Modules

December 31, 2020

Contents

Part I
Introduction to Modules

In this document, we will study the theory of modules over a commutative ring[1].

1 Basic Definitions

1.1 Definition of an R-Module

Definition 1.1. Let R be a commutative ring[2]. An R-**module** M consists of an abelian group on which R acts by additive maps: there is a scalar multiplication function $R \times M \to M$ denoted by $(a, m) \mapsto am$ such that for all $u, v \in M$, $a, b \in R$ we have

1. $1u = u$ and $a(bu) = (ab)u$.
2. $a(u + v) = au + av$ and $(a + b)u = au + bu$.

Throughout these notes, we often write "let M be an R-module" or "let I be an ideal in R" without specifying what R is. In either case, it is understood that R is a commutative ring. We will also say "let M be a module over R" instead of "let M be an R-module". Sometimes the base ring R isn't important to know and we will refer to M simply as a module rather than an R-module.

1.1.1 Consistency in Notation

When learning Mathematics, it's a good practice to write things down in an organized way. Doing so will help organize ideas and concepts in your mind, making it easier to work with them. For instance, we will typically use the capital letters R, S or A, B to denote rings. Similarly, we will typically use the capital letters M, N to denote modules. If M is an R-module, then we will typically use lower case letters a, b, c to denote elements of R and use lower case letters u, v, w to denote elements of M. Many authors use the lower case letters r, s to denote elements of R and use the lower case letter m, n to denote elements of M. This is completely fine! Sometimes we will even use the lower case letters r, s to denote elements of R. In fact, if we are dealing with a ring R together with a ring A, then we will try to use the lower case letters r, s to denote elements of R and the lower case letters a, b to denote elements of A. However we will try to avoid using the lower case letters m, n to denote elements of M. This is because we try to use lower case letters like i, j, k, l, m, n as indices. For instance, we may write an element in M as

$$\sum_{i=1}^{m} a_i u_i = a_1 u_1 + \cdots + a_m u_m. \tag{1}$$

where the a_i are elements of R and the u_i are elements of M. The lower case m here is simply the number of terms in (1).

Throughout this document, the reader will find many more examples of consistency in notation as in the case described above. Keep in mind however that this rule is not set in stone; we may violate it. The point however is that if you try to be as consistent as possible with your notation, it will make learning Mathematics much easier (and more fun!).

1.1.2 Examples of R-Modules

Let R be a ring and let X be a nonempty set. At the moment, the ring R and the set X have nothing to do with each other, however we'd like to turn X into an R-module somehow. How can we do this? Well, the first step would be to give X the **structure of an abelian group**! In particular, we need define an addition map $+\colon X \times X \to X$ such that the pair $(X, +)$ forms an abelian group. In this case, we say addition $+$ **gives** X **the structure of an abelian group**. Once X is given the structure of an abelian group, the next thing we'd need to do is to define a scalar multiplication map $\cdot\colon R \times X \to X$ such that the triple $(X, +, \cdot)$ forms an R-module. In this case, we say addition $+$ and multiplication $\cdot$ **gives** X **the structure of an** R**-module**. We often use this language when describing modules.

[1] There is a theory of modules over a non-commutative ring, but we leave that topic to another document.

[2] For us, all rings have an identity element by definition. Note that some authors define rings to be associative $\mathbb{Z}$-algebras which do not necessarily have an identity element.

Example 1.1. Let R be a ring and let $n \geq 1$. Then the set $R^n = \{(a_1, \dots, a_n) \mid a_i \in R\}$ can be given the structure of an R-module as follows: addition and scalar multiplication are defined by

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) := (a_1 + b_1, \dots, a_n + b_n) \quad \text{and} \quad a(a_1, \dots, a_n) := (aa_1, \dots, aa_n)$$

$a \in R$ and $(a_1, \dots, a_n), (b_1, \dots, b_n) \in R^n$. Check that addition and scalar multiplication defined in this way really does give R^n an R-module structure.

Example 1.2. One of the reasons why we study R-modules is because they help us obtain information about the ring R itself. For instance, if R is a principal ideal domain, then it turns out that every finitely generated R-module is isomorphic to a direct sum of a free module plus a torsion module. The proof of this fact uses the in an essential way the fact that R is a principal ideal domain.

1.2 Definition of an R-Linear Map

Definition 1.2. Let M and N be R-modules. A map $\varphi \colon M \to N$ is called an R**-linear map** if for all a, b in R and u, v in M, we have

$$\varphi(au + bv) = a\varphi(u) + b\varphi(v).$$

An R-linear map $\varphi \colon M \to N$ is also called an R**-module homomorphism**. A bijective R-module homomorphism is called an R**-module isomorphism**. If $\varphi \colon M \to N$ is an R-module isomorphism, then we say M is **isomorphic to** N, and we denote this by $M \cong N$. The collection of all R-modules and R-linear maps forms a category[3] which we will denote by $\mathbf{Mod}_R$.

Remark. Note that $\varphi(0) = \varphi(0 + 0) = \varphi(0) + \varphi(0)$ implies $\varphi(0) = 0$.

When the base ring R is understood from context, we will sometimes drop "R" in "R-linear map" and simply write "linear map". We also write "let $\varphi \colon M \to N$ be an R-linear map" without specifying what R, M, and N is. In thise case, it is understood that R is a commutative ring and that M and N are R-modules.

1.3 Submodules, Kernels, and Quotient Modules

Definition 1.3. Let $\varphi \colon M \to N$ be an R-linear map.

1. The **kernel** of φ, denoted $\ker \varphi$, is defined to be the set

$$\ker \varphi := \{u \in M \mid \varphi(u) = 0\}.$$

   In a moment, we will show that $\ker \varphi$ can be given the structure of an R-module.

2. The **image** of φ, denoted $\operatorname{im} \varphi$, is defined to be the set

$$\operatorname{im} \varphi := \{\varphi(u) \in N \mid u \in M\}.$$

   In a moment, we will show that $\operatorname{im} \varphi$ can be given the structure of an an R-module.

3. If M is a subset of N and φ is the inclusion map, then we say M is an R**-submodule** of N. In this case, we also define the **quotient** of N with respect to M, denoted N/M, to be the set

$$N/M = \{v + M \mid v \in N\}.$$

   That is, N/M is the set of equivalence classes of elements of N, where $v_1, v_2 \in N$ are equivalent if $v_1 - v_2 \in M$. An equivalent class in N/M is denoted by $v + M$ or more simply by $\overline{v}$. In this case, we call v a **representative** of the equivalence class $\overline{v}$. From basic group theory, we know that N/M has the structure of an abelian group, where addition is defined by $\overline{v_1} + \overline{v_2} = \overline{v_1 + v_2}$ for all $\overline{v_1}, \overline{v_2} \in N/M$. In fact, N/M has the structure of an R-module, where scalar multiplication is defined by $a\overline{v} = \overline{av}$ for all $a \in R$ and $\overline{v} \in N/M$. One checks that this is well-defined and together with addition defined above does indeed give N/M the structure of an R-module.

4. The **cokernel** of φ, denote $\operatorname{coker} \varphi$, is defined to be the R-module

$$\operatorname{coker} \varphi = N/\operatorname{im} \varphi. \tag{2}$$

   In a moment, we will show that $\operatorname{im} \varphi$ can be given the structure of an an R-submodule of N, so that definition (2) makes sense.

[3] See the Appendix for an introduction to Category Theory.

Remark. Let N be an R-module and let M be a subset of N. Then M is an R-submodule of N if and only if M is nonempty and $au + bv \in M$ for all $a, b \in R$ and $u, v \in M$. Equivalently, M is an R-submodule of N if and only if M is nonempty $au + v \in M$ for all $a \in R$ and $u, v \in M$. This is sometimes called the **submodule criterion test**. If M satisfies the submodule criterion test, then it is easy to check that we can give it the structure of an R-module by using the R-module operations from N.

Proposition 1.1. *Let $\varphi\colon M \to N$ be an R-linear map. Then* $\ker \varphi$ *is a submodule of M and* $\operatorname{im} \varphi$ *is a submodule of N.*

Proof. Let us first show that $\ker \varphi$ is a submodule of M. Observe that $\ker \varphi$ is nonempty since $0 \in \ker \varphi$. Let $a \in R$ and let $u, v \in \ker \varphi$. Then we have

$$\begin{aligned} \varphi(au + v) &= a\varphi(u) + \varphi(v) \\ &= a \cdot 0 + 0 \\ &= 0 + 0 \\ &= 0. \end{aligned}$$

It follows that $au + v \in \ker \varphi$. Thus $\ker \varphi$ is a submodule of M.

Now we will show that $\operatorname{im} \varphi$ is a submodule of N. Observe that $\operatorname{im} \varphi$ is nonempty since $\varphi(0) \in \operatorname{im} \varphi$. Let $a \in R$ and let $\varphi(u), \varphi(v) \in \operatorname{im} \varphi$. Then we have

$$\begin{aligned} a\varphi(u) + \varphi(v) &= \varphi(au) + \varphi(v) \\ &= \varphi(au + v). \end{aligned}$$

It follows that $a\varphi(u) + \varphi(v) \in \operatorname{im} \varphi$. Thus $\operatorname{im} \varphi$ is a submodule of N. □

1.4 Base Change

Throughout this subsection, let $f\colon R \to S$ be a ring homomorphism.

1.4.1 Restriction of scalars functor

If N is an S-module, then we can restrict it to an R-module N_R where N_R has the same underlying abelian group structure as N but with scalar multiplication given by

$$a \cdot v = f(a)v$$

for all $a \in R$ and $v \in N$. This is called **restriction of scalars** since in the case where $R \subseteq S$ we are just restricting the S-action to an R-action. If $\psi\colon N \to N'$ is an S-module linear map, then we define an R-module linear map $\psi_R\colon N_R \to N'_R$ by

$$\psi_R(v) = \psi(v)$$

for all $v \in N_R$. Let us check that ψ_R is indeed an R-linear map. We just need to check that ψ_R respects scalar multiplication since additivity is clear. Let $a \in R$ and let $v \in N_R$. Then

$$\begin{aligned} \psi_R(a \cdot v) &= \psi_R(f(a)v) \\ &= \psi(f(a)v) \\ &= f(a)\psi(v) \\ &= a \cdot \psi(v) \\ &= a \cdot \psi_R(v). \end{aligned}$$

It follows that ψ_R is an R-module linear map. It is easy to check that we obtain a functor

$$-_R\colon \mathbf{Mod}_S \to \mathbf{Mod}_R.$$

1.4.2 Extension of scalars functor

If M is an R-module, then we can extend it to an S-module $S \otimes_R M$ where scalar multiplication is defined by

$$a \cdot (b \otimes u) = ab \otimes u$$

for all $a, b \in S$ and $u \in M$. This is called **extension of scalars** since in the case where $R \subseteq S$ we are just extending the R-action to an S-action. If $\varphi\colon M \to M'$ is an R-module linear map, then we define an S-module linear map $1 \otimes \varphi\colon S \otimes_R M \to S \otimes_R M$ on elementary tensors $a \otimes u \in S \otimes_R M$ by

$$(1 \otimes \varphi)(a \otimes u) = a \otimes \varphi(u),$$

and then extend this linearly everywhere else. We just need to check that $1 \otimes \varphi$ respects scalar multiplication since additivity is clear. Let $a \in S$ and let $b \otimes u$ be an elementary tensor in $S \otimes_R M$. Then

$$\begin{aligned}(1 \otimes \varphi)(a \cdot (b \otimes u)) &= (1 \otimes \varphi)(ab \otimes u)\\ &= ab \otimes \varphi(u)\\ &= a \cdot (b \otimes \varphi(u))\\ &= a \cdot ((1 \otimes \varphi)(b \otimes u)).\end{aligned}$$

It follows that $1 \otimes \varphi$ is an R-module linear map. It is easy to check that we obtain a functor

$$S \otimes_R - \colon \mathbf{Mod}_R \to \mathbf{Mod}_S.$$

1.4.3 Restricting scalars and extending scalars form an adjoint pair

Proposition 1.2. *The functors $-_R \colon \mathbf{Mod}_S \to \mathbf{Mod}_R$ and $- \otimes_R S \colon \mathbf{Mod}_R \mapsto \mathbf{Mod}_S$ are adjoint functors. In a formula*

$$\mathrm{Hom}_R(M, N_R) \cong \mathrm{Hom}_S(M \otimes_R S, N)$$

for all R-modules M and for all S

Example 1.3. Let I be an ideal in R. Let us calculate $\mathrm{Hom}_R(R/I, R/I)$. We have

$$\begin{aligned}\mathrm{Hom}_R(R/I, R/I) &\cong \mathrm{Hom}_{R/I}((R/I) \otimes_R (R/I), R/I)\\ &\cong \mathrm{Hom}_{R/I}(R/I, R/I)\\ &\cong R/I.\end{aligned}$$

1.4.4 Base Change

There is another type of R-module that can be viewed as an S-module. For simplicity, assume that $R \subset S$ is an extension of rings. Suppose M is an R-module and N is an S-module. Through restriction of scalars, we can view N as an R-module. Thus we can consider $\mathrm{Hom}_R(N, M)$. In fact, $\mathrm{Hom}_R(N, M)$ can be viewed as an S-module via the action

$$b \cdot \varphi(v) = \varphi(bv)$$

for all $b \in S$, $\varphi \in \mathrm{Hom}_R(N, M)$, and $v \in N$.

Theorem 1.1. *Let $R \subset S$ be a ring extension and let $\varphi \in \mathrm{Hom}_S(N, N')$ and let $\psi \in \mathrm{Hom}_R(M, M')$ where M, M' are R-modules and N, N' are S-modules. Then $\varphi^* \colon \mathrm{Hom}_R(N', M) \to \mathrm{Hom}_R(N, M)$ and $\psi_* \colon \mathrm{Hom}_R(N, M) \to \mathrm{Hom}_R(N, M')$ are S-module homomorphisms.*

1.4.5 Translated Modules

In this section, we want to discuss how to translate an A-module M by an element $x \in M$. Let $M^x := \{y + x \mid y \in M\}$. We define addition and scaling operations as follows. Suppose a is an element in A and, $y + x$ and $y' + x$ are two elements in M^x. Then

$$(y + x) \dot{+} (y' + x) = y + y' + x$$

$$a \cdot (y + x) = a \cdot y + x.$$

Addition $\dot{+}$ makes M^x into an abelian group with identity being x, and one can check that all of the conditions for M^x to be an A-module are satisfied.

We can generalize the above constrution as follows: Let $\varphi : M \to M^\varphi$ be an isomorphism from M to some set M^φ. We define addition and scaling operations as follows: Suppose $a \in A$ and $x, y \in M^\varphi$. Then we define

$$x \dot{+} y = \varphi\left(\varphi^{-1}(x) + \varphi^{-1}(y)\right)$$

$$a \cdot x = \varphi\left(a\varphi^{-1}(x)\right)$$

Addition $\dotplus$ makes M^{φ} into an abelian group with identity being $\varphi(0)$. For instance, we have associativity:

$$\begin{aligned}
(x \dotplus y) \dotplus z &= \varphi\left(\varphi^{-1}(x)+\varphi^{-1}(y)\right) \dotplus z \\
&= \varphi\left(\varphi^{-1}\left(\varphi\left(\varphi^{-1}(x)+\varphi^{-1}(y)\right)\right) \dotplus \varphi^{-1}(z)\right) \\
&= \varphi\left(\left(\varphi^{-1}(x)+\varphi^{-1}(y)\right) \dotplus \varphi^{-1}(z)\right) \\
&= \varphi\left(\varphi^{-1}(x)+\left(\varphi^{-1}(y) \dotplus \varphi^{-1}(z)\right)\right) \\
&= \varphi\left(\varphi^{-1}(x)+\varphi\left(\varphi^{-1}\left(\varphi^{-1}(y) \dotplus \varphi^{-1}(z)\right)\right)\right) \\
&= x \dotplus \varphi\left(\varphi^{-1}(y)+\varphi^{-1}(z)\right) \\
&= x \dotplus (y \dotplus z).
\end{aligned}$$

and we have commutativity:

$$\begin{aligned}
x \dotplus y &= \varphi\left(\varphi^{-1}(x)+\varphi^{-1}(y)\right) \\
&= \varphi\left(\varphi^{-1}(y)+\varphi^{-1}(x)\right) \\
&= y \dotplus x.
\end{aligned}$$

One can check that all of the conditions for M^{φ} to be an A-module are satisfied. For instance, suppose $a, b \in A$, and $x, y \in M^{\varphi}$, we have

$$\begin{aligned}
a \cdot (x \dotplus y) &= a \cdot \left(\varphi\left(\varphi^{-1}(x)+\varphi^{-1}(y)\right)\right) \\
&= \varphi\left(a\left(\varphi^{-1}\left(\varphi\left(\varphi^{-1}(x)+\varphi^{-1}(y)\right)\right)\right)\right) \\
&= \varphi\left(a\left(\varphi^{-1}(x)+\varphi^{-1}(y)\right)\right) \\
&= \varphi\left(a\varphi^{-1}(x)+a\varphi^{-1}(y)\right) \\
&= \varphi\left(\varphi^{-1}(a \cdot x)+\varphi^{-1}(a \cdot y)\right) \\
&= a \cdot x \dotplus a \cdot y.
\end{aligned}$$

and

$$\begin{aligned}
(a+b) \cdot x &= \varphi\left((a+b)\varphi^{-1}(x)\right) \\
&= \varphi\left(a\varphi^{-1}(x)+b\varphi^{-1}(x)\right) \\
&= \varphi\left(\varphi^{-1}(a \cdot x)+\varphi^{-1}(b \cdot x)\right) \\
&= a \cdot x \dotplus b \cdot x
\end{aligned}$$

and

$$\begin{aligned}
(ab) \cdot x &= \varphi\left(ab\varphi^{-1}(x)\right) \\
&= \varphi\left(a\varphi^{-1}\left(\varphi(b\varphi^{-1}(x))\right)\right) \\
&= a \cdot (\varphi(b\varphi^{-1}(x))) \\
&= a \cdot (b \cdot x)
\end{aligned}$$

The way we defined addition and A-scaling on M^{φ} makes φ an A-linear map. Indeed, we have

$$\begin{aligned}
\varphi(ax+by) &= \varphi(\varphi^{-1}(\varphi(ax))+\varphi^{-1}(\varphi(by))) \\
&= \varphi(ax) \dotplus \varphi(by) \\
&= \varphi(a\varphi^{-1}(\varphi(x))) \dotplus \varphi(b\varphi^{-1}(\varphi(y))) \\
&= a \cdot \varphi(x) \dotplus b \cdot \varphi(y)
\end{aligned}$$

for all $a, b \in A$ and $x, y \in M$.

Now suppose $M^{\varphi} = M$ and let φ be additive, that is, $\varphi(x+y) = \varphi(x) + \varphi(y)$ for all $x, y \in M$. Then $\dotplus$ is the same $+$ since φ^{-1} is additive and

$$\begin{aligned} x \dotplus y &= \varphi(\varphi^{-1}(x) + \varphi^{-1}(y)) \\ &= \varphi(\varphi^{-1}(x+y)) \\ &= x + y \end{aligned}$$

for all $x, y \in M$. On the other hand, we can still have a different scaling map, as long as φ is not A-linear.

2 Free Modules

2.0.1 Generating Sets

Definition 2.1. Let M be an R-module and let $\{u_\lambda\}_{\lambda \in \Lambda}$ be a collection of elements in M. We say $\{u_\lambda\}$ **generates** M if for all $u \in M$ there exists $u_{\lambda_1}, \dots u_{\lambda_n} \in \{u_\lambda\}$ and $a_{\lambda_1}, \dots, a_{\lambda_n} \in R$ such that

$$u = a_{\lambda_1} u_{\lambda_1} + a_{\lambda_2} u_{\lambda_2} + \cdots + a_{\lambda_n} u_{\lambda_n}.$$

If $\{u_\lambda\}$ generates M, then we say $\{u_\lambda\}$ is a **generating set** for M. We say M is **finitely-generated** if there exists a finite generating set for M.

2.0.2 Free Modules

Definition 2.2. Let M be an R-module and let $u_1, \dots, u_n \in M$. We say the set $\{u_1, \dots, u_n\}$ is a **basis for** M if the following conditions hold:

1. it generates M as an R-module: for each $u \in M$ there exists $a_1, \dots, a_n \in R$ such that
$$u = a_1 u_1 + \cdots + a_n u_n,$$
2. it is linearly independent: if $a_1, \dots, a_n \in R$ such that
$$a_1 u_1 + \cdots + a_n u_n = 0,$$
then $a_i = 0$ for all $1 \leq i \leq n$.

More generally, let $\{u_\lambda\}$ be a collection of elements in M indexed over some (possibly infinite) set Λ. We say the set $\{u_\lambda\}$ is a **basis for** M if

1. it generates M as an R-module: for each $u \in M$ there exists $u_{\lambda_1}, \dots, u_{\lambda_n} \in \{u_\lambda\}$ and $a_{\lambda_1}, \dots, a_{\lambda_n} \in R$ such that
$$u = a_{\lambda_1} u_{\lambda_1} + \cdots + a_{\lambda_n} u_{\lambda_n}.$$
2. every finite subset of $\{u_\lambda\}$ is linearly independent: if $a_{\lambda_1}, \dots, a_{\lambda_n} \in R$ such that
$$a_{\lambda_1} u_{\lambda_1} + \cdots + a_{\lambda_n} u_{\lambda_n} = 0,$$
then $a_{\lambda_i} = 0$ for all $1 \leq i \leq n$.

We say M is a **free R-module** if it has a basis.

Example 2.1. R^n is the **standard free R-module of rank** n. It has as basis the **standard basis elements** e_i where e_i is the vector with 1 in the ith entry and 0 everywhere else.

Example 2.2. If I is a nonzero ideal in R, then R/I is not a free R-module. Indeed, if r is a nonzero element in I, then for all $s \in R$, we have $r\overline{s} = \overline{rs} = 0$ in R/I. In other words, "**torsion**" makes linear independence fail for elements of R/I when taking coefficients from R.

2.0.3 Universal Mapping Property of Free R-Modules

Free modules are characterized by the following universal mapping property: Let F be a free R-module with basis $\{e_\lambda\}$ indexed over a set Λ. Then for all R-modules M and for all $\{u_\lambda\} \subseteq M$ there exists a unique R-module homomorphism $\varphi \colon F \to M$ such that $\varphi(e_\lambda) = u_\lambda$ for all $\lambda \in \Lambda$. In terms of diagrams, this is pictured as follows:

$$\begin{tikzcd}
\{e_\lambda\} \arrow[r, hook] \arrow[dr, "e_\lambda \mapsto u_\lambda"'] & F \arrow[d, dashed, "\exists!\varphi"] \\
 & M
\end{tikzcd}$$

Using the universal mapping property of free R-modules, let us prove the following theorem:

Theorem 2.1. *If F and G are finite rank free R-modules with basis $e_1, \dots, e_n$ and $f_1, \dots, f_n$ respectively, then $F \cong G$.*

Proof. By the universal mapping property of free R-modules there exists a unique R-module homomorphism $\varphi \colon F \to G$ such that $\varphi(e_i) = f_i$ for all $i = 1, \dots, n$. Similarly, there exists a unique R-module homomorphism $\psi \colon G \to F$ such that $\psi(f_i) = e_i$ for all $i = 1, \dots, n$. In particular, we see that $\psi \circ \varphi \colon F \to F$ satisfies $(\psi \circ \varphi)(e_i) = e_i$. But we also have $1(e_i) = e_i$ for all $i = 1, \dots, n$, where $1 \colon F \to F$ is the identity map. Therefore by uniqueness of the map in the universal mapping property of free R-modules, we must have $\psi \circ \varphi = 1$. A similar argument shows that $\varphi \circ \psi = 1$. □

Corollary. *Let F be a free R-module with basis $e_1, \dots, e_n \in F$. Then $F \cong R^n$.*

Remark. Note that you can prove Theorem (2.1) without the universal mapping property of free R-modules, but the point is that you'd have to show well-definedness, linearity, etc... of the maps constructed. The point is that all of this is built into the universal mapping property of free R-modules.

2.0.4 Representing R-module Homomorphisms By Matrices

Let F be a R-module with basis $\beta = \{\beta_1, \dots, \beta_m\}$ and let G be a free R-module with basis $\gamma = \{\gamma_1, \dots, \gamma_n\}$. If $v \in F$, then for each $1 \leq i \leq m$, there exists unique $a_i \in R$ such that

$$v = \sum_{i=1}^{m} a_i \beta_i.$$

Since the a_i are uniquely determined, we are justified in making the following definition:

Definition 2.3. The **column representation of v with respect to the basis** β, denoted $[v]_\beta$, is defined by

$$[v]_\beta := \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix}.$$

Proposition 2.1. *Let $[\cdot]_\beta \colon V \to R^m$ be given by*

$$[\cdot]_\beta(v) = [v]_\beta$$

for all $v \in V$. Then $[\cdot]_\beta$ is an isomorphism.

Proof. We first show that $[\cdot]_\beta$ is R-linear. Let $v_1, v_2 \in V$ and $c_1, c_2 \in R$. Then for each $1 \leq i \leq m$, there exists unique $a_{i1}, a_{i2} \in R$ such that

$$v_1 = \sum_{i=1}^{m} a_{i1} \beta_i \quad \text{and} \quad v_2 = \sum_{i=1}^{m} a_{i2} \beta_i.$$

Therefore we have

$$\begin{aligned} a_1 v_1 + a_2 v_2 &= a_1 \sum_{i=1}^{m} a_{i1} \beta_i + a_2 \sum_{i=1}^{m} a_{i2} \beta_i \\ &= \sum_{i=1}^{m} (a_1 a_{i1} + a_2 a_{i2}) \beta_i. \end{aligned}$$

This implies

$$\begin{aligned}
[a_1v_1 + a_2v_2]_\beta &= \begin{pmatrix} a_1a_{11} + a_2a_{12} \\ \vdots \\ a_1a_{m1} + a_2a_{m2} \end{pmatrix} \\
&= a_1 \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix} + a_2 \begin{pmatrix} a_{12} \\ \vdots \\ a_{m2} \end{pmatrix} \\
&= a_1[v_1]_\beta + a_2[v_2]_\beta.
\end{aligned}$$

Therefore $[\cdot]_\beta$ is linear. To see that $[\cdot]_\beta$ is an isomorphism, note that $[\beta_i] = e_i$, where e_i is the column vector in K^n whose i-th entry is 1 and whose entry everywhere else is 0. Thus, $[\cdot]_\beta$ restricts to a bijection on basis sets

$$[\cdot]_\beta \colon \{\beta_1, \ldots, \beta_m\} \to \{e_1, \ldots, e_n\},$$

and so it must be an isomorphism. □

2.0.5 Matrix Representation of a Linear Map

Let φ be an R-linear map from F to G. Then for each $1 \leq i \leq m$ and $1 \leq j \leq n$, there exists unique elements $a_{ji} \in R$ such that

$$\varphi(\beta_i) = \sum_{j=1}^{n} a_{ji}\gamma_j \tag{3}$$

for all $1 \leq i \leq m$. Since the a_{ji} are uniquely determined, we are justified in making the following definition:

Definition 2.4. The **matrix representation of φ with respect to the bases β and γ**, denoted $[\varphi]_\beta^\gamma$, is defined to be the $n \times m$ matrix

$$[\varphi]_\beta^\gamma := \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix}.$$

Proposition 2.2. *Let φ be a linear map from F to G. Then*

$$[\varphi]_\beta^\gamma [v]_\beta = [\varphi(v)]_\gamma$$

for all $v \in F$.

Remark. In terms of diagrams, this proposition says that the following diagram is commutative

$$\begin{tikzcd}
R^m \arrow[r, "{[\varphi]_\beta^\gamma}"] & R^n \\
F \arrow[u, "{[\cdot]_\beta}"] \arrow[r, "\varphi"'] & G \arrow[u, "{[\cdot]_\gamma}"']
\end{tikzcd}$$

Definition 2.5. Let M be an A-module. M is called of **finite presentation** or **finitely presented** if there exists an $n \times m$-matrix φ such that M is isomorphic to the cokernel of the map $\varphi : A^m \to A^n$. We call φ a **presentation matrix** of M. We write

$$\begin{tikzcd}
A^m \arrow[r, "\varphi"] & A^n \arrow[r] & M \arrow[r] & 0
\end{tikzcd}$$

to denote a presentation of M.

Constructive module theory is concerned with modules of finite presentation, that is, with modules which can be given as the cokernel of some matrix. All operations with modules are then represented by operations with the corresponding presentation matrices. We shall see later on that every finitely generated module over a Noetherian ring is finitely presented. As polynomial rings and localizations thereof are Noetherian every finitely generated module over these rings is of finite presentation.

Example 2.3. Let $A = \mathbb{Q}[x, y, z]$ and let M be the submodule of A^2 generated by the column vectors $(xy, yz)^t$ and $(xz, z^2)^t$. This means we have a map

$$\begin{tikzcd}
A^2 \arrow[rr, "\begin{pmatrix} xy & xz \\ yz & z^2 \end{pmatrix}"] & & M \\
e_1 \arrow[r, mapsto] & & xye_1 + yze_2 \\
e_2 \arrow[r, mapsto] & & xze_1 + z^2e_2
\end{tikzcd}$$

To obtain a presentation of N, we need to compute the kernel of this map. The kernel is generated by the column vector $(-z, y)^t$. So $(-z, y)^t$ is the presentation matrix of M.

$$\begin{tikzcd}
A \arrow[r, "\begin{pmatrix} -z \\ y \end{pmatrix}"] & A^2 \arrow[r, "\begin{pmatrix} xy & xz \\ yz & z^2 \end{pmatrix}"] & M \\
e_1 \arrow[r, mapsto] & -ze_1 + ye_2 & \\
 & e_1 \arrow[r, mapsto] & xye_1 + yze_2 \\
 & e_2 \arrow[r, mapsto] & xze_1 + z^2e_2
\end{tikzcd}$$

Lemma 2.2. *Let M and N be two A-modules with presentations*

$$A^m \xrightarrow{\varphi} A^n \xrightarrow{\pi} M \longrightarrow 0 \quad \textit{and} \quad A^r \xrightarrow{\psi} A^s \xrightarrow{\kappa} N \longrightarrow 0.$$

1. *Let $\lambda : M \to N$ be an A-module homomorphism, then there exist A-module homomorphisms $\alpha : A^m \to A^r$ and $\beta : A^n \to A^s$ such that the following diagram commutes:*

$$\begin{tikzcd}
A^m \arrow[r, "\varphi"] \arrow[d, "\alpha"] & A^n \arrow[r, "\pi"] \arrow[d, "\beta"] & M \arrow[r] \arrow[d, "\lambda"] & 0 \\
A^r \arrow[r, "\psi"] & A^s \arrow[r, "\kappa"] & N \arrow[r] & 0.
\end{tikzcd}$$

that is, $\beta \circ \varphi = \psi \circ \alpha$ and $\lambda \circ \pi = \kappa \circ \beta$.

2. *Let $\beta : A^n \to A^s$ be an A-module homomorphism such that $\beta(Im(\varphi)) \subset Im(\psi)$. Then there exist A-module homomorphisms $\alpha : A^m \to A^r$ and $\lambda : M \to N$ such that the corresponding diagram commutes.*

Proof. (1) : Let $\{e_1, \dots, e_n\}$ be an A-basis for A^n and choose $x_i \in A^s$ such that $\kappa(x_i) = (\lambda \circ \pi)(e_i)$. We define $\beta(\sum_{i=1}^n a_i e_i) = \sum_{i=1}^n a_i x_i$. Obviously β is an A-module homomorphism and $\lambda \circ \pi = \kappa \circ \beta$. Let $\{f_1, \dots, f_m\}$ be a basis of A^m. Then $(\kappa \circ \beta \circ \varphi)(f_i) = (\lambda \circ \pi \circ \varphi)(f_i) = 0$, so $\beta(\varphi(f_i)) \in \mathrm{Ker}(\kappa)$. Therefore, there exists $y_i \in A^r$ such that $\psi(y_i) = (\beta \circ \varphi)(f_i)$. We define $\alpha(\sum_{i=1}^n b_n f_i) = \sum_{i=1}^n b_i y_i$. Again α is an A-module homomorphism and $\psi \circ \alpha = \beta \circ \varphi$.

(2) : Define $\lambda(m) = (\kappa \circ \beta)(\tilde{m})$, for some $\tilde{m} \in A^n$ with $\pi(\tilde{m}) = m$. To see that this definition does not depend on the choice of $\tilde{m}$, let $\tilde{m} + \varphi(x)$ be another lift where $x \in A^m$. Then $(\kappa \circ \beta)(\tilde{m} + \varphi(x)) = (\kappa \circ \beta)(\tilde{m}) + (\kappa \circ \beta \circ \varphi)(x) = (\kappa \circ \beta)(\tilde{m})$. Obviously, λ is an A-module homomorphism satisfying $\lambda \circ \pi = \kappa \circ \beta$. We can define α as in (1). □

3 Short Exact Sequences and Splitting Modules

Definition 3.1. A sequence of R-modules and R-linear maps

$$L \xrightarrow{\varphi} M \xrightarrow{\psi} N$$

is called **exact at** M if $\operatorname{im} \varphi = \ker \psi$. A **short exact sequence** is a sequence of R-modules and R-linear maps

$$0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$$

which is exact at L, M, and N.

3.0.1 Five Lemma

Proposition 3.1. *Suppose the following diagram of R-modules and R-homomorphisms is commutative with exact rows*

$$\begin{tikzcd}
M_1 \arrow[r, "\varphi_1"] \arrow[d, "\psi_1"] & M_2 \arrow[r, "\varphi_2"] \arrow[d, "\psi_2"] & M_3 \arrow[r, "\varphi_3"] \arrow[d, "\psi_3"] & M_4 \arrow[r, "\varphi_4"] \arrow[d, "\psi_4"] & M_5 \arrow[d, "\psi_5"] \\
M_1' \arrow[r, "\varphi_1'"] & M_2' \arrow[r, "\varphi_2'"] & M_3' \arrow[r, "\varphi_3'"] & M_4' \arrow[r, "\varphi_4'"] & M_5'
\end{tikzcd}$$

1. *If ψ_2, ψ_4 are surjective and ψ_5 is injective, then ψ_3 is surjective.*
2. *If ψ_2, ψ_4 are injective and ψ_1 is surjective, then ψ_3 is injective.*

Proof.

1. Suppose ψ_2, ψ_4 are surjective and ψ_5 is injective and let $u_3' \in M_3'$. Since ψ_4 is surjective, we may choose a $u_4 \in M_4$ such that $\psi_4(u_4) = \varphi_3'(u_3')$. Observe that

$$\begin{aligned}\psi_5\varphi_4(u_4) &= \varphi_4'\psi_4(u_4)\\ &= \varphi_4'\varphi_3'(u_3')\\ &= 0.\end{aligned}$$

It follows that $\varphi_4(u_4) = 0$ since ψ_5 is injective. Therefore we may choose a $u_3 \in M_3$ such that $\varphi_3(u_3) = u_4$ (by exactness of the top row). Now observe that

$$\begin{aligned}\varphi_3'(u_3' - \psi_3(u_3)) &= \varphi_3'(u_3') - \varphi_3'\psi_3(u_3)\\ &= \psi_4(u_4) - \psi_4\varphi_3(u_3)\\ &= \psi_4(u_4) - \psi_4(u_4)\\ &= 0.\end{aligned}$$

Therefore we may choose a $u_2' \in M_2'$ such that $\varphi_2'(u_2') = u_3' - \psi_3(u_3)$ (by exactness of the bottom row). Since ψ_2 is surjective, we may choose a $u_2 \in M_2$ such that $\psi_2(u_2) = u_2'$. Finally we see that

$$\begin{aligned}\psi_3(\varphi_2(u_2) + u_3) &= \psi_3\varphi_2(u_2) + \psi_3(u_3)\\ &= \varphi_2'\psi_2(u_2) + \psi_3(u_3)\\ &= \varphi_2'(u_2') + \psi_3(u_3)\\ &= u_3' - \psi_3(u_3) + \psi_3(u_3)\\ &= u_3'.\end{aligned}$$

It follows that ψ_3 is surjective.

2. Suppose ψ_2, ψ_4 are injective and ψ_1 is surjective and let $u_3 \in \ker\psi_3$. Observe that

$$\begin{aligned}\psi_4\varphi_3(u_3) &= \varphi_3'\psi_3(u_3)\\ &= \varphi_3'(0)\\ &= 0.\end{aligned}$$

It follows that $\varphi_3(u_3) = 0$ since ψ_4 is injective. Therefore we may choose a $u_2 \in M_2$ such that $\varphi_2(u_2) = u_3$ (by exactness of the top row). Now observe that

$$\begin{aligned}\varphi_2'\psi_2(u_2) &= \psi_3\varphi_2(u_2)\\ &= \psi_3(u_3)\\ &= 0.\end{aligned}$$

Therefore we may choose a $u_1' \in M_1'$ such that $\varphi_1'(u_1') = \psi_2(u_2)$ (by exactness of the bottom row). Since ψ_1 is surjective, we may choose a $u_1 \in M_1$ such that $\psi_1(u_1) = u_1'$. Now observe that

$$\begin{aligned}\psi_2\varphi_1(u_1) &= \varphi_1'\psi_1(u_1)\\ &= \varphi_1'(u_1')\\ &= \psi_2(u_2).\end{aligned}$$

It follows that $\varphi_1(u_1) = u_2$ since ψ_2 is injective. Therefore

$$\begin{aligned}u_3 &= \varphi_2(u_2)\\ &= \varphi_2\varphi_1(u_1)\\ &= 0,\end{aligned}$$

which implies $\ker\psi_3 = 0$. Thus ψ_3 is injective. □

3.0.2 The 3×3 Lemma

Proposition 3.2. *Consider the following diagram*

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & M_1 \arrow[r, "\varphi_1"] \arrow[d, "\psi_1"] & M_2 \arrow[r, "\varphi_2"] \arrow[d, "\psi_2"] & M_3 \arrow[r] \arrow[d, "\psi_3"] & 0 \\
0 \arrow[r] & M_1' \arrow[r, "\varphi_1'"] \arrow[d, "\psi_1'"] & M_2' \arrow[r, "\varphi_2'"] \arrow[d, "\psi_2'"] & M_3' \arrow[r] \arrow[d, "\psi_3'"] & 0 \\
0 \arrow[r] & M_1'' \arrow[r, "\varphi_1''"] \arrow[d] & M_2'' \arrow[r, "\varphi_2''"] \arrow[d] & M_3'' \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

If the columns and top two rows are exact, then the bottom row is exact.

Proof. We first show φ_1'' is injective. Let $u_1'' \in \ker \varphi_1''$. Since ψ_1' is surjective (by exactness of first column) we may choose a $u_1' \in M_1'$ such that $\psi_1'(u_1') = u_1''$. Then

$$\begin{aligned}
\psi_2'\varphi_1'(u_1') &= \varphi_1''\psi_1'(u_1') \\
&= \varphi_1''(u_1'') \\
&= 0
\end{aligned}$$

implies $\varphi_1'(u_1') \in \ker \psi_2'$. Therefore there exists a unique $u_2 \in M_2$ such that $\psi_2(u_2) = \varphi_1'(u_1')$ (by exac Then

$$\begin{aligned}
\psi_3\varphi_2(u_2) &= \varphi_2'\psi_2(u_2) \\
&= \varphi_2'\varphi_1'(u_1') \\
&= 0
\end{aligned}$$

implies $\varphi_2(u_2) = 0$ since ψ_3 is injective (by exactness of third column). Thus $u_2 \in \ker \varphi_2$ and so there exists a unique $u_1 \in M_1$ such that $\varphi_1(u_1) = u_2$ (by exactness of first row). Therefore

$$\begin{aligned}
\varphi_1'\psi_1(u_1) &= \psi_2\varphi_1(u_1) \\
&= \psi_2(u_2) \\
&= \varphi_1'(u_1')
\end{aligned}$$

implies $\psi_1(u_1) = u_1'$ since φ_1' is injective (by exactness of second row). Thus

$$\begin{aligned}
u_1'' &= \psi_1'(u_1') \\
&= \psi_1'\psi_1(u_1) \\
&= 0.
\end{aligned}$$

Now we show $\ker \varphi_2'' = \operatorname{im} \varphi_1''$. Let $u_2'' \in \ker \varphi_2''$. Since ψ_2' is surjective (by exactness of second colunn), we may choose a $u_2' \in M_2'$ such that $\psi_2'(u_2') = u_2''$. Then

$$\begin{aligned}
\psi_3'\varphi_2'(u_2') &= \varphi_2''\psi_2'(u_2') \\
&= \varphi_2''(u_2'') \\
&= 0
\end{aligned}$$

implies $\varphi_2'(u_2') \in \ker \psi_3'$. Therefore there exists a unique $u_3 \in M_3$ such that $\psi_3(u_3) = \varphi_2'(u_2')$ (by exactness of third column). Since φ_2 is surjective, we may choose a $u_2 \in M_2$ such that $\varphi_2(u_2) = u_3$. Then

$$\begin{aligned}
\varphi_2'(\psi_2(u_2) - u_2') &= \varphi_2'\psi_2(u_2) - \varphi_2'(u_2') \\
&= \psi_3\varphi_2(u_2) - \varphi_2'(u_2') \\
&= \psi_3(u_3) - \varphi_2'(u_2') \\
&= \varphi_2'(u_2') - \varphi_2'(u_2') \\
&= 0
\end{aligned}$$

implies $\psi_2(u_2) - u_2' \in \ker \varphi_2'$. Therefore there exists a uniuqe $u_1' \in M_1'$ such that $\varphi_1'(u_1') = \psi_2(u_2) - u_2'$ (by exactness of second row). Therefore

$$\begin{aligned}
\varphi_1''\psi_1'(u_1') &= \psi_2'\varphi_1'(u_1') \\
&= \psi_2'(\psi_2(u_2) - u_2') \\
&= \psi_2'\psi_2(u_2) - \psi_2'(u_2') \\
&= \psi_2'(u_2') \\
&= u_2''.
\end{aligned}$$

It follows that $u_2'' \in \operatorname{im} \varphi_1''$. Thus $\ker \varphi_2'' \subseteq \operatorname{im} \varphi_1''$. For the reverse inclusion, let $u_2'' \in M_2''$. Choose $u_1'' \in M_1''$ such that $\varphi_1''(u_1'') = u_2''$. Since ψ_1' is surjective (by exactness of first column), we may choose a $u_1' \in M_1'$ such that $\psi_1'(u_1') = u_1''$. Then

$$\begin{aligned}
0 &= \psi_3'\varphi_2'\varphi_1'(u_1') \\
&= \varphi_2''\psi_2'\varphi_1'(u_1') \\
&= \varphi_2''\varphi_1''\psi_1'(u_1') \\
&= \varphi_2''\varphi_1''(u_1'') \\
&= \varphi_2''(u_2'')
\end{aligned}$$

implies $u_2'' \in \ker \varphi_2''$. Thus $\ker \varphi_2'' \supseteq \operatorname{im} \varphi_1''$.

