The Basics of Homological Algebra

Dylan C. Beck

Contents

1 Hom and (Contravariant) Ext **1**

2 Tensor Products and Tor **11**

3 Existence of Injective Modules **20**

4 Appendix **26**

4.1 Rings, Ideals, and Modules 26

4.2 Localization as a Functor 37

4.3 Further Properties of Hom and Ext 42

4.4 Further Properties of Tensor Products and Tor 43

4.5 Commutative Diagrams 45

1 Hom and (Contravariant) Ext

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 note; 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

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

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

Proposition 1.1. *Let M be an R-module. We have that* $\operatorname{Hom}_R(R,M) \cong M$ *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 $\psi : \operatorname{Hom}_R(R,M) \to M$ 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. $\square$

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 $\operatorname{Hom}_R(A,\beta) : \operatorname{Hom}_R(A,B) \to \operatorname{Hom}_R(A,C)$ defined by $\operatorname{Hom}_R(A,\beta)(\alpha) = \beta \circ \alpha$.

Proposition 1.2. *Let R be a commutative ring. Let A be an R-module. Let $\mathscr{R}$ be the category of R-modules. The map* $\operatorname{Hom}_R(A,-) : \mathscr{R} \to \mathscr{R}$ *that sends B to* $\operatorname{Hom}_R(A,B)$ *and sends an R-module homomorphism $\beta : B \to C$ to the R-module homomorphism* $\operatorname{Hom}_R(A,\beta)$ *is a* **covariant functor**.

Proof. We have already established that $\operatorname{Hom}_R(A,B)$ is an R-module for any R-module B. By definition of covariant functor, it suffices to show that (1.) $\operatorname{Hom}_R(A,\mathrm{id}_B) = \mathrm{id}_{\operatorname{Hom}_R(A,B)}$ for any R-module B and (2.) $\operatorname{Hom}_R(A,\gamma\circ\beta) = \operatorname{Hom}_R(A,\gamma)\circ\operatorname{Hom}_R(A,\beta)$ for any R-module homomorphisms

$\beta : B \to C$ and $\gamma : C \to D$. Observe that $\operatorname{Hom}_R(A, \operatorname{id}_B)(\alpha)(a) = (\operatorname{id}_B \circ \alpha)(a) = \alpha(a)$ for every R-module homomorphism $\alpha : A \to B$ and every element $a \in A$, hence (1.) holds. Likewise, we have that $\operatorname{Hom}_R(A, \gamma \circ \beta)(\alpha) = \gamma \circ \beta \circ \alpha = \gamma \circ \operatorname{Hom}_R(A, \beta)(\alpha) = \operatorname{Hom}_R(A, \gamma) \circ \operatorname{Hom}_R(A, \beta)(\alpha)$ 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 $\operatorname{Hom}_R(\alpha, C) : \operatorname{Hom}_R(B, C) \to \operatorname{Hom}_R(A, C)$ defined by $\operatorname{Hom}_R(\alpha, C)(\beta) = \beta \circ \alpha$. One can demonstrate in a manner analogous to Proposition 1.2 that the map $\operatorname{Hom}_R(-, C) : \mathscr{R} \to \mathscr{R}$ that sends B to $\operatorname{Hom}_R(B, C)$ and sends an R-module homomorphism $\alpha : A \to B$ to the R-module homomorphism $\operatorname{Hom}_R(\alpha, C)$ is a **contravariant functor**, i.e., $\operatorname{Hom}_R(\beta \circ \alpha, C) = \operatorname{Hom}_R(\alpha, C) \circ \operatorname{Hom}_R(\beta, C)$.

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 1.3. *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 1.2, 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 $0 \to \operatorname{Hom}_R(M,A) \xrightarrow{\operatorname{Hom}_R(M,\alpha)} \operatorname{Hom}_R(M,B) \xrightarrow{\operatorname{Hom}_R(M,\beta)} \operatorname{Hom}_R(M,C)$; however, the induced cochain complex $0 \to \operatorname{Hom}_R(M,A) \xrightarrow{\operatorname{Hom}_R(M,\alpha)} \operatorname{Hom}_R(M,B) \xrightarrow{\operatorname{Hom}_R(M,\beta)} \operatorname{Hom}_R(M,C) \to 0$ is exact at $\operatorname{Hom}_R(M,C)$ if and only if $\operatorname{Hom}_R(M,\beta)$ 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 1.4. *Let R be a commutative ring. We say that an R-module P is* **projective** *if it satisfies any of the following equivalent conditions.*

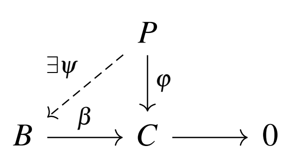
(i.) *If $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ is a short exact sequence of R-modules, then the sequence*

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

is exact, i.e., the functor $\operatorname{Hom}_R(P,-)$ 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.*



(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 1.3, 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.

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

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 $\operatorname{Hom}_R(P, -)$ 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 $\psi = \gamma \circ \rho \in \operatorname{Hom}_R(P, B)$. □

Corollary 1.5. *Every free R-module is projective.*

By Proposition 1.3, if we apply the contravariant functor $\operatorname{Hom}_R(-, N)$ 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 $0 \to \operatorname{Hom}_R(C, N) \xrightarrow{\operatorname{Hom}_R(\beta, N)} \operatorname{Hom}_R(B, N) \xrightarrow{\operatorname{Hom}_R(\alpha, N)} \operatorname{Hom}_R(A, N)$. Like before, the induced map $\operatorname{Hom}_R(\alpha, N)$ 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 1.6. *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*

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

is exact, i.e., the functor $\operatorname{Hom}_R(-, Q)$ *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.*

$$\begin{array}{ccccc} & & Q & & \\ & & {\scriptstyle\varphi}\uparrow & \nwarrow {\scriptstyle\exists\psi} & \\ 0 & \longrightarrow & A & \xrightarrow{\alpha} & B \end{array}$$

(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 1.3, 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.

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

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 a later proposition. 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 1.7. 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

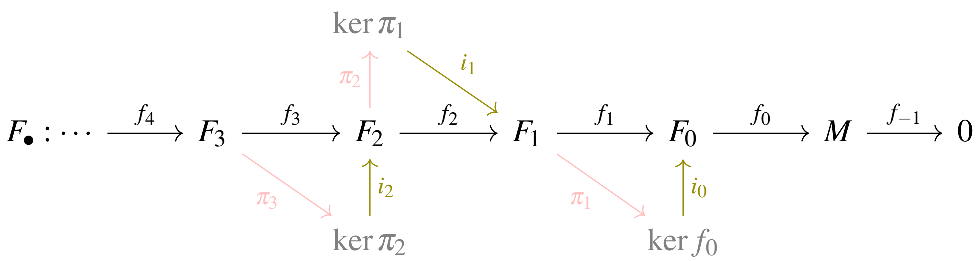
$$Z_\bullet : \cdots \xrightarrow{z_{n+1}} Z_n \xrightarrow{z_n} \cdots \xrightarrow{z_2} Z_1 \xrightarrow{z_1} Z_0 \xrightarrow{z_0} M \xrightarrow{z_{-1}} 0$$

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 1.8. *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. □

Combined, Proposition 1.8 and Corollary 1.5 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

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

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

Proposition 1.9. *Let N be an R-module. The following properties hold.*

(1.) *We have that* $\operatorname{Ext}_R^0(M, N) \cong \operatorname{Hom}_R(M, N)$ *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*
$$\cdots \to \operatorname{Ext}_R^{i-1}(M'', N) \to \operatorname{Ext}_R^i(M', N) \to \operatorname{Ext}_R^i(M, N) \to \operatorname{Ext}_R^i(M'', N) \to \operatorname{Ext}_R^{i+1}(M', N) \to \cdots.$$

(3.) *We have that* $\operatorname{Ext}_R^i(M,N) = 0$ *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 1.3, we may apply $\operatorname{Hom}_R(-,N)$ to obtain the sequence of R-modules

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

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

(3.) We assume first that N is injective. By Proposition 1.6, the functor $\operatorname{Hom}_R(-,N)$ is exact, hence for any R-module M and any projective resolution $P_\bullet$ of M, the induced cochain complex $\operatorname{Hom}_R(P_\bullet,N)$ is exact. We conclude that $\operatorname{Ext}_R^i(M,N) = 0$ for all integers $i \geq 1$. Conversely, suppose that $\operatorname{Ext}_R^i(M,N) = 0$ 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 1.4, N is injective.

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

One can show that $\operatorname{Ext}_R^i(-,N)$ 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 1.9 implies that the functors $\operatorname{Ext}_R^i(-,N)$ measure the injective "defect" of N.

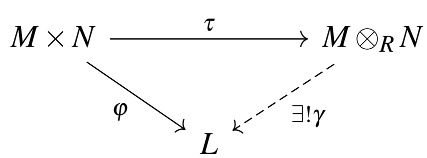
One might naturally expect that in order to rigorously define the projective "defect" of an R-module M, we must look at the cohomology modules of the induced cochain complex obtained by applying $\operatorname{Hom}_R(M,-)$ to an injective resolution of some R-module; however, it is unclear that an arbitrary 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 1.9. We begin by constructing a functor from the category of R-modules to itself that forms an "adjoint pair" with the covariant functor $\operatorname{Hom}_R(M,-)$.

