Canonical Modules

Dylan C. Beck

Contents

1 Maximal Cohen-Macaulay Modules **1**

2 Canonical Modules **4**

3 Appendix **7**

3.1 Rings, Ideals, and Modules 7

3.2 Krull Dimension and Height 14

3.3 Regular Sequences and Associated Primes 18

3.4 Depth and the Cohen-Macaulay Condition 26

3.5 Systems of Parameters and Regular Local Rings 34

3.6 Homological Algebra 39

3.7 Injective Modules and Injective Hulls 62

1 Maximal Cohen-Macaulay Modules

We will assume throughout this section that $(R,\mathfrak{m},k)$ is a Noetherian local ring with unique maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$. By Definition 3.65, the dimension of a finitely generated R-module M is $\dim(M) = \dim(R/\operatorname{ann}_R(M))$; the latter is at most $\dim(R)$ by Proposition 3.33. Previously, in Theorem 3.58, we established that $\operatorname{depth}(M) = \inf\{i \geq 0 \mid \operatorname{Ext}^i_R(k,M) \neq 0\}$ is a well-

defined invariant that measures the maximum length of an M-regular sequence in $\mathfrak{m}$. By Proposition 3.67, we have that $\operatorname{depth}(M) \leq \dim(M)$. Equality holds if and only if M is Cohen-Macaulay by Definition 3.70. Combined, these inequalities show that $\operatorname{depth}(M) \leq \dim(M) \leq \dim(R)$. We say that a finitely generated R-module M is **maximal Cohen-Macaulay** if $\operatorname{depth}(M) = \dim(R)$. For instance, any Cohen-Macaulay local ring is a maximal Cohen-Macaulay module over itself.

Our immediate interest is to illustrate that the maximal Cohen-Macaulay modules and the finitely generated modules of finite injective dimension over a Cohen-Macaulay local ring are "orthogonal" with respect to Ext. Crucially, this holds as a corollary of the following.

Theorem 1.1 (Ischebeck)**.** *[Isc69, Satz 2.6] Let $(R,\mathfrak{m},k)$ be a Noetherian local ring. Let M and N be nonzero finitely generated R-modules. If M has finite projective dimension or N has finite injective dimension, then* $\operatorname{depth}(R) - \operatorname{depth}(M) = \sup\{i \geq 0 \mid \operatorname{Ext}^i_R(M,N) \neq 0\}$.

Corollary 1.2. *Let $(R,\mathfrak{m},k)$ be a Cohen-Macaulay local ring. Let M and N be nonzero finitely generated R-modules. The following properties hold.*

(1.) *The R-module M is maximal Cohen-Macaulay if and only if* $\operatorname{Ext}^i_R(M,B) = 0$ *for all integers $i \geq 1$ and all finitely generated R-modules B of finite injective dimension.*

(2.) *The R-module N has finite injective dimension if and only if* $\operatorname{Ext}^i_R(A,N) = 0$ *for all integers $i \geq 1$ and all maximal Cohen-Macaulay R-modules A.*

Proof. (1.) By Theorem 1.1, we have that $\operatorname{depth}(R) - \operatorname{depth}(M) = \sup\{i \geq 0 \mid \operatorname{Ext}^i_R(M,N) \neq 0\}$ for all finitely generated R-modules B of finite injective dimension, hence the claim holds.

(2.) One direction is immediate: if N has finite injective dimension, then Theorem 1.1 guarantees that $\operatorname{Ext}^i_R(A,N) = 0$ for all integers $i \geq 1$ and all maximal Cohen-Macaulay R-modules A. Conversely, suppose that $\operatorname{Ext}^i_R(A,N) = 0$ for all integers $i \geq 1$ and all maximal Cohen-Macaulay R-modules A. Given any R-module M, there exists a free resolution $F_\bullet$ of M; its construction in Proposition 3.90 illustrates that for each free module F_i of $F_\bullet$ with $i \geq 0$, there exist R-modules K_{i-1} and K_i such that $0 \to K_i \to F_i \to K_{i-1} \to 0$ is a short exact sequence, where we adopt the notation $K_{-1} = M$. By Proposition 3.91, for each of these short exact sequences, there exists a long

exact sequence of Ext; the form of this long exact sequence in tandem with our hypothesis that F_i is free and Proposition 3.111 yields isomorphisms $\operatorname{Ext}^n_R(K_i,N) \cong \operatorname{Ext}^{n+1}_R(K_{i-1},N)$ for each integer $n \geq 1$ and all integers $i \geq 0$. By the Depth Lemma, we have that K_i is maximal Cohen-Macaulay for all integers $i \geq d = \operatorname{depth}(R)$, hence by assumption, we have that $\operatorname{Ext}^n_R(K_d,N) = 0$ for all integers $n \geq 1$. Our previous isomorphism yields that $\operatorname{Ext}^{n+1}_R(K_{d-1},N) = 0$ for all integers $n \geq 1$. Continuing in this manner, we find that $\operatorname{Ext}^{n+d+1}_R(M,N) = 0$ for all integers $n \geq 1$; this holds for any R-module M, hence N has finite injective dimension by Proposition 3.114. □

Using their Intersection Theorem, Peskine and Szpiro proved the following conjecture for local rings that either (a.) have prime characteristic or (b.) are essentially of finite type over a field of characteristic zero (cf. [PS73]). Later, Paul C. Roberts established that the Intersection Theorem for all Noetherian local rings (cf. [Rob87]), hence we obtain the following theorem.

Theorem 1.3 (Bass's Conjecture of 1963)**.** *Let $(R,\mathfrak{m},k)$ be a Noetherian local ring. If there exists a finitely generated R-module of finite injective dimension, then R is Cohen-Macaulay.*

One can also demonstrate that the converse holds as follows.

Proposition 1.4. *[LW12, Proposition 11.1] If $(R,\mathfrak{m},k)$ is a Cohen-Macaulay local ring, then there exists a finitely generated R-module of finite injective dimension.*

Proof. Consider a system of parameters $x_1,\ldots,x_n$ of R. By definition, the quotient ring $\bar{R} = R/\underline{x}$ of R by the parameter ideal $\underline{x} = (x_1,\ldots,x_n)$ has dimension zero, hence it is an Artinian local ring with unique maximal ideal $\bar{\mathfrak{m}} = \mathfrak{m}/\underline{x}$ and residue field k. By Proposition 3.130, the injective hull E of the residue field over $\bar{R}$ has finite length as an $\bar{R}$-module, hence it has finite length as an R-module by Proposition 3.19. Consequently, E is finitely generated as an R-module by Proposition 3.16 so that $\operatorname{Hom}_R(\bar{R},E)$ is finitely generated as an R-module. By hypothesis that R is Cohen-Macaulay, the ideal $\underline{x}$ is generated by an R-regular sequence by Proposition 3.78, hence it has a finite free resolution $F_\bullet$ by Proposition 3.44. By applying the contravariant functor $\operatorname{Hom}_R(-,E)$ to $F_\bullet$, we obtain an injective resolution of $\bar{R}$ with finitely many nonzero terms. □

2 Canonical Modules

Combined, Bass's Conjecture of 1963 and Proposition 1.4 show that Cohen-Macaulayness is a necessary and sufficient condition for a Noetherian local ring to admit a finitely generated module of finite injective dimension. Consequently, we assume throughout the remainder of this section that $(R,\mathfrak{m},k)$ is a Cohen-Macaulay local ring, as our primary concern lies in the study maximal Cohen-Macaulay modules of finite injective dimension. Recall that the (Cohen-Macaulay) type of a finitely generated R-module M is $r(M) = \dim_k \operatorname{Ext}_R^{\operatorname{depth}(M)}(k,M)$, i.e., the k-vector space dimension of the first non-vanishing Ext module of k and M. By definition, if M is maximal Cohen-Macaulay, then $\operatorname{depth}(M) = \dim(R)$ so that $r(M) = \dim_k \operatorname{Ext}_R^{\dim(R)}(k,M)$. On the other hand, if M has finite injective dimension, then Theorem 3.59 implies that $\operatorname{injdim}_R(M) = \operatorname{depth}(R) = \dim(R)$. Ultimately, these invariants all coincide, hence $r(M)$ encodes much information. Our specific interest lies with maximal Cohen-Macaulay modules of finite injective dimension of type one.

Definition 2.1. Let $(R,\mathfrak{m},k)$ be a Cohen-Macaulay local ring. We say that a finitely generated R-module ω is a **canonical module** for R if ω satisfies all of the following conditions.

(1.) ω is maximal Cohen-Macaulay over R, i.e., $\operatorname{depth}(\omega) = \dim(R)$.

(2.) ω has finite injective dimension over R, i.e., $\operatorname{injdim}_R(\omega) = \operatorname{depth}(R)$.

(3.) ω has type one, i.e., $\dim_k \operatorname{Ext}_R^{\operatorname{depth}(\omega)}(k,\omega) = 1$.

By our previous exposition and Proposition 3.114, one can check whether a finitely generated module is a canonical module by the vanishing of its Ext modules with k in the first component.

Proposition 2.2 (Ext Vanishing Criterion for Canonical Modules)**.** *Let $(R,\mathfrak{m},k)$ be a Cohen-Macaulay local ring. A finitely generated R-module ω is a canonical module if and only if*

$$\operatorname{Ext}_R^i(k,\omega) \cong \begin{cases} k & \text{if } i = \dim(R) \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. By Definition 2.1, if ω is a finitely generated R-module that is a canonical module for R, then $\operatorname{depth}(\omega) = \dim(R) = \operatorname{depth}(R) = \operatorname{injdim}_R(\omega)$ and $\dim_k \operatorname{Ext}_R^{\dim(R)}(k,\omega) = 1$. By Theorem 3.58, we have that $\operatorname{depth}(\omega)$ is the smallest non-negative integer for which $\operatorname{Ext}_R^i(k,M)$ does not vanish. By Proposition 3.114, we have that $\operatorname{Ext}_R^i(k,\omega) = 0$ vanishes for all integers $i \geq \operatorname{injdim}_R(\omega) + 1$. Unravelling these details shows that $\operatorname{Ext}_R^i(k,\omega) = 0$ for all integers other than $i = \dim(R)$ and $\operatorname{Ext}_R^{\dim(R)}(k,\omega) \cong k$. Conversely, if the specified vanishing of Ext criterion is satisfied, then ω has finite injective dimension $\operatorname{depth}(\omega)$. By Theorem 3.59, we conclude that $\dim(R) = \operatorname{depth}(R) = \operatorname{injdim}(\omega) = \operatorname{depth}(\omega)$, i.e., ω is maximal Cohen-Macaulay of type one. □

One of the most important features of a canonical module of a Cohen-Macaulay local ring R is that it provides a duality on the category of R-modules that preserves depth and hence (maximal) Cohen-Macaulayness. We collect this property and others in the following. We will omit the proofs of the next two theorems out of necessity, but the interested reader may look to [BH93, Section 3.3] for reference — especially [BH93, Theorems 3.3.4, 3.3.5, and 3.3.12].

Theorem 2.3. *Let $(R,\mathfrak{m})$ be a Cohen-Macaulay local ring that admits a canonical module ω.*

(1.) *If ω' is a canonical module for R, then there exists an R-module isomorphism $\varphi : \omega \to \omega'$. Put another way, a canonical module for R is unique up to isomorphism.*

(2.) *We have that $\operatorname{Hom}_R(\omega,\omega') \cong R$ for any canonical modules ω and ω' of R.*

(3.) *Let M be a Cohen-Macaulay R-module. Let $M^\vee = \operatorname{Ext}_R^{\operatorname{depth}(R)-\operatorname{depth}(M)}(M,\omega)$.*

  (a.) The R-module $M^\vee$ is Cohen-Macaulay with $\operatorname{depth}(M^\vee) = \operatorname{depth}(M)$.

  (b.) We have that $\operatorname{Ext}_R^i(M,\omega) = 0$ for all integers $i \neq \operatorname{depth}(R) - \operatorname{depth}(M)$.

  (c.) We have that $(M^\vee)^\vee \cong M$, i.e., $(-)^\vee$ provides a duality on Cohen-Macaulay modules.

(4.) *Let M be a maximal Cohen-Macaulay (MCM) R-module. Let $M^\vee = \operatorname{Hom}_R(M,\omega)$.*

  (a.) The R-module $M^\vee$ is maximal Cohen-Macaulay.

  (b.) We have that $\operatorname{Ext}_R^i(M,\omega) = 0$ for all integers $i \geq 1$.

(c.) We have that $(M^\vee)^\vee \cong M$, i.e., $(-)^\vee$ provides a duality on MCM R-modules.

(5.) *We have that $\omega/\underline{x}\omega$ is a canonical module for $R/\underline{x}R$ for all R-regular sequences $\underline{x}$ of R.*

(6.) *We have that ω_P is a canonical module for R_P for all prime ideals P of R.*

(7.) *We have that $\widehat{\omega}_{\mathfrak{m}}$ is a canonical module for $\widehat{R}_{\mathfrak{m}}$.*

Theorem 2.4. *[BH93, Theorem 3.3.7] Let $(R,\mathfrak{m})$ be a Cohen-Macaulay local ring that admits a canonical module ω_R. Let $(S,\mathfrak{n})$ be a Cohen-Macaulay local ring. If there exists a local ring homomorphism $\varphi : (R,\mathfrak{m}) \to (S,\mathfrak{n})$ such that S is finitely generated as an R-module via the action $r \cdot s = \varphi(r)s$, then $\operatorname{Ext}_R^{\dim(R)-\dim(S)}(S,\omega_R)$ is a canonical module for S.*

Corollary 2.5. *Let $\varphi : (R,\mathfrak{m}) \to (S,\mathfrak{n})$ be a module-finite extension of Cohen-Macaulay local rings. If R admits a canonical module ω_R, then $\operatorname{Hom}_R(S,\omega_R)$ is a canonical module for S.*

Even more, if a Cohen-Macaulay local ring R admits a canonical module ω_R, then ω_R has the additional property that it "spans" the intersection between the collections of maximal Cohen-Macaulay R-modules and the finitely generated R-modules of finite injective dimension.

Proposition 2.6. *[LW12, Proposition 11.7] Let R be a Cohen-Macaulay local ring that admits a canonical module ω_R. Every maximal Cohen-Macaulay R-module of finite injective dimension can be written as a direct sum of finitely many copies of ω_R.*

Proof. By writing $M^\vee$ as the homomorphic image of a free R-module F by an R-module homomorphism with kernel K, we obtain a short exact sequence of R-modules $0 \to K \to F \to M^\vee \to 0$. By Theorem 2.3(4a.) and the Depth Lemma, we have that

$$\operatorname{depth}(R) \geq \operatorname{depth}(K) \geq \min\{\operatorname{depth}(F), \operatorname{depth}(M^\vee)+1\} = \min\{\operatorname{depth}(R), \operatorname{depth}(R)+1\},$$

i.e., $\operatorname{depth}(K) = \operatorname{depth}(R)$ and K is maximal Cohen-Macaulay. By applying $(-)^\vee = \operatorname{Hom}_R(-,\omega_R)$, we obtain a short exact sequence of R-modules $0 \to M \to F^\vee \to K^\vee \to 0$ by parts (4b.) and (4c.) of Theorem 2.3. Considering that $K^\vee$ is maximal Cohen-Macaulay and M has finite injective

dimension by assumption, we conclude that $\mathrm{Ext}^1_R(K^\vee, M) = 0$ by Corollary 1.2. Consequently, Proposition 3.112 implies that the sequence $0 \to M \to F^\vee \to K^\vee \to 0$ splits so that M is a direct summand of $F^\vee$. Once again, by Theorem 2.3(4c.), we find that $M^\vee$ is a direct summand of the free R-module $(F^\vee)^\vee \cong F$, hence $M^\vee$ is a projective R-module by Proposition 3.86. Every finitely generated projective module over a local ring is free by Proposition 3.102; thus, $M^\vee$ is a finitely generated free R-module, i.e., $M^\vee \cong R^n$ for some integer $n \geq 0$. Ultimately, the canonical duality of Theorem 2.3 yields that $M \cong (M^\vee)^\vee \cong (R^n)^\vee = \mathrm{Hom}_R(R^n, \omega_R) \cong \omega_R^n$. □

3 Appendix

3.1 Rings, Ideals, and Modules

Unless otherwise stated, we will assume throughout this thesis that R is a commutative unital ring with additive identity 0_R and multiplicative identity 1_R. Recall that an **ideal** I of R is a subgroup of $(R, +)$ that is closed under multiplication by elements of R, i.e., we have that $ri \in I$ for every element $r \in R$ and $i \in I$. We say that a proper ideal P of R is **prime** if and only if the quotient ring $R/P = \{r + P \mid r \in R\}$ is a **domain**. We say that a proper ideal M of R is **maximal** if and only if R/M is a **field**. By convention and for convenience, we make the following definitions, as well.

Definition 3.1. We denote by $\mathrm{Spec}(R)$ the collection of prime ideals of R, i.e.,

$$\mathrm{Spec}(R) = \{P \subseteq R \mid P \text{ is a prime ideal of } R\}.$$

Occasionally, we will write $\mathrm{MaxSpec}(R) = \{M \subseteq R \mid M \text{ is a maximal ideal of R }\}$. We refer to $\mathrm{Spec}(R)$ as the **spectrum** of R; likewise, $\mathrm{MaxSpec}(R)$ is the **maximal spectrum** of R.

Example 3.2. Let $\mathbb{Z}$ denote the ring of integers. We have that $\mathrm{Spec}(\mathbb{Z}) = \{p\mathbb{Z} \mid p \text{ is prime}\} \cup \{0\}$ because $\mathbb{Z}$ is a Euclidean domain and $\mathrm{MaxSpec}(\mathbb{Z}) = \mathrm{Spec}(\mathbb{Z}) \setminus \{0\}$.

By the Fundamental Theorem of Arithmetic, every positive integer can be written as a product of positive powers of distinct primes. Consequently, given any integer n, there exist distinct primes

$p_1, \ldots, p_k$ and positive integers $e_1, \ldots, e_k$ such that $n = \pm p_1^{e_1} \cdots p_k^{e_k}$. Every ideal of $\mathbb{Z}$ is principal, and we have that $a\mathbb{Z} \subseteq b\mathbb{Z}$ if and only if $b \mid a$, hence the ideal $n\mathbb{Z}$ induces a chain of ideals beginning with itself and ending with $p_i\mathbb{Z}$ for some prime p_i appearing in the prime factorization of n.

Generally, we use the following definition to describe this property of a ring.

Definition 3.3. We say that R is **Noetherian** if any of the following equivalent conditions hold.

(i.) Every ascending chain of ideals of R stabilizes. Explicitly, for every sequence of inclusions of ideals $I_1 \subseteq I_2 \subseteq \cdots$, there exists an integer $n \gg 0$ such that $I_k = I_n$ for all integers $k \geq n$.

(ii.) Every nonempty collection of ideals has a maximal element with respect to inclusion.

(iii.) Every ideal I of R is finitely generated. Explicitly, there exist elements $x_1, \ldots, x_n \in I$ such that for every element $x \in I$, we have that $x = r_1 x_1 + \cdots + r_n x_n$ for some elements $r_1, \ldots, r_n \in R$.

Theorem 3.4 (Hilbert's Basis Theorem)**.** *If R is Noetherian, then $R[x]$ is Noetherian.*

Example 3.5. Let k be a field. Observe that the only ideals of k are $\{0_k\}$ and k: indeed, the ideals of k (or any commutative unital ring) are in one-to-one correspondence with the kernels of the unital ring homomorphisms $k \to S$ as S ranges over all commutative unital rings. Every nonzero element of k is a unit, so any unital ring homomorphism $\varphi : k \to S$ must be injective or identically zero, i.e., $\ker \varphi = \{0_k\}$ or $\ker \varphi = k$. Both of these are finitely generated ideals, as k is generated as an ideal by 1_k (as with any ring). Consequently, any field k is Noetherian by Definition 3.3. By Hilbert's Basis Theorem, any polynomial ring or finitely generated algebra over k is Noetherian.

Even more, Example 3.5 shows that the only maximal ideal of a field is the zero ideal.

Definition 3.6. We say that R is **local** if R admits a unique maximal ideal $\mathfrak{m}$. For emphasis, we write $(R, \mathfrak{m}, k)$ to denote the local ring R with unique maximal ideal $\mathfrak{m}$ and **residue field** $k = R/\mathfrak{m}$.

Proposition 3.7. *Let R be a commutative unital ring. The following conditions are equivalent.*

(i.) *R admits a unique maximal ideal, i.e., R is local.*

(ii.) *For every element $r \in R$, either r or $1_R + r$ is a unit.*

Particularly, the unique maximal ideal of a local ring R consists of all non-unit elements of R.

Example 3.8. Given a field k and indeterminate x, consider the quotient ring $S = k[x]/(x^2)$. We denote by $\bar{x}$ the class of x modulo (x^2). By the Correspondence Theorem, the ideals of S are in bijection with the ideals of $k[x]$ that contain (x^2) via the map that sends an ideal I of $k[x]$ to the ideal $I/(x^2)$ of S. Considering that $k[x]$ is a principal ideal domain, the ideals of S are (0_S), $(\bar{x})$, and S, corresponding to the ideals (x^2), (x), and $k[x]$, respectively. Of these, $(\bar{x})$ is maximal by the Third Isomorphism Theorem. Consequently, $(S, \mathfrak{m})$ is a local ring with maximal ideal $\mathfrak{m} = (\bar{x})$.

Other than the ideals of a commutative unital ring, the following definition introduces algebraic structures associated to R by which one may understand the properties of R.

Definition 3.9. We say that an abelian group $(M, +)$ is a (unital) R-**module** if there is a map $\cdot : R \times M \to M$ sending $(r, m) \mapsto r \cdot m$ such that for all elements $r, s \in R$ and $m, n \in M$, we have that

(i.) $r \cdot (m + n) = r \cdot m + r \cdot n$,

(ii.) $(r + s) \cdot m = r \cdot m + s \cdot m$,

(iii.) $r \cdot (s \cdot m) = (rs) \cdot m$, and

(iv.) $1_R \cdot m = m$.

Clearly, R is an R-module via its own multiplication. We will reserve the notation 0 for the zero element of M. Often, it will be convenient to write $r \cdot m$ as rm with the understanding that r is an element of R that is acting on the element m of the R-module M via the specified action.

Like with any algebraic structure, the substructures of a module are of central importance to its study. If M is an R-module, then $N \subseteq M$ is an R-**submodule** if N is closed under addition and R-scalar multiplication and $0 \in N$. By definition, the R-submodules of R are precisely its ideals.

If M and N are any R-modules, then an R-**module homomorphism** $\varphi : M \to N$ is a function such that $\varphi(m + m') = \varphi(m) + \varphi(m')$ and $\varphi(rm) = r\varphi(m)$ for all elements $m, m' \in M$ and $r \in R$. Equivalently, one could say that an R-module homomorphism is an R-linear transformation.

We say that M is **faithful** if $rm = 0$ implies that $r = 0_R$ for every nonzero element $m \in M$. Put another way, if the **annihilator** $\operatorname{ann}_R(M) = \{r \in R \mid rm = 0 \text{ for all elements } m \in M\}$ of M is zero, then M is a faithful R-module. One can immediately verify that $\operatorname{ann}_R(M)$ is an ideal of R.

Crucially, if M is an R-module and I is an ideal of M such that $IM = 0$, then M can be viewed as an R/I-module via the action $(r+I) \cdot m = rm$. Explicitly, if $r+I = s+I$, then $r-s$ belongs to I so that $rm - sm = (r-s)m = 0$. But this implies that $(r+I) \cdot m = rm = sm = (s+I) \cdot m$, and the action is well-defined. Particularly, if $\mathfrak{m}$ is a maximal ideal of R, then $R/\mathfrak{m}$ is a field. Further, if $\mathfrak{m}M = 0$, then M is an $R/\mathfrak{m}$-vector space, and it admits a basis. We will return to this idea soon.

We say that an R-module M is **finitely generated** if there exist elements $x_1, \ldots, x_n \in M$ such that for every element $x \in M$, there exist elements $r_1, \ldots, r_n \in R$ such that $x = r_1x_1 + \cdots + r_nx_n$. Put another way, the elements $x_1, \ldots, x_n \in M$ generate M as an R-module if $M = R\langle x_1, \ldots, x_n \rangle$. We state a fundamental result relating the finitely generated R-modules and prime ideals of R.

Lemma 3.10 (Prime Avoidance Lemma)**.** *[BH93, Lemma 1.2.2] Let R be a commutative unital ring with prime ideals $P_1, \ldots, P_n$. Let M be an R-module with $x_1, \ldots, x_n \in M$. Let $N = R\langle x_1, \ldots, x_n \rangle$. If $N_{P_i} \not\subseteq P_iM_{P_i}$ for any integer $1 \leq i \leq n$, then there exists an element $x \in N$ such that $x \notin P_iM_{P_i}$ for any integer $1 \leq i \leq n$. Particularly, if I is a finitely generated ideal of R such that $I \not\subseteq P_i$ for any integer $1 \leq i \leq n$, then there exists an element $r \in I$ such that $r \notin P_i$ for any integer $1 \leq i \leq n$.*

Every finitely generated module over a local ring $(R, \mathfrak{m})$ admits a unique number of minimal generators by **Nakayama's Lemma**. Considering its importance and ubiquity, we record it below.