The last step is to show φ_2'' is surjective. Let $u_3'' \in M_3''$. Since ψ_3' is surjective (by exactness of third column), we may choose a $u_3' \in M_3'$ such that $\psi_3'(u_3') = u_3''$. Since φ_2' is surjective (by exactness of second row), we may choose a $u_2' \in M_2'$ such that $\varphi_2'(u_2') = u_3'$. Then

$$\begin{aligned}
\varphi_2''\psi_2'(u_2') &= \psi_3'\varphi_2'(u_2') \\
&= \psi_3'(u_3') \\
&= u_3''
\end{aligned}$$

implies φ_2'' is surjective. □

3.0.3 The Snake Lemma

Proposition 3.3. *Consider the following commutative diagram with exact rows*

$$\begin{tikzcd}
 & M_1 \arrow[r, "\varphi_1"] \arrow[d, "\psi_1"] & M_2 \arrow[r, "\varphi_2"] \arrow[d, "\psi_2"] & M_3 \arrow[r] \arrow[d, "\psi_3"] & 0 \\
0 \arrow[r] & M_1' \arrow[r, "\varphi_1'"] & M_2' \arrow[r, "\varphi_2'"] & M_3' &
\end{tikzcd} \tag{4}$$

Then there exists an exact sequence

$$\ker \psi_1 \xrightarrow{\widetilde{\varphi_1}} \ker \psi_2 \xrightarrow{\widetilde{\varphi_2}} \ker \psi_3 \xrightarrow{\partial} \operatorname{coker} \psi_1 \xrightarrow{\overline{\varphi_1'}} \operatorname{coker} \psi_2 \xrightarrow{\overline{\varphi_2'}} \operatorname{coker} \psi_3. \tag{5}$$

Moreover, if φ_1 is injective, then $\widetilde{\varphi_1}$ is injective; and if φ_2' is surjective, then $\overline{\varphi_2'}$ is surjective.

Proof.

Step 1: We first define the maps in question. Define $\widetilde{\varphi_1} \colon \ker \psi_1 \to \ker \psi_2$ by

$$\widetilde{\varphi_1}(u_1) = \varphi_1(u_1)$$

for all $u_1 \in \ker \psi_1$. Note that $\widetilde{\varphi_1}$ lands in $\ker \psi_2$ by the commutativity of the diagram. Indeed,

$$\begin{aligned}
\psi_2\widetilde{\varphi_1}(u_1) &= \psi_2\varphi_1(u_1) \\
&= \varphi_1'\psi_1(u_1) \\
&= \varphi_1'(0) \\
&= 0
\end{aligned}$$

implies $\widetilde{\varphi_1}(u_1) \in \ker \psi_2$ for all $u_1 \in \ker \psi_1$. Also note that $\widetilde{\varphi_1}$ is an R-module homomorphism since φ_1 is an R-module homomorphism. Similarly, we define $\widetilde{\varphi_2} \colon \ker \psi_2 \to \ker \psi_3$ by

$$\widetilde{\varphi_2}(u_2) = \varphi_2(u_2)$$

for all $u_2 \in \ker \psi_2$.

Next we define $\partial \colon \ker \psi_3 \to \operatorname{coker} \psi_1$ as follows: let $u_3 \in \ker \psi_3$. Choose $u_2 \in M_2$ such that $\varphi_2(u_2) = u_3$ (such an element exists because φ_2 is surjective by exactness of the first row). By the commutativity of the diagram, we have

$$\begin{aligned}\varphi_2'\psi_2(u_2) &= \psi_3\varphi_2(u_2)\\ &= \psi_3(u_3)\\ &= 0.\end{aligned}$$

It follows that $\psi_2(u_2) \in \ker \varphi_2'$. Therefore there exists a unique $u_1' \in M_1'$ such that $\varphi_1'(u_1') = \psi_2(u_2)$ (by exactness of the second row). We set

$$\partial(u_3) = \overline{u_1'}$$

where $\overline{u_1'}$ is the coset in $\operatorname{coker} \psi_1$ with u_1' as a representative. We must check that ∂ defined in this is in fact a well-defined map. There was one choice that we made in our construction, namely the lift of u_3 under φ_2 to u_2. So let v_2 be another element in M_2 such that $\varphi_2(v_2) = u_3$. Denote by v_1' to be the unique element in M_1' such that $\varphi_1'(v_1') = \psi_2(v_2)$. We must show that $\overline{u_1'} = \overline{v_1'}$ in $\operatorname{coker} \psi_1$. In other words, we must show that $v_1' - u_1' \in \operatorname{im} \psi_1$. Observe that

$$\begin{aligned}\varphi_2(v_2 - u_2) &= \varphi_2(v_2) - \varphi_2(u_2)\\ &= u_3 - u_3\\ &= 0\end{aligned}$$

implies $v_2 - u_2 \in \ker \varphi_2$. It follows that there exists a unique element $u_1 \in M_1$ such that $\varphi_1(u_1) = v_2 - u_2$ (by exactness of the first row). Then

$$\begin{aligned}\varphi_1'\psi_1(u_1) &= \psi_2\varphi_1(u_1)\\ &= \psi_2(v_2 - u_2)\\ &= \psi_2(v_2) - \psi_2(u_2)\\ &= \varphi_1'(v_1') - \varphi_1'(u_1')\\ &= \varphi_1'(v_1' - u_1')\end{aligned}$$

implies $\psi_1(u_1) = v_1' - u_1'$ since φ_1' is injective (by exactness of the second row). It follows that $v_1' - u_1' \in \operatorname{im} \psi_1$, and hence ∂ is well-defined.

Finally, we define $\overline{\varphi_1'} \colon \operatorname{coker} \psi_1 \to \operatorname{coker} \psi_2$ by

$$\overline{\varphi_1'}(\overline{u_1'}) = \overline{\varphi_1'(u_1')}$$

for all $\overline{u_1'} \in \operatorname{coker} \psi_1$. The map $\overline{\varphi_1'}$ is well-defined by the commutativity of the diagram. Indeed, let v_1' be another representative of the coset $\overline{u_1'}$ in $\operatorname{coker} \psi_1$. Choose $u_1 \in M_1$ such that $v_1' - u_1' = \psi_1(u_1)$. Then

$$\begin{aligned}\psi_2\varphi_1(u_1) &= \varphi_1'\psi_1(u_1)\\ &= \varphi_1'(v_1' - u_1')\\ &= \varphi_1'(v_1') - \varphi_1'(u_1').\end{aligned}$$

It follows that $\varphi_1'(v_1') - \varphi_1'(u_1') \in \operatorname{im} \psi_2$, and hence $\varphi_1'(v_1')$ and $\varphi_1'(u_1')$ represent the same coset in $\operatorname{coker} \psi_2$. Similarly, we define $\overline{\varphi_2'} \colon \operatorname{coker} \psi_2 \to \operatorname{coker} \psi_3$ by

$$\overline{\varphi_2'}(\overline{u_2'}) = \overline{\varphi_2'(u_2')}$$

for all $\overline{u_2'} \in \operatorname{coker} \psi_2$.

Step 2: Now that we've defined the maps in question, we will now show that the sequence (5) is exact as well as prove the "moreover" part of the proposition. First we show exactness at $\ker \psi_2$. Observe that

$$\begin{aligned}\widetilde{\varphi_2}\widetilde{\varphi_1}(u_1) &= \varphi_2\varphi_1(u_1)\\ &= 0\end{aligned}$$

for all $u_1 \in \ker \psi_1$. It follows that $\ker \widetilde{\varphi_2} \supseteq \operatorname{im} \widetilde{\varphi_1}$. Conversely, let $u_2 \in \ker \widetilde{\varphi_2}$. Thus $u_2 \in \ker \varphi_2 \cap \ker \psi_2$. By exactness of the top row in (4), we may choose a $u_1 \in M_1$ such that $\varphi_1(u_1) = u_2$. Moreover,

$$\begin{aligned}\varphi_1'\psi_1(u_1) &= \psi_2\varphi_1(u_1)\\ &= \psi_2(u_2)\\ &= 0\end{aligned}$$

implies $\psi_1(u_1) = 0$ since φ_1' is injective (by exactness of the bottom row in (4)). Therefore $u_1 \in \ker\psi_1$, and so $u_2 \in \operatorname{im}\widetilde{\varphi_1}$. Thus $\ker\widetilde{\varphi_2} \subseteq \operatorname{im}\widetilde{\varphi_1}$.

Next we show exactness at $\ker\psi_3$: let $u_3 \in \ker\partial$. Choose $u_2 \in M_2$ and $u_1' \in M_1'$ such that $\varphi_2(u_2) = u_3$ and $\varphi_1'(u_1') = \psi_2(u_2)$. Then

$$\begin{aligned} 0 &= \partial(u_3) \\ &= \overline{u_1'} \end{aligned}$$

implies $u_1' \in \operatorname{im}\psi_1$. Choose $u_1 \in M_1$ such that $\psi_1(u_1) = u_1'$. Then

$$\begin{aligned} \psi_2(u_2 - \varphi_1(u_1)) &= \psi_2(u_2) - \psi_2\varphi_1(u_1) \\ &= \psi_2(u_2) - \varphi_1'\psi_1(u_1) \\ &= \psi_2(u_2) - \varphi_1'(u_1') \\ &= \psi_2(u_2) - \psi_2(u_2) \\ &= 0 \end{aligned}$$

implies $u_2 - \varphi_1(u_1) \in \ker\psi_2$. Furthermore, we have

$$\begin{aligned} \varphi_2(u_2 - \varphi_1(u_1)) &= \varphi_2(u_2) - \varphi_2\varphi_1(u_1) \\ &= \varphi_2(u_2) \\ &= u_3. \end{aligned}$$

It follows that $u_3 \in \operatorname{im}\widetilde{\varphi_2}$. Thus $\ker\partial \subseteq \operatorname{im}\widetilde{\varphi_2}$. Convsersely, let $u_3 \in \operatorname{im}\widetilde{\varphi_2}$. Choose $u_2 \in \ker\psi_2$ such that $\varphi_2(u_2) = u_3$. Then $0 \in M_1'$ is the unique element in M_1' which maps to $\psi_2(u_2) = 0$. Thus $\partial(u_3) = \overline{0}$ which implies $\ker\partial \supseteq \operatorname{im}\widetilde{\varphi_2}$.

Next we show exactness at $\operatorname{coker}\psi_1$: let $\overline{u_1'} \in \ker\overline{\varphi_1'}$. Then $\varphi_1'(u_1') = \psi_2(u_2)$ for some $u_2 \in M_2$. Moreover,

$$\begin{aligned} \psi_3\varphi_2(u_2) &= \varphi_2'\psi_2(u_2) \\ &= \varphi_2'\varphi_1'(u_1') \\ &= 0 \end{aligned}$$

implies $\varphi_2(u_2) \in \ker\psi_3$. Also we have $\partial(\varphi_2(u_2)) = \overline{u_1'}$, and so $\overline{u_1'} \in \operatorname{im}\partial$. Thus $\ker\overline{\varphi}_1' \subseteq \operatorname{im}\partial$. Conversely, let $\overline{u_1'} \in \operatorname{im}\partial$. Choose $u_3 \in M_3$ and $u_2 \in M_2$ such that $\varphi_2(u_2) = u_3$ and $\psi_2(u_2) = \varphi_1'(u_1')$. It follows that

$$\begin{aligned} \overline{\varphi_1'}(\overline{u_1'}) &= \overline{\varphi_1'(u_1')} \\ &= \overline{\psi_2(u_2)} \\ &= \overline{0} \end{aligned}$$

in $\operatorname{coker}\psi_2$. Thus $\ker\overline{\varphi_1'} \supseteq \operatorname{im}\partial$.

Next we check exactness at $\operatorname{coker}\psi_2$: let $\overline{u_2'} \in \ker\overline{\varphi_2'}$. Choose $u_3 \in M_3$ such that $\psi_3(u_3) = \varphi_2'(u_2')$ and choose $u_2 \in M_2$ such that $\varphi_2(u_2) = u_3$. Since

$$\begin{aligned} \varphi_2'(u_2' - \psi_2(u_2)) &= \varphi_2'(u_2') - \varphi_2'\psi_2(u_2) \\ &= \varphi_2'(u_2') - \psi_3\varphi_2(u_2) \\ &= \varphi_2'(u_2') - \psi_3(u_3) \\ &= \varphi_2'(u_2') - \varphi_2'(u_2') \\ &= 0, \end{aligned}$$

it follows that $u_2' - \psi_2(u_2) \in \ker\varphi_2'$. Therefore there exists a unique $u_1' \in M_1'$ such that $\varphi_1'(u_1') = u_2' - \psi_2(u_2)$ (by exactness of the bottom row in (4)). Then

$$\begin{aligned} \overline{\varphi_1'}(\overline{u_1'}) &= \overline{\varphi_1'(u_1')} \\ &= \overline{u_2' - \psi_2(u_2)} \\ &= \overline{u_2'} \end{aligned}$$

in $\operatorname{coker}\psi_2$. It follows that $\overline{u_2'} \in \operatorname{im}\overline{\varphi_2'}$ and hence $\ker\overline{\varphi_2'} \subseteq \operatorname{im}\overline{\varphi_1'}$. Conversely, let $\overline{u_2'} \in \operatorname{im}\overline{\varphi_2'}$. Choose $u_1' \in M_1'$ such that $\varphi_1'(u_1') = u_2'$. Then

$$\begin{aligned} 0 &= \varphi_2'\varphi_1'(u_1') \\ &= \varphi_2'(u_2') \end{aligned}$$

implies $u_2' \in \ker \varphi_2$. Therefore $\overline{\varphi_2'}(\overline{u_2'}) = \overline{0}$ in $\operatorname{coker} \psi_3$, and it follows that $\ker \overline{\varphi_2'} \supseteq \operatorname{im} \overline{\varphi_1'}$.

Finally, we prove the moreover part of this proposition. Suppose that φ_1 is injective. We want to show that $\widetilde{\varphi_1}$ is injective. Let $u_1 \in \ker \widetilde{\varphi_1}$. Then

$$\begin{aligned} 0 &= \widetilde{\varphi_1}(u_1) \\ &= \varphi_1(u_1) \end{aligned}$$

implies $u_1 = 0$ since φ_1 is injective. It follows that $\widetilde{\varphi_1}$ is injective. Now suppose that φ_2' is surjective. We want to show that $\overline{\varphi_2'}$ is surjective. Let $\overline{u_3'} \in \operatorname{coker} \psi_3$. Since φ_2' is surjective, we may choose a $u_2' \in M_2'$ such that $\varphi_2'(u_2') = u_3'$. Then

$$\begin{aligned} \overline{\varphi_2'}(\overline{u_2'}) &= \overline{\varphi_2'(u_2')} \\ &= \overline{u_3'}. \end{aligned}$$

It follows that $\overline{\varphi_2'}$ is surjective. □

3.0.4 Split Short Exact Sequences

Let M be an R-module and let N be an R-submodule of M. Then

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r, hook] & M \arrow[r] & M/N \arrow[r] & 0 \end{tikzcd} \tag{6}$$

is a short exact sequence. It turns out that a short exact sequence like (**??**) is isomorphic to a short exact sequence like (6) in the following way:

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r, "f"] \arrow[d] & M \arrow[r, "g"] \arrow[d, "id"] & P \arrow[r] \arrow[d, "\varphi"] & 0 \\ 0 \arrow[r] & f(N) \arrow[r, hook] & M \arrow[r] & M/f(N) \arrow[r] & 0 \end{tikzcd}$$

where the unlabled arrows are the obvious ones and φ is defined as follows: Given $p \in P$, choose $\widetilde{p} \in M$ such that $g(\widetilde{p}) = p$. Then set $\varphi(p) = \overline{\widetilde{p}}$. This is well-defined since if $\widetilde{p}' \in M$ was another lift of p, then $g(\widetilde{p} - \widetilde{p}') = 0$ implies $\widetilde{p} - \widetilde{p}' \in \operatorname{Ker}(g) = \operatorname{Im}(f)$. So $\widetilde{p}' = f(k) + \widetilde{p}$ for some $k \in K$, and hence $\overline{\widetilde{p}'} = \overline{f(k) + \widetilde{p}} = \overline{\widetilde{p}}$. It is also easy to verify that all vertical arrows are in fact A-module isomorphisms.

Example 3.1. Let I and J be ideals in R such that $I + J = R$. Then there is a short exact sequence of R-modules given by

$$\begin{tikzcd} 0 \arrow[r] & I \cap J \arrow[r, "\varphi"] & I \oplus J \arrow[r, "\psi"] & R \arrow[r] & 0 \\ & x \arrow[r, mapsto] & (x, -x) & & \\ & & (i,j) \arrow[r, mapsto] & i + j & \end{tikzcd}$$

Definition 3.2. A short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & L \arrow[r, "\varphi"] & M \arrow[r, "\psi"] & N \arrow[r] & 0 \end{tikzcd}$$

is called **split** when there is an R-module isomorphism $\theta\colon M \to L \oplus N$ such that the diagram

$$\begin{tikzcd} 0 \arrow[r] & L \arrow[r, "\varphi"] \arrow[d, "\mathrm{id}"] & M \arrow[r, "\psi"] \arrow[d, "\theta"] & N \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\ 0 \arrow[r] & L \arrow[r, "\iota_1"] & L \oplus N \arrow[r, "\pi_2"] & N \arrow[r] & 0 \end{tikzcd}$$

commutes, where the bottom maps to and from the direct sum are the standard embedding and projection; that is

$$\iota_1(u) = (u, 0) \quad \text{and} \quad \pi_2(u, v) = v$$

for all $u \in L$ and $(u, v) \in N$.

Theorem 3.1. *Let*

$$\begin{tikzcd}
0 \arrow[r] & L \arrow[r, "\varphi"] & M \arrow[r, "\psi"] & N \arrow[r] & 0
\end{tikzcd}$$

be a short exact sequence of R-modules. The following are equivalent:

1. *There is an R-linear map $\widetilde{\varphi}\colon M \to L$ such that $\widetilde{\varphi}\varphi(u) = u$ for all $u \in L$.*
2. *There is an R-linear map $\widetilde{\psi}\colon N \to M$ such that $\psi\widetilde{\psi}(w) = w$ for all $w \in N$.*
3. *The short exact sequence splits.*

Proof. We first show that (2) and (3) are equivalent. One direction is easy, so let us prove the other one. Suppose $\widetilde{\psi}\colon N \to M$ is an R-linear map such that $\psi\widetilde{\psi}(w) = w$ for all $w \in N$. Define $\vartheta\colon L \oplus N \to M$ by

$$\vartheta(u, w) = \varphi(u) + \widetilde{\psi}(w)$$

for all $(u, w) \in L \oplus N$. The map ϑ is easily checked to be R-linear. We claim it is an isomorphism. Indeed, we first show that it is injective. Suppose $(u, w) \in \ker\vartheta$. Then $-\widetilde{\psi}(w) = \varphi(u)$. Therefore

$$\begin{aligned} 0 &= -\psi\varphi(u) \\ &= \psi\widetilde{\psi}(u)) \\ &= u, \end{aligned}$$

which also implies

$$\begin{aligned} 0 &= -\psi\varphi(0) \\ &= -\psi\varphi(u) \\ &= \psi\widetilde{\psi}(w) \\ &= w, \end{aligned}$$

and so $(u, w) = (0, 0)$. It follows that ϑ is injective.

Now we will show ϑ is surjective. Let $v \in M$. Observe that

$$\begin{aligned} \psi(v - \widetilde{\psi}\psi(v)) &= \psi(v) - \psi\widetilde{\psi}\psi(v)) \\ &= \psi(v) - \psi(v) \\ &= 0. \end{aligned}$$

It follows that $v - \widetilde{\psi}\psi(v) \in \ker\psi$. So we may choose a $u \in L$ such that $\varphi(u) = v - \widetilde{\psi}\psi(v)$ by exactness of the short exact sequence. Then $(u, \psi(v)) \in L \oplus N$, and moreover we have

$$\begin{aligned} \vartheta(u, \psi(v)) &= \varphi(u) + \widetilde{\psi}\psi(v) \\ &= v - \widetilde{\psi}\psi(v) + \widetilde{\psi}\psi(v) \\ &= v. \end{aligned}$$

It follows that ϑ is surjective. Thus $\vartheta^{-1}\colon L \oplus N \to M$ is an isomorphism. It remains to check that ϑ^{-1} splits the short exact sequence. Let $u \in L$. Then u is the unique element in L which maps to $\varphi(u)$ under φ, and so

$$\begin{aligned} \vartheta^{-1}\varphi(u) &= (u, \psi\varphi(u)) \\ &= (u, 0) \\ &= \iota_1(u). \end{aligned}$$

Thus the left square commutes. Similarly, let $v \in M$ and let u be the unique element in L such that $\varphi(u) = v - \widetilde{\psi}\psi(v)$. Then

$$\begin{aligned} \pi_2\vartheta^{-1}(v) &= \pi_2(u, \psi(v)) \\ &= \psi(v). \end{aligned}$$

Thus the right square commutes too. This concludes the proof that (2) and (3) are equivalent.

Now we will show that (1) and (3) are equivalent. One direction is easy, so let us prove the other one. Suppose $\widetilde{\varphi}\colon M \to L$ is an R-linear map such that $\widetilde{\varphi}\varphi(u) = u$ for all $u \in L$. Define a map $\theta\colon M \to L \oplus N$ by

$$\theta(v) = (\widetilde{\varphi}(v), \psi(v))$$

for all $v \in M$. The map θ is easily checked to be R-linear. We claim it is an isomorphism. Indeed, we first show that it is injective. Suppose $v \in \ker\theta$. Then $\widetilde{\varphi}(v) = 0$ and $\psi(v) = 0$. So we may choose a $u \in L$ such that $\varphi(u) = v$ by exactness of the short exact sequence. Then

$$\begin{aligned} 0 &= \varphi\widetilde{\varphi}(v) \\ &= \varphi\widetilde{\varphi}\varphi(u) \\ &= \varphi(u) \\ &= v. \end{aligned}$$

It follows that θ is injective.

Now we will show θ is surjective. Let $(u, w) \in L \oplus N$. Since ψ is surjective, we may choose a $v \in M$ such that $\psi(v) = w$. Then $v + \varphi(u - \widetilde{\varphi}(v)) \in M$ and we have

$$\begin{aligned} \theta(v + \varphi(u - \widetilde{\varphi}(v))) &= (\widetilde{\varphi}(v + \varphi(u - \widetilde{\varphi}(v))), \psi(v + \varphi(u - \widetilde{\varphi}(v))) \\ &= (\widetilde{\varphi}(v) + \widetilde{\varphi}\varphi(u) - \widetilde{\varphi}\varphi\widetilde{\varphi}(v), \psi(v) + \psi\varphi(u) - \psi\varphi\widetilde{\varphi}(v)) \\ &= (\widetilde{\varphi}(v) + u - \widetilde{\varphi}(v), \psi(v)) \\ &= (u, w). \end{aligned}$$

It follows that θ is surjective. □

We want to stress that being split is not just saying that there is an isomorphism $M \to L \oplus N$ of R-modules, but *how* the isomorphism works with the maps f and g in the exact sequence: The commutativity of the diagram says $\varphi \colon L \to M$ behaves like the standard embedding $\iota_1 \colon L \to L \oplus N$ and $\psi \colon M \to N$ behaves like the standard projection $\pi_2 \colon L \oplus N \to N$. Here is an example of a short exact sequece which does not split, even though we have $M \cong L \oplus N$.

Example 3.2. Define $\varphi \colon \mathbb{Z} \to \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ by

$$\varphi(a) = (2a, 0)$$

for all $a \in \mathbb{Z}$ and define $\psi \colon \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}} \to (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ by

$$\psi(a, \overline{a_1}, \overline{a_2}, \dots) = (\overline{a}, \overline{a_1}, \overline{a_2}, \dots)$$

for all $(a, \overline{a_1}, \overline{a_2}, \dots) \in \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$. Then

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z} \arrow[r, "\varphi"] & \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}} \arrow[r, "\psi"] & (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}} \arrow[r] & 0 \end{tikzcd}$$

is a short exact sequence which does not split. Indeed, assume for a contradiction that it did split. Then there exists an R-linear map $\widetilde{\psi} \colon (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}} \to \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ such that $\psi\widetilde{\psi} = 1$. Let $\pi_1 \colon \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}} \to \mathbb{Z}$ be and $\pi_2 \colon \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}} \to (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ be the natural projection maps and denote $\pi_1 \circ \widetilde{\psi} = \widetilde{\psi}_1$ and $\pi_2 \circ \widetilde{\psi} = \widetilde{\psi}_2$. First note that $\widetilde{\psi}_1 \colon (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}} \to \mathbb{Z}$ must be the zero map since 2 is a nonzerodivisor on $\mathbb{Z}$ and $2 \in \operatorname{Ann}((\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}})$. Indeed, we have

$$\begin{aligned} 2\widetilde{\psi}_1((\overline{a_n})) &= \widetilde{\psi}_1((\overline{2a_n})) \\ &= \widetilde{\psi}_1(0) \\ &= 0 \end{aligned}$$

implies $\widetilde{\psi}_1((\overline{a_n})) = 0$ for all $(\overline{a_n}) \in (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$. Now let $(\overline{a_n}) \in (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ with $\overline{a_1} = \overline{1}$ and denote $(b_n) = \widetilde{\psi}_2((\overline{a_n}))$. Then

$$\begin{aligned} (\overline{a_n}) &= \psi\widetilde{\psi}((\overline{a_n})) \\ &= \psi(\widetilde{\psi}_1((\overline{a_n})), \widetilde{\psi}_2((\overline{a_n}))) \\ &= \psi(0, (b_n)) \\ &= (\overline{0}, \overline{b_1}, \overline{b_2}, \dots). \end{aligned}$$

This is a contradiction since $\overline{a_1} = \overline{1}$.

Example 3.3. Let I and J be ideals in R such that $I+J=R$. Then the short exact sequence given in Example (3.1) splits. Indeed, choose $x \in I$ and $y \in J$ such that $x+y=1$. Define $\widetilde{\psi}\colon R \to I \oplus J$ by

$$\widetilde{\psi}(a) = (ax, ay)$$

for all $a \in R$. The map $\widetilde{\psi}$ is easily checked to be an R-linear map. Moreover, we have

$$\begin{aligned} \psi\widetilde{\psi}(a) &= \psi(ax, ay) \\ &= ax + ay \\ &= a(x+y) \\ &= a \end{aligned}$$

for all $a \in R$. Therefore $\widetilde{\psi}$ splits this short exact sequence. In particular, we obtain an isomorphism

$$(I \cap J) \oplus R \cong I \oplus J,$$

where the addition map $I \oplus J \to R$ can now be viewed as a projection $(I \cap J) \oplus R \to R$.

If $I \cap J$ happens to be a principal ideal in R, say $I \cap J = \langle x \rangle$, then there is an R-module isomorphism $\mu_x\colon R \to I \cap J$ given by

$$\mu_x(a) = xa$$

for all $a \in R$. In particular, we obtain a sequence of isomorphisms

$$R \oplus R \cong (I \cap J) \oplus R \cong I \oplus J.$$

For example, in $\mathbb{Z}[\sqrt{-5}]$ we have

$$\mathbb{Z}[\sqrt{-5}] \oplus \mathbb{Z}[\sqrt{-5}] \cong \langle 3, 1+\sqrt{-5} \rangle \oplus \langle 3, 1-\sqrt{-5} \rangle.$$

3.0.5 Splicing Short Exact Sequences Together

Proposition 3.4. *Suppose for each $i \in \mathbb{Z}$, we are given short exact sequences of the form*

$$\begin{tikzcd} 0 \arrow[r] & K_i \arrow[r, "\phi_i"] & M_i \arrow[r, "\psi_i"] & K_{i-1} \arrow[r] & 0 \end{tikzcd} \tag{7}$$

Then we can splice these short exact sequences together to get a long exact sequence of the form

$$\begin{tikzcd} \cdots \arrow[r] & M_{i+1} \arrow[r, "\varphi_{i+1}"] & M_i \arrow[r, "\varphi_i"] & M_{i-1} \arrow[r] & \cdots \end{tikzcd} \tag{8}$$

where $\varphi_i = \phi_{i-1} \circ \psi_i$.

Proof. It follows the short exact sequences (7) that

$$\begin{aligned} \ker \varphi_i &= \ker(\phi_{i-1} \circ \psi_i) \\ &= \ker \psi_i \\ &= \operatorname{im} \phi_i \\ &= \operatorname{im}(\phi_i \circ \psi_{i+1}) \\ &= \operatorname{im} \varphi_{i+1}. \end{aligned}$$

It follows that (8) is exact. □

Corollary. *Every long exact of R-modules can be formed by splicing together suitable short exact sequences.*

Proof. Let

$$\begin{tikzcd} \cdots \arrow[r] & M_{i+1} \arrow[r, "\varphi_{i+1}"] & M_i \arrow[r, "\varphi_i"] & M_{i-1} \arrow[r] & \cdots \end{tikzcd} \tag{9}$$

be an exact sequence of R-modules. For each $i \in \mathbb{Z}$, we break (9) into short exact sequences of the form

$$\begin{tikzcd} 0 \arrow[r] & \ker \varphi_i \arrow[r, "\iota_i"] & M_i \arrow[r, "\widetilde{\varphi}_i"] & \operatorname{im} \varphi_i \arrow[r] & 0 \end{tikzcd} \tag{10}$$

where ι_i is the inclusion map and $\widetilde{\varphi}_i$ is just φ_i but with range $\operatorname{im} \varphi_i$ rather than M_{i-1}. In fact, since $\ker \varphi_{i-1} = \operatorname{im} \varphi_i$, we can rewrite (11) as

$$\begin{tikzcd} 0 \arrow[r] & \ker \varphi_i \arrow[r, "\iota_i"] & M_i \arrow[r, "\varphi_i"] & \ker \varphi_{i-1} \arrow[r] & 0 \end{tikzcd} \tag{11}$$

Since $\varphi_i = \iota_{i-1} \circ \widetilde{\varphi}_i$, it follows from Proposition (3.4) that splicing these short exact sequences together gives us our original long exact sequence (9) . □

3.1 Pullbacks and Pushouts

Proposition 3.5. *Let M, N, and P be R-modules, let $\psi\colon N \to M$ be an R-linear map, and let $\varphi\colon P \twoheadrightarrow M$ be a surjective R-linear map. Define the **pullback of** $\psi\colon N \to M$ **and** $\varphi\colon P \twoheadrightarrow M$ to be the R-module*

$$N \times_M P = \{(u,v) \in N \times P \mid \psi(u) = \varphi(v)\}$$

equipped with the R-linear maps $\pi_1\colon N \times_M P \to N$ and $\pi_2\colon N \times_M P \to P$ given by

$$\pi_1(u,v) = u \quad \textit{and} \quad \pi_2(u,v) = v$$

for all $(u,v) \in N \times_M P$. Then there exists an isomorphism $\overline{\varphi}\colon P/\pi_1(N \times_M P) \to M/N$ given by

$$\overline{\varphi}(\overline{v}) = \overline{\varphi(v)}$$

for all $\overline{v} \in P/\pi_1(N \times_M P)$. Moreover, the following diagram commutative

$$\begin{tikzcd}
N \times_M P \arrow[r, "\pi_2"] \arrow[d, "\pi_1"] & P \arrow[r] \arrow[d, "\varphi"] & P/\pi_1(N \times_M P) \arrow[r] \arrow[d, "\overline{\varphi}"] & 0 \\
N \arrow[r, "\psi"] & M \arrow[r] & M/\psi(N) \arrow[r] & 0
\end{tikzcd}$$

Proof. We first need to check that $\overline{\varphi}$ is well-defined. Suppose $v + v'$ is another representative of $\overline{v}$ where $v' \in \operatorname{im}(\pi_2)$. Choose $(u', v') \in N \times_M P$ such that $\pi_1(u', v') = v'$ (so $\varphi(v') = \psi(u')$). Then

$$\begin{aligned}
\overline{\varphi}(\overline{v+v'}) &= \overline{\varphi(v+v')} \\
&= \overline{\varphi(v) + \varphi(v')} \\
&= \overline{\varphi(v) + \psi(u')} \\
&= \overline{\varphi(v)}.
\end{aligned}$$

Thus $\overline{\varphi}$ is well-defined. Clearly, $\overline{\varphi}$ is a surjective R-linear map since φ is a surjective R-linear map. It remains to show that $\overline{\varphi}$ is injective. Suppose $\overline{v} \in \ker \overline{\varphi}$. Then $\varphi(v) \in \operatorname{im} \psi$. Choose $u \in N$ such that $\psi(u) = \varphi(v)$. Then $(u,v) \in N \times_M P$ and $v = \pi_2(u,v)$. It follows that $\overline{v} = 0$ in $P/\pi_2(N \times_M P)$. □

Proposition 3.6. *Let M, N, and E be R-modules, let $\psi\colon M \to N$ be an R-linear map, and let $\varphi\colon M \to E$ be an injective R-linear map. Define the **pushout of** $\psi\colon M \to N$ **and** $\varphi\colon M \to E$ to be the R-module*

$$E +_M N = E \times N / \{(\psi(w), -\varphi(w)) \mid w \in M\}$$

equipped with the R-linear maps $\iota_1\colon E \to E +_M N$ and $\iota_2\colon N \to E +_M N$ given by

$$\iota_1(u) = (u,0) \quad \textit{and} \quad \iota_2(v) = (0,v)$$

for all $u \in E$ and $v \in N$. Then φ restricts to an isomorphism $\varphi|_{\ker \psi}\colon \ker \psi \to \ker \iota_1$. Moreover, the following diagram commutative is commutative

$$\begin{tikzcd}
0 \arrow[r] & \ker \psi \arrow[r] \arrow[d, "\varphi|_{\ker \psi}"] & M \arrow[r, "\psi"] \arrow[d, "\varphi"] & N \arrow[d, "\iota_2"] \\
0 \arrow[r] & \ker \iota_1 \arrow[r] & E \arrow[r, "\iota_1"] & E +_M N
\end{tikzcd}$$

Proof. We first need to check that the restriction of φ to $\ker \psi$ lands in $\ker \iota_1$. Suppose $w \in \ker \psi$. Then observe that

$$\begin{aligned}
\iota_1 \varphi(w) &= [\varphi(w), 0] \\
&= [0, -\psi(w)] \\
&= [0, 0],
\end{aligned}$$

where we write $[u,v]$ for the equivalence class of (u,v) in $E +_M N$. It follows that $\varphi(w) \in \ker \iota_1$. Thus the map $\varphi|_{\ker \psi}\colon \ker \psi \to \ker \iota_1$ makes sense.

Clearly, $\varphi|_{\ker \psi}$ is an injective R-linear map since φ is an injective R-linear map. It remains to show that $\varphi|_{\ker \psi}$ is surjective. Suppose $u \in \ker \iota_1$ (so $[u,0] = [0,0]$). This implies that there exists a $w \in M$ such that $u = \varphi(w)$ and $\psi(w) = 0$. In other words, this implies the map $\varphi|_{\ker \psi}$ is surjective. □

4 Modules over a PID

4.1 Annihilators and Torsion

Definition 4.1. Let R be an integral domain, let M be an R-module, and let $u \in M$. We define the **annihilator** of u to be

$$0 :_R u = \{a \in R \mid au = 0\}.$$

We say $0 :_R u$ is the set of all elements in R which **kills** u. If $0 :_R u \neq 0$, then we say u is a **torsion element** of M. We denote by M_{tor} to be the set of all torsion elements of M. We say M is **torsion-free** if $M_{\text{tor}} = 0$, that is, the only torsion element of M is 0. We say M is **torsion** if $M_{\text{tor}} = M$, that is, every element in M is a torsion element.

Proposition 4.1. *Let R be an integral domain, let M be an R-module, and let $u \in M$. Then $0 :_R u$ is an ideal of R and M_{tor} is a R-submodule of M.*

Proof. We first show that $0 :_R u$ is an ideal of R. Observe that $0 \in 0 :_R u$ which implies $0 :_R u$ is nonempty. Let $x, y \in 0 :_R u$ and let $a \in R$. Then

$$\begin{aligned}(ax+y)u &= axu + yu \\ &= 0 + 0 \\ &= 0\end{aligned}$$

implies $ax + y \in 0 :_R u$. It follows that $0 :_R u$ is an ideal of R.

Now we will show that M_{tor} is an R-submodule of M. Observe that $0 \in M_{\text{tor}}$ which implies M_{tor} is nonempty. Let $u, v \in M_{\text{tor}}$ and let $a \in R$. Choose $x, y \in R\backslash\{0\}$ such that $xu = 0$ and $yv = 0$. Then $xy \neq 0$ since R is an integral domain, and moreover we have

$$\begin{aligned}xy(au+v) &= xyau + xyv \\ &= ya(xu) + x(yv) \\ &= 0 + 0 \\ &= 0,\end{aligned}$$

which implies $0 :_R (au + v) \neq 0$. It follows that $au + v \in M_{\text{tor}}$, which implies M_{tor} is an R-submodule of M. □

Proposition 4.2. *Let R be a PID, let p be a prime in R, let M be an R-module, and let $u \in M$. Suppose $p^k u = 0$ for some $k \geq 0$. Then*

$$0 :_R u = \langle p^i \rangle$$

for some $0 \leq i \leq k$.

Proof. Choose $i \geq 0$ to be the smallest integer such that $p^i u = 0$. We claim that $\langle p^i \rangle = 0 :_R u$. Since $p^i \in 0 :_R u$, we certainly have $0 :_R u \supseteq \langle p^i \rangle$. If $0 :_R u \supseteq \langle q^j \rangle$ for some other prime $q \neq p$, then

$$\begin{aligned}0 :_R u &\supseteq \langle p^i, q^j \rangle \\ &= \langle 1 \rangle\end{aligned}$$

since $\gcd(p^i, q^j) = 1$. In this case, $i = 0$. Otherwise, $i \neq 0$ and $0 :_R u = \langle p^i \rangle$. □

4.2 Embedding finitely generated torsion-free module in R^d

Lemma 4.1. *Every finitely generated torsion-free module M over an integral domain R can be embedded in a finite free R-module. More precisely, if $M \neq 0$, then there is an embedding $M \hookrightarrow R^d$ for some $d \geq 1$ such that the image of M intersects the standard coordinate axis of R^d.*

Proof. Let K be the fraction field of R and $u_1, \dots, u_n$ be a generating set for M as an R-module. We will show n is an upper bounded on the size of any R-linearly independent subset of M. Let $\varphi \colon R^n \to M$ be the linear map given by

$$\varphi(e_i) = u_i$$

for all $1 \leq i \leq n$. Let $v_1, \dots, v_k$ be linearly independent in M. Choose $\widetilde{v}_1, \dots, \widetilde{v}_k \in R^n$ such that

$$\varphi(\widetilde{v}_j) = v_j$$

for all $1 \leq j \leq k$. We claim that $\{\widetilde{v}_1, \dots, \widetilde{v}_k\}$ is linearly independent. Indeed, suppose

$$a_1 \widetilde{v}_1 + \cdots + a_k \widetilde{v}_k = 0 \tag{12}$$

for some $a_1, \dots, a_k \in R$. Then applying φ to both sides of (12) gives us

$$a_1 v_1 + \cdots + a_k v_k = 0$$

which implies $a_1 = \cdots = a_k = 0$ since $\{v_1, \dots, v_k\}$ is linearly independent. Therefore $\{\widetilde{v}_1, \dots, \widetilde{v}_k\}$ is linearly independent. In fact, we claim that $\{\widetilde{v}_1, \dots, \widetilde{v}_k\}$ is K-linearly independent in K^n. Indeed, suppose

$$x_1 \widetilde{v}_1 + \cdots + x_k \widetilde{v}_k = 0 \tag{13}$$

for some $x_1 \dots, x_k \in K$. Let $d \in R$ be the common denominator of $x_1, \dots, x_k$. Then multiplying d to both sides of (13) gives us

$$(dx_1)\widetilde{v}_1 + \cdots + (dx_k)\widetilde{v}_k = 0$$

which implies $dx_1 = \cdots = dx_k = 0$ since $\{\widetilde{v}_1, \dots, \widetilde{v}_k\}$ is R-linearly independent. This further implies $x_1 = \cdots = x_k = 0$ since $d \neq 0$ and R is an integral domain. Thus $\{\widetilde{v}_1, \dots, \widetilde{v}_k\}$ is K-linearly independent in K^n. Now it follows from linear algebra over fields that $k \leq n$.

From the bound $k \leq n$, there is a linearly independent subset of M with maximal size, say $w_1, \dots, w_d$. Then

$$\sum_{j=1}^{d} Rw_j \cong R^d.$$

We will find a scalar multiple of M inside of this. For any $u \in M$, the set $\{u, w_1, \dots, w_d\}$ is linearly independent by maximality of d, so there is a nontrivial relation

$$au + \sum_{i=1}^{d} a_i w_i = 0,$$

where $a, a_1, \dots, a_d \in R$, necessarily with $a \neq 0$. Thus

$$au \in \sum_{j=1}^{d} Rw_j.$$

In particular, for each $1 \leq i \leq n$, there exists a nonzero $a_i \in R$ such that

$$a_i u_i \in \sum_{j=1}^{d} Rw_j.$$

Setting $a = a_1 \cdots a_n$ and using the fact that R is an integral domain and M is torsion free, we see that

$$au_i \in \sum_{j=1}^{d} Rw_j$$

for all i. So $aM \subseteq \sum_{j=1}^{d} Rw_j$. Since R is an integral domain, multiplying by a is an isomorphism of M with aM, so we have the sequence of R-linear maps

$$\begin{aligned} M &\to aM \\ &\hookrightarrow \sum_{j=1}^{d} Rw_j \\ &\to R^d \end{aligned}$$

where the last map is an isomorphism. □

4.3 Submodules of a finite free module over a PID

Theorem 4.2. *When R is a PID, any submodule of a free R-module of rank n is free of rank $\leq n$.*

Proof. We may assume the free R-module is literally R^n and will induct on n. The case where $n = 1$ is true since R is a PID: every R-submodule of R is an ideal, hence of the form Ra since all ideals in R are principal, and $Ra \cong R$ as R-modules when $a \neq 0$ since R is an integral domain. Say $n \geq 1$ and the theorem is proved for R^n. Let $M \subseteq R^{n+1}$ be a submodule. We want to show M is free of rank $\leq n + 1$. View

$$M \subseteq R^{n+1} = R \oplus R^n$$

and let $\pi\colon R \oplus R^n \to R^n$ be the projection to the second component of this direct sum. Then

$$N = \pi(M) \subseteq R^n$$

is free of rank $\leq n$ by the induction hypothesis. Since π maps M onto N and N is free (and hence projective), we have

$$M \cong N \oplus \ker \pi|_M$$

and $\ker \pi|_M = M \cap (R \oplus 0)$. All submodules of $R \oplus 0 \cong R$ are free of rank ≤ 1. Thus $N \oplus \ker \pi|_M$ is free of rank $\leq n+1$, so M is as well. □

Remark. Using Zorn's Lemma, one can show that Theorem (4.2) holds for non-finitely generated free modules too: any submodule of a free module over a PID is free.

Corollary. *When R is a PID, every finitely generated torsion-free R-module is a finite free R-module.*

Proof. By Lemma (4.1), such a module embeds into a finite free R-module, so it is finite free too by Theorem (4.2). □

Corollary. *Let R be a PID. Let M, M', M'' be R-modules such that*

$$M'' \subseteq M' \subseteq M$$

and such that $M \cong R^n \cong M''$. Then $M' \cong R^n$.

Proof. Since M is free of rank n and M' is a submodule, Theorem (4.2) tells us that $M' \cong A^m$ with $m \leq n$. Using Theorem (4.2) again on M'' as a submodule of M', we see that $M'' \cong R^k$ with $k \leq m$. By hypothesis, $M'' \cong R^k$. Therefore $k = n$ since R is commutative and hence $m = n$. □

4.4 Finitely generated modules over PID is isomorphic to free + torsion

Corollary. *Let R be a PID and let M be a finitely generated R-module. Then*

$$M \cong F \oplus M_{\mathrm{tor}}$$

where F is free.