2 Tensor Products and Tor

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 2.1 (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 2.2. *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.

$$\begin{array}{ccc} M \times N & \xrightarrow{\tau_1} & M \otimes_R N \\ \downarrow \sigma_1 & \swarrow \exists \gamma_1 & \\ N \otimes_R M & & \end{array} \qquad \begin{array}{ccc} N \times M & \xrightarrow{\tau_2} & N \otimes_R M \\ \downarrow \sigma_2 & \swarrow \exists \gamma_2 & \\ M \otimes_R N & & \end{array}$$

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 $r_1,\dots,r_k \in I$ and $x_1,\dots,x_k \in M$ such that $m-n = r_1x_1+\cdots+r_kx_k$. Considering that $r_i+I = 0_R+I$ for each integer $1 \le i \le k$, we find that

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

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 2.3. *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 $\eta : \operatorname{Hom}_R(M,M')\otimes_R \operatorname{Hom}_R(N,N') \to \operatorname{Hom}_R(M\otimes_R N, M'\otimes_R N')$.*

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 $\eta : \operatorname{Hom}_R(M, M') \otimes_R \operatorname{Hom}_R(N, N') \to \operatorname{Hom}_R(M \otimes_R N, M' \otimes_R N')$; it is not difficult to verify that η is R-linear, but we leave the details to the reader. □

Remark 2.4. 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 2.5. *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 2.4, 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 2.5, 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 2.6. *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 2.7. *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 2.6. 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 2.8. *Every commutative ring R is flat as a module over itself.*

Proof. Consider an injective R-module homomorphism $\alpha : A \to B$. By Proposition 2.2(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 2.9. *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 2.2(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 $\oplus_{i \in I}(L_i \otimes_R A)$, 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 2.8, as it is a direct sum of copies of R. □

Corollary 2.10. *Let R be a commutative ring. Every projective R-module is flat.*

Proof. By Proposition 1.4(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 2.9. □

Corollary 2.11. *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 $x_1, \dots, x_n$ of L whose images in $L/\mathfrak{m}L$ form an $R/\mathfrak{m}$-vector space basis. By Nakayama's Lemma, we have that $L = R\langle x_1, \dots, x_n \rangle$. Consequently, the canonical R-module homomorphism $\pi : R^n \to L$ defined by $\pi(r_1, \dots, r_n) = r_1 x_1 + \cdots + r_n x_n$ 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 2.6, 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 2.2, 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 4.9). 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 4.13 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 2.12. *[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 2.13. 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 2.10, 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 2.14. *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 2.2 and 2.6, 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 $\operatorname{Tor}_0^R(M,N) = \ker \ell_0^* / \operatorname{img} \ell_1^* = (M \otimes_R L_0)/[M \otimes_R (\operatorname{img} \ell_1)]$, hence our previous computation shows that $\operatorname{Tor}_0^R(M,N) \cong M \otimes_R (L_0/(\operatorname{img} \ell_1)) \cong M \otimes_R N$, as desired.

(3.) If M is flat, then $M \otimes_R -$ is exact by Proposition 2.7, 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 $\operatorname{Tor}_i^R(M,N) = 0$ for all integers $i \geq 1$. Conversely, suppose that $\operatorname{Tor}_i^R(M,N) = 0$ 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 2.7, 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 2.14 that the R-modules $\operatorname{Tor}_i^R(M,-)$ measure the flat "defect" of M. By Proposition 2.2, 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]).

One of the most important results in homological algebra is the Tensor-Hom Adjunction that relates the functors Hom and the tensor product. Let R and S be commutative rings. We say that an abelian group $(B,+)$ is an (R,S)-**bimodule** if it is an R-module via the action $\cdot$, an S-module via the action $*$, and these actions are "compatible" in the sense that $(r \cdot b) * s = r \cdot (b * s)$ for all elements $r \in R$, $s \in S$, and $b \in B$. Observe that if A is an R-module and B is an (R,S)-bimodule, then the tensor product $A \otimes_R B$ is a R-module via $r(a \otimes_R b) = (ra) \otimes_R b = a \otimes_R (rb)$ and a right S-module via $(a \otimes_R b)s = a \otimes_R (bs)$. One can check that $A \otimes_R B$ is an (R,S)-bimodule.

Theorem 2.15 (Tensor-Hom Adjunction)**.** *Let R and S be commutative rings. Let A be an R-module. Let B be an (R,S)-bimodule. Let C be an S-module. There exists a $\mathbb{Z}$-module isomorphism $\alpha : \operatorname{Hom}_S(A \otimes_R B, C) \to \operatorname{Hom}_R(A, \operatorname{Hom}_S(B,C))$ defined by $\alpha(\varphi)(a) : b \mapsto \varphi(a \otimes_R b)$ for all elements $a \in A$ and $b \in B$ and each S-module homomorphism $\varphi : A \otimes_R B \to C$.*

Proof. Before establishing the claim, we begin with a thorough examination of the objects therein. Each element of $\operatorname{Hom}_S(A \otimes_R B, C)$ is an S-module homomorphism $\varphi : A \otimes_R B \to C$. By definition, the pure tensors of $A \otimes_R B$ generate it as an S-module, hence every element of $\operatorname{Hom}_S(A \otimes_R B, C)$ is uniquely determined by its image on the pure tensors of $A \otimes_R B$. Likewise, the elements of $\operatorname{Hom}_R(A, \operatorname{Hom}_S(B,C))$ are R-module homomorphisms that send an element $a \in A$ to an S-module homomorphism $\psi_a : B \to C$. Consequently, for each S-module homomorphism $\varphi : A \otimes_R B \to C$, the designation of the S-module homomorphism $\psi_{\varphi,a} : B \to C$ onto which φ is mapped for each element $a \in A$ induces a function $\alpha : \operatorname{Hom}_S(A \otimes_R B, C) \to \operatorname{Hom}_R(A, \operatorname{Hom}_S(B,C))$. Considering that φ and the tensor product are (right) S-linear, the map $\psi_{\varphi,a} : B \to C$ defined by $\psi_{\varphi,a}(b) = \varphi(a \otimes_R b)$ is an S-module homomorphism that satisfies $\psi_{\varphi,a} = \alpha(\varphi)(a)$ as in the statement of the theorem.

We must prove first that α is $\mathbb{Z}$-linear. Given any S-module homomorphisms $\varphi : A \otimes_R B \to C$ and $\gamma : A \otimes_R B \to C$ and any element $n \in \mathbb{Z}$, we have that

$$\psi_{n\varphi+\gamma,a}(b) = (n\varphi + \gamma)(a \otimes_R b) = n\varphi(a \otimes_R b) + \gamma(a \otimes_R b) = (n\psi_{\varphi,a} + \psi_{\gamma,a})(b)$$

for all elements $a \in A$ and $b \in B$. By our previous identification, we conclude that α is $\mathbb{Z}$-linear.

If $\varphi : A \otimes_R B \to C$ lies in $\ker \alpha$, then $\psi_{\varphi,a}$ is the zero homomorphism for each element $a \in A$. Consequently, we find that $\varphi(a \otimes_R b) = \psi_{\varphi,a}(b) = 0$ for all elements $a \in A$ and $b \in B$. Considering that the pure tensors generate $A \otimes_R B$, we conclude that φ is the zero homomorphism.

Last, suppose that $\psi : A \to \operatorname{Hom}_R(B,C)$ is an R-module homomorphism. Let ψ_a denote the S-module homomorphism $\psi(a) : B \to C$, as in the opening paragraph of the proof. Consider the map $\sigma : A \times B \to C$ defined by $\sigma(a,b) = \psi_a(b)$. By assumption that ψ and its images ψ_a are all biadditive, it follows that $\sigma(a+a',b) = \psi_{a+a'}(b) = (\psi_a + \psi_{a'})(b) = \psi_a(b) + \psi_{a'}(b) = \sigma(a,b) + \sigma(a',b)$

and $\sigma(a, b+b') = \psi_a(b+b') = \psi_a(b) + \psi_a(b') = \sigma(a,b) + \sigma(a,b')$ for all elements $a, a' \in A$ and $b, b' \in B$. We conclude that σ is a biadditive R-module homomorphism, hence the Universal Property of the Tensor Product guarantees the existence of a biadditive $\mathbb{Z}$-module homomorphism $\gamma : A \otimes_R B \to C$ such that $\gamma(a \otimes_R b) = \sigma(a,b) = \psi_a(b)$ for all elements $a \in A$ and $b \in B$. Consequently, we find that ψ is the image of γ under α, hence α is surjective. $\square$

3 Existence of Injective Modules

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

Theorem 3.1 (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 3.2. *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 3.3. *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 $\operatorname{ev}(am+m')(\varphi) = \varphi(am+m') = \varphi(am)+\varphi(m') = a\varphi(m)+\varphi(m') = a\operatorname{ev}(m)(\varphi)+\operatorname{ev}(m')(\varphi)$ 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 $\operatorname{ev}(m)(a\varphi+\psi) = a\operatorname{ev}(m)(\varphi)+\operatorname{ev}(m)(\psi)$ 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 1.6, $\operatorname{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z})$ 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 $F^* = \operatorname{Hom}_{\mathbb{Z}}\left(\bigoplus_{\varphi \in M^*} \mathbb{Z}, \mathbb{Q}/\mathbb{Z}\right) \cong \prod_{\varphi \in M^*}(\mathbb{Q}/\mathbb{Z})$. Ultimately, $\pi^* \circ \operatorname{ev} : M \to F^*$ 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 3.2 and [Rot09, Proposition 3.28(i)]. □

Lemma 3.4. *Let R be a commutative ring. If P is a projective R-module and Q is an injective $\mathbb{Z}$-module, then $P^Q = \operatorname{Hom}_{\mathbb{Z}}(P, Q)$ 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 1.6, it suffices to show that $\operatorname{Hom}_R(-, P^Q)$ 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 2.2(1.) and 2.10. By applying Proposition 1.6, we find that

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

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

Proposition 3.5. *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 3.3, there exists an injective $\mathbb{Z}$-module Q and an injective $\mathbb{Z}$-module homomorphism $\varphi : M \to Q$. By Proposition 1.3, this induces an injective $\mathbb{Z}$-module homomorphism $\operatorname{Hom}_{\mathbb{Z}}(R, \varphi) : \operatorname{Hom}_{\mathbb{Z}}(R, M) \to \operatorname{Hom}_{\mathbb{Z}}(R, Q)$. Crucially, $\operatorname{Hom}_{\mathbb{Z}}(R, Q)$ is an injective R-module by Lemma 3.4, hence it suffices to find an injective R-module homomorphism $M \to \operatorname{Hom}_{\mathbb{Z}}(R, Q)$.