Lemma 3.11 (Nakayama's Lemma)**.** *Let $(R, \mathfrak{m}, k)$ be a local ring with unique maximal ideal $\mathfrak{m}$ and residue field k. Let M be a finitely generated R-module. If the images of $x_1, \ldots, x_n$ modulo $\mathfrak{m}M$ form a basis of the k-vector space $M/\mathfrak{m}M$, then $M = R\langle x_1, \ldots, x_n \rangle$.*

One common variation of Nakayama's Lemma is presented in the following corollary. We omit the proof of the necessity of Nakayama's Lemma, but we do establish its sufficiency.

Corollary 3.12. *Let $(R, \mathfrak{m}, k)$ be a local ring. Let M be a finitely generated R-module. If I is a proper ideal of R and N is an R-submodule of M such that $M = IM + N$, then $M = N$.*

Proof. Let $x_1, \ldots, x_n$ denote a system of generators of M such that $x_1 + \mathfrak{m}M, \ldots, x_n + \mathfrak{m}M$ forms a basis for the k-vector space $M/\mathfrak{m}M$. By hypothesis that $M = IM + N$, for each integer $1 \leq i \leq n$, there exist elements $r_{i,1}, \ldots, r_{i,n} \in I$ and $y_i \in N$ such that $x_i = y_i + \sum_{j=1}^{n} r_{i,j} x_j$. Consequently, we have that $x_i + \mathfrak{m}M = y_i + \mathfrak{m}M$ so that $y_1 + \mathfrak{m}M, \ldots, y_n + \mathfrak{m}M$ forms a basis of $M/\mathfrak{m}M$. We conclude by Nakayama's Lemma that $M = R\langle y_1, \ldots, y_n \rangle$ so that $M = N$, as desired. □

We denote by $\mu(M) = \dim_k(M/\mathfrak{m}M)$ the unique number of minimal generators of M, as guaranteed by Nakayama's Lemma. Our next definition generalizes Definition 3.3.

Definition 3.13. We say that M is **Noetherian** if any of the following equivalent conditions hold.

(i.) Every ascending chain of R-submodules of M stabilizes.

(ii.) Every nonempty collection of R-submodules of M has a maximal element under inclusion.

(iii.) Every R-submodule of M is finitely generated.

If R is Noetherian, then the following condition is equivalent to the above conditions.

(iv.) The R-module M is finitely generated.

We refer to a chain of R-modules $0 \subsetneq M_1 \subsetneq \cdots \subseteq M_{n-1} \subsetneq M$ as a **composition series** of M if there does not exist an R-submodule N of M such that $M_i \subsetneq N \subsetneq M_{i+1}$ for any integer $0 \leq i \leq n-1$. Put another way, a composition series of M is a maximal ascending chain of R-submodules of M beginning with 0 and ending with M. One of the most important invariants of M is its **length**

$$\ell_R(M) = \inf\{n \geq 0 \mid M \text{ admits a composition series } 0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_{n-1} \subsetneq M\}.$$

If R is a field and M is an R-module, then M is an R-vector space, and its length coincides with its R-vector space dimension. Consequently, length is a generalization of vector space dimension to modules over commutative unital rings other than fields. Considering that finite-dimensional vector spaces exhibit pleasant properties, we are motivated to investigate length of general modules.

Definition 3.14. We say that M is **Artinian** if any of the following equivalent conditions hold.

(i.) Every descending chain of R-submodules of M stabilizes.

(ii.) Every nonempty collection of R-submodules of M has a minimal element under inclusion.

Proposition 3.15. *Let R be a commutative unital ring. The following are equivalent.*

(i.) *An R-module M is Noetherian and Artinian.*

(ii.) *An R-module M has finite length over R.*

Proof. Clearly, the claim holds if $M = 0$. We will assume henceforth that M is a nonzero R-module. (i.) If M is both Noetherian and Artinian, then we may construct a composition series of M as follows. By assumption that M is nonzero, there exists an R-submodule of M that strictly contains 0. By Definition 3.14, we may find a nonzero R-submodule M_1 of M that is minimal with respect to inclusion among all R-submodules of M that strictly contain 0. If $M_1 = M$, then we are done; otherwise, we may find a nonzero R-submodule M_2 of M that is minimal with respect to inclusion among all R-submodules of M that strictly contain M_1. Continuing in this manner yields a strictly ascending chain of R-submodules $0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots$. By hypothesis that M is Noetherian, this must be finite, hence we obtain a chain of R-submodules $0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_{n-1} \subsetneq M$ of M; it is by construction a composition series of M, hence we conclude that $\ell_R(M) \leq n$.

(ii.) Conversely, suppose that M has finite length n over R. We claim that every descending chain of R-submodules of M stabilizes. On the contrary, suppose that there exists an infinite descending chain $M_1 \supsetneq M_2 \supsetneq \cdots$ of R-submodules of M. Observe that the first $n+2$ terms of this chain yield a chain $M_{n+2} \subsetneq M_{n+1} \subsetneq \cdots \subsetneq M_2 \subsetneq M_1$. By hypothesis, M_{n+2} is nonzero, hence we may append M and the zero module to obtain a chain $0 \subsetneq M_{n+2} \subsetneq M_{n+1} \subsetneq \cdots \subsetneq M_2 \subsetneq M_1 \subseteq M$ of length at least $n+1$. Because we can refine this chain to a composition series of M of length larger than $\ell_R(M) = n$, we have reached a contradiction. Likewise, there cannot exist an infinite ascending chain of R-submodules of M. We conclude that M is Noetherian and Artinian. □

Corollary 3.16. *If M has finite length as an R-module, then M is finitely generated over R.*

Length is an especially important invariant over local rings. Our next proposition gives a useful equivalent condition for a module over a local ring to have finite length.

Proposition 3.17. *Let $(R, \mathfrak{m}, k)$ be a local ring. The following are equivalent.*

(i.) *A R-module M is Noetherian and admits an integer $n \geq 0$ such that $\mathfrak{m}^n M = 0$.*

(ii.) *An R-module M has finite length over R.*

Proof. (i.) By definition of length, it suffices to exhibit a finite composition series of M. By assumption that $\mathfrak{m}^n M = 0$ for some integer $n \geq 0$, there exists a chain of R-submodules

$$0 = \mathfrak{m}^n M \subsetneq \mathfrak{m}^{n-1} M \subsetneq \cdots \subsetneq \mathfrak{m} M \subsetneq M.$$

(We may assume without loss of generality that $\mathfrak{m}^{n-1} M$ is nonzero.) Observe that for each integer $0 \leq i \leq n-1$, we have that $M_i = \mathfrak{m}^i M / \mathfrak{m}^{i+1} M$ is a quotient of the Noetherian R-module $\mathfrak{m}^i M$, hence it is finitely generated. Each module M_i satisfies $\mathfrak{m} M_i = 0$, hence we may view each M_i as a k-vector space. By our exposition preceding Definition 3.14, the length of each finite-dimensional k-vector space M_i is finite, hence each M_i admits a finite composition series. By the Correspondence Theorem, a finite composition series of M_i induces a strict chain of R-submodules of M beginning with $\mathfrak{m}^{i+1} M$ and ending with $\mathfrak{m}^i M$ such that each successive containment is minimal. Combining each chain successively from $i = n-1$ to $i = 0$ yields a composition series for M.

(ii.) By Proposition 3.15, if M has finite length over R, then M is a Noetherian R-module. On the contrary, assume that $\mathfrak{m}^n M$ is nonzero for each integer $n \geq 0$. By definition, for each integer $n \geq 0$, there exist elements $r_1, \ldots, r_n \in \mathfrak{m}$ and $m \in M$ such that $r_1 \cdots r_n m$ is nonzero. Consider the sequence of R-modules $0 \subseteq R(r_1 \cdots r_n m) \subseteq \cdots \subseteq R(r_1 m) \subseteq Rm \subseteq M$. We claim that each containment is strict; otherwise, there would exist an integer $0 \leq k \leq n-1$ and an element $s \in R$ such that $r_1 \cdots r_k m = s r_1 \cdots r_{k+1} m$. By rearranging, we would obtain $(1_R - s r_{k+1}) r_1 \cdots r_k m = 0$. By Proposition 3.7, we would find that $1_R - s r_{k+1}$ is a unit so that $r_1 \cdots r_k m = 0$ — a contradiction. Consequently, for each integer $n \geq 0$, we have constructed a composition series of M of length $n+1$. But this is impossible by assumption that M has finite length over R. $\square$

Corollary 3.18. *Let $(R,\mathfrak{m},k)$ be a local ring. If R is Artinian as an R-module, then R has finite length as an R-module. Particularly, every Artinian local ring is Noetherian.*

Proof. By hypothesis that R is Artinian, the descending chain of ideals $\mathfrak{m} \supsetneq \mathfrak{m}^2 \supsetneq \cdots$ stabilizes, hence we must have that $\mathfrak{m}^n = 0$ for some integer $n \geq 0$. By the proof of Proposition 3.17, there exist k-vector spaces $V_i = \mathfrak{m}^i/\mathfrak{m}^{i+1}$ for each integer $0 \leq i \leq n-1$. Every descending chain of k-vector subspaces of V_i corresponds to a descending chain of ideals of R. By hypothesis that R is Artinian, the k-vector spaces V_i must be finitely generated so that R admits a composition series of finite length as in the proof of Proposition 3.17. Last, R is Noetherian by Proposition 3.15. □

By the proof of Proposition 3.17, we obtain the following important and useful fact.

Proposition 3.19. *Let R be a commutative unital ring. Let M be an R-module such that $IM = 0$ for some ideal I of R. We have that $\ell_R(M)$ is finite if and only if $\ell_{R/I}(M)$ is finite.*

Proof. If $IM = 0$, then M is an R/I-module via the action $(r+I)\cdot M = rm$. Consequently, a composition series holds for M as an R-module if and only if it holds for M as an R/I-module. □

3.2 Krull Dimension and Height

One of the most important invariants of a commutative unital ring is its dimension.

Definition 3.20. We define the **(Krull) dimension** of R to be the extended natural number

$$\dim(R) = \sup\{n \mid P_0 \supsetneq P_1 \supsetneq \cdots \supsetneq P_n \text{ and } P_0, P_1, \ldots, P_n \in \operatorname{Spec}(R)\},$$

i.e., $\dim(R)$ is the supremum of the lengths of strictly descending chains of prime ideals of R.

Example 3.21. Let k be a field. We have already seen in Example 3.5 that k is a Noetherian ring with $\operatorname{Spec}(k) = \{0_k\} = \operatorname{MaxSpec}(k)$. (By an abuse of notation, we use 0_k to denote both the zero element and the zero ideal of k.) Consequently, we have that $\dim(k) = 0$: indeed, 0_k is the only prime ideal of k, hence the only strictly descending chain of prime ideals of k is 0_k.

By definition, a commutative ring R has Krull dimension 0 if and only if every prime ideal of R is maximal. Using this observation, we make the following generalization of Example 3.21.

Proposition 3.22. *Let $(R, \mathfrak{m}, k)$ be a local ring. The following are equivalent.*

(i.) *R is Artinian*

(ii.) *R is Noetherian and* $\dim(R) = 0$.

Example 3.23. By Example 3.2, we have that $\mathrm{Spec}(\mathbb{Z}) = \{p\mathbb{Z} \mid p \text{ is a prime}\} \cup \{0\}$. Consequently, every strictly descending chain of prime ideals of $\mathbb{Z}$ is of the form $p\mathbb{Z} \supsetneq \{0\}$ for some prime p. (We assume implicitly that a prime p is nonzero.) We conclude that $\dim(\mathbb{Z}) = 1$.

On the other hand, we note that $\mathbb{Z}$ is a principal ideal domain, hence every nonzero ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some integer $n > 0$. By the Fundamental Theorem of Arithmetic, we may write $n = p_1^{e_1} \cdots p_k^{e_k}$ for some distinct primes $p_1, \ldots, p_n$ and integers $e_1, \ldots, e_k \geq 0$, so any ascending chain of ideals beginning with $n\mathbb{Z}$ stabilizes in $\mathbb{Z}$. By Definition 3.3, $\mathbb{Z}$ is Noetherian.

Proposition 3.24. *A principal ideal domain has (Krull) dimension at most one.*

Proof. Every nonzero prime ideal of a principal ideal domain is maximal. Consequently, every maximal strictly descending chain of prime ideals consists of a nonzero prime (maximal) ideal and the zero ideal. We conclude that the (Krull) dimension of a PID is at most one. □

Corollary 3.25. *Let k be a field. We have that* $\dim(k[x]) = 1$.

One can show moreover that the n-variate polynomial ring over a field k has dimension n.

Proposition 3.26. *Let k be a field. We have that* $\dim(k[x_1, \ldots, x_n]) = n$.

Essentially, the idea is to proceed by induction: the base case has already been established by Corollary 3.25; however, even in this case, the proof is beyond the scope of this expository note.

Generally, the following result holds for polynomial rings over Noetherian rings.

Proposition 3.27. *Let R be a Noetherian ring. We have that* $\dim(R[x_1, \ldots, x_n]) = \dim(R) + n$.

Remark 3.28. There exist Noetherian rings of infinite Krull dimension (cf. [Tom16, Nagata's Example]). On the other hand, there exist commutative unital rings of finite Krull dimension that are not Noetherian (cf. [SA12]). Both of these examples are quite involved, which illustrates that such rings are more pathological than ubiquitous. Even more, we will soon see that every Noetherian local ring has finite Krull dimension (cf. Corollary 3.35).

Computing the dimension of an arbitrary commutative unital ring can be computationally burdensome. Our immediate aim is therefore to introduce several concepts and facts that can be used to simplify this procedure. We begin by describing the dimension of R in a different way.

Definition 3.29. We define the **height** of a prime ideal P of R to be the extended natural number

$$\mathrm{ht}(P) = \sup\{n \mid P \supsetneq P_1 \supsetneq \cdots \supsetneq P_n \text{ and } P_1, \ldots, P_n \in \mathrm{Spec}(R)\},$$

i.e., $\mathrm{ht}(P)$ is the supremum of the lengths of strictly descending chains of prime ideals contained in P. Given an arbitrary ideal I of R, we define $\mathrm{ht}(I) = \inf\{\mathrm{ht}(P) \mid P \supseteq I \text{ and } P \in \mathrm{Spec}(R)\}$.

Proposition 3.30. *We have that* $\dim(R) = \sup\{\mathrm{ht}(M) \mid M \in \mathrm{MaxSpec}(R)\}$. *Put another way, the (Krull) dimension of R is the supremum of the heights of the maximal ideals of R.*

Proof. Every strictly descending chain of prime ideals begins with (or can be extended to a strictly descending chain of prime ideals that begins with) a maximal ideal because every maximal ideal is prime and every (prime) ideal is contained in a maximal ideal. Consequently, every maximal strictly descending chain of prime ideals begins with a maximal ideal, and the inequality $\geq$ holds. Conversely, every strictly descending chain of prime ideals contained in a maximal ideal M gives rise to a strictly descending chain of prime ideals of R, and the inequality $\leq$ holds. □

Remark 3.31. There exist commutative unital rings in which two maximal ideals have different heights. In fact, there exist Hilbert domains with this property (cf. [Rob73]).

Example 3.32. By Proposition 3.30, for a local ring $(R, \mathfrak{m})$, we have that $\dim(R) = \mathrm{ht}(\mathfrak{m})$. Particularly, for any prime ideal P of R, we have that $\dim(R_P) = \mathrm{ht}(P)$.

Our next two propositions show that height is a well-behaved invariant.

Proposition 3.33. *Let I and J be ideals of a commutative unital ring R.*

(1.) *If $I \subseteq J$, then* $\mathrm{ht}(I) \leq \mathrm{ht}(J)$.

(2.) *We have that* $\mathrm{ht}(I) = \mathrm{ht}(\sqrt{I})$, *where $\sqrt{I}$ is the* **radical** *of I, i.e.,*

$$\sqrt{I} = \{r \in R \mid r^n \in I \text{ for some integer } n \geq 1\}.$$

(3.) *We have that* $\mathrm{ht}(I) + \dim(R/I) \leq \dim(R)$.

(4.) *If R is an integral domain that is a finitely generated algebra over a field, then*

$$\mathrm{ht}(I) + \dim(R/I) = \dim(R).$$

Proof. (1.) Observe that any prime ideal P such that $P \supseteq J$ satisfies $P \supseteq I$, hence any prime ideal that satisfies $\mathrm{ht}(J) = \mathrm{ht}(P)$ must satisfy $\mathrm{ht}(I) \leq \mathrm{ht}(P) = \mathrm{ht}(J)$.

(2.) Observe that a prime ideal P satisfies $P \supseteq I$ if and only if it satisfies $P \supseteq \sqrt{I}$. One direction is clear in view of the fact that $I \subseteq \sqrt{I}$. Conversely, if $P \supseteq I$, then for any element $r \in \sqrt{I}$, we have that $r^n \in I$ implies that $r^n \in P$ so that $r \in P$ by the primality of P, i.e., $P \supseteq \sqrt{I}$.

(3.) Let P be a prime ideal of R such that $\mathrm{ht}(I) = \mathrm{ht}(P)$. If $\mathrm{ht}(P)$ is infinite, then we obtain an infinite strictly descending chain of prime ideals $P \supseteq P_1 \supseteq \cdots$, hence $\dim(R)$ is infinite. Otherwise, we obtain a strictly descending chain of prime ideals $P \supsetneq P_1 \supsetneq \cdots \supsetneq P_{n-1} \supsetneq P_n$. On the other hand, every strictly descending chain of prime ideals of R/I corresponds to a strictly descending chain of prime ideals of R such that the smallest (with respect to inclusion) prime ideal contains I. By construction, the longest among these ends with P, so we obtain a strictly descending chain of prime ideals $Q_m \supsetneq \cdots Q_1 \supsetneq P \supsetneq P_1 \cdots \supsetneq P_n$ of R. By definition, we have that

$$\mathrm{ht}(I) + \dim(R/I) = n + m \leq \dim(R).$$

We omit the proof of (4.) for the sake of simplicity. □

Theorem 3.34 (Krull's Height Theorem)**.** *Let R be a commutative unital ring. Let I be a proper ideal of R. If I is finitely generated by at least n generators, then* $\mathrm{ht}(I) \leq n$.

Corollary 3.35. *Every Noetherian local ring has finite (Krull) dimension.*

Proof. If $(R, \mathfrak{m})$ is a Noetherian local ring, then $\dim(R) = \mathrm{ht}(\mathfrak{m})$ by Example 3.32. Even more, $\mathfrak{m}$ is finitely generated by Definition 3.3, hence $\mathrm{ht}(\mathfrak{m})$ is finite by Krull's Height Theorem. □

Corollary 3.36. *Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring with unique maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$. Let $\mu(\mathfrak{m}) = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$, where $\mathfrak{m}/\mathfrak{m}^2$ is viewed as a k-vector space.*

(1.) *We have that $\mu(\mathfrak{m})$ is the minimum number of generators of $\mathfrak{m}$.*

(2.) *We have that* $\dim(R) \leq \mu(\mathfrak{m})$.

Proof. Observe that (1.) holds by Nakayama's Lemma; (2.) holds by Krull's Height Theorem. □

On its own, the invariant $\mu(\mathfrak{m})$ of a Noetherian local ring $(R, \mathfrak{m})$ is of critical importance.

Definition 3.37. Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring with residue field $k = R/\mathfrak{m}$. We refer to the invariant $\mu(\mathfrak{m}) = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$ as the **embedding dimension** of R.

3.3 Regular Sequences and Associated Primes

Eventually, we will extend the property of Proposition 3.33(4.) to a more general class of Noetherian commutative unital rings, but in order to accomplish this, we must relate the topological invariant of (Krull) dimension with some homological invariant. Unless otherwise stated, we assume throughout this section that R is a commutative unital ring and M is an arbitrary R-module.

Definition 3.38. We say that an element $x \in R$ is M-**regular** whenever

(i.) $xm = 0$ implies that $m = 0$ and

(ii.) $xM \neq M$.

If x only satisfies condition (i.), we say that x is **weakly M-regular**. We note that some authors refer to such an element as a **non-zero divisor** of M. Under this naming convention, an element $x \in R$ that does not satisfy condition (i.) of Definition 3.38 is called a **zero divisor** of M.

Remark 3.39. We note that condition (ii.) of Definition 3.38 is a provision to prevent the "degenerate" case. Particularly, if $M = 0$, then $xm = 0$ implies that $m = 0$ trivially, hence every element of R is M-regular for the zero module. On the other hand, every unit u of a ring satisfies $uR = R$, so we would like to restrict our attention to non-units acting on nonzero modules.

We will soon focus exclusively on the case that $(R, \mathfrak{m})$ is a local ring and M is a finitely generated R-module. If it were the case that $x \in \mathfrak{m}$ satisfies $xM = M$, it would follow by Nakayama's Lemma that $M = 0$, hence condition (i.) would be satisfied trivially. On the other hand, if $M \neq 0$, then $xM \neq M$ for any element $x \in \mathfrak{m}$ by the contrapositive of Nakayama's Lemma. Consequently, condition (ii.) in Definition 3.38 is satisfied by any element of $\mathfrak{m}$ (i.e., any non-unit of R).

Example 3.40. Every nonzero non-unit of $\mathbb{Z}$ is $\mathbb{Z}$-regular because $\mathbb{Z}$ is a domain that is not a field. In fact, this is the case with any domain that is not a field. On the other hand, for any nonzero element n of $\mathbb{Z}$, we have that $n\mathbb{Q} = \mathbb{Q}$, hence a nonzero integer is only weakly $\mathbb{Q}$-regular.

Definition 3.41. We say that a sequence $\underline{x} = (x_1, \ldots, x_n) \in R$ is an **M-regular sequence** if

(i.) x_1 is an M-regular element of R and

(ii.) x_{i+1} is an $M/(x_1, \ldots, x_i)M$-regular element of R for each integer $1 \leq i \leq n-1$.

Like before, we say that $\underline{x}$ is a **weakly M-regular** sequence if x_1 is weakly M-regular or x_{i+1} is weakly $M/(x_1, \ldots, x_i)M$-regular for some integer $1 \leq i \leq n-1$.

Unfortunately, a permutation of a (weakly) M-regular sequence may not be (weakly) M-regular.

Example 3.42. [BH93, Exercise 1.1.3] Consider the polynomial ring $S = k[x, y, z]$ over a field k. Observe that x is an S-regular element because it is a nonzero element of the domain S. Further, we have that $y - xy$ is an $S/(x)$-regular element because it is equal to y modulo x and $S/(x) \cong k[y, z]$.

Last, we have that $z - xz$ is an $S/(x, y - xy)$-regular element because $(x, y - xy) = (x, y)$ implies that $S/(x, y - xy) \cong k[z]$ and $z - xz$ is equal to z modulo $(x, y - xy)$. We conclude therefore that $(x, y - xy, z - xz)$ is an S-regular sequence. On the other hand, the sequence $(y - xy, z - xz, x)$ is not S-regular because $(z - xz)y = z(y - xy)$ shows that $z - xz$ is not $S/(y - xy)$-regular.

If $(R, \mathfrak{m})$ is Noetherian local, then a permutation of an M-regular sequence is again M-regular.

Proposition 3.43. *[BH93, Proposition 1.1.6] Let $(R, \mathfrak{m})$ be Noetherian local ring. Let M be a finitely generated R-module. Any permutation of an M-regular sequence is M-regular.*

Before we continue, it is worth mentioning the following propositions.

Proposition 3.44. *Let $(R, \mathfrak{m})$ be a Noetherian local ring. If $\underline{x} = (x_1, \ldots, x_n)$ forms an R-regular sequence, then $R/\underline{x}R$ admits a finite free resolution as an R-module.*

Proof. We proceed by induction on n. If $x \in R$ is R-regular, then there exists a short exact sequence $0 \to R \xrightarrow{\cdot x} R \to R/xR \to 0$. Clearly, this is a finite free resolution of R/xR as an R-module.