Proof. Observe that M/M_{tor} is torsion-free and finitely generated as an R-module. Indeed, it is torsion-free since if $au \in M_{\mathrm{tor}}$ for some $a \neq 0$, then $u \in M_{\mathrm{tor}}$ since R is an integral domain. It is finitely generated since it is the homomorphic image of a finitely generated module. Therefore by the previous theorem, M/M_{tor} is free. Therefore the short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & M_{\mathrm{tor}} \arrow[r] & M \arrow[r] & M/M_{\mathrm{tor}} \arrow[r] & 0 \end{tikzcd}$$

splits. Thus $M \cong F \oplus M_{\mathrm{tor}}$ where $F = M/M_{\mathrm{tor}}$ is free. □

Theorem 4.3. *Let R be a PID and let M be a torsion R-module. For any prime p in R, set*

$$\Gamma_p(M) = \bigcup_{k \geq 0} (0 :_M p^k) = \{u \in M \mid p^k u = 0 \text{ for some } k \geq 0\}.$$

Then

$$M \cong \bigoplus_{p \text{ prime}} \Gamma_p(M).$$

Furthermore, if M is finitely-generated, then $\Gamma_p(M) = 0$ for all but finitely many p.

Proof. Suppose $0 \neq a \in A$. Then there exists $0 \neq r \in R$ such that $ra = 0$. Write

$$r = p_1^{b_1} \cdots p_k^{b_k}.$$

Now observe that

$$\begin{gathered} (p_2^{b_2} p_3^{b_3} \cdots p_k^{b_k})a \in A_{p_2} \\ (p_1^{b_2} p_3^{b_3} \cdots p_k^{b_k})a \in A_{p_3} \\ \vdots \\ (p_1^{b_2} p_2^{b_3} \cdots p_{k-1}^{b_{k-1}})a \in A_{p_k} \end{gathered}$$

We claim that $a \in A_{p_1} + A_{p_2} \cdots + A_{p_k}$. Indeed,

$$\gcd(p_2^{b_2}p_3^{b_3}\cdots p_k^{b_k}, p_1^{b_2}p_3^{b_3}\cdots p_k^{b_k}, \dots, p_1^{b_2}p_2^{b_3}\cdots p_{k-1}^{b_{k-1}}) = 1.$$

Thus there exists $r_1, r_2, \dots, r_k$ such that

$$\sum r_i p_1^{b_1} \cdots \widehat{p_i^{b_i}} \cdots p_k^{b_k} = 1.$$

Therefore

$$\begin{aligned} a &= \sum r_i p_1^{b_1} \cdots \widehat{p_i^{b_i}} \cdots p_k^{b_k} a \\ &\in A_{p_1} + A_{p_2} \cdots + A_{p_k}. \end{aligned}$$

To see that the sum is direct, suppose $a \in A_p \cap \sum_{q \neq p} A_q$. Choose $k \in \mathbb{N}$ such that $p^k a = 0$ and choose $a_{q_i} \in A_{q_i}$ with $q_i^{k_i} a = 0$ such that

$$a = a_{q_1} + \cdots + a_{q_m}.$$

If $\alpha = \prod_{i=1}^m q_i^{k_i}$, then $p^k a = 0$ and $\alpha a = 0$. Since $\gcd(\alpha, p^k) = 1$, we see that a is killed by all of R. Thus $a = 0$ since $1 \in R$. □

4.5 Aligned Bases

There is a convenient way of picturing any submodule of a finite free module over a PID: bases can be chosen for the module and submodule that are aligned nicely, as follows.

Definition 4.2. Let R be a PID, let M be a finite free R-module, and let M' be a submodule of M. A basis $\{u_1, \dots, u_n\}$ of M and a basis $\{a_1 u_1, \dots, a_m u_m\}$ of M' with $a_i \in R \backslash \{0\}$ and $m \leq n$ is called a pair of **aligned** bases.

Theorem 4.4. *Any finite free R-module M of rank $n \geq 1$ and nonzero submodule M' of rank $m \leq n$ admit a pair of aligned bases: there is a basis $u_1, \dots, u_n$ of M and nonzero $a_1, \dots, a_m \in R$ such that*

$$M = \bigoplus_{i=1}^n R u_i \quad \textit{and} \quad M' = \bigoplus_{j=1}^m R a_j u_j.$$

Proof. Define S to be the set of ideals $\varphi(M')$ where $\varphi \colon M \to R$ is R-linear. This includes nonzero ideals; for example, let M have R-basis $\{e_1, \dots, e_n\}$. Choose any nonzero $u' \in M'$ and write

$$u' = a_1 e_1 + \cdots + a_n e_n.$$

Then since $u' \neq 0$, we must have $a_i \neq 0$ for some i, and so $e_i^\star(u') = a_i$ is nonzero. Hence $e_i^\star(M') \neq 0$.

Any nonzero ideal in R is contained in only finitely many ideals since R is a PID, so S contains maximal members with respect to inclusion. Call one of these maximal members Ra_1, so $a_1 \neq 0$. Thus $Ra_1 = \varphi_1(M')$ for some linear map $\varphi_1 \colon M \to R$. There exists some $v' \in M'$ such that

$$a_1 = \varphi_1(v').$$

Eventually we are going to show that φ_1 takes the value 1 on M.

We claim that for any linear map $\varphi \colon M \to R$, we have $a_1 \mid \varphi(v')$. To show this, set $\varphi(v') = a_\varphi \in R$. Since R is a PID, we have $Ra_1 + Ra_\varphi = Rd$ for some d, so $Ra_1 \subseteq Rd$. Then there exists $x, y \in R$ such that $d = xa_1 + ya_\varphi$. Thus

$$\begin{aligned} d &= xa_1 + ya_\varphi \\ &= x\varphi_1(v') + y\varphi(v') \\ &= (x\varphi_1 + y\varphi)(v'), \end{aligned}$$

and so $dR \subseteq (x\varphi_1 + y\varphi)(M') \in S$. Hence

$$\begin{aligned} \varphi_1(M') &= Ra_1 \\ &\subseteq Rd \\ &\subseteq (x\varphi_1 + y\varphi)(M'). \end{aligned}$$

Since $x\varphi_1 + y\varphi$ is a linear map $M \to R$, it belongs to S, so maximality of $\varphi_1(M')$ in S implies

$$\begin{aligned} \varphi_1(M') &= (x\varphi_1 + y\varphi)(M') \\ &= Rd. \end{aligned}$$

Hence

$$\begin{aligned} Ra_1 &= Rd \\ &= Ra_1 + Ra_\varphi, \end{aligned}$$

which implies $a_\varphi \in R$, and so $a_1 \mid a_\varphi$.

With the claim proved, we are ready to build aligned bases in M and M'. Letting $\{e_1, \ldots, e_n\}$ be a basis for M, we have

$$v' = c_1e_1 + \cdots + c_ne_n$$

for some $c_i \in R$. The ith coordinate function for this basis is a linear map $M \to R$ taking the value c_i at v', and so c_i is a multiple of a_1 by our claim. Writing $c_i = a_1b_i$, we have

$$\begin{aligned} v' &= \sum_{i=1}^{n} c_ie_i \\ &= \sum_{i=1}^{n} a_1b_ie_i \\ &= a_1\left(b_1e_1 + \cdots + b_ne_n\right) \\ &= a_1v_1, \end{aligned}$$

say. Then

$$\begin{aligned} a_1 &= \varphi_1(v') \\ &= \varphi_1(a_1v_1) \\ &= a_1\varphi_1(v_1), \end{aligned}$$

and so $\varphi_1(v_1) = 1$. We have found an element of M at which φ_1 takes the value 1.

The module M can be written as $Rv_1 + \ker\varphi_1$ since any $v \in M$

$$v = \varphi_1(v)v_1 + (v - \varphi_1(v))v_1.$$

Also $Rv_1 \cap \ker\varphi_1$. Thus $M = Rv_1 \oplus \ker\varphi_1$. Since M is free of rank n its submodule $\ker\varphi_1$ is free and necessarily of rank $n-1$.

How does M' fit in this decomposition of M? For any $w \in M'$ we have

$$w = \varphi_1(w)v_1 + (w - \varphi_1(w)v_1)$$

and the first term is

$$\begin{aligned} \varphi_1(w)v_1 &\in \varphi_1(M')v_1 \\ &= (Ra_1)v_1 \\ &= Ra_1v_1 \\ &= Rv' \\ &\subseteq M', \end{aligned}$$

so $w - \varphi_1(w)v_1 \in M'$ too. Therefore

$$M' = (M' \cap Rv_1) \oplus (M' \cap \ker\varphi_1).$$

So $M = Rv_1 \oplus \ker\varphi_1$ and $M' = Ra_1v_1 \oplus (M' \cap \ker\varphi_1)$. The last equation tells us $M' \cap \ker\varphi_1$ is free of rank $m-1$ since M' is free of rank m. If $m = 1$ then we're done. If $m > 1$, then we can describe how $M' \cap \ker\varphi_1$ sits in $\ker\varphi_1$ by induction on the rank: we have a basis $v_2, \ldots, v_n$ of $\ker\varphi_1$ and $a_2, \ldots, a_m \in R\backslash\{0\}$ such that $a_2v_2, \ldots, a_mv_m$ is a basis of $M' \cap \ker\varphi_1$. □

5 Tensor Products

5.1 Definition of Tensor Products via UMP

Definition 5.1. Let M and N be R-modules. The **tensor product** $M \otimes_R N$ is an R-module equipped with a bilinear map $\otimes\colon M \times N \to M \otimes_R N$ such that for each bilinear map $B\colon M \times N \to P$ there is a unique linear map $L\colon M \otimes_R N \to P$ making the following diagram commute.

$$\begin{tikzcd}
& M \otimes_R N \arrow[dd, dotted, "L"] \\
M \times N \arrow[ur, "\otimes"] \arrow[dr, "B"'] & \\
& P
\end{tikzcd}$$

Let R-modules T and T', and bilinear maps $b\colon M \times N \to T$ and $b'\colon M \times N \to T'$, satisfy the universal mapping property of the tensor product. From universality of $b\colon M \times N \to T$, the map $b'\colon M \times N \to T'$ factors uniquely through T: there exists a unique linear map $f\colon T \to T'$ making

$$\begin{tikzcd}
& T \arrow[dd, dotted, "f"] \\
M \times N \arrow[ur, "b"] \arrow[dr, "b'"'] & \\
& T'
\end{tikzcd} \tag{14}$$

commute. From universality of $b'\colon M \times N \to T'$, the map $b\colon M \times N \to T$ factors uniquely through T': there exists a unique linear map $f'\colon T' \to T$ making

$$\begin{tikzcd}
& T' \arrow[dd, dotted, "f'"] \\
M \times N \arrow[ur, "b'"] \arrow[dr, "b"'] & \\
& T
\end{tikzcd} \tag{15}$$

commute. We combine (16) and (15) into the commutative diagram

$$\begin{tikzcd}
& T \arrow[d, "f"] \\
M \times N \arrow[ur, "b"] \arrow[r, "b'"] \arrow[dr, "b"'] & T' \arrow[d, "f'"] \\
& T
\end{tikzcd} \tag{16}$$

Removing the middle, we have the commutative diagram

$$\begin{tikzcd}
& T \arrow[dd, "f' \circ f"] \\
M \times N \arrow[ur, "b"] \arrow[dr, "b"'] & \\
& T
\end{tikzcd} \tag{17}$$

From universality of (T, b), a unique linear map $T \to T$ fits in (17). The identity map works, so $f' \circ f = 1_T$. Similarly, $f \circ f' = 1_{T'}$ by stacking (16) and (15) in the other order. Thus T and T' are isomorphic R-modules by f and also $f \circ b = f'$, which means f identifies b with b'. So two tensor products of M and N can be identified with each other in a unique way compatible with the distinguished bilinear maps to them from $M \times N$.

5.2 Construction of Tensor Product

Theorem 5.1. *A tensor product of M and N exists.*

Proof. Consider $M \times N$ simply as a set. We form the free R-module on this set:

$$F_R(M \times N) = \bigoplus_{(u,v) \in M \times N} R\delta_{(u,v)}.$$

Let D be the submodule of $F_R(M \times N)$ □

5.3 The Covariant Functor $-\otimes_R N$

Proposition 5.1. *Let N be an R-module. We obtain a covariant functor*

$$-\otimes_R N \colon \mathbf{Mod}_R \to \mathbf{Mod}_R$$

from the category of R-modules to itself, where the R-module M is assigned to the R-module $M\otimes_R N$ and where the R-linear map $\varphi\colon M\to M'$ is assigned to the R-linear map $\varphi\otimes 1\colon M\otimes_R N\to M'\otimes_R N$, where $\varphi\otimes 1$ is defined by

$$(\varphi\otimes 1)(u\otimes v)=\varphi(u)\otimes v$$

for all elementary tensors $u\otimes v\in M\otimes_R N$.

Proof. We need to check that $-\otimes_R N$ preserves compositions and identities. We first check that it preserves compositions. Let $\varphi\colon M\to M'$ and $\varphi'\colon M'\to M''$ be two R-linear maps and let $u\otimes v$ be an elementary tensor in $M\otimes_R N$. Then

$$\begin{aligned}((\varphi'\otimes 1)(\varphi\otimes 1))(u\otimes v)&=(\varphi'\otimes 1)((\varphi\otimes 1)(u\otimes v))\\&=(\varphi'\otimes 1)(\varphi(u)\otimes v)\\&=(\varphi'(\varphi(u))\otimes v\\&=(\varphi'\varphi)(u)\otimes v\\&=(\varphi'\varphi\otimes 1)(u\otimes v).\end{aligned}$$

It follows that $(\varphi'\otimes 1)(\varphi\otimes 1)=\varphi'\varphi\otimes 1$. Hence $-\otimes_R N$ preserves compositions. Next we check that $-\otimes_R N$ preserves identities. Let M be an R-module and $u\otimes v$ be an elementary tensor in $M\otimes_R N$. Then we have

$$\begin{aligned}(1_M\otimes 1)(u\otimes v)&=1_M(u)\otimes v\\&=u\otimes v\\&=1_{M\otimes_R N}(u\otimes v).\end{aligned}$$

It follows that $1_M\otimes 1=1_{M\otimes_R N}$. Hence $-\otimes_R N$ preserves identities. □

5.3.1 Right Exactness of $-\otimes_R N$

Proposition 5.2. *The sequence of R-modules and R-linear maps*

$$M_1\xrightarrow{\varphi_1}M_2\xrightarrow{\varphi_2}M_3\longrightarrow 0 \tag{18}$$

is exact if and only if for all R-modules N the induced sequence

$$M_1\otimes_R N\xrightarrow{\varphi_1\otimes N}M_2\otimes_R N\xrightarrow{\varphi_2\otimes N}M_3\otimes_R N\longrightarrow 0 \tag{19}$$

is exact.

Proof. The sequence

$$M_1\otimes_R N\longrightarrow M_2\otimes_R N\longrightarrow M_3\otimes_R N\longrightarrow 0 \tag{20}$$

is exact for all R-modules N if and only if for all R-modules N and P the induced sequence

$$0\longrightarrow \mathrm{Hom}_R(M_3\otimes_R N,P)\longrightarrow \mathrm{Hom}_R(M_2\otimes_R N,P)\longrightarrow \mathrm{Hom}_R(M_1\otimes_R N,P) \tag{21}$$

is exact by Proposition (**??**). Then (21) is exact for all R-modules N and P if and only the sequence

$$0\to \mathrm{Hom}_R(M_3,\mathrm{Hom}_R(N,P))\to \mathrm{Hom}_R(M_2,\mathrm{Hom}_R(N,P))\to \mathrm{Hom}_R(M_1,\mathrm{Hom}_R(N,P)) \tag{22}$$

is exact for all R-modules N and P, by tensor-hom adjointness. Then (22) is exact for all R-modules N and P if and only if for all R-modules K

$$0\longrightarrow \mathrm{Hom}_R(M_3,K)\longrightarrow \mathrm{Hom}_R(M_2,K)\longrightarrow \mathrm{Hom}_R(M_1,K) \tag{23}$$

is exact since any R-module K is isomorphic to an R-module of the form $\mathrm{Hom}_R(N,P)$ (take $N=R$ and $P=K$) and because of naturality of Hom as in (7.5). Finally, (24) is exact if and only if

$$M_1\longrightarrow M_2\longrightarrow M_3\longrightarrow 0 \tag{24}$$

is exact again by Proposition (**??**). □

5.4 Tensor Product Properties

5.4.1 Tensor product of finitely presented R-modules is finitely presented

Proposition 5.3. *Let M be an N be finitely presented R-modules with presentations*

$$F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \to 0 \quad \text{and} \quad G_1 \xrightarrow{\psi_1} G_0 \xrightarrow{\psi_0} N \to 0.$$

Then

$$(F_1 \otimes_R G_0) \oplus (F_0 \otimes_R G_1) \xrightarrow{\phi_1} F_0 \otimes_R G_0 \xrightarrow{\phi_0} M \otimes_R N \to 0 \tag{25}$$

is a presentation of $M \otimes_R N$, where ϕ_0 is defined by

$$\phi_0(u_0 \otimes v_0) = \varphi_0(u_0) \otimes v_0 - u_0 \otimes \psi_0(v_0)$$

for all elementary tensors $u_0 \otimes v_0 \in F_0 \otimes_R G_0$, and where ϕ_1 is defined by

$$\phi_1(u_1 \otimes v_0) = \varphi_1(u_1) \otimes v_0 \quad \text{and} \quad \phi_1(u_0 \otimes v_1) = u_0 \otimes \psi_1(v_1)$$

for all $u_1 \otimes v_0 \in F_1 \otimes_R G_0$ and $u_0 \otimes v_1 \in F_0 \otimes_R G_1$.

Proof. The assignment

$$(u_0, v_0) \mapsto \varphi_0(u_0) \otimes v_0 - u_0 \otimes \psi_0(v_0)$$

is R-bilinear and thus ϕ_0 is a well-defined R-linear map. Similarly, the assignments

$$(u_1, v_0) \mapsto \varphi_0(u_0) \otimes v_0 \quad \text{and} \quad (u_0, v_1) \mapsto u_0 \otimes \psi_1(v_1)$$

are R-bilinear and thus ϕ_1 is a well-defined R-linear map. Let us check that (**??**) is exact. □

5.4.2 Tensor product commutes with direct sums

Proposition 5.4. *Let M be an R module and let $\{L_i\}$ be a collection of R-modules indexed over a set I. Then*

$$\left(\bigoplus_{i \in I} L_i\right) \otimes_R M \cong \bigoplus_{i \in I} (L_i \otimes_R M).$$

Proof. For all R-modules N, we have

$$\begin{aligned}
\mathrm{Hom}_R\left(\left(\bigoplus_{i \in I} L_i\right) \otimes_R M, N\right) &\cong \mathrm{Hom}_R\left(\bigoplus_{i \in I} L_i, \mathrm{Hom}_R(M, N)\right) \\
&\cong \prod_{i \in I} \mathrm{Hom}_R(L_i, \mathrm{Hom}_R(M, N)) \\
&\cong \prod_{i \in I} \mathrm{Hom}_R(L_i \otimes_R M, N) \\
&\cong \mathrm{Hom}_R\left(\bigoplus_{i \in I} (L_i \otimes_R M), N\right).
\end{aligned}$$

It follows that

$$\left(\bigoplus_{i \in I} L_i\right) \otimes_R M \cong \bigoplus_{i \in I} (L_i \otimes_R M).$$

□

5.5 Tensor-Hom Adjointness

Lemma 5.2. *Let B be an A-algebra, let M_1, M_2 be B-modules, and let M_3 be an A-module. Then we have an isomorphism of B-modules*

$$\mathrm{Hom}_B(M_1, \mathrm{Hom}_A(M_2, M_3)) \cong \mathrm{Hom}_A(M_1 \otimes_B M_2, M_3). \tag{26}$$

Moreover (26) is natural in M_1, M_2, and M_3.

Proof. We define

$$\Psi_{M_1,M_2,M_3}\colon \mathrm{Hom}_B(M_1,\mathrm{Hom}_A(M_2,M_3)) \to \mathrm{Hom}_A(M_1\otimes_B M_2, M_3)$$

to be the map which sends a $\psi \in \mathrm{Hom}_B(M_1,\mathrm{Hom}_A(M_2,M_3))$ to the map $\Psi(\psi)\in \mathrm{Hom}_A(M_1\otimes_B M_2, M_3)$ defined by

$$\Psi(\psi)(u_1\otimes u_2) = (\psi(u_1))(u_2) \tag{27}$$

for all elementary tensors $u_1\otimes u_2 \in M_1\otimes_B M_2$. Note that $\Psi(\psi)$ is a well-defined A-linear map since the map $M_1\times M_2\to M_3$ given by

$$(u_1,u_2)\mapsto (\psi(u_1))(u_2)$$

is A-bilinear. Indeed, let $a\in A$. Then we have

$$\begin{aligned}(\psi(au_1))(u_2) &= (a\psi(u_1))(u_2)\\ &= (\psi(u_1))(au_2)\\ &= a((\psi(u_1))(u_2))\end{aligned}$$

since both ψ and $\psi(u_1)$ are A-linear. Similarly, if $v_1\in M_1$, then

$$\begin{aligned}(\psi(u_1+v_1))(u_2) &= (\psi(u_1)+\psi(v_1))(u_2)\\ &= (\psi(u_1))(u_2)+(\psi(v_1))(u_2),\end{aligned}$$

and if $v_2\in M_2$, then

$$(\psi(u_1))(u_2+v_2) = (\psi(u_1))(u_2)+(\psi(u_1))(v_2).$$

Thus $\Psi(\psi)$ is a well-defined A-linear map.

Let us check that Ψ is B-linear. Let $b,b'\in B$ and $\psi,\psi'\in \mathrm{Hom}_B(M_1,\mathrm{Hom}_A(M_2,M_3))$. We want to show that

$$\Psi(b\psi+b'\psi') = b\Psi(\psi)+b'\Psi(\psi') \tag{28}$$

We will show (28) holds, by showing that the two maps agree on all elementary tensors in $M_1\otimes_B M_2$. So $u_1\otimes u_2\in M_1\otimes_B M_2$. Then

$$\begin{aligned}\Psi(b\psi+b'\psi')(u_1\otimes u_2) &= ((b\psi+b'\psi')(u_1))(u_2)\\ &= ((b\psi)(u_1)+(b'\psi')(u_1))(u_2)\\ &= (\psi(bu_1)+\psi(b'u_1))(u_2)\\ &= (\psi(bu_1))(u_2)+(\psi(b'u_1))(u_2)\\ &= \Psi(\psi)(bu_1\otimes u_2)+\Psi(\psi')(b'u_1\otimes u_2)\\ &= (b\Psi(\psi))(u_1\otimes u_2)+(b'\Psi(\psi'))(u_1\otimes u_2).\\ &= (b\Psi(\psi)+b'\Psi(\psi))(u_1\otimes u_2)\end{aligned}$$

It follows that Ψ is B-linear.

To show that Ψ is an isomorphism of B-modules, we construct its inverse. We define

$$\Phi_{M_1,M_2,M_3}\colon \mathrm{Hom}_A(M_1\otimes_B M_2,M_3)\to \mathrm{Hom}_B(M_1,\mathrm{Hom}_A(M_2,M_3))$$

to be the map given by

$$(\Phi(\varphi)(u_1))(u_2) = \varphi(u_1\otimes u_2)$$

for all $\varphi\in \mathrm{Hom}_A(M_1\otimes_B M_2,M_3)$, $u_1\in M_1$, and $u_2\in M_2$. We claim that Ψ and Φ are inverse to each other. Indeed, we have

$$\begin{aligned}\Psi(\Phi(\varphi))(u_1\otimes u_2) &= (\Phi(\varphi)(u_1))(u_2)\\ &= \varphi(u_1\otimes u_2)\end{aligned}$$

for all $\varphi\in\mathrm{Hom}_A(M_1\otimes_B M_2,M_3)$ and $u_1\otimes u_2\in M_1\otimes_B M_2$. Thus $\Psi\Phi=1$. Similarly, we have

$$\begin{aligned}(\Phi(\Psi(\psi))(u_1))(u_2) &= \Psi(\psi)(u_1\otimes u_2)\\ &= (\psi(u_1))(u_2)\end{aligned}$$

for all $\psi\in\mathrm{Hom}_B(M_1,\mathrm{Hom}_A(M_2,M_3))$ and $u_1\in M_1$ and $u_2\in M_2$. Thus $\Phi\Psi=1$.

Naturality in M_1 means that if $\lambda\colon M_1\to M_1'$ is an R-module homomorphism, then we have a commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}_S(M_1', \mathrm{Hom}_R(M_2, M_3)) \arrow[r, "\Psi_{M_1',M_3}"] \arrow[d, "\lambda^*"'] & \mathrm{Hom}_R(M_1' \otimes_S M_2, M_3) \arrow[d, "(\lambda\otimes 1)^*"] \\
\mathrm{Hom}_S(M_1, \mathrm{Hom}_R(M_2, M_3)) \arrow[r, "\Psi_{M_1,M_3}"'] & \mathrm{Hom}_R(M_1 \otimes_S M_2, M_3)
\end{tikzcd}$$

Thus we want to show for all $\psi \in \mathrm{Hom}_S(M_1', \mathrm{Hom}_R(M_2, M_3))$, we have

$$(\lambda \otimes 1)^* \left(\Psi_{M_1',M_3}(\psi)\right) = \Psi_{M_1,M_3}(\lambda^*(\psi)) \tag{29}$$

To see that (29) is equal, we apply all elementary tensors to both sides. Let $u_1 \otimes u_2 \in M_1 \otimes_S M_2$. Then we have

$$\begin{aligned}
\left((\lambda \otimes 1)^* \left(\Psi_{M_1',M_3}(\psi)\right)\right)(u_1 \otimes u_2) &= (\Psi_{M_1,M_3}(\psi))\,((\lambda \otimes 1)(u_1 \otimes u_2)) \\
&= (\Psi_{M_1,M_3}(\psi))\,(\lambda(u_1) \otimes u_2) \\
&= (\psi(\lambda(u_1))(u_2) \\
&= ((\lambda^*(\psi))(u_1))(u_2) \\
&= (\Psi_{M_1,M_3}(\lambda^*(\psi)))\,(u_1 \otimes u_2) \\
&= (\Psi_{M_1,M_3}(\lambda^*(\psi)))\,(u_1 \otimes u_2).
\end{aligned}$$

Similarly, naturality in M_3 means that if $\lambda \colon M_3 \to M_3'$ is an R-module homomorphism, then we have a commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}_S(M_1, \mathrm{Hom}_R(M_2, M_3)) \arrow[r, "\Psi_{M_1,M_3}"] \arrow[d, "(\lambda_*)_*"'] & \mathrm{Hom}_R(M_1 \otimes_S M_2, M_3) \arrow[d, "\lambda_*"] \\
\mathrm{Hom}_S(M_1, \mathrm{Hom}_R(M_2, M_3')) \arrow[r, "\Psi_{M_1,M_3'}"'] & \mathrm{Hom}_R(M_1 \otimes_S M_2, M_3')
\end{tikzcd}$$

Thus we want to show for all $\psi \in \mathrm{Hom}_S(M_1, \mathrm{Hom}_R(M_2, M_3))$, we have

$$\lambda_* \left(\Psi_{M_1,M_3}(\psi)\right) = \Psi_{M_1,M_3'}((\lambda_*)_*(\psi)) \tag{30}$$

To see that (30) is equal, we apply all elementary tensors to both sides. Let $u_1 \otimes u_2 \in M_1 \otimes_S M_2$. Then we have

$$\begin{aligned}
(\lambda_* \left(\Psi_{M_1,M_3}(\psi)\right))\,(u_1 \otimes u_2) &= \lambda\left((\Psi_{M_1,M_3}(\psi))\,(u_1 \otimes u_2)\right) \\
&= \lambda\left((\psi(u_1))(u_2)\right) \\
&= (\lambda_*(\psi(u_1)))(u_2) \\
&= ((\lambda_*)_*(\psi))(u_1))(u_2) \\
&= \left(\Psi_{M_1,M_3'}((\lambda_*)_*(\psi))\right)\,(u_1 \otimes u_2).
\end{aligned}$$

□

6 Localization

Throughout this section, all rings are assumed to be commutative. A notion of localization can still be defined for noncommutative rings, however we will not take this route.

6.1 Multiplicatively Closed Sets

Definition 6.1. Let R be a ring. A subset $S \subset R$ is called **multiplicatively closed** if $1 \in S$ and $s, t \in S$ implies $st \in S$.

Remark. One can also say that a subset $S \subset R$ is called multiplicatively closed if it is closed under products of elements, where the "empty product" is understood to be 1.

6.1.1 Examples of multiplicatively closed sets

Example 6.1. Let $\mathfrak{p} \subset R$ be a prime ideal. Then $R \setminus \mathfrak{p}$ is a multiplicatively closed set.

Example 6.2. Let R be a ring and let $a \in R$. Then the set $\{a^n \mid n \in \mathbb{Z}_{\geq 0}\}$ is a multiplicatively closed set.

Example 6.3. The set of all nonzero homogeneous polynomials in the polyomial ring $R[x_1, \dots, x_n]$ is a multiplicatively closed set.

6.1.2 Image of multiplicatively closed set is multiplicatively closed

Proposition 6.1. *Let $\varphi\colon A \to B$ be a ring homomorphism and let S be a multiplicatively closed subset of A. Then $\varphi(S)$ is a multiplicatively closed subset of B.*

Proof. Since φ is a ring homomorphism, it takes the identity to the identity, and so $1 \in \varphi(S)$. Also, if $\varphi(s), \varphi(t) \in \varphi(S)$, then

$$\begin{aligned} \varphi(s)\varphi(t) &= \varphi(st) \\ &\in \varphi(S). \end{aligned}$$

Thus $\varphi(S)$ is multiplicatively closed. □

6.1.3 Inverse image of multiplicatively closed set is multiplicatively closed

Proposition 6.2. *Let $\varphi\colon A \to B$ be a ring homomorphism and let T be a multiplicatively closed subset of B. Then $\varphi^{-1}(T)$ is a multiplicatively closed subset of A.*

Proof. Since φ is a ring homomorphism, it takes the identity to the identity, and so $1 \in \varphi^{-1}(T)$. Also, if $s, t \in \varphi^{-1}(T)$, then $\varphi(s), \varphi(t) \in T$, and so

$$\begin{aligned} \varphi(st) &= \varphi(s)\varphi(t) \\ &\in T \end{aligned}$$

implies $st \in \varphi^{-1}(T)$. Thus $\varphi^{-1}(T)$ is multiplicatively closed. □

6.2 Localization of ring with respect to multiplicatively closed set

Definition 6.2. We define the **localization of** R **with respect to** S, denoted R_S or $S^{-1}R$, as follows: as a set R_S is given by

$$R_S := \left\{ \frac{a}{s} \mid a \in R, s \in S \right\}$$

where a/s denotes the equivalence class of $(a, s) \in R \times S$ with respect to the following equivalence relation:

$$(a, s) \sim (a', s') \text{ if and only if there exists } s'' \in S \text{ such that } s''s'a = s''sa'. \tag{31}$$

We give R_S a ring structure by defining addition and multiplication on R_S by

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{s_2 a_1 + s_1 a_2}{s_1 s_2} \quad \text{and} \quad \frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2}, \tag{32}$$

for a_1/s_1 and a_2/s_2 in R_S, where $1/1$ serves as the multiplicative identity element in R_S and $0/0$ serves as the additive identity in R_S. The ring R_S comes equipped with a natural ring homomoprhism $\rho_S\colon R \to R_S$, given by

$$\rho_S(a) = \frac{a}{1}$$

for all $a \in R$.

Proposition 6.3. *With the notation as above, R_S is a ring. Furthermore, $\rho_S\colon R \to R_S$ is a ring homomorphism.*

Proof. There are several things we need to check. We will break this into steps

Step 1: We show that the relation (31) is in fact a equivalence relation. First we show reflexivity of $\sim$. Let $(a, s) \in R \times S$. Then since $1 \in S$ and $1 \cdot sa = 1 \cdot sa$, we have $(a, s) \sim (a, s)$. Next we show symmetry of $\sim$. Suppose $(a, s) \sim (a', s')$. Choose $s'' \in S$ such that $s''s'a = s''sa'$. Then by symmetry of equality, we have

$s''sa' = s''s'a$. Therefore $(a', s') \sim (a, s)$. Finally, we show transitivity of $\sim$. Suppose $(a_1, s_1) \sim (a_2, s_2)$ and $(a_2, s_2) \sim (a_3, s_3)$. Choose $s_{12}, s_{23} \in S$ such that

$$s_{12}s_2a_1 = s_{12}s_1a_2 \quad \text{and} \quad s_{23}s_3a_2 = s_{23}s_2a_3$$

Then $s_{23}s_{12}s_2 \in S$ and

$$\begin{aligned}(s_{23}s_{12}s_2)(s_3a_1) &= s_{23}(s_{12}s_2a_1)s_3 \\ &= s_{23}(s_{12}s_1a_2)s_3 \\ &= s_{12}s_1(s_{23}s_3a_2) \\ &= s_{12}s_1(s_{23}s_2a_3) \\ &= (s_{12}s_{23}s_2)(s_1a_3).\end{aligned}$$

Thus $\sim$ is in fact an equivalence relation.

Step 2: Addition and multiplication defined in (32) are well-defined. Suppose $a_1/s_1 = a'_1/s'_1$ and $a_2/s_2 = a'_2/s'_2$. Choose $s''_1, s''_2 \in S$ such that

$$s''_1s'_1a_1 = s''_1s_1a'_1 \quad \text{and} \quad s''_2s'_2a_2 = s''_2s_2a'_2.$$

Then $s''_1s''_2 \in S$ and

$$\begin{aligned}s''_1s''_2(s_2a_1 + s_1a_2)s'_1s'_2 &= s''_2s_2(s''_1s'_1a_1)s'_2 + s''_1s_1(s''_2s'_2a_2)s'_1 \\ &= s''_2s_2(s''_1s_1a'_1)s'_2 + s''_1s_1(s''_2s_2a'_2)s'_1 \\ &= s''_2s_2(s''_1s_1a'_1)s'_2 + s''_1s_1(s''_2s_2a'_2)s'_1 \\ &= s''_1s''_2(s'_2a'_1 + s'_1a'_2)s_1s_2\end{aligned}$$

implies

$$\frac{s_2a_1 + s_1a_2}{s_1s_2} = \frac{s'_2a'_1 + s'_1a'_2}{s'_1s'_2}.$$

Similarly, $s''_1s''_2$ and

$$\begin{aligned}s''_1s''_2a_1a_2s'_1s'_2 &= (s''_1s'_1a_1)(s''_2s'_2a_2) \\ &= (s''_1s_1a'_1)(s''_2s_2a'_2) \\ &= s''_1s''_2a'_1a'_2s_1s_2\end{aligned}$$

implies

$$\frac{a_1a_2}{s_1s_2} = \frac{a'_1a'_2}{s'_1s'_2}.$$

Thus we have shown that addition and multiplication in (32) are well-defined.

Step 3: Now we check that addition and multiplication in (32) gives us a ring structure. First let us show that addition in (32) gives us an abelian group with $0/1$ being the additive identity. We begin by checking associativity. Let $a_1/s_1, a_2/s_2, a_3/s_3 \in R_S$. Then

$$\begin{aligned}\left(\frac{a_1}{s_1} + \frac{a_2}{s_2}\right) + \frac{a_3}{s_3} &= \frac{s_2a_1 + s_1a_2}{s_1s_2} + \frac{a_3}{s_3} \\ &= \frac{s_3(s_2a_1 + s_1a_2) + (s_1s_2)a_3}{(s_1s_2)s_3} \\ &= \frac{s_3(s_2a_1) + s_3(s_1a_2) + (s_1s_2)a_3}{s_1(s_2s_3)} \\ &= \frac{(s_2s_3)a_1 + s_1(s_3a_2) + s_1(s_2a_3)}{s_1(s_2s_3)} \\ &= \frac{(s_2s_3)a_1 + s_1(s_3a_2 + s_2a_3)}{s_1(s_2s_3)} \\ &= \frac{a_1}{s_1} + \frac{s_3a_2 + s_2a_3}{s_2s_3} \\ &= \frac{a_1}{s_1} + \left(\frac{a_2}{s_2} + \frac{a_3}{s_3}\right).\end{aligned}$$

Thus addition in (32) is associative. Now we check commutativity. Let $a_1/s_1, a_2/s_2 \in R_S$. Then

$$\begin{aligned}\frac{a_1}{s_1}+\frac{a_2}{s_2} &= \frac{s_2a_1+s_1a_2}{s_1s_2}\\ &= \frac{s_1a_2+s_2a_1}{s_2s_1}\\ &= \frac{a_2}{s_2}+\frac{a_1}{s_1}.\end{aligned}$$

Thus addition in (32) is commutative. Now we check that $0/1$ is the identity. Let $a/s \in R_S$. Then

$$\begin{aligned}\frac{0}{1}+\frac{a}{s} &= \frac{s\cdot 0+1\cdot a}{1\cdot s}\\ &= \frac{0+a}{s}\\ &= \frac{a}{s}.\end{aligned}$$

Thus addition in (32) is commutative. Thus $0/1$ is the identity. Finally we check that every element has an inverse. Let $a/s \in R_S$. Then

$$\begin{aligned}\frac{a}{s}+\frac{-a}{s} &= \frac{a-a}{s}\\ &= \frac{0}{s}\\ &= \frac{0}{1}.\end{aligned}$$

implies $-a/s$ is the inverse to a/s. Therefore $(R_S,+)$ forms an abelian group with $0/1$ being identity element.

Now let us show that $(R_S,+,\cdot)$ is a ring. We first check that multiplication in (32) is associative. Let $a_1/s_1, a_2/s_2, a_3/s_3 \in R_S$. Then

$$\begin{aligned}\left(\frac{a_1}{s_1}\frac{a_2}{s_2}\right)\frac{a_3}{s_3} &= \frac{a_1a_2}{s_1s_2}\frac{a_3}{s_3}\\ &= \frac{(a_1a_2)a_3}{(s_1s_2)s_3}\\ &= \frac{a_1(a_2a_3)}{s_1(s_2s_3)}\\ &= \frac{a_1}{s_1}\frac{a_2a_3}{s_2s_3}\\ &= \frac{a_1}{s_1}\left(\frac{a_2}{s_2}\frac{a_3}{s_3}\right).\end{aligned}$$

Therefore multiplication in (32) is associative. Next we check that multiplication in (32) distributes over addition. Let $a_1/s_1, a_2/s_2, a_3/s_3 \in R_S$. Then

$$\begin{aligned}\frac{a_1}{s_1}\left(\frac{a_2}{s_2}+\frac{a_3}{s_3}\right) &= \frac{a_1}{s_1}\left(\frac{s_3a_2+s_2a_3}{s_2s_3}\right)\\ &= \frac{a_1(s_3a_2+s_2a_3)}{s_1s_2s_3}\\ &= \frac{a_1s_3a_2+a_1s_2a_3}{s_1s_2s_3}\\ &= \frac{s_3a_1a_2+s_2a_1a_3}{s_1s_2s_3}\\ &= \frac{s_3a_1a_2}{s_1s_2s_3}+\frac{s_2a_1a_3}{s_1s_2s_3}\\ &= \frac{a_1a_2}{s_1s_2}+\frac{a_1a_3}{s_1s_3}\\ &= \frac{a_1}{s_1}\frac{a_2}{s_2}+\frac{a_1}{s_1}\frac{a_3}{s_3}\end{aligned}$$

Thus multiplication in (32) distributes over addition. Finally, let us check that $1/1$ is the identity element in R_S under multplication. Let $a/s \in R_S$. Then

$$\begin{aligned}\frac{1}{1}\cdot\frac{a}{s} &= \frac{1\cdot a}{1\cdot s}\\ &= \frac{a}{s}.\end{aligned}$$

Thus $1/1$ is the identity element in R_S under multiplication.

Step 4: For the final step, we prove that $\rho_S \colon R \to R_S$ is a ring homomorphism. First note that it sends the identity to the identity. Next, let $a, b \in R$. Then

$$\begin{aligned}\rho_S(a+b) &= \frac{a+b}{1} \\ &= \frac{1 \cdot a + 1 \cdot b}{1 \cdot 1} \\ &= \frac{a}{1} + \frac{b}{1} \\ &= \rho_S(a) + \rho_S(b)\end{aligned}$$

and

$$\begin{aligned}\rho_S(ab) &= \frac{ab}{1} \\ &= \frac{ab}{1 \cdot 1} \\ &= \frac{a}{1} \cdot \frac{b}{1} \\ &= \rho_S(a)\rho_S(b).\end{aligned}$$

Thus ρ_S is a ring homomorphism. □

6.2.1 Universal Mapping Property of Localization

Proposition 6.4. *Let S be a multiplicatively closed subset of a ring A and let $\varphi \colon A \to B$ be a ring homomorphism such that $\varphi(S) \subseteq B^\times$. Then there exists a unique ring homomorphism $\widetilde{\varphi} \colon A_S \to B$ such that $\widetilde{\varphi}\rho_S = \varphi$.*

Proof. We define $\widetilde{\varphi} \colon A_S \to B$ by

$$\widetilde{\varphi}\left(\frac{a}{s}\right) = \varphi(a)\varphi(s)^{-1} \tag{33}$$

for all $a/s \in A_S$. We need to verify that (33) is well-defined. Suppose $a'/s' = a/s$. Choose $s'' \in S$ such that $s''sa' = s''s'a$. Then $\varphi(a') = \varphi(s'')\varphi(s')\varphi(s'')^{-1}\varphi(s)^{-1}\varphi(a)$ in B, and so

$$\begin{aligned}\widetilde{\varphi}\left(\frac{a'}{s'}\right) &= \varphi(a')\varphi(s')^{-1} \\ &= \varphi(s'')\varphi(s')\varphi(s'')^{-1}\varphi(s)^{-1}\varphi(a)\varphi(s')^{-1} \\ &= \varphi(a)\varphi(s)^{-1} \\ &= \widetilde{\varphi}\left(\frac{a}{s}\right).\end{aligned}$$

Thus (33) is well-defined. It is also easily seen to be a ring homomorphism which satisfies

$$\begin{aligned}(\widetilde{\varphi}\rho_S)(a) &= \widetilde{\varphi}(\rho_S(a)) \\ &= \widetilde{\varphi}\left(\frac{a}{1}\right) \\ &= \frac{\varphi(a)}{\varphi(1)} \\ &= \frac{\varphi(a)}{1} \\ &= \varphi(a).\end{aligned}$$

for all $a \in A$. Thus $\widetilde{\varphi}\rho_S = \varphi$. This shows existence.

For uniqueness, suppose $\widetilde{\varphi}$ and $\widetilde{\varphi}'$ are two such maps. Then we have

$$\begin{aligned}
\widetilde{\varphi}\left(\frac{a}{s}\right) &= \widetilde{\varphi}\left(\frac{1}{s}\cdot\frac{a}{1}\right) \\
&= \widetilde{\varphi}\left(\frac{1}{s}\right)\widetilde{\varphi}\left(\frac{a}{1}\right) \\
&= \left(\widetilde{\varphi}\left(\frac{s}{1}\right)\right)^{-1}\widetilde{\varphi}\left(\frac{a}{1}\right) \\
&= \left(\widetilde{\varphi}'\left(\frac{s}{1}\right)\right)^{-1}\widetilde{\varphi}'\left(\frac{a}{1}\right) \\
&= \widetilde{\varphi}'\left(\frac{1}{s}\right)\widetilde{\varphi}'\left(\frac{a}{1}\right) \\
&= \widetilde{\varphi}'\left(\frac{1}{s}\cdot\frac{a}{1}\right) \\
&= \widetilde{\varphi}'\left(\frac{a}{s}\right)
\end{aligned}$$

for all $a/s \in A_S$. Thus $\widetilde{\varphi} = \widetilde{\varphi}'$. □

6.2.2 Properties of ρ_S

Proposition 6.5. *Let S be a multiplicatively closed subset of R. Then*

1. *ρ_S is injective if and only if S does not contain any zero divisors;*
2. *ρ_S is an isomorphism if and only if S consists of units.*

Proof. 1. Suppose ρ_S is injective and assume for a contradiction that S contains a zero divisor, say $s \in S$ with $st = 0$ for some $t \in R\backslash\{0\}$. Then observe that $t \neq 0$ but $t/1 = 0$ since $st = 0$ where $s \in S$. This contradicts the fact that ρ_S is injective.