Consider the map $\mu : M \to \operatorname{Hom}_{\mathbb{Z}}(R, M)$ 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 $\operatorname{Hom}_{\mathbb{Z}}(R, \varphi) \circ \mu : M \to \operatorname{Hom}_{\mathbb{Z}}(R, Q)$ is an injective $\mathbb{Z}$-module homomorphism.

Given any element $r \in R$, observe that $(\operatorname{Hom}_{\mathbb{Z}}(R, \varphi) \circ \mu)(rm) = \varphi \circ \mu(rm)$ is the $\mathbb{Z}$-module homomorphism that sends an element $s \in R$ to the element $\varphi(rsm)$ of Q. Likewise, the composite map $(\operatorname{Hom}_{\mathbb{Z}}(R, \varphi) \circ \mu)(m)$ 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 $\operatorname{Hom}_{\mathbb{Z}}(R, Q)$ defined in Lemma 3.4, it follows that $r[(\operatorname{Hom}_{\mathbb{Z}}(R, \varphi) \circ \mu)(m)]$ and $(\operatorname{Hom}_{\mathbb{Z}}(R, \varphi) \circ \mu)(rm)$ are identical on R, hence they are equal. We conclude that $\operatorname{Hom}_{\mathbb{Z}}(R, \varphi) \circ \mu$ is an R-module homomorphism, and our proof is complete. □

Ultimately, Proposition 3.5 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

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

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

Proposition 3.6. *Let M be an R-module. The following properties hold.*

(1.) *We have that* $\operatorname{Ext}^0_R(M,N) \cong \operatorname{Hom}_R(M,N)$ *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*
$$\cdots \to \operatorname{Ext}^{i-1}_R(M,N'') \to \operatorname{Ext}^i_R(M,N') \to \operatorname{Ext}^i_R(M,N) \to \operatorname{Ext}^i_R(M,N'') \to \operatorname{Ext}^{i+1}_R(M,N') \to \cdots.$$

(3.) *We have that* $\operatorname{Ext}^i_R(M,N) = 0$ *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 3.6. □

One can show that $\operatorname{Ext}^i_R(M,-)$ 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 3.6 that the functors $\operatorname{Ext}^i_R(M,-)$ measure the projective "defect" of M. Later, in our discussion of canonical modules, we will need the following proposition.

Proposition 3.7. *[Rot09, Proposition 7.24] Let R be a commutative ring with R-modules A and C. If* $\operatorname{Ext}^1_R(C,A) = 0$, *then every short exact sequence* $0 \to A \to B \to C \to 0$ *splits.*

Proof. Consider a short exact sequence $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$. By applying $\operatorname{Hom}_R(C,-)$, we obtain a long exact sequence of Ext in which the terms $\operatorname{Hom}_R(C,B) \xrightarrow{\gamma} \operatorname{Hom}_R(C,C) \xrightarrow{\alpha^*} \operatorname{Ext}^1_R(C,A)$ appear. By hypothesis that $\operatorname{Ext}^1_R(C,A) = 0$, we find that $\operatorname{Hom}_R(C,C) = \ker \alpha^* = \operatorname{img} \gamma$, hence γ is surjective.

Particularly, there exists an R-module homomorphism $\beta' : C \to B$ such that $\mathrm{id}_C = \beta \circ \beta'$. By the Splitting Lemma, we conclude that the short exact sequence $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ 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 3.8. *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 $I_i = \mathrm{img}\, q^i$ for each integer $i \geq -1$. For all integers $n \geq i+2$, there exist R-modules isomorphisms $\mathrm{Ext}_R^{n-i}(A, I_i) \cong \mathrm{Ext}_R^{n-i-1}(A, I_{i+1})$.*

Proof. We will illustrate that $\mathrm{Ext}_R^{n+1}(A,M) \cong \mathrm{Ext}_R^n(A, I_0)$; the remaining isomorphisms follow similarly. By hypothesis that $Q^\bullet$ is an injective resolution of M, we may obtain an injective resolution of $I_0 = \mathrm{img}\, q^0$ 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 $\ker q^1 = \mathrm{img}\, q^0 = I^0 = \mathrm{img}\, i$ 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

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

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

Proposition 3.9. *Let R be a commutative ring. The following are equivalent.*

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

(ii.) *The R-module M satisfies $\mathrm{Ext}_R^{n+1}(A,M) = 0$ 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 3.8, for every R-module A, we have that $\mathrm{Ext}_R^{n+1}(A,M) \cong \mathrm{Ext}_R^1(A,Q^n)$. But Q^n is injective, hence the latter Ext vanishes by Proposition 1.9. Conversely, suppose that $\mathrm{Ext}_R^{n+1}(A,M) = 0$ for all R-modules A. Consider an injective resolution $Q^\bullet$ of M. By Lemma 3.8, we have that $\mathrm{Ext}_R^{n+1}(A,M) \cong \mathrm{Ext}_R^1(A,I_n)$, 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 3.10. *[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*

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

References

[BH93] W. Bruns and J. Herzog. *Cohen–Macaulay Rings*. 2nd ed. Vol. 39. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1993.

[Gat13] A. Gathmann. *Commutative Algebra*. 2013. URL: https://www.mathematik.uni-kl.de/~gathmann/de/commalg.php.

[Rot09] J.J. Rotman. *An Introduction to Homological Algebra*. second. Universitext. Springer, 2009.

4 Appendix

4.1 Rings, Ideals, and Modules

Unless otherwise stated, we will assume throughout this appendix 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 4.1. We denote by $\operatorname{Spec}(R)$ the collection of prime ideals of R, i.e.,

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

Occasionally, we will write $\operatorname{MaxSpec}(R) = \{M \subseteq R \mid M \text{ is a maximal ideal of R }\}$. We refer to $\operatorname{Spec}(R)$ as the **spectrum** of R; likewise, $\operatorname{MaxSpec}(R)$ is the **maximal spectrum** of R. We define also the **Jacobson radical** $\operatorname{Jac}(R)$ of R as the intersection of all maximal ideals of R.

Example 4.2. Let $\mathbb{Z}$ denote the ring of integers. We have that $\operatorname{Spec}(\mathbb{Z}) = \{p\mathbb{Z} \mid p \text{ is prime}\} \cup \{0\}$ because $\mathbb{Z}$ is a Euclidean domain and $\operatorname{MaxSpec}(\mathbb{Z}) = \operatorname{Spec}(\mathbb{Z}) \setminus \{0\}$.

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 $p_1, \dots, p_k$ and positive integers $e_1, \dots, e_k$ 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 4.3. 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 $x_1, \dots, x_n \in I$ such that for every element $x \in I$, we have that $x = r_1 x_1 + \cdots + r_n x_n$ for some elements $r_1, \dots, r_n \in R$.

Example 4.4. 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 4.3.

One can show that if R is a Noetherian ring, then any polynomial ring over R, any quotient of R by an ideal, and any finitely generated R-algebra is itself a Noetherian ring. By the previous example, any polynomial ring or finitely generated algebra over a field is a Noetherian ring. Even more, Example 4.4 shows that the only maximal ideal of a field is the zero ideal.

Definition 4.5. 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 4.6. *Let R be a commutative unital ring. The following conditions are equivalent.*

(i.) *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 4.7. 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 $\mathfrak{m} = (\bar{x})$.