We will assume inductively that the claim holds for some integer $n \geq 2$. Consider the R-regular sequence $\underline{x} = (x_1, \ldots, x_n)$. By Propositions 3.101 and 3.102, it suffices to show that $R/\underline{x}R$ has finite projective dimension as an R-module. Observe that $I = (\bar{x}_2, \ldots, \bar{x}_n)$ is generated by a $\bar{R} = R/x_1R$-regular sequence, hence $R/\underline{x}R = \bar{R}/I$ admits a finite free resolution as a $\bar{R}$-module by induction. Call this free resolution $F_\bullet : 0 \to F_n \to \cdots \to F_1 \to F_0 \to R/\underline{x}R \to 0$. Each of the free $\bar{R}$-modules F_i with $1 \leq i \leq n-1$ induces a short exact sequence $0 \to K_i \to F_i \to K_{i-1} \to 0$ of $\bar{R}$-modules, and we obtain the short exact sequences $0 \to F_n \to F_{n-1} \to K_{n-1} \to 0$ and $0 \to K_0 \to F_0 \to R/\underline{x}R \to 0$ at the left- and right-hand endpoints of $F_\bullet$. Even more, each of the free $\bar{R}$-modules F_i has finite projective dimension as an R-module by the base case of the induction: by definition, F_i is the direct sum of copies of $\bar{R} = R/x_1R$, so the direct sum of copies of a projective resolution of $\bar{R}$ as an R-module yields projective resolution of F_i as an R-module. Using Corollary 3.118 on the short exact sequence $0 \to F_n \to F_{n-1} \to K_{n-1} \to 0$ shows that K_{n-1} has finite projective dimension as an R-module. By the same rationale, the short exact sequence $0 \to K_{n-1} \to F_{n-1} \to K_{n-2} \to 0$

guarantees that K_{n-2} has finite projective dimension as an R-module. Continuing in this manner, we find that $R/\underline{x}R$ has finite projective dimension as an R-module, as desired. □

We have characterized nonzero elements of R whose action on any nonzero element of M results in a nonzero element of M as (weakly) M-regular (or as a non-zero divisor on M). We will now investigate those elements of R whose action on a given nonzero element of M is always zero.

Definition 3.45. Let M be a nonzero R-module. We define the R-**annihilator** of a nonzero element $m \in M$ as $\operatorname{ann}_R(m) = \{r \in R \mid rm = 0\}$. Often, we will refer to this simply as the annihilator of m. We define also the R-**annihilator** of the entire module M as $\operatorname{ann}_R(M) = \bigcap_{m \in M} \operatorname{ann}_R(m)$.

Observe that the annihilator of any nonzero element $m \in M$ is an ideal of R: indeed, if r and s belong to $\operatorname{ann}_R(m)$, then we have that $(r+s)m = rm + sm = 0$ and $(ar)m = a(rm) = a(0) = 0$ for all elements $a \in R$. Consequently, we may consider the case that $\operatorname{ann}_R(m)$ is a prime ideal of R.

Definition 3.46. Let M be a nonzero R-module. We say that a prime ideal P of R is an **associated prime** of M if there exists a nonzero element $m \in M$ such that $P = \operatorname{ann}_R(m)$.

Example 3.47. Let $S = k[x]$ be the univariate polynomial ring over a field k. Let $M = k[x]/(x^2)$. We will denote by $\bar{x}$ the class of x modulo x^2. Observe that $x\bar{x} = \bar{x}^2 = \bar{0}_k$, hence the ideal of S generated by x is contained in the annihilator of $\bar{x}$, i.e., $(x) \subseteq \operatorname{ann}_S(\bar{x})$. But (x) is a maximal ideal of S and $\operatorname{ann}_R(\bar{x})$ is a proper ideal of S, hence we have that $\operatorname{ann}_S(\bar{x}) = (x)$ is an associated prime of M. Observe that (x) is also a minimal prime ideal of S. We will soon see that this is no coincident.

Before we proceed, we should investigate sufficient conditions for the existence of associated primes of a nonzero module. Unfortunately, this requires additional tools that are not immediately relevant to us; instead, we state the following proposition without proof.

Proposition 3.48. *Every nonzero module M over a Noetherian ring R admits an associated prime. Further, if M is Noetherian, then M admits only finitely many associated primes.*

We denote by $\operatorname{Ass}_R(M)$ the collection of associated primes of a nonzero module M over a Noetherian ring R. By the previous proposition, if M is Noetherian, then $|\operatorname{Ass}_R(M)| < \infty$.

We will now relate the associated primes of M and M-regular elements.

Proposition 3.49. *Let R be Noetherian. Let M be an R-module. The following are equivalent.*

(i.) *The element $x \in R$ is a zero divisor on M.*

(ii.) *The element $x \in R$ belongs to some associated prime P of M.*

Put another way, the collection of zero divisors of M is the union of all associated primes of M.

Proof. Let $x \in R$ be a zero divisor on M. By Proposition 3.48, M admits an associated prime P. If $x = 0_R$, then x belongs to P because every ideal of R contains 0_R. We may assume that x is nonzero. By hypothesis that x is a zero divisor on M, there exists a nonzero element $m \in M$ such that $xm = 0$, hence x belongs to $\text{ann}_R(m)$. Given that $\text{ann}_R(m)$ is prime, our proof is complete. We assume therefore that $\text{ann}_R(m)$ is not prime. By hypothesis that R is Noetherian, the collection

$$\mathfrak{A} = \{\text{ann}_R(m') \mid m' \in M, \text{ann}_R(m') \text{ is a proper ideal of } R, \text{and } \text{ann}_R(m) \subseteq \text{ann}_R(m')\}$$

has a maximal element P because it contains $\text{ann}_R(m)$ by construction. We claim that P is a prime ideal. Consider the case that some elements y and z of R satisfy $yz \in P$ and $z \notin P$. Observe that $P \subseteq \text{ann}_R(ym')$ because every element of P annihilates m' and so must annihilate ym'. On the other hand, we have that $z(ym') = (yz)m' = 0$ by assumption that $yz \in P$, hence z is an element of $\text{ann}_R(ym') \setminus P$. By the maximality of P and the fact that $\text{ann}_R(m) \subseteq \text{ann}_R(ym')$, we must have that $\text{ann}_R(ym') = R$ so that $ym' = 1_R(ym') = 0$ and y annihilates m', i.e., we have that $y \in P$. We conclude that P is an associated prime ideal of M that contains $\text{ann}_R(m)$ and x.

Conversely, if $x \in R$ belongs to some associated prime ideal P of M, then there exists a nonzero element $m \in M$ such that $xm = 0$, hence x is a zero divisor on M. □

Corollary 3.50. *Let R be Noetherian. Let M be an R-module. The following are equivalent.*

(1.) The element $x \in R$ is M-regular.

(2.) The element $x \in R$ does not belong to any associated prime P of M.

Corollary 3.51. *Let R be a Noetherian ring. Let M be an R-module. Let I be an ideal of R that consists of zero divisors of M. There exists an associated prime P of M such that $I \subseteq P$.*

Proof. We prove the contrapositive. Given that $I \nsubseteq P$ for all associated primes P of M, there exists an element $x \in I$ such that $x \notin P$ for any associated prime P by the Prime Avoidance Lemma. By Corollary 3.50, we conclude that x is M-regular, i.e., x is not a zero divisor on M. □

One can also view the property that P is an associated prime of M as a homological condition.

Proposition 3.52. *Let M be a nonzero R-module. Consider the following conditions.*

(i.) *P is an associated prime of M.*

(ii.) *M contains an R-submodule that is isomorphic to R/P for some prime ideal P.*

(iii.) *There exists a nonzero R-module homomorphism $\psi : R/P \to M$ for some prime ideal P of R. Put another way, we have that $\mathrm{Hom}_R(R/P, M) \neq 0$ for some prime ideal P of R.*

We have that (i.) $\iff$ (ii.) $\implies$ (iii.). Conversely, if either (a.) P is a maximal ideal of R or (b.) the associated primes of M are the minimal primes of R, then (iii.) $\implies$ (i.).

Proof. By definition, if P is an associated prime of M, then there exists a nonzero element $m \in M$ such that $P = \mathrm{ann}_R(m)$. Consider the map $\varphi : R \to M$ defined by $\varphi(r) = rm$. One can easily verify that this is an R-module homomorphism, hence $\varphi(R)$ is an R-submodule of M. By definition, we have that $\ker \varphi = \{r \in R \mid rm = 0\} = \mathrm{ann}_R(m) = P$, and we conclude that $R/P \cong \varphi(R)$.

Conversely, if M contains an R-submodule that is isomorphic to R/P for some prime ideal P of R, then there exists an injective R-module homomorphism $\varphi : R/P \to M$. Consequently, we have that $P = \ker \varphi = \{r + P \mid r\varphi(1_R + P) = 0\} = \mathrm{ann}_R(\varphi(1_R + P))$ is an associated prime of M.

If M contains an R-submodule N such that $\varphi : R/P \to N$ is an R-module isomorphism, then the composite map $\psi : R/P \xrightarrow{\varphi} N \xrightarrow{\subseteq} M$ is a nonzero R-module homomorphism.

Last, we will assume that there exists a nonzero R-module homomorphism $\psi : R/P \to M$ for some prime ideal P of R. Recall that $\psi : R/P \to M$ is an R-module homomorphism if and only if

(a.) ψ is well-defined, i.e., $r+P = 0_R+P$ implies that $\psi(r+P) = 0$ and

(b.) ψ is R-linear, i.e., $\psi(r+P) = r \cdot \psi(1_R+P)$ for all elements $r \in R$.

Combined, these properties say that every nonzero R-linear homomorphism $R/P \to M$ is uniquely determined by the nonzero element $\psi(1_R+P) \in M$ and $\psi(1_R+P)$ must be annihilated by P. Consequently, we find that $P \subseteq \operatorname{ann}_R(\psi(1_R+P))$. Given that (a.) P is a maximal ideal of R, we conclude that $P = \operatorname{ann}_R(\psi(1_R+P))$ is an associated prime of M. On the other hand, if P is not maximal, it follows by Corollary 3.51 that $P \subseteq Q$ for some associated prime Q of M. Given that (b.) the associated primes of M are the minimal primes of R, we conclude that $P = Q$. □

We shall soon discuss the connection between regular sequences contained in the maximal ideal $\mathfrak{m}$ of a Noetherian local ring $(R,\mathfrak{m},k)$ and the nonzero R-linear maps $k \to M$. Before we are able to state this relationship explicitly, we investigate the deeper interplay between the M-regular elements of R contained in the annihilator of some R-module N and the R-linear maps $N \to M$.

Proposition 3.53. *[BH93, Proposition 1.2.3] Let M and N be R-modules. The following hold.*

(1.) If $\operatorname{ann}_R(N)$ *contains an M-regular element, then* $\operatorname{Hom}_R(N,M) = 0$.

(2.) Conversely, if R is Noetherian and M and N are finitely generated, then $\operatorname{Hom}_R(N,M) = 0$ *implies that* $\operatorname{ann}_R(N)$ *contains an M-regular element.*

Proof. (1.) Consider an R-module homomorphism $\varphi : N \to M$. For every element $n \in N$ and $x \in \operatorname{ann}_R(N)$, we have that $\varphi(xn) = \varphi(0) = 0$. Considering that φ is R-linear and x belongs to R, we have that $0 = \varphi(xn) = x\varphi(n)$. Given that x is M-regular, we have that $\varphi(n) = 0$. But this holds for every element $n \in N$, hence we conclude that φ is the zero map so that $\operatorname{Hom}_R(N,M) = 0$.

(2.) Let R be Noetherian, and let M and N be finitely generated. We will establish the contrapositive. We assume to this end that $\operatorname{ann}_R(N)$ consists of zero divisors of M. By Corollary 3.51, there exists an associated prime P of M such that $\operatorname{ann}_R(N) \subseteq P$. Observe that $R \setminus P \subseteq R \setminus \operatorname{ann}_R(N)$ does not contain any zero divisors of N, hence P belongs to $\operatorname{Supp}(N)$. Let k denote the residue field R_P/PR_P of the local ring (R_P, PR_P). By Nakayama's Lemma, we have that $N_P \otimes_{R_P} k \cong N_P/PN_P$

is a nonzero finite-dimensional k-vector space, hence it is isomorphic to $k^{\oplus n}$ for some integer $n \geq 1$. By forming the composite map $N_P \to N_P/PN_P \cong k^{\oplus n} \to k$, we obtain a surjective homomorphism $N_P \to k$. Observe that PR_P is an associated prime of M_P, hence there exists an element $m \in M_P$ such that $PR_P = \operatorname{ann}_{R_P}(m)$. Consequently, the multiplication map $\cdot m : R_P/PR_P \to M_P$ is a well-defined R-module homomorphism. By composition, we obtain a nonzero element of $\operatorname{Hom}_{R_P}(N_P, M_P) \cong \operatorname{Hom}_R(N,M)_P$ so that $\operatorname{Hom}_R(N,M)$ is nonzero. □

Example 3.54. Let $S = k[x,y]$ be the bivariate polynomial ring over a field k. Let $M = S/(x^2)$, and let $N = S/(x,y)$. Observe that x and y annihilate N, hence we have that $\operatorname{ann}_S(N) = (x,y)$. On the other hand, the element $y \in \operatorname{ann}_S(N)$ is M-regular. We conclude that $\operatorname{Hom}_S(N,M) = 0$.

Our next proposition is the basis for the proof of the main theorem of the next section.

Proposition 3.55. *Given any R-modules M and N and a weakly M-regular sequence $(x_1, \ldots, x_n)$ in $\operatorname{ann}_R(N)$, we have that $\operatorname{Hom}_R(N, M/(x_1,\ldots,x_n)M) \cong \operatorname{Ext}^n_R(N,M)$.*

Proof. We proceed by induction on n. Observe that $\operatorname{Ext}^0_R(N,M) \cong \operatorname{Hom}_R(N,M)$ by Proposition 3.111, hence the claim holds for $n = 0$. We will assume inductively that the claim holds for all integers $1 \leq i \leq n-1$. We note that x_i is an $M/(x_1,\ldots,x_{i-1})M$-regular element by hypothesis for each integer $1 \leq i \leq n$, hence Proposition 3.53 implies that $\operatorname{Ext}^{i-1}_R(N,M) = 0$ for each integer $1 \leq i \leq n$ by induction. By Proposition 3.111, the short exact sequence

$$0 \to M \xrightarrow{x_n \cdot} M \to M/x_nM \to 0$$

induces a long exact sequence of Ext. But as we observed in the previous paragraph, the lower Ext vanish by induction, hence we obtain an exact sequence that begins with

$$0 \to \operatorname{Ext}^{n-1}_R(N, M/x_nM) \xrightarrow{\psi} \operatorname{Ext}^n_R(N,M) \xrightarrow{\varphi} \operatorname{Ext}^n_R(N,M).$$

By construction, the R-modules $\operatorname{Ext}^i_R(N,-)$ preserve multiplication for all indices $i \geq 0$, hence we have that φ is multiplication by x_n. By hypothesis that x_n belongs to $\operatorname{ann}_R(N)$, we find that φ is the

zero map. We conclude that ψ is an isomorphism, i.e., $\operatorname{Ext}_R^{n-1}(N, M/x_nM) \cong \operatorname{Ext}_R^n(N,M)$. Using induction in the second equivalence, we obtain the desired result as follows.

$$\operatorname{Ext}_R^n(N,M) \cong \operatorname{Ext}_R^{n-1}(N, M/x_nM)$$

$$\cong \operatorname{Hom}_R\left(N, \frac{M/x_nM}{(x_1,\ldots,x_{n-1})M/x_nM}\right)$$

$$\cong \operatorname{Hom}_R(N, M/(x_1,\ldots,x_n)M) \qquad \square$$

3.4 Depth and the Cohen-Macaulay Condition

We will assume throughout this section that $(R,\mathfrak{m},k)$ is a Noetherian local ring with unique maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$. We will also assume that M is a finitely generated R-module. Our next proposition illustrates the nice behavior of R and M in this setting.

Proposition 3.56. *Let $(R,\mathfrak{m},k)$ be a Noetherian local ring. Let M be a finitely generated R-module. The following properties hold.*

(1.) R has finite (Krull) dimension. Further, we have that $\dim(R) = \operatorname{ht}(\mathfrak{m})$.

(2.) R admits finitely many associated primes. In particular, R admits an associated prime.

(3.) An element $x \in R$ is R-regular if and only if x does not belong to any associated prime of R.

(4.) M is a Noetherian R-module.

(5.) Every permutation of an M-regular sequence is an M-regular sequence.

(6.) M admits finitely many associated primes. In particular, M admits an associated prime.

(7.) An element $x \in R$ is M-regular if and only if x does not belong to any associated prime of M.

(8.) We have that $\operatorname{Hom}_R(k,M) = 0$ *if and only if* $\mathfrak{m}$ *contains an M-regular element.*

(9.) Given any M-regular sequence $(x_1,\dots,x_n)\in\mathfrak{m}$, for all integers $0\leq i\leq n-1$, we have that

$$\operatorname{Ext}^i_R(k,M)\cong\operatorname{Hom}_R(k,M/(x_1,\dots,x_i)M)=0.$$

Proof. Observe that property (1.) holds by Corollary 3.35. Property (2.) holds by Proposition 3.48, and property (6.) holds by the same proposition as soon as we establish property (4.). Properties (3.) and (7.) hold by Corollary 3.50. Property (5.) holds by Proposition 3.42. Property (8.) holds by Proposition 3.53. Property (9.) holds by the proof of Proposition 3.55.

One can show that property (4.) is equivalent to the condition that M is finitely generated when R is a Noetherian ring. Explicitly, if M is finitely generated by n elements, then M is isomorphic to a quotient of the Noetherian R-module R^n, hence M is Noetherian. Conversely, if M is Noetherian, then M is finitely generated by the analog of the third condition of Definition 3.3. □

By hypothesis that R is Noetherian, every ascending chain of ideals of R eventually stabilizes. Consequently, we can recursively build M-regular sequences of elements in the maximal ideal $\mathfrak{m}$ of R. Observe that if $\mathfrak{m}$ is an associated prime of M, then every element $x\in\mathfrak{m}$ is a zero divisor on M. Conversely, if $\mathfrak{m}$ is not an associated prime of M, then there exists an M-regular element $x_1\in\mathfrak{m}$. We can subsequently ask if there exists an M/x_1M-regular element $x_2\in\mathfrak{m}$. Continuing in this way, we obtain an ascending chain of ideals $(x_1)\subseteq(x_1,x_2)\subseteq\cdots$ that must eventually stabilize. One natural question to ask of this is, "How many elements can we possibly fit in an M-regular sequence?" Our immediate task is to answer this question. We introduce the tools to do so next.

Definition 3.57. We say that an M-regular sequence $\underline{x}=(x_1,\dots,x_n)$ is a **maximal M-regular sequence** if $\mathfrak{m}$ consists of zero divisors for $M/\underline{x}M$, i.e., $\mathfrak{m}$ is an associated prime of $M/\underline{x}M$.

Theorem 3.58 (Rees)**.** *Every maximal M-regular sequence in $\mathfrak{m}$ consists of the same number of terms. Particularly, this invariant is referred to as the* **depth** *of M, and it is given by*

$$\operatorname{depth}(M)=\inf\{i\geq 0\mid\operatorname{Ext}^i_R(k,M)\neq 0\}.$$

Proof. Consider a maximal M-regular sequence $\underline{x} = (x_1, \ldots, x_n)$ in $\mathfrak{m}$. By definition, each element x_{i+1} is $M/(x_1, \ldots, x_i)M$-regular for each integer $0 \leq i \leq n-1$. Consequently, we have that

$$\operatorname{Ext}^i_R(k, M) \cong \operatorname{Hom}_R(k, M/(x_1, \ldots, x_i)M) = 0$$

for each integer $0 \leq i \leq n-1$ by Proposition 3.56. On the other hand, by hypothesis that $\underline{x}$ is a maximal M-regular sequence in $\mathfrak{m}$, it follows that $\mathfrak{m}$ consists of zero divisors of $M/\underline{x}M$. By Corollary 3.51, we conclude that $\mathfrak{m}$ is an associated prime of $M/\underline{x}M$. By Proposition 3.52, we conclude that $\operatorname{Hom}_R(k, M/\underline{x}M) \neq 0$ so that $\operatorname{Ext}^n_R(k, M) \cong \operatorname{Hom}_R(k, M/\underline{x}M) \neq 0$. □

We refer to the k-vector space dimension of $\operatorname{Ext}^{\operatorname{depth}(M)}_R(k, M)$ as the (Cohen-Macaulay) **type** of M, denoted by $r(M) = \dim_k \operatorname{Ext}^{\operatorname{depth}(M)}_R(k, M)$. We will return to this invariant later.

Our next proposition yields a surprising formula for the injective dimension of any R-module of finite injective dimension. We omit the proof for the sake of brevity.

Theorem 3.59. *[BH93, Theorem 3.1.17] If* $\operatorname{injdim}_R(M) < \infty$, *then* $\operatorname{injdim}_R(M) = \operatorname{depth}(R)$.

We note the following necessary and sufficient condition for a module to have depth zero.

Corollary 3.60. *We have that* $\operatorname{depth}(M) = 0$ *if and only if* $\mathfrak{m}$ *is an associated prime of* M.

Proof. Observe that $\operatorname{depth}(M) = 0$ if and only if $\operatorname{Ext}^0_R(k, M) \neq 0$ if and only if $\operatorname{Hom}_R(k, M) \neq 0$ if and only if $\mathfrak{m}$ is an associated prime of M by Proposition 3.52. □

Example 3.61. Let k be a field. Let $k[\![x, y]\!]$ denote the ring of bivariate formal power series. Observe that $k[\![x, y]\!]$ is a Noetherian local ring: it is the completion of the Noetherian ring $k[x, y]$ at the homogeneous maximal ideal (x, y). Consider the Noetherian local ring $R = k[\![x, y]\!]/(x^2, xy)$. We claim that $\operatorname{depth}(R) = 0$. Each of the generators of the maximal ideal $\mathfrak{m} = (\bar{x}, \bar{y})$ is a zero divisor on R, hence we conclude that $\mathfrak{m}$ is an associated prime of R and $\operatorname{depth}(R) = 0$ by Corollary 3.60.

Our next proposition illustrates that depth behaves well with respect to short exact sequences.

Lemma 3.62 (Depth Lemma)**.** *Let $(R,\mathfrak{m},k)$ be a Noetherian local ring. For any short exact sequence of finitely generated R-modules $0 \to L \to M \to N \to 0$, the following inequalities hold.*

(1.) $\operatorname{depth}(L) \geq \min\{\operatorname{depth}(M), \operatorname{depth}(N)+1\}$

(2.) $\operatorname{depth}(M) \geq \min\{\operatorname{depth}(L), \operatorname{depth}(N)\}$

(3.) $\operatorname{depth}(N) \geq \min\{\operatorname{depth}(L)-1, \operatorname{depth}(M)\}$

Further, if $\operatorname{depth}(M) \geq \operatorname{depth}(N)+1$, *then we have that* $\operatorname{depth}(L) = \operatorname{depth}(N)+1$.

Proof. Consider a short exact sequence $0 \to L \to M \to N \to 0$ of finitely generated modules over a local ring $(R,\mathfrak{m},k)$. We have that $\operatorname{depth}(L) = \min\{i \mid \operatorname{Ext}^i_R(k,L) \neq 0\}$, hence we may apply $\operatorname{Hom}_R(k,-)$ to our short exact sequence to obtain a long exact sequence

$$0 \to \operatorname{Hom}_R(k,L) \to \operatorname{Hom}_R(k,M) \to \operatorname{Hom}_R(k,N)$$

$$\to \operatorname{Ext}^1_R(k,L) \to \operatorname{Ext}^1_R(k,M) \to \operatorname{Ext}^1_R(k,N) \to \cdots.$$

(i.) Given that $\operatorname{depth}(L) = d$, we have that $\operatorname{Ext}^d_R(k,L) \neq 0$ and $\operatorname{Ext}^i_R(k,L) = 0$ for all integers $0 \leq i \leq d-2$. Consequently, there are R-module isomorphisms $\operatorname{Ext}^i_R(k,M) \cong \operatorname{Ext}^i_R(k,N)$ for all integers $0 \leq i \leq d-1$, and the rest of our long exact sequence can be written as

$$0 \to \operatorname{Ext}^{d-1}_R(k,M) \to \operatorname{Ext}^{d-1}_R(k,N) \to \operatorname{Ext}^d_R(k,L) \to \operatorname{Ext}^d_R(k,M) \to \operatorname{Ext}^d_R(k,N) \to \cdots.$$

We claim that $\operatorname{depth}(L) \geq \min\{\operatorname{depth}(M), \operatorname{depth}(N)+1\}$. On the contrary, we will assume that $\operatorname{depth}(M) \geq \operatorname{depth}(L)+1$ and $\operatorname{depth}(N) \geq \operatorname{depth}(L)$. But this implies that

$$\operatorname{Ext}^{d-1}_R(k,M) = \operatorname{Ext}^d_R(k,M) = 0$$

and $\operatorname{Ext}^d_R(k,L) \cong \operatorname{Ext}^{d-1}_R(k,N) = 0$ — a contradiction. We conclude that

$$\operatorname{depth}(L) \geq \min\{\operatorname{depth}(M), \operatorname{depth}(N)+1\}.$$

We note that the other assertions are proved in a similar way. □

Even more, depth behaves well with respect to taking quotients by regular sequences.