Conversely, suppose S does not contain any zero divisors and assume for a contradiction that ρ_S is not injective. Choose $t \in R\backslash\{0\}$ such that $1/t = 0$. Then there exists an $s \in S$ such that $st = 0$. This implies s is a zero divisor, which contradicts the fact that S does not contain any zero divisors.

2. By the universal mapping property of localization applied to the identity map $1_R \colon R \to R$, there exists a ring homomorphism $\psi\colon R_S \to R$ such that $\psi\rho_S = 1_R$. Applying the universal mapping property of localization to the map $\rho_S\colon R \to R_S$, we see that $1_{R_S}\colon R_S \to R_S$ is the *unique* homomorphism which satisfies $1_{R_S}\rho_S = \rho_S$, but observe that we also have

$$\begin{aligned}
(\rho_S\psi)\rho_S &= \rho_S(\psi\rho_S) \\
&= \rho_S 1_R \\
&= \rho_S.
\end{aligned}$$

Thus by uniqueness, we have $1_{R_S} = \rho_S\psi$. It follows that ρ_S is an isomorphism with ψ being its inverse. □

6.2.3 Prime Ideals in R_S

Recall that we denote by $\operatorname{Spec} R$ to be the set of all prime ideals in R. If S is a multiplicatively closed subset of R, then we can give a simple description of $\operatorname{Spec} R_S$ in terms of a subset of $\operatorname{Spec} R$.

Theorem 6.1. *Let S be a multiplicatively closed subset of R. Then we have a bijection*

$$\Psi\colon \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p}\cap S = \emptyset\} \to \operatorname{Spec} R_S$$

given by $\Psi(\mathfrak{p}) = \mathfrak{p}_S$ for all prime ideals $\mathfrak{p}$ in R such that $\mathfrak{p}\cap S = \emptyset$. Then inverse to Ψ, which we denote by

$$\Phi\colon \operatorname{Spec} R_S \to \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p}\cap S = \emptyset\}$$

is given by $\Phi(\mathfrak{q}) = \rho^{-1}(\mathfrak{q})$ for all prime ideals $\mathfrak{q}$ in R_S where $\rho\colon R \to R_S$ is the canonical localization map.

Proof. First note that both Ψ and Φ land in their designated target spaces. Indeed, for any prime ideal $\mathfrak{q}$ in $\operatorname{Spec} R_S$, the ideal $\rho^{-1}(\mathfrak{q})$ is easily seen to be prime in R. Also if $\mathfrak{p}$ is a prime ideal in R such that $\mathfrak{p}\cap S = \emptyset$, then $\mathfrak{p}_S$ is a prime ideal in R_S. Indeed, let $x/s, y/t \in \mathfrak{p}_S$, where $x, y \in \mathfrak{p}$ and $s, t \in S$, and suppose $(x/s)(y/t) \in \mathfrak{p}_S$.

Then $xy/st \in \mathfrak{p}_S$, which implies $xy \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime, we have either $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. Without loss of generality, say $x \in \mathfrak{p}$. Then clearly $x/s \in \mathfrak{p}_S$. This implies $\mathfrak{p}_S$ is prime.

We now want to show that these two maps are inverse to each other. First let us show that Ψ is injective. Let $\mathfrak{p}$ and $\mathfrak{p}'$ be two distinct primes in R such that $\mathfrak{p} \cap S = \mathfrak{p}' \cap S = \emptyset$. Without loss of generality, say $\mathfrak{p} \not\subseteq \mathfrak{p}'$. Choose $x \in \mathfrak{p} \backslash \mathfrak{p}'$. Then observe that $x/1 \in \mathfrak{p}_S$. Furthermore, we also have $x/1 \notin \mathfrak{p}'_S$. Indeed, assume for a contradiction $x/1 \in \mathfrak{p}'_S$. Then $x/1 = y/s$ with $y \in \mathfrak{p}'_S$ and $s \in S$. Then there exists $t \in S$ such that $tsx = ty \in \mathfrak{p}'$. As $\mathfrak{p}'$ is prime and $s, t \notin \mathfrak{p}'$, we must have $x \in \mathfrak{p}'$, which is a contradiction. This shows that $\mathfrak{p}_S$ and $\mathfrak{p}'_S$ are distinct, and hence Ψ is injective.

Now we will show Ψ is surjective. Let $\mathfrak{q} \in \operatorname{Spec} R_S$. We claim that $\mathfrak{q} = \rho^{-1}(\mathfrak{q})_S$. Indeed, we have

$$\begin{aligned}\rho^{-1}(\mathfrak{q})_S &= \{x/s \mid x \in \rho^{-1}(\mathfrak{q}) \text{ and } s \in S\} \\ &= \{x/s \mid x/1 \in \mathfrak{q} \text{ and } s \in S\} \\ &= \mathfrak{q},\end{aligned}$$

where equality in the last line follows from the fact that $\mathfrak{q}$ is prime: if $x/s \in \mathfrak{q}$, then $x/1 \in \mathfrak{q}$ since $1/s \notin \mathfrak{q}$ and $x/s = (x/1)(1/s)$. Thus Ψ is surjective and hence a bijection. In proving that Ψ is surjective, we also see that the inverse of Ψ is Φ. □

6.3 Localization of module with respect to multiplicatively closed set

Definition 6.3. Let S be a multiplicatively closed subset of R and let M be an R-module. We define the **localization of** M **with respect to** S, denoted M_S or $S^{-1}M$, as follows: as a set M_S is given by

$$M_S := \left\{ \frac{u}{s} \mid u \in M, s \in S \right\}$$

where u/s denotes the equivalence class of $(u,s) \in M \times S$ with respect to the following equivalence relation:

$$(u,s) \sim (u',s') \text{ if and only if there exists } s'' \in S \text{ such that } s''s'u = s''su'. \tag{34}$$

We give M_S an R_S-module structure by ring defining addition and scalar multiplication on M_S by

$$\frac{u_1}{s_1} + \frac{u_2}{s_2} = \frac{s_2u_1 + s_1u_2}{s_1s_2} \quad \text{and} \quad \frac{a}{s}\frac{u}{t} = \frac{au}{st}, \tag{35}$$

for $u_1/s_1, u_2/s_2, u/t \in M_S$ and $a/s \in R_S$, with $0/0$ being the additive identity in M_S.

Proposition 6.6. *With the notation above, M_S is an R_S-module. By restricting scalars via the ring the homomoprhism $\rho_S \colon R \to R_S$, it is also an R-module. More specifically, the R-module scalar multiplication is given by*

$$a \cdot \frac{u}{s} = \frac{au}{s}$$

for all $a \in R$ and $u/s \in M_S$.

Proof. The proof of this is similar to the proof of (6.3), but we include it here for completeness. Again, there are several things we need to check, so we break it up into steps.

Step 1: We show that the relation (31) is in fact a equivalence relation. First we show reflexivity of $\sim$. Let $(u,s) \in M \times S$. Then since $1 \in S$ and $1 \cdot su = 1 \cdot su$, we have $(u,s) \sim (u,s)$. Next we show symmetry of $\sim$. Suppose $(u,s) \sim (u',s')$. Choose $s'' \in S$ such that $s''s'u = s''su'$. Then by symmetry of equality, we have $s''su' = s''s'u$. Therefore $(u',s') \sim (u,s)$. Finally, we show transitivity of $\sim$. Suppose $(u_1,s_1) \sim (u_2,s_2)$ and $(u_2,s_2) \sim (u_3,s_3)$. Choose $s_{12}, s_{23} \in S$ such that

$$s_{12}s_2u_1 = s_{12}s_1u_2 \quad \text{and} \quad s_{23}s_3u_2 = s_{23}s_2u_3$$

Then $s_{23}s_{12}s_2 \in S$ and

$$\begin{aligned}(s_{23}s_{12}s_2)(s_3u_1) &= s_{23}(s_{12}s_2u_1)s_3 \\ &= s_{23}(s_{12}s_1u_2)s_3 \\ &= s_{12}s_1(s_{23}s_3u_2) \\ &= s_{12}s_1(s_{23}s_2u_3) \\ &= (s_{12}s_{23}s_2)(s_1u_3).\end{aligned}$$

Thus $\sim$ is in fact an equivalence relation.

Step 2: Addition and multiplication in (35) are well-defined. Suppose $u_1/s_1 = u_1'/s_1'$ and $u_2/s_2 = u_2'/s_2'$. Choose $s_1'', s_2'' \in S$ such that

$$s_1''s_1'u_1 = s_1''s_1u_1' \quad \text{and} \quad s_2''s_2'u_2 = s_2''s_2u_2'.$$

Then $s_1''s_2'' \in S$ and

$$\begin{aligned} s_1''s_2''(s_2u_1 + s_1u_2)s_1's_2' &= s_2''s_2(s_1''s_1'u_1)s_2' + s_1''s_1(s_2''s_2'u_2)s_1' \\ &= s_2''s_2(s_1''s_1u_1')s_2' + s_1''s_1(s_2''s_2u_2')s_1' \\ &= s_2''s_2(s_1''s_1u_1')s_2' + s_1''s_1(s_2''s_2u_2')s_1' \\ &= s_1''s_2''(s_2'u_1' + s_1'u_2')s_1s_2 \end{aligned}$$

implies

$$\frac{s_2u_1 + s_1u_2}{s_1s_2} = \frac{s_2'u_1' + s_1'u_2'}{s_1's_2'}.$$

Similarly, $s_1''s_2'' \in S$ and

$$\begin{aligned} s_1''s_2''u_1u_2s_1's_2' &= (s_1''s_1'u_1)(s_2''s_2'u_2) \\ &= (s_1''s_1u_1')(s_2''s_2u_2') \\ &= s_1''s_2''u_1'u_2's_1s_2 \end{aligned}$$

implies

$$\frac{a_1a_2}{s_1s_2} = \frac{a_1'a_2'}{s_1's_2'}.$$

Thus we have shown that addition and scalar multiplication in (35) are well-defined.

Step 3: Now we show that addition and multiplication in (35) gives us an R_S-module structure. First let us show that addition in (35) gives us an abelian group with $0/1$ being the additive identity. We begin by checking associativity. Let $u_1/s_1, u_2/s_2, u_3/s_3 \in M_S$. Then

$$\begin{aligned} \left(\frac{u_1}{s_1} + \frac{u_2}{s_2}\right) + \frac{u_3}{s_3} &= \frac{s_2u_1 + s_1u_2}{s_1s_2} + \frac{u_3}{s_3} \\ &= \frac{s_3(s_2u_1 + s_1u_2) + (s_1s_2)u_3}{(s_1s_2)s_3} \\ &= \frac{s_3(s_2u_1) + s_3(s_1u_2) + (s_1s_2)u_3}{s_1(s_2s_3)} \\ &= \frac{(s_2s_3)u_1 + s_1(s_3u_2) + s_1(s_2u_3)}{s_1(s_2s_3)} \\ &= \frac{(s_2s_3)u_1 + s_1(s_3u_2 + s_2u_3)}{s_1(s_2s_3)} \\ &= \frac{u_1}{s_1} + \frac{s_3u_2 + s_2u_3}{s_2s_3} \\ &= \frac{u_1}{s_1} + \left(\frac{u_2}{s_2} + \frac{u_3}{s_3}\right). \end{aligned}$$

Thus addition in (35) is associative. Now we check commutativity. Let $u_1/s_1, u_2/s_2 \in M_S$. Then

$$\begin{aligned} \frac{u_1}{s_1} + \frac{u_2}{s_2} &= \frac{s_2u_1 + s_1u_2}{s_1s_2} \\ &= \frac{s_1u_2 + s_2u_1}{s_2s_1} \\ &= \frac{u_2}{s_2} + \frac{u_1}{s_1}. \end{aligned}$$

Thus addition in (35) is commutative. Now we check that $0/1$ is the identity. Let $u/s \in M_S$. Then

$$\begin{aligned} \frac{0}{1} + \frac{u}{s} &= \frac{s \cdot 0 + 1 \cdot u}{1 \cdot s} \\ &= \frac{0 + u}{s} \\ &= \frac{u}{s}. \end{aligned}$$

Thus $0/1$ is the identity. Finally we check that every element has an inverse. Let $u/s \in M_S$. Then

$$\begin{aligned}\frac{u}{s}+\frac{-u}{s} &= \frac{u-u}{s} \\ &= \frac{0}{s} \\ &= \frac{0}{1}.\end{aligned}$$

implies $-u/s$ is the inverse to u/s. Therefore $(M_S, +)$ forms an abelian group with $0/1$ being the identity element.

Now let us show that $(M_S, +, \cdot)$ is an R_S-module. We first check that scalar multiplication in (35) is associative. Let $a_1/s_1, a_2/s_2 \in R_S$ and let $u/s \in M_S$. Then

$$\begin{aligned}\left(\frac{a_1}{s_1}\frac{a_2}{s_2}\right)\frac{u}{s} &= \frac{a_1a_2}{s_1s_2}\frac{u}{s} \\ &= \frac{(a_1a_2)u}{(s_1s_2)s} \\ &= \frac{a_1(a_2u)}{s_1(s_2s)} \\ &= \frac{a_1}{s_1}\frac{a_2u}{s_2s} \\ &= \frac{a_1}{s_1}\left(\frac{a_2}{s_2}\frac{u}{s}\right).\end{aligned}$$

Therefore scalar multiplication in (35) is associative. Next we check that scalar multiplication in (35) distributes over addition. Let $a/s \in R_S$ and $u_1/s_1, u_2/s_2 \in M_S$. Then

$$\begin{aligned}\frac{a}{s}\left(\frac{u_1}{s_1}+\frac{u_2}{s_2}\right) &= \frac{a}{s}\left(\frac{s_2u_1+s_1u_2}{s_1s_2}\right) \\ &= \frac{a(s_2u_1+s_1u_2)}{ss_1s_2} \\ &= \frac{as_2u_1+as_1u_2}{ss_1s_2} \\ &= \frac{s_2au_1+sau_2}{ss_1s_2} \\ &= \frac{s_2au_1}{ss_1s_2}+\frac{sau_2}{ss_1s_2} \\ &= \frac{au_1}{ss_1}+\frac{au_2}{ss_2} \\ &= \frac{a}{s}\frac{u_1}{s_1}+\frac{a}{s}\frac{u_2}{s_2}.\end{aligned}$$

Similarly, let $a_1/s_1, a_2/s_2 \in R_S$ and $u/s \in M_S$. Then

$$\begin{aligned}\left(\frac{a_1}{s_1}+\frac{a_2}{s_2}\right)\frac{u}{s} &= \left(\frac{s_2a_1+s_1a_2}{s_1s_2}\right)\frac{u}{s} \\ &= \frac{(s_2a_1+s_1a_2)u}{s_1s_2s} \\ &= \frac{s_2a_1u+s_1a_2u}{s_1s_2s} \\ &= \frac{s_2a_1u+s_1a_2u}{s_2s_1s} \\ &= \frac{s_2a_1u}{s_2s_1s}+\frac{s_1a_2u}{s_1s_2s} \\ &= \frac{a_1u}{s_1s}+\frac{a_2u}{s_2s} \\ &= \frac{a_1}{s_1}\frac{u}{s}+\frac{a_2}{s_2}\frac{u}{s}.\end{aligned}$$

Thus multiplication in (35) distributes over addition. Finally, let us check that $1/1$ fixes M_S. Let $u/s \in M_S$. Then

$$\begin{aligned}\frac{1}{1}\cdot\frac{u}{s} &= \frac{1\cdot u}{1\cdot s} \\ &= \frac{u}{s}.\end{aligned}$$

Thus $1/1$ fixes M_S. □

6.4 Localization as a functor

Proposition 6.7. *Let S be a multiplicatively closed subset of R. We obtained a functor*

$$-_S \colon \mathbf{Mod}_R \to \mathbf{Mod}_{R_S}$$

*called **localization** where an R-module M is mapped to the R_S-module M_S and where the R-linear map $\varphi \colon M \to N$ is mapped to the R_S-linear map $\varphi_S \colon M_S \to N_S$ given by*

$$\varphi_S\left(\frac{u}{s}\right) = \frac{\varphi(u)}{s} \tag{36}$$

for all $u/s \in M_S$.

Proof. We first check that (36) is well-defined. Suppose $u/s = u'/s'$. Choose $s'' \in S$ such that $s''s'u = s''su'$. Then $s''s'\varphi(u) = s''s\varphi(u')$ by R-linearity of φ, and hence $\varphi(u)/s = \varphi(u')/s'$. Thus (36) is well-defined.

Now let us check that φ_S is an R_S-linear map. Let $a_1/s_1, a_2/s_2 \in R_S$ and let $u_1/t_1, u_2/t_2 \in M_S$. Then

$$\begin{aligned}
\varphi_S\left(\frac{a_1}{s_1}\frac{u_1}{t_1} + \frac{a_2}{s_2}\frac{u_2}{t_2}\right) &= \varphi_S\left(\frac{s_2t_2a_1u_1 + s_1t_1a_2u_2}{s_1t_1s_2t_2}\right) \\
&= \frac{\varphi(s_2t_2a_1u_1 + s_1t_1a_2u_2)}{s_1t_1s_2t_2} \\
&= \frac{s_2t_2a_1\varphi(u_1) + s_1t_1a_2\varphi(u_2)}{s_1t_1s_2t_2} \\
&= \frac{a_1}{s_1}\frac{\varphi(u_1)}{t_1} + \frac{a_2}{s_2}\frac{\varphi(u_2)}{t_2} \\
&== \frac{a_1}{s_1}\varphi_S\left(\frac{u_1}{t_1}\right) + \frac{a_2}{s_2}\varphi_S\left(\frac{u_2}{t_2}\right).
\end{aligned}$$

Thus φ_S is an R_S-linear map.

Now to see that $-_S$ is a functor, we need to check that it preserves identities and compositions. First we show it preserves identities. Let M be an R-module. Then

$$\begin{aligned}
(1_M)_S\left(\frac{u}{s}\right) &= \frac{1_M(u)}{s} \\
&= \frac{u}{s} \\
&= 1_{M_S}\left(\frac{u}{s}\right)
\end{aligned}$$

for all $u/s \in M_S$. Thus $(1_M)_S = 1_{M_S}$, and hence $-_S$ preserves identities. Next we show it preserves compositions. Let $\varphi \colon M \to M'$ and $\varphi' \colon M' \to M''$ be two R-linear maps. Then

$$\begin{aligned}
(\varphi'\varphi)_S\left(\frac{u}{s}\right) &= \frac{(\varphi'\varphi)(u)}{s} \\
&= \frac{\varphi'(\varphi(u))}{s} \\
&= \varphi'_S\left(\frac{\varphi(u)}{s}\right) \\
&= \varphi'_S\left(\varphi_S\left(\frac{u}{s}\right)\right) \\
&= (\varphi'_S\varphi_S)\left(\frac{u}{s}\right)
\end{aligned}$$

for all $u/s \in M_S$. Thus $(\varphi'\varphi)_S = \varphi'_S\varphi_S$, and hence $-_S$ preserves compositions. □

6.4.1 Natural isomorphism between functors $R_S \otimes_R -$ and $-_S$

Lemma 6.2. *Let N be an R-module. Every element in $R_S \otimes_R N$ can be expressed as an elementary tensor of the form $(1/s) \otimes v$ with $s \in S$ and $v \in N$.*

Proof. Let $\sum_{i=1}^{n}(a_i/s_i)\otimes v_i$ be a general tensor in $R_S\otimes_R N$. Then

$$\begin{aligned}\frac{a_1}{s_1}\otimes v_1+\cdots+\frac{a_n}{s_n}\otimes v_n &= \frac{a_1s_2\cdots s_n}{s_1s_2\cdots s_n}\otimes v_1+\cdots+\frac{s_1s_2\cdots a_n}{s_1s_2\cdots s_n}\otimes v_n\\ &= \frac{1}{s_1s_2\cdots s_n}\otimes a_1s_2\cdots s_nv_1+\cdots+\frac{1}{s_1s_2\cdots s_n}\otimes s_1s_2\cdots a_nv_n\\ &= \frac{1}{s_1s_2\cdots s_n}\otimes(a_1s_2\cdots s_nv_1+\cdots+s_1s_2\cdots a_nv_n)\\ &= \frac{1}{s}\otimes v,\end{aligned}$$

where $s=s_1s_2\cdots s_n$ and $v=a_1s_2\cdots s_nv_1+\cdots+s_1s_2\cdots a_nv_n$. □

Proposition 6.8. *Let S be a multiplicatively closed subset of R. Then we have a natural isomorphism between functors*

$$R_S\otimes_R -\colon \mathbf{Mod}_R\to\mathbf{Mod}_{R_S}\quad\textit{and}\quad -_S\colon\mathbf{Mod}_R\to\mathbf{Mod}_{R_S}$$

Proof. For each R-module M, we define $\eta_M\colon R_S\otimes_R M\to M_S$ by

$$\eta_M\left(\frac{1}{s}\otimes u\right)=\frac{u}{s}$$

for all $(1/s)\otimes u\in R_S\otimes_R M$. By Lemma (6.2), every tensor in $R_S\otimes_R M$ can be expressed as an elementary tensor of the form $(1/s)\otimes u$, and so η_M really is defined on all of $R_S\otimes_R M$. Also η_M is a well-defined R-linear map since the map $R_S\times M\to M_S$ given by

$$\left(\frac{1}{s},u\right)\mapsto\frac{u}{s}$$

is readily seen to be R-bilinear. The map η_M is surjective since every element in M_S can be expressed in the form u/s. Let us show that η_M is injective. Suppose $(1/s)\otimes u\in\ker\eta_M$. Then $u/s=0/1$. Then exists a $t\in S$ such that

$$\begin{aligned}tu&=t\cdot 1\cdot u\\&=t\cdot s\cdot 0\\&=0.\end{aligned}$$

This implies

$$\begin{aligned}\frac{1}{s}\otimes u&=\frac{t}{st}\otimes u\\&=\frac{1}{st}\otimes tu\\&=\frac{1}{st}\otimes 0\\&=0.\end{aligned}$$

Thus η_M is injective, and hence an isomorphism.

Now we will show that η is a natural transformation. Let $\varphi\colon M\to N$ be an R-linear map. We need to show that the diagram below commutes

$$\begin{tikzcd} R_S\otimes_R M \arrow[r, "\eta_M"] \arrow[d, "1\otimes\varphi"'] & M_S \arrow[d, "\varphi_S"] \\ R_S\otimes_R N \arrow[r, "\eta_N"'] & N_S \end{tikzcd} \tag{37}$$

Let $(1/s) \otimes u \in R_S \otimes_R M$. Then

$$\begin{aligned}(\varphi_S \eta_M)\left(\frac{1}{s} \otimes u\right) &= \varphi_S\left(\eta_M\left(\frac{1}{s} \otimes u\right)\right)\\ &= \varphi_S\left(\frac{u}{s}\right)\\ &= \frac{\varphi(u)}{s}\\ &= \eta_N\left(\frac{1}{s} \otimes \varphi(u)\right)\\ &= \eta_N\left((1 \otimes \varphi)\left(\frac{1}{s} \otimes u\right)\right)\\ &= (\eta_N(1 \otimes \varphi))\left(\frac{1}{s} \otimes u\right).\end{aligned}$$

Therefore the diagram (37) commutes. □

6.4.2 Localization is Essentially Surjective

Proposition 6.9. *Let S be a multiplicatively closed subset of R. Then the localization functor $-_S$ is essentially surjective.*

Proof. Let M be an R_S-module. Then M is also an R-module via the action

$$a \cdot u = \frac{a}{1} \cdot u$$

for all $a \in R$ and $u \in M$. Then $R_S \otimes_R M$ is an R_S-module via the action

$$\frac{a}{s} \cdot \left(\frac{b}{t} \otimes u\right) = \frac{ab}{st} \otimes u$$

for all a/s and b/t in R_S and for all $u \in M$. We claim that M is isomorphic to $R_S \otimes_R M$ as R_S-modules. Indeed, let $\varphi \colon R_S \otimes_R M \to M$ be given by

$$\varphi\left(\frac{1}{s} \otimes u\right) = \frac{1}{s} \cdot u$$

for all $(1/s) \otimes u \in R_S \otimes M$. This map is well-defined and R-linear since the corresponding map $R_S \times M \to M$, given by

$$\left(\frac{a}{s}, u\right) \mapsto \frac{a}{s} \cdot u$$

is R-bilinear. This map is injective since if $(1/s) \cdot u = 0$, then $u = 0$, which implies $(1/s) \otimes u = 0$. Finally, the map is surjective since if $u \in M$, then $\varphi((1/1) \otimes u) = u$. Therefore localization is essentially surjective since $M_S \cong R_S \otimes_R M$. □

6.5 Properties of Localization

The following proposition is used quite often:

Proposition 6.10. *Let N be an R-mdoule and let L and M be R-submodules of N. The following are equivalent:*

1. *$L = M$;*
2. *$L_{\mathfrak{p}} = M_{\mathfrak{p}}$ for all prime ideals $\mathfrak{p} \subseteq R$;*
3. *$L_{\mathfrak{m}} = M_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m} \subseteq R$.*

Proof. That 1 implies 2 and that 2 implies 3 are obvious. So it suffices to show 3 implies 1. First we show $M \subseteq L$. Let $u \in M$. If $L :_R u = R$, then $u \in L$ (since $1 \cdot u \in L$). Otherwise $L :_R u$ is contained in some maximal ideal $\mathfrak{m}$. Then observe that $u/1 \notin L_{\mathfrak{m}}$. Indeed, we have $u/1 \in L_{\mathfrak{m}}$ if and only if there exists an $s \in R \backslash \mathfrak{m}$ such that $su \in L$, but since $\mathfrak{m}$ is the set of all such s, we see that $u/1 \notin L_{\mathfrak{m}}$. This contradicts the fact that $M_{\mathfrak{m}} = L_{\mathfrak{m}}$. Thus we must have $L :_R u = R$, which implies $u \in L$. Thus $M \subseteq L$. The reverse inclusion is proved similarly. □

6.5.1 Localization Commutes with Arbitrary Sums, Finite Intersections, and Radicals

Proposition 6.11. *Let $S \subseteq R$ be a multiplicative set, let M be an R-modules, and let $\{M_\lambda\}$ be a collection of R-submodules of M indexed over a set Λ. Then*

1. *Localization commutes with arbitrary sums: $(\sum_{\lambda \in \Lambda} M_\lambda)_S = \sum_{\lambda \in \Lambda} (M_\lambda)_S$.*
2. *Localization commutes with finite intersections: if $\Lambda = \{1, \dots, n\}$ is finite, then $(\bigcap_{i=1}^n M_i)_S = \bigcap_{i=1}^n (M_i)_S$.*
3. *Localization commutes with radicals: let $I \subseteq R$ be an ideal. Then $(\sqrt{I})_S = \sqrt{I_S}$.*

Proof.
1. Let $u/s \in (\sum_{\lambda \in \Lambda} M_\lambda)_S$. So $s \in S$ and $u \in \sum_{\lambda \in \Lambda} M_\lambda$, which means we can express it in the form

$$u = u_{\lambda_1} + \cdots + u_{\lambda_n}$$

where $u_{\lambda_i} \in M_{\lambda_i}$ for all $1 \leq i \leq n$. Then

$$\begin{aligned} \frac{u}{s} &= \frac{u_{\lambda_1} + \cdots + u_{\lambda_n}}{s} \\ &= \frac{u_{\lambda_1}}{s} + \cdots + \frac{u_{\lambda_n}}{s} \\ &\in \sum_{\lambda \in \Lambda} (M_\lambda)_S. \end{aligned}$$

Therefore $(\sum_{\lambda \in \Lambda} M_\lambda)_S \subseteq \sum_{\lambda \in \Lambda} (M_\lambda)_S$.

Conversely, suppose $\sum_{i=1}^n u_{\lambda_i}/s_{\lambda_i} \in \sum_{\lambda \in \Lambda} (M_\lambda)_S$ where $u_{\lambda_i} \in M_{\lambda_i}$ and $s_{\lambda_i} \in S$ for all $1 \leq i \leq n$. Then

$$\begin{aligned} \sum_{i=1}^n \frac{u_{\lambda_i}}{s_{\lambda_i}} &= \sum_{i=1}^n \frac{s_{\lambda_1} \cdots s_{\lambda_{i-1}} u_{\lambda_i} s_{\lambda_{i+1}} \cdots s_{\lambda_{jn}}}{s_{\lambda_1} \cdots s_{\lambda_n}} \\ &= \frac{1}{s_{\lambda_1} \cdots s_{\lambda_n}} \sum_{i=1}^n s_{\lambda_1} \cdots s_{\lambda_{i-1}} u_{\lambda_i} s_{\lambda_{i+1}} \cdots s_{\lambda_{jn}} \\ &\in \left(\sum_{\lambda \in \Lambda} M_\lambda \right)_S. \end{aligned}$$

Therefore $(\sum_{\lambda \in \Lambda} M_\lambda)_S \supseteq \sum_{\lambda \in \Lambda} (M_\lambda)_S$.

2. Let $u/s \in (\bigcap_{i=1}^n M_i)_S$. So $u \in \bigcap_{i=1}^n M_i$ and $s \in S$. This means $u \in M_i$ for all $1 \leq i \leq n$. Thus $u/s \in \bigcap_{i=1}^n (M_i)_S$. This implies $(\bigcap_{i=1}^n M_i)_S \subseteq \bigcap_{i=1}^n (M_i)_S$.

Conversely, let $u/s \in \bigcap_{i=1}^n (M_i)_S$. Then $u/s = u_i/s_i$ where $u_i \in M_i$ and $s_i \in S$ for all $1 \leq i \leq n$. For each $1 \leq i \leq n$, choose $s_i' \in S$ such that $s_i' s_i u = s_i' s u_i$. Then

$$\begin{aligned} \frac{u}{s} &= \frac{s_1' s_1 \cdots s_n' s_n u}{s_1' s_1 \cdots s_n' s_n s} \\ &\in \left(\bigcap_{i=1}^n M_i \right)_S. \end{aligned}$$

This implies $(\bigcap_{i=1}^n M_i)_S \supseteq \bigcap_{i=1}^n (M_i)_S$.

3. Let $x/s \in (\sqrt{I})_S$. Then $s \in S$ and $x \in \sqrt{I}$, which means $x^n \in I$ for some $n \in \mathbb{N}$. Then

$$\begin{aligned} \left(\frac{x}{s} \right)^n &= \frac{x^n}{s^n} \\ &\in I_S \end{aligned}$$

which implies $x/s \in \sqrt{I_S}$. Therefore $(\sqrt{I})_S \subseteq \sqrt{I_S}$.

Conversely, let $x/s \in \sqrt{I_S}$. Then $(x/s)^n \in I_S$ for some $n \in \mathbb{N}$. So $x^n \in I$, which implies $x \in \sqrt{I}$. Therefore $(\sqrt{I})_S \supseteq \sqrt{I_S}$. □

6.6 Total Ring of Fractions

Definition 6.4. Let A be a ring and let S be the set of all nonzerodivisors in A. We define the **total ring of fractions** of A to be $Q(A) := S^{-1}A$.

Proposition 6.12. *Let A be a ring and $B = A/(\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r)$ with $\mathfrak{p}_i \subset A$ prime ideals. Then*

$$Q(B) \cong \bigoplus_{i=1}^{r} Q(A/\mathfrak{p}_i).$$

In particular, $Q(B)$ is a direct sum of fields.

Proof. Let $S = A\backslash(\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r)$. Then

$$\begin{aligned} S^{-1}B &= S^{-1}\left(A/(\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r)\right) \\ &\cong S^{-1}A/S^{-1}(\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r) \\ &= S^{-1}A/(S^{-1}\mathfrak{p}_1 \cap \cdots \cap S^{-1}\mathfrak{p}_r) \\ &\cong \bigoplus_{i=1}^{r}\left(S^{-1}A/S^{-1}\mathfrak{p}_i\right) \\ &\cong \bigoplus_{i=1}^{r}\left(S^{-1}(A/\mathfrak{p}_i)\right) \end{aligned}$$

Finally, we have $S^{-1}B = \overline{S}^{-1}B = Q(B)$ and $S^{-1}(A/\mathfrak{p}_i) = \overline{S}^{-1}(A/\mathfrak{p}_i) = Q(A/\mathfrak{p}_i)$.

□

Let $S = A\backslash(\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r)$. Then

$$\begin{aligned} S^{-1}B &= S^{-1}\left(A/(Q_1 \cap \cdots \cap Q_r)\right) \\ &\cong S^{-1}A/S^{-1}(Q_1 \cap \cdots \cap Q_r) \\ &= S^{-1}A/(S^{-1}Q_1 \cap \cdots \cap S^{-1}Q_r) \\ &\cong \bigoplus_{i=1}^{r}\left(S^{-1}A/S^{-1}Q_i\right) \\ &\cong \bigoplus_{i=1}^{r}\left(S^{-1}(A/Q_i)\right) \end{aligned}$$

Finally, we have $S^{-1}B = \overline{S}^{-1}B = Q(B)$ and $S^{-1}(A/\mathfrak{p}_i) = \overline{S}^{-1}(A/\mathfrak{p}_i) = Q(A/\mathfrak{p}_i)$. The maximal ideals in $S^{-1}A$ are $S^{-1}\mathfrak{p}_i$. Assume $S^{-1}Q_i$ and $S^{-1}Q_j$ are not relatively prime. Then $S^{-1}Q_i + S^{-1}Q_j \subset S^{-1}\mathfrak{p}_k$ for some k. This implies $Q_i + Q_j \subset \mathfrak{p}_k$, which implies $\mathfrak{p}_i \subset \mathfrak{p}_k$ and $\mathfrak{p}_j \subset \mathfrak{p}_k$, which is a contradiction.

Proposition 6.13. *Let S and T be two multiplicatively closed sets in the ring A. Define $ST = \{st \mid s \in S \text{ and } t \in T\}$. Then*

1. *ST is multiplicatively closed.*
2. *There is exists an isomorphism $\varphi : i(T)^{-1}(S^{-1}A) \to (ST)^{-1}A$, where $i(T)$ is the multiplicative set given by*

   $$i(T) = \left\{\frac{t}{s} \mid t \in T, s \in S\right\}.$$

   In particular, if $S \subset T$, then $i(T)^{-1}(S^{-1}A) \cong T^{-1}A$.

Proof.

1. Suppose s_1t_1 and s_2t_2 are two elements in ST. Then

   $$(s_1t_1)(s_2t_2) = (s_1s_2)(t_1t_2) \in ST.$$

   Also, $1 = 1 \cdot 1 \in ST$. Therefore ST is multiplicatively closed.

2. Let $\varphi : i(T)^{-1}(S^{-1}A) \to (ST)^{-1}A$ be given by mapping $(a/s_1)/(t/s_2)$ to as_2/s_1t. We first need to check that this is well-defined. Suppose $(a'/s_1')/(t'/s_2') \sim (a/s_1)/(t/s_2)$. This means there exists a $t''/s'' \in i(T)$ such that
$$\frac{t''}{s''}\left(\frac{a't}{s_1's_2} - \frac{at'}{s_1s_2'}\right) = 0,$$
which means that there exists an $s \in S$ such that
$$st''(a'ts_1s_2' - at's_1's_2) = 0.$$
But this implies that $as_2/s_1t \sim a's_2'/s_1't'$ since $st'' \in ST$. Therefore φ is well-defined. The map φ is clearly surjective. We will show that φ is also injective. Suppose $as_2/s_1t = 0$. This implies that there exists $st' \in ST$ such that $st'as_2 = 0$. But this implies $(a/s_1)/(t/s_2) = 0$ since $(t'/1) \in i(T)$ with
$$\frac{t'}{1}\frac{a}{s_1} = \frac{at'}{s_1} = 0,$$
since $ss_2 \in S$ with $ss_2(at') = 0$. Finally, that φ is in fact an A-module morphism is easy to verify, and we leave as an exercise for the reader.

□

Lemma 6.3. *Let A be a Noetherian ring and let S be the set of all zerodivisors. Then*
$$S = \bigcup_{\mathfrak{p}\in Ass(\langle 0\rangle)} \mathfrak{p}.$$

Proof. Let $a \in A$ be a zerodivisor. Then there exists a nonzero $b \in A$ such that $ab = 0$. Let I denote the ideal $0 : b$. Then I has a primary decomposition, since A is Noetherian, as
$$I = Q_1 \cap \cdots \cap Q_k,$$
where $\mathfrak{p}_i = \sqrt{Q_i}$ are the associated prime ideals. Moreover, there exists $b_i \in A$ such that $\mathfrak{p}_i = I : b_i = 0 : bb_i$. Then $\mathfrak{p}_i$ are associated prime ideals of A and $a \in I \subset \mathfrak{p}_i$ implies $a \in \bigcup_{\mathfrak{p}\in \mathrm{Ass}(\langle 0\rangle)} \mathfrak{p}$. Therefore $S \subset \bigcup_{\mathfrak{p}\in \mathrm{Ass}(\langle 0\rangle)} \mathfrak{p}$. The reverse inclusion is trivial. □

Proposition 6.14. *Let A be a Noetherian ring and let $\mathfrak{p} \in Ass(\langle 0\rangle)$. Then*
$$A_{\mathfrak{p}} = Q(A)_{\mathfrak{p}Q(A)}.$$

Proof. Let S be the set of all nonzerodivisors and let $T = A\backslash\mathfrak{p}$. Then $S \subset T$ by Lemma (6.3). Therefore
$$Q(A)_{\mathfrak{p}Q(A)} = i(T)^{-1}(S^{-1}A) \cong T^{-1}A = A_{\mathfrak{p}}$$
by Proposition (6.13). □

Lemma 6.4. *Let A be a ring, $S \subset A$ be a multiplicatively closed subset and M, N be A-modules with $N \subset M$. Then*
$$(M/N)_S \cong M_S/N_S.$$

Proof. Let $\varphi : (M/N)_S \to M_S/N_S$ be the map given by $\varphi(\overline{m}/s) \mapsto \overline{m/s}$. The map is easily seen to be well-defined:
$$\varphi(\overline{m+n}/s) = \overline{(m+n)/s} = \overline{m/s}.$$
It is also clearly surjective. To show that it is injective, suppose $\varphi(\overline{m}/s) = \overline{m/s} = \overline{0}$. Then $m/s = n/s'$ for some $n/t \in N_S$. This implies there exists $s'' \in A\backslash\mathfrak{p}$ such that $s''s'm = s''sn$. But then $\overline{m}/s = 0$, since $\overline{s''s'm} = \overline{s''sn} = 0$, with $s''s' \in A\backslash\mathfrak{p}$. □

Proposition 6.15. *Let A be a ring, $S \subset A$ a multiplicatively closed subset, N, M be A-modules, and $\varphi : M \to N$ be an A-module homomorphism. Then*

1. *$Ker(\varphi_S) = Ker(\varphi)_S$.*

2. *$Im(\varphi_S) = Im(\varphi)_S$.*

3. *$Coker(\varphi_S) = Coker(\varphi)_S$.*

Remark. In particular, localization with respect to S is an **exact functor**. That is, if $0 \to M' \to M \to M'' \to 0$ is an exact sequence of A-modules, then $0 \to M'_S \to M_S \to M''_S \to 0$ is an exact sequence of A_S-modules.

Proof.

1. Suppose $m/s \in \mathrm{Ker}(\varphi_S)$. This implies there exists $s' \in A \backslash \mathfrak{m}$ such that $s'\varphi(m) = \varphi(s'm) = 0$. But then $s'm \in \mathrm{Ker}(\varphi)$, and $m/s = s'm/s's \in \mathrm{Ker}(\varphi)_S$. Conversely, suppose $m/s \in \mathrm{Ker}(\varphi)_S$. Then $\varphi_S(m/s) = \varphi(m)/s = 0$, and therefore $m/s \in \mathrm{Ker}(\varphi_S)$.

2. Suppose $\varphi_S(m/s) \in \mathrm{Im}(\varphi_S)$. Then $\varphi_S(m/s) = \varphi(m)/s \in \mathrm{Im}(\varphi)_S$. Conversely, suppose $\varphi(m)/s \in \mathrm{Im}(\varphi)_S$. Then $\varphi(m)/s = \varphi_S(m/s) \in \mathrm{Im}(\varphi_S)$.

3. Finally, using Lemma (6.4), we have

$$\begin{aligned}\mathrm{Coker}(\varphi_S) &= N_S/\mathrm{Im}(\varphi_S)\\ &= N_S/\mathrm{Im}(\varphi)_S\\ &= (N/\mathrm{Im}(\varphi)_S\\ &= \mathrm{Coker}(\varphi)_S.\end{aligned}$$

□

Proposition 6.16. *Let A be a ring and let M be an A-module. The following conditions are equivalent:*

1. $M = \langle 0 \rangle$.
2. $M_{\mathfrak{p}} = \langle 0 \rangle$ *for all prime ideals* $\mathfrak{p}$.
3. $M_{\mathfrak{m}} = \langle 0 \rangle$ *for all maximal ideals* $\mathfrak{m}$.

Proof. (1) implies (2) and (2) implies (3) is obvious. To prove (3) implies (1), assume m is a nonzero element in M. Then $\mathrm{Ann}(m)$ is an ideal in A, hence it must be contained in a maximal ideal in A, say $\mathfrak{m}$. However, this would imply that $M_{\mathfrak{m}} \neq 0$ since $m/1$ would be a nonzero element: Everything which kills m, is contained in $\mathfrak{m}$. We have reached a contradiction, and therefore there are no nonzero elements in M, in other words $M = \langle 0 \rangle$. □

Proposition 6.17. *Let A be a ring, M an A-module and N, L submodules of M. Then $N = L$ if and only if $N_{\mathfrak{m}} = L_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m}$ in A.*

Proof. If $N = L$, then we certainly have $N_{\mathfrak{m}} = L_{\mathfrak{m}}$ for all prime ideals $\mathfrak{m}$. Conversely, suppose $N_{\mathfrak{m}} = L_{\mathfrak{m}}$ for all prime ideals $\mathfrak{m}$. To obtain a contradiction, assume there exists an $n \in N$ such that $n \notin L$. Then $L :_A n = \{a \in A \mid an \in L\}$ is a proper ideal in A since $1 \notin L :_A n$. Therefore it is contained in a maximal ideal, say $\mathfrak{m}$. But this implies $N_{\mathfrak{m}} \neq L_{\mathfrak{m}}$, since $n/1 \in N_{\mathfrak{m}}$ but $n/1 \notin L_{\mathfrak{m}}$: If $n/1 = \ell/s$ for some $\ell \in L$, then there exists some $s' \in A \backslash \mathfrak{m}$ such that $s'sn = s'\ell \in L$, but $s's \notin \mathfrak{m} \supset n :_A L$, which is a contradiction. Therefore we must have $N \subset L$. By the same reasoning, we can show $L \subset N$. Therefore $L = N$. □

Corollary. *Let A be a ring, N, M be A-modules, and $\varphi : M \to N$ be an A-module homomorphism. Then*

1. *φ is injective if and only if $\varphi_{\mathfrak{m}}$ is surjective for all maximal ideals $\mathfrak{m}$.*
2. *φ is surjective if and only if $\varphi_{\mathfrak{m}}$ is injective for all maximal ideals $\mathfrak{m}$.*

Proof.

1. Suppose $\varphi_{\mathfrak{m}}$ is injective for all maximal ideals $\mathfrak{m}$ in A. Then $0 \cong \mathrm{Ker}(\varphi_{\mathfrak{m}}) \cong \mathrm{Ker}(\varphi)_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m}$ in A. Therefore by Proposition (6.16), we must have $\mathrm{Ker}(\varphi) \cong 0$. Conversely, suppose φ is injective. Then $\mathrm{Ker}(\varphi) \cong 0$ implies $0 \cong \mathrm{Ker}(\varphi)_{\mathfrak{m}} \cong \mathrm{Ker}(\varphi_{\mathfrak{m}})$ for all maximal ideals $\mathfrak{m}$ in A.