Using a process analogous to the construction of the rational numbers $\mathbb{Q}$ from the integers $\mathbb{Z}$, one can always obtain a local ring from a given ring. Recall that a set $S \subseteq R$ is **multiplicatively closed** if S contains 1_R and for any elements $s, t \in S$, we have that $st \in S$. Given any multiplicatively closed set $S \subseteq R$, one can construct an equivalence relation on $R \times S$ by declaring that $(r,s) \sim (r',s')$ if and only if there exists an element $t \in S$ such that $t(rs' - r's) = 0_R$. One need only check that if $(r,s) \sim (r',s')$ and $(r',s') \sim (r'',s'')$, then $(r,s) \sim (r'',s'')$. But in this case, there exist elements $t, t' \in S$ such that $t(rs' - r's) = 0_R$ and $t'(r's'' - r''s') = 0_R$, hence the product $s'tt'$ belongs to S and satisfies $s'tt'(rs'' - r''s) = 0_R$. Like with rational numbers, we denote by r/s the equivalence class of (r,s) modulo $\sim$. Consider the set of equivalence classes of $(R \times S)/\sim$, denoted by

$$S^{-1}R = \left\{ \frac{r}{s} : r \in R, s \in S, \text{ and } \frac{r}{s} = \frac{r'}{s'} \iff \text{there exists } t \in S \text{ such that } t(rs' - r's) = 0_R \right\}.$$

We refer to $S^{-1}R$ as the **localization** of R with respect to S. Observe that by definition, if $0_R \in S$, then $S^{-1}R = \{0_R\}$. Consequently, we will always assume that $0_R \notin S$.

Proposition 4.8. *Let R be a commutative unital ring with a multiplicatively closed subset S.*

(1.) *$S^{-1}R$ is a commutative unital ring with respect to $\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'}$ and $\frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}$.*

(2.) *There is a canonical ring homomorphism $\lambda : R \to S^{-1}R$ defined by $\lambda(r) = \frac{r}{1_R}$.*

(3.) *For any ideal I of R, we have that $IS^{-1}R = \lambda(I) = \left\{ \frac{i}{s} : i \in I \text{ and } s \in S \right\}$.*

(4.) *For any ideal I of $S^{-1}R$, we have that $\lambda^{-1}(I)S^{-1}R = \lambda(\lambda^{-1}(I)) = I$.*

(5.) *The canonical ring homomorphism $\lambda : R \to S^{-1}R$ induces a one-to-one correspondence between $\operatorname{Spec}(S^{-1}R)$ and the prime ideals of R such that $P \cap S = \emptyset$.*

$$\{P \in \operatorname{Spec}(R) \mid P \cap S = \emptyset\} \leftrightarrow \operatorname{Spec}(S^{-1}R), P \mapsto \lambda(P) = PS^{-1}R$$

(6.) *(Existence of Local Maximal Ideals) If I is an ideal of R such that $I \cap S = \emptyset$, then there exists* *a prime ideal P of R such that $P \cap S = \emptyset$ and $S^{-1}P$ is a maximal ideal of $S^{-1}R$. Particularly, the prime ideal P is the largest (with respect to inclusion) ideal of R that is disjoint from S.*

(7.) *If P is a prime ideal of R, then $W = R \setminus P$ is a multiplicatively closed set. Further, the localization $R_P = W^{-1}R$ is a local ring with unique maximal ideal PR_P.*

Proof. We omit the proofs of properties (1.), (2.), (3.), and (4.), as they are routine to check.

(5.) We establish first that the map is well-defined, i.e., we show that if P is a prime ideal of R such that $P \cap S = \emptyset$, then the ideal $\lambda(P) = PS^{-1}R$ of $S^{-1}R$ is prime. Given any elements $a/s, b/t \in S^{-1}R$ such that $(a/s)(b/t) \in \lambda(P)$, we claim that either $a/s \in \lambda(P)$ or $b/t \in \lambda(P)$. By definition, we have that $(a/s)(b/t) = ab/st$ belongs to $\lambda(P)$ if and only if there exist some elements $c \in P$ and $u, v \in S$ such that $v(abu - stc) = 0_R$ or $vabu = vstc$. By hypothesis that c belongs to P, we conclude that $vabu$ belongs to P. Considering that P is a prime ideal of R, one of the elements a, b, u, or v must belong to P. By construction, neither u nor v belongs to P, so either a or b belong to P. Consequently, either a/s or b/t belong to $\lambda(P)$, and we conclude that $\lambda(P)$ is prime.

Our previous paragraph establishes that the map is well-defined. We proceed to show that it has a well-defined inverse. Consider the map $P \mapsto \lambda^{-1}(P)$. If $PS^{-1}R$ is a prime ideal of $S^{-1}R$, then its contraction $\lambda^{-1}(P)$ is a prime ideal of R. Further, every element of S is mapped onto a unit by λ, hence if $\lambda^{-1}(P) \cap S$ were nonempty, then $P = \lambda(\lambda^{-1}(P))$ would be the entire ring $S^{-1}R$ — a contradiction. We conclude that the map $P \mapsto \lambda^{-1}(P)$ is well-defined. By property (2.) above, we have that $\lambda(\lambda^{-1}(P)) = P$ for all prime ideals P of $S^{-1}R$, hence the map $P \mapsto \lambda^{-1}(P)$ has a left-inverse. On the other hand, we claim that $\lambda^{-1}(\lambda(P)) = P$ so that the map $P \mapsto \lambda^{-1}(P)$ has a right-inverse. Clearly, it is always the case that $P \subseteq \lambda^{-1}(\lambda(P))$. Conversely, let x be an element of $\lambda^{-1}(\lambda(P))$. By definition, we have that $\lambda(x)$ belongs to $\lambda(P)$, hence there exist elements $s, t \in S$ and $p \in P$ such that $t(xs - p) = 0_R$. But this implies that txs belongs to the prime ideal P so that x belongs to P by assumption that $s, t \in S$ and $P \cap S = \emptyset$. We conclude that $\lambda^{-1}(\lambda(P)) = P$.

(6.) Observe that the collection $\mathscr{D} = \{I \subseteq R \mid I \text{ is an ideal of } R \text{ and } I \cap S = \emptyset\}$ is partially ordered by inclusion. Further, it is nonempty because it contains the zero ideal of R. Given any chain $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ of ideals in $\mathscr{D}$, the union $\cup_{n=1}^{\infty} I_n$ is an ideal of R that is disjoint from S. Consequently, every chain in $\mathscr{D}$ has an upper bound in $\mathscr{D}$, hence $\mathscr{D}$ has a maximal element P by Zorn's Lemma. We claim that P is a prime ideal of R. Consider some elements $a, b \in R$ such that $ab \in P$. On the contrary, if neither $a \in P$ nor $b \in P$, then we would have that $P \subsetneq aR + P$ and $P \subsetneq bR + P$. By the maximality of P, there would exist elements $s \in (aR+P) \cap S$ and $t \in (bR+P) \cap S$. Observe that $(aR+P)(bR+P) \subseteq P$ so that $st \in (aR+P)(bR+P)$ belongs to P — a contradiction.

(7.) By definition, a prime ideal P of R is a proper ideal such that $ab \in P$ implies that $a \in P$ or $b \in P$. Equivalently, if neither $a \in P$ nor $b \in P$, then $ab \in R \setminus P$, i.e., $W = R \setminus P$ is multiplicatively closed. By properties (1.) and (5.), $\operatorname{Spec}(R_P)$ is in bijection with $\{Q \in \operatorname{Spec}(R) \mid Q \cap W = \emptyset\} = \{Q \in \operatorname{Spec}(R) \mid Q \subseteq P\}$. We conclude that PR_P is the unique maximal ideal of the local ring R_P. $\square$

By definition, the zero ideal of a domain D is prime. Consequently, we may construct the local ring $\operatorname{Frac}(D) = W^{-1}R$ for the multiplicatively closed set $W = D \setminus \{0_D\}$. Observe that $\operatorname{Frac}(D)$ is the **field of fractions** of D: every nonzero element d/w of $\operatorname{Frac}(D)$ has multiplicative inverse w/d. Particularly, we have that $\operatorname{Frac}(\mathbb{Z}) = \mathbb{Q}$. Generally, the set S of non-zero divisors of a commutative unital ring is multiplicatively closed; the ring $Q(R) = S^{-1}R$ is the **total ring of fractions** of R.

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 4.9. We say that an abelian group $(M, +)$ is an R-**module** if there is a map $\cdot : R \times M \to M$ that sends $(r, m) \mapsto r \cdot m$ 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.

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

Lemma 4.10 (Prime Avoidance Lemma)**.** *[BH93, Lemma 1.2.2] Let R be a commutative unital ring with prime ideals $P_1, \dots, P_n$. Let M be an R-module with $x_1, \dots, x_n \in M$. Let $N = R\langle x_1, \dots, x_n \rangle$. If $N_{P_i} \not\subseteq P_i M_{P_i}$ for any integer $1 \leq i \leq n$, then there exists an element $x \in N$ such that $x \notin P_i M_{P_i}$ 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 $1 \leq i \leq n$.*

One of the most valuable results on finitely generated modules is the **Cayley-Hamilton Theorem**; the reader might be familiar with its use in linear algebra, but we state it in generality.