Proposition 3.63. *Let $\underline{x} = (x_1, \ldots, x_n)$ be an M-regular sequence. We have that*

$$\operatorname{depth}(M/\underline{x}M) = \operatorname{depth}(M) - n.$$

Proof. By the proof of Proposition 3.55, we have that $\operatorname{Ext}^i_R(k,M) \cong \operatorname{Ext}^{i-n}_R(k, M/\underline{x}M)$ for all integers $i \geq n$. By hypothesis, we have that $\operatorname{depth}(M) \geq n$, hence we conclude that

$$\begin{aligned}
\operatorname{depth}(M) - n &= \inf\{i \geq 0 \mid \operatorname{Ext}^i_R(k,M) \neq 0\} - n \\
&= \inf\{i - n \geq 0 \mid \operatorname{Ext}^i_R(k,M) \neq 0\} \\
&= \inf\{i - n \geq 0 \mid \operatorname{Ext}^{i-n}_R(k, M/\underline{x}M) \neq 0\} \\
&= \operatorname{depth}(M/\underline{x}M),
\end{aligned}$$

where the first and last equalities hold by Theorem 3.58 and the third holds by isomorphism. □

Unlike with taking quotients, localizing at a prime ideal can sometimes increase depth.

Proposition 3.64. *Let P be a prime ideal of R. We have that*

(1.) $\operatorname{depth}(M) \leq \dim(R/P)$ *if P is an associated prime of M and*

(2.) $\operatorname{depth}(M) \leq \dim(R/P) + \operatorname{depth}(M_P)$.

Proof. (1.) We proceed by induction on $\operatorname{depth}(M)$. Given that $\operatorname{depth}(M) = 0$, the claim holds trivially. Given that $\operatorname{depth}(M) = 1$, by Proposition 3.60, $\mathfrak{m}$ is not an associated prime of M, hence

for any associated prime P of M, we have that $\mathfrak{m} \supsetneq P$ so that $\dim(R/P) \geq 1$, and the claim holds. Consider the case that $\operatorname{depth}(M) \geq 2$. By definition, there exists an M-regular element $x \in \mathfrak{m}$. Given an associated prime P of M, we have that $P = \operatorname{ann}_R(m)$ for some nonzero element $m \in M$, hence the collection $\mathfrak{C} = \{\operatorname{ann}_R(m) \mid m \in M \text{ is nonzero and } \operatorname{ann}_R(m) \subseteq P\}$ is nonempty. By Proposition 3.56(4.), M is Noetherian, hence there exists a maximal element of $\mathfrak{C}$, i.e., a maximal ideal $\operatorname{ann}_R(a)$ that is annihilated by P. On the contrary, if a belonged to xM, then there would exist a nonzero element $b \in M$ such that $a = xb$. Observe that P annihilates a, hence P annihilates xb, so P must annihilate b because x is M-regular. Consequently, we would find that $\operatorname{ann}_R(b) \subseteq P$ $\operatorname{ann}_R(a) \subsetneq \operatorname{ann}_R(b)$ — a contradiction. We conclude that a does not belong to xM, hence P annihilates $a + xM$ so that P consists of zero divisors of M/xM. By Corollary 3.51, P belongs to some associated prime Q of M/xM. We claim that $P \subsetneq Q$, from which it follows that

$$\dim(R/P) - 1 \geq \dim(R/Q) \geq \operatorname{depth}(M/xM) = \operatorname{depth}(M) - 1$$

by induction, and we conclude that $\operatorname{depth}(M) \leq \dim(R/P)$. Observe that $x \notin P$ by hypothesis that P annihilates m and x is M-regular, hence x belongs to $R \setminus P$ so that $(M/xM)_P = 0$ (cf. Example 3.32). On the other hand, as Q is an associated prime of M/xM, there exists a nonzero element $m' + xM \in M/xM$ such that $Q = \operatorname{ann}_R(m' + xM) = \{r \in R \mid rm' \in xM\}$. Consequently, for every element $s \in R \setminus Q$, we have that $sm' \notin xM$ so that $(M/xM)_Q \neq 0$. We conclude that $P \subsetneq Q$.

(2.) By convention, if $M_P = 0$, then $\operatorname{depth}(M_P)$ is infinite, and the claim holds. Our proof is also complete if $\operatorname{depth}(M) \leq \dim(R/P)$. We may assume therefore that $\operatorname{depth}(M) > \dim(R/P)$ and M_P is nonzero. Consequently, by (1.), P is not an associated prime of M, hence P cannot belong to any associated prime of M. By Corollary 3.51, there exists an M-regular element $x \in P$. By Proposition 3.63, we have that $\operatorname{depth}(M/xM) = \operatorname{depth}(M) - 1$ and $\operatorname{depth}(M_P/xM_P) = \operatorname{depth}(M_P) - 1$. By induction on $\operatorname{depth}(M)$, we conclude that $\operatorname{depth}(M) \leq \dim(R/P) + \operatorname{depth}(M_P)$. □

Observe that the depth of a module measures its "homological bigness." On the other hand, the (Krull) dimension of a module measures its "topological bigness." Our immediate aim is to

compare the two invariants. Before we do, we demonstrate that depth and dimension behave well with respect to taking the quotient by a regular sequence (known colloquially as "cutting down").

Definition 3.65. We define the (Krull) **dimension** of a module as $\dim(M) = \dim(R/\operatorname{ann}_R(M))$.

Proposition 3.66. *Let $\underline{x} = (x_1, \ldots, x_n)$ be an M-regular sequence. We have that*

$$\dim(M/\underline{x}M) = \dim(M) - n.$$

Proposition 3.67. *We have that* $\operatorname{depth}(M) \leq \dim(M)$.

Proof. By Theorem 3.58, it follows that $\operatorname{depth}(M)$ is equal to the number of terms of any maximal M-regular sequence. Observe that for any maximal M-regular sequence $\underline{x} = (x_1, \ldots, x_n)$ in $\mathfrak{m}$, we have that $\dim(M/\underline{x}M) = \dim(M) - n$ by Proposition 3.66. By Definition 3.65, we have that $\dim(M/\underline{x}M) = \dim(R/\operatorname{ann}_R(M/\underline{x}M)) \geq 0$ so that $\operatorname{depth}(M) = n \leq \dim(M)$. □

Our next example illustrates that this inequality may be strict.

Example 3.68. Let k be a field. Consider the Noetherian local ring $R = k[\![x,y]\!]/(x^2,xy)$ of Example 3.61. We claim that $\dim(R) = 1$. Observe that $\operatorname{ht}(x^2,xy) = \operatorname{ht}(x,xy) = \operatorname{ht}(x) = 1$ in $k[\![x,y]\!]$, hence $\dim(R) \leq \dim(k[\![x,y]\!]) - \operatorname{ht}(x^2,xy) = 2-1 = 1$ by Proposition 3.33(4.). On the other hand, $(\bar{x},\bar{y}) \supsetneq (\bar{x})$ is a strictly descending chain of prime ideals in R so that $\dim(R) = 1 > 0 = \operatorname{depth}(R)$.

We note that Examples 3.47 and 3.61 are exemplary of a more general phenomenon.

Proposition 3.69. *Every minimal prime of R is an associated prime of R.*

Proof. Observe that a minimal prime ideal P of R must have $\operatorname{ht}(P) = 0$, hence we have that $\operatorname{depth}(R_P) \leq \dim(R_P) = \operatorname{ht}(P) = 0$. By Corollary 3.60, we have that PR_P is an associated prime of R_P, hence there exists an element r/s of R_P such that $PR_P = \operatorname{ann}_{R_P}(r/s)$. Using properties of localization, we conclude that $P = \operatorname{ann}_R(r)$ (cf. [Gat13, Proposition 6.7] for details). □

We have seen in Proposition 3.67 that M is at least as "topologically large" as it is "homologically large." Consequently, it is worth investigating when these two notions of size agree.

Definition 3.70. We say that a nonzero module M over a Noetherian local ring is **Cohen-Macaulay** if $\text{depth}(M) = \dim(M)$. By convention, the zero module is Cohen-Macaulay, and a Noetherian local ring R is Cohen-Macaulay if it is Cohen-Macaulay as an R-module.

Example 3.71. Let k be a field. Let $S = k[\![x,y]\!]$ denote the bivariate ring of formal power series. Observe that (x,y) is an S-regular sequence, hence we have that $0 = \dim(S/(x,y)) = \dim(S) - 2$ by Proposition 3.66. On the other hand, we have that $2 \leq \text{depth}(S) \leq \dim(S) = 2$ by Theorem 3.58 and Proposition 3.67. We conclude that $k[\![x,y]\!]$ is Cohen-Macaulay.

Our next proposition illustrates that Cohen-Macaulay rings behave well with respect to "cutting down" by an R-regular sequence. Quite importantly, this allows us to reduce to the 0-dimensional case by taking the quotient of a Cohen-Macaulay ring by a maximal R-regular sequence.

Proposition 3.72. *Let $\underline{x} = (x_1, \ldots, x_n)$ be an R-regular sequence. We have that R is Cohen-Macaulay if and only if $R/\underline{x}R$ is Cohen-Macaulay.*

Proof. By Proposition 3.63, we have that $\text{depth}(R/\underline{x}R) = \text{depth}(R) - n$. By Proposition 3.66, we have that $\dim(R/\underline{x}R) = \dim(R) - n$. Consequently, we have that $\dim(R) = \text{depth}(R)$ if and only if $\dim(R) - n = \text{depth}(R) - n$ if and only if $\dim(R/\underline{x}R) = \text{depth}(R/\underline{x}R)$. □

Our next proposition illustrates that the ideals of Cohen-Macaulay local rings exhibit behavior similar to the ideals of a domain that is a finitely generated algebra over a field. Particularly, Proposition 3.33(4.) holds for the ideals of a Cohen-Macaulay local ring.

Proposition 3.73. *Let $(R, \mathfrak{m}, k)$ be a Cohen-Macaulay local ring of dimension d.*

(1.) *For each prime ideal P of R, we have that R_P is Cohen-Macaulay.*

(2.) *For each prime ideal P of R, we have that* $\text{ht}(P) + \dim(R/P) = \dim(R)$. *Consequently, for any ideal I of R, we have that* $\text{ht}(I) + \dim(R/I) = \dim(R)$.

(3.) *We have that* $\text{Ass}_R(R) = \text{MinSpec}(R) = \{P \in \text{Spec}(R) \mid \dim(R/P) = \dim(R)\}$.

Proof. (1.) We proceed by induction on the dimension d of R. Observe that if $d = 0$, every prime ideal of R has $\dim(R_P) = \mathrm{ht}(P) = 0$, and the claim holds by Proposition 3.67. We will assume the claim holds for $d-1$. Consider a strictly descending chain of prime ideals

$$\mathfrak{m} \supsetneq P_1 \supsetneq \cdots \supsetneq P_{n-1} \supsetneq P_n = P$$

of maximum length n. Observe that $\dim(R/P_1) = 1$. Certainly, the inequality $\geq$ holds by the Correspondence Theorem. On the other hand, if it were a strict inequality $>$, then we would obtain a longer strictly descending chain of prime ideals of R — a contradiction. On the other hand, we have that $\dim(R_{P_1}) \leq d-1$ because $\mathfrak{m}$ can be appended to any strictly descending chain of prime ideals contained in P_1. By Proposition 3.64, we find that

$$\mathrm{depth}(R_{P_1}) \geq \mathrm{depth}(R) - \dim(R/P_1) = \mathrm{depth}(R) - 1 = d - 1 \geq \dim(R_{P_1})$$

by hypothesis that R is Cohen-Macaulay. By a similar rationale (or induction on the length n), we find that $\mathrm{depth}(R_P) \geq \dim(R_P)$, and our claim holds by induction.

(2.) By part (1.), R_P is Cohen-Macaulay, from which it follows that $\dim(R_P) = \mathrm{depth}(R_P)$. By Proposition 3.33(3.), the inequality $\leq$ holds. Conversely, by Proposition 3.64, we have that $\mathrm{ht}(P) + \dim(R/P) = \dim(R_P) + \dim(R/P) = \mathrm{depth}(R_P) + \dim(R/P) \geq \mathrm{depth}(R) = \dim(R)$.

(3.) By Proposition 3.69, the inclusion $\supseteq$ holds. Conversely, if P is an associated prime of R, then $\mathrm{ht}(P) = \dim(R_P) = \mathrm{depth}(R_P) = 0$ by Corollary 3.60, hence P is a minimal prime of R. Given any minimal prime P of R, we have that $\dim(R) = \dim(R/P) + \mathrm{ht}(P) = \dim(R/P)$. □

3.5 Systems of Parameters and Regular Local Rings

Every ideal of a Noetherian local ring that is generated by a regular sequence can be extended to an ideal whose radical is equal to the maximal ideal. One of our main objectives in this section is to establish that for a Cohen-Macaulay local ring, the converse holds. We will assume throughout that $(R, \mathfrak{m}, k)$ is a Noetherian local ring with maximal ideal $\mathfrak{m}$, residue field $k = R/\mathfrak{m}$, and $\dim(R) = d$.

Definition 3.74. We say that a collection of elements $x_1, \ldots, x_d \in \mathfrak{m}$ is a **system of parameters** (or s.o.p.) whenever there exists an integer $n \gg 0$ such that the ideal $I = (x_1, \ldots, x_d)$ satisfies $\mathfrak{m}^n \subseteq I \subseteq \mathfrak{m}$ (or equivalently, if $\sqrt{I} = \mathfrak{m}$, i.e., I is $\mathfrak{m}$-primary). We refer to an ideal of R that is generated by a system of parameters as a **parameter ideal**. If the elements $x_1, \ldots, x_d$ are R-regular, moreover, we say that $(x_1, \ldots, x_d)$ is a **regular system of parameters**.

Proposition 3.75. *If I is a parameter ideal of R, then $\mu(I) = \dim_k(I/\mathfrak{m}I) \geq \dim(R) = d$.*

Proof. Observe that $d = \dim(R) = \mathrm{ht}(\mathfrak{m}) = \mathrm{ht}(\sqrt{I}) = \mathrm{ht}(I) \leq \mu(I)$ by Krull's Height Theorem. □

Equivalently, the quotient of R by a parameter ideal I is Artinian, i.e., $\dim(R/I) = 0$.

Proposition 3.76. *The following conditions are equivalent.*

(i.) *There exist elements $x_1, \ldots, x_d \in \mathfrak{m}$ such that $I = (x_1, \ldots, x_d)$ satisfies $\mathfrak{m}^n \subseteq I \subseteq \mathfrak{m}$.*

(ii.) *There exist elements $x_1, \ldots, x_d \in \mathfrak{m}$ such that $I = (x_1, \ldots, x_d)$ satisfies $\dim(R/I) = 0$.*

Proof. We will assume first that condition (i.) holds. Consider a prime ideal P of R that contains I. Observe that $\mathfrak{m}^n \subseteq I \subseteq P$ implies that $\mathfrak{m} \subseteq P$, from which we conclude that $P = \mathfrak{m}$. Put another way, we have that $\mathrm{Spec}(R/I) = \{\mathfrak{m}/I\}$ so that $\dim(R/I) = 0$, as desired.

Conversely, suppose that condition (ii.) holds. Each of the generators of I belongs to $\mathfrak{m}$, hence we have that $I \subseteq \mathfrak{m}$. On the other hand, if there were another prime ideal P of R such that $I \subseteq P \subsetneq \mathfrak{m}$, then we would obtain a strictly descending chain of ideals $\mathfrak{m}/I \supsetneq P/I$ of R/I of length 1 — a contradiction. We conclude that $\mathfrak{m}$ is the only prime ideal of R lying over I, hence we have that $\sqrt{I} = \mathfrak{m}$. Considering that R is Noetherian, this is equivalent to $\mathfrak{m}^n \subseteq I \subseteq \mathfrak{m}$. □

Our next proposition illustrates that the quotient of a ring by an ideal generated by elements of a system of parameters behaves similarly to the quotient of a ring by a regular sequence.

Proposition 3.77. *If $x_1, \ldots, x_i \in \mathfrak{m}$ belong to a system of parameters for R, then*

$$\dim(R/(x_1, \ldots, x_i)) = d - i.$$

Proof. We proceed by induction on i. We assume first that x_1 belongs to a system of parameters. By definition, there exist elements $y_2, \ldots, y_d \in \mathfrak{m}$ such that $I = (x_1, y_2, \ldots, y_d)$ is a parameter ideal. Let $I' = (y_2, \ldots, y_d)$, $R' = R/x_1R$, and $\dim(R') = d'$. Observe that $R/I \cong R'/I'$, from which it follows that $\dim(R'/I') = \dim(R/I) = 0$ by Proposition 3.76. We conclude that I' is a parameter ideal of R', hence by Proposition 3.75, we must have that $d-1 \geq \mu(I') \geq \dim(R') = \dim(R/x_1R)$. Conversely, if the images of $z_1, \ldots, z_{d'} \in R$ generate a parameter ideal of R', then $x_1, z_1, \ldots, z_{d'}$ generate a parameter ideal of R. By the same rationale as before, we have that $d'+1 \geq \dim(R)$ so that $\dim(R/x_1R) \geq d-1$. We assume now that the claim holds for $i-1$. Let $x_1, \ldots, x_i$ belong to a system of parameters of R. Let $I' = (x_2, \ldots, x_i)$, and let $R' = R/x_1R$. By induction, we have that $\dim(R'/I') = \dim(R') - (i-1) = (d-1) - (i-1) = d-i$, and our proof is complete. □

We establish one of the main results of this section.

Proposition 3.78. *The following conditions are equivalent.*

(i.) *Every system of parameters of R is an R-regular sequence.*

(ii.) *There exists a system of parameters of R that is an R-regular sequence.*

(iii.) *R is Cohen-Macaulay.*

Proof. Clearly, condition (i.) implies condition (ii.). On the other hand, if there exists a system of parameters of R that is an R-regular sequence, then we must have that $\operatorname{depth}(R) \geq \dim(R)$. By Proposition 3.67, we conclude that R is Cohen-Macaulay, hence condition (ii.) implies condition (iii.). Last, we will assume that R is Cohen-Macaulay. We proceed by induction on the dimension d of R. We may assume that the claim holds for $d-1$ because the case $d = 0$ is vacuously true. Consider a system of parameters $x_1, \ldots, x_d \in \mathfrak{m}$. Observe that x_1 cannot belong to any minimal prime P of R; otherwise, we would have that $d-1 = \dim(R/x_1R) \geq \dim(R/P) = \dim(R) = d$ by Propositions 3.73 and 3.77 — a contradiction. Consequently, x_1 does not belong to any associated prime of R by Proposition 3.73. We conclude by Corollary 3.50 that x_1 is R-regular. By induction, we conclude that $(\bar{x}_2, \ldots, \bar{x}_d)$ is an R/x_1R-regular sequence, hence $(x_1, \ldots, x_d)$ is an R-regular sequence. Considering that this holds for any system of parameters, we are done. □

We say that a Noetherian local ring $(R, \mathfrak{m}, k)$ is a **regular local ring** if its dimension is as large as possible, i.e., $\dim(R) = \mu(\mathfrak{m}) = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$. Consequently, the maximal ideal of a regular local ring is generated by a system of parameters; moreover, it is generated by an R-regular sequence.

Proposition 3.79. *If $(R, \mathfrak{m})$ is a regular local ring, then $\mathfrak{m}$ is generated by an R-regular sequence.*

Proof. We proceed by induction on $d = \dim(R)$. Let $x_1 \in \mathfrak{m}$ be any minimal generator of $\mathfrak{m}$. One can prove that every regular local ring R is a domain, so x_1 is a non-zero divisor of R. Because x_1 belongs to $\mathfrak{m}$, it is a non-unit, hence x_1R does not equal R and x_1 is R-regular. We conclude that $\mathfrak{m} = x_1R$ is generated by an R-regular sequence. We will assume therefore that the claim holds for $d-1$. Let $x_1, \ldots, x_d$ be a minimal system of generators of $\mathfrak{m}$. By definition, $x_1, \ldots, x_d$ is a system of parameters for $\mathfrak{m}$, hence by Proposition 3.77, we have that

$$\dim(\bar{R}) = \dim(R/x_1R) = d - 1 = \mu(\bar{x}_2, \ldots, \bar{x}_d) = \mu(\bar{\mathfrak{m}}).$$

Consequently, $(\bar{R}, \bar{\mathfrak{m}})$ is a regular local ring of dimension $d-1$. By induction, $(\bar{x}_2, \ldots, \bar{x}_d)$ is a $\bar{R}$-regular sequence. But x_1 is R-regular, hence $(x_1, \ldots, x_d)$ is an R-regular sequence. □

Corollary 3.80. *Every regular local ring is Cohen-Macaulay; the converse is not true.*

Proof. By Proposition 3.79, the unique maximal ideal of a regular local ring is generated by a regular sequence; such a Noetherian local ring is Cohen-Macaulay by Proposition 3.78.

Conversely, consider the Noetherian local ring $S = k[\![x, y]\!]/(x^2, y^2)$. Let $\bar{x}$ and $\bar{y}$ denote the class of x and y modulo (x^2, y^2). Observe that S has dimension 0, hence S is a Cohen-Macaulay local ring. Explicitly, the prime ideals of S correspond to prime ideals of $k[\![x, y]\!]$ that contain (x^2, y^2). But any such prime ideal must contain both x and y, hence the only prime ideal of S is $(\bar{x}, \bar{y})$. On the other hand, the maximal ideal of S is exactly $\bar{\mathfrak{m}} = (\bar{x}, \bar{y})$ with $\mu(\bar{\mathfrak{m}}) = 2 > 0 = \dim(S)$. □

By Proposition 3.77, the dimension of a Noetherian local ring modulo a subset S of a system of parameters drops by $|S|$. By the proof of Proposition 3.79, the quotient of a regular local ring by

a minimal generator of the maximal ideal is a regular local ring. Our next proposition illustrates that this property holds for any ideal generated by a subset of a regular system of parameters.

Proposition 3.81. *[BH93, Proposition 2.2.4] Let $(R,\mathfrak{m},k)$ be a regular local ring of dimension d. Let I be a proper ideal of R. The following statements are equivalent.*

(i.) *R/I is a regular local ring.*

(ii.) *I is generated by a subset of a regular system of parameters.*

Proof. Given that I is generated by a subset $\{x_1,\dots,x_k\}$ of a (regular) system of parameters of R, it follows that $\dim(R/I) = d-k = \mu(\mathfrak{m}/I)$, hence R/I is a regular local ring.

Conversely, suppose that R/I is a regular local ring. One can prove that a regular local ring is a domain, hence I is a prime ideal of R. Further, we have that $\mu(\mathfrak{m}/I) = \dim(R/I) = d'$. Observe that $(\mathfrak{m}/I)^2 = (\mathfrak{m}^2+I)/I$, hence we have that $\mu(\mathfrak{m}/I) = \dim_k(\mathfrak{m}/(\mathfrak{m}^2+I))$. Consider the short exact sequence of k-vector spaces

$$0 \to \frac{I}{\mathfrak{m}^2\cap I} \xrightarrow{\varphi} \frac{\mathfrak{m}}{\mathfrak{m}^2} \xrightarrow{\psi} \frac{\mathfrak{m}}{\mathfrak{m}^2+I} \to 0$$

determined by $\varphi(x+\mathfrak{m}^2\cap I) = x+\mathfrak{m}^2$ and $\psi(x+\mathfrak{m}^2) = x+\mathfrak{m}^2+I$. By the Rank-Nullity Theorem, we have that $\dim_k(\mathfrak{m}/(\mathfrak{m}^2+I)) + \dim_k(I/(\mathfrak{m}^2\cap I)) = \dim_k(\mathfrak{m}/\mathfrak{m}^2) = \mu(\mathfrak{m}) = d$, from which it follows that $\dim_k(I/(\mathfrak{m}^2\cap I)) = d - \dim_k(\mathfrak{m}/(\mathfrak{m}^2+I)) = d-d'$. Consequently, by Nakayama's Lemma, we obtain elements $x_1,\dots,x_{d-d'}$ of I that belong to a minimal generating set of $\mathfrak{m}$. By hypothesis that $(R,\mathfrak{m})$ is a regular local ring, it follows that $x_1,\dots,x_{d-d'}$ belong to a regular system of parameters, hence we find that $\dim(R/(x_1,\dots,x_{d-d'})) = d-(d-d') = d'$ by Proposition 3.77. On the other hand, we have that $\mu(\mathfrak{m}/(x_1,\dots,x_{d-d'}) = d'$, hence we have that $R/(x_1,\dots,x_{x-d'})$ is a regular local ring. Particularly, $(x_1,\dots,x_{d-d'})$ is a prime ideal of R that is contained in the prime ideal I of R and satisfies $\dim(R/(x_1,\dots,x_{d-d'}) = \dim(R/I)$. We conclude by the Correspondence Theorem that $I = (x_1,\dots,x_{d-d'})$ is generated by a subset of a regular system of parameters. □

Regular local rings are in some sense the "best behaved" class of Noetherian local rings. By

Corollary 3.80, every regular local ring is Cohen-Macaulay, but there exist Cohen-Macaulay local rings that are not regular. Consequently, one might naturally wonder "how far" a Cohen-Macaulay local ring is from being regular. We aim to address this question in the coming sections.

We conclude this section with the following landmark result of Cohen.

