathbb{Z}_{\hat{p}}$ and $p\mathbb{Z}_{\hat{p}}$ is the unique maximal ideal of $\mathbb{Z}_{\hat{p}}$. Furthermore, since the set of elements divisible by p form the maximal ideal $p\mathbb{Z}_{\hat{p}}$ in $\mathbb{Z}_{\hat{p}}$, we have $\mathbb{Z}_{\hat{p}}/p\mathbb{Z}_{\hat{p}} \cong \mathbb{Z}/p\mathbb{Z}$, where the mapping $x = \sum_{i=0}^{\infty} a_i p^i \longmapsto a_0 \bmod p$ defines the surjective ring homomorphism $\varphi : \mathbb{Z}_{\hat{p}} \to \mathbb{Z}/p\mathbb{Z}$, with kernel $\{x \in \mathbb{Z}_{\hat{p}} \mid a_0 = 0\} = p\mathbb{Z}_{\hat{p}}$. Finally, to show that every ideal of $\mathbb{Z}_{\hat{p}}$ is of the form $p^n\mathbb{Z}_{\hat{p}}$ for some $n \geq 0$, let $I \neq \{0\}$ be a non-zero ideal of $\mathbb{Z}_{\hat{p}}$ and $0 \neq a \in I$. Writing $a = p^n u$ with a p-adic unit u, hence $p^n = u^{-1}a \in I$ and $p^n\mathbb{Z}_{\hat{p}} \subseteq I$. Conversely, for any $b \in I$ and $k \geq n$, write $b = p^k u = p^n p^{k-n} u \in p^n\mathbb{Z}_{\hat{p}}$, thus, $I \subseteq p^n\mathbb{Z}_{\hat{p}}$. □

Definition 3.2.27. The quotient field $\mathbb{Q}_{\hat{p}}$ of $\mathbb{Z}_{\hat{p}}$ is called the field of *p-adic numbers, i.e.* $\mathbb{Q}_{\hat{p}} = Frac(\mathbb{Z}_{\hat{p}})$. Each $y \in \mathbb{Q}_{\hat{p}}$ has the form $y = \frac{x}{p^r}$, $r \geq 0$, $x \in \mathbb{Z}_{\hat{p}}$. But, by Proposition 3.2.26, $x = p^n u \implies y = p^m u$, where $m \in \mathbb{Z}$ and u is a unit in $\mathbb{Z}_{\hat{p}}$.

Proposition 3.2.28. *Let $R = \mathbb{Z}_{\hat{p}}$ and $M = \mathbb{Q}_{\hat{p}}/\mathbb{Z}_{\hat{p}} = \{\bar{p}^n u \mid n < 0, u \text{ is unit in } \mathbb{Z}_{\hat{p}}\}$. Then M is a 0-secondary $\mathbb{Z}_{\hat{p}}$-module.*

Proof. Consider $\bar{x} \in M$ and $r \in \mathbb{Z}_{\hat{p}}$, by definition $\bar{x} = \bar{p}^n u$ for $n < 0$ and $r = \bar{p}^m v$ for $m \geq 0$, with u, v units in $\mathbb{Z}_{\hat{p}}$. Then, $r\bar{x} = \bar{p}^{m+n} uv = 0$ if $m + n \geq 0 \implies \forall \bar{x} \in M$ we must have $r = 0$. Thus, $r^n M = 0$, for some $n > 0$, only if $r = 0$, that is, $\mathbb{Z}_{\hat{p}}$ is not nilpotent on M. Next, note that for every $r \in \mathbb{Z}_{\hat{p}}$, we have $r\bar{x} = \bar{p}^{m+n} uv = \bar{p}^k w \in M$, for some k and w a unit in $\mathbb{Z}_{\hat{p}}$ $\implies rM \subseteq M$. Now, let $\bar{x} = \bar{p}^n u \in M$, with $n < 0$, then $\bar{p}^n u = \bar{p}^{m+k} vw = (\bar{p}^m v)(\bar{p}^k w) = s\bar{y}$, where $k = n - m$, $m > 0 \implies s \in R$, $\bar{y} \in M$. Thus, $M \subseteq rM$ and M is secondary. Furthermore, $\sqrt{Ann_R(M)} = 0 \implies M$ is 0-secondary. □

Remark 3.2.29. Since $\mathbb{Z}$ is embedded in $\mathbb{Z}_{\hat{p}}$ as a subring, Proposition 3.2.28 can in fact be extended to all subrings, that is, M is 0-secondary for all subrings of R.