Theorem 4.11 (Cayley-Hamilton Theorem)**.** *Let R be a commutative unital ring. Let M be a finitely generated R-module. For any ideal I and any R-module homomorphism $\varphi : M \to M$ such that $\varphi(M) \subseteq IM$, there exists a monic polynomial $t^n + i_1 t^{n-1} + \cdots + i_{n-1} t + i_n$ with $i_1, \dots, i_n \in I$ such that $\varphi^n + i_1 \varphi^{n-1} + \cdots + i_{n-1} \varphi + i_n \operatorname{id}_M$ is the zero homomorphism on M.*

Proof. Let $x_1, \dots, x_n$ be a system of R-module generators of M. By hypothesis that $\varphi(M) \subseteq IM$, we may view M as an $R[t]$-module via the action $t \cdot x = \varphi(x)$. Considering that $M = R\langle x_1, \dots, x_n \rangle$ and $\varphi(M) \subseteq IM$ by assumption, for each integer $1 \leq j \leq n$, there exist elements $i_{j,1}, \dots, i_{j,n} \in I$ such that $t \cdot x_j = \varphi(x_j) = \sum_{k=1}^n i_{j,k} x_k$ or $\sum_{k=1}^n (\delta_{j,k} t - i_{j,k}) x_k = 0_R$, where $\delta_{j,k}$ is the Kronecker delta. Consider the matrix A whose jth row and kth column is $\delta_{j,k} s - i_{j,k}$. Observe that the previous identity shows that $A\mathbf{x} = \mathbf{0}$ for the column vector $\mathbf{x} = \langle x_1, \dots, x_n \rangle^t$. Using the fact that $\operatorname{adj}(A)A$ is $\det(A)$ times the $n \times n$ identity matrix, we conclude that $\det(A)\mathbf{x} = \mathbf{0}$. Consequently, $\det(A)$ is a monic polynomial in t with coefficients in I that acts as the zero homomorphism on M. □

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 4.12 (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 $x_1, \dots, x_n$ modulo $\mathfrak{m}M$ form a basis of the k-vector space $M/\mathfrak{m}M$, then $M = R\langle x_1, \dots, x_n \rangle$.*

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 4.13. *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 $x_1, \dots, x_n$ denote a system of generators of M such that $x_1 + \mathfrak{m}M, \dots, x_n + \mathfrak{m}M$ 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 $r_{i,1}, \dots, r_{i,n} \in I$ 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 $y_1 + \mathfrak{m}M, \dots, y_n + \mathfrak{m}M$ forms a basis of $M/\mathfrak{m}M$. We conclude by Nakayama's Lemma that $M = R\langle y_1, \dots, y_n \rangle$ 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 4.3.

Definition 4.14. 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 describe two paramount results on Noetherian modules over Noetherian rings.

Lemma 4.15 (Artin-Rees Lemma)**.** *Let R be Noetherian. For any ideal I and finitely generated R-modules $N \subseteq M$, there exists an integer $k \geq 1$ such that $I^n M \cap N = I^{n-k}(I^k M \cap N)$ for all $n \geq k$.*

Theorem 4.16 (Krull's Intersection Theorem)**.** *Let R be a Noetherian ring. For any proper ideal I of R and any finitely generated R-module M, we have that $\bigcap_{n \geq 0} I^n M = I\big(\bigcap_{n \geq 0} I^n M\big)$. Even more, there exists an element $x \in I$ such that $(1_R - x)\bigcap_{n \geq 0} I^n M = 0$. If R is local, then $\bigcap_{n \geq 0} I^n M = 0$.*

Proof. Observe that $N = \bigcap_{n \geq 0} I^n M$ is a finitely generated R-submodule of M and $N = I^n M \cap N$ for all integers $n \geq 0$. By the Artin-Rees Lemma, there exists an integer $k \geq 1$ such that

$$N = I^n M \cap N = I^{n-k}(I^k M \cap N) = I^{n-k} N$$

for all integers $n \geq k$. We conclude that $N = IN$, i.e., we have that $\operatorname{id}_N(N) \subseteq IN$. By the Cayley-Hamilton Theorem, there exists a monic polynomial $t^n + i_1 t^{n-1} + \cdots + i_{n-1} t + i_n$ with $i_1, \dots, i_n \in I$ such that $(1_R + i_1 + \cdots + i_{n-1} + i_n)\operatorname{id}_N$ is the zero endomorphism on N. Consequently, we find that $(1_R + i_1 + \cdots + i_{n-1} + i_n)N = 0$ so that $(1_R - x)N = 0$ with $x = -(i_1 + \cdots + i_{n-1} + i_n) \in I$.

Last, if R is local, then we conclude that $\bigcap_{n \geq 0} I^n M = N = 0$ by Corollary 4.13. □

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 4.17. 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 4.18. *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 4.17, 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 4.19. *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 4.20. *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 4.17, 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 4.18, 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 $r_1, \dots, r_n \in \mathfrak{m}$ 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 $r_1 \cdots r_k m = sr_1 \cdots r_{k+1} m$. By rearranging, we would obtain $(1_R - sr_{k+1}) r_1 \cdots r_k m = 0$. By Proposition 4.6, we would find that $1_R - sr_{k+1}$ 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. □

Corollary 4.21. *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 4.20, 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 4.20. Last, R is Noetherian by Proposition 4.18. □

By the proof of Proposition 4.20, we obtain the following important and useful fact.

Proposition 4.22. *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. □

We define the **colength** of an R-submodule N of an R-module M to be the length of the quotient module M/N, i.e., the colength of N in M is $\ell_R(M/N)$. If I is an ideal of R with finite colength, then R/I is Artinian and Noetherian by Proposition 4.18. Conversely, if R is Noetherian and R/I is Artinian, then R/I is Noetherian and Artinian, hence I has finite colength.

We say that an ideal I of R is P-**primary** for a prime ideal P of R if $P = \sqrt{I}$. Observe that if $P^n \subseteq I \subseteq P$ for some integer $n \gg 0$, then $P = \sqrt{I}$ so that I is P-primary. We establish next a necessary and sufficient condition for ideals of finite colength in a Noetherian local ring.

Proposition 4.23. *Let $(R, \mathfrak{m})$ be a local ring. Let I be an ideal of R. If I has finite colength, then I is $\mathfrak{m}$-primary. Conversely, if R is Noetherian and I is $\mathfrak{m}$-primary, then I has finite colength.*

Proof. By definition, if I has finite colength, then R/I has finite length as an R-module. By Proposition 4.20, we have that $\mathfrak{m}^n(R/I) = 0$ for some integer $n \gg 0$ so that $\mathfrak{m}^n \subseteq I \subseteq \mathfrak{m}$ and I is $\mathfrak{m}$-primary. Conversely, if I is $\mathfrak{m}$-primary, then $\mathfrak{m} = \sqrt{I}$. By hypothesis that R is Noetherian, this is equivalent to the condition that $\mathfrak{m}^n \subseteq I \subseteq \mathfrak{m}$ for some integer $n \gg 0$, from which it follows that $\mathfrak{m}^n(R/I) = 0$. Even more, we have that $\dim(R/I) = 0$ so that R/I is Artinian, from which it follows that R/I has finite length as an R-module, i.e., I has finite colength. □

4.2 Localization as a Functor

Let S be a multiplicatively closed subset of a commutative ring R. Our aim in this section is to illustrate that localization of an R-module with respect to S is an exact functor. Localization of a commutative ring at a prime ideal yields a commutative local ring, hence this fact reduces many questions to the local case. Given an R-module M, we may construct its localization at S in the same manner as in the section on Rings, Ideals, and Modules. Consider the equivalence relation on $M \times S$ induced by declaring that $(m, s) \sim (m', s')$ if and only if there exists an element $t \in S$ such that $t(s'm - sm') = 0$; then, the localization of M with respect to S is

$$S^{-1}M = \left\{ \frac{m}{s} : m \in M, s \in S, \text{ and } \frac{m}{s} = \frac{m'}{s'} \iff \text{there exists } t \in S \text{ such that } t(s'm - sm') = 0 \right\}.$$

Proposition 4.24. *Let S be a multiplicatively closed subset of a commutative ring R. Let M be an R-module. The localization of M with respect to S is an $S^{-1}R$-module via the action $\frac{r}{u} \cdot \frac{m}{v} = \frac{rm}{uv}$.*

Proof. We illustrate first that this action is well-defined. By definition, if $\frac{r}{u} = \frac{s}{v}$ in $S^{-1}R$, then there exists an element $t \in S$ such that $rtv = stu$. Given any element $\frac{m}{w}$ of $S^{-1}M$, we have that $rtvwm = stuwm$ so that $\frac{r}{u} \cdot \frac{m}{w} = \frac{rm}{uw} = \frac{sm}{vw} = \frac{s}{v} \cdot \frac{m}{w}$. We must now verify that the action satisfies the distributive laws; the other two properties hold by definition. Observe that for any elements $r_1, r_2 \in R$, $u_1, u_2, v \in S$, and $m \in M$, we have that

$$\left(\frac{r_1}{u_1} + \frac{r_2}{u_2}\right) \cdot \frac{m}{v} = \frac{r_1u_2 + r_2u_1}{u_1u_2} \cdot \frac{m}{v} = \frac{r_1u_2m + r_2u_1m}{u_1u_2v} = \frac{r_1u_2m}{u_1u_2v} + \frac{r_2u_1m}{u_1u_2v} = \frac{r_1}{u_1} \cdot \frac{m}{v} + \frac{r_2}{u_2} \cdot \frac{m}{v}.$$

We note that a similar analysis shows that multiplication distributes over addition in $S^{-1}M$. □

Consequently, localization with respect to S converts an R-module into an $S^{-1}R$-module. Given any R-module homomorphism $\varphi : M \to N$, consider the map $S^{-1}\varphi : S^{-1}M \to S^{-1}N$ defined by $S^{-1}\varphi\left(\frac{m}{s}\right) = \frac{\varphi(m)}{s}$. Observe that for any elements $r \in R$, $u, v, w \in S$, and $m, n \in M$, we have that

$$S^{-1}\varphi\left(\frac{r}{u} \cdot \frac{m}{v} + \frac{n}{w}\right) = \varphi\left(\frac{rwm + uvn}{uvw}\right) = \frac{\varphi(rwm + uvn)}{uvw} = \frac{rw\varphi(m) + uv\varphi(n)}{uvw} = \frac{r}{u} \cdot \frac{\varphi(m)}{v} + \frac{\varphi(n)}{w},$$

hence the induced map $S^{-1}\varphi$ is an $S^{-1}R$-module homomorphism. Considering that $S^{-1}M$ is an R-module with respect to the action $r \cdot \frac{m}{s} = \frac{rm}{s}$, the map $S^{-1}\varphi$ is also an R-module homomorphism.