Theorem 3.82 (Cohen Structure Theorem)**.** *[Coh46] A complete commutative unital Noetherian local ring is the homomorphic image of a complete Noetherian regular local ring. Explicitly, if* $(R,\mathfrak{m},k)$ *is a complete commutative unital Noetherian local ring, then one of the following holds.*

(1.) *If* R *contains a field, then* $R \cong k[\![x_1,\ldots,x_n]\!]/I$ *for some integer* $n \geq 0$ *and some ideal* I*.*

(2.) *If* R *has mixed characteristic* $p > 0$ *and* $p \notin \mathfrak{m}^2$*, then* $R \cong C[\![x_1,\ldots,x_n]\!]/I$ *for some integer* $n \geq 0$ *and local ring* $(C,\mathfrak{n})$ *that is a field or a complete discrete valuation ring with* $\mathfrak{n} = pC$*.*

3.6 Homological Algebra

Broadly, homological algebra is the study of homomorphisms between algebraic structures such as groups, rings, and modules. One of the most basic motivations to study homological algebra is the observation that the Isomorphism Theorems hold in each of the aforementioned settings, hence it is natural to seek to generalize these theorems to all algebraic structures that behave like groups, rings, and modules. In this section, we will develop many of the tools needed throughout this thesis; we refer the interested reader to [Rot09] for many more interesting details.

Unless otherwise stated, we assume that a commutative ring R possesses a multiplicative identity 1_R. Given any R-modules M and N, we may consider the set of R-module homomorphisms

$$\mathrm{Hom}_R(M,N) = \{\varphi : M \to N \mid \varphi \text{ is an } R\text{-module homomorphism}\}.$$

One can readily verify that $\mathrm{Hom}_R(M,N)$ is itself an R-module via the action $(r\cdot\varphi)(x) = r\varphi(x)$. Our next two propositions illuminate key properties of $\mathrm{Hom}_R(M,N)$ we will soon exploit.

Proposition 3.83. *Let* M *be an* R*-module. We have that* $\mathrm{Hom}_R(R,M) \cong M$ *as* R*-modules.*

Proof. Observe that an R-module homomorphism $\varphi : R \to M$ is uniquely determined by $\varphi(1_R)$. Explicitly, for any element $r \in R$, we have that $\varphi(r) = r\varphi(1_R)$, hence φ can be identified with the R-module homomorphism that sends $r \mapsto r\varphi(1_R)$. Consequently, we obtain an R-module homomorphism $\psi : \mathrm{Hom}_R(R,M) \to M$ defined by $\psi(\varphi) = \varphi(1_R)$. Clearly, it is surjective: for each element $m \in M$, choose the R-module homomorphism $\varphi : R \to M$ defined by $\varphi(r) = rm$. Likewise, we have that $\varphi \in \ker \psi$ if and only if $\varphi(1_R) = 0_R$ if and only if $\varphi(r) = 0$ for all elements $r \in R$ if and only if φ is the zero homomorphism. We conclude that ψ is an R-module isomorphism. □

Observe that for any R-module homomorphisms $\alpha : A \to B$ and $\beta : B \to C$, there exists an R-module homomorphism $\beta \circ \alpha : A \to C$. Consequently, for any R-module homomorphism $\beta : B \to C$, there is a map $\mathrm{Hom}_R(A,\beta) : \mathrm{Hom}_R(A,B) \to \mathrm{Hom}_R(A,C)$ defined by $\mathrm{Hom}_R(A,\beta)(\alpha) = \beta \circ \alpha$.

Proposition 3.84. *Let R be a commutative ring. Let A be an R-module. Let $\mathscr{R}$ be the category of R-modules. The map $\mathrm{Hom}_R(A,-) : \mathscr{R} \to \mathscr{R}$ that sends B to $\mathrm{Hom}_R(A,B)$ and sends an R-module homomorphism $\beta : B \to C$ to the R-module homomorphism $\mathrm{Hom}_R(A,\beta)$ is a* **covariant functor**.

Proof. We have already established that $\mathrm{Hom}_R(A,B)$ is an R-module for any R-module B. By definition of covariant functor, it suffices to show that (1.) $\mathrm{Hom}_R(A,\mathrm{id}_B) = \mathrm{id}_{\mathrm{Hom}_R(A,B)}$ for any R-module B and (2.) $\mathrm{Hom}_R(A,\gamma\circ\beta) = \mathrm{Hom}_R(A,\gamma)\circ\mathrm{Hom}_R(A,\beta)$ for any R-module homomorphisms $\beta : B \to C$ and $\gamma : C \to D$. Observe that $\mathrm{Hom}_R(A,\mathrm{id}_B)(\alpha)(a) = (\mathrm{id}_B \circ \alpha)(a) = \alpha(a)$ for every R-module homomorphism $\alpha : A \to B$ and every element $a \in A$, hence (1.) holds. Likewise, we have that $\mathrm{Hom}_R(A,\gamma\circ\beta)(\alpha) = \gamma\circ\beta\circ\alpha = \gamma\circ\mathrm{Hom}_R(A,\beta)(\alpha) = \mathrm{Hom}_R(A,\gamma)\circ\mathrm{Hom}_R(A,\beta)(\alpha)$ for any R-module homomorphisms $\alpha : A \to B$, $\beta : B \to C$, and $\gamma : C \to D$ so that (2.) holds. □

Likewise, for any R-module homomorphisms $\alpha : A \to B$ and $\beta : B \to C$, there is an induced map $\mathrm{Hom}_R(\alpha,C) : \mathrm{Hom}_R(B,C) \to \mathrm{Hom}_R(A,C)$ defined by $\mathrm{Hom}_R(\alpha,C)(\beta) = \beta \circ \alpha$. One can demonstrate in a manner analogous to Proposition 3.84 that the map $\mathrm{Hom}_R(-,C) : \mathscr{R} \to \mathscr{R}$ that sends B to $\mathrm{Hom}_R(B,C)$ and sends an R-module homomorphism $\alpha : A \to B$ to the R-module homomorphism $\mathrm{Hom}_R(\alpha,C)$ is a **contravariant functor**, i.e., $\mathrm{Hom}_R(\beta\circ\alpha,C) = \mathrm{Hom}_R(\alpha,C)\circ\mathrm{Hom}_R(\beta,C)$.

We say that a sequence of R-modules and R-module homomorphisms $A \xrightarrow{\alpha} B \xrightarrow{\beta} C$ is **exact at** B whenever $\ker\beta = \operatorname{img}\alpha$. Consequently, a sequence of R-modules and R-module homomorphisms $\cdots \xrightarrow{\varphi_{n+1}} M_n \xrightarrow{\varphi_n} M_{n-1} \xrightarrow{\varphi_{n-1}} \cdots$ is **exact** whenever it is exact at M_i for each integer i. Particularly, a sequence $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ is a **short exact sequence** if and only if $C = \ker(C \to 0) = \operatorname{img}\beta$ (i.e., β is surjective), $\ker\beta = \operatorname{img}\alpha$, and $\ker\alpha = \operatorname{img}(0 \to A) = 0$ (i.e., α is injective).

Proposition 3.85. *Let M and N be R-modules. If $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ is a short exact sequence of R-modules, the sequences $0 \to \operatorname{Hom}_R(M,A) \xrightarrow{\operatorname{Hom}_R(M,\alpha)} \operatorname{Hom}_R(M,B) \xrightarrow{\operatorname{Hom}_R(M,\beta)} \operatorname{Hom}_R(M,C)$ and $0 \to \operatorname{Hom}_R(C,N) \xrightarrow{\operatorname{Hom}_R(\beta,N)} \operatorname{Hom}_R(B,N) \xrightarrow{\operatorname{Hom}_R(\alpha,N)} \operatorname{Hom}_R(A,N)$ are also exact. Consequently, the functors $\operatorname{Hom}_R(M,-)$ and $\operatorname{Hom}_R(-,N)$ are* **left-exact** *on the category of R-modules.*

Proof. We will prove the first claim; the second follows analogously. By Proposition 3.84, the first sequence is well-defined, so it suffices to prove that it is exact. Consider an R-module homomorphism $\varphi : M \to A$ such that $\alpha \circ \varphi = \operatorname{Hom}_R(M,\alpha)(\varphi)$ is the zero homomorphism. By hypothesis, we have that $\ker\alpha = 0$ and $\alpha \circ \varphi(x) = 0$ for all elements $x \in M$, hence we conclude that φ is the zero homomorphism. Consequently, the first sequence is exact at $\operatorname{Hom}_R(M,A)$.

By assumption that $\ker\beta = \operatorname{img}\alpha$, it follows that $\beta \circ \alpha \circ \varphi$ is the zero homomorphism for any R-module homomorphism $\varphi : M \to A$. Conversely, take an R-module homomorphism $\psi : M \to B$ such that $\beta \circ \psi$ is the zero homomorphism. By definition, we have that $\psi(x)$ belongs to $\ker\beta$ for all elements $x \in M$. Considering that $\ker\beta = \operatorname{img}\alpha$ by assumption, for each element $x \in M$, there exists an element $a_x \in A$ such that $\psi(x) = \alpha(a_x)$. By hypothesis that φ and α are R-module homomorphisms, for every element $x \in M$ and $r \in R$, there exist elements $a_x, a_y, a_{rx+y} \in A$ such that $\alpha(ra_x + a_y) = r\alpha(a_x) + \alpha(a_y) = r\psi(x) + \psi(y) = \psi(rx+y) = \alpha(a_{rx+y})$ and $ra_x + a_y = a_{rx+y}$ by assumption that α is injective. We conclude that the map $\sigma : M \to A$ defined by $\sigma(x) = a_x$ is an R-module homomorphism that satisfies $\psi = \alpha \circ \sigma$, from which it follows that ψ is in the image of $\operatorname{Hom}_R(M,\alpha)$, i.e., the first sequence is exact at $\operatorname{Hom}_R(M,B)$. □

Our previous proposition ensures that if we apply the covariant functor $\operatorname{Hom}_R(M,-)$ to any short exact sequence of R-modules $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$, we obtain an exact sequence of R-

modules $0 \to \mathrm{Hom}_R(M,A) \xrightarrow{\mathrm{Hom}_R(M,\alpha)} \mathrm{Hom}_R(M,B) \xrightarrow{\mathrm{Hom}_R(M,\beta)} \mathrm{Hom}_R(M,C)$; however, the induced cochain complex $0 \to \mathrm{Hom}_R(M,A) \xrightarrow{\mathrm{Hom}_R(M,\alpha)} \mathrm{Hom}_R(M,B) \xrightarrow{\mathrm{Hom}_R(M,\beta)} \mathrm{Hom}_R(M,C) \to 0$ is exact at $\mathrm{Hom}_R(M,C)$ if and only if $\mathrm{Hom}_R(M,\beta)$ is surjective if and only if for every R-module homomorphism $\varphi : M \to C$, there exists an R-module homomorphism $\psi : M \to B$ such that $\varphi = \beta \circ \psi$.

Proposition 3.86. *Let R be a commutative ring. We say that an R-module P is* **projective** *if it satisfies any of the following equivalent conditions.*

(i.) *If $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ is a short exact sequence of R-modules, then the sequence*

$$0 \to \mathrm{Hom}_R(P,A) \xrightarrow{\mathrm{Hom}_R(P,\alpha)} \mathrm{Hom}_R(P,B) \xrightarrow{\mathrm{Hom}_R(P,\beta)} \mathrm{Hom}_R(P,C) \to 0$$

is exact, i.e., the functor $\mathrm{Hom}_R(P,-)$ is **right-exact** *on the category of R-modules.*

(ii.) *If $\beta : B \to C$ is a surjective R-module homomorphism and $\varphi : P \to C$ is any R-module homomorphism, then there exists an R-module homomorphism $\psi : P \to B$ such that $\varphi = \beta \circ \psi$.*

(iii.) *There exist R-modules B and C, a surjective R-module homomorphism β, and R-modules homomorphisms φ and ψ such that the following diagram commutes.*

$$\begin{array}{ccccc} & & & & P \\ & & \overset{\exists\psi}{\swarrow} & & \downarrow \varphi \\ B & \xrightarrow{\beta} & C & \longrightarrow & 0 \end{array}$$

(iv.) *Every short exact sequence $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} P \to 0$ of R-modules splits. Explicitly, there exists an R-module isomorphism $\psi : B \to A \oplus C$ such that $\psi \circ \alpha$ is the first component inclusion map $A \to A \oplus C$ and $\beta \circ \psi^{-1}$ is the second component projection map $A \oplus C \to C$.*

(v.) *There exists an R-module Q such that $P \oplus Q$ is a free R-module.*

Proof. By Proposition 3.85, one can readily deduce that the first three conditions are equivalent, so it suffices to prove that (ii.) $\implies$ (iv.) $\implies$ (v.) $\implies$ (i.). Consider a short exact sequence of R-modules $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} P \to 0$. By hypothesis, there exists an R-module homomorphism $\psi : P \to B$ such that $\mathrm{id}_P = \beta \circ \psi$. Particularly, the following diagram of R-modules commutes.

$$\begin{array}{ccccccccc} & & & & & & P & & \\ & & & & & \swarrow^{\psi} & \downarrow{\scriptstyle \mathrm{id}_P} & & \\ 0 & \longrightarrow & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & P & \longrightarrow & 0 \end{array}$$

By assumption that β is surjective, for any element $p \in P$, there exists an element $b \in B$ such that $p = \beta(b)$ and $\psi(p) = \psi \circ \beta(b)$. Conversely, for every element $b \in B$, we have that $\beta(b) \in P$, and we may consider the element $\psi \circ \beta(b)$ of B. Ultimately, for any element $b \in B$, observe that

$$\beta(b - \psi \circ \beta(b)) = \beta(b) - \beta \circ \psi \circ \beta(b) = \beta(b) - \mathrm{id}_P \circ \beta(b) = \beta(b) - \beta(b) = 0$$

so that $b - \psi \circ \beta(b)$ belongs to $\ker \beta$. By hypothesis that $\ker \beta = \operatorname{img} \alpha$, there exists an element $a \in A$ such that $b - \psi \circ \beta(b) = \alpha(a)$ and $b = \alpha(a) + \psi \circ \beta(b)$. We conclude that $B = \operatorname{img} \alpha + \operatorname{img} \psi$. We claim moreover that $\operatorname{img} \alpha \cap \operatorname{img} \psi = \{0\}$. For if $x \in \operatorname{img} \alpha \cap \operatorname{img} \psi$, then $\alpha(a) = x = \psi(y)$ for some elements $a \in A$ and $y \in P$. Consequently, we have that $y = \beta \circ \psi(y) = \beta(x) = \beta \circ \alpha(a) = 0$ and $x = \psi(y) = \psi(0) = 0$. We conclude that $B = \operatorname{img} \alpha \oplus \operatorname{img} \psi \cong A \oplus P$, where the isomorphism follows from the fact that α is injective by hypothesis and ψ is injective because β is a left-inverse. Ultimately, the R-module isomorphism $\varphi : B \to A \oplus P$ defined by $\varphi(\alpha(a) + \psi(p)) = (a, p)$ satisfies that $\varphi \circ \alpha$ is the inclusion map $A \to A \oplus P$ and $\beta \circ \varphi^{-1}$ is the projection map $A \oplus P \to P$.

Every R-module is the homomorphic image of a free R-module. Particularly, there exists a free R-module F and an R-module K such that $0 \to K \to F \to P \to 0$ is a short exact sequence of R-modules. If condition (iv.) holds, then we have that $F = P \oplus K$ is a free R-module.

Last, we will assume that property (v.) holds. Consider a short exact sequence of R-modules $0 \to A \to B \to C \to 0$ with the surjective map $\beta : B \to C$ specified. We claim that $\mathrm{Hom}_R(P, -)$ is right-exact, i.e., we must show that for every R-module homomorphism $\varphi : P \to C$, there exists an R-module homomorphism $\psi : P \to B$ such that $\varphi = \beta \circ \psi$. By hypothesis, there exists an R-module Q such that $F = P \oplus Q$ is free. Consequently, there exists an R-module basis $\mathscr{B} = \{f_i \mid i \in I\}$ of F. Let $\rho : P \to F$ denote the first component inclusion map, and let $\sigma : F \to P$ denote the second component projection map. By assumption that β is surjective, every element of C can be written as $\beta(b)$ for some element $b \in B$. We may therefore find elements b_i of B such that $\beta(b_i) = \varphi \circ \sigma(f_i)$

for each index i. By the freeness of F, there exists a unique homomorphism $\gamma : F \to B$ such that $\gamma(f_i) = b_i$. Observe that $\beta \circ \gamma(f_i) = \beta(b_i) = \varphi \circ \sigma(f_i)$ so that $\beta \circ \gamma = \varphi \circ \sigma$, as $\mathscr{B}$ is a basis. We conclude that $\varphi = \varphi \circ \sigma \circ \rho = \beta \circ \gamma \circ \rho = \beta \circ \psi$ for the map $\psi = \gamma \circ \rho \in \mathrm{Hom}_R(P,B)$. □

Corollary 3.87. *Every free R-module is projective.*

By Proposition 3.85, if we apply the contravariant functor $\mathrm{Hom}_R(-,N)$ to any short exact sequences of R-modules $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$, we obtain an exact sequence of R-modules $0 \to \mathrm{Hom}_R(C,N) \xrightarrow{\mathrm{Hom}_R(\beta,N)} \mathrm{Hom}_R(B,N) \xrightarrow{\mathrm{Hom}_R(\alpha,N)} \mathrm{Hom}_R(A,N)$. Like before, the induced map $\mathrm{Hom}_R(\alpha,N)$ is surjective if and only if for every R-module homomorphism $\varphi : A \to N$, there exists an R-module homomorphism $\psi : B \to N$ such that $\varphi = \psi \circ \alpha$.

Proposition 3.88. *Let R be a commutative ring. We say that an R-module Q is* **injective** *if it satisfies any of the following equivalent conditions.*

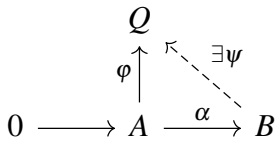
(i.) *If $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ is a short exact sequence of R-modules, then the sequence*

$$0 \to \mathrm{Hom}_R(C,Q) \xrightarrow{\mathrm{Hom}_R(\beta,Q)} \mathrm{Hom}_R(B,Q) \xrightarrow{\mathrm{Hom}_R(\alpha,Q)} \mathrm{Hom}_R(A,Q) \to 0$$

is exact, i.e., the functor $\mathrm{Hom}_R(-,Q)$ is right-exact on the category of R-modules.

(ii.) *If $\alpha : A \to B$ is an injective R-module homomorphism and $\varphi : A \to Q$ is any R-module homomorphism, then there exists an R-module homomorphism $\psi : B \to Q$ such that $\varphi = \psi \circ \alpha$.*

(iii.) *There exist R-modules A and B, an injective R-module homomorphism α, and R-modules homomorphisms φ and ψ such that the following diagram commutes.*



(iv.) *Every short exact sequence $0 \to Q \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ of R-modules splits. Explicitly, there exists an R-module isomorphism $\psi : B \to Q \oplus C$ such that $\psi \circ \alpha$ is the first component inclusion map $Q \to Q \oplus C$ and $\beta \circ \psi^{-1}$ is the second component projection map $Q \oplus C \to C$.*

(v.) *If Q is an R-submodule of M, then there exists an R-module P such that $M = P \oplus Q$.*

Proof. Conditions (i.), (ii.), and (iii.) are equivalent by Proposition 3.85, so it suffices to establish that (iii.) $\implies$ (iv.) $\implies$ (v.) $\implies$ (ii.). Observe that any short exact sequence of R-modules whose first nonzero term is Q can be completed to a commutative diagram of R-modules as follows.

$$\begin{array}{ccccccccc} & & & & Q & & & & \\ & & & & \uparrow{\scriptstyle \mathrm{id}_Q} & \nwarrow{\scriptstyle \exists \psi} & & & \\ 0 & \longrightarrow & Q & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & \longrightarrow & 0 \end{array}$$

Consequently, the R-module homomorphism $\psi : B \to Q$ satisfies $\mathrm{id}_Q = \psi \circ \alpha$. Given any element $b \in B$, we have that $b = \alpha \circ \psi(b) + (b - \alpha \circ \psi(b))$. Observe that

$$\psi(b - \alpha \circ \psi(b)) = \psi(b) - \psi \circ \alpha \circ \psi(b) = \psi(b) - \psi(b) = 0,$$

hence we have that $b - \alpha \circ \psi(b) \in \ker \psi$. We conclude that $B = \operatorname{img} \alpha + \ker \psi$. Even more, the sum is direct: if $b \in \operatorname{img} \alpha \cap \ker \psi$, then $b = \alpha(q)$ so that $0 = \psi(b) = \psi \circ \alpha(q) = q$ and $b = \alpha(0) = 0$. By hypothesis that α is injective, we find that $\operatorname{img} \alpha \cong Q$. On the other hand, for every element $c \in C$, there exists an element $b \in B$ such that $c = \beta(b)$. Considering that $B = \operatorname{img} \alpha \oplus \ker \psi$, there exist unique elements $q \in Q$ and $x \in \ker \psi$ such that $c = \beta(b) = \beta(\alpha(q) + x) = \beta(x)$, where the third equality follows from the fact that $\ker \beta = \operatorname{img} \alpha$. We conclude that $\ker \psi \cong C$. Ultimately, we find that $B = \operatorname{img} \alpha \oplus \ker \psi \cong Q \oplus C$ via the R-module homomorphism $\psi(\alpha(q) + x) = (q, \beta(x))$.

Observe that if Q is an R-submodule of M, then the inclusion $Q \subseteq M$ induces a short exact sequence of R-modules $0 \to Q \to M \to M/Q \to 0$. If every short exact sequence of R-modules splits, then we have that $M \cong Q \oplus (M/Q)$, hence Q is a direct summand of M.

We prove (v.) $\implies$ (ii.) as a corollary of Proposition 3.110. Explicitly, Q is an R-submodule of an injective R-module E, so it is a direct summand of E. But this implies that Q is injective. $\square$

Our next example illustrates that some modules are neither projective nor injective.

Example 3.89. Let $n \geq 2$ be an integer. Let $M = \mathbb{Z}/n\mathbb{Z}$ be the cyclic group of order n. Observe that M is a $\mathbb{Z}$-module because it is an abelian group; however, it is not projective because for

any abelian group G, the $\mathbb{Z}$-module $(\mathbb{Z}/n\mathbb{Z}) \oplus G$ has torsion. On the other hand, multiplication by n is an injective $\mathbb{Z}$-module homomorphism $n\cdot : \mathbb{Z} \to \mathbb{Z}$; however, for the canonical surjection $\pi : \mathbb{Z} \to M$, there does not exist a $\mathbb{Z}$-module homomorphism $\psi : \mathbb{Z} \to M$ such that $\pi = \psi \circ \cdot n$, as the latter is always zero. Consequently, the $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$ is neither projective nor injective.

Consequently, we may seek to measure the injective (or projective) "defect" of a module over a commutative unital ring. We define this notion rigorously as follows.

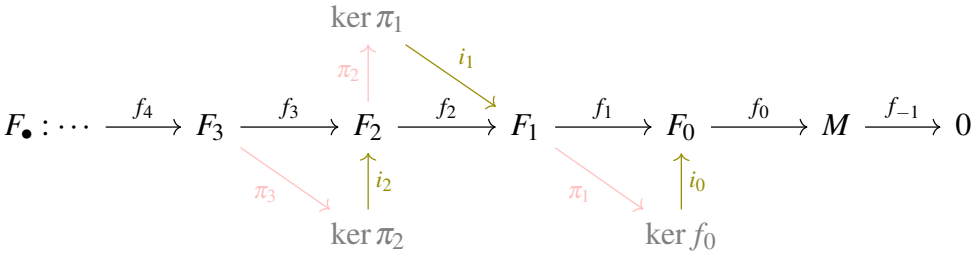
Let M be an R-module. We say that a sequence of R-modules and R-module homomorphisms

$$Z_\bullet : \cdots \xrightarrow{z_{n+1}} Z_n \xrightarrow{z_n} \cdots \xrightarrow{z_2} Z_1 \xrightarrow{z_1} Z_0 \xrightarrow{z_0} M \xrightarrow{z_{-1}} 0$$

is a (left) **resolution** of M if $Z_\bullet$ is exact at M and Z_i for each integer $i \geq 0$. If the R-modules Z_i are free for each integer $i \geq 0$, then $Z_\bullet$ is simply called a **free resolution** of M.