Proposition 3.2.30. *Consider the short exact sequence*

$$0 \longrightarrow K \longrightarrow M \longrightarrow N \longrightarrow 0$$

of R-modules. If K, N are representable $\mathbb{Z}$-modules then M is not necessarily representable.

Proof. Let $K, N = \mathbb{Z}/p\mathbb{Z}$ and $M = \bigoplus_p \mathbb{Z}/p\mathbb{Z}$, p prime. Then the short sequence

$$0 \longrightarrow K \xrightarrow{i} M \xrightarrow{\pi} N \longrightarrow 0$$

is exact at every position, and where i is an injective homomorphism from K to M and π is the natural projection of M onto N. Now, by Example 3.2.18 K, M are secondary and therefore representable, however, by Example 3.2.19 M is not representable. □

Proposition 3.2.31. *Let p be a prime, $H_n = \{z \in \mathbb{C} \mid z^{p^n} = 1\}$, where $(H_n, \cdot)$ is cyclic group of order p^n, and define $C_{p^\infty} = \bigcup_{n=0}^{\infty} H_n$. Then, C_{p^∞} is an Artinian 0-secondary $\mathbb{Z}$-module.*

Proof. First note that $H_n \leqslant H_{n+1}$ for all $n \geq 0$. Let $\zeta_n \in H_n$ denote the p^nth primitive root of 1. Then, since $(\zeta_{n+1}^p)^{p^n} = \zeta_{n+1}^{p^{n+1}} = 1$, we see that $\zeta_{n+1}^p \in H_n$, that is, ζ_{n+1}^p is also a p^nth primitive root. Thus, $H_0 \leqslant \ldots \leqslant H_{n-1} \leqslant H_n \leqslant H_{n+1} \leqslant \ldots$. Next, we show that any $H \leqslant C_{p^\infty}$, $H_n = H$, that is, every submodule of C_{p^∞} occurs as one of the H_n for some n. Now, let $H \leqslant \bigcup_{n=0}^{\infty} H_n$ and let n be minimum such that $\zeta_{n+1} \notin H \Leftrightarrow H_{n+1} \nleqslant H$. So, $H_n \leqslant H$. Let $z \in H$, then $\exists m$ such that $z^{p^m} = 1 \Rightarrow ord(z) \mid p^m$, so $ord(z) = p^r$ for some $r \leq m$. This implies that $z \in H_r$ is a generator of H_r, i.e. $z = \zeta_r^k \in \langle \zeta_r \rangle = H_r$. Then, $\zeta_r = z^l \in H \Rightarrow \zeta_r \in H \Rightarrow r \leq n \Rightarrow H_r \leqslant H_n$, so $z \in H_n \Rightarrow H \leqslant H_n \Rightarrow H = H_n$. Thus, C_{p^∞} is Artinian.

To show that C_{p^∞} is secondary, let $\varphi_n(z) = n \star z$ be the map given by z^n, thus, $\varphi_n(C_{p^\infty}) = (C_{p^\infty})^n$. $C_{p^\infty} \neq 0$ is clear.

Claim: $\forall n \in \mathbb{Z}$, φ_n must be either nilpotent or surjective.