Proposition 4.25. *Let S be a multiplicatively closed subset of a commutative ring R. Let $\mathscr{R}$ be the category of R-modules. The map $S^{-1}(-)$ that sends an R-module M to $S^{-1}M$ (viewed as either an R-module or an $S^{-1}R$-module) and sends an R-module homomorphism $\varphi : M \to N$ to the module homomorphism $S^{-1}\varphi : S^{-1}M \to S^{-1}N$ is a covariant functor that preserves bijections.*

Proof. Clearly, the induced map $S^{-1}\,\mathrm{id}_M$ is the identity on $S^{-1}M$. Given any R-module homomorphisms $\varphi : A \to B$ and $\psi : B \to C$, it is straightforward to verify that $S^{-1}(\psi \circ \varphi) = S^{-1}\psi \circ S^{-1}\varphi$. We conclude that $S^{-1}(-)$ is a functor. Consider a bijective R-module homomorphism $\gamma : M \to N$. If $\frac{m}{s}$ lies in the kernel of $S^{-1}\gamma$, then there exists an element $t \in S$ such that $\gamma(tm) = t\gamma(m) = 0$. By hypothesis that γ is injective, we conclude that $tm = 0$, from which it follows that $\frac{m}{s} = 0$. On the other hand, for any element $\frac{n}{s}$ of $S^{-1}M$, there exists an element $m \in M$ such that $\frac{n}{s} = \frac{\gamma(m)}{s} = S^{-1}\gamma\left(\frac{m}{s}\right)$

by assumption that γ is surjective. We conclude that $S^{-1}\gamma$ is a bijection. □

Corollary 4.26. *Let S be a multiplicatively closed subset of a commutative ring R. If there is a short exact sequence of R-modules $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$, then there is an induced short exact sequence $0 \to S^{-1}A \xrightarrow{S^{-1}\alpha} S^{-1}B \xrightarrow{S^{-1}\beta} S^{-1}C \to 0$ (of either R-modules or $S^{-1}R$-modules).*

Proof. By Proposition 4.25, we have that $S^{-1}\alpha$ is injective and $S^{-1}\beta$ is surjective, so it suffices to check the exactness of the sequence at $S^{-1}B$. Considering that $S^{-1}\beta \circ S^{-1}\alpha = S^{-1}(\beta \circ \alpha) = 0$, we have that $\operatorname{img}(S^{-1}\alpha) \subseteq \ker(S^{-1}\beta)$. If $\frac{b}{s}$ lies in the kernel of $S^{-1}\beta$, then there exists an element $t \in S$ such that $\beta(tb) = t\beta(b) = 0$. Consequently, we may find an element $a \in A$ such that $\alpha(a) = tb$ and $1_R(s\alpha(a) - stb) = 0$. We conclude that $\frac{b}{s} = \frac{\alpha(a)}{st} = S^{-1}\alpha\big(\frac{a}{st}\big)$ and $\ker(S^{-1}\beta) \subseteq \operatorname{img}(S^{-1}\alpha)$. □

Observe that if M is an R-module, then $S^{-1}R \otimes_R M$ is an R-module. On the other hand, we may view $S^{-1}R \otimes_R M$ as an $S^{-1}R$-module via the action $\frac{a}{b} \cdot \big(\frac{r}{s} \otimes_R m\big) = \frac{ar}{bs} \otimes_R m$ by the proof of Proposition 4.25. Consider the map $\varphi : S^{-1}R \times M \to S^{-1}M$ defined by $\varphi\big(\frac{r}{s}, m\big) = \frac{rm}{s}$. Observe that φ is multiplication in the second coordinate, hence it is R-linear in the second coordinate. On the other hand, for any elements $a, r, s \in R$, $u, v \in S$, and $m \in M$, we have that

$$\varphi\Big(a \cdot \frac{r}{u} + \frac{s}{v}, m\Big) = \varphi\bigg(\frac{arv + su}{uv}, m\bigg) = \frac{(arv + su)m}{uv} = \frac{arvm}{uv} + \frac{sum}{uv} = a \cdot \varphi\Big(\frac{r}{u}, m\Big) + \varphi\Big(\frac{s}{v}, m\Big),$$

hence φ is R-linear in the first coordinate. We conclude that φ is a bilinear R-module homomorphism. By the Universal Property of the Tensor Product, there exists a bilinear R-module homomorphism $\gamma : S^{-1}R \otimes_R M \to S^{-1}M$ that satisfies $\gamma\big(\frac{r}{s} \otimes_R m\big) = \frac{rm}{s}$. We exhibit an R-module homomorphism $\psi : S^{-1}M \to S^{-1}R \otimes_R M$ such that $\gamma \circ \psi$ and $\psi \circ \gamma$ are the identity homomorphisms. Given any element $\frac{m}{s} \in S^{-1}M$, let $\psi\big(\frac{m}{s}\big) = \frac{1_R}{s} \otimes_R m$. Observe that if $\frac{m}{s} = \frac{m'}{s'}$, then there exists an element $t \in S$ such that $s'tm = stm'$. Consequently, we have that

$$\frac{1_R}{s} \otimes_R m = \frac{s't}{ss't} \otimes_R m = \frac{1_R}{ss't} \otimes_R (s'tm) = \frac{1_R}{ss't} \otimes_R (stm') = \frac{st}{ss't} \otimes_R m' = \frac{1_R}{s'} \otimes_R m',$$

hence ψ is well-defined. By definition of the tensor product, ψ is R-linear, hence it is an R-module homomorphism. Clearly, we have that $\gamma \circ \psi$ is the identity of $S^{-1}M$. Conversely, we have that $\psi \circ \gamma$ is the identity on the pure tensors of $S^{-1}R \otimes_R M$, hence it is the identity on $S^{-1}R \otimes_R M$. One can easily verify that both γ and ψ are $S^{-1}R$-module homomorphisms, hence we obtain the following.

Proposition 4.27. *Let S be a multiplicatively closed subset of a commutative ring R. Let M be an R-module. We have that $S^{-1}M \cong S^{-1}R \otimes_R M$ as an R-module and as an $S^{-1}R$-module.*

Corollary 4.28. *Let S be a multiplicatively closed subset of a commutative ring R. The R-module $S^{-1}R$ is flat, i.e., the tensor product $S^{-1}R \otimes_R -$ preserves exact sequences.*

Proof. This follows as a direct consequence of Propositions 4.26 and 4.27. □

Corollary 4.29. *Let S be a multiplicatively closed subset of a commutative ring R. Localization commutes with direct sums, i.e., for any (possibly infinite) index set I and any family of R-modules $(M_i)_{i \in I}$, we have that $S^{-1}(\bigoplus_{i \in I} M_i) \cong \bigoplus_{i \in I}(S^{-1}M_i)$.*

Proof. By Proposition 4.27, we have that $S^{-1}M_i \cong S^{-1}R \otimes_R M_i$ for each index i. Consequently, the desired result follows immediately from Proposition 2.2. □

Our next proposition lists many of the desirable properties of localization.

Corollary 4.30. *Let S be a multiplicatively closed subset of a commutative ring R. Let $N \subseteq M$ be R-modules. The following properties hold.*

(1.) *Localization commutes with quotients, i.e., $S^{-1}(M/N) \cong (S^{-1}M)/(S^{-1}N)$.*

(2.) *Localization preserves the property of being finitely generated.*

(3.) *Localization preserves the property of being Noetherian.*

(4.) *Localization preserves the property of being free (or projective).*

(5.) *Localization preserves integral extensions.*

(6.) *Localization commutes with the integral closure, i.e., $S^{-1}\overline{R} = \overline{S^{-1}R}$.*

(7.) *Localization preserves reducedness.*

Proof. (1.) Use Corollary 4.26 on the short exact sequence $0 \to N \to M \to M/N \to 0$; then, apply the First Isomorphism Theorem to obtain the desired result.

(2.) Consider a finitely generated R-module $M = R\langle x_1, \dots, x_n \rangle$. Every element $m \in M$ can be written as $m = r_1 x_1 + \cdots + r_n x_n$ for some elements $r_1, \dots, r_n \in R$. Consequently, every element $\frac{m}{s} \in S^{-1}M$ can be written as $\frac{m}{s} = \frac{r_1}{s}\frac{x_1}{1_R} + \cdots + \frac{r_n}{s}\frac{x_n}{1_R}$ so that $S^{-1}M = S^{-1}R\left\langle \frac{x_1}{1_R}, \dots, \frac{x_n}{1_R} \right\rangle$.