2. Suppose $\varphi_{\mathfrak{m}}$ is surjective for all maximal ideals $\mathfrak{m}$ in A. Then $N_{\mathfrak{m}} = \mathrm{Im}(\varphi_{\mathfrak{m}}) = \mathrm{Im}(\varphi)_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m}$ in A. Therefore $N = \mathrm{Im}(\varphi)$, by Proposition (6.17). Conversely, suppose φ is injective. Then $N = \mathrm{Im}(\varphi)$ implies $N_{\mathfrak{m}} = \mathrm{Im}(\varphi)_{\mathfrak{m}}$, which implies $\varphi_{\mathfrak{m}}$ is surjective for all maximal ideals $\mathfrak{m}$ in A.

□

Proposition 6.18. *Let A be a ring, $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be prime ideals in A, and $\langle 0 \rangle \neq M$ a finitely generated A-module such that $M_{\mathfrak{p}_i} \neq \langle 0 \rangle$ for all i. Then there exists $m \in M$ such that $m/1 \notin \mathfrak{p}_i M_{\mathfrak{p}_i}$ for all i.*

Proof. Nakayama's lemma implies that $M_{\mathfrak{p}_i}/\mathfrak{p}_i M_{\mathfrak{p}_i} \neq 0$. Therefore we may choose $m_i/1 \in M_{\mathfrak{p}_i}$ such that if $am_i \in \mathfrak{p}_i M$, then $a \in \mathfrak{p}_i$. In particular, this means $m_i/1 \notin \mathfrak{p}_i M_{\mathfrak{p}_i}$ for all i. We now want to glue these local solutions together. Start with $m_i/1 \in M_{\mathfrak{p}_i}$ and $m_j/1 \in M_{\mathfrak{p}_j}$. If $m_i/1 \notin \mathfrak{p}_j M_{\mathfrak{p}_j}$, then ignore the $m_j/1$ term and keep the $m_i/1$ term. Similarly, if $m_j/1 \notin \mathfrak{p}_i M_{\mathfrak{p}_i}$, then drop $m_i/1$ and keep the $m_j/1$ term. If both $m_i/1 \in \mathfrak{p}_j M_{\mathfrak{p}_j}$ and $m_j/1 \in \mathfrak{p}_i M_{\mathfrak{p}_i}$, then add the terms $m_i/1$ and $m_j/1$ to get $(m_i + m_j)/1$. Now assume, we have constructed an element $m/1 \notin \mathfrak{p}_i M_{\mathfrak{p}_i}$ for $i = 1, 2, \dots k-1$, and assume $m/1 \in \mathfrak{p}_k M_{\mathfrak{p}_k}$. Choose $x_i \in \mathfrak{p}_i$ such that $x_i \notin \mathfrak{p}_k$ for all $i = 1, 2, \dots, k-1$. Then $x_1 x_2 \cdots x_{k-1} m_k/1 \in \mathfrak{p}_i M_{\mathfrak{p}_i}$ for $i = 1, 2, \dots, k-1$ and $x_1 x_2 \cdots x_{k-1} m_k/1 \notin \mathfrak{p}_k M_{\mathfrak{p}_k}$. This implies $m/1 + x_1 x_2 \cdots x_{k-1} m_k/1 = (m + x_1 x_2 \cdots x_{k-1} m_k)/1 \notin \mathfrak{p}_i M_{\mathfrak{p}_i}$ for $i = 1, 2, \dots, k$. □

A key fact about localization is that every linear map $\varphi : M \to N$ of $A_\mathfrak{p}$-modules comes from the localization of a linear map of A-modules. That is, we have have a commutative diagram

$$\begin{tikzcd}
M \arrow[r, "\varphi"] & N \\
M \otimes_A A_\mathfrak{p} \arrow[u] \arrow[r, "\varphi_\mathfrak{p}"'] & N \otimes_A A_\mathfrak{p} \arrow[u]
\end{tikzcd}$$

where the vertical arrows are isomorphisms, given by mapping $m \otimes 1/s$ to m/s and $n \otimes 1/s$ to n/s respectively. Thus, when we talk about a linear map of $A_\mathfrak{p}$-modules, we may assume it has the form $\varphi_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$.

6.7 Localization commutes with Hom and Tensor Products

Lemma 6.5. *Let A be a ring, $\mathfrak{p}$ an ideal in A, and M, N A-modules. Then there exists an injective linear $\Psi : Hom_A(N, M)_\mathfrak{p} \to Hom_{A_\mathfrak{p}}(N_\mathfrak{p}, M_\mathfrak{p})$. Moreover, if N is finitely presented, then this map is also surjective, and hence an isomorphism.*

Proof. Define $\Psi_N : \mathrm{Hom}_A(N, M)_\mathfrak{p} \to \mathrm{Hom}_{A_\mathfrak{p}}(N_\mathfrak{p}, M_\mathfrak{p})$ by sending the element $\varphi/s \in \mathrm{Hom}_A(N, M)_\mathfrak{p}$ to map $\Psi_N(\varphi/s)$ given by:

$$\Psi_N\left(\frac{\varphi}{s}\right)\left(\frac{n}{t}\right) = \frac{\varphi(n)}{st}.$$

We need to be sure this is well-defined. Let φ'/s' be another representation, so that there exists an $s'' \notin \mathfrak{p}$ such that $s''s'\varphi = s''s\varphi'$. Then

$$\begin{aligned}
\Psi_N\left(\frac{\varphi'}{s'}\right)\left(\frac{n}{t}\right) &= \frac{\varphi'(n)}{s't} \\
&= \frac{\varphi(n)}{st},
\end{aligned}$$

since $s''st\varphi'(n) = s''s't\varphi(n)$ for all $n/t \in N_\mathfrak{p}$. Next, we check that $\Psi_N(\varphi/s)$ is $A_\mathfrak{p}$- linear:

$$\begin{aligned}
\Psi_N\left(\frac{\varphi}{s}\right)\left(\frac{t'n + tn'}{tt'}\right) &= \frac{\varphi(t'n + tn')}{stt'} \\
&= \frac{t'\varphi(n) + t\varphi(n')}{stt'} \\
&= \frac{\varphi(n)}{st'} + \frac{\varphi(n')}{st'} \\
&= \Psi_N\left(\frac{\varphi}{s}\right)\left(\frac{n}{t}\right) + \Psi_N\left(\frac{\varphi}{s}\right)\left(\frac{n'}{t'}\right),
\end{aligned}$$

for all n/t and n'/t' in $N_\mathfrak{p}$, and

$$\begin{aligned}
\Psi_N\left(\frac{\varphi}{s}\right)\left(\frac{a}{u} \cdot \frac{n}{t}\right) &= \frac{\varphi(an)}{sut} \\
&= \frac{a}{u} \cdot \frac{\varphi(n)}{st} \\
&= \frac{a}{u} \cdot \Psi_N\left(\frac{\varphi}{s}\right)\left(\frac{n}{t}\right).
\end{aligned}$$

for all a/u in $A_\mathfrak{p}$ and n/t in $N_\mathfrak{p}$. So $\Psi_N(\varphi/s) \in \mathrm{Hom}_{A_\mathfrak{p}}(N_\mathfrak{p}, M_\mathfrak{p})$. Next, suppose

$$\Psi_N\left(\frac{\varphi}{s}\right)\left(\frac{n}{t}\right) = 0,$$

for all $n/t \in N_\mathfrak{p}$. Then there exists an $u_n \in A \backslash \mathfrak{p}$ such that $u_n\varphi(n) = 0$ for all $n \in N$. But this implies $\varphi/s = 0$, so Ψ_N is injective.

Now we want to show the second part of the lemma. First assume that N is a free A-module with basis $e_1, \dots, e_k$. Then $N_\mathfrak{p}$ is a free $A_\mathfrak{p}$-module with basis $e_1/1, \dots, e_k/1$. Suppose $\varphi \in \operatorname{Hom}_{A_\mathfrak{p}}(N_\mathfrak{p}, M_\mathfrak{p})$. Then φ is completely determined by where it maps the basis elements, say, $\varphi(e_i/1) = m_i/s_i$ for all $i = 1, \dots, k$. Define $\varphi_i \in \operatorname{Hom}_A(N, M)$ by

$$\varphi_i(e_j) = \begin{cases} s_i & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

Then $\varphi_1/s_1 + \cdots + \varphi_k/s_k \in \operatorname{Hom}_A(N, M)_\mathfrak{p}$, and $\Psi_N(\varphi_1/s_1 + \cdots + \varphi_k/s_k) = \varphi$ since they act the same on the basis vectors $e_1/1, \dots, e_k/1$. If, now, N is a finitely presented A-module, then there is an exact sequence

$$A^t \longrightarrow A^s \longrightarrow N \longrightarrow 0$$

Since $\operatorname{Hom}_A(-, M)$ is a left exact contravariant functor, and localization preserves homology, we obtain a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Hom}_A(N, M)_\mathfrak{p} \arrow[r] \arrow[d, dashed, "\Psi_N"] & \operatorname{Hom}_A(A^s, M)_\mathfrak{p} \arrow[r] \arrow[d, "\Psi_{A^s}"] & \operatorname{Hom}_A(A^t, M)_\mathfrak{p} \arrow[d, "\Psi_{A^t}"] \\
0 \arrow[r] & \operatorname{Hom}_{A_\mathfrak{p}}(N_\mathfrak{p}, M_\mathfrak{p}) \arrow[r] & \operatorname{Hom}_{A_\mathfrak{p}}(A^s_\mathfrak{p}, M_\mathfrak{p}) \arrow[r] & \operatorname{Hom}_{A_\mathfrak{p}}(A^t_\mathfrak{p}, M_\mathfrak{p})
\end{tikzcd}$$

Since Ψ_{A^s} and Ψ_{A^t} are isomorphisms, and easy diagram chase tells us that there must exist a unique isomorphism $\Psi_N : \operatorname{Hom}_A(N, M)_\mathfrak{p} \to \operatorname{Hom}_{A_\mathfrak{p}}(N_\mathfrak{p}, M_\mathfrak{p})$ which makes this diagram commute. □

Lemma 6.6. *Let A be a ring, $\mathfrak{p}$ an ideal in A, and M, N A-modules. Then $N_\mathfrak{p} \otimes_A M_\mathfrak{p} = N_\mathfrak{p} \otimes_{A_\mathfrak{p}} M_\mathfrak{p} = (N \otimes_A M)_\mathfrak{p}$.*

Remark. Notice that we are saying $N_\mathfrak{p} \otimes_A M_\mathfrak{p}$ is literally the same set as $N_\mathfrak{p} \otimes_{A_\mathfrak{p}} M_\mathfrak{p}$ and $(N \otimes_A M)_\mathfrak{p}$.

Proof. For the first identity, we just need to show that $\frac{n}{s} \otimes m = n \otimes \frac{m}{s}$ for every $m \in M$, $n \in N$ and $s \in A \backslash \mathfrak{p}$. We have

$$\begin{aligned} \frac{n}{s} \otimes m &= \frac{n}{s} \otimes \frac{sm}{s} \\ &= \frac{sn}{s} \otimes \frac{m}{s} \\ &= n \otimes \frac{m}{s}. \end{aligned}$$

For second identity, we show that every element in $N_\mathfrak{p} \otimes_{A_\mathfrak{p}} M_\mathfrak{p}$ has the form $\frac{(n_1 \otimes m_1 + \cdots + n_k \otimes m_k)}{s}$, where $s \in A \backslash \mathfrak{p}$. Start with an arbitrary element $\frac{n_1}{s_1} \otimes m_1 + \cdots + \frac{n_k}{s_k} \otimes m_k$ in $N_\mathfrak{p} \otimes_{A_\mathfrak{p}} M_\mathfrak{p}$, where $s_i \in A \backslash \mathfrak{p}$. We have

$$\frac{n_1}{s_1} \otimes m_1 + \cdots + \frac{n_k}{s_k} \otimes m_k = \frac{1}{s_1 s_2 \cdots s_k} \left(s_2 \cdots s_k n_1 \otimes m_1 + \cdots + s_1 \cdots s_{k-1} n_k \otimes m_k \right),$$

which proves the claim. □

6.8 Local Rings

Definition 6.5. A ring A is called **local** if it has exactly one maximal ideal $\mathfrak{m}$. If A is local, then we call $A/\mathfrak{m}$ the **residue field** of A. Rings with finitely many maximal ideals are called **semi-local**.

Lemma 6.7. *Let A be a ring.*

1. *A is a local ring if and only if the set of non-units is an ideal (which is then the maximal ideal).*

2. *Let $\mathfrak{m} \subset A$ be a maximal ideal such that every element of the form $1 + a$, where $a \in \mathfrak{m}$, is a unit. Then A is local.*

Proof.

1. Let A be a local ring with maximal ideal $\mathfrak{m}$ and let $x \in A$ be a non-unit. Then $\langle x \rangle \neq 1$, and so $\langle x \rangle$ is contained in a maximal ideal. Since there is only one maximal ideal, we must have $\langle x \rangle \subset \mathfrak{m}$, i.e. $x \in \mathfrak{m}$. Therefore $\mathfrak{m}$ contains the set of all non-units. Since the set of all non-units already contains $\mathfrak{m}$, we see that $\mathfrak{m}$ is the set of all non-units. To prove the converse, let A be a ring and let $\mathfrak{m}$ be the set of all non-units in A. Suppose $\mathfrak{m}$ is an ideal and let $\mathfrak{m}_1$ and $\mathfrak{m}_2$ be two maximal ideals in A. Then $\mathfrak{m} \supset \mathfrak{m}_1$ and $\mathfrak{m} \supset \mathfrak{m}_2$. Since $\mathfrak{m}_1$ and $\mathfrak{m}_2$ are maximal ideals, we must have equality, thus $\mathfrak{m}_1 = \mathfrak{m} = \mathfrak{m}_2$.

2. Let $u \in A \backslash \mathfrak{m}$. Since $\mathfrak{m}$ is maximal, $\langle \mathfrak{m}, u \rangle = A$ and, hence, $1 = uv + a$ for some $v \in A$ and $a \in \mathfrak{m}$. By assumption, $uv = 1 - a$ is a unit. Hence, u is a unit and $\mathfrak{m}$ is the set of non-units. The claim follows from (1).

□

6.9 The Covariant Functor $-_S$

Proposition 6.19. *Let S be a multiplicatively closed subset of R. We obtain a functor*

$$-_S \colon \mathbf{Mod}_R \to \mathbf{Mod}_{R_S}$$

from the category of R-modules to the category of R_S-modules, where the R-module M is assigned to the R_S-module M_S and where the R-linear map $\varphi \colon M \to M'$ is assigned to the R_S-linear map $\varphi_S \colon M_S \to M'_S$, where φ_S is defined by

$$\varphi_S\left(\frac{u}{s}\right) = \frac{\varphi(u)}{s}$$

for all $u/s \in M_S$.

Proof. We need to check that $-_S$ preserves compositions and identities. We first check that it preserves compositions. Let $\varphi \colon M \to M'$ and $\varphi' \colon M' \to M''$ be two R-linear maps and let $u/s \in M_S$. Then

$$\begin{aligned}
(\varphi'_S \varphi_S)\left(\frac{u}{s}\right) &= \varphi'_S\left(\varphi_S\left(\frac{u}{s}\right)\right) \\
&= \varphi'_S\left(\frac{\varphi(u)}{s}\right) \\
&= \frac{\varphi'(\varphi(u))}{s} \\
&= \frac{(\varphi'\varphi)(u)}{s} \\
&= (\varphi'\varphi)_S\left(\frac{u}{s}\right).
\end{aligned}$$

It follows that $\varphi'_S \varphi_S = (\varphi'\varphi)_S$. Hence $-_S$ preserves compositions. Next we check that $-_S$ preserves identities. Let M be an R-module and $u/s \in M_S$. Then we have

$$\begin{aligned}
(1_M)_S\left(\frac{u}{s}\right) &= \frac{1_M(u)}{s} \\
&= \frac{u}{s} \\
&= 1_{M_S}\left(\frac{u}{s}\right).
\end{aligned}$$

It follows that $(1_M)_S = 1_{M_S}$. Hence $-_S$ preserves identities. □

6.9.1 Natural Isomorphism from $-_S$ to $- \otimes_R R_S$

Proposition 6.20. *Let S be a multiplicatively closed subset of R. Then there exists a natural isomorphism*

$$\tau \colon - \otimes_R R_S \to -_S$$

of functors.

Proof. Let M be an R-module. We first observe that every tensor in $M \otimes_R R_S$ can be expressed as an elementary tensor of the form $u \otimes (1/s)$ where $u \in M$ and $s \in S$. Indeed, let $\sum_{i=1}^k u_i \otimes (a_i/s_i)$ be any tensor. Then we have

$$\begin{aligned}
u_1 \otimes \frac{a_1}{s_1} + \cdots + u_k \otimes \frac{a_k}{s_k} &= u_1 \otimes \frac{a_1 s_2 \cdots s_k}{s_1 s_2 \cdots s_k} + \cdots + u_k \otimes \frac{s_1 \cdots s_{k-1} a_k}{s_1 s_2 \cdots s_k} \\
&= (a_1 s_2 \cdots s_k u_1 + \cdots + s_1 \cdots s_{k-1} a_k u_k) \otimes \frac{1}{s_1 s_2 \cdots s_k} \\
&= \widetilde{u} \otimes \frac{1}{\widetilde{s}},
\end{aligned}$$

where

$$\widetilde{u} = a_1 s_2 \cdots s_k u_1 + \cdots + s_1 \cdots s_{k-1} a_k u_k \in M \quad \text{and} \quad s = s_1 s_2 \cdots s_k \in S.$$

Define $\tau_M \colon M \otimes_R R_S \to M_S$ by

$$\tau_M\left(u \otimes \frac{1}{s}\right) = \frac{u}{s}$$

for all $u \otimes (1/s) \in M \otimes_R R_S$. The map τ_M is easily checked to be well-defined, surjective, and an R-linear map (in fact an R_S-linear map). To show it is injective, let $u \otimes (1/s) \in \ker \varphi$. Then since $\varphi(u)/s = 0$, we may choose a $t \in S$ such that $t\varphi(u) = 0$. Then

$$\begin{aligned} u \otimes \frac{1}{s} &= u \otimes \frac{t}{st} \\ &= tu \otimes \frac{1}{st} \\ &= 0 \otimes \frac{1}{st} \\ &= 0. \end{aligned}$$

Thus $\ker \tau_M = 0$, which implies τ_M is injective.

Thus for each R-module M, we obtain an isomorphism $\tau_M \colon M \otimes_R R_S \to M_S$. We claim that τ_- is natural in M, so that it is a natural isomorphism. Indeed, let $\varphi \colon M \to M'$ be an R-linear map. We need to check that the following diagram commutes

$$\begin{tikzcd} M \otimes_R R_S \arrow[r, "\tau_M"] \arrow[d, "\varphi\otimes 1"'] & M_S \arrow[d, "\varphi_S"] \\ M' \otimes_R R_S \arrow[r, "\tau_{M'}"'] & M'_S \end{tikzcd} \tag{38}$$

Let $u \otimes \frac{1}{s} \in M \otimes_R R_S$. Then we have

$$\begin{aligned} (\varphi_S \tau_M)\left(u \otimes \frac{1}{s}\right) &= \varphi_S\left(\tau_M\left(u \otimes \frac{1}{s}\right)\right) \\ &= \varphi_S\left(\frac{u}{s}\right) \\ &= \frac{\varphi(u)}{s} \\ &= \tau_{M'}\left(\varphi(u) \otimes \frac{1}{s}\right) \\ &= \tau_{M'}\left((\varphi \otimes 1)\left(u \otimes \frac{1}{s}\right)\right) \\ &= (\tau_{M'}(\varphi \otimes 1))\left(u \otimes \frac{1}{s}\right). \end{aligned}$$

□

Corollary. *Let S be a multiplicatively closed subset of R. Then $-_S$ is exact.*

Proof. The functor $- \otimes_R R_S$ is exact since R_S is a flat R-module. Thus $-_S$ must be exact too since $-_S$ is naturally isomorphic to $- \otimes_R R_S$. □

6.9.2 Localization is Essentially Surjective

Throughout the rest of this section, let S be a multiplicatively closed subset of R.

Proposition 6.21. *Localization is essentially surjective.*

Proof. Let us first show that localization is essentially surjective. Let M be an R_S-module. Then M is also an R-module via the action

$$a \cdot u = \frac{a}{1} \cdot u$$

for all $a \in R$ and $u \in M$. Then $R_S \otimes_R M$ is an R_S-module via the action

$$\frac{a}{s} \cdot \left(\frac{b}{t} \otimes u\right) = \frac{ab}{st} \otimes u$$

for all a/s and b/t in R_S and for all $u \in M$. We claim that M is isomorphic to $R_S \otimes_R M$ as R_S-modules. Indeed, let $\varphi \colon R_S \otimes_R M \to M$ be given by

$$\varphi\left(\frac{1}{s} \otimes u\right) = \frac{1}{s} \cdot u$$

for all $(1/s) \otimes u \in R_S \otimes M$ [4]. This map is well-defined and linear since the corresponding map $R_S \times M \to M$, given by $(a/s, u) \mapsto (a/s) \cdot u$, is bilinear. This map is injective since if $(1/s) \cdot u = 0$, then $u = 0$, which implies $(1/s) \otimes u = 0$. Finally, the map is surjective since if $u \in M$, then $\varphi((1/1) \otimes u) = u$. Therefore localization is essentially surjective since $M_S \cong R_S \otimes_R M$. □

7 Hom

Let M and N be R-modules. We denote by $\mathrm{Hom}_R(M, N)$ to be the set of all R-linear maps from M to N. In fact, $\mathrm{Hom}_R(M, N)$ is more than just a set, it is an abelian group, where addition is defined pointwise: if $\varphi, \psi \in \mathrm{Hom}_R(M, N)$, then we define $\varphi + \psi \in \mathrm{Hom}_R(M, N)$ to be the R-linear map given by

$$(\varphi + \psi)(u) = \varphi(u) + \psi(u)$$

for all $u \in M$. If R is commutative, then $\mathrm{Hom}_R(M, N)$ is more than just an abelian group; it has the structure of an R-module, where scalar multiplication is defined pointwise: if $\varphi \in \mathrm{Hom}_R(M, N)$ and $a \in R$, then we define $a\varphi \in \mathrm{Hom}_R(M, N)$ to be the R-linear map given by

$$(a\varphi)(u) = \varphi(au)$$

for all $u \in M$. Note that if R is not commutative, then $a\varphi$ is R-linear if and only if $a \in Z(R)$. Indeed, given $a, b \in R$, we have

$$\begin{aligned} (a\varphi)(bu) &= \varphi(abu) \\ &= \varphi(bau) \\ &= b\varphi(au) \\ &= b(a\varphi)(u), \end{aligned}$$

where we were allowed to commute a and b since $a \in Z(R)$.

7.1 Properties of Hom

7.1.1 Universal Mapping Property for Products

Proposition 7.1. *Let M be an R-module, let I be an index set, and let N_i be an R-module for each $i \in I$. Then*

1. $\mathit{Hom}_R\left(\bigoplus_{i\in I} N_i, M\right) \cong \prod_{i\in I} \mathit{Hom}_R\left(N_i, M\right)$.
2. $\mathit{Hom}_R\left(M, \prod_{i\in I} N_i\right) \cong \prod_{i\in I} \mathit{Hom}_R\left(M, N_i\right)$
3. *If, moreover, M is finitely generated, then* $\mathit{Hom}_R\left(M, \bigoplus_{i\in I} N_i\right) \cong \bigoplus_{i\in I} \mathit{Hom}_R\left(M, N_i\right)$.

Remark. In other words, the contravariant functor $\mathrm{Hom}_R(-, M)$ takes direct sums to direct products, the covariant functor $\mathrm{Hom}_R(M, -)$ takes direct products to direct products, and if M is finitely-generated, then the covariant functor $\mathrm{Hom}_R(M, -)$ also takes direct sums to direct sums.

Proof. 1. For each $i \in I$, let $\iota_i \colon N_i \to \bigoplus_{i\in I} N_i$ denote the ith inclusion map. Define a map $\Psi \colon \mathrm{Hom}_R\left(\bigoplus_{i\in I} N_i, M\right) \to \prod_{i\in I} \mathrm{Hom}_R\left(N_i, M\right)$ by

$$\Psi(\varphi) = (\varphi|_{N_i}) = (\varphi \circ \iota_i)$$

for all $\varphi \in \mathrm{Hom}_R\left(\bigoplus_{i\in I} N_i, M\right)$. The map Ψ is R-linear as it is a composition of R-linear maps in each component. To see that it is an isomorphism, we construct an inverse map. Define a map $\Phi \colon \prod_{i\in I} \mathrm{Hom}_R\left(N_i, M\right) \to \mathrm{Hom}_R\left(\bigoplus_{i\in I} N_i, M\right)$ by

$$\Phi((\varphi_i))(y_{i_1} + \cdots + y_{i_n}) = \varphi_{i_1}(y_{i_1}) + \cdots + \varphi_{i_n}(y_{i_n})$$

for all $(\varphi_i) \in \prod_{i\in I} \mathrm{Hom}_R\left(N_i, M\right)$ and $y_{i_1} + \cdots + y_{i_n} \in \bigoplus_{i\in I} N_i$.

Let us check that Ψ is indeed the inverse to Φ. Let $\varphi \in \mathrm{Hom}_R\left(\bigoplus_{i\in I} N_i, M\right)$ and let $y_{i_1} + \cdots + y_{i_n} \in \bigoplus_{i\in I} N_i$. Then

$$\begin{aligned} (\Phi\Psi)(\varphi)(y_{i_1} + \cdots + y_{i_n}) &= \Phi(\varphi|_{N_i})(y_{i_1} + \cdots + y_{i_n}) \\ &= \varphi|_{N_{i_1}}(y_{i_1}) + \cdots + \varphi|_{N_{i_n}}(y_{i_n}) \\ &= \varphi(y_{i_1}) + \cdots + \varphi(y_{i_n}) \\ &= \varphi(y_{i_1} + \cdots + y_{i_n}). \end{aligned}$$

[4] Note that every element in $R_S \otimes_R M$ can be put into an elementary tensor form $(1/s) \otimes u$.

It follows that $\Phi\Psi = 1$.

Conversely, let $(\varphi_i) \in \prod_{i \in I} \operatorname{Hom}_R(N_i, M)$. Observe that for each $i \in I$, we have

$$(\Phi(\varphi_i) \circ \iota_i)(y) = \varphi_i(y)$$

for all $y \in N_i$. It follows that $\Phi(\varphi_i) \circ \iota_i = \varphi_i$. Therefore

$$\begin{aligned}(\Psi\Phi)((\varphi_i)) &= \Psi(\Phi(\varphi_i)) \\ &= (\Phi(\varphi_i) \circ \iota_i) \\ &= (\varphi_i).\end{aligned}$$

This implies $\Psi\Phi = 1$.

2. Define a map $\Psi \colon \operatorname{Hom}_R(M, \prod_{i \in I} N_i) \to \prod_{i \in I} \operatorname{Hom}_R(M, N_i)$ by

$$\Psi(\varphi) = (\pi_i \circ \varphi)_{i \in I}$$

for all $\varphi \in \operatorname{Hom}_R(M, \prod_{i \in I} N_i)$, where $\pi_i \colon \prod_{i \in I} N_i \to N_i$ is the projection to the ith coordinate. We claim that Ψ is an isomorphism.

We first check that it is R-linear. Let $a, b \in R$ and $\varphi, \psi \in \operatorname{Hom}_R(M, \prod_{i \in I} N_i)$. Then

$$\begin{aligned}\Psi(a\varphi + b\psi) &= (\pi_i \circ (a\varphi + b\psi)) \\ &= (a(\pi_i \circ \varphi) + b(\pi_i \circ \psi)) \\ &= a(\pi_i \circ \varphi) + b(\pi_i \circ \psi) \\ &= a\Psi(\varphi) + b\Psi(\psi).\end{aligned}$$

Thus Ψ is R-linear. To show that Ψ is an isomorphism, we construct its inverse. Let $(\varphi_i) \in \prod_{i \in I} \operatorname{Hom}_R(M, N_i)$. Define $\Phi((\varphi_i)) \colon M \to \prod_{i \in I} N_i$ by

$$\Phi((\varphi_i))(x) := (\varphi_i(x))$$

for all $x \in M$. Then clearly Φ and Ψ are inverse to each other. Indeed, let $\varphi \in \operatorname{Hom}_R(M, \prod_{i \in I} N_i)$. Then

$$\begin{aligned}\Phi(\Psi(\varphi))(x) &= \Phi((\pi_i \circ \varphi))(x) \\ &= ((\pi_i \circ \varphi)(x)) \\ &= \varphi(x)\end{aligned}$$

for all $x \in M$. Thus $\Phi(\Psi(\varphi)) = \varphi$. Conversely, let $(\varphi_i) \in \prod_{i \in I} \operatorname{Hom}_R(M, N_i)$. Then

$$\begin{aligned}\Psi(\Phi(\varphi_i)) &= (\pi_i \circ \Phi(\varphi_i)) \\ &= (\pi_i \circ \varphi)) \\ &= \varphi(x)\end{aligned}$$

3. Let $\varphi \in \bigoplus_{i \in I} \operatorname{Hom}_R(M, N_i)$ and let

$$\varphi = \sum_{k=1}^{n} \varphi_{i_k}$$

be the unique decomposition of φ, where $\varphi_{i_k} \in \operatorname{Hom}_R(M, N_{i_k})$ for each $1 \leq k \leq n$. We can view φ as an element in $\operatorname{Hom}_R(M, \bigoplus_{i \in I} N_i)$. Indeed, for each $x \in M$, we have

$$\varphi(x) = \sum_{k=1}^{n} \varphi_{i_k}(x) \in \bigoplus_{i \in I} N_i.$$

Thus we have

$$\bigoplus_{i \in I} \operatorname{Hom}_R(M, N_i) \subset \operatorname{Hom}_R\left(M, \bigoplus_{i \in I} N_i\right).$$

For the other direction, suppose that $\{x_1, \dots, x_n\}$ is a generating set for M and let $\varphi \in \operatorname{Hom}_R(M, \bigoplus_{i \in I} N_i)$. For each $1 \leq k \leq n$, let

$$\varphi(x_k) = y_{i_{1,k}} + \cdots + y_{i_{n_k,k}}$$

be the unique decomposition of $\varphi(x_k)$. It follows that

$$\varphi(M) \subset \bigoplus_{\substack{1\leq k\leq n\\ 1\leq j\leq n_k}} N_{i_{j,k}}.$$

In particular, we may view φ as an element in

$$\begin{aligned}\mathrm{Hom}_R\left(M, \bigoplus_{\substack{1\leq k\leq n\\ 1\leq j\leq n_k}} N_{i_{j,k}}\right) &\cong \bigoplus_{\substack{1\leq k\leq n\\ 1\leq j\leq n_k}} \mathrm{Hom}_R(M, N_{i_{j,k}})\\ &\subset \bigoplus_{i\in I}\mathrm{Hom}_R(M, N_i).\end{aligned}$$

□

7.1.2 Hom Commutes with Localization Under Certain Conditions

Recall that the localization functor $-_S$ is essentially surjective. This means that every R_S-module is isomorphic to an R_S-module of the form M_S where M is an R-module. We now want to show that the localization functor is faithful, but not necessarily full.

Lemma 7.1. *Let S be a multiplicatively closed subset of R and let M and N be R-modules. Then there exists an injective R_S-linear map*

$$\Psi\colon \mathrm{Hom}_R(M,N)_S \to \mathrm{Hom}_{R_S}(M_S, N_S).$$

Moreover, if M is finitely presented, then this map is also surjective, and hence an isomorphism.

Proof. We define $\Psi\colon \mathrm{Hom}_R(M,N)_S \to \mathrm{Hom}_{R_S}(M_S, N_S)$ by

$$\Psi_M\left(\frac{\varphi}{s}\right)\left(\frac{u}{t}\right) = \frac{\varphi(u)}{st}. \tag{39}$$

for all $\varphi/s \in \mathrm{Hom}_R(M,N)_S$ and $u/t \in M_S$. We need to check that (39) is well-defined. Let φ'/s' and u'/t' be two different representations of φ/s and u/t respectively. Choose $s'', t'' \in S$ such that $s''s'\varphi = s''s\varphi'$ and $t''t'u = t''tu'$. Then

$$\begin{aligned}\Psi_M\left(\frac{\varphi'}{s'}\right)\left(\frac{u'}{t'}\right) &= \frac{\varphi'(u')}{s't'}\\ &= \frac{s''s\varphi'(t''tu')}{s''st''ts't'}\\ &= \frac{s''s'\varphi(t''t'u)}{s''st''ts't'}\\ &= \frac{\varphi(u)}{st}.\end{aligned}$$

Thus (39) is well-defined.

Next, we check that $\Psi_M(\varphi/s)$ is R_S-linear: we have

$$\begin{aligned}\Psi_M\left(\frac{\varphi}{s}\right)\left(\frac{t'u+tu'}{tt'}\right) &= \frac{\varphi(t'u+tu')}{stt'}\\ &= \frac{t'\varphi(u)+t\varphi(u')}{stt'}\\ &= \frac{\varphi(u)}{st'} + \frac{\varphi(u')}{st'}\\ &= \Psi_M\left(\frac{\varphi}{s}\right)\left(\frac{u}{t}\right) + \Psi_M\left(\frac{\varphi}{s}\right)\left(\frac{u'}{t'}\right),\end{aligned}$$

for all u/t and u'/t' in M_S, and

$$\begin{aligned}\Psi_M\left(\frac{\varphi}{s}\right)\left(\frac{a}{t'}\cdot\frac{u}{t}\right) &= \frac{\varphi(au)}{st't}\\ &= \frac{a}{t'}\cdot\frac{\varphi(u)}{st}\\ &= \frac{a}{t'}\cdot\Psi_M\left(\frac{\varphi}{s}\right)\left(\frac{u}{t}\right).\end{aligned}$$

for all a/t' in R_S and u/t in M_S. Thus $\Psi_M(\varphi/s)$ is R_S-linear.

Finally, we check that Ψ is injective. Suppose

$$\Psi_M\left(\frac{\varphi}{s}\right)\left(\frac{u}{t}\right) = 0,$$

for all $u/t \in N_{\mathfrak{p}}$. Then there exists an $s_u \in S$ such that $s_u\varphi(u) = 0$ for all $u \in M$. But this implies $\varphi/s = 0$, so Ψ_M is injective.

Now we want to show the second part of the lemma. First assume that M is a finite free R-module with basis $e_1, \dots, e_m$. Then M_S is a free R_S-module with basis $e_1/1, \dots, e_m/1$. Suppose $\varphi \in \mathrm{Hom}_{R_S}(M_S, N_S)$. Then φ is completely determined by where it maps the basis elements, say,

$$\varphi\left(\frac{e_i}{1}\right) = \frac{v_i}{t_i}$$

for all $i = 1, \dots, m$. For each $1 \leq i \leq m$, let $\varphi_i \colon M \to N$ be the unique R-linear map such that

$$\varphi_i(e_j) = \begin{cases} v_i & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$\frac{\varphi_1}{t_1} + \cdots + \frac{\varphi_m}{t_m} \in \mathrm{Hom}_R(M,N)_S \quad \text{and} \quad \Psi_M\left(\frac{\varphi_1}{t_1} + \cdots + \frac{\varphi_m}{t_m}\right) = \varphi$$

since they act the same on the basis vectors $e_1/1, \dots, e_m/1$. Thus, in the case where M is a finite free R-module, the map Ψ_M is surjective.

Now we assume that M is a finitely presented R-module, then there is an exact sequence

$$\begin{tikzcd} G \arrow[r] & F \arrow[r] & M \arrow[r] & 0 \end{tikzcd}$$

where F and G are finite free R-modules. The since $\mathrm{Hom}_R(-,N)$ is left exact contravariant and $-_S$ is exact covariant, we obtain a commutative diagram with exact rows

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Hom}_R(M,N)_S \arrow[r] \arrow[d, dashed, "\Psi_M"] & \mathrm{Hom}(F,N)_S \arrow[r] \arrow[d, "\Psi_F"] & \mathrm{Hom}(G,N)_S \arrow[d, "\Psi_G"] \\ 0 \arrow[r] & \mathrm{Hom}_{R_S}(M_S,N_S) \arrow[r] & \mathrm{Hom}_{R_S}(F_S,N_S) \arrow[r] & \mathrm{Hom}_{R_S}(G_S,N_S) \end{tikzcd}$$

where the columns are isomorphisms. An easy diagram chase tells us that

$$\Psi_M \colon \mathrm{Hom}_R(M,N)_S \to \mathrm{Hom}_{R_S}(M_S,N_S)$$

is the unique isomorphism which makes this diagram commute. □

7.2 Functorial Properties of Hom

7.2.1 The Covariant Functor $\mathrm{Hom}_R(M,-)$

Proposition 7.2. *Let M be an R-module. We obtain a covariant functor*

$$\mathrm{Hom}_R(M,-) \colon \mathbf{Mod}_R \to \mathbf{Mod}_R$$

from the category of R-modules to itself, where the R-module N is assigned to the R-module $\mathrm{Hom}_R(M,N)$ and where the R-linear map $\varphi \colon N \to N'$ is assigned to the R-linear map $\varphi_* \colon \mathrm{Hom}_R(M,N) \to \mathrm{Hom}_R(M,N')$, where φ_* is defined by

$$\varphi_*(\psi) = \varphi\psi$$

for all $\psi \in \mathrm{Hom}_R(M,N)$.

Proof. We need to check that $\mathrm{Hom}_R(M,-)$ preserves compositions and identities. We first check that it preserves compositions. Let $\varphi \colon N \to N'$ and $\varphi' \colon M' \to N''$ be two R-linear maps and let $\psi \in \mathrm{Hom}_R(M,N)$. Then we have

$$\begin{aligned} (\varphi'\varphi)_*(\psi) &= \varphi'\varphi\psi \\ &= \varphi'_*(\varphi\psi) \\ &= \varphi'_*(\varphi_*(\psi)) \\ &= (\varphi'_*\varphi_*)(\psi) \end{aligned}$$

It follows that $(\varphi'\varphi)_* = \varphi'_*\varphi_*$. Hence $\mathrm{Hom}_R(M, -)$ preserves compositions. Next we check that $\mathrm{Hom}_R(M, -)$ preserves identities. Let N be an R-module and let $\psi \in \mathrm{Hom}_R(M, N)$. Then we have

$$\begin{aligned}(1_N)_*(\psi) &= 1_N\psi \\ &= \psi \\ &= 1_{\mathrm{Hom}_R(M,N)}(\psi).\end{aligned}$$

It follows that $(1_N)_* = 1_{\mathrm{Hom}_R(M,N)}$. Hence $\mathrm{Hom}_R(M, -)$ preserves identities. □

7.2.2 The Contravariant Functor $\mathrm{Hom}_R(-, N)$

Proposition 7.3. *Let N be an R-module. We obtain a contravariant functor*

$$\mathrm{Hom}_R(-, N)\colon \mathbf{Mod}_R \to \mathbf{Mod}_R$$

from the category of R-modules to itself, where the R-module M is assigned to the R-module $\mathrm{Hom}_R(M, N)$ and where the R-linear map $\varphi\colon M \to M'$ is assigned to the R-linear map $\varphi^*\colon \mathrm{Hom}_R(M', N) \to \mathrm{Hom}_R(M, N)$, where φ^* is defined by

$$\varphi^*(\psi') = \psi'\varphi$$

for all $\psi' \in \mathrm{Hom}_R(M', N)$.

Proof. We need to check that $\mathrm{Hom}_R(-, N)$ preserves compositions and identities. We first check that it preserves compositions. Let $\varphi\colon M \to M'$ and $\varphi'\colon M' \to M''$ be two R-linear maps and let $\psi'' \in \mathrm{Hom}_R(M'', N)$. Then we have

$$\begin{aligned}(\varphi'\varphi)^*(\psi'') &= \psi''\varphi'\varphi \\ &= (\varphi'^*(\psi''))\varphi \\ &= \varphi^*(\varphi'^*(\psi'')) \\ &= (\varphi^*\varphi'^*)(\psi'')\end{aligned}$$

It follows that $(\varphi'\varphi)^* = (\varphi^*\varphi'^*)$. Hence $\mathrm{Hom}_R(-, N)$ preserves compositions. Next we check that $\mathrm{Hom}_R(-, N)$ preserves identities. Let M be an R-module and let $\psi \in \mathrm{Hom}_R(M, N)$. Then we have

$$\begin{aligned}(1_M)^*(\psi) &= \psi 1_M \\ &= \psi \\ &= 1_{\mathrm{Hom}_R(M,N)}(\psi).\end{aligned}$$

It follows that $(1_M)^* = 1_{\mathrm{Hom}_R(M,N)}$. Hence $\mathrm{Hom}_R(-, N)$ preserves identities. □

7.2.3 Left Exactness of $\mathrm{Hom}_R(-N)$

Proposition 7.4. *The sequence of R-modules*

$$\begin{tikzcd} M_1 \arrow[r, "\varphi_1"] & M_2 \arrow[r, "\varphi_2"] & M_3 \arrow[r] & 0 \end{tikzcd} \quad (40)$$

is exact if and only if for all R-modules N the induced sequence

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Hom}_R(M_3, N) \arrow[r, "\varphi_2^*"] & \mathrm{Hom}_R(M_2, N) \arrow[r, "\varphi_1^*"] & \mathrm{Hom}_R(M_1, N) \end{tikzcd} \quad (41)$$

is exact.

Proof. Suppose that (40) is exact and let N be any R-module. We first show exactness at $\mathrm{Hom}_R(M_3, N)$. Let $\psi_3 \in \ker \varphi_2^*$. Then

$$\begin{aligned}0 &= \varphi_2^*(\psi_3) \\ &= \psi_3\varphi_2 \\ &= \psi_3,\end{aligned}$$

where we used the fact that φ_2 is surjective to obtain the third line from the second line. Therefore φ_2^* is injective, which implies exactness at $\mathrm{Hom}_R(M_3, N)$.

Next we show exactness at $\mathrm{Hom}_R(M_2, N)$. Let $\psi_2 \in \ker \varphi_1^*$. Then

$$\begin{aligned} 0 &= \varphi_1^*(\psi_2) \\ &= \psi_2\varphi_1 \end{aligned}$$

implies ψ_2 kills the image of φ_1. We define $\psi_3 \colon M_3 \to N$ as follows: let $u_3 \in M_3$. Choose $u_2 \in M_2$ such that $\varphi_2(u_2) = u_3$ (such a choice is possible since φ_2 is surjective). We define

$$\psi_3(u_3) = \psi_2(u_2).$$

The map ψ_3 is well-defined since ψ_2 kills the image of φ_1. Indeed, if $v_2 \in M_2$ was another lift of u_3 under φ_2, then

$$\begin{aligned} v_2 - u_2 &\in \ker \varphi_2 \\ &= \mathrm{im}\, \varphi_1. \end{aligned}$$

Thus

$$\begin{aligned} \psi_2(v_2) &= \psi_2(v_2 - u_2 + u_2) \\ &= \psi_2(v_2 - u_2) + \psi_2(u_2) \\ &= \psi_2(u_2). \end{aligned}$$

Thus the map ψ_3 is well-defined. The map ψ_3 is also R-linear. Indeed, let $a, b \in R$ and let $u_3, v_3 \in M_3$. Choose lifts of u_3, v_3 under φ_2, say $u_2, v_2 \in M_2$ (so $\varphi_2(u_2) = u_3$ and $\varphi(v_2) = v_3$). Then $au_2 + bv_2$ is easily seen to be a lift of $au_3 + bv_3$ under φ and so we have

$$\begin{aligned} \psi_3(au_3 + bv_3) &= \psi_2(au_2 + bv_2) \\ &= a\psi_2(u_2) + b\psi_2(v_2) \\ &= a\psi_3(u_3) + b\psi_3(v_3). \end{aligned}$$

Thus ψ_3 is R-linear. Finally, observe that

$$\begin{aligned} \varphi_2^*(\psi_3)(u_2) &= (\psi_3\varphi_2)(u_2) \\ &= \psi_3(\varphi_2(u_2)) \\ &= \psi_3(u_3) \\ &= \psi_2(u_2) \end{aligned}$$

for all $u_2 \in M_2$. It follows that $\psi_2 = \varphi_2^*(\psi_3)$, and hence $\psi_2 \in \mathrm{im}\, \varphi_2^*$. Therefore we have exactness at $\mathrm{Hom}_R(M_2, N)$.