Proposition 3.90. *Every R-module admits a free resolution.*

Proof. Let M be an R-module. Observe that there exists a free R-module F_0 indexed by M and a surjective R-module homomorphism $f_0 : F_0 \to M$; its kernel injects into F_0 via the inclusion map $i_0 : \ker f_0 \to F_0$. Considering that $\ker f_0$ is an R-module, there exists a free R-module F_1 indexed by $\ker f_0$ and a surjective R-module homomorphism $\pi_1 : F_1 \to \ker f_0$. Consequently, the composition $f_1 = i_0 \circ \pi_1$ yields a map $f_1 : F_1 \to F_0$ such that $\operatorname{img} f_1 = \operatorname{img} \pi_1 = \ker f_0$. Likewise, the R-module $\ker \pi_1$ injects into F_1 via the inclusion map $i_1 : \ker \pi_1 \to F_1$, and there exists a free R-module F_2 indexed by $\ker \pi_1$ and a surjective R-module homomorphism $\pi_2 : F_2 \to \ker \pi_1$. Consequently, the composition $f_2 = i_1 \circ \pi_2$ yields a map $f_2 : F_2 \to F_1$ such that $\operatorname{img} f_2 = \operatorname{img} \pi_2 = \ker \pi_1 = \ker f_1$. Continuing in this manner produces the following commutative diagram of R-modules.



Consequently, the sequence $F_\bullet$ is a resolution of M in which each of the R-modules F_i is free. $\square$

Combined, Proposition 3.90 and Corollary 3.87 imply that any R-module M admits a **projective resolution**, i.e., a (left) resolution $P_\bullet : \cdots \xrightarrow{p_{n+1}} P_n \xrightarrow{p_n} \cdots \xrightarrow{p_2} P_1 \xrightarrow{p_1} P_0 \xrightarrow{p_0} M \xrightarrow{p_{-1}} 0$ in which P_i is projective for each integer $i \geq 0$. Given an R-module N, consider the cochain complex

$$\mathrm{Hom}_R(P_\bullet, N) : 0 \to \mathrm{Hom}_R(P_0, N) \xrightarrow{p_0^*} \mathrm{Hom}_R(P_1, N) \xrightarrow{p_1^*} \cdots \xrightarrow{p_{n-1}^*} \mathrm{Hom}_R(P_n, N) \xrightarrow{p_n^*} \cdots$$

with cochain maps defined by $p_i^* = \mathrm{Hom}_R(p_{i+1}, N)$ for each integer $i \geq 0$. We define the ith cohomology module $\mathrm{Ext}_R^i(M,N) = \ker p_i^* / \mathrm{img}\, p_{i-1}^*$ for each integer $i \geq 0$. Crucially, Cartan and Eilenberg demonstrated that $\mathrm{Ext}_R^i(M,N)$ is independent of the choice of a projective resolution of M, hence the R-modules $\mathrm{Ext}_R^i(M,N)$ are well-defined (cf. [Rot09, Proposition 6.56]).

Proposition 3.91. *Let N be an R-module. The following properties hold.*

(1.) *We have that $\mathrm{Ext}_R^0(M,N) \cong \mathrm{Hom}_R(M,N)$ for all R-modules M.*

(2.) *Every short exact sequence of R-modules $0 \to M' \to M \to M'' \to 0$ induces an exact sequence*
$$\cdots \to \mathrm{Ext}_R^{i-1}(M'',N) \to \mathrm{Ext}_R^i(M',N) \to \mathrm{Ext}_R^i(M,N) \to \mathrm{Ext}_R^i(M'',N) \to \mathrm{Ext}_R^{i+1}(M',N) \to \cdots.$$

(3.) *We have that $\mathrm{Ext}_R^i(M,N) = 0$ for all $i \geq 1$ and all R-modules M if and only if N is injective.*

Proof. (1.) Consider a projective resolution $P_\bullet$ of M that ends with the terms $P_1 \xrightarrow{p_1} P_0 \xrightarrow{p_0} M \to 0$. By Proposition 3.85, we may apply $\mathrm{Hom}_R(-,N)$ to obtain the sequence of R-modules

$$0 \to \mathrm{Hom}_R(M,N) \xrightarrow{\mathrm{Hom}_R(p_0,N)} \mathrm{Hom}_R(P_0,N) \xrightarrow{\mathrm{Hom}_R(p_1,N)} \mathrm{Hom}_R(P_1,N)$$

exact in the first two places. Consequently, we find that $\ker p_0^* = \mathrm{img}\,\mathrm{Hom}_R(p_0,N) \cong \mathrm{Hom}_R(M,N)$ by the First Isomorphism Theorem. We conclude that $\mathrm{Ext}_R^0(M,N) = \ker p_0^* \cong \mathrm{Hom}_R(M,N)$.

(3.) We assume first that N is injective. By Proposition 3.88, the functor $\mathrm{Hom}_R(-,N)$ is exact, hence for any R-module M and any projective resolution $P_\bullet$ of M, the induced cochain complex $\mathrm{Hom}_R(P_\bullet,N)$ is exact. We conclude that $\mathrm{Ext}_R^i(M,N) = 0$ for all integers $i \geq 1$. Conversely, suppose

that $\operatorname{Ext}^i_R(M,N) = 0$ for all $i \geq 1$ and all R-modules M. Consequently, for any short exact sequence of R-modules $0 \to M' \to M \to M'' \to 0$, there exists a long exact sequence of R-modules that begins $0 \to \operatorname{Hom}_R(M'',N) \to \operatorname{Hom}_R(M,N) \to \operatorname{Hom}_R(M',N) \to 0$. By Proposition 3.86, N is injective.

We omit the proof of property (2.), but we refer the reader to [Rot09, Corollary 6.46]. □

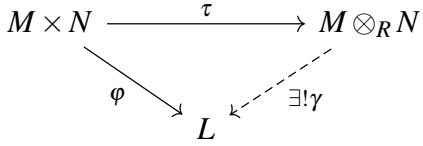
One can show that $\operatorname{Ext}^i_R(-,N)$ is a contravariant functor from the category of R-modules to itself that preserves multiplication (cf. [Rot09, Theorem 6.37 and Proposition 6.38]), hence Proposition 3.91 implies that the functors $\operatorname{Ext}^i_R(-,N)$ measure the injective "defect" of N.

One might naturally expect that in order to rigorously define the projective "defect" of an R-module M, we must look at the cohomology modules of the induced cochain complex obtained by applying $\operatorname{Hom}_R(M,-)$ to an injective resolution of some R-module; however, it is unclear that an arbitrary R-module admits an injective resolution. Consequently, we must first establish that every R-module admits an injective resolution; then, we will proceed in a manner analogous to the exposition preceding Proposition 3.91. We begin by constructing a functor from the category of R-modules to itself that forms an "adjoint pair" with the covariant functor $\operatorname{Hom}_R(M,-)$.

Let M and N be R-modules. Consider the free R-module F with basis $M \times N$. Explicitly, we view F as the set of all finite formal R-linear combinations of pairs of elements of F with pointwise addition and scalar multiplication. Let $\mathscr{R}$ denote the R-submodule of F generated by all elements of the form $(m_1+m_2,n)-(m_1,n)-(m_2,n)$, $(m,n_1+n_2)-(m,n_1)-(m,n_2)$, $(rm,n)-r(m,n)$, and $(m,rn)-r(m,n)$ for any element $r \in R$. We define the **tensor product** of M and N with respect to R as the quotient R-module $M \otimes_R N = F/\mathscr{R}$. Observe that every element of $M \otimes_R N$ is of the form $\sum_{i=1}^k r_i(m_i,n_i) + \mathscr{R}$ for some integer $k \geq 0$, some elements $r_1,\ldots,r_k \in R$, and some distinct elements $m_1,\ldots,m_k \in M$, and $n_1,\ldots,n_k \in N$. Conventionally, we write such an element as $\sum_{i=1}^k r_i(m_i \otimes_R n_i)$; elements of the form $m \otimes_R n$ are called the **pure tensors** of $M \otimes_R N$, hence by definition, the pure tensors generated $M \otimes_R N$ as an R-module. Even more, by construction, there is a canonical R-module homomorphism $\tau : M \times N \to M \otimes_R N$ defined by $(m,n) \mapsto m \otimes_R n$; it is R-**bilinear**, i.e., it satisfies $\tau(m_1+m_2,n) = \tau(m_1,n)+\tau(m_2,n)$, $\tau(m,n_1+n_2) = \tau(m,n_1)+\tau(m,n_2)$, and $\tau(rm,n) = r\tau(m,n) = \tau(m,rn)$ for all elements $m,m_1,m_2 \in M$, $n,n_1,n_2 \in N$, and $r \in R$.

One can alternatively describe the tensor product of M and N with respect to R as the unique solution to the following universal mapping problem. Given any R-modules M and N, we seek an R-module T and a bilinear R-module homomorphism $\tau : M \times N \to T$ such that for any R-module L and any bilinear R-module homomorphism $\varphi : M \times N \to L$, there exists a unique bilinear R-module homomorphism $\gamma : T \to L$ such that $\varphi = \gamma \circ \tau$ (cf. [Gat13, Propositions 5.4 and 5.5]).

Proposition 3.92 (Universal Property of the Tensor Product)**.** *Let R be a commutative ring. Let M and N be R-modules. If L is an R-module such that there exists a bilinear R-module homomorphism $\varphi : M \times N \to L$, then there exists a unique bilinear R-module homomorphism $\gamma : M \otimes_R N \to L$ such that $\varphi = \gamma \circ \tau$, i.e., such that the following diagram of R-modules commutes.*



Unsurprisingly, the Universal Property of the Tensor Product yields an abundance of results.

Proposition 3.93. *Let R be a commutative ring. Let M and N be R-modules.*

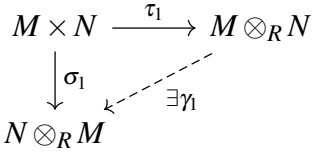
(1.) *We have that $M \otimes_R N \cong N \otimes_R M$.*

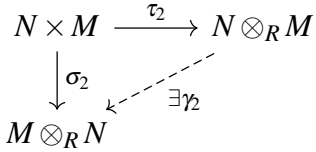
(2.) *We have that $R \otimes_R M \cong M$.*

(3.) *We have that $(R/I) \otimes_R M \cong M/IM$ for any ideal I of R.*

(4.) *For any (possibly infinite) index set I and any family of R-modules $(M_i)_{i \in I}$, we have that $(\bigoplus_{i \in I} M_i) \otimes_R N \cong \bigoplus_{i \in I} (M_i \otimes_R N)$, i.e., the tensor product commutes with direct sums.*

Proof. (1.) By the Universal Property of the Tensor Product, the bilinear R-module homomorphisms $\sigma_1 : M \times N \to N \otimes_R M$ and $\sigma_2 : N \times M \to M \otimes_R N$ defined by $\sigma_1(m,n) = n \otimes_R m$ and $\sigma_2(n,m) = m \otimes_R n$ induce the following commutative diagrams of R-modules.





We claim that γ_1 and γ_2 are inverses, hence they are isomorphisms. Observe that for every element $(m,n) \in M \times N$, we have that $\tau_2(n,m) = n \otimes_R m = \sigma_1(m,n) = \gamma_1 \circ \tau_1(m,n) = \gamma_1(m \otimes_R n)$. Consequently, we find that $\gamma_2 \circ \gamma_1(m \otimes_R n) = \gamma_2 \circ \tau_2(n,m) = \sigma_2(n,m) = m \otimes_R n$ so that $\gamma_2 \circ \gamma_1$ is the identity homomorphism on the pure tensors of $M \otimes_R N$. Considering that the pure tensors generated $M \otimes_R N$ as an R-module, we conclude that $\gamma_2 \circ \gamma_1$ is the identity homomorphism on $M \otimes_R N$. Conversely, $\gamma_1 \circ \gamma_2$ is the identity homomorphism on $N \otimes_R M$, as desired.

(2.) By definition, the R-module action of R on M induces a bilinear R-module homomorphism $\mu : R \times M \to M$ defined by $\mu(r,m) = rm$. Once again, the Universal Property of the Tensor Product guarantees the existence of a bilinear R-module homomorphism $\gamma : R \otimes_R M \to M$ that satisfies $rm = \mu(r,m) = \gamma \circ \tau(r,m) = \gamma(r \otimes_R m)$ for all elements $(r,m) \in R \times M$. We will construct an inverse homomorphism for γ. Consider the map $\varphi : M \to R \otimes_R M$ defined by $\varphi(m) = 1_R \otimes_R m$. By the properties of the tensor product, φ is an R-module homomorphism. Observe that for every element $m \in M$, we have that $m = 1_R m = \gamma(1_R \otimes_R m) = \gamma \circ \varphi(m)$. Conversely, for any pure tensor $r \otimes_R m$, we have that $r \otimes_R m = r(1_R \otimes_R m) = r\varphi(m) = \varphi(rm) = \varphi \circ \gamma(r \otimes_R m)$.

(3.) We may view M/IM as an R/I-module via the action $(r+I) \cdot (m+IM) = rm + IM$. Consequently, we obtain a bilinear R-module homomorphism $\mu : (R/I) \times M \to M/IM$ defined by $\mu(r+I,m) = rm+IM$; the Universal Property of the Tensor Product ensures that there is a bilinear R-module homomorphism $\gamma : (R/I) \otimes_R M \to M/IM$ that sends $(r+I) \otimes_R m \mapsto rm+IM$. We claim that the R-linear map $\varphi : M/IM \to (R/I) \otimes_R M$ defined by $\varphi(m+IM) = (1_R+I) \otimes_R m$ is well-defined. If $m+IM = n+IM$, then there exist elements $r_1, \ldots, r_k \in I$ and $x_1, \ldots, x_k \in M$ such that $m-n = r_1x_1 + \cdots + r_kx_k$. Considering that $r_i + I = 0_R + I$ for each integer $1 \leq i \leq k$, we find that

$$(1_R+I) \otimes_R (m-n) = (1_R+I) \otimes_R \left(\sum_{i=1}^{k} r_i x_i \right) = \sum_{i=1}^{k} [(r_i+I) \otimes_R x_i] = 0$$

so that $\varphi(m+IM) = (1_R+I) \otimes_R m = (1_R+I) \otimes_R n = \varphi(n+IM)$. One can check in a manner analogous to the previous paragraph the φ and γ are inverse homomorphisms.

(4.) Given any (possibly infinite) index set I and any family of R-modules $(M_i)_{i \in I}$, the tensor

product yields a bilinear R-module homomorphism $\sigma : (\bigoplus_{i\in I} M_i) \times N \to \bigoplus_{i\in I}(M_i \otimes_R N)$ that sends $((m_i)_{i\in I}, n) \mapsto (m_i \otimes_R n)_{i\in I}$. By the Universal Property of the Tensor Product, there exists a bilinear R-module homomorphism $\gamma : (\bigoplus_{i\in I} M_i) \otimes_R N \to \bigoplus_{i\in I}(M_i \otimes_R N)$ such that $\sigma = \gamma \circ \tau$. Likewise, for each index $i \in I$, there exists an R-module homomorphism $\varphi_i : M_i \otimes_R N \to (\bigoplus_{i\in I} M_i) \otimes_R N$ that sends $m_i \otimes_R n \mapsto (\delta_{ij} m_j)_{j\in I} \otimes_R n$ for the Kronecker delta δ_{ij}. By definition, the elements of $\bigoplus_{i\in I}(M_i \otimes_R N)$ are I-tuples with finitely many nonzero components, hence we obtain an R-module homomorphism $\varphi : \bigoplus_{i\in I}(M_i \otimes_R N) \to (\bigoplus_{i\in I} M_i) \otimes_R N$ that sends $(m_i \otimes_R n)_{i\in I} \mapsto \sum_{i\in I} \varphi_i(m_i \otimes_R n)$. One can readily verify that γ and φ are inverses on the pure tensors, hence they are inverses. □

Our next proposition extends the notion of a tensor product to R-module homomorphisms.

Proposition 3.94. *Let R be a commutative ring. Let $\varphi : M \to M'$ and $\psi : N \to N'$ be R-module homomorphisms. There exists a bilinear R-module homomorphism $\gamma_{\varphi,\psi} : M \otimes_R N \to M' \otimes_R N'$ defined by $\gamma_{\varphi,\psi}(m \otimes_R n) = \varphi(m) \otimes_R \psi(n)$. Consequently, the assignment $\eta(\varphi \otimes_R \psi) = \gamma_{\varphi,\psi}$ induces an R-module homomorphism $\eta : \mathrm{Hom}_R(M,M') \otimes_R \mathrm{Hom}_R(N,N') \to \mathrm{Hom}_R(M \otimes_R N, M' \otimes_R N')$.*

Proof. Consider the map $\sigma : M \times N \to M' \otimes_R N'$ defined by $\sigma(m,n) = \varphi(m) \otimes_R \varphi(n)$. By hypothesis that φ and ψ are R-module homomorphisms, it follows that σ is a bilinear R-module homomorphism by construction of the tensor product. Consequently, by the Universal Property of the Tensor Product, there exists a unique bilinear R-module homomorphism $\gamma_{\varphi,\psi} : M \otimes_R N \to M' \otimes_R N'$ defined by $\gamma_{\varphi,\psi}(m \otimes_R n) = \varphi(m) \otimes_R \psi(n)$. Put another way, the assignment $\eta(\varphi \otimes_R \psi) = \gamma_{\varphi,\psi}$ induces a well-defined map $\eta : \mathrm{Hom}_R(M,M') \otimes_R \mathrm{Hom}_R(N,N') \to \mathrm{Hom}_R(M \otimes_R N, M' \otimes_R N')$; it is not difficult to verify that η is R-linear, but we leave the details to the reader. □

Remark 3.95. Often, the induced R-module homomorphism $\gamma_{\varphi,\psi} : M \otimes_R N \to M' \otimes_R N'$ is denoted simply by $\varphi \otimes_R \psi$; this is an abuse of notation, but the meaning is clear.

Corollary 3.96. *Let R be a commutative ring. Let M be an R-module. Let $\mathscr{R}$ be the category of R-modules. The map $M \otimes_R - : \mathscr{R} \to \mathscr{R}$ that sends A to $M \otimes_R A$ and sends an R-module homomorphism $\varphi : A \to A'$ to the R-module homomorphism $\mathrm{id}_M \otimes_R \varphi$ is a covariant functor.*

Proof. By construction, $M \otimes_R N$ is an R-module for any R-module N; we need only establish that (1.) $\mathrm{id}_M \otimes_R \mathrm{id}_N = \mathrm{id}_{M\otimes_R N}$ for any R-module N and (2.) $\mathrm{id}_M \otimes_R (\psi \circ \varphi) = (\mathrm{id}_M \otimes_R \psi) \circ (\mathrm{id}_M \otimes_R \varphi)$ for any R-module homomorphisms $\varphi : N \to N'$ and $\psi : N' \to N''$. By Remark 3.95, we have that $(\mathrm{id}_M \otimes_R \mathrm{id}_N)(m \otimes_R n) = m \otimes_R n = \mathrm{id}_{M\otimes_R N}(m \otimes_R n)$; because these maps agree on the pure tensors of $M \otimes_R N$, they are equal as homomorphisms. On the other hand, for any R-module homomorphisms $\varphi : N \to N'$ and $\psi : N' \to N''$, we have that $(\mathrm{id}_M \otimes_R (\psi \circ \varphi))(m \otimes_R n) = m \otimes_R (\psi \circ \varphi(n))$ and similarly $(\mathrm{id}_M \otimes_R \psi) \circ (\mathrm{id}_M \otimes_R \varphi)(m \otimes_R n) = (\mathrm{id}_M \otimes_R \psi)(m \otimes_R \varphi(n)) = m \otimes_R (\psi \circ \varphi(n))$. □

Given a functor from the category of R-modules to itself, one naturally wonders about its behavior on short exact sequences of R-modules. By Corollary 3.96, for any short exact sequence of R-modules $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ and any R-module M, we obtain an induced sequence of R-modules $M \otimes_R A \xrightarrow{\mathrm{id}_M \otimes_R \alpha} M \otimes_R B \xrightarrow{\mathrm{id}_M \otimes_R \beta} M \otimes_R C$. By hypothesis that β is surjective, for each element $c \in C$, there exists an element $b \in B$ such that $c = \beta(b)$. Consequently, for each pure tensor $m \otimes_R c$ of $M \otimes_R C$, there exists a pure tensor $m \otimes_R b$ of $M \otimes_R B$ such that $m \otimes_R c = m \otimes_R \beta(b)$. Considering that the pure tensors of $M \otimes_R C$ generate it as an R-module, we conclude that the induced map $\mathrm{id}_M \otimes_R \beta : M \otimes_R B \to M \otimes_R C$ is surjective; this proves the following.

Proposition 3.97. *Let M be an R-module. If $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ is a short exact sequence of R-modules, then the induced sequence $M \otimes_R A \xrightarrow{\mathrm{id}_M \otimes_R \alpha} M \otimes_R B \xrightarrow{\mathrm{id}_M \otimes_R \beta} M \otimes_R C \to 0$ is also exact. Consequently, the functor $M \otimes_R -$ is right-exact on the category of R-modules.*

Proposition 3.98. *Let R be a commutative ring. We say that an R-module L if* **flat** *if it satisfies any of the following equivalent conditions.*

(i.) *If $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ is a short exact sequence of R-modules, then the sequence*

$$0 \to L \otimes_R A \xrightarrow{\mathrm{id}_L \otimes_R \alpha} L \otimes_R B \xrightarrow{\mathrm{id}_L \otimes_R \beta} L \otimes_R C \to 0$$

is exact, i.e., the functor $L \otimes_R -$ is left-exact on the category of R-modules.

(ii.) *If $\alpha : A \to B$ is an injective R-module homomorphism, then the induced R-module homomorphism* $\mathrm{id}_L \otimes_R \alpha : L \otimes_R A \to L \otimes_R B$ *is injective.*

(iii.) *For any ideal I of R, the map* $\mathrm{id}_L \otimes_R i : L \otimes_R I \to L$ *that sends $\ell \otimes_R r \mapsto r\ell$ is injective.*

Proof. Conditions (i.) and (ii.) are equivalent by Proposition 3.97. Considering that the inclusion $I \subseteq R$ of an ideal I of R induces an injective R-module homomorphism, it follows that (ii.) implies (iii.). We refer the reader to [Rot09, Proposition 3.58] for the proof that (iii.) implies (i.). □

Corollary 3.99. *Every commutative ring R is flat as a module over itself.*

Proof. Consider an injective R-module homomorphism $\alpha : A \to B$. By Proposition 3.93(2.), there exist R-module isomorphisms $\varphi : A \to R \otimes_R A$ and $\psi : B \to R \otimes_R B$ defined by $\varphi(a) = 1_R \otimes_R a$ and $\psi(b) = 1_R \otimes_R b$. Observe that $\psi \circ \alpha(a) = 1_R \otimes_R \alpha(a) = (\mathrm{id}_R \otimes_R \alpha) \circ \varphi(a)$ for all elements $a \in A$, hence $\psi \circ \alpha$ and $(\mathrm{id}_R \otimes_R \alpha) \circ \varphi$ are equal as R-module homomorphisms. Considering that φ, ψ, and α are injective, $\mathrm{id}_R \otimes_R \alpha$ must be injective, from which it follows that R is a flat R-module. □

Corollary 3.100. *Let R be a commutative ring. A direct sum of R-modules is flat if and only if each direct summand is flat. Particularly, any free R-module is flat.*

Proof. Let $(L_i)_{i \in I}$ be a family of R-modules indexed by some (possibly infinite) set I. Consider an injective R-module homomorphism $\alpha : A \to B$. For each index $i \in I$, there exists an R-module homomorphism $\mathrm{id}_{L_i} \otimes_R \alpha : L_i \otimes_R A \to L_i \otimes_R B$; together, these induce an R-module homomorphism $\gamma : \bigoplus_{i \in I}(L_i \otimes_R A) \to \bigoplus_{i \in I}(L_i \otimes_R B)$ that acts as $\mathrm{id}_{L_i} \otimes_R \alpha$ on the ith component of the direct sum. By Proposition 3.93(3.), there exists R-module isomorphisms $\varphi : \bigoplus_{i \in I}(L_i \otimes_R A) \to (\bigoplus_{i \in I} L_i) \otimes_R A$ and $\psi : \bigoplus_{i \in I}(L_i \otimes_R B) \to (\bigoplus_{i \in I} L_i) \otimes_R B$. Let $S = \bigoplus_{i \in I} L_i$. Observe that $\psi \circ \gamma$ and $(\mathrm{id}_S \otimes_R \alpha) \circ \varphi$ are equal on the pure tensors of $\bigoplus_{i \in I}(L_i \otimes_R A)$, hence they are equal as R-module homomorphisms. Consequently, $S = \bigoplus_{i \in I} L_i$ is flat if and only if $\mathrm{id}_S \otimes_R \alpha$ is injective if and only if γ is injective if and only if $\mathrm{id}_{L_i} \otimes_R \alpha$ is injective for all indices if and only if each direct summand L_i is flat.