(3.) If M is Noetherian, then every R-submodule of M is finitely generated. One can verify that every $S^{-1}R$-submodule of $S^{-1}M$ is of the form $S^{-1}N$ for some R-submodule N of M. By part (2.) above, every $S^{-1}R$-submodule of $S^{-1}M$ is finitely generated, hence $S^{-1}M$ is Noetherian.

(4.) If F is a free R-module, then it is a direct sum of copies of R, hence $S^{-1}F$ is a direct sum of copies of $S^{-1}R$ by Proposition 4.29. Likewise, if P is a projective R-module, then it is a direct summand of a free R-module, and $S^{-1}P$ is a direct summand of a free $S^{-1}R$-module.

(5.) Let $R \subseteq T$ be an integral extension. By Corollary 4.26, the inclusion $S^{-1}R \subseteq S^{-1}T$ is a ring extension. Given any element $\frac{x}{s}$ of $S^{-1}T$, there exist elements $a_1, \dots, a_{n-1}, a_n \in R$ such that

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0_R.$$

By assumption that S is multiplicatively closed, the elements $s, \dots, s^{n-1}, s^n$ belong to S, hence

$$\left(\frac{x}{s}\right)^n + \frac{a_1}{s}\left(\frac{x}{s}\right)^{n-1} + \cdots + \frac{a_{n-1}}{s^{n-1}}\left(\frac{x}{s}\right) + \frac{a_n}{s^n} = \frac{0_R}{s^n}$$

demonstrates that $\frac{x}{s}$ is integral over $S^{-1}R$. We conclude that $S^{-1}T$ is integral over $S^{-1}R$.

(6.) By part (4.) above, we find that $S^{-1}\overline{R} \subseteq \overline{S^{-1}R}$. Conversely, consider an equation

$$\left(\frac{x}{u}\right)^n + \frac{a_1}{v_1}\left(\frac{x}{u}\right)^{n-1} + \cdots + \frac{a_{n-1}}{v_{n-1}}\left(\frac{x}{u}\right) + \frac{a_n}{v_n} = 0$$

of integral dependence over $S^{-1}R$. Observe that if $d = uv_1 \cdots v_{n-1}v_n$, then by multiplying the previous displayed equation by $d^n/1_R$ and setting $c_i = a_i(uv_1 \cdots v_{n-1}v_n)^i/v_i$, we find that

$$\frac{(v_1 \cdots v_{n-1}v_n x)^n + c_1(v_1 \cdots v_{n-1}v_n x)^{n-1} + \cdots + c_{n-1}(v_1 \cdots v_{n-1}v_n x) + c_n}{1_R} = 0.$$

Consequently, there exists an element $t \in S$ such that t annihilates the element of R in the numerator. By multiplying this element by t^n, we obtain an expression of integral dependence

$$(tv_1 \cdots v_{n-1}v_n x)^n + tc_1(tv_1 \cdots v_{n-1}v_n x)^{n-1} + \cdots + t^{n-1}c_{n-1}(tv_1 \cdots v_{n-1}v_n x) + t^n c_n = 0_R.$$

We conclude that $tv_1 \cdots v_{n-1}v_n x$ belongs to $\overline{R}$. Considering that each of the elements $t, v_1, \ldots, v_{n-1}$ lies in S, the element $\frac{x}{u} = \frac{tv_1 \cdots v_{n-1}v_n x}{tv_1 \cdots v_{n-1}v_n u}$ belongs to $S^{-1}\overline{R}$ and $\overline{S^{-1}R} \subseteq S^{-1}\overline{R}$.

(7.) We prove the contrapositive, i.e., we show that if $S^{-1}R$ is not reduced, then R is not reduced. Consider a nonzero nilpotent element $\frac{r}{s} \in S^{-1}R$ such that $\frac{r^n}{s^n} = \left(\frac{r}{s}\right)^n = 0$. By definition of $S^{-1}R$, there exists a nonzero element $t \in S$ such that $r^n t = 0_R$ and $(rt)^n = 0_R$, hence the element $rt \in R$ is nilpotent; it must be nonzero because $\frac{r}{s}$ is nonzero by assumption. □

Localization admits even more useful properties that we omit for the sake of brevity. We direct the reader to the end of [Rot09, Section 4.7] for further information (cf. pages 198 to 202).

4.3 Further Properties of Hom and Ext

We begin with the observation that Hom commutes with direct products.

Proposition 4.31. *Let R be a commutative ring. For any (possibly infinite) index set I and any families of R-modules $(M_i)_{i\in I}$ and $(N_i)_{i\in I}$, we have that* $\operatorname{Hom}_R\left(\bigoplus_{i\in I} M_i, N\right) \cong \prod_{i\in I} \operatorname{Hom}_R(M_i, N)$ *and* $\operatorname{Hom}_R\left(M, \prod_{i\in I} N_i\right) \cong \prod_{i\in I} \operatorname{Hom}_R(M, N_i)$*. Particularly, it holds that* $\operatorname{Hom}_R(R^n, N) \cong N^n$.

Proof. Let $\sigma_i : M_i \to \bigoplus_{i\in I} M_i$ denote the ith component inclusion map, i.e., the R-module homomorphism that sends an element $m \in M_i$ to the I-tuple of elements with m in the ith component and zeros elsewhere. Given any R-module homomorphism $\varphi : \bigoplus_{i\in I} M_i \to N$, the I-tuple of composite maps $(\varphi \circ \sigma_i)_{i\in I}$ yields an element of $\prod_{i\in I} \operatorname{Hom}_R(M_i, N)$. Consider the R-module homomorphism $\psi : \operatorname{Hom}_R(\bigoplus_{i\in I} M_i, N) \to \prod_{i\in I} \operatorname{Hom}_R(M_i, N)$ defined by $\psi(\varphi) = (\varphi \circ \sigma_i)_{i\in I}$. Observe that φ belongs to $\ker\psi$ if and only if $\varphi \circ \sigma_i$ is the zero homomorphism for each index $i \in I$ if and only if φ is the zero homomorphism on $\bigoplus_{i\in I} M_i$, hence ψ is injective. Given any element γ of $\prod_{i\in I} \operatorname{Hom}_R(M_i, N)$, we may write $\gamma = (\gamma_i)_{i\in I}$ for some R-module homomorphisms $\gamma_i : M_i \to N$. Consider the R-module homomorphism $\varphi : \bigoplus_{i\in I} M_i \to N$ that sends $(m_i)_{i\in I} \mapsto \sum_{i\in I} \gamma_i(m_i)$. By definition, an element of $\bigoplus_{i\in I} M_i$ has only finitely many nonzero components, so $\sum_{i\in I} \gamma_i(m_i)$ is a well-defined element of N. Observe that for each index $i \in I$, we have that $\gamma_i(m_i) = \varphi \circ \sigma_i(m_i)$, hence we conclude that $\gamma = (\gamma_i)_{i\in I} = (\varphi \circ \sigma_i)_{i\in I}$ so that ψ is surjective.

Let $\pi_i : \prod_{i\in I} N_i \to N_i$ denote ith component projection map, i.e., the R-module homomorphism that sends an element $(n_i)_{i\in I} \in \prod_{i\in I} N_i$ to the element $n_i \in N_i$. One can show that the R-module homomorphism $\tau : \operatorname{Hom}_R(M, \prod_{i\in I} N_i) \to \prod_{i\in I} \operatorname{Hom}_R(M, N_i)$ defined by $\tau(\varphi) = (\pi_i \circ \varphi)_{i\in I}$ is bijective in an analogous manner to the previous paragraph. We note that the last statement of the proposition follows by Proposition 1.1 applied to $\operatorname{Hom}_R(R^n, N) \cong \operatorname{Hom}_R(R, N)^n$. □

Corollary 4.32. *Let R be a commutative ring. Let M and N be R-modules. If M is finitely generated and N is Noetherian, then $\operatorname{Hom}_R(M, N)$ is finitely generated as an R-module. Particularly, if R is Noetherian and M and N are finitely generated, then $\operatorname{Hom}_R(M, N)$ is finitely generated.*

Proof. By assumption, we have that $M = R\langle x_1, \dots, x_n\rangle$ for some elements $x_1, \dots, x_n$. Consequently, there exists a short exact sequence of R-modules $0 \to K \to R^n \to M \to 0$; the induced sequence of R-modules $0 \to \operatorname{Hom}_R(M, N) \to \operatorname{Hom}_R(R^n, N) \to \operatorname{Hom}_R(K, N)$ is exact by Proposition 1.3. Put another way, there is an injective R-module homomorphism $\operatorname{Hom}_R(M, N) \to \operatorname{Hom}_R(R^n, N)$, so we may identity $\operatorname{Hom}_R(M, N)$ as an R-submodule of $\operatorname{Hom}_R(R^n, N)$. By Proposition 4.31, the latter R-module is isomorphic to N^n; it is Noetherian by hypothesis, hence we conclude that $\operatorname{Hom}_R(M, N)$ is finitely generated. We note that the last statement holds because if R is Noetherian, then an R-module is Noetherian if and only if it is finitely generated. □

4.4 Further Properties of Tensor Products and Tor

Our next proposition provides an analog of Corollary 4.32 for the tensor product.