Conversely, suppose that (40) is exact for all R-modules N. We first show φ_2 is surjective. Set $N = M_3/\mathrm{im}\, \varphi_2$ and let $\pi \colon M_3 \to M_3/\mathrm{im}\, \varphi_2$ be the quotient map. Observe that

$$\begin{aligned} \varphi_2^*(\pi) &= \pi\varphi_2 \\ &= 0 \\ &= \varphi_2^*(0). \end{aligned}$$

It follows from injectivity of φ_2^* that $\pi = 0$. In other words, $M_3 = \mathrm{im}\, \varphi_2$, hence φ_2 is surjective.

Next we show exactness at M_2. First set $N = M_3$. Then exactness of (40) implies

$$\begin{aligned} 0 &= (\varphi_1^*\varphi_2^*)(1_{M_3}) \\ &= (\varphi_1^*(\varphi_2^*(1_{M_3})) \\ &= \varphi_1^*(1_{M_3}\varphi_2) \\ &= 1_{M_3}\varphi_2\varphi_1 \\ &= \varphi_2\varphi_1. \end{aligned}$$

Thus $\ker \varphi_2 \supseteq \mathrm{im}\, \varphi_1$. For the reverse inclusion, set $N = M_2/\mathrm{im}\, \varphi_1$ and let $\pi \colon M_2 \to M_2/\mathrm{im}\, \varphi_1$ be the quotient map. Then

$$\begin{aligned} \varphi_1^*(\pi) &= \pi\varphi_1 \\ &= 0 \end{aligned}$$

implies there exists $\psi_3 \colon M_3 \to M_2/\operatorname{im}\varphi_1$ such that $\pi = \varphi_2^*(\psi_3)$ by exactness of (40). Thus, if $u_2 \in \ker \varphi_2$, then

$$\begin{aligned} 0 &= \psi_3(0) \\ &= \psi_3(\varphi_2(u_2)) \\ &= (\psi_3\varphi_2)(u_2) \\ &= (\varphi_2^*(\psi_3))(u_2) \\ &= \pi(u_2) \end{aligned}$$

implies $u_2 \in \operatorname{im}\varphi_1$. Thus $\ker\varphi_2 \subseteq \operatorname{im}\varphi_1$. □

7.2.4 Naturality

Proposition 7.5. *Let $\varphi \colon M \to M'$ be an R-linear map. Then we obtain an induced natural transformation*

$$\operatorname{Hom}_R(\varphi, -) \colon \operatorname{Hom}_R(M, -) \to \operatorname{Hom}_R(M', -)$$

between functors.

Proof. Let $\psi \colon N \to N'$ be an R-linear map. We need to check that the following diagram commutes

$$\begin{tikzcd} \operatorname{Hom}_R(M,N) \arrow[r, "\varphi^*"] \arrow[d, "\psi_*"'] & \operatorname{Hom}_R(M',N) \arrow[d, "\psi_*"] \\ \operatorname{Hom}_R(M,N') \arrow[r, "\varphi^*"'] & \operatorname{Hom}_R(M',N') \end{tikzcd} \tag{42}$$

Let $\phi \in \operatorname{Hom}_R(M,N)$. Then we have

$$\begin{aligned} (\psi_*\varphi^*)(\phi) &= \psi_*(\varphi^*(\phi)) \\ &= \psi_*(\phi\varphi) \\ &= \psi\phi\varphi \\ &= \varphi^*(\psi\phi) \\ &= \varphi^*(\psi_*(\phi)) \\ &= (\varphi^*\psi_*)(\phi). \end{aligned}$$

It follows that $\psi_*\varphi^* = \varphi^*\psi_*$, and so the diagram (42) commutes. □

Remark. By a similar argument, every R-linear map $\psi \colon N \to N'$ induces a natural transformation

$$\operatorname{Hom}_R(-, \psi) \colon \operatorname{Hom}_R(-, N) \to \operatorname{Hom}_R(-, N').$$

8 Nakayama's Lemma and its Consequences

Nakayama's Lemma is a powerful tool we use in Commutative Algebra. In order to know Commutative Algebra, one must be familiar with Nakayama's Lemma. Before we state and prove Nakayama's Lemma, we need to discuss the Jacobson radical of a ring.

Definition 8.1. The **Jacobson radical** of R, denoted $\operatorname{rad}(R)$, is defined by the formula

$$\operatorname{rad}(R) := \bigcap_{\substack{\mathfrak{m} \subset R \\ \mathfrak{m} \text{ maximal}}} \mathfrak{m}.$$

Example 8.1. Suppose $(R, \mathfrak{m})$ is a local ring. Then $\operatorname{rad}(R) = \mathfrak{m}$.

Proposition 8.1. *Let $x \in \operatorname{rad}(R)$. Then $1 - x \in R^\times$.*

Proof. Suppose that $1 - x \notin R^\times$. Then there exists a maximal ideal which contains $1 - x$, choose $\mathfrak{m}$ to be this maximal ideal. But then this implies $x \notin \mathfrak{m}$, contradicting the fact that $x \in \operatorname{rad}(R)$. □

8.1 Nakayama's Lemma

We now state and prove Nakayama's Lemma:

Lemma 8.1. *(Nakayama). Let R be a ring, let I be an ideal contained in $\mathrm{rad}(R)$, let M a finitely generated R-module, and let $N \subset M$ a submodule such that $M = IM + N$. Then $M = N$. In particular, if $M = IM$, then $M = 0$.*

Proof. Assume $M \neq N$, and let $u_1, \dots, u_s \in M$ such that their classes form a system of generators of M/N and where s is minimal. Since $u_s \in M = IM + N$, there exists $x_1, \dots, x_s \in I$ and $v \in N$ such that

$$u_s = \sum_{r=1}^{s} x_r u_r + v.$$

This implies

$$(1 - x_s)u_s = \sum_{r=1}^{s-1} x_r u_r + v.$$

Since x_s is contained in every maximal ideal, $1 - x_s$ is a unit in R, and so

$$u_s = \sum_{r=1}^{s-1} x_r (1 - x_s)^{-1} u_r + (1 - x_s)^{-1} v,$$

which contradicts the minimality of the chosen system of generators. □

Corollary. *Let $(R, \mathfrak{m})$ be a local ring, let M a finitely-generated R-module, and let $u_1, \dots, u_s$ be elements in M such that their classes form a system of generators for the $(R/\mathfrak{m})$-vector space $M/\mathfrak{m}M$. Then $u_1, \dots, u_s$ generates M as an R-module.*

Proof. Since $\overline{u}_1, \dots, \overline{u}_s$ generates $M/\mathfrak{m}M$ as an $(R/\mathfrak{m})$-vector space, we have

$$M = \mathfrak{m}M + \sum_{r=1}^{s} R u_r. \tag{43}$$

Indeed, let $u \in M$. Choose $a_1, \dots, a_s \in R$ such that

$$\overline{u} = \sum_{r=1}^{s} \overline{a}_r \overline{u}_r = \sum_{r=1}^{s} a_r \overline{u}_r.$$

This implies $u - \sum_{r=1}^{s} a_r u_r \in \mathfrak{m}M$. Thus

$$u = \left(u - \sum_{r=1}^{s} a_r u_r \right) + \sum_{r=1}^{s} a_r u_r,$$

shows us that $u \in \mathfrak{m}M + \sum_{r=1}^{s} R u_r$. Combining (43) with Nakayama's Lemma, we see that

$$M = \sum_{r=1}^{s} R u_r.$$

□

Remark. The finite generation hypothesis is crucial. For a counterexample, consider the local ring $R = \mathbb{Z}_{(p)}$ and the quotient R-module $\mathbb{Q}/\mathbb{Z}_{(p)}$. In this case $\mathfrak{m} = pR$, so

$$\begin{aligned} M/\mathfrak{m}M &= M/pM \\ &= 0, \end{aligned}$$

since every element of $\mathbb{Q}$ has the form px for some $x \in \mathbb{Q}$. However, obviously $M \neq 0$ (and also M is not finitely generated as an R-module in this case).

Example 8.2. Let $R = K[x, y, z]_{\langle x,y,z \rangle}$, let $\mathfrak{m} = \langle x, y, z \rangle$, and let M be the R-module with presentation

$$\begin{tikzcd} R^2 \arrow[r, "\begin{pmatrix} 0 & y \\ xy-1 & xz \\ xy+1 & xz \end{pmatrix}"] & R^3 \arrow[r] & M \arrow[r] & 0. \end{tikzcd}$$

Let $u_i \in M$ be the image the standard basis element $e_i \in R^3$ for $i = 1, 2, 3$. The set $\{u_1, u_2, u_3\}$ is *not* a minimal generating set of M. Indeed, since the functor $- \otimes_R (R/\mathfrak{m})$ is right-exact, we obtain a presentation of the $(R/\mathfrak{m})$-vector space $M/\mathfrak{m}M$:

$$\begin{tikzcd}
(R/\mathfrak{m})^2 \arrow[r, "\begin{pmatrix} 0 & 0 \\ -1 & 0 \\ 1 & 0 \end{pmatrix}"] & (R/\mathfrak{m})^3 \arrow[r] & M/\mathfrak{m}M \arrow[r] & 0
\end{tikzcd}$$

This presentation matrix has rank 1, and so $M/\mathfrak{m}M$ is a 2-dimensional K-vector space. In fact, it's not hard to see that

$$M/\mathfrak{m}M = K\overline{u}_1 + K\overline{u}_3,$$

since the equation $-\overline{u}_2 + \overline{u}_3 = 0$ tells us that $\overline{u}_2$ is superfluous. According to Nakayama's Lemma, we should be able to lift $\overline{u}_1, \overline{u}_3 \in M/\mathfrak{m}M$ to a minimal generating set of M. In particular, $\{u_1, u_3\}$ should be a minimal generating set of M. To see that it is, we use the fact that $xy - 1$ is a unit in R to perform the following sequence of elementary row and column operations:

$$\begin{pmatrix} 0 & y \\ xy-1 & xz \\ xy+1 & xz \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & y \\ xy-1 & xz \\ 0 & \frac{-2xz}{xy-1} \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & y \\ xy-1 & 0 \\ 0 & \frac{-2xz}{xy-1} \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & y \\ 1 & 0 \\ 0 & \frac{-2xz}{xy-1} \end{pmatrix}.$$

Letting $\{e_1', e_2'\}$ denote the standard basis for R^2, then this sequence of elementary row operations corresponds base changes:

$$\{e_1, e_2, e_3\} \to \{e_1, (xy-1)e_2 + (xy+1)e_3, e_3\} \qquad \text{and} \qquad \{e_1', e_2'\} \to \left\{ e_1', \frac{-xz}{xy-1}e_1' + e_2' \right\}.$$

So we see that $\begin{pmatrix} 0 & y \\ 1 & 0 \\ 0 & \frac{-2xz}{xy-1} \end{pmatrix}$ can be used as a presentation matrix for M. Again, the trivial condition $u_2 = 0$ implies that we can toss u_2 out, so that

$$M = Ru_1 + Ru_3.$$

8.2 Krull's Intersection Theorem

We now prove the following important corollary of Nakayama's Lemma:

Corollary. *(Krull's interesection theorem) Let R be a Noetherian ring, let I be an ideal contained in the Jacobson radical of R, and let M a finitely generated R-module. Then*

$$\bigcap_{k \in \mathbb{N}} I^k M = 0.$$

Proof. Let $N := \bigcap_k I^k M$. Then N is a finitely generated R-module since it is a submodule of the finitely generated module M over the Noetherian ring R. By Nakayama's Lemma, it is sufficient to show that $IN = N$. Let

$$\mathcal{L} := \{L \subset M \text{ submodule } \mid L \cap N = IN\}.$$

The set $\mathcal{L}$ is nonempty since $IN \in \mathcal{L}$. Since R is Noetherian, the set $\mathcal{L}$ has a maximal element, choose $L \in \mathcal{L}$ to be such a maximal element. It remains to prove that $I^k M \subset L$ for some k, because this implies

$$\begin{aligned} N &= I^k M \cap N \\ &\subset L \cap N \\ &= IN, \end{aligned}$$

and from Nakayama's Lemma, we would conclude that $N = 0$. Since I is finitely generated, it suffices to prove that for any $x \in I$ there is some positive integer $n \in \mathbb{N}$ such that $x^n M \subset L$ (If $I = \langle x_1, \dots, x_s \rangle$ with $x_r^{n_r} M \subset L$ for each $1 \leq r \leq s$, then $I^{n_1 + \cdots + n_s} M \subset L$).

Let $x \in I$ and consider the chain of ideals

$$L :_M x \subset L :_M x^2 \subset \cdots.$$

This chain stabilizes because R is Noetherian. Choose $n \in \mathbb{N}$ with $L :_M x^n = L :_M x^{n+1}$. We claim that $x^n M \subset L$. Indeed, by the maximality of L it is enough to prove that $(L + x^n M) \cap N \subset IN$ since obviously,

$$\begin{aligned} IN &= L \cap N \\ &\subset (L + x^n M) \cap N. \end{aligned}$$

Let $u \in (L + x^n M) \cap N$, so $u = v + x^n w$, with $v \in L$ and $w \in M$. Now

$$\begin{aligned} x^{n+1} w &= xu - xv \\ &\in IN + L \\ &= L \cap N + L \\ &= L, \end{aligned}$$

which implies $w \in L :_M x^{n+1} = L :_M x^n$. Therefore, $x^n w \in L$, and, consequently, $u \in L$. This implies $u \in L \cap N = IN$. □

8.3 Filtered Rings and Modules

Definition 8.2. A **filtered ring** is a ring R together with a descending sequence $(I_n)_{n \in \mathbb{Z}_{\geq 0}}$ of ideals in R which satisfies $I_0 = R$ and $R_m R_m \subseteq R_{m+n}$. A **filtered module** over the filtered ring R is an R-module M together with descending sequence $(M_n)_{n \in \mathbb{Z}}$ of submodules of M which satisfies $M_0 = M$ and $R_m M_n \subseteq M_{m+n}$. We often specify a filtered ring in terms of the sequence (R_n). Similarly, we often specify a filtered module in terms of its sequence (M_n).

Definition 8.3. Let R be a ring and let Q be an ideal in R. Then (Q^n) is a filtered ring. We call (Q^n) the **standard Q-filtration** of R. A filtered module (M_n) over the filtered ring (Q^n) is called a **Q-filtration** of M_0. Let M be any R-module. It is easy to see that if (M_n) is a descending sequence of submodules of M such that $M = M_0$, then (M_n) is a Q-filtration of M if and only if $QM_n \subseteq M_{n+1}$ for all $n \in \mathbb{Z}$. A Q-filtration (M_n) of M is called **stable** if $QM_n = M_{n+1}$ for all sufficiently large n. We denote by $\mathfrak{F}_Q(M)$ to be the set of all Q-filtrations of M. If Q is understood from context, then we will drop Q from the subscript and simply write $\mathfrak{F}(M)$.

Unless otherwise specified, we fix a ring R, an ideal Q in R, and an R-module M. We give R the structure of a filtered ring via the standard Q-filtration (Q^n). We wish to study Q-filtrations of M.

8.3.1 Equivalence Relation $\mathfrak{F}(M)$

Definition 8.4. Let (M_n) and (M'_n) be two Q-filtrations of M. We say $(M_n) \geq (M'_n)$ if there exists $d \in \mathbb{N}$ such that $M_{n+d} \subseteq M'_n$ for all $n \in \mathbb{N}$. If $(M_n) \geq (M'_n)$ and $(M'_n) \geq (M_n)$, then we say (M_n) and (M'_n) are **equivalent Q-filtrations** and denoted this by $(M_n) \sim (M'_n)$.

Proposition 8.2. *The relation $\sim$ is an equivalence relation.*

Proof. Reflexivity and symmetry of $\sim$ are clear. To see transitivity also holds, suppose $(M_n) \sim (M'_n)$ and $(M'_n) \sim (M''_n)$. Choose $d \in \mathbb{N}$ such that $M_{n+d} \subset M'_n$ and $M'_{n+d} \subset M_n$ for all $n \in \mathbb{N}$ and choose $d' \in \mathbb{N}$ such that $M'_{n+d'} \subset M''_n$ and $M''_{n+d'} \subset M'_n$. Then for all $n \in \mathbb{N}$, we have

$$M_{n+d+d'} \subseteq M'_{n+d'} \subseteq M''_n.$$

Similarly for for all $n \in \mathbb{N}$, we have

$$M''_{n+d+d'} \subseteq M'_{n+d} \subseteq M_n.$$

It follows that $(M_n) \sim (M''_n)$. □

Remark. Note that if (M_n) is a stable Q-filtration, then $(M_n) \sim (Q^n M)$. In particular, if (M'_n) is another stable Q-filtration, then $(M_n) \sim (M'_n)$.

8.3.2 Preimage of Filtration is Filtration

Proposition 8.3. *Let N be an R-module, let $\varphi \colon N \to M$ be an R-module homomorphism of A-modules, and let (M_n) be a Q-filtration of M. Then $(\varphi^{-1}(M_n))$ is a Q-filtration of N. Moreover, if (M'_n) is another Q-filtration of M such that $(M'_n) \sim (M_n)$, then $(\varphi^{-1}(M'_n)) \sim (\varphi^{-1}(M_n))$.*

Proof. We first show that $(\varphi^{-1}(M_n))$ is a Q-filtration of N. Clearly $(\varphi^{-1}(M_n))$ is a descending chain of submodules of N with $\varphi^{-1}(M_0) = N$. Also we have

$$\begin{aligned} Q\varphi^{-1}(M_n) &\subset \varphi^{-1}(QM_n) \\ &\subset \varphi^{-1}(M_{n+1}) \end{aligned}$$

for all $n \geq 0$. Thus $(\varphi^{-1}(M_n))$ is a Q-filtration of N.

Now we will show $(\varphi^{-1}(M_n))$ is equivalent to $(\varphi^{-1}(M'_n))$. Choose a positive integer k such that $M_{n+k} \subset M'_n$ and $M'_{n+k} \subset M_n$ for all $n \geq 0$. Then $\varphi^{-1}(M_{n+k}) \subset \varphi^{-1}(M'_n)$ and $\varphi^{-1}(M'_{n+k}) \subset \varphi^{-1}(M_n)$. Thus $(\varphi^{-1}(M_n))$ is equivalent to $(\varphi^{-1}(M'_n))$. □

Remark. Thus, a homomorphism of R-modules $\varphi\colon N \to M$ induces a well-defined map

$$\mathcal{C}^\infty_Q(\varphi)\colon \mathcal{C}^\infty_Q(M) \to \mathcal{C}^\infty_Q(N).$$

8.3.3 Blowups

Definition 8.5. The **blowup algebra of** Q **in** R is the graded R-algebra

$$\mathrm{B}_Q(R) := R + Qt + Q^2t^2 + Q^3t^3 + \cdots \cong \bigoplus_{n\geq 0} Q^n,$$

where we view t as an indeterminate variable which keeps track of the grading: the homogeneous component in degree n is

$$\mathrm{B}_Q(R)_n := Q^n t^n,$$

and where multiplication is uniquely determined by

$$(xt^m)(yt^n) = xyt^{m+n}$$

for all $xt^m \in Q^m t^m$ and $yt^n \in Q^n t^n$. The **blowup module of** Q **with respect to** M is the graded R-module

$$B_Q(M) := M + QMt + Q^2Mt^2 + Q^3Mt^3 + \cdots \cong \bigoplus_{n\geq 0} Q^n M.$$

where the R-module action is uniquely determined by

$$(xt^m)(ut^n) = xut^{m+n}$$

for all $xt^m \in Q^m t^m$ and $ut^n \in Q^n M t^n$.

Proposition 8.4. *The blowup algebra* $\mathrm{B}_Q(R)$ *is a Noetherian ring.*

Proof. Since R is Noetherian, Q is a finitely-generated R-ideal, say $Q = \langle f_1, \dots, f_s \rangle_R$. This implies that the irrelevant ideal $Qt\mathrm{B}_Q(R)$ in $\mathrm{B}_Q(R)$ is a finitely-generated $\mathrm{B}_Q(R)$-ideal, with $Qt\mathrm{B}_Q(R) = \langle f_1 t, \dots, f_s t \rangle_{\mathrm{B}_Q(R)}$. Therefore there is an R-algebra homomorphism

$$\varphi\colon R[X_1, \dots, X_s] \to \mathrm{B}_Q(R)$$

induced by $\varphi(X_r) = tf_r$ for all $1 \leq r \leq s$. This homomorphism is a surjective ring homomorphism from a Noetherian ring, and hence $\mathrm{B}_Q(R)$ is a Noetherian ring. □

Example 8.3. Let $R = K[x,y]/\langle y^2 - x^3 - x^2 \rangle$, let $Q = \langle \overline{x}, \overline{y} \rangle$, and let

$$\varphi\colon R[u,v] \to \mathrm{B}_Q(R)$$

be the surjective R-algebra homomorphism induced by $u \mapsto \overline{x}t$ and $v \mapsto \overline{y}t$. The kernel of φ is an ideal which is homogeneous in the variables u, v

$$\ker \varphi = \langle v^2 - (\overline{x} + 1)u^2, \overline{x}v - \overline{y}u \rangle.$$

In particular, $\mathrm{B}_Q(R)$ corresponds to an algebraic subset $Z \subset \mathbb{A}^2 \times \mathbb{P}^1$.

8.3.4 Artin-Rees Lemma

In this subsubsection, suppose M is finitely-generated. We are almost ready to state and prove Artin-Rees Lemma, but before we do so, let us give a criterion for stability: Let (M_n) be a Q-filtration. We set $\overline{M}$ to be the $\mathrm{B}_Q(R)$-module given by

$$\overline{M} := M + M_1 t + M_2 t^2 + \cdots .$$

Furthermore, for each $n \geq 0$, let

$$\begin{aligned}\overline{M}_n &:= M + M_1 t + \cdots + M_{n-1}t^{n-1} + \mathrm{B}_Q(R) M_n t^n \\ &= M + M_1 t + \cdots + M_{n-1}t^{n-1} + M_n t^n + Q M_n t^{n+1} + Q^2 M_n t^{n+2} + \cdots .\end{aligned}$$

Observe that $\overline{M}_n \subset \overline{M}_{n+1}$ for all $n \geq 0$ and $\bigcup_{n=0}^{\infty} \overline{M}_n = \overline{M}$. Thus the sequence of $\mathrm{B}_Q(R)$-modules $(\overline{M}_n)$ is an ascending sequence whose union is $\overline{M}$.

Lemma 8.2. *(Criterion for stability). $\overline{M}$ is a finitely-generated $\mathrm{B}_Q(R)$-module if and only if (M_n) is Q-stable.*

Proof. Suppose $\overline{M}$ is finitely-generated. Then $\overline{M}$ is Noetherian, and so the ascending sequence $(\overline{M}_n)$ of submodules of $\overline{M}$ must terminate, say at $k \geq 0$. This implies $\overline{M}_k = \overline{M}$ since the union of the ascending sequence is $\overline{M}$, and this happens if and only if $M_{n+k} = Q^n M_k$ for all $n \geq 0$. Hence (M_n) is Q-stable.

Conversely, suppose (M_n) is Q-stable. Then as arged above, there exists a $k \geq 0$ such that $\overline{M}_k = \overline{M}$. Choose such a $k \geq 0$ and observe that the submodules M_n are finitely-generated R-modules for all $n \geq 0$ (and hence finitely-generated $\mathrm{B}_Q(R)$-modules too). Thus

$$\begin{aligned}\overline{M} &= \overline{M}_k \\ &= M + M_1 t + \cdots + M_{k-1}t^{k-1} + \mathrm{B}_Q(R) M_k t^k\end{aligned}$$

is a finitely-generated $\mathrm{B}_Q(R)$-module. □

Now we state and prove Artin-Rees Lemma:

Lemma 8.3. *(Artin-Rees Lemma) Let (M_n) be a stable Q-filtration of M and let N be a submodule of M. Then $(M_n \cap N)$ is a stable Q-filtration of N.*

Proof. By Proposition (8.3), we know that $(M_n \cap N)$ is a Q-filtration of N since it is the sequence obtained from the inverse image of the inclusion map $N \hookrightarrow M$. It remains to show that $(M_n \cap N)$ is stable. Appealing to (8.2), we just need to show that $\overline{N}$ is a finitely-generated $\mathrm{B}_Q(R)$-module, where

$$\overline{N} := N + (M_1 \cap N)t + (M_2 \cap N)t^2 + \cdots .$$

This is clear though since $\overline{N}$ is a $\mathrm{B}_Q(R)$-submodule of $\overline{M}$ which is finitely-generated, and since $\mathrm{B}_Q(R)$ is Noetherian, $\overline{N}$ must be finitely-generated too. □

8.3.5 Consequences of Artin-Rees Lemma

We begin with an alternative proof of Krull's Intersection Theorem:

Lemma 8.4. *(Krull's Interesection Theorem) Let $(R, \mathfrak{m})$ be a Noetherian local ring, let Q be an ideal in R, and let M be a finitely-generated R-module. Then*

$$\bigcap_{n \in \mathbb{N}} Q^n M = 0.$$

Proof. Set $N := \bigcap_{n \in \mathbb{N}} Q^n M$. By Artin-Rees, the Q-filtration $(N \cap Q^n M)$ is stable. Thus there exists a positive integer k such that

$$\begin{aligned}QN &= Q\left(N \cap Q^k M\right) \\ &= N \cap Q^{k+1} M \\ &= N,\end{aligned}$$

and by Nakayama's lemma, this implies $N = 0$. □

Proposition 8.5. *Let R be a Noetherian ring, let $\mathfrak{p}$ be a prime ideal of R, and let I be an ideal of R. For any homomorphism $\varphi \colon I \to R/\mathfrak{p}$, there exists a positive integer d such that φ factors through*

$$I/(\mathfrak{p}^d \cap I) \cong (\mathfrak{p}^d + I)/\mathfrak{p}^d.$$

Proof. By Artin-Rees, $(I \cap \mathfrak{p}^n)$ is a stable $\mathfrak{p}$-filtration. Therefore this exists a positive integer d such that $I \cap \mathfrak{p}^d = \mathfrak{p}\left(I \cap \mathfrak{p}^{d-1}\right)$. This implies $I \cap \mathfrak{p}^d \subset \ker \varphi$. □

Proposition 8.6. *Let A be a ring, Q an ideal in A, and let*

$$\begin{tikzcd} 0 \arrow[r] & M_1 \arrow[r] & M_2 \arrow[r] & M_3 \arrow[r] & 0 \end{tikzcd}$$

be a short exact sequence of A-modules. Then

$$\begin{tikzcd} 0 \arrow[r] & B_Q(M_1) \arrow[r] & B_Q(M_2) \arrow[r] & B_Q(M_3) \end{tikzcd}$$

is exact.

Proof. □

8.4 Topology Induced by Q-Filtration

Throughout this subsection, let M be an R-module and let Q be an ideal in R.

Definition 8.6. Let (M_n) be a Q-filtration of M. For each $u \in M$ and $m \geq 0$ we define

$$\mathrm{B}_{1/m}^{(M_n)}(u) := u + M_m. \tag{44}$$

The reason we write $1/m$ in the subscript and not m in the subscript will become apparent soon enough. If the Q-filtration (M_n) is understood from context, then we will drop it from the superscript in $\mathrm{B}_{1/m}^{(M_n)}(u)$ in order to clean notation. Next we define

$$\mathcal{B}^{(M_n)} = \left\{\mathrm{B}_{1/m}^{(M_n)}(u) \mid u \in M \text{ and } m \geq 0\right\}.$$

Again if (M_n) is understood from context, then we will drop it from the superscript in $\mathcal{B}^{(M_n)}$. Finally, let $\tau(\mathcal{B})$ be the smallest topology which contains $\mathcal{B}$. The toplogy $\tau(\mathcal{B})$ is called the **topology induced by the filtration** (M_n).

Proposition 8.7. *$\mathcal{B}$ is a basis for $\tau(\mathcal{B})$.*

Proof. First note that $\mathcal{B}$ covers M. Indeed, for any $m \geq 0$ we have

$$M \subseteq \bigcup_{u \in M} \mathrm{B}_{1/m}(u).$$

In fact, we already have $M = \mathrm{B}_0(0)$! Next let $u, v \in M$ and let $n \geq m \geq 0$. Then observe that

$$\mathrm{B}_{1/m}(u) \cap \mathrm{B}_{1/n}(v) = \begin{cases} \mathrm{B}_{1/n}(v) & \text{if } u - v \in M_m \\ \emptyset & \text{else} \end{cases}$$

In particular we see that $\mathcal{B}$ is a basis for $\tau(\mathcal{B})$. □

Proposition 8.8. *Let (M_n) and (M'_n) be two Q-filtrations of M. Then $\tau(\mathcal{B}^{(M_n)}) \supseteq \tau(\mathcal{B}^{(M'_n)})$ if and only if $(M_n) \geq (M'_n)$. In particular, $\tau(\mathcal{B}^{(M_n)}) = \tau(\mathcal{B}^{(M'_n)})$ if and only if $(M_n) \sim (M'_n)$.*

Proof. Observe that $\tau(\mathcal{B}^{(M_n)}) \supseteq \tau(\mathcal{B}^{(M'_n)})$ if and only if for each $u + M'_m \in \mathcal{B}^{(M'_n)}$ there exists a $u + M_{\pi(m)} \in \mathcal{B}^{(M_n)}$ such that $u + M'_m \supseteq u + M_{\pi(m)}$, or equivalently, such that $M'_m \supseteq M_{\pi(m)}$. Since (M_n) is descending, this is equivalent to there being some $d \in \mathbb{N}$ such that $M'_m \supseteq M_{m+d}$. □

Definition 8.7. Suppose (M_n) is a Q-stable filtration (so $(M_n) \sim (Q^n M)$). Then the topology $\tau(\mathcal{B}^{(M_n)})$ is called the **Q-adic topology**. By Proposotion (8.8), any choice of a stable Q-filtration would result in the same topology.

8.4.1 Hausdorff Criterion

Proposition 8.9. *Let (M_n) be a Q-filtration of M and equip M with the topology induced by (M_n). Then M is Hausdorff if and only if $\bigcap_{n=1}^{\infty} M_n = 0$.*

Proof. Suppose $\bigcap_{n=1}^{\infty} M_n = 0$ and let $u, v \in M$ be distinct elements. Since $\bigcap_{n=1}^{\infty} M_n = 0$, there exists some $m \in \mathbb{N}$ such that $u - v \notin M_m$. Then note that $\mathrm{B}_{1/m}(u)$ and $\mathrm{B}_{1/m}(v)$ are open neighborhoods of u and v respectively, both of which are disjoint from one another. It follows that M is Hausdorff.

Conversely, suppose M is Hausdorff and assume for a contradiction that $\bigcap_{n=1}^{\infty} M_n \neq 0$. Choose any nonzero $u \in \bigcap_{n=1}^{\infty} M_n$. Then 0 and u are two distinct elements of M, but there does not exist an open neighborhood of 0 and an open neighborhood of u both of which are disjoint from each other. Indeed, if U is an open neighborhood of 0 and V is an open neighborhood of u, then we can choose $n \in \mathbb{N}$ such that $M_n \subseteq U$ and $M_n \subseteq V$. But $0 \in M_n$ and $u \in M_n$, so $0 \in V$ and $u \in U$. Thus U and V have nonempty intersection. This is a contradiction as M is Hausdorff. □

8.4.2 Subspace topology agrees with topology induced by filtration

Let M be an R-module equipped with the topology induced by a Q-filtration (M_n) of M and let N be an R-submodule of M. There are two ways give N a topology. The first way is to give it the subspace topology. The second way is to give it the topology induced by the Q-filtration $(M_n \cap N)$ of N. In fact, these two ways give the same topology:

Proposition 8.10. *With the notation above, we have $\tau(\mathcal{B}^{(M_n)}) \cap N = \tau(\mathcal{B}^{(M_n \cap N)})$.*

Proof. Let $v \in N$ and $m \geq 0$. Then

$$\begin{aligned} \mathrm{B}_{1/m}^{(M_n \cap N)}(v) &= v + M_m \cap N \\ &= (v + M_m) \cap N \\ &= \mathrm{B}_{1/m}(v) \cap N. \end{aligned}$$

It follows that $\tau(\mathcal{B}^{(M_n \cap N)})$ and $\tau(\mathcal{B}^{(M_n)}) \cap N$ have the same basis, and hence $\tau(\mathcal{B}^{(M_n)}) \cap N = \tau(\mathcal{B}^{(M_n \cap N)})$. □

8.4.3 Artin-Rees Lemma

Let M be an R-module equipped with the topology induced by a Q-filtration (M_n) of M and let N be an R-submodule of M. As we've seen above, the subspace topology of N and the topology induced by the Q-filtration $(M_n \cap N)$ of N are in fact the same topology. There is another topology that we can give N. Namely, we consider the topology on N induced by the Q-filtration $(Q^n N)$. If R is Noetherian, M is finitely-generated, and (M_n) is stable, then the Artin-Rees Lemma tells us that $\tau(\mathcal{B}^{(Q^n N)}) = \tau(\mathcal{B}^{(M_n \cap N)})$.

8.4.4 Pseudometric Induced by Q-Filtration

Let (M_n) be a Q-filtration of M. Define $\mathrm{d}_{(M_n)} \colon M \times M \to \mathbb{N}$ by

$$\mathrm{d}_{(M_n)}(u,v) = \begin{cases} 1/n & \text{if } u - v \in M_n \backslash M_{n+1} \\ 0 & \text{if } u - v \in \bigcap_{n \in \mathbb{N}} M_n \end{cases}$$

As usual we supress (M_n) from the subscript of $\mathrm{d}_{(M_n)}$ whenever context is clear. Observe that d is pseudo-metric. Indeed, it is obviously symmetric. It also satisfies the strong triangle inequality:

$$\mathrm{d}(u,w) \leq \max(\mathrm{d}(u,v), \mathrm{d}(v,w))$$

for all $u, v, w \in M$. Indeed, suppose $u, v, w \in M$ such that $u - v \in M_m \backslash M_{m+1}$ and $v - w \in M_n \backslash M_{n+1}$, where without loss of generality, we may assume $n \geq m$. Then $u - w = (u - v) + (v - w) \in M_m$. Thus we certainly have

$$\begin{aligned} \mathrm{d}(u - w) &\leq 1/m \\ &= \max(1/m, 1/n) \\ &= \max(\mathrm{d}(u,v), \mathrm{d}(v,w)). \end{aligned}$$

Finally note that $\mathrm{d}(u,u) = 0$ for all $u \in M$. However there may exist two distinct $u, v \in M$ such that $\mathrm{d}(u,v) = 0$. This is why d is just a pseudo-metric and not a genuine metric: it doesn't necessarily satisfy positive-definiteness. Observe that for each $u \in M$ and $m \geq 0$, we have

$$\begin{aligned} \mathrm{B}_{1/m}(u) &= u + M_m \\ &= \{u + v \mid v \in M_m\} \\ &= \{w \mid u - w \in M_m\} && \text{setting } w = u + v \\ &= \{w \mid \mathrm{d}(u,w) \leq 1/m\}. \end{aligned}$$

Thus the $\mathrm{B}_{1/m}(u)$'s are precisely the open balls in the pseudometric space induced by the pseudo-metric d.

8.5 Convergence, Cauchy Sequences, and Completion

Throughout this subsection, let M be an R-module and equip it with the topology induced by a Q-filtration (M_n) of M.

8.5.1 Basic Definitions

Since $\tau(\mathcal{B})$ is a pseudo-metric space, it makes since to talk about concepts like Cauchy sequences and completions.

Definition 8.8. Let (u_n) be a sequence of elements in M.

1. We say the sequence (u_n) converges to an element $u \in M$ if for all $k \in \mathbb{N}$ there exists $N \in \mathbb{N}$ such that
$$n \geq N \text{ implies } u_n - u \in M_k.$$
In this case, we say (u_n) is a **convergent sequence** and that it **converges** to u. We denote this by $u_n \to u$ as $n \to \infty$, or $\lim_{n\to\infty} u_n = u$, or even just $u_n \to u$.

2. We say the sequence (u_n) is **Cauchy** if for all $k \in \mathbb{N}$ there exists $N \in \mathbb{N}$ such that
$$n, m \geq N \text{ implies } u_m - u_n \in M_k.$$
The set of all Cauchy sequences in M will be denoted $\mathfrak{C}_{(M_n)}(M)$. The set of all Cauchy sequences which converge to 0 is denoted $\mathfrak{C}^0_{(M_n)}(M)$. If the Q-filtration is If the Q-filtration (M_n) is understood from context, then we will drop (M_n) from the subscript and just write $\mathfrak{C}(M)$ and $\mathfrak{C}^0(M)$.

3. We say M is **complete** if every Cauchy sequence in M is a convergent sequence in M.

8.5.2 Analytic Description of Completion

In analysis, one learns about how to construct a completion of a given metric space (X, d). Let us briefly recall how this works. We define $\mathfrak{C}(X)$ to be the set of all Cauchy sequences in X. The metric d on X induces a pseudometric $\widetilde{\mathrm{d}}$ on $\mathfrak{C}(X)$, defined by
$$\widetilde{\mathrm{d}}((x_n), (y_n)) = \lim_{n\to\infty} \mathrm{d}(x_n, y_n). \tag{45}$$
One shows that (45) is a well-defined pseudometric on $\mathfrak{C}(X)$ and that $\mathfrak{C}(X)$ is a complete pseudometric space. To get a genuine metric space, we put an equivalence relation on $\mathfrak{C}(X)$, namely we say $(x_n) \sim (y_n)$ if and only if $\widetilde{\mathrm{d}}((x_n), (y_n)) = 0$. One then shows that the pseudometric $\widetilde{\mathrm{d}}$ on $\mathfrak{C}_X$ induces a genuine metric $[\widetilde{\mathrm{d}}]$ on $[\mathfrak{C}(X)] = \mathfrak{C}(X)/\sim$. Finally one shows that $([\mathfrak{C}(X)], [\widetilde{\mathrm{d}}])$ is a **completion** of (X, d). This means that $[\mathfrak{C}(X)]$ is complete and that the natural map $\iota \colon X \to [\mathfrak{C}(X)]$ given by $x \mapsto (\overline{x})$ is an isometric embedding with dense image. It can be shown that completions are unique up to a unique isometry which respects inclusion maps. Thus we typically refer to $[\mathfrak{C}(X)]$ as *the* completion of X.

8.5.3 Algebraic Description of Completion

Returning to our setting, note that $\mathfrak{C}^0(M)$ plays the role of the equivalence relation $\sim$ above, namely $(u_n) \sim (v_n)$ if and only if $(u_n - v_n) \in \mathfrak{C}^0(M)$. It is easy to then see that $[\mathfrak{C}(M)] = \mathfrak{C}(M)/\mathfrak{C}^0(M)$ is the completion of M. In fact, we have more structure on $[\mathfrak{C}(M)]$. Indeed, $\mathfrak{C}(M)$ is a R-module and $\mathfrak{C}^0(M)$ is an R-submodule of $\mathfrak{C}(M)$, where addition and multiplication are defined pointwise. Thus we have an R-module structure on $[\mathfrak{C}(M)]$. Here's is a really nice description of $[\mathfrak{C}(M)]$ as an R-module:

Theorem 8.5. *We have an R-module isomorphism*
$$[\mathfrak{C}(M)] \cong \varprojlim M/M_k.$$

Proof. We define $\Phi \colon [\mathfrak{C}(M)] \to \varprojlim M/M_k$ as follows: let $[(u_n)] \in [\mathfrak{C}(M)]$, so (u_n) is a Cauchy sequence which represents the coset $[(u_n)]$. For each $k \in \mathbb{N}$, choose $\pi(k) \in \mathbb{N}$ such that $m, n \geq \pi(k)$ implies $u_n - u_m \in M_k$. In particular, this means $m, n \geq \pi(k)$ implies $\overline{u}_n = \overline{u}_m = \overline{u}_{\pi(k)}$ in M/M_k. Here we think of $\pi \colon \mathbb{N} \to \mathbb{N}$ as a strictly increasing function and we refer to it as a **stabilizing function** for the Cauchy sequence (u_n). We are now ready to define Φ. We set
$$\Phi([(u_n)_{n\in\mathbb{N}}]) = (\overline{u}_{\pi(k)})_{k\in\mathbb{N}}. \tag{46}$$
Note that (46) really does land in $\varprojlim M/M_k$ since π is a stabilizing function for the Cauchy sequence (u_n). We need to check that (46) is well-defined since it clearly depends on many choices.

First, suppose $\rho \colon \mathbb{N} \to \mathbb{N}$ is another stabilizing function for the Cauchy sequence (u_n). So for each $k \in \mathbb{N}$ we have $m, n \geq \rho(k)$ implies $\overline{u}_n = \overline{u}_m$ in M/M_k. Then choosing $n \geq \max(\rho(k), \pi(k))$ would give us $\overline{u}_{\pi(k)} = \overline{u}_n = \overline{u}_{\rho_{(k)}}$ in M/M_k. Thus our construction of Φ does not depend on the choice of a stabilizing function. Next, suppose $(u_n + \varepsilon_n)$ is another representative of the coset $[(u_n)]$ where $\varepsilon_n \to 0$. For each $k \in \mathbb{N}$, choose $\rho(k) \in \mathbb{N}$ such that $n \geq \rho(k)$ implies $\varepsilon_n \in M_k$, and set $\varrho = \max(\pi, \rho)$. Then for each $k \in \mathbb{N}$, we have $\overline{\varepsilon}_{\varrho(k)} = \overline{\varepsilon}_{\rho(k)} = 0$ and $\overline{u}_{\varrho(k)} = \overline{u}_{\pi(k)}$ in M/M_k. Thus

$$(\overline{u}_{\varrho(k)} + \overline{\varepsilon}_{\varrho(k)}) = (\overline{u}_{\pi(k)}).$$

This shows us that Φ does not depend on the choice of a representative of the coset $[(u_n)]$. All choice have been accounted for, and hence Φ is well-defined.

Let us now check that Φ is R-linear. Let $a, b \in R$ and suppose $[(u_n)], [(v_n)] \in [\mathfrak{C}(M)]$. We can choose a common stabilizing function $\pi \colon \mathbb{N} \to \mathbb{N}$ for the Cauchy sequences (u_n) and (v_n), meaning for each $k \in \mathbb{N}$ we have $m, n \geq \pi(k)$ implies $\overline{u}_n = \overline{u}_{\pi(k)}$ and $\overline{v}_n = \overline{v}_{\pi(k)}$ in M/M_k. Then observe that π is a stabilizing function for the Cauchy sequence $(au_n + bv_n)$, hence

$$\begin{aligned}\Phi([(au_n + bv_n)]) &= (a\overline{u}_{\pi(k)} + b\overline{v}_{\pi(k)}) \\ &= a(\overline{u}_{\pi(k)}) + b(\overline{v}_{\pi(k)}) \\ &= a\Phi([u_n]) + b\Phi([v_n]).\end{aligned}$$

Let us now check that Φ is surjective. Let $(\overline{u}_k) \in \varprojlim M/M_k$. So for each $k \in \mathbb{N}$ we have $n, m \geq k$ implies $\overline{u}_n = \overline{u}_m$ in M/M_k. However this is precisely the same thing as saying (u_n) is a Cauchy sequence in M with the identity function $1 \colon \mathbb{N} \to \mathbb{N}$ being a stabilizing function for (u_n). Thus $\Phi([(u_n)]) = (u_k)$, and so we see that Φ is surjective.