Last, a free R-module is flat by Corollary 3.99, as it is a direct sum of copies of R. □

Corollary 3.101. *Let R be a commutative ring. Every projective R-module is flat.*

Proof. By Proposition 3.86(v.), a projective R-module is a direct summand of a free R-module. Every free R-module is flat; a direct summand of a flat R-module is flat by Corollary 3.100. □

Corollary 3.102. *Over a local ring, a finitely generated flat module is free.*

Proof. Let $(R,\mathfrak{m})$ be a local ring. Let L be a finitely generated flat R-module. Consider a system of generators $x_1,\ldots,x_n$ of L whose images in $L/\mathfrak{m}L$ form an $R/\mathfrak{m}$-vector space basis. By Nakayama's Lemma, we have that $L = R\langle x_1,\ldots,x_n\rangle$. Consequently, the canonical R-module homomorphism $\pi : R^n \to L$ defined by $\pi(r_1,\ldots,r_n) = r_1x_1 + \cdots + r_nx_n$ induces a short exact sequence of R-modules $0 \to K \xrightarrow{i} R^n \xrightarrow{\pi} L \to 0$, where $K = \ker\pi$ and $i : K \to R^n$ is the inclusion. By Proposition 3.97, there exists an exact sequence of R-modules $(R/\mathfrak{m}) \otimes_R K \to (R/\mathfrak{m}) \otimes_R R^n \to (R/\mathfrak{m}) \otimes_R L \to 0$. Combining (2.) and (4.) of Proposition 3.93, we obtain an exact sequence of $R/\mathfrak{m}$-vector spaces $K/(\mathfrak{m}K) \to (R/\mathfrak{m})^n \to L/(\mathfrak{m}L) \to 0$ (cf. the discussion following Definition 3.9). By hypothesis, the $R/\mathfrak{m}$-vector space dimension of $L/(\mathfrak{m}L)$ is n, so the Rank-Nullity Theorem implies that $K/(\mathfrak{m}K) = 0$ and $\mathfrak{m}K = K$. Corollary 3.12 yields $\ker\pi = K = 0$ so that L is a free R-module. □

Even if the ring is not local, a flat module over a Noetherian ring is projective.

Proposition 3.103. *[Rot09, Corollary 3.57] Over a Noetherian ring, a finitely generated flat module is projective. Particularly, flatness and projectivity are equivalent.*

Generally, the tensor product fails to preserve left-exactness of short exact sequences.

Example 3.104. Let $n \geq 2$ be an integer. Let $M = \mathbb{Z}/n\mathbb{Z}$ be the cyclic group of order n. Observe that the multiplication map $\cdot n : \mathbb{Z} \to \mathbb{Z}$ is injective because $\mathbb{Z}$ is a domain; however, the induced map $(\mathbb{Z}/n\mathbb{Z}) \otimes_R \mathbb{Z} \xrightarrow{\cdot n} (\mathbb{Z}/n\mathbb{Z}) \otimes_R \mathbb{Z}$ is identically zero. Consequently, $\mathbb{Z}/n\mathbb{Z}$ is not flat as a $\mathbb{Z}$-module.

Like before, we may rigorously define the flat "defect" of an R-module M as follows. Begin with a projective resolution $L_\bullet : \cdots \xrightarrow{\ell_{n+1}} L_n \xrightarrow{\ell_n} \cdots \xrightarrow{\ell_2} L_1 \xrightarrow{\ell_1} L_0 \xrightarrow{\ell_0} N \to 0$ of some R-module N. (By Corollary 3.101, this is a **flat resolution** of N.) Consider the induced chain complex

$$M \otimes_R L_\bullet : \cdots \xrightarrow{\ell^*_{n+1}} M \otimes_R L_n \xrightarrow{\ell^*_n} \cdots \xrightarrow{\ell^*_2} M \otimes_R L_1 \xrightarrow{\ell^*_1} M \otimes_R L_0 \to 0$$

with chain maps defined by $\ell_i^* = \mathrm{id}_M \otimes_R \ell_i$ for each integer $i \geq 0$. We define the ith homology module $\mathrm{Tor}_i^R(M,N) = \ker \ell_i^* / \operatorname{img} \ell_{i+1}^*$ for each integer $i \geq 0$; these are independent of the choice of a projective resolution of N, hence they are well-defined (cf. [Rot09, Corollary 6.21]).

Proposition 3.105. *Let M be an R-module. The following properties hold.*

(1.) *We have that $\mathrm{Tor}_0^R(M,N) \cong M \otimes_R N$ for all R-modules N.*

(2.) *Every short exact sequence of R-modules $0 \to N' \to N \to N'' \to 0$ induces an exact sequence*
$$\cdots \to \mathrm{Tor}_{i+1}^R(M,N'') \to \mathrm{Tor}_i^R(M,N') \to \mathrm{Tor}_i^R(M,N) \to \mathrm{Tor}_i^R(M,N'') \to \mathrm{Tor}_{i-1}^R(M,N') \to \cdots.$$

(3.) *We have that $\mathrm{Tor}_i^R(M,N) = 0$ for all integers $i \geq 1$ and all R-modules N if and only if M is flat.*

Proof. (1.) Given any R-module N, we may consider a flat resolution $L_\bullet$ of N that ends with the terms $L_1 \xrightarrow{\ell_1} L_0 \xrightarrow{\ell_0} N \to 0$. By applying the right-exact covariant functor $M \otimes_R -$, we obtain a chain complex ending in $M \otimes_R L_1 \xrightarrow{\ell_1^*} M \otimes_R L_0 \xrightarrow{\ell_0^*} 0$ with chain maps $\ell_i^* = \mathrm{id}_M \otimes_R \ell_i$. Consequently, we find that $\ker \ell_0^* = M \otimes_R L_0$ and $\operatorname{img} \ell_1^* = \operatorname{img}(\mathrm{id}_M \otimes_R \ell_1) = M \otimes_R (\operatorname{img} \ell_1)$, where the second equality holds because the pure tensors of $M \otimes_R (\operatorname{img} \ell_1)$ generate $\operatorname{img}(\mathrm{id}_M \otimes_R \ell_1)$. Consider the short exact sequence of R-modules $0 \to \operatorname{img} \ell_1 \xrightarrow{\subseteq} L_0 \to L_0/(\operatorname{img} \ell_1) \to 0$. By Proposition 3.93 and 3.97, we obtain a sequence of R-modules $M \otimes_R (\operatorname{img} \ell_1) \to M \otimes_R L_0 \to M \otimes_R (L_0/(\operatorname{img} \ell_1)) \to 0$ that is exact in the last two places. Considering that the map on the left is the identity on both components, we conclude that $M \otimes_R (L_0/(\operatorname{img} \ell_1)) \cong (M \otimes_R L_0)/[M \otimes_R (\operatorname{img} \ell_1)]$ by the First Isomorphism Theorem. By definition, we have that $\mathrm{Tor}_0^R(M,N) = \ker \ell_0^* / \operatorname{img} \ell_1^* = (M \otimes_R L_0)/[M \otimes_R (\operatorname{img} \ell_1)]$, hence our previous computation shows that $\mathrm{Tor}_0^R(M,N) \cong M \otimes_R (L_0/(\operatorname{img} \ell_1)) \cong M \otimes_R N$, as desired.

(3.) If M is flat, then $M \otimes_R -$ is exact by Proposition 3.98, hence for any flat resolution $L_\bullet$ of any R-module N, the chain complex $M \otimes_R L_\bullet$ is exact. We conclude that $\mathrm{Tor}_i^R(M,N) = 0$ for all integers $i \geq 1$. Conversely, suppose that $\mathrm{Tor}_i^R(M,N) = 0$ for all integers $i \geq 1$ and all R-modules N. For any short exact sequence of R-modules $0 \to N' \to N \to N'' \to 0$, there exists a long exact sequence that begins $0 \to M \otimes_R N' \to M \otimes_R N \to M \otimes_R N'' \to 0$. By Proposition 3.98, M is flat.

We omit the proof of property (2.), but we refer the reader to [Rot09, Corollary 6.30]. □

One can show that $\operatorname{Tor}_i^R(M,-)$ is a covariant functor from the category of R-modules to itself that preserves multiplication (cf. [Rot09, Theorem 6.17 and Proposition 6.18]), hence we may deduce from Proposition 3.105 that the R-modules $\operatorname{Tor}_i^R(M,-)$ measure the flat "defect" of M. By Proposition 3.93, the R-modules $M \otimes_R N$ and $N \otimes_R M$ are isomorphic for any pair of R-modules M and N, hence one can establish a similar theory for the covariant functors $\operatorname{Tor}_i^R(-,N)$. Ultimately, there is an isomorphism of functors $\operatorname{Tor}_R^i(M,-)$ and $\operatorname{Tor}_R^i(-,N)$ for all R-modules M and N, hence there is no need to make any distinction between the two (cf. [Rot09, Theorem 6.32]).

We are now able to return to our discussion of injective modules. We begin with the following.

Theorem 3.106 (Baer's Criterion)**.** *Let R be a commutative unital ring. Let I be a nonzero ideal of R. An R-module Q is injective if and only if for every R-module homomorphism $\varphi : I \to Q$, there exists an R-module homomorphism $\widetilde{\varphi} : R \to Q$ such that $\widetilde{\varphi}(i) = \varphi(i)$ for each element $i \in I$.*

Corollary 3.107. *Let $\mathbb{Z}$ be the abelian group of integers. Let $\mathbb{Q}$ be the abelian group of rational numbers. The quotient group $\mathbb{Q}/\mathbb{Z}$ is injective as a $\mathbb{Z}$-module.*

Proof. By Baer's Criterion, it suffices to show that any $\mathbb{Z}$-module homomorphism $\varphi : n\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ lifts to a $\mathbb{Z}$-module homomorphism $\widetilde{\varphi} : \mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ such that $\widetilde{\varphi}(na) = \varphi(na)$ for any $a \in \mathbb{Z}$. Consider the map $\widetilde{\varphi} : \mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ defined by $\widetilde{\varphi}(a) = \dfrac{a}{n}\varphi(n)$. By hypothesis that φ is a $\mathbb{Z}$-module homomorphism, it follows that $\widetilde{\varphi}$ is a $\mathbb{Z}$-module homomorphism such that $\widetilde{\varphi}(na) = \dfrac{na}{n}\varphi(n) = \varphi(na)$. $\square$

We prove next that every R-module can be identified with an R-submodule of an injective R-module; this analogizes the fact that any R-module is the homomorphic image of a free R-module.

Lemma 3.108. *Every $\mathbb{Z}$-module embeds in an injective $\mathbb{Z}$-module. Explicitly, for every $\mathbb{Z}$-module M, there exists an injective $\mathbb{Z}$-module Q and an injective $\mathbb{Z}$-module homomorphism $\varphi : M \to Q$.*

Proof. Given any $\mathbb{Z}$-module M, consider its character group $M^* = \operatorname{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$. We may subsequently define the character group $M^{**} = \operatorname{Hom}_{\mathbb{Z}}(M^*, \mathbb{Q}/\mathbb{Z})$ of M^* that consists of all $\mathbb{Z}$-module homomorphisms that send a $\mathbb{Z}$-module homomorphism $\varphi : M \to \mathbb{Q}/\mathbb{Z}$ to an element of $\mathbb{Q}/\mathbb{Z}$. Consequently, we may define a map $\operatorname{ev} : M \to M^{**}$ satisfying $\operatorname{ev}(m)(\varphi) = \varphi(m)$. Observe that

$\mathrm{ev}(am+m')(\varphi) = \varphi(am+m') = \varphi(am)+\varphi(m') = a\varphi(m)+\varphi(m') = a\,\mathrm{ev}(m)(\varphi)+\mathrm{ev}(m')(\varphi)$ for any integer a, any elements $m,m' \in M$, and any $\mathbb{Z}$-module homomorphism $\varphi : M \to \mathbb{Q}/\mathbb{Z}$, hence ev is a $\mathbb{Z}$-module homomorphism. One can verify that $\mathrm{ev}(m)(a\varphi+\psi) = a\,\mathrm{ev}(m)(\varphi)+\mathrm{ev}(m)(\psi)$ for any integer a and $\mathbb{Z}$-module homomorphisms $\varphi : M \to \mathbb{Q}/\mathbb{Z}$ and $\psi : M \to \mathbb{Q}/\mathbb{Z}$, hence ev is well-defined. Last, we claim that ev is injective. By the contrapositive, it suffices to show that every nonzero element $m \in M$ induces a $\mathbb{Z}$-linear homomorphism $\widetilde{\varphi} : M \to \mathbb{Q}/\mathbb{Z}$ for which $\widetilde{\varphi}(m)$ is nonzero. By hypothesis that $m \in M$ is nonzero, the $\mathbb{Z}$-module $C = \mathbb{Z}\langle m\rangle$ is nonzero. If $nm = 0$ for some integer $n \geq 2$, then the assignment $m \mapsto \dfrac{1}{n}+\mathbb{Q}/\mathbb{Z}$ induces a well-defined $\mathbb{Z}$-linear homomorphism $\varphi : C \to \mathbb{Q}/\mathbb{Z}$ defined by $\varphi(am) = \dfrac{a}{n}+\mathbb{Q}/\mathbb{Z}$. Otherwise, the assignment $m \mapsto \dfrac{1}{2}+\mathbb{Q}/\mathbb{Z}$ induces a well-defined $\mathbb{Z}$-linear homomorphism $\varphi : C \to \mathbb{Q}/\mathbb{Z}$ defined by $\varphi(am) = \dfrac{a}{2}+\mathbb{Q}/\mathbb{Z}$. Either way, by the injectivity of $\mathbb{Q}/\mathbb{Z}$ as a $\mathbb{Z}$-module, the inclusion homomorphism $i : C \to M$ can be extended to a $\mathbb{Z}$-linear map $\widetilde{\varphi} : M \to \mathbb{Q}/\mathbb{Z}$ such that $\varphi = \widetilde{\varphi} \circ i$ and $\widetilde{\varphi}(m) = \varphi(m)$ is nonzero.

Considering that M^* is a $\mathbb{Z}$-module, there exists a free $\mathbb{Z}$-module F and a surjective $\mathbb{Z}$-module homomorphism $\pi : F \to M$, i.e., there exists an exact sequence of $\mathbb{Z}$-modules $F \xrightarrow{\pi} M^* \to 0$. By Proposition 3.88, $\mathrm{Hom}_{\mathbb{Z}}(-,\mathbb{Q}/\mathbb{Z})$ induces an exact sequence of $\mathbb{Z}$-modules $0 \to M^{**} \xrightarrow{\pi^*} F^*$. Observe that if $F = \bigoplus_{\varphi\in M^*}\mathbb{Z}$, then $F^* = \mathrm{Hom}_{\mathbb{Z}}\left(\bigoplus_{\varphi\in M^*}\mathbb{Z}, \mathbb{Q}/\mathbb{Z}\right) \cong \prod_{\varphi\in M^*}(\mathbb{Q}/\mathbb{Z})$. Ultimately, $\pi^* \circ \mathrm{ev} : M \to F^*$ is an injective $\mathbb{Z}$-module homomorphism, so our proof is complete in view of the fact that F^* is an injective $\mathbb{Z}$-module by Corollary 3.107 and [Rot09, Proposition 3.28(i)]. □

Lemma 3.109. *Let R be a commutative ring. If P is a projective R-module and Q is an injective $\mathbb{Z}$-module, then $P^Q = \mathrm{Hom}_{\mathbb{Z}}(P,Q)$ is an injective R-module.*

Proof. We may define an R-module action on P^Q via $(r\cdot\varphi)(x) = \varphi(rx)$ because the identity

$$[(r+s)\cdot\varphi](x) = \varphi((r+s)x) = \varphi(rx+sx) = \varphi(rx)+\varphi(sx) = (r\cdot\varphi+s\cdot\varphi)(x)$$

holds for all elements $r,s \in R$ and $x \in P$, as φ is a group homomorphism. By Proposition 3.88, it suffices to show that $\mathrm{Hom}_R(-,P^Q)$ is right-exact on the category of R-modules. Given any short

exact sequence of R-modules $0 \to A \to B \to C \to 0$, we obtain an exact sequence of R-modules

$$0 \to A \otimes_R P \to B \otimes_R P \to C \otimes_R P \to 0$$

by Propositions 3.93(1.) and 3.101. By applying Proposition 3.88, we find that

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(C \otimes_R P, Q) \to \mathrm{Hom}_{\mathbb{Z}}(B \otimes_R P, Q) \to \mathrm{Hom}_{\mathbb{Z}}(A \otimes_R P, Q) \to 0$$

is a short exact sequence of $\mathbb{Z}$-modules. Last, the Tensor-Hom Adjunction yields a short exact sequence $0 \to \mathrm{Hom}_R(C, P^Q) \to \mathrm{Hom}_R(B, P^Q) \to \mathrm{Hom}_R(A, P^Q) \to 0$ of R-modules, as desired. $\square$

Proposition 3.110. *Every R-module embeds into an injective R-module.*

Proof. Let M be an R-module. By definition, $(M, +)$ is an abelian group, hence it is a $\mathbb{Z}$-module. By Lemma 3.108, there exists an injective $\mathbb{Z}$-module Q and an injective $\mathbb{Z}$-module homomorphism $\varphi : M \to Q$. By Proposition 3.85, this induces an injective $\mathbb{Z}$-module homomorphism $\mathrm{Hom}_{\mathbb{Z}}(R, \varphi) : \mathrm{Hom}_{\mathbb{Z}}(R, M) \to \mathrm{Hom}_{\mathbb{Z}}(R, Q)$. Crucially, $\mathrm{Hom}_{\mathbb{Z}}(R, Q)$ is an injective R-module by Lemma 3.109, hence it suffices to find an injective R-module homomorphism $M \to \mathrm{Hom}_{\mathbb{Z}}(R, Q)$.

Consider the map $\mu : M \to \mathrm{Hom}_{\mathbb{Z}}(R, M)$ defined by $\mu(m)(r) = rm$ for all elements $r \in R$. Observe that $\mu(m+m')(r) = r(m+m') = rm + rm' = (\mu(m) + \mu(m'))(r)$ for all elements $r \in R$ and any elements $m, m' \in M$. We conclude that μ is a $\mathbb{Z}$-module homomorphism. Even more, if $\mu(m)$ is the zero homomorphism, then $m = 1_R m = \mu(m)(1_R) = 0$, hence μ is injective. Consequently, the map $\mathrm{Hom}_{\mathbb{Z}}(R, \varphi) \circ \mu : M \to \mathrm{Hom}_{\mathbb{Z}}(R, Q)$ is an injective $\mathbb{Z}$-module homomorphism.

Given any element $r \in R$, observe that $(\mathrm{Hom}_{\mathbb{Z}}(R, \varphi) \circ \mu)(rm) = \varphi \circ \mu(rm)$ is the $\mathbb{Z}$-module homomorphism that sends an element $s \in R$ to the element $\varphi(rsm)$ of Q. Likewise, the composite map $(\mathrm{Hom}_{\mathbb{Z}}(R, \varphi) \circ \mu)(m)$ is the $\mathbb{Z}$-module homomorphism that sends an element $s \in R$ to the element $\varphi(sm)$ of Q. By the R-module structure of $\mathrm{Hom}_{\mathbb{Z}}(R, Q)$ defined in Lemma 3.109, it follows that $r[(\mathrm{Hom}_{\mathbb{Z}}(R, \varphi) \circ \mu)(m)]$ and $(\mathrm{Hom}_{\mathbb{Z}}(R, \varphi) \circ \mu)(rm)$ are identical on R, hence they are equal. We conclude that $\mathrm{Hom}_{\mathbb{Z}}(R, \varphi) \circ \mu$ is an R-module homomorphism, and our proof is complete. $\square$

Ultimately, Proposition 3.110 implies that every R-module N admits an **injective resolution**, i.e., a (right) resolution $Q^\bullet : 0 \to N \to Q^0 \xrightarrow{q^0} Q^1 \xrightarrow{q^1} \cdots \xrightarrow{q^n} Q^{n+1} \xrightarrow{q^{n+1}} \cdots$ in which Q^i is injective for each integer $i \geq 0$. Given an R-module M, consider the cochain complex

$$\mathrm{Hom}_R(M,Q^\bullet) : 0 \to \mathrm{Hom}_R(M,Q^0) \xrightarrow{q^0_*} \mathrm{Hom}_R(M,Q^1) \xrightarrow{q^1_*} \cdots \xrightarrow{q^n_*} \mathrm{Hom}_R(M,Q^n) \xrightarrow{q^{n+1}_*} \cdots$$

with cochain maps defined by $q^i_* = \mathrm{Hom}_R(M,q^i)$ for each integer $i \geq 0$. We define the ith cohomology module $\mathrm{Ext}^i_R(M,N) = \ker q^i_* / \operatorname{img} q^{i-1}_*$ for each integer $i \geq 0$. Like before, $\mathrm{Ext}^i_R(M,N)$ is independent of the choice of an injective resolution of N (cf. [Rot09, Proposition 6.40]).

Proposition 3.111. *Let M be an R-module. The following properties hold.*

(1.) *We have that $\mathrm{Ext}^0_R(M,N) \cong \mathrm{Hom}_R(M,N)$ for all R-modules N.*

(2.) *Every short exact sequence of R-modules $0 \to N' \to N \to N'' \to 0$ induces an exact sequence*
$\cdots \to \mathrm{Ext}^{i-1}_R(M,N'') \to \mathrm{Ext}^i_R(M,N') \to \mathrm{Ext}^i_R(M,N) \to \mathrm{Ext}^i_R(M,N'') \to \mathrm{Ext}^{i+1}_R(M,N') \to \cdots$.

(3.) *We have that $\mathrm{Ext}^i_R(M,N) = 0$ for all $i \geq 1$ and all R-modules N if and only if M is projective.*

Proof. We omit the proof, as it is analogous to the proof of Proposition 3.111. □

One can show that $\mathrm{Ext}^i_R(M,-)$ is a covariant functor from the category of R-modules to itself that preserves multiplication (cf. [Rot09, Theorem 6.37 and Proposition 6.38]), hence we may deduce from Proposition 3.111 that the functors $\mathrm{Ext}^i_R(M,-)$ measure the projective "defect" of M. Later, in our discussion of canonical modules, we will need the following proposition.

Proposition 3.112. *[Rot09, Proposition 7.24] Let R be a commutative ring with R-modules A and C. If $\mathrm{Ext}^1_R(C,A) = 0$, then every short exact sequence $0 \to A \to B \to C \to 0$ splits.*

If an R-module M admits an injective resolution with finitely many nonzero injective modules, then its **injective dimension** is the minimum length of all of such resolutions, i.e.,

$$\mathrm{injdim}_R(M) = \inf\{n \mid Q^\bullet : 0 \to M \to Q^0 \to Q^1 \to \cdots \to Q^n \to 0 \text{ is an injective resolution of } M\}.$$

Otherwise, we say that M does not have finite injective dimension. Our next proposition describes the injective dimension of a module in terms of Ext. Before this, we need the following lemma.

Lemma 3.113. *Let R be a commutative ring. Let A be an R-module. Let M be an R-module with an injective resolution $Q^\bullet : 0 \to M \xrightarrow{q^{-1}} Q^0 \xrightarrow{q^0} Q^1 \xrightarrow{q^1} \cdots$. Let $I_i = \operatorname{img} q^i$ for each integer $i \geq -1$. For all integers $n \geq i+2$, there exist R-modules isomorphisms $\operatorname{Ext}_R^{n-i}(A, I_i) \cong \operatorname{Ext}_R^{n-i-1}(A, I_{i+1})$.*

Proof. We will illustrate that $\operatorname{Ext}_R^{n+1}(A,M) \cong \operatorname{Ext}_R^n(A, I_0)$; the remaining isomorphisms follow similarly. By hypothesis that $Q^\bullet$ is an injective resolution of M, we may obtain an injective resolution of $I_0 = \operatorname{img} q^0$ by taking $Q_0^\bullet : 0 \to I_0 \xrightarrow{i} Q^1 \xrightarrow{q^1} Q^2 \xrightarrow{q^2} \cdots$; indeed, it suffices to note that $\ker q^1 = \operatorname{img} q^0 = I^0 = \operatorname{img} i$ by construction, and the rest of the resolution is exact by assumption. Consequently, if we relabel the injective modules Q^i as X^{i-1} and the maps q^i as χ^{i-1}, we find that

$$\operatorname{Ext}_R^{n+1}(A,M) = \frac{\ker q_*^n}{\operatorname{img} q_*^{n+1}} = \frac{\ker \chi_*^{n-1}}{\operatorname{img} \chi_*^n} = \operatorname{Ext}_R^n(A, I_0).$$

Because Ext is independent of the choice of injective resolution, the isomorphism holds. □

Proposition 3.114. *Let R be a commutative ring. The following are equivalent.*

(i.) *The R-module M has* $\operatorname{injdim}_R(M) \leq n$.

(ii.) *The R-module M satisfies* $\operatorname{Ext}_R^{n+1}(A,M) = 0$ *for all R-modules A.*

Proof. If M is an R-module of injective dimension no larger than n, then there exists an injective resolution $Q^\bullet : 0 \to M \to Q^0 \to Q^1 \to \cdots \to Q^n \to 0$. By Lemma 3.113, for every R-module A, we have that $\operatorname{Ext}_R^{n+1}(A,M) \cong \operatorname{Ext}_R^1(A, Q^n)$. But Q^n is injective, hence the latter Ext vanishes by Proposition 3.91. Conversely, suppose that $\operatorname{Ext}_R^{n+1}(A,M) = 0$ for all R-modules A. Consider an injective resolution $Q^\bullet$ of M. By Lemma 3.113, we have that $\operatorname{Ext}_R^{n+1}(A,M) \cong \operatorname{Ext}_R^1(A, I_n)$, hence by assumption, we conclude that I_n is an injective R-module. Consequently, we obtain a finite injective resolution of M of length n by truncating the injective resolution $Q^\bullet$ at I_n. □

Using the tools introduced in the next section, we will determine a pleasant formula the injective dimension of a module of finite injective dimension. Until then, we note the following.