Proposition 4.33. *Let R be a commutative ring. If M and N are finitely generated R-modules, then the tensor product $M \otimes_R N$ is finitely generated as an R-module.*

Proof. Every element of $M \otimes_R N$ can be written as $\sum_{i=1}^{k} r_i(m_i \otimes_R n_i)$ for some integer $k \geq 0$, some elements $r_1, \dots, r_k \in R$, and some distinct elements $m_1, \dots, m_k \in M$ and $n_1, \dots, n_k \in N$. Each of the elements m_i can be written in terms of the generators of M, and each of the elements n_i can be written in terms of the generators of N. Consequently, if $M = R\langle x_1, \dots, x_r \rangle$ and $N = R\langle y_1, \dots, y_s \rangle$, the bilinearity of the map τ implies that $M \otimes_R N = R\langle x_i \otimes_R y_j \mid 1 \leq i \leq r \text{ and } 1 \leq j \leq s \rangle$. □

Remarkably, one can characterize flat R-modules in the following manner.

Proposition 4.34. *Let R be a commutative ring. The following properties are equivalent.*

(i.) *L is a flat R-module.*

(ii.) *If $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} L \to 0$ is a short exact sequence of R-modules, then the induced sequence $0 \to M \otimes_R A \xrightarrow{\text{id}_M \otimes_R \alpha} M \otimes_R B \xrightarrow{\text{id}_M \otimes_R \beta} M \otimes_R L \to 0$ is exact for any R-module M.*

Proof. Given any R-module M, consider the free R-module F indexed by M and the canonical surjection $\pi : F \to M$ with kernel K. Observe that there is a short exact sequence of R-modules $0 \to K \xrightarrow{i} F \xrightarrow{\pi} M \to 0$ such that the R-module homomorphism $i : K \to F$ is the inclusion map. By applying the right-exact functors $K \otimes_R -$, $F \otimes_R -$, and $M \otimes_R -$ to any short exact sequence of R-modules $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} L \to 0$, we obtain the following diagram of R-modules.

$$
\begin{array}{ccccccccc}
 & & K \otimes_R A & \xrightarrow{\text{id}_K \otimes_R \alpha} & K \otimes_R B & \xrightarrow{\text{id}_K \otimes_R \beta} & K \otimes_R L & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle i \otimes_R \text{id}_A} & & \downarrow{\scriptstyle i \otimes_R \text{id}_B} & & \downarrow{\scriptstyle i \otimes_R \text{id}_L} & & \\
0 & \longrightarrow & F \otimes_R A & \xrightarrow{\text{id}_F \otimes_R \alpha} & F \otimes_R B & \xrightarrow{\text{id}_F \otimes_R \beta} & F \otimes_R L & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \pi \otimes_R \text{id}_A} & & \downarrow{\scriptstyle \pi \otimes_R \text{id}_B} & & \downarrow{\scriptstyle \pi \otimes_R \text{id}_L} & & \\
 & & M \otimes_R A & \xrightarrow{\text{id}_M \otimes_R \alpha} & M \otimes_R B & \xrightarrow{\text{id}_M \otimes_R \beta} & M \otimes_R L & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}
$$

One can readily verify that the diagram commutes on the pure tensors of each tensor product, hence the diagram commutes. Even more, the columns and rows of the diagram are exact by Proposition

2.6 and Corollary 2.9. By the Snake Lemma, we obtain a short exact sequence of R-modules

$$\ker(i \otimes_R \mathrm{id}_A) \to \ker(i \otimes_R \mathrm{id}_B) \to \ker(i \otimes_R \mathrm{id}_L) \to M \otimes_R A \to M \otimes_R B \to M \otimes_R L \to 0.$$

By Proposition 2.7, we conclude that if L is flat, then $i \otimes_R \mathrm{id}_L$ is injective so that $\ker(i \otimes_R \mathrm{id}_L) = 0$ and $0 \to M \otimes_R A \xrightarrow{\mathrm{id}_M \otimes_R \alpha} M \otimes_R B \xrightarrow{\mathrm{id}_M \otimes_R \beta} M \otimes_R L \to 0$ is exact.

We obtain the converse as a corollary of a later proposition. Explicitly, if condition (ii.) holds, then $\mathrm{Tor}_1^R(M, L) = 0$ for all R-modules M so that L is a flat R-module. $\square$

4.5 Commutative Diagrams

One of the most useful facts in homological algebra is the following.

Lemma 4.35 (Snake Lemma)**.** *Consider the following commutative diagram of R-modules.*

$$\begin{array}{ccccccc} & & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & \longrightarrow & 0 \\ & & \downarrow{\varphi} & & \downarrow{\psi} & & \downarrow{\gamma} & & \\ 0 & \longrightarrow & D & \xrightarrow{\delta} & E & \xrightarrow{\varepsilon} & F & & \end{array}$$

If the rows of this diagram are exact, then there exists an exact sequence of R-modules

$$\ker \varphi \xrightarrow{\alpha'} \ker \psi \xrightarrow{\beta'} \ker \gamma \xrightarrow{\chi} \frac{D}{\operatorname{img} \varphi} \xrightarrow{\delta'} \frac{E}{\operatorname{img} \psi} \xrightarrow{\varepsilon'} \frac{F}{\operatorname{img} \gamma}.$$

Even more, if α is injective and ε is surjective, then α' is injective and ε' is surjective.

Proof. One can (and should) prove the Snake Lemma (at least once) via the method of "diagram chasing." We leave the details to the enjoyment of the reader (cf. [Gat13, Lemma 4.7]). $\square$

Using the Snake Lemma, one can deduce the following useful fact.

Corollary 4.36 (Short Five Lemma)**.** *Consider the following commutative diagram of R-modules.*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & \longrightarrow & 0 \\ & & \downarrow{\varphi} & & \downarrow{\psi} & & \downarrow{\gamma} & & \\ 0 & \longrightarrow & D & \xrightarrow{\delta} & E & \xrightarrow{\varepsilon} & F & \longrightarrow & 0 \end{array}$$

If the rows of this diagram are exact, then ψ is injective (or surjective) if φ and γ are injective (or surjective). Even more, if any two of φ, ψ, and γ are isomorphisms, the third is an isomorphism.

Proof. By the Snake Lemma, there exists an exact sequence of R-modules

$$\ker\varphi \to \ker\psi \to \ker\gamma \to \frac{D}{\operatorname{img}\varphi} \to \frac{E}{\operatorname{img}\psi} \to \frac{F}{\operatorname{img}\gamma}.$$

If φ and γ are injective, then $\ker\varphi = 0$ and $\ker\gamma = 0$ imply that $\ker\psi = 0$. If φ and γ are surjective, then $D = \operatorname{img}\varphi$ and $F = \operatorname{img}\gamma$ imply that $E/\operatorname{img}\psi = 0$, i.e., $E = \operatorname{img}\psi$. If any two of φ, ψ, and γ are isomorphisms, then the kernel and cokernel of the third map will be trapped between zeros in the exact sequence; this forces both of these modules to be zero so the map is an isomorphism. □

Using the Short Five Lemma, we obtain the Splitting Lemma (cf. [Gat13, Corollary 4.14]); however, it is possible to provide a proof by elementary means as follows.

Lemma 4.37 (Splitting Lemma)**.** *A short exact sequence of R-modules* $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ **splits** *if any of the following equivalent conditions holds.*

(i.) *There exists an R-module homomorphism* $\varphi : B \to A$ *such that* $\mathrm{id}_A = \varphi \circ \alpha$.

(ii.) *There exists an R-module homomorphism* $\gamma : C \to B$ *such that* $\mathrm{id}_C = \beta \circ \gamma$.

(iii.) *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* $A \oplus C \to C$.

Proof. By the proofs of Propositions 1.4 and 1.6, it suffices to prove that (iii.) $\implies$ (i.) and (iii.) $\implies$ (ii.). Observe that if $\psi \circ \alpha$ is the first component inclusion map $A \to A \oplus C$, then the first component projection map $\pi_1 : A \oplus C \to A$ satisfies that $\mathrm{id}_A = \pi_1 \circ \psi \circ \alpha$. Likewise, if $\beta \circ \psi^{-1}$ is the second component projection map, then the second component inclusion map $\sigma_2 : C \to A \oplus C$ satisfies $\mathrm{id}_C = \beta \circ \psi^{-1} \circ \sigma_2$. We conclude that (iii.) $\implies$ (i.) and (iii.) $\implies$ (i.). □

One can also prove a general version of the Short Five Lemma from which the above follows.

Lemma 4.38 (Five Lemma)**.** *Consider the following commutative diagram of R-modules.*

$$\begin{array}{ccccccccc}
A_1 & \xrightarrow{\alpha_1} & A_2 & \xrightarrow{\alpha_2} & A_3 & \xrightarrow{\alpha_3} & A_4 & \xrightarrow{\alpha_4} & A_5 \\
\downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_3} & & \downarrow{\scriptstyle \varphi_4} & & \downarrow{\scriptstyle \varphi_5} \\
B_1 & \xrightarrow{\beta_1} & B_2 & \xrightarrow{\beta_2} & B_3 & \xrightarrow{\beta_3} & B_4 & \xrightarrow{\beta_4} & B_5
\end{array}$$

If the rows of this diagram are exact, then the following statements hold.

1.) *If φ_1 is surjective and φ_2 and φ_4 are injective, then φ_3 is injective.*

2.) *If φ_5 is injective and φ_2 and φ_4 are surjective, then φ_3 is surjective.*

Particularly, if φ_1, φ_2, φ_4, and φ_5 are isomorphisms, then φ_3 is an isomorphism.