Finally, let us check that Φ is injective. Suppose $[(u_n)] \in \ker \Phi$. Thus $u_{\pi(k)} \in M_k$ for all $k \in \mathbb{N}$. In particular, we see that $u_{\pi(n)} \to 0$ as $n \to \infty$. However $(u_{\pi(n)})$ being a subsequence of the Cauchy sequence (u_n) forces $u_n \to 0$ as $n \to \infty$ as well. Thus $[(u_n)] = 0$ in $[\mathfrak{C}(M)]$. It follows that Φ is injective. □

Suppose (M'_n) is another Q-filtration of M such that $(M_n) \geq (M'_n)$. Thus there exists some $d \in \mathbb{N}$ such that $M'_n \supseteq M_{n+d}$ for all $n \in \mathbb{Z}$. An (M'_n)-Cauchy sequence is automatically an (M_n)-Cauchy sequence nce the topology induced by (M_n) is *stronger* than the topology induced by (M'_n). Thus we have an inclusion

$$\mathfrak{C}_{(M_n)}(M) \subseteq \mathfrak{C}_{(M'_n)}(M).$$

Furthermore, if a sequence converges to 0 in the (M_n)-topology, then it also converges to 0 in the weaker (M'_n)-topology. Thus we have an inclusion

$$\mathfrak{C}^0_{(M_n)}(M) \subseteq \mathfrak{C}^0_{(M'_n)}(M).$$

Thus we have a natural map

$$\Psi_{(M'_n),(M_n)} \colon [\mathfrak{C}_{(M_n)}(M)] \to [\mathfrak{C}_{(M'_n)}(M)].$$

Let us denote $\Phi_{(M_n)}$ to be the isomorphism constructed in the proof of (8.5). The analagous isomorphism with respect to the Q-filtration (M'_n) is then denoted $\Phi_{(M'_n)}$.

On the other hand, since $M_{n+d} \subseteq M'_n$ for all $n \in \mathbb{N}$, we have natural maps $M/M_{n+d} \to M/M'_n$

Proposition 8.11. *With the notation above, we have a commutative diagram*

$$\begin{tikzcd}
{[\mathfrak{C}_{(M'_n)}(M)]} \arrow[r] & \lim M/M'_k \\
{[\mathfrak{C}_{(M_n)}(M)]} \arrow[r] \arrow[u] & \lim M/M_k \arrow[u]
\end{tikzcd}$$

Proof. Let $[(u_n)] \in [\mathfrak{C}_{(M_n)}(M)]$. Choose a stabilizing function $\pi \colon \mathbb{N} \to \mathbb{N}$ for the (u_n) as an (M_n)-Cauchy sequence. Then observe that for each $k \in \mathbb{N}$, we have $n \geq \pi(k+d)$ implies $u_n \in M_{k+d} \subseteq M'_k$. In particular, the function $\pi_d \colon \mathbb{N} \to \mathbb{N}$, defined by $\pi_d(m) = \pi(d+m)$, is a stabilizing function for (u_n) as an (M'_n)-Cauchy sequence. Thus

$$\Phi_{(M'_n)}[(u_n)] = (\overline{u}_{\pi_d(k)}).$$

□

It is natural to wonder if in fact we have $\Phi_{(M_n)} = \Phi_{(M'_n)}$. Then answer is yes! Indeed, let $[(u_n)] \in [\mathfrak{C}(M)]$ and choose a stabilizing function $\pi \colon \mathbb{N} \to \mathbb{N}$ for (u_n) with respect to $\mathrm{d}_{(M_n)}$. Then for each $k \in \mathbb{N}$ we have $m, n \geq \pi(k+d)$ implies $\overline{u}_n = \overline{u}_m$ in M/M_{k+d}, hence $\overline{u}_n = \overline{u}_m$ in M/M'_k since $M_{k+d} \subseteq M'_k$. In particular, we see that

$$\Phi_{(M_n)}([u_n]) = (\overline{u}_{\pi(k)})$$

9 Modules of Finite Length

Definition 9.1. Let A be a ring and let M be an A-module.

1. Let $\mathcal{C}(M)$ denote the set of all **chains of submodules** of M, that is,
$$\mathcal{C}(M) := \{\mathcal{M} = (M = M_0 \supset M_1 \supset \cdots \supset M_n = 0) \mid M_i \neq M_{i+1}\}.$$
2. If $\mathcal{M} = (M = M_0 \supset M_1 \supset \cdots \supset M_n = 0) \in \mathcal{C}(M)$, then **length**$(\mathcal{M}) := n$.
3. If length$(M) < \infty$, then we say M is **Artinian**. If A is Artinian as an A-module, then we say A is an **Artinian ring**.

Remark. The set $\mathcal{C}(M)$ forms a poset in the following way: Given $\mathcal{M}, \mathcal{M}' \in \mathcal{C}(M)$, we say $\mathcal{M}' \geq \mathcal{M}$ if we can obtain $\mathcal{M}$ by removing some submodules in the chain $\mathcal{M}'$.

Definition 9.2. Let A be a ring, M an A-module, and $\mathcal{M} := (M = M_0 \supset M_1 \supset \cdots \supset M_n = 0)$ a chain of submodules of M.

1. We say $\mathcal{M}$ is a **composition series** for M if M_i/M_{i+1} is a nonzero simple module for each i.
2. We define the **length** of M, denoted length(M), to be the least length of a composition series for M.

Remark.

1. If $\mathcal{M}$ is not a composition series, then there exists some i such that M_i/M_{i+1} is not simple. Thus, there exists a nonzero proper submodule M'/M_{i+1} of M_i/M_{i+1}. Let $\mathcal{M}'$ be the chain of submodules of M given by $\mathcal{M}' = (M = M_0 \cdots \supset M_i \supset M' \supset M_{i+1} \supset \cdots \supset M_n = 0)$. Then $\mathcal{M}' \geq \mathcal{M}$ and length$(\mathcal{M}') =$ length$(\mathcal{M}) + 1$. So a composition series must be maximal with respect to the partial order.
2. A simple module must be generated by any nonzero element. Thus, if $\mathcal{M}$ is a composition series, then each $M_i/M_{i+1} \cong A/\mathfrak{p}$ for some maximal ideal $\mathfrak{p}$, which may be described by $\mathfrak{p} = \operatorname{Ann}(M_i/M_{i+1})$.

Theorem 9.1. *Let A be a ring, and let M be an A-module. Then M has a finite composition series if and only if M is Artinian and Noetherian. If M has a finite composition series $\mathcal{M} := (M = M_0 \supset M_1 \supset \cdots \supset M_n = 0)$ of length n, then:*

1. *Every chain of submodules of M has length less than or equal to n, and can be refined to a composition series.*
2. *The sum of the localization maps $M \to M_\mathfrak{p}$, for $\mathfrak{p}$ a prime ideal, gives an isomorphism of A-modules*
$$M \cong \bigoplus_{\mathfrak{p}} M_\mathfrak{p},$$
where the sum is taken over all maximal ideals $\mathfrak{p}$ such that some $M_i/M_{i+1} \cong A/\mathfrak{p}$. The number of M_i/M_{i+1} isomorphic to $A/\mathfrak{p}$ is the length of $M_\mathfrak{p}$ as an $A_\mathfrak{p}$-module, and is thus independent of the composition series chosen.
3. *We have $M = M_\mathfrak{p}$ if and only if M is annihilated by some power of $\mathfrak{p}$.*

Proof. First suppose that M is Artinian and Noetherian, so that it satisfies both ascending chain condition and descending chain condition on submodules. By the ascending chain condition we may choose a maximal proper submodule M_1, a maximal proper submodule M_2 of M_1, and so on. By the descending chain condition this sequence of submodules must terminate, and it can only terminate when some $M_n = 0$. In this case, $M = M_0 \supset M_1 \supset \cdots \supset M_n = 0$ is a compostion series for M.

1. Suppose $N \subset M$ is a proper submodule. We shall show that length$(N) <$ length(M). The idea is simple: We intersect the terms of the given composition series for M with N and derive a shorter composition series for N. The quotient $(N \cap M_i)/(N \cap M_{i+1})$ is isomorphic to
$$(N \cap M_i + M_{i+1})/M_{i+1} \subset M_i/M_{i+1}.$$
Since M_i/M_{i+1} is simple, we have either $(N \cap M_i)/(N \cap M_{i+1}) = 0$ or else $(N \cap M_i)/(N \cap M_{i+1})$ is simple and $N \cap M_i + M_{i+1} = M_i$. We claim that the latter possibility cannot happen for every i. Assuming on the contrary that it did, we prove by descending induction on i that $N \supset M_i$ for every i, and we get a contradiction from the statement $N \supset M_0 = M$. If $i = n$, then clearly $N \supset M_i$. Supposing by induction

that $N \supset M_{i+1}$, we see that $N \cap M_i = N \cap M_i + M_{i+1} = M_i$, and it follows that $N \supset M_i$. From these facts, we see that the sequence of submodules

$$N \supset N \cap M_1 \supset \cdots \supset N \cap M_n = 0$$

can be changed, by leaving out the terms $N \cap M_i$ such that $N \cap M_i = N \cap M_{i+1}$, to a composition series for N whose length is less than n. Since we could do this for any composition series for M, we get

$$\text{length}(N) < \text{length}(M).$$

Suppose now that $M = N_0 \supset N_1 \supset \cdots \supset N_k$ is a chain of submodules. We shall show by induction on length(M) that $k \leq$ length(M). This is obvious if length$(M) = 0$, since then $M = 0$. By the argument above, length$(N_1) <$ length(M); so by induction, the length of the chain $N_1 \supset \cdots \supset N_k$ is $k - 1 \leq$ length(N_1). Since length$(N_1) <$ length(M), it follows that $k \leq$ length(M). From the definition of length, it now follows that every maximal chain of submodules has length n, and every chain of submodules can be refined to a maximal chain. Further, n is a uniform bound on the lengths of all ascending or descending chains of submodules, so that M has both ascending chain condition and descending chain condition.

2. It suffices to show that the given map becomes an isomorphism after localizing at any maximal ideal $\mathfrak{q}$ of A. This will be easy once we understand what happens when we localize a module of finite length. We begin with the case when M has length 1, that is, when M is a simple module. In this case, $M \cong A/\mathfrak{p}$ for some maximal ideal $\mathfrak{p} = \text{Ann}(M)$. If $\mathfrak{p} = \mathfrak{q}$, then since $A/\mathfrak{q}$ is a field, the elements outside of $\mathfrak{q}$ acts as units on $A/\mathfrak{q}$, and we see that $(A/\mathfrak{q})_\mathfrak{q} = A/\mathfrak{q}$. If on the other hand $\mathfrak{p} \neq \mathfrak{q}$, then since $\mathfrak{p}$ is maximal, $\mathfrak{p} \not\subset \mathfrak{q}$, so $\mathfrak{p}_\mathfrak{q} = A_\mathfrak{q}$. Thus
$$(A/\mathfrak{p})_\mathfrak{q} = A_\mathfrak{q}/\mathfrak{p}_\mathfrak{q} = 0.$$
It follows in particular from this that if $\mathfrak{q}$ and $\mathfrak{q}'$ are distinct prime ideals, then $(M_\mathfrak{q})_{\mathfrak{q}'} = 0$. We now return to the general case, where length$(M) = n < \infty$. The composition series for M localizes to a sequence of submodules
$$M_\mathfrak{q} = (M_0)_\mathfrak{q} \supset (M_1)_\mathfrak{q} \supset \cdots \supset (M_n)_\mathfrak{q} = 0.$$
The modules M_i/M_{i+1} have length 1, so the case already treated shows that $(M_i/M_{i+1})_\mathfrak{q} = M_i/M_{i+1}$ if $\mathfrak{q} = \text{Ann}\left(M_i/M_{i+1}\right)$ and $(M_i/M_{i+1})_\mathfrak{q} = 0$ otherwise. Thus $M_\mathfrak{q}$ has a finite composition series corresponding to the subseries of the one for M, obtained by keeping only those $(M_i)_\mathfrak{q}$ such that $M_i/M_{i+1} \cong A/\mathfrak{q}$. In particular, if none of the modules M_i/M_{i+1} is isomorphic to $A/\mathfrak{q}$, then $M_\mathfrak{q} = 0$; and if $\mathfrak{q}$ and $\mathfrak{q}'$ are distinct maximal ideals, then $(M_\mathfrak{q})_{\mathfrak{q}'} = 0$. Now consider the map
$$\alpha : M \to \bigoplus_{\mathfrak{p}} M_\mathfrak{p},$$
where the sum is taken over all maximal ideals $\mathfrak{p}$ such that some $M_i/M_{i+1} \cong A/\mathfrak{p}$. We see from the above that we could harmlessly extend the sum to all maximal ideals; the new terms are all 0. For any maximal ideal $\mathfrak{q}$ and any module M, we have $(M_\mathfrak{q})_\mathfrak{q} = M_\mathfrak{q}$, so the identity map is one part of the localization of α:
$$\alpha_\mathfrak{q} : M_\mathfrak{q} \to \left(\bigoplus_{\mathfrak{p} \in \text{Max}(A)} M_\mathfrak{p} \right)_\mathfrak{q} = \bigoplus_{\mathfrak{p} \in \text{Max}(A)} (M_\mathfrak{p})_\mathfrak{q}.$$
But if $\mathfrak{p} \neq \mathfrak{q}$ and M has finite length, then we have seen that $(M_\mathfrak{p})_\mathfrak{q} = 0$. Thus $\alpha_\mathfrak{q}$ is the identity map for every maximal ideal $\mathfrak{q}$, and it follows that α is an isomorpism.

3. Suppose that M is annihilated by a power of a maximal ideal $\mathfrak{p}$. If $\mathfrak{q} \neq \mathfrak{p}$ is another maximal ideal, then $\mathfrak{p}$ contains an element not in $\mathfrak{q}$. This element acts as a unit on $M_\mathfrak{q}$. Thus, by part 2, $M \cong M_\mathfrak{p}$. Conversely suppose that $M \cong M_\mathfrak{p}$. The preceeding description of localization shows that every factor $M_i/M_{i+1} \cong A/\mathfrak{p}$. By induction, we see that $\mathfrak{p}^d M \subset M_d$, and in particular $\mathfrak{p}^n M = 0$.

□

Example 9.1. Let $A = K[x, y]$, $I = \langle x^3, x^2y, xy^2, y^3 \rangle$, and $M = A/I$. We want to calculate the length of M. By Theorem (9.1, it suffices to find a composition series for M and calculate its length. A composition series for M is given by
$$0 = M_6 \subset M_5 \subset M_4 \subset M_3 \subset M_2 \subset M_1 \subset M_0 = M,$$

where

$$\begin{aligned} M_5 &= \langle x^2, xy^2, y^3 \rangle / I \\ M_4 &= \langle x^2, y^2 \rangle / I \\ M_3 &= \langle x^2, xy, y^2 \rangle / I \\ M_2 &= \langle x, y^2 \rangle / I \\ M_1 &= \langle x, y \rangle / I, \end{aligned}$$

and $M_i / M_{i+1} \cong A/\langle x, y \rangle$ for all i. Thus, length$(M) = 6$.

10 Injective Modules

Definition 10.1. Let E be an R-module. We say E is **injective** if for every injective homorphisms $\varphi \colon M \to N$ and for every homomorphism $\psi \colon M \to E$ there exists a homomorphism $\widetilde{\psi} \colon N \to E$ such that $\widetilde{\psi} \circ \varphi = \psi$. In this case, we say $\widetilde{\psi}$ **extends** ψ **along** φ. If φ is the inclusion map $M \subset N$, then we will simply say $\widetilde{\psi}$ **extends** ψ. We illustrate this with the following diagram:

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "\psi"'] & N \arrow[dl, dashed, "\widetilde{\psi}"] \\ E & \end{tikzcd}$$

An equivalent definition of being injective is given in the following proposition:

Proposition 10.1. *Let E be an R-module. Then E is injective if and only if the contravariant functor $\mathrm{Hom}_R(-, E)$ is exact.*

Proof. Suppose that E is injective. Let

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r, "\varphi"] & M \arrow[r, "\psi"] & M'' \arrow[r] & 0 \end{tikzcd}$$

be an exact sequence of R-modules. Since $\mathrm{Hom}_R(-, E)$ is left exact, we only need to check that

$$\begin{tikzcd} \mathrm{Hom}_R(M, E) \arrow[r, "\varphi^*"] & \mathrm{Hom}_R(M', E) \arrow[r] & 0 \end{tikzcd}$$

is exact at $\mathrm{Hom}_R(M', E)$. This is equivalent to showing that φ^* is surjective. Let $\lambda \in \mathrm{Hom}_R(M', E)$. Since E is injective, and $\varphi : M' \to M$ is a monomorphism, there exists $\widetilde{\lambda} \in \mathrm{Hom}_R(M', E)$ such that $\varphi^*(\widetilde{\lambda}) = \widetilde{\lambda} \circ \varphi = \lambda$. But $\varphi^*(\widetilde{\lambda}) = \widetilde{\lambda} \circ \varphi$, so φ^* is surjective. In fact, this map is surjective if and only if E is injective by definition. □

10.1 Baer's Criterion

Let E be an R-module. If we want to determine if E is injective, then it turns out that we do not necessarily need to check that the condition in Definition (10.1) holds for *every* injective homomorphism $\varphi \colon M \to N$; we only need to check that it holds for every morphism of the type $I \subset R$ where I is an ideal in R. This is called Baer's Criterion. Before we show this, let us first show that we need only consider inclusions $M \subset N$:

Proposition 10.2. *Let E be an R-module. Then E is injective if and only if for every inclusion of R-modules $M \subset N$ and for every homomorphism $\psi \colon M \to E$ there exists a homomorphism $\widetilde{\psi} \colon N \to E$ such that $\widetilde{\psi}|_M = \psi$.*

Proof. One direction is obvious. To prove the other direction, let $\varphi \colon M \to N$ be an injective homomorphism of R-modules and let $\psi \colon M \to E$ be a homorphism. Since φ is injective, it induces an isomorphism $\varphi \colon M \to \varphi(M)$ of R-modules. Let φ^{-1} be the inverse homomorphism to this isomorphism. Then $\varphi(M) \subset N$ and $\psi \circ \varphi^{-1} \colon \varphi(M) \to E$ is a homomorphism, and so by hypothesis, there exists $\widetilde{\psi} \colon N \to E$ such that $\widetilde{\psi}|_{\varphi(M)} = \psi \circ \varphi^{-1}$. This implies

$$\begin{aligned} \widetilde{\psi} \circ \varphi &= \widetilde{\psi}|_{\varphi(M)} \circ \varphi \\ &= \psi \circ \varphi^{-1} \circ \varphi \\ &= \psi. \end{aligned}$$

Therefore E is injective. □

Now we will state and prove Baer's Criterion:

Theorem 10.1. *(Baer's Criterion) Let E be an R-module. Then E is injective if and only if for every ideal $I \subset R$ and for every homomorphism $\psi\colon I \to E$ there exists a morphism $\widetilde{\psi}\colon R \to E$ such that $\widetilde{\psi}|_I = \psi$.*

Proof. One direction is obvious. For the other direction, let $M \subset N$ be an inclusion of A-modules and let $\psi\colon M \to E$ be a homomorphism. Define the partially ordered set $(\mathscr{F}, \leq)$ where

$$\mathscr{F} := \{\psi'\colon M' \to N \mid M \subset M' \subset N \text{ and } \psi' \text{ extends } \psi\}.$$

and the where partial order $\leq$ is defined by

$$\psi' \leq \psi'' \text{ if and only if } \psi'' \text{ extends } \psi'.$$

If $\mathscr{T}$ is a totally ordered subset of $\mathscr{F}$, then it has an upper bound (namely we take the direct limit of a all $\psi' \in \mathscr{T}$). Therefore by Zorn's lemma, there is a homomorphism $\psi'\colon N' \to E$ with $M \subset N' \subset N$ which is maximal with respect to the property that ψ' extends ψ. We claim that $N' = N$. We will prove this by contradiciton: assume that $N' \neq N$. Choose an element $u \in N \backslash N'$ and consider the ideal

$$I = \{a \in R \mid au \in N'\}.$$

It is a nonempty proper ideal of R since $0 \in I$ and $1 \notin I$. By hypothesis, the composite

$$I \xrightarrow{\cdot u} N' \xrightarrow{\psi'} E$$

extends to a homomorphism $\widetilde{\psi}\colon R \to E$. Define $\psi''\colon N' + Ru \to E$ by the formula

$$\psi''(v + au) = \psi'(v) + \widetilde{\psi}(a)$$

for all $v + au \in N' + Rn$. To see that this is well-defined, suppose $v_1 + a_1 u$ and $v_2 + a_2 u$ represent the same element in $N' + Ru$. Then $v_2 - v_1 = (a_1 - a_2)u$ implies $a_1 - a_2 \in I$. Therefore $\widetilde{\psi}(a_1 - a_2) = \psi'((a_1 - a_2)u)$, and so

$$\begin{aligned}
\psi''(v_2 + a_2 u) &= \psi'(v_2) + \widetilde{\psi}(a_2) \\
&= \psi'(v_2 - (v_2 - v_1))) + \widetilde{\psi}(a_1 + (a_2 - a_1)) \\
&= \psi'(v_2 + (a_1 - a_2)u) + \widetilde{\psi}(a_1 + (a_2 - a_1)) \\
&= \psi'(v_1) + \psi'((a_1 - a_2)u) + \widetilde{\psi}(a_1) + \psi'((a_2 - a_1)u) \\
&= \psi'(v_1) + \widetilde{\psi}(a_1).
\end{aligned}$$

Thus ψ'' is well-defined. We also note that ψ'' extends ψ'. Since ψ' was maximal, this leads to a contradiction. So we must have $N' = N$. □

Remark. Saying that every map $\varphi\colon I \to E$ extends to a map $\widetilde{\varphi}\colon R \to E$ is equivalent to saying $\mathrm{Ext}^1_R(R/I, E) = 0$. To see this, consider the short exact sequence

$$\begin{tikzcd}
0 \arrow[r] & I \arrow[r] & R \arrow[r] & R/I \arrow[r] & 0
\end{tikzcd}$$

Applying the contravariant functor $\mathrm{Hom}_R(-, E)$, we obtain the long exact sequence

$$\begin{tikzcd}
\mathrm{Hom}_R(I, E) \arrow[drr, rounded corners] & \mathrm{Hom}_R(R, E) \arrow[l] & \mathrm{Hom}_R(R/I, E) \arrow[l] & 0 \arrow[l] \\
& 0 \cong \mathrm{Ext}^1_R(R, E) & \mathrm{Ext}^1_R(R/I, E) \arrow[l] &
\end{tikzcd}$$

It's easy to check that this exact sequence implies $\mathrm{Ext}^1_R(R/I, E) \cong 0$ if and only if $\mathrm{Hom}_R(R, E) \to \mathrm{Hom}_R(I, E)$ is surjective.

10.2 Localization, Direct Sums, and Direct Products of Injective Modules

Lemma 10.2. *Let E an R-module, let $\{E_\lambda\}_{\lambda\in\Lambda}$ be a colletion of R-modules indexed by a set Λ, and let S be a multiplicatively closed subset of R. Then*

1. *$\prod_{\lambda\in\Lambda} E_\lambda$ is injective if and only if all the E_λ are injective.*
2. *If R is Noetherian, then $\bigoplus_{\lambda\in\Lambda} E_\lambda$ is injective if and only if all the E_λ are injective.*
3. *If R is Noetherian and E is an injective, then E_S is an injective R_S-module.*
4. *E is injective if and only if any monomorphism $\varphi\colon E\to M$ splits, that is, there exists a morphism $\psi\colon M\to E$ such that $\psi\circ\varphi = \mathrm{id}_E$.*

Proof.
1. Since

$$\mathrm{Hom}_R\left(M, \prod_{\lambda\in\Lambda} E_\lambda\right) \cong \prod_{\lambda\in\Lambda} \mathrm{Hom}_R\left(M, E_\lambda\right)$$

for all R-modules M, the functor $\mathrm{Hom}_R\left(-, \prod_{\lambda\in\Lambda} E_\lambda\right)$ is exact if and only if the functors $\mathrm{Hom}_R\left(-, E_\lambda\right)$ are exact for all $\lambda\in\Lambda$.

2. First assume that $\bigoplus_{\lambda\in\Lambda} E_\lambda$ is injective. Let $\lambda\in\Lambda$, let I be an ideal in R, and let $\varphi\colon I\to E_\lambda$ be an R-module homomorphism. Since $\bigoplus_{\lambda\in\Lambda} E_\lambda$ is injective, the composition

$$I \to E_\lambda \hookrightarrow \bigoplus_{\lambda\in\Lambda} E_\lambda$$

extends to a map $\widetilde{\varphi}\colon R\to\bigoplus_{\lambda\in\Lambda} E_\lambda$. Letting $\pi_\lambda\colon \bigoplus_{\lambda\in\Lambda} E_\lambda \to E_\lambda$ denote the projection to the λth component, the map $\pi_\lambda\circ\widetilde{\varphi}$ extends φ. Thus E_λ is injective for all $\lambda\in\Lambda$. Note that this direction did not depend on the fact that R is Noetherian.

Converesely, assume each E_λ is injective. By Theorem (10.1), it is enough to show that for an ideal I of R, any homomorphism $\varphi\colon I\to\bigoplus_{\lambda\in\Lambda} E_\lambda$ extends to R. Since R is Noetherian, I is finitely generated, and so there exists a finite subset $\{\lambda_1,\dots,\lambda_n\}$ of Λ such that

$$\begin{aligned}\operatorname{im}\varphi &\subseteq \bigoplus_{i=1}^n E_{\lambda_i}\\ &\cong \prod_{i=1}^n E_{\lambda_i}.\end{aligned}$$

From (1), we know that $\prod_{i=1}^n E_{\lambda_i}$ is injective, and therefore we may extend φ. Thus $\bigoplus_{\lambda\in\Lambda} E_\lambda$ is injective.

3. Let $\varphi\colon I_S\to E_S$ be an R_S-module homomorphism. Since R is a Noetherian ring, the ideal I is finitely presented, and thus there exists $\psi\colon I\to E$ such that $\psi_S=\varphi$. Since E is injective, we may choose an extension $\widetilde{\psi}\colon R\to E$ of ψ. Then $\widetilde{\psi}_S\colon R_S\to E_S$ is an extension of $\varphi\colon I_S\to E_S$.

4. One direction is obvious, so we only prove the nonobvious direction. Assume that any injective R-linear map out of E splits. Let $\varphi\colon M\to N$ be an injective R-linear map and let $\psi\colon M\to E$ be any R-linear map. We need to construct a map $\widetilde{\psi}\colon N\to E$ such that $\widetilde{\psi}\circ\varphi=\psi$. To do this, consider the pushout module

$$E+_M N = (E\times N)/\{(\psi(u), -\varphi(u)) \mid u\in M\}$$

together its natural maps $\iota_1\colon E\to E+_M N$ and $\iota_2\colon N\to E+_M N$, given by

$$\iota_1(v) = [v, 0] \qquad \text{and} \qquad \iota_2(w) = [0, w]$$

for all $v\in E$ and $w\in N$ where $[v,w]$ denotes the equivalence class in $E+_M N$ with (v,w) as one of its representatives. Observe that

$$\begin{aligned}\iota_1(\psi(u)) &= [\psi(u), 0]\\ &= [0, \varphi(u)]\\ &= \iota_2(\varphi(u))\end{aligned}$$

for all $u\in M$. Therefore, we have a commutative diagram

$$\begin{tikzcd}
M \arrow[r, "\varphi"] \arrow[d, "\psi"'] & N \arrow[d, "\iota_2"] \\
E \arrow[r, "\iota_1"'] & E +_M N
\end{tikzcd}$$

We claim that ι_1 is injective. Indeed, suppose $v \in \ker \iota_1$. Then $[v, 0] = [0, 0]$ implies if $(v, 0) = (\psi(u), -\varphi(u))$ for some $u \in M$. Then $\varphi(u) = 0$ implies $u = 0$ since φ is injective, and therefore

$$\begin{aligned} v &= \psi(u) \\ &= \psi(0) \\ &= 0. \end{aligned}$$

Thus ι_1 is injective. Therefore by hypothesis the map $\iota_1 \colon E \to E +_M N$ splits, say by $\lambda \colon E +_M N \to E$, where $\lambda \circ \iota_1 = 1_E$. Finally, we obtain a map $\widetilde{\psi} \colon N \to E$ by setting $\widetilde{\psi} := \lambda \circ \iota_2$. Then

$$\begin{aligned} \widetilde{\psi} \circ \varphi &= \lambda \circ \iota_2 \circ \varphi \\ &= \lambda \circ \iota_1 \circ \psi \\ &= \psi, \end{aligned}$$

shows that $\widetilde{\psi}$ has the desired property. □

Proposition 10.3. *Let R be a ring. Then R is Noetherian if and only if every direct sum of injective R-modules is injective.*

Proof. We proved one direction in Lemma (11.3). For the other direction, assume R is not Noetherian. Then R contains a strictly ascending chain of ideals

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots .$$

Let $I = \bigcup_j I_j$. The natural maps

$$I \hookrightarrow R \to R/I_j \hookrightarrow \mathrm{E}_R(R/I_j)$$

give us a homomorphism $I \to \prod_j \mathrm{E}_R(A/I_j)$, whose image lies in the submodule $\bigoplus_j \mathrm{E}_R(R/I_j)$. To see this, note for $x \in I$, we must have $x \in I_k$ for some k. This implies the image of x lies in the submodule $\bigoplus_{j=1}^{k-1} \mathrm{E}_R(R/I_j)$.

Therefore we have a homomorphism $\varphi \colon I \to \bigoplus_j \mathrm{E}_R(R/I_j)$. But φ does not extend to a homomorphism $R \to \bigoplus_j \mathrm{E}_R(R/I_j)$. □

Proposition 10.4. *Let $R \to S$ be a flat ring map. If E is an injective as an S-module, then E is injective as an R-module.*

Proof. This is true because

$$\mathrm{Hom}_R(M, E) \cong \mathrm{Hom}_R(M \otimes_R S, E)$$

and the fact that tensoring with S is exact. □

Proposition 10.5. *Let $R \to S$ be an epimorphism of rings. If E is an injective as an R-module, then E is injective as an S-module.*

Proof. This is true because

$$\mathrm{Hom}_R(N, E) = \mathrm{Hom}_S(N, E)$$

for any S-module N. □

10.3 Divisible Modules

Definition 10.2. Let M be an R-module. We say M is **divisible** if $aM = M$ for every nonzerodivisor $a \in R$.

10.3.1 Image of divisible module is divisible

Proposition 10.6. *Let $\varphi \colon M \twoheadrightarrow N$ be a surjective map of R-modules and suppose M is divisible. Then N is divisible.*

Proof. Let $a \in R$ be a nonzerodivisor and let $v \in N$. We must find a $v' \in N$ such that $av' = v$. It will then follow that $aN = N$, which will imply N is divisible. Since φ is surjective, we may choose a $u \in M$ such that $\varphi(u) = v$. Since M is divisible, we may choose a $u' \in M$ such that $au' = u$. Then setting $v' = \varphi(u')$, we have

$$\begin{aligned} av' &= a\varphi(u') \\ &= \varphi(au') \\ &= \varphi(u) \\ &= v. \end{aligned}$$

Thus N is divisible. □

10.3.2 Injectives modules are divisible (with converse being true in a PID)

Proposition 10.7. *Let M be an R-module. If M is injective, then M is divisible. The converse holds if R is a PID.*

Proof. Suppose M is injective and let $a \in R$ be a nonzerodivisor. Then the map $\varphi \colon M \to aM$, given by

$$\varphi(u) = au$$

for all $u \in M$ is an injective R-linear map. Thus we obtain a splitting map of φ, say $\psi \colon aM \to M$. Thus if $u \in M$, then we have

$$\begin{aligned} u &= (\psi\varphi)(u) \\ &= \psi(\varphi(u)) \\ &= \psi(au) \\ &= a\psi(u). \end{aligned}$$

This implies $M = aM$, that is, M is divisible.

For the converse direction, assume that R is a PID and that M is a divisible R-module. Let $\varphi \colon \langle x \rangle \to M$ be a homomorphism, where $\langle x \rangle$ is an ideal in R. Let $a \in R$ be a nonzerodivisor and set $u = \varphi(x)$. Since $M = xM$, we have $u = xv$ for some $v \in M$. Then the map $\widetilde{\varphi} \colon R \to M$, given by

$$\widetilde{\varphi}(a) = av$$

for all $a \in R$, extends φ. Indeed, it is clearly R-linear. Also

$$\begin{aligned} \widetilde{\varphi}(bx) &= (bx)v \\ &= b(xv) \\ &= bu \\ &= b\varphi(x) \\ &= \varphi(bx) \end{aligned}$$

for all $bx \in \langle x \rangle$. It follows from Baer's Criterion that M is injective. □

Example 10.1. Since $\mathbb{Z}$ is a PID and $\mathbb{Q}/\mathbb{Z}$ is divisible as a $\mathbb{Z}$-module, Proposition (10.7) implies $\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module.

10.3.3 Decomposition of module over PID

Proposition 10.8. *Assume that R is a PID and let M be any R-module. Then M may be decomposed as $M = D \oplus N$ where D is divisible and N has no nontrivial divisible subgroups.*

Proof. We first argue using Zorn's Lemma that M contains a maximal divisible submdoule. Consider the partially ordered set $(\mathscr{F}, \subseteq)$, where $\mathscr{F}$ is the family of all divisible submodules of M:

$$\mathscr{F} = \{D \subseteq M \mid D \text{ is divisible submodule of } M\},$$

and where the partial order $\subseteq$ is set inclusion. Note that $\mathscr{F}$ is nonempty since the zero module is divisible. Let $\{D_i \mid i \in I\}$ be a totally ordered subset of $\mathscr{F}$. We claim that

$$\bigcup_{i \in I} D_i$$

is a divisible submodule of M, and hence an upper bound of $\{D_i \mid i \in I\}$.

To see this, we first show that $\bigcup_{i \in I} D_i$ is a submodule of M. Indeed, it is nonempty since $0 \in \bigcup_{i \in I} D_i$. Also, if $a \in R$ and $u, v \in \bigcup_{i \in I} D_i$, then there exists an $i \in I$ such that $u, v \in D_i$ since $\{D_i \mid i \in I\}$ is totally ordered, and so

$$au + v \in D_i \subseteq \bigcup_{i \in I} D_i.$$

Thus $\bigcup_{i \in I} D_i$ is a submodule of M.

Now we show that $\bigcup_{i \in I} D_i$ is divisible. Let a be a nonzero divisor in R and let u be an element in $\bigcup_{i \in I} D_i$. Then there exists an $i \in I$ such that $u \in D_i$, and as D_i is divisible, there exists a

$$v \in D_i \in \bigcup_{i \in I} D_i$$

such that $av = u$. It follows that $\bigcup_{i \in I} D_i$ is divisible.

Thus the conditions for Zorn's Lemma are satisfied and so there exists a maximal divisible submodule of M, say $D \subseteq M$. Since every divisible module over a PID is injective, we see that D is injective, and thus we have a direct sum decomposition of M say

$$M = D \oplus N$$

where N is a submodule of M. To finish the proof, assume for a contradiction that N has a nontrivial divisible submodule, say $L \subseteq N$. We claim that $D + L$ is a divisible submodule of M which properly contains D. Indeed, it is divisible since if $a \in R$ is a nonzerodivisor and $x + y \in D + L$ where $x \in D$ and $y \in L$, then we can choose $u \in D$ and $v \in L$ such that $au = x$ and $av = y$ since D and L are divisible, and so

$$\begin{aligned} a(u+v) &= au + av \\ &= x + y \end{aligned}$$

implies $D + L$ is divisible. It also properly contains D since $L \subseteq N$ is nontrivial. Thus $D + L$ is a divisible submodule of M which properly contains D. This is a contradiction as D was chosen to be a maximal divisible submodule of M. □

Proposition 10.9. *Let A be an integral domain. Then its quotient field $Q(A)$ is an injective A-module.*

Proof. We show this using Baer's criterion. Let $\varphi : I \to Q(A)$ be an A-linear map where I is an ideal of A. If $I = 0$, extend by the zero map. Otherwise, let $0 \neq x \in I$ and define the map $\widetilde{\varphi} : A \to Q(A)$ by $a \mapsto a\varphi(x)/x$. This map is obviously A-linear and if $y \in I$, then

$$\begin{aligned} \widetilde{\varphi}(y) &= \frac{y\varphi(x)}{x} \\ &= \frac{\varphi(yx)}{x} \\ &= \frac{x\varphi(y)}{x} \\ &= \varphi(y). \end{aligned}$$

□

Lemma 10.3. *Let S be an R-algebra, let E be an injective R-module, and let P a projective S-module. Then $\mathrm{Hom}_R(P, E)$ is an injective S-module.*

Proof. The functor $\mathrm{Hom}_S(-, \mathrm{Hom}_R(P, E))$ is exact if and only if the functor $\mathrm{Hom}_R(- \otimes_S P, E)$ is exact, but tensor-hom adjunction. Now notice that the functor $- \otimes_S P$ is exact since P is projective (and hence flat), and the functor $\mathrm{Hom}_R(-, E)$ is exact since E is injective. Thus $\mathrm{Hom}_R(- \otimes_S P, E)$ is a composition of exact functors, and so it must be exact too. □

10.4 Injective Hulls

We will now prove that any R-module M can be embedded into an injective module. We first prove this for $R = \mathbb{Z}$.

Lemma 10.4. *Let M be a $\mathbb{Z}$-module. Then there exists an injective module E and a monomorphism $\varphi\colon M \to E$.*

Proof. Recall that $\mathbb{Q}/\mathbb{Z}$ is injective. For a $\mathbb{Z}$-module N, define

$$N^\vee := \mathrm{Hom}_{\mathbb{Z}}(N, \mathbb{Q}/\mathbb{Z}).$$

We now have a natural map $M \to M^{\vee\vee}$, denoted by $u \mapsto \widehat{u}$, where

$$\widehat{u}(\varphi) = \varphi(u)$$

for all $u \in M$ and $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$. We claim that the map $M \to M^{\vee\vee}$ is a monomorphism. Indeed, suppose $u \in M$ with $\varphi(u) \neq 0$. Denote $n := \mathrm{ord}(u)$ (so $nu = 0$ with n being as small as possible) and let $\varphi\colon \langle u \rangle \to \mathbb{Q}/\mathbb{Z}$ be the unique homomorphism such that $\varphi(u) = [1/n]$. Then φ is not the zero map. Since $\mathbb{Q}/\mathbb{Z}$ is injective, we can extend φ to a nonzero map $\widetilde{\varphi}\colon M \to \mathbb{Q}/\mathbb{Z}$. Then

$$\begin{aligned} \widehat{u}(\widetilde{\varphi}) &= \widetilde{\varphi}(\widehat{u}) \\ &= \varphi(u) \\ &\neq 0 \end{aligned}$$

implies $\widehat{u} \neq 0$.

Now let $\bigoplus_{\lambda \in \Lambda} \mathbb{Z} \to M^\vee$ be a surjection. Since the contraviarant functor $\mathrm{Hom}_\mathbb{Z}(-, \mathbb{Q}/\mathbb{Z})$ is left exact, we get an embedding

$$\begin{aligned} M &\rightarrowtail M^{\vee\vee} \\ &= \mathrm{Hom}_\mathbb{Z}\left(M^\vee, \mathbb{Q}/\mathbb{Z}\right) \\ &\rightarrowtail \mathrm{Hom}_\mathbb{Z}\left(\bigoplus_{\lambda\in\Lambda} \mathbb{Z}, \mathbb{Q}/\mathbb{Z}\right) \\ &\cong \prod_{\lambda\in\Lambda} \mathbb{Q}/\mathbb{Z}, \end{aligned}$$

where $\prod_{\lambda\in\Lambda} \mathbb{Q}/\mathbb{Z}$ is injective by Lemma (11.3). □

Now we prove it for an arbitrary commutative ring.

Theorem 10.5. *Let M be an R-module. Then there is an injective module E and a monomorphism $\varphi \colon M \to E$.*

Proof. First we consider M as a $\mathbb{Z}$-module. Then there exists a $\mathbb{Z}$-injective module E_1 such that we have a monomorphism $\varphi_1 \colon M \to E_1$, by Lemma (10.4). Since R is projective over itself, $\mathrm{Hom}_\mathbb{Z}(R, E_1)$ is injective as an R-module, by Lemma (10.3). Let $\Psi \colon M \to \mathrm{Hom}_\mathbb{Z}(R, E_1)$ be given by

$$\Psi(u)(a) = \varphi_1(au)$$

for all $a \in R$ and $u \in M$. Then Ψ is R-linear and injective. Indeed, it is R-linear since φ_1 is $\mathbb{Z}$-linear. Also, it is injective since if $\Psi(u) = 0$, then

$$\begin{aligned} 0 &= \Psi(u)(1) \\ &= \varphi_1(u), \end{aligned}$$

which implies $u = 0$ since φ_1 is injective. □

10.5 Essential Extensions

Definition 10.3. Let $M \subset E$ be an inclusion of R-modules. We say E is an **essential extension** of M, denoted $M \subset_e E$, if every nonzero submodule of E intersects M nontrivially, that is, if N is a nonzero submodule of E, then $N \cap M \neq 0$. Such an essential extension is called **maximal**, denoted $M \subset_m E$ if no module properly containing E is an essential extension of M, that is, we say E is maximal if $E \subset F$ where the inlusion is strict, then there exists a submodule $N \subset F$ such that $N \cap M = 0$.

Proposition 10.10. *Let M, E, E_1, and E_2 be R-modules*

1. *Suppose $M \subset E_1$ and $M \subset_e E_2$. Then $E_1 \subset_e E_2$.*
2. *Suppose $M \subset_e E_1$ and $E_1 \subset_e E_2$. Then $M \subset_e E_2$.*
3. *E is an essential extension of M if and only if for any nonzero $u \in E$, we have $\langle u \rangle \cap M \neq 0$.*

Proof. 1. Let N be a nonzero submodule of E_2. Since $M \subset_e E_2$, we have $N \cap M \neq 0$. Then since $M \subset E_1$, we have

$$\begin{aligned} E_1 \cap N &\supset M \cap N \\ &\neq 0. \end{aligned}$$

It follows that $E_1 \subset_e E_2$.

2. Let N be a nonzero submodule of E_2. Since $E_1 \subset_e E_2$, we have $N \cap E_1 \neq 0$. Since $N \cap E_1$ is a nonzero submodule of E_1 and $M \subset_e E_1$, we have

$$\begin{aligned} M \cap N &= (M \cap E_1) \cap N \\ &= M \cap (E_1 \cap N) \\ &\neq 0. \end{aligned}$$

It follows that $M \subset_e E_2$.