Proof of Claim: Since there exists no integer $n > 0$ such that $z^n = 1$ for all $z \in C_{p^\infty}$, thus, φ_n is nilpotent if and only if $n = 0$. Consider next the surjectivity of φ_n, that is, $\varphi(C_{p^\infty}) = (C_{p^\infty})^n = C_{p^\infty}$. Let $z \in C_{p^\infty}$. Since, $z^{p^k} = (z^p)^{p^{k-1}} = 1$, this implies that $\exists m = p^{k-1}$ such that $z^{pm} = 1$. Suppose next that $(n, p) = 1 \implies 1 = an + bp \implies 1 = an + bp^k$ for some k. Then, $z = z^1 = z^{an+bp^k} = (z^a)^n \in (C_{p^\infty})^n$ and $z^a \in C_{p^\infty}$ as $(z^a)^{p^k} = 1$. Finally, if $n = p^l r$ with $(r, p) = 1$, then $(C_{p^\infty})^{p^l r} = ((C_{p^\infty})^r)^{p^l} = (C_{p^\infty})^{p^l}$, thus, it

remains to show that $(C_{p^\infty})^{p^l} = C_{p^\infty}$. Let $z \in C_{p^\infty} \implies z = e^{(2\pi ir/p^m)}$ for $0 < r \leq p^m - 1$ and some m, then, $z = (e^{(2\pi ir/p^{m+l})})^{p^l} \in (C_{p^\infty})^{p^l} \implies C_{p^\infty} \subseteq (C_{p^\infty})^{p^l}$. Let $z \in (C_{p^\infty})^{p^l} \implies z = \omega^{p^l}$ where $\omega = e^{2\pi ir/p^k}$ for $0 < r \leq p^k - 1$ and some k, but, $z^{p^k} = (\omega^{p^l})^{p^k} = 1 \implies (C_{p^\infty})^{p^l} \subseteq C_{p^\infty}$. Thus, C_{p^∞} is secondary. *End of Proof of Claim.*

Since the $Ann_{\mathbb{Z}}(C_{p^\infty}) = \{n \mid (C_{p^\infty})^n = 1\} = 0$ this shows that C_{p^∞} is, in fact, a 0-secondary $\mathbb{Z}$-module. □

Proposition 3.2.32. *C_{p^∞} is isomorphic to the p-primary component of $\mathbb{Q}/\mathbb{Z}$.*

Proof. Define the map $\varphi : (e^{2\pi ir/p^n}) \mapsto \sum_p r/p^n + \mathbb{Z}$, where $r \in \mathbb{Z}$. It is clear that φ is an injective homomorphism. To show that φ is surjective, let $a/b \in \mathbb{Q}/\mathbb{Z}$, and write $b = \prod_p p^n$. Since the numbers b/p^n are pairwise relatively prime, there are integers m with $1 = \sum_p m(b/p^n)$. Therefore, $a/b = \sum_p am/p^n = \varphi(am/p^n)$. □

Bibliography

[1] Borevich, Z. I. and Shafarevich, I. R., *Number Theory*. Academic Press, 1966.

[2] Dummit, D. and Foote, R., *Abstract Algebra*. Wiley, 2004.

[3] Eisenbud, D., *Commutative Algebra*. Springer, 1997.

[4] Gouvêa, F. Q., *p-adic Numbers*. Springer, 1997.

[5] Kato, K., Kurokawa, N., and Saito, T., *Number Theory 1: Fermat's Dream*. American Mathematical Society, 1996.

[6] Kunz, E., *Introduction to Commutative Algebra and Algebraic Geometry*. Birkhäuser, 1985.

[7] MacDonald, I. G., "Secondary representation of modules over a commutative ring," *Sympos. Math.*, no. 11, pp. 23–43, 1973.

[8] Matsumura, H., *Commutative Ring Theory*. Cambridge University Press, 1989.

[9] Reid, M., *Undergraduate Commutative Algebra*. Cambridge University Press, 1995.

[10] Rotman, J. J., *An Introduction to Homological Algebra*. Springer, 2009.

[11] Serre, J. P., *A Course in Arithmetic*. Springer, 1973.

[12] Sharp, R. Y., *Steps in Commutative Algebra*. Cambridge University Press, 1990.