Proposition 3.115. *[BH93, Proposition 3.1.14] Let $(R,\mathfrak{m},k)$ be a Noetherian local ring. Let M be a finitely generated R-module. We have that*

$$\operatorname{injdim}_R(M) = \sup\{i \geq 0 \mid \operatorname{Ext}^i_R(k,M) \neq 0\}.$$

One can likewise define the **projective dimension** of an R-module M as

$$\operatorname{projdim}_R(M) = \inf\{n \mid P_\bullet : \cdots \to P_n \to \cdots \to P_1 \to P_0 \to M \to 0 \text{ is a projective resolution of } M\}.$$

Like with injective dimension, the projective dimension of a module can be checked by the vanishing of Tor. We state two facts that are analogous to Lemma 3.113 and Proposition 3.114; we omit the proofs, as they are almost identical to the proofs of the aforementioned results.

Lemma 3.116. *Let R be a commutative ring. Let M be an R-module. Let B be an R-module with an projective resolution $P_\bullet : \cdots \xrightarrow{p_2} P_1 \xrightarrow{p_1} P_0 \xrightarrow{p_0} B \xrightarrow{p_{-1}} 0$. Let $K_i = \ker p_i$ for each integer $i \geq -1$. For all integers $n \geq i+2$, there exist R-modules isomorphisms $\operatorname{Tor}^R_{n-i}(M,K_i) \cong \operatorname{Tor}^R_{n-i-1}(M,K_{i+1})$.*

Proposition 3.117. *Let R be a commutative ring. The following are equivalent.*

(i.) *The R-module M has $\operatorname{projdim}_R(M) \leq n$.*

(ii.) *The R-module M satisfies $\operatorname{Tor}^R_{n+1}(M,B) = 0$ for all R-modules B.*

Corollary 3.118. *If $0 \to A \to B \to C \to 0$ is a short exact sequence of R-modules such that two modules have finite projective dimension, then the third module has finite projective dimension.*

Proof. We will prove that if A and B have finite projective dimension, then C has finite projective dimension; the other two cases follow similarly. By Proposition 3.117, if $\operatorname{projdim}_R(A) = m$ and $\operatorname{projdim}_R(B) = n$, then for all R-modules M, we have that $\operatorname{Tor}^R_i(A,M) = 0$ for all integers $i \geq m+1$ and $\operatorname{Tor}^R_j(B,M) = 0$ for all integers $j \geq n+1$. Consequently, for all R-modules M and all integers $k \geq \max\{m,n\}+1$, we have that $\operatorname{Tor}^R_k(C,M) = 0$ by Proposition 3.105. □

One of the most important results concerning projective dimension is the following.

Theorem 3.119 (Auslander-Buchsbaum Formula)**.** *[AB57, Theorem 3.7] Let $(R,\mathfrak{m})$ be a Noetherian local ring. If M is a finitely generated R-module with finite projective dimension, then*

$$\operatorname{projdim}_R(M) + \operatorname{depth}(M) = \operatorname{depth}(R).$$

Proposition 3.120. *For any (possibly infinite) index set I and any family of R-modules $(M_i)_{i\in I}$ of finite projective dimension, $\bigoplus_{i\in I} M_i$ has finite projective dimension.*

Proof. For each index $i \in I$, there exists a finite projective resolution $P_\bullet^i$ of M_i. □

3.7 Injective Modules and Injective Hulls

Our next propositions illuminate some important features of families of injective modules.

Proposition 3.121. *Let R be a commutative ring. If $(Q_i)_{i\in I}$ is a family of injective R-modules for some (possibly infinite) index set I, then $\prod_{i\in I} Q_i$ is an injective R-module. Particularly, every finite direct sum of injective R-modules is injective.*

Proof. By Proposition 3.88, it suffices to complete the following commutative diagram.

$$\begin{array}{ccccc} & & \prod_{i\in I} Q_i & & \\ & & \uparrow{\scriptstyle \varphi} & \nwarrow{\scriptstyle \exists \psi} & \\ 0 & \longrightarrow & A & \xrightarrow{\alpha} & B \end{array}$$

Observe that the ith component projection maps $\pi_i : \prod_{i\in I} Q_i \to Q_i$ induce R-module homomorphisms $\pi_i \circ \varphi : A \to Q_i$ for each index $i \in I$. By hypothesis that each of the R-modules Q_i is injective, it follows that there exist R-module homomorphisms $\psi_i : B \to Q_i$ such that $\pi_i \circ \varphi = \psi_i \circ \alpha$ for each index $i \in I$. Consider the R-module homomorphism $\psi : B \to \prod_{i\in I} Q_i$ defined by $\psi(b) = (\psi_i(b))_{i\in I}$. Observe that $\psi \circ \alpha(a) = (\psi_i \circ \alpha(a))_{i\in I} = (\pi_i \circ \varphi(a))_{i\in I} = (\varphi(a)_i)_{i\in I} = \varphi(a)$ for each element $a \in A$. We conclude that $\varphi = \psi \circ \alpha$, hence $\prod_{i\in I} Q_i$ is an injective R-module. □

Proposition 3.122. *Every direct summand of an injective R-module is injective.*

Proof. Let Q be an injective R-module such that $Q = M \oplus N$ for some R-modules M and N. Let $\sigma_1 : M \to Q$ be the first component inclusion map. Consider the following commutative diagram.

$$\begin{array}{ccccc} & & M & \xrightarrow{\sigma_1} & Q \\ & & \varphi\uparrow & & \\ 0 & \longrightarrow & A & \xrightarrow{\alpha} & B \end{array}$$

Observe that $\sigma_1 \circ \varphi : A \to Q$ yields an R-module homomorphism, hence there exists an R-module homomorphism $\psi : B \to Q$ with the property that $\psi \circ \alpha = \sigma_1 \circ \varphi$. On the other hand, the first component projection map $\pi_1 : Q \to M$ induces an R-module homomorphism $\pi_1 \circ \psi : B \to M$ such that $\mathrm{id}_M \circ \varphi = (\pi_1 \circ \sigma_1) \circ \varphi = (\pi_1 \circ \psi) \circ \alpha$. Considering that $(\mathrm{id}_M \circ \varphi)(a) = \varphi(a)$ for all elements $a \in A$, we conclude that $\varphi = (\pi_1 \circ \varphi) \circ \alpha$ so that M is an injective R-module. □

Every R-module embeds into an injective R-module. Given an R-module M, one might naturally search for a "smallest" injective module containing an isomorphic copy of M.

Proposition 3.123. *[Wal05, Proposition 1.6] Let M and E be nonzero R-modules. Let $\varphi : M \to E$ be an injective R-module homomorphism. The following statements are equivalent.*

(1.) *Every nonzero R-submodule F of E satisfies $F \cap \varphi(M) \neq 0$.*

(2.) *Every nonzero element of E has a nonzero multiple in $\varphi(M)$.*

(3.) *If there exists a nonzero R-module E' and an R-module homomorphism $\psi : E \to E'$ such that $\psi \circ \varphi$ is injective, then ψ must be injective.*

We say that E is an **essential extension** *of M (via φ) if any of the above properties hold.*

Proof. Let e be a nonzero element of E. If the first property holds, then the nonzero R-submodule Re of E satisfies $Re \cap \varphi(M) \neq 0$, hence there is a nonzero multiple of e in $\varphi(M)$. Consequently, we find that (1.) $\implies$ (2.). We will assume now that there exists a nonzero R-module E' and an R-module homomorphism $\psi : E \to E'$ such that $\psi \circ \varphi$ is injective. If the second property holds, then ψ must be injective; otherwise, we could find elements $e \in \ker \psi$, $r \in R$, and $m \in M$ such that $re = \varphi(m)$ is nonzero, and this would yield the contradiction $0 = r\psi(e) = \psi(re) = \psi \circ \varphi(m)$. We conclude that (2.) $\implies$ (3.). Last, suppose that the third property holds. Let F be a nonzero R-submodule of E. Observe that the canonical surjection $\pi : E \to E/F$ has kernel F, hence it is not

injective. By the contrapositive of the third property, the composite map $\pi \circ \varphi : M \to E/F$ cannot be injective, i.e., there exists a nonzero element in $F \cap \varphi(M)$ so that $F \cap \varphi(M) \neq 0$. □

Proposition 3.124. *Let M be an R-module. The following conditions hold.*

(1.) *Essentiality is a transitive property. Explicitly, if E' is an essential extension of E and E is an essential extension of M, then E' is an essential extension of M.*

(2.) *Essentiality is closed under inclusion. Explicitly, if $E' \supseteq E \supseteq M$ and $E' \supseteq M$ is an essential extension, then $E' \supseteq E$ is an essential extension and $E \supseteq M$ is an essential extension.*

Particularly, if E is an essential extension of M (via any injective R-module homomorphism), then $E' \supseteq E$ is an essential extension if and only if $E' \supseteq M$ is an essential extension.

Proof. (1.) If E' is an essential extension of E via ψ, then every nonzero element e of E' has a nonzero multiple $re = \psi(f)$ in $\psi(E)$. If E is an essential extension of M via φ, then the nonzero element f of E has a nonzero multiple $sf = \varphi(m)$ in $\varphi(M)$. Ultimately, we conclude that there is a nonzero multiple $rse = \psi \circ \varphi(m)$ of e in $\psi \circ \varphi(M)$, hence E' is an essential extension of M.

(2.) If $E' \supseteq M$ is an essential extension, then every nonzero element of E has a nonzero multiple in M. Considering that $E \supseteq M$, it follows that every nonzero element of E' has a nonzero multiple in E, hence $E' \supseteq E$ is an essential extension. Likewise, every nonzero element of E can be viewed as an element of E', hence every nonzero element of E has a nonzero multiple in M.

Last, suppose that $\varphi : M \to E$ is an essential extension of M. Consider the inclusion map $i_E : E \to E'$. Observe that E' is an essential extension of E via i_E if and only if every nonzero element e of E' has a nonzero multiple in $i_E(E)$ if and only if every nonzero element e of E' has a nonzero multiple in $i_E \circ \varphi(M)$ if and only if E' is an essential extension of M via $i_E \circ \varphi$. □

Every R-module is an essential extension of itself. If E is an essential extension of M via some R-module homomorphism φ, we say that E is a **proper essential extension** of M if $\varphi(M) \subsetneq E$. Our next proposition characterizes injective modules by their lack of proper essential extensions.

Proposition 3.125. *An R-module is injective if and only if admits no proper essential extensions.*

Proof. We will assume first that Q is an injective R-module. Let E be an essential extension of Q. By Proposition 3.123, there exists an injective R-module homomorphism $\varphi : Q \to E$. By applying Proposition 3.88 to the R-module homomorphisms $\varphi : Q \to E$ and $\mathrm{id}_Q : Q \to Q$, we obtain an R-module homomorphism $\psi : E \to Q$ such that $\mathrm{id}_Q = \psi \circ \varphi$. Because id_Q is surjective, ψ must be surjective. By the third part of Proposition 3.123, we conclude that $\psi : E \to Q$ is injective. Consequently, ψ is an isomorphism, hence we conclude that $\varphi(Q) = \psi^{-1}(Q) = E$.

Conversely, suppose that Q is an R-module that admits no proper essential extensions. By Proposition 3.110, there exists an injective R-module Q' and an injective R-module homomorphism $\varphi : Q \to Q'$. If Q' is an essential extension of Q via φ, then we must have that $\varphi(Q) = Q'$, hence φ is an isomorphism and Q is injective. Otherwise, Q' is not an essential extension of Q via φ, hence there exists a nonzero R-module $M \subseteq Q'$ such that $M \cap \varphi(Q) = 0$. Consider the nonempty collection $\mathscr{E} = \{M \subseteq Q' \mid M \text{ is an } R\text{-module and } M \cap \varphi(Q) = 0\}$. Observe that for any chain $M_1 \subseteq M_2 \subseteq \cdots$ of R-modules in $\mathscr{E}$, the union $\cup_{i \geq 1} M_i$ belongs to $\mathscr{E}$ by the Distributive Law. Consequently, Zorn's Lemma implies that $\mathscr{E}$ admits a maximal element M. Consider the nonzero R-module homomorphism $\psi : Q \to Q'/M$ defined by $\psi(x) = \varphi(x) + M$. By definition, if $x \in \ker \psi$, then $\varphi(x)$ belongs to $M \cap \varphi(Q)$ so that $\varphi(x) = 0$. But this implies that $x = 0$, as φ is injective, hence ψ is injective. Consequently, if there exists a nonzero R-module E and an R-module homomorphism $\gamma : Q'/M \to E$ such that $\gamma \circ \psi$ is injective, then γ must be injective. By Proposition 3.123(3.), the map $\psi : Q \to Q'/M$ is an essential extension of Q, hence ψ must be an isomorphism by assumption that Q has no proper essential extensions. Particularly, for every element $y \in Q'$, there exists an element $x \in Q$ and an element $m \in M$ such that $y = \varphi(x) + m$ so that $Q' = \varphi(Q) + M$. By construction, we have that $M \cap \varphi(Q) = 0$, so we conclude that $Q' = \varphi(Q) \oplus M$. Considering that Q' is injective, it follows that $Q \cong \varphi(Q)$ is injective by Proposition 3.122. □

Our next proposition clarifies the meaning of a "largest" essential extension of M.

Proposition 3.126. *Let M and E be nonzero R-modules. Let $\varphi : M \to E$ be an injective R-module homomorphism. The following conditions are equivalent.*

(i.) *E is an essential extension of M via φ and an injective R-module.*

(ii.) *E is an essential extension of M via φ and no proper extension of E is essential over M.*

We say that E is a **maximal essential extension** *of M (via φ) if either of these properties holds.*

Proof. We will assume first that E is an injective R-module that is an essential extension of M via φ. We claim that any essential extension of M can be identified with an R-submodule of E. Consider an essential extension $\gamma : M \to E'$. By Proposition 3.88, there exists an R-module homomorphism $\psi : E' \to E$ such that $\varphi = \psi \circ \gamma$. By the injectivity of φ, it follows that $(\ker \psi) \cap \gamma(M) = 0$. By Proposition 3.123, we conclude that $\ker \psi = 0$, hence $E' \cong \psi(E)$ is an R-submodule of E.

Conversely, suppose that E is an essential extension of M via φ such that no proper extension of E is essential over M. If E were to admit a proper essential extension $\psi : E \to E'$, then E' would be an essential extension of M via $\psi \circ \varphi$ by Proposition 3.124 — a contradiction. We conclude that E admits no proper essential extensions, hence E is injective by Proposition 3.125. □

Theorem 3.127 (Eckmann-Schöpf)**.** *Every R-module admits a maximal essential extension.*

Proof. By Proposition 3.110, there exists an injective R-module Q and an injective R-module homomorphism $\varphi : M \to Q$. Consider the collection $\mathscr{E} = \{E \subseteq Q \mid E \supseteq \varphi(M) \text{ is essential}\}$ of R-submodules of Q such that $E \supseteq \varphi(M)$ is an essential extension. Observe that $\mathscr{E}$ contains $\varphi(M)$. Even more, the union $\cup_{i \geq 1} E_i$ of any chain $E_1 \subseteq E_2 \subseteq \cdots$ of R-modules in $\mathscr{E}$ is an essential extension of $\varphi(M)$: indeed, any nonzero element of $\cup_{i \geq 1} E_i$ lies in E_i for some integer $i \geq 1$, so it has a nonzero multiple in $\varphi(M)$ by the essentiality of the extension $E_i \supseteq \varphi(M)$. By Zorn's Lemma, we conclude that $\mathscr{E}$ has a maximal element E. By definition, this is an essential extension $E \supseteq \varphi(M)$ that lies in Q with the property that $E' \supsetneq \varphi(M)$ is not an essential extension of $\varphi(M)$ for any R-module $E \subsetneq E' \subseteq Q$; we prove in general that if $E' \supsetneq E$, then $E' \supsetneq \varphi(M)$ is not an essential extension.

On the contrary, assume that $E' \supsetneq E$ and $E' \supsetneq \varphi(M)$ is an essential extension. Crucially, observe that $E' \supsetneq E$ is an essential extension by Proposition 3.124. By applying Proposition 3.88 to the inclusion homomorphisms $i : E \to E'$ and the inclusion $j : E \to Q$, we obtain an R-module

homomorphism $\psi : E' \to Q$ such that $j = \psi \circ i$. Considering that j is injective, it follows that $(\ker \psi) \cap E = 0$ so that $(\ker \psi) \cap \varphi(M) = 0$. By hypothesis that $E' \supsetneq \varphi(M)$ is an essential extension, we conclude that $\ker \psi = 0$ so that $E' \cong \psi(E') \subseteq Q$ is an essential extension of $\varphi(M)$ in Q. But this contradicts the last sentence of the previous paragraph. We conclude that E is maximal with respect to inclusion among all R-modules E' such that $E' \supseteq \varphi(M)$ is an essential extension. $\square$

Conventionally, a maximal essential extension of an R-module M is an **injective hull** of M. By Proposition 3.126, any injective hull of M is an injective R-module, and any injective hull of M is a "largest" essential extension of M by definition. Our next proposition illustrates that any two injective hulls of M are isomorphic, so we may henceforth refer to *the* injective hull $E_R(M)$ of M.

Proposition 3.128. *Let M be an R-module. If E and E' are any two injective hulls of M, then there exists an R-module isomorphism $\psi : E \to E'$ such that $\psi(m) = m$ for every element $m \in M$.*

Proof. Both E and E' are injective by Proposition 3.126, hence the inclusions $M \subseteq E$ and $M \subseteq E'$ induce an R-module homomorphism $\psi : E \to E'$. Observe that ψ is the inclusion $M \subseteq E'$ on M, hence we have that $(\ker \psi) \cap M = 0$. By Proposition 3.123, we must have that $\ker \psi = 0$, hence ψ is injective. Consequently, we find that $\psi(E) \cong E$ is an injective R-submodule of E'. By Proposition 3.88, there exists an R-submodule B of E such that $E' = \psi(E) \oplus B$ so that $\psi(E) \cap B = 0$. Considering that $M \subseteq E$, it follows that $M = \psi(M) \subseteq \psi(E)$ by construction of ψ. We conclude that $B \cap M = 0$. By the second part of Proposition 3.123, we conclude that $B = 0$ and $E' = \psi(E)$. $\square$

We prove at last that the injective hull of an R-module is the "smallest" injective module containing an isomorphic copy of M, which resolves the search initiated before Proposition 3.123.

Proposition 3.129. *Let M be an R-module. If Q is any R-module such that there exists an injective R-module homomorphism $\varphi : M \to Q$, then φ extends to an embedding $\widetilde{\varphi} : E_R(M) \to Q$.*

Proof. By Proposition 3.88, the injective homomorphisms $\varphi : M \to Q$ and $\psi : M \to E_R(M)$ induce an R-module homomorphism $\widetilde{\varphi} : E_R(M) \to Q$ with $(\ker \widetilde{\varphi}) \cap \psi(M) = 0$. By construction, $E_R(M)$ is an essential extension of M via ψ, hence we find that $\ker \widetilde{\varphi} = 0$, as desired. $\square$

One of the principle uses of the injective hull of a module is in the construction of "dual" that preserves length. Explicitly, we will assume henceforth that $(R,\mathfrak{m},k)$ is a Noetherian local ring. Let E denote the injective hull $E_R(k)$ of the residue field of R. Given any R-module M, we denote by $D_R(M) = \mathrm{Hom}_R(M,E)$ the **Matlis dual** of M. We obtain the following.

Proposition 3.130. *[BH93, Proposition 3.2.12] Let $(R,\mathfrak{m},k)$ be a Noetherian local ring. Let E be the injective hull of the residue field of R. Let M be an R-module. Let N be an R-module of finite length. Let $D_R(-) = \mathrm{Hom}_R(-,E)$ denote the Matlis dual. The following properties hold.*

(1.) *We have that $\mathrm{Hom}_R(k,E) \cong k$ and $\mathrm{Ext}^i_R(k,E) = 0$ for all integers $i \geq 1$.*

(2.) *The Matlis dual preserves the length of any module of finite length, i.e., $\ell_R(N) = \ell_R(D_R(N))$.*

(3.) *The canonical map $M \to D_R(D_R(M))$ that sends $m \mapsto \mathrm{ev}_m$ is an isomorphism.*

(4.) *The Matlis dual satisfies $\mu(M) = \dim_k(M/\mathfrak{m}M) = r(D_R(M))$ and $r(M) = \mu(D_R(M))$.*

Further, if R is Artinian, then E is a finitely generated faithful R-module satisfying

(5.) *$\ell_R(E) = \ell_R(R)$;*

(6.) *the canonical map $R \to \mathrm{Hom}_R(E,E)$ that sends $r \mapsto \mathrm{ev}_r$ is an isomorphism; and*

(7.) *$\mu(E) = r(R)$ and $r(R) = 1$.*

Conversely, any finitely generated faithful R-module of type 1 is isomorphic to E.

Proof. (1.) By the construction of E, there exists an injective R-module homomorphism $\varphi : k \to E$. Consider the k-vector space $V = \{e \in E \mid \mathfrak{m}e = 0\}$. By the R-linearity of φ, it follows that $\varphi(k) \subseteq V$. We claim that equality holds. On the contrary, if this containment were strict, then we could find a complementary k-vector subspace W of $\varphi(k)$. Put another way, there would exist a nonzero k-vector subspace W of V such that $W \cap \varphi(k) = 0$. But E is an essential extension of k via φ, so this is impossible. We conclude that $V = \varphi(k)$. By the proof of Proposition 3.52, there exists an

R-module isomorphism $\mathrm{Hom}_R(k,E) \cong V$, hence we find that $\mathrm{Hom}_R(k,E) \cong V = \varphi(k) \cong k$. Because E is injective, we conclude that $\mathrm{Ext}^i_R(k,E) = 0$ for all integers $i \geq 1$ by Proposition 3.88.

(2.) We proceed by induction on $\ell_R(N)$. Observe that if $\ell_R(N) = 1$, then there exists an R-module isomorphism $N \cong k$. By the previous part, we conclude that $N \cong \mathrm{Hom}_R(N,E)$ so that $\ell_R(N) = \ell_R(D_R(N))$. Consider the case that $\ell_R(N) \geq 2$. By definition, there exists a proper R-submodule $N' \subsetneq N$. Using the inclusion, we obtain an induced short exact sequence of R-modules $0 \to N' \to N \to C \to 0$. Length is additive on short exact sequences, i.e., $\ell_R(N) = \ell_R(N') + \ell_R(C)$, so we must have that $\ell_R(N') < \ell_R(N)$ and $\ell_R(C) < \ell_R(N)$. By applying the right-exact contravariant functor $D_R(-)$, we obtain a short exact sequence $0 \to D_R(C) \to D_R(N) \to D_R(N') \to 0$. By induction, we have that $\ell_R(D_R(C)) = \ell_R(C)$ and $\ell_R(D_R(N')) = \ell_R(N')$, hence the additivity of length on short exact sequences once again shows that $\ell_R(D_R(N)) = \ell_R(N') + \ell_R(C) = \ell_R(N)$.

(5.) By Proposition 3.83, we have that $D_R(R) = \mathrm{Hom}_R(R,E) \cong E$. By the second part of this proposition, we have that $\ell_R(D_R(R)) = \ell_R(R)$. Combined, these two observations imply that $\ell_R(E) = \ell_R(D_R(R)) = \ell_R(R)$; the latter is finite by hypothesis that R is Artinian and Proposition 3.15. We conclude that E is a finitely generated R-module by Proposition 3.16.

(6.) By the third part of this proposition, it follows that R is isomorphic to $D_R(D_R(R))$. By the paragraph above, we have that $D_R(R) \cong E$ so that $R \cong D_R(D_R(R)) \cong \mathrm{Hom}_R(E,E)$. Because $\mathrm{Hom}_R(E,E)$ consists of all R-module actions on E, we conclude that E is faithful.

Last, if M is a finitely generated faithful R-module of type 1, then $\mu(D_R(M)) = 1$ by the fourth part above. Put another way, there exists an ideal I of R such that $\mathrm{Hom}_R(M,E) \cong R/I$. Using the fact that $M \cong D_R(D_R(M))$, we conclude that $M \cong \mathrm{Hom}_R(R/I,E) \cong \{e \in E \mid Ie = 0\}$. By hypothesis that M is faithful, we must have that $\mathrm{ann}_R(M) = 0$; the isomorphism of the previous line guarantees that $\{e \in E \mid Ie = 0\}$ is faithful so that $I = 0$ and $M \cong \mathrm{Hom}_R(R,E) \cong E$.

We have omitted the proofs of items (3.), (4.), and (7.) for sake of brevity. □