3. One direction is obvious, so suppose we have $\langle u \rangle \cap M \neq 0$ for all $u \in E$ and let N be a nonzero submodule of E. Choose a nonzero element $w \in N$. Then

$$\begin{aligned} N \cap M &\supset \langle w \rangle \cap M \\ &\neq 0. \end{aligned}$$

□

Example 10.2. Let I be an ideal in R. Then

$$0 :_M I \subset_{\mathrm{e}} \bigcup_{n=1}^{\infty} 0 :_M I^n.$$

Indeed, let u be a nonzero element in $\bigcup_{n=1}^{\infty} 0 :_M I^n$. Choose n is the smallest natural number such that $u\mathfrak{m}^n = 0$. Then

$$\begin{aligned} 0 &\neq u\mathfrak{m}^{n-1} \\ &\subset \langle u \rangle \cap (0 :_M \mathfrak{m}). \end{aligned}$$

Example 10.3. Consider the formal power series ring $R = K[[x]]$ where K is field and let $M = R_x/R$. Every element of M is killed by a power of the maximal ideal, hence

$$M = \bigcup_{n=1}^{\infty} 0 :_M \mathfrak{m}^n.$$

The **socle** of M is defined to be $\operatorname{soc} M := 0 :_M \mathfrak{m}$. Thus by the previous example, we have $\operatorname{soc} M \subset_{\mathrm{e}} M$. It is easy to see that $\operatorname{soc} M$ is the 1-dimensional $\mathbb{C}$-vector space generated by $[1/x]$, that is, the image of $1/x$ in M. On the other hand,

$$\prod_{\mathbb{N}} \operatorname{soc} M \subset \prod_{\mathbb{N}} M$$

is not an essential extension since the element

$$([1/x^n]) \in \prod_{\mathbb{N}} M$$

does not have a nonzero multiple in $\prod_{\mathbb{N}} \operatorname{soc} M$.

10.5.1 Injective Modules are Modules with no Proper Essential Extensions

Lemma 10.6. *Let M be an R-module. Then M is an injective R-module if and only if M has no proper essential extensions.*

Proof. Suppose that M is injective and let $M \subset_{\mathrm{e}} E$ be an essential extension. Since $M \subset E$ and M is injective, we see that M is a direct summand of E, that is $E = M \oplus N$ for some submodule $N \subset E$. Then $M \cap N = 0$ implies $N = 0$, hence $M = E$.

Conversely, suppose that M has no proper essential extension. Embed M into an injective module E and let N be a maximal submodule of E such that $M \cap N = 0$ (Zorn). Then E/N is an essential extension of M by construction, hence $M = E/N$, and therefore $E = M \oplus N$. Then M is injective since E is injective, by Lemma (11.3). □

Lemma 10.7. *Let A be a ring and let M be an A-module. Then M has a maximal essential extension.*

Proof. Embed M into an injective A-module E. We claim that there are maximal essential extensions of M in E. We order the set of essential extensions of M in E by inclusion. The union of a chain of essential extensions is again essential. Therefore, there exists a maximal essential extension by Zorn's lemma. We claim that such an extension is a maximal essential extension in general. Let N be such a maximal essential extension inside E and suppose that N' is an essential extension of N, where N' is not necessarily contained in E. Since $N \to N'$ is an inclusion, and E is injective, we can extend the inclusion $N \to E$ to a map $\varphi : N' \to E$. Since $\operatorname{Ker}(\varphi) \cap M = 0$ by construction, it follows that φ is injective, but this contradicts the maximality of N inside E. □

Theorem 10.8. *Let A be a ring and $M \subset E$ and inclusion of A-modules. The following are equivalent:*

1. *E is a maximal essential exentsion of M.*
2. *E is injective, and is essential over M.*
3. *E is minimal injective over M.*

Proof.

($1 \implies 2$): Follows from Remark (**??**) and Lemma (10.6)

($2 \implies 3$): Suppose that E' is an injective A-module such that $M \subset E' \subset E$. Then the map $E' \subset E$ splits, so $E = E' \oplus N$ for some A-module $N \subset E$. Since $M \subset E'$, we have $M' \cap N = 0$. This implies $N = 0$ since E is essential over M.

($3 \implies 1$): From the proof of Lemma (10.7), it follows that there is a maximal essential extension E' of M contained in E. By ($1 \implies 2$), we see that E' is injective. Since E was a minimal injective module containing M, we have $E = E'$. □

Definition 10.4. If $M \subset E$ satisfies any of the equivalent properties of Theorem (10.8), then E is called an **injective hull** of M.

Lemma 10.9. *Let E and E' be injective hulls of M. Then there exists an isomorphism $\varphi : E \to E'$ which is the identity on M.*

Proof. The map $M \to E'$ can be extended, by injectivity of E, to a map $\varphi : E \to E'$. The map is identity on M and as before since $\operatorname{Ker}(\varphi) \cap M = 0$, it follows by essentiality that φ is injective. Since E' was minimal injective, it follows that φ is surjective as well. □

We use the notation $E(M)$ to denote the injective hull of M, which by the previous lemma, is well-defined up to an isomorphism that fixes M.

Lemma 10.10.

1. *If E is an injective module containing M, then E contains a copy of $E(M)$.*
2. *If $N \supset_e M$, then N can be enlarged to a copy of $E(M)$ and $E(M) = E(N)$.*

Proof.

1. We know that there is a maximal essential extension of M contained in E.
2. A maximal essential extension of N is a maximal essential extension of M.

□

Lemma 10.11. *Let A be a ring, $M_i \subset E_i$ for all $i \in I$ be A-modules over A. Then*

$$\bigoplus_{i \in I} M_i \subset_e \bigoplus_{i \in I} E_i \quad \textit{if and only if} \quad M_i \subset_e E_i$$

for all $i \in I$.

Lemma 10.12. *Let A be a ring and let $M_1, \dots, M_n$ be A-modules. Then*

$$E\left(\bigoplus_{i=1}^{n} M_i\right) = \bigoplus_{i=1}^{n} E\left(M_i\right).$$

10.6 Injective Resolutions and Injective Dimension

Definition 10.5. Let A be a ring and M an A-module. We say that a complex of injective A-modules

$$\mathcal{E} : E_0 \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} E_2 \longrightarrow \cdots$$

is an **injective resolution** of M if $\operatorname{Ker}(\psi_1) = M$ and $\mathcal{E}$ is exact except at E_0. If $\mathcal{E}$ is an injective resolution, then we say that $\mathcal{E}$ is a **minimal injective resolution** if and only if each E_n is the injective hull of $\operatorname{Ker}(\psi_{n+1})$. Every module has a minimal injective resolution, which is unique up to isomorphism. The **injective dimension** of M, denoted $\operatorname{id}_A(M)$, is the length of this resolution (which may be ∞).

Proposition 10.11. *Let A be a Noetherian ring, M an A-module, and S a multiplicatively closed set. Then*

$$id_{A_S}(M_S) \leq id_A(M).$$

Proof. This follows from exactness of localization and Lemma (11.3). □

Proposition 10.12. *Let A be a ring and M an A-module. The following conditions are equivalent*

1. *$id(M) \leq n$;*
2. *$Ext_A^{n+1}(N, M) = 0$ for all A-modules N;*
3. *$Ext_A^{n+1}(A/I, M) = 0$ for all ideals I of A.*

Proof.
1 $\implies$ 2 follows from the fact that $\mathrm{Ext}_A^{n+1}(N, M)$ can be computed from an injective resolution of M.
2 $\implies$ 3 is trivial.
3 $\implies$ 1: Let

$$0 \to M \to E^0 \to E^1 \to E^2 \to \cdots \to E^{n-1} \to C \to 0$$

be an exact sequence, where the modules E^j are injective. From the fact that $\mathrm{Ext}_A^i(A/I, E) = 0$ for $i > 0$ if E is an injective A-module, the above exact sequence yields the isomorphism

$$\mathrm{Ext}_A^1(A/I, C) \cong \mathrm{Ext}_A^{n+1}(A/I, M),$$

and so $\mathrm{Ext}_A^1(A/I, C) = 0$ for all ideals I of A. It follows that C is injective from Remark (10.1). □

We can sharpen Proposition (10.12) if A is a Noetherian ring. We first observe:

Lemma 10.13. *Let A be a Noetherian ring, M an A-module, N a finitely generated A-module, and $n > 0$ an integer. Suppose that $\mathrm{Ext}_A^n(A/\mathfrak{p}, M) = 0$ for all $\mathfrak{p} \in \mathrm{Supp}(N)$. Then $\mathrm{Ext}_A^n(N, M) = 0$.*

Proof. N has a finite filtration whose factors are isomorphic to $A/\mathfrak{p}$ for certain $\mathfrak{p} \in \mathrm{Supp}(N)$. Hence the lemma follows from the additivity of the vanish of $\mathrm{Ext}_A^n(-, M)$. □

Corollary. *Let A be a Noetherian ring and M an A-module. The following are equivalent:*

1. *$\mathrm{id}_A(M) \leq n$;*
2. *$\mathrm{Ext}_A^{n+1}(A/\mathfrak{p}, M) = 0$ for all $\mathfrak{p} \in \mathrm{Spec}(A)$.*

Proposition 10.13. *Let $(A, \mathfrak{m}, k)$ be a Noetherian local ring, $\mathfrak{p}$ a prime ideal different from $\mathfrak{m}$, and M a finitely generated A-module. If $\mathrm{Ext}_A^{n+1}(A/\mathfrak{q}, M) = 0$ for all prime ideals $\mathfrak{q} \in \mathbf{V}(\mathfrak{p})$, with $\mathfrak{q} \neq \mathfrak{p}$, then $\mathrm{Ext}_A^n(A/\mathfrak{p}, M) = 0$.*

Proof. We choose an element $x \in \mathfrak{m} \backslash \mathfrak{p}$. The element is $(A/\mathfrak{p})$-regular, and therefore we get the exact sequence

$$0 \longrightarrow A/\mathfrak{p} \xrightarrow{\cdot x} A/\mathfrak{p} \longrightarrow A/\langle x, \mathfrak{p} \rangle \longrightarrow 0$$

which induces the exact sequence

$$\mathrm{Ext}_A^n(A/\mathfrak{p}, M) \xrightarrow{\cdot x} \mathrm{Ext}_A^n(A/\mathfrak{p}, M) \longrightarrow \mathrm{Ext}_A^{n+1}(A/\langle x, \mathfrak{p} \rangle, M).$$

Since $\mathbf{V}(x, \mathfrak{p}) \subset \{\mathfrak{q} \in \mathbf{V}(\mathfrak{p}) \mid \mathfrak{q} \neq \mathfrak{p}\}$, Lemma (10.13) and our assumption imply

$$\mathrm{Ext}_A^{n+1}(A/\langle x, \mathfrak{p} \rangle, M) = 0,$$

so that multiplication by x on the finitely generated A-module $\mathrm{Ext}_A^n(A/\mathfrak{p}, M)$ is a surjective homomorphism. The desired result follows from Nakayama's lemma. □

It is now easy to derive the following useful formula for the injective dimension of a finitely generated module.

Proposition 10.14. *Let $(A, \mathfrak{m}, k)$ be a Noetherian local ring, and M a finitely generated A-module. Then*

$$\mathit{id}_A(M) = \sup\{i \mid \mathrm{Ext}_A^i(k, M) \neq 0\}.$$

Proof. We set $t = \sup\{i \mid \mathrm{Ext}_A^i(k, M) \neq 0\}$. It is clear that $\mathrm{id}_A(M) \geq t$. To prove the converse inequality, note that the repeated application of Proposition (10.13) yields $\mathrm{Ext}_A^i(A/\mathfrak{p}, M) = 0$ for all $\mathfrak{p} \in \mathrm{Spec}(A)$ and all $i > t$. This implies $\mathrm{id}_A(M) \leq t$. □

Remark. To see how the repeated application of Proposition (10.13) yields $\mathrm{Ext}_A^i(A/\mathfrak{p}, M) = 0$ for all $\mathfrak{p} \in \mathrm{Spec}(A)$ and all $i > t$, suppose $\mathfrak{p}$ has dimension 1. Thus, $\mathbf{V}(\mathfrak{p}) = \{\mathfrak{m}\}$. Then $\mathrm{Ext}^{t+1}(A/\mathfrak{m}, M) = 0$ implies $\mathrm{Ext}_A^t(A/\mathfrak{p}, M) = 0$ and $\mathrm{Ext}^{t+2}(A/\mathfrak{m}, M) = 0$ implies $\mathrm{Ext}_A^{t+1}(A/\mathfrak{p}, M) = 0$. Next, suppose $\mathfrak{q}$ has dimension 2. Then for all primes $\mathfrak{p} \in \mathbf{V}(\mathfrak{q})$ where $\mathfrak{q} \neq \mathfrak{p}$, we've just shown that $\mathrm{Ext}_A^{t+1}(A/\mathfrak{p}, M) = 0$, and this implies $\mathrm{Ext}_A^t(A/\mathfrak{q}, M) = 0$.

Proposition 10.15. *Let A be a ring, M be an A-module, $x \in A$ be an A-regular and M-regular element, and*

$$\mathcal{E} : E_0 \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} E_2 \longrightarrow \cdots$$

be a minimal injective resolution of M. Set $E_i' := \mathrm{Hom}_A(A/x, E_i) \cong \{m \in E_i \mid xm = 0\}$. The complex

$$\mathcal{E}' : E_1' \xrightarrow{\varphi_2} E_2' \xrightarrow{\varphi_3} E_3' \longrightarrow \cdots$$

is a minimal injective resolution of M/xM over A/x. Thus,

$$id_{A/x}(M/xM) = id_A(M) - 1.$$

and if N is an A-module annihilated by x, then

$$Ext_A^{i+1}(N, M) \cong Ext_{A/x}^{i}(N, M/xM)$$

for all $i \geq 0$.

Proof. Lemma (10.3) tells us that E_i' are injective (A/x)-modules. The homology of the complex

$$\mathrm{Hom}_A(A/x, \mathcal{E}) : E_0' \xrightarrow{\varphi_1} E_1' \xrightarrow{\varphi_2} E_2' \xrightarrow{\varphi_3} E_3' \longrightarrow \cdots$$

is by definintion $\mathrm{Ext}_A^*(A/x, M)$. On the other hand, M is an essential submodule of E_0, and M contains no submodule annihilated by x, so E_0 contains no submodule annihilated by x. Thus $E_0' = 0$, and we see that $\mathrm{Hom}_A(A/x, \mathcal{E}) = \mathcal{E}'$.

Computing $\mathrm{Ext}_A^*(A/x, M)$ instead from the free resolution

$$0 \longrightarrow A \xrightarrow{\cdot x} A \longrightarrow A/x \longrightarrow 0,$$

we see that $\mathrm{Ext}_A^1(A/x, M) = M/xM$ while $\mathrm{Ext}_A^i(A/x, M) = 0$ for $i \neq 1$. Thus, $\mathcal{E}'$ is an injective resolution of M/xM. Note that the numbering of the terms of $\mathcal{E}'$ is such that $\mathrm{Ext}_{A/x}^i(N, M/xM)$ is the homology of $\mathrm{Hom}_{A/x}(N, \mathcal{E}')$ at $\mathrm{Hom}_{A/x}(N, E_{j+1}')$; strictly speaking, we should say that $\mathcal{E}'[1]$ is an injective resolution of M/xM.

To see that $\mathcal{E}'$ is minimal, note that $\mathrm{Ker}\left(\varphi_{n+1} : E_n' \to E_{n+1}'\right)$ is the intersection of the essential submodule $\mathrm{Ker}\left(\varphi_{n+1} : E_n \to E_{n+1}\right)$ with E_n', and is thus essential in E_n'. It follows at once that $\mathrm{id}_{A/x}(M/xM) = \mathrm{id}_A(M) - 1$. If x annihilates the A-module N, then every map from N to an E_i has image killed by x, so

$$\mathrm{Hom}_A(N, \mathcal{E}) = \mathrm{Hom}_A(N, \mathcal{E}') = \mathrm{Hom}_{A/x}(N, \mathcal{E}').$$

Taking homology, and taking into account the shift in numbering, we get the last statement of the proposition. □

Remark. Recall that if $(A, \mathfrak{m})$ is a local ring, M is an A-module, and $x \in \mathfrak{m}$ is A-regular and M-regular, then $\mathrm{pd}_{A/x}(M/xM) = \mathrm{pd}_A(M)$. The idea behind that proof was to start with a minimal projective resolution of M,

$$\mathcal{P} : \cdots \longrightarrow P_2 \xrightarrow{\varphi_2} P_1 \xrightarrow{\varphi_1} P_0$$

and show that the sequence

$$\mathcal{P} \otimes (A/x) : \cdots \longrightarrow P_2/xP_2 \xrightarrow{\overline{\varphi}_2} P_1/xP_1 \xrightarrow{\overline{\varphi}_1} P_0/xP_0$$

was a minimal projective resolution of M/xM.

To exploit this result, we need to know the modules of finite injective dimension over a zero-dimensional ring.

Proposition 10.16. *Let A be a local Cohen-Macaulay ring. If M is a maximal Cohen-Macaulay module of finite injective dimension, then $id_A(M) = dim(A)$. If $dim(A) = 0$, then M is a direct sum of copies of ω_A, and $M \cong \omega_A$ if and only if $End_A(M) = A$.*

Proof. Suppose first that $\dim(A) = 0$. Let $D = \mathrm{Hom}_A(-, \omega_A)$ be the dualizing functor. If M has finite injective dimension, then applying D to an injective resolution of M we see that $D(M)$ is a module of finite projective dimension, and is thus free by the Auslander-Buchsbaum formula. Applying D again we see that $M = D^2 M$ is a direct sum of copies of $D(A) = \omega_A$. Using D, we see that the endomorphism ring of ω_A^n is the same as the endomorphism ring of A^n. Thus it is equal to A if and only if $n = 1$.

If $\dim(A) = d$ is arbitrary, then we may choose a regular sequence $x_1, \ldots, x_d$ of A that is a regular sequence on M, and use Proposition (16.6) to conclude that

$$\begin{aligned} \mathrm{id}_A(M) &= d + \mathrm{id}_{A/\langle x_1, \ldots, x_d \rangle}\left(M/\langle x_1, \ldots, x_d \rangle M\right) \\ &= d + 0 \\ &= d. \end{aligned}$$

□

10.7 Injective Modules over Noetherian Rings

Lemma 10.14. *Let A be a Noetherian ring, $S \subset A$ a multiplicatively closed set and M an A-module. Then $E_A(M)_S \cong E_{A_S}(M_S)$.*

Proof. We show that $E_A(M)_S$ is an injective hull of the A_S-module M_S. We know from Lemma (11.3) that $E_A(M)_S$ is an injective A_S-module. It remains to be show that $E_A(M)_S$ is an essential extension of M_S. Choose $e/s \in E_A(M)_S$, where $e \in E_A(M)$ and $s \in S$. We want to show that $A_S(e/s) \cap M_S \neq 0$. We may assume e/s has the form $e/1$, since $A_S(e/s) = A_S(e/1)$. Let

$$I_1 := M :_A e = \{a \in A \mid ae \in M\}.$$

Since $E_A(M)$ is an essential extension of M, we have $ae \neq 0$ for some $a \in I_1$. Since A is Noetherian, I_1 is finitely generated, say $I_1 = \langle a_1, \ldots, a_k \rangle$. Then $a_i e/1 \in M_S$ for each i. If, for some i, we have $a_i e/1 \neq 0$, we are done. So assume $a_i e/1 = 0$ for all i. Then there exists $s_1 \in S$ such that $s_1(a_i e) = a_i(s_1 e) = 0$ for all i. Since $A_S(e/1) = A_S(s_1 e/1)$, we may replace e with $s_1 e$. Let

$$I_2 := M :_A s_1 e = I_1 : s_1.$$

Since $E_A(M)$ is an essential extension of M, we have $a(s_1 e) \neq 0$ for some $a \in I_2$. This implies $I_2 \supsetneq I_1$, since I_1 annihilates $s_1 e$. Proceeding inductively, we obtain a sequence of ideals

$$I_1 \subset I_2 \subset \cdots,$$

which must terminate since A is Noetherian, say $I_n = I_{n+1}$. Then it easily follows that there exists some $a \in I_n$ such that $a(s_n \cdots s_1 e)/1 \neq 0$, for if this was not the case, then we could construct an s_{n+1} as above, and deduce that $I_{n+1} \supsetneq I_n$, which is a contradiction.

□

Proof. Note that $\bigoplus_{i=1}^n E(M_i)$ is injective, and by the previous lemma it is essential over $\bigoplus_{i=1}^n M_i$, hence we are done. □

In the next theorem, we determine the indecomposable injective A-modules of a Noetherian ring A. Recall that an A-module M is **decomposable** if there exist nonzero submodules M_1, M_2 of M such that $M = M_1 \oplus M_2$; otherwise it is **indecomposable**.

Theorem 10.15. *Let A be a Noetherian ring.*

1. *For all $\mathfrak{p} \in Spec(A)$, the module $E(A/\mathfrak{p})$ is indecomposable.*
2. *Let $E \neq 0$ be an injective A-module and let $\mathfrak{p} \in Ass(E)$. Then $E(A/\mathfrak{p})$ is a direct summand of E. In particular, if E is indecomposable, then $E \cong E(A/\mathfrak{p})$.*
3. *Let $\mathfrak{p}, \mathfrak{q} \in Spec(A)$. Then $E(A/\mathfrak{p}) \cong E(A/\mathfrak{q})$ if and only if $\mathfrak{p} = \mathfrak{q}$.*

Proof.

1. Suppose $E(A/\mathfrak{p})$ is decomposable. Then there exist nonzero submodules N_1, N_2 of $E(A/\mathfrak{p})$ such that $N_1 \cap N_2 = 0$. It follows that

   $$(N_1 \cap (A/\mathfrak{p})) \cap (N_2 \cap (A/\mathfrak{p})) = (N_1 \cap N_2) \cap (A/\mathfrak{p}) = 0.$$

   On the other hand, since $A/\mathfrak{p} \subset_e E(A/\mathfrak{p})$ is an essential extension, we have

   $$N_1 \cap (A/\mathfrak{p}) \neq 0 \neq N_2 \cap (A/\mathfrak{p}).$$

   This contradicts the fact that $A/\mathfrak{p}$ is a domain: $N_1 \cap (A/\mathfrak{p})$ and $N_2 \cap (A/\mathfrak{p})$ are ideals in $A/\mathfrak{p}$. Denoting these ideals as I_1 and I_2 respectively, in a domain we have $I_1 \cap I_2 = 0$ implies either $I_1 = 0$ or $I_2 = 0$.

2. $A/\mathfrak{p}$ may be considered as a submodule of E since $\mathfrak{p} \in \mathrm{Ass}(E)$. It follows that there exists an injective hull $E(A/\mathfrak{p})$ of $A/\mathfrak{p}$ such that $E(A/\mathfrak{p}) \subset E$. As $E(A/\mathfrak{p})$ is injective, it is a direct summand of E.

3. Statement 3 follows from the next lemma.

□

Lemma 10.16. *Let A be a Noetherian ring, $\mathfrak{p} \in Spec(A)$, and M a finitely generated A-module. Then*

1. *$Ass(M) = Ass(E(M))$; in particular, one has $\{\mathfrak{p}\} = Ass(E(A/\mathfrak{p}))$.*

2. $k(\mathfrak{p}) \cong Hom_{A_\mathfrak{p}}(k(\mathfrak{p}), E(A/\mathfrak{p})_\mathfrak{p}) \cong Hom_A(A/\mathfrak{p}, E(A/\mathfrak{p}))_\mathfrak{p}$.

Proof.

1. It is clear that $\mathrm{Ass}(M) \subset \mathrm{Ass}(E(M))$. Conversely, suppose $\mathfrak{p} \in \mathrm{Ass}(E(M))$. Then there exists $e \in E(M)$ such that $\mathfrak{p} = 0 : e$. Since $M \subset_e E(M)$ is essential, we have $Ae \cap M \neq 0$. Thus, there exists $a \in A \backslash \mathfrak{p}$ such that $ae \in M$. Then

$$\begin{aligned} 0 : ae &= (0 : e) : a \\ &= \mathfrak{p} : a \\ &= \mathfrak{p}, \end{aligned}$$

implies $\mathfrak{p} \in \mathrm{Ass}(M)$.

2. Since $E(A/\mathfrak{p})_\mathfrak{p} \cong E_{A_\mathfrak{p}}(k(\mathfrak{p}))$, we assume that $(A, \mathfrak{m}, k)$ is local and $\mathfrak{p} = \mathfrak{m}$ is the maximal ideal. The k-vector space $\mathrm{Hom}_A(k, E(k))$ may be identified with

$$V = \{e \in E(k) \mid \mathfrak{m}e = 0\} = \mathrm{Soc}(E(k)),$$

which contains k. If $V \neq k$, then there exists a nonzero vector subspace W of V with $k \cap W = 0$. This, however, contradicts the essentiality of the extension $k \subset E(k)$. The second isomorphism follows from

$$\mathrm{Hom}_{A_\mathfrak{p}}(k(\mathfrak{p}), E(A/\mathfrak{p})_\mathfrak{p}) = \mathrm{Hom}_{A_\mathfrak{p}}(A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}, E(A/\mathfrak{p})_\mathfrak{p}) \cong \mathrm{Hom}_{A_\mathfrak{p}}((A/\mathfrak{p})_\mathfrak{p}, E(A/\mathfrak{p})_\mathfrak{p}) \cong \mathrm{Hom}_A(A/\mathfrak{p}, E(A/\mathfrak{p}))_\mathfrak{p}$$

□

The importance of the indecomposable injective A-modules results from the following:

Theorem 10.17. *Let A be a Noetherian ring. Every injective A-module E is a direct sum of indecomposable injective A-modules, and this decomposition is unique in the following sense: for any $\mathfrak{p} \in Spec(A)$, the number of indecomposable summands in the decomposition of E which are isomorphic to $E(A/\mathfrak{p})$ depends only on E and $\mathfrak{p}$ (and not on the particular decomposition). In fact, this number equals*

$$dim_{k(\mathfrak{p})}\left(Hom_{A_\mathfrak{p}}(k(\mathfrak{p}), E_\mathfrak{p})\right).$$

Proof. Consider the set $\mathcal{I}$ of all subsets of the set of indecomposable injective submodules of E with the property: if $\mathcal{F} \in \mathcal{I}$, then the sum of all modules belonging to $\mathcal{F}$ is direct. The set $\mathcal{I}$ is partially ordered by inclusion. By Zorn's lemma it has a maximal element $\mathcal{F}'$. Let F be the sum of all the modules in $\mathcal{F}'$. The module F is a direct sum of injective modules, and hence is itself injective. Therefore F is a direct summand of E, and we can write $E = F \oplus H$, where H is injective since it is a direct summand of E. Suppose $H \neq 0$, then there exists $\mathfrak{p} \in \mathrm{Ass}(H)$, and so $E(A/\mathfrak{p})$ is a direct summand of H. Thus we may enlarge $\mathcal{F}'$ by $E(A/\mathfrak{p})$, contradicting the maximality of $\mathcal{F}'$. We conclude that $H = 0$ and $E = F$.

Suppose that $E = \bigoplus_{\lambda \in \Lambda} E_\lambda$ is the given decomposition. Then

$$\mathrm{Hom}_{A_\mathfrak{p}}(k(\mathfrak{p}), E_\mathfrak{p}) \cong \mathrm{Hom}_{A_\mathfrak{p}}\left(k(\mathfrak{p}), \bigoplus_{\lambda \in \Lambda}(E_\lambda)_\mathfrak{p}\right) \cong \bigoplus_{\lambda \in \Lambda} \mathrm{Hom}_{A_\mathfrak{p}}\left(k(\mathfrak{p}), (E_\lambda)_\mathfrak{p}\right),$$

where we used the fact that $k(\mathfrak{p})$ is finitely generated in the second isomorphism. By Lemma (10.16), we have

$$\bigoplus_{\lambda \in \Lambda} \mathrm{Hom}_{A_\mathfrak{p}}\left(k(\mathfrak{p}), (E_\lambda)_\mathfrak{p}\right) \cong \bigoplus_{\lambda \in \Lambda_0} \mathrm{Hom}_{A_\mathfrak{p}}\left(k(\mathfrak{p}), (E_\lambda)_\mathfrak{p}\right)$$

where $\Lambda_0 = \{\lambda \in \Lambda \mid E_\lambda \cong E(A/\mathfrak{p})\}$. If we again use Lemma (10.16), we finally get

$$\mathrm{Hom}_{A_\mathfrak{p}}(k(\mathfrak{p}), E_\mathfrak{p}) \cong \bigoplus_{\lambda \in \Lambda_0} \mathrm{Hom}_{A_\mathfrak{p}}\left(k(\mathfrak{p}), (E_\lambda)_\mathfrak{p}\right) \cong k(\mathfrak{p})^{\Lambda_0}$$

□

Theorem 10.18. *Let A be a Noetherian ring and E an injective A-module. Then*

$$E \cong \bigoplus_i E_A(A/\mathfrak{p}_i),$$

where $\mathfrak{p}_i$ are prime ideals of A. Moreover, any such direct sum is an injective A-module.

Proof. Let E be an injective A-module. By Zorn's Lemma, there exists a maximal family $\{E_i\}$ of injective submodules of E such that $E_i \cong E_A(A/\mathfrak{p}_i)$, and their sum in E is a direct sum. Let $E' = \bigoplus_i E_i$, which is an injective module, and hence is a direct summand of E. There exists an A-module E'' such that $E = E' \bigoplus E''$. If $E'' \neq 0$, pick a nonzero element $x \in E''$. Let $\mathfrak{p}$ be an associated prime of Ax. Then $A/\mathfrak{p} \hookrightarrow Ax \subseteq E''$, so there is a copy of $E_A(A/\mathfrak{p})$ contained in E'' and $E'' = E_A(A/\mathfrak{p}) \bigoplus E'''$, contradicting the maximality of the family $\{E_i\}$. □

Theorem 10.19. *Let A be a Noetherian ring, $\mathfrak{p}$ be a prime ideal of A, $E = E_A(A/\mathfrak{p})$ and let $k = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$. Then*

1. *If $x \in A \backslash \mathfrak{p}$, then $E \xrightarrow{\cdot x} E$ is an isomorphism, and so $E = E_\mathfrak{p}$.*
2. *$0 :_E \mathfrak{p} = k$.*
3. *$k \subseteq E$ is an essential extension of $A_\mathfrak{p}$-modules and $E = E_{A_\mathfrak{p}}(k)$.*
4. *E is $\mathfrak{p}$-torsion and $Ass(E) = \{\mathfrak{p}\}$.*
5. *$Hom_{A_\mathfrak{p}}(k, E) = k$ and $Hom_{A_\mathfrak{p}}(k, E_A(A/\mathfrak{q})_\mathfrak{p}) = 0$ for primes $\mathfrak{q} \neq \mathfrak{p}$.*

Proof.

1. Since $A/\mathfrak{p}$ is a domain and $Q(A/\mathfrak{p}) = k$, Proposition (10.9) tells us that k is an essential extension of $A/\mathfrak{p}$, so E contains a copy of k and we may assume $A/\mathfrak{p} \subseteq k \subseteq E$. Multiplication by $x \in A\backslash\mathfrak{p}$ is injective on k, and hence also on its essential extension E. The submodule xE is injective, so it is a direct summand of E. But $k \subseteq xE \subseteq E$ are essential extensions, so $xE = E$.

2. $0 :_E \mathfrak{p} = 0 :_E \mathfrak{p}A_\mathfrak{p}$ is a vector space over the field k, and hence the inclusion $k \subseteq 0 :_E \mathfrak{p}$ splits. But $k \subseteq 0 :_E \mathfrak{p} \subseteq E$ is an essential extension, so $0 :_E \mathfrak{p} = k$.

3. The containment $k \subseteq E$ is an essential extension of A-modules, hence also of $A_\mathfrak{p}$-modules. Suppose $E \subseteq M$ is an essential extension of $A_\mathfrak{p}$-modules, pick $m \in M$. Then m has a nonzero multiple $(a/s)m \in E$, where $s \in A\backslash\mathfrak{p}$. But then am is a nonzero multiple of m in E, so $E \subseteq M$ is an essential extension of A-modules, and therefore $M = E$.

4. Let $\mathfrak{q} \in \mathrm{Ass}(E)$. Then there exists $x \in E$ such that $Ax \subseteq E$ and $0 :_A x = \mathfrak{q}$. Since $A/\mathfrak{p} \subseteq E$ is essential, x has a nonzero multiple $y = ax$ in $A/\mathfrak{p}$. But then the $\mathfrak{p} = 0 :_A y = 0 :_E ax = (0 :_E x) :_A a$ implies $\mathfrak{q} = \mathfrak{p}$. Therefore $\mathrm{Ass}(E) = \{\mathfrak{p}\}$. Now suppose $x \in E$. Then $0 :_E x$ must be $\mathfrak{p}$-primary since $\mathfrak{p}$ is the only associated prime of $0 :_E x \hookrightarrow E$. In particular, $0 :_E x \supset \mathfrak{p}^n$ for some n, and this proves our claim.

5. For the first assertion,
$$\mathrm{Hom}_{A_\mathfrak{p}}(k, E) = \mathrm{Hom}_{A_\mathfrak{p}}(A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}, E) \cong 0 :_E \mathfrak{p}A_\mathfrak{p} = k.$$
For the first assertion, if $\mathfrak{q} \subsetneq \mathfrak{p}$, then $\mathfrak{q}^n \subsetneq \mathfrak{p}$. Therefore since $E_A(A/\mathfrak{q})$ is $\mathfrak{q}$-torsion, we see that $E_A(A/\mathfrak{q})_\mathfrak{p} = 0$ if $\mathfrak{q} \subsetneq \mathfrak{p}$. In the case $\mathfrak{q} \subseteq \mathfrak{p}$, we have
$$\mathrm{Hom}_{A_\mathfrak{p}}(k, E_A(A/\mathfrak{q})_\mathfrak{p}) \cong 0 :_{E_A(A/\mathfrak{q})_\mathfrak{p}} \mathfrak{p}A_\mathfrak{p} = 0 :_{E_A(A/\mathfrak{q})} \mathfrak{p}A_\mathfrak{p}.$$
If this is nonzero, then there is a nonzero element of $E_A(A/\mathfrak{q})$ killed by $\mathfrak{p}$, which forces $\mathfrak{q} = \mathfrak{p}$ since $\mathrm{Ass}(E_A(A/\mathfrak{q})) = \{\mathfrak{q}\}$.

□

Theorem 10.20. *Let A be a Noetherian ring and $\mathfrak{p}$ be a prime ideal of A. Then*

1. *If $x \in A\backslash\mathfrak{p}$, then $E_A(A/\mathfrak{p}) \xrightarrow{\cdot x} (A/\mathfrak{p})$ is an isomorphism, and so $E_A(A/\mathfrak{p}) = E_A(A/\mathfrak{p})_\mathfrak{p}$.*
2. *$Hom_A(A/\mathfrak{p}, E_A(A/\mathfrak{p})) = 0 :_{E_A(A/\mathfrak{p})} \mathfrak{p} = 0 :_{E_A(A/\mathfrak{p})_\mathfrak{p}} k(\mathfrak{p}) = 0 :_{E_{A_\mathfrak{p}}(k(\mathfrak{p}))} k(\mathfrak{p}) = Hom_{A_\mathfrak{p}}(k(\mathfrak{p}), E_{A_\mathfrak{p}}(k(\mathfrak{p})) = k(\mathfrak{p})$.*
3. *$Ass(E_A(A/\mathfrak{p})) = \{\mathfrak{p}\}$ and $E_A(A/\mathfrak{p})$ is $\mathfrak{p}$-torsion.*
4. *$Hom_{A_\mathfrak{p}}(k(\mathfrak{p}), E_A(A/\mathfrak{q})_\mathfrak{p}) = 0$ for primes $\mathfrak{q} \neq \mathfrak{p}$.*

Proof.

1. Since $A/\mathfrak{p}$ is a domain and $Q(A/\mathfrak{p}) = k$, Proposition (10.9) tells us that k is an essential extension of $A/\mathfrak{p}$, so E contains a copy of k and we may assume $A/\mathfrak{p} \subseteq k \subseteq E$. Multiplication by $x \in A\backslash\mathfrak{p}$ is injective on k, and hence also on its essential extension E. The submodule xE is injective, so it is a direct summand of E. But $k \subseteq xE \subseteq E$ are essential extensions, so $xE = E$.

2. $0 :_E \mathfrak{p} = 0 :_E \mathfrak{p}A_{\mathfrak{p}}$ is a vector space over the field k, and hence the inclusion $k \subseteq 0 :_E \mathfrak{p}$ splits. But $k \subseteq 0 :_E \mathfrak{p} \subseteq E$ is an essential extension, so $0 :_E \mathfrak{p} = k$.

3. The containment $k \subseteq E$ is an essential extension of A-modules, hence also of $A_{\mathfrak{p}}$-modules. Suppose $E \subsetneq M$ is an essential extension of $A_{\mathfrak{p}}$-modules, pick $m \in M$. Then m has a nonzero multiple $(a/s)m \in E$, where $s \in A \backslash \mathfrak{p}$. But then am is a nonzero multiple of m in E, so $E \subseteq M$ is an essential extension of A-modules, and therefore $M = E$.

4. Let $\mathfrak{q} \in \mathrm{Ass}(E)$. Then there exists $x \in E$ such that $Ax \subseteq E$ and $0 :_A x = \mathfrak{q}$. Since $A/\mathfrak{p} \subseteq E$ is essential, x has a nonzero multiple $y = ax$ in $A/\mathfrak{p}$. But then the $\mathfrak{p} = 0 :_A y = 0 :_E ax = (0 :_E x) :_A a$ implies $\mathfrak{q} = \mathfrak{p}$. Therefore $\mathrm{Ass}(E) = \{\mathfrak{p}\}$. Now suppose $x \in E$. Then $0 :_E x$ must be $\mathfrak{p}$-primary since $\mathfrak{p}$ is the only associated prime of $0 :_E x \hookrightarrow E$. In particular, $0 :_E x \supset \mathfrak{p}^n$ for some n, and this proves our claim.

5. For the first assertion,
$$\mathrm{Hom}_{A_{\mathfrak{p}}}(k, E) = \mathrm{Hom}_{A_{\mathfrak{p}}}(A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}, E) \cong 0 :_E \mathfrak{p}A_{\mathfrak{p}} = k.$$
For the first assertion, if $\mathfrak{q} \subsetneq \mathfrak{p}$, then $\mathfrak{q}^n \subsetneq \mathfrak{p}$. Therefore since $E_A(A/\mathfrak{q})$ is $\mathfrak{q}$-torsion, we see that $E_A(A/\mathfrak{q})_{\mathfrak{p}} = 0$ if $\mathfrak{q} \subsetneq \mathfrak{p}$. In the case $\mathfrak{q} \subseteq \mathfrak{p}$, we have
$$\mathrm{Hom}_{A_{\mathfrak{p}}}(k, E_A(A/\mathfrak{q})_{\mathfrak{p}}) \cong 0 :_{E_A(A/\mathfrak{q})_{\mathfrak{p}}} \mathfrak{p}A_{\mathfrak{p}} = 0 :_{E_A(A/\mathfrak{q})} \mathfrak{p}A_{\mathfrak{p}}.$$
If this is nonzero, then there is a nonzero element of $E_A(A/\mathfrak{q})$ killed by $\mathfrak{p}$, which forces $\mathfrak{q} = \mathfrak{p}$ since $\mathrm{Ass}(E_A(A/\mathfrak{q})) = \{\mathfrak{q}\}$.

□

Theorem 10.21. *Let A be a Noetherian ring and let E be an injective A-module. Then*
$$E = \bigoplus_{\mathfrak{p} \in Spec(A)} E_A(A/\mathfrak{p})^{\alpha_{\mathfrak{p}}}$$
and the numbers $\alpha_{\mathfrak{p}}$ are independent of the direct sum decomposition.

Proof. By Theorem (10.18), there is a direct sum
$$E \cong \bigoplus_i E_A(A/\mathfrak{p}_i).$$
Theorem (10.20) implies $\alpha_{\mathfrak{p}}$ is the dimension of the $k(\mathfrak{p})$-vector space
$$\mathrm{Hom}_{A_{\mathfrak{p}}}(k(\mathfrak{p}), E_{\mathfrak{p}}),$$
which does not depend on the decomposition. □

11 Flatness

11.1 Definition of Flatness

Definition 11.1. Let F be an R-module. We say F is **flat** if for every injective R-linear map $\varphi \colon M \to N$, the induced map $1 \otimes \varphi \colon F \otimes_R M \to F \otimes_R N$ is again injective. An R-algebra A is called flat if it is flat as an R-module.

An equivalent definition of being flat is given in the following proposition:

Proposition 11.1. *Let F be an R-module. Then F is flat if and only if the covariant function $F \otimes_R -$ is exact.*

Proof. Suppose that F is flat. Let
$$\begin{tikzcd} 0 \arrow[r] & M_1 \arrow[r, "\varphi_1"] & M_2 \arrow[r, "\varphi_2"] & M_3 \arrow[r] & 0 \end{tikzcd}$$
be an exact sequence of R-modules. Since $F \otimes_R -$ is right exact, we only need to check that
$$\begin{tikzcd} 0 \arrow[r] & F \otimes_R M_1 \arrow[r, "1 \otimes \varphi_1"] & F \otimes_R M_2 \end{tikzcd}$$
is exact at $F \otimes_R M_1$. This is equivalent to showing $1 \otimes \varphi_1$ is injective, and this is holds since F is flat. Conversely, suppose $F \otimes_R -$ is exact. Let $\varphi \colon M \to N$ be any injective R-linear map. Since $F \otimes_R -$ is exact, the induced map $1 \otimes \varphi \colon F \otimes_R M \to F \otimes_R N$ is also injective. In other words, F is flat. □

Example 11.1. Free modules are flat.

Example 11.2. Let $x \in R$. Then R/x not a flat R-module. Indeed, let I be any finitely generated ideal in R. Then

$$I/Ix \cong I \otimes_R R/x \to I(R/x) \cong I/(I \cap x)$$

is injective if and only if $Ix = I \cap x$. In particular, if I contains x, then this map is not injective.

Example 11.3. Let $R = K[x]$ and $A = K[x,y]/\langle xy, y^2 \rangle$. Then A is an R-algebra via the unique map $\varphi\colon R \to A$ such that $\varphi(x) = \overline{x}$, but A is not flat as an R-module since $\langle x \rangle \otimes_R A \to \overline{x}A$ is not injective. For instance, $x \otimes \overline{y} \mapsto \overline{xy} = 0$ in xA, but $x \otimes \overline{y} \neq 0$ in $\langle x \rangle \otimes_A B$.

11.2 Criterion for Flatness Using Tor

Theorem 11.1. *Let M be an R-module. Then M is flat if and only if*

$$\mathrm{Tor}_1^R(R/I, M) \cong 0$$

for all finitely generated ideals I in R.

Remark. Before we give a proof, we first make the following observation; namely that if I is an ideal in R, then $\mathrm{Tor}_1^R(R/I, M) \cong 0$ if and only if $I \otimes_R M \to M$ is injective. Indeed, applying $- \otimes_R M$ to the short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & I \arrow[r] & R \arrow[r] & R/I \arrow[r] & 0 \end{tikzcd}$$

gives us the exact sequence

$$\begin{tikzcd} 0 \cong \mathrm{Tor}_1^R(R, M) \arrow[r] & \mathrm{Tor}_1^R(R/I, M) \arrow[r] & I \otimes_R M \arrow[r] & R \otimes_R M \cong M. \end{tikzcd} \tag{47}$$

From the exact sequence (47), we see that $\mathrm{Tor}_1^R(R/I, M) \cong 0$ if and only if $I \otimes_R M \to M$ is injective.

Proof. Suppose M is flat and let I be a finitely generated ideal in R. It follows from Remark (11.2) that $\mathrm{Tor}_1^R(R/I, M) \cong 0$. Since I was arbitrary, this implies $\mathrm{Tor}_1^R(R/I, M) \cong 0$ for all finitely generated ideals $I \subset R$.

Now assume $\mathrm{Tor}_1^R(R/I, M) \cong 0$ for all finitely generated ideals $I \subset R$. Thus $I \otimes_R M \to M$ is injective for all finitely generated ideals $I \subset R$ by Remark (11.2). What we need to show is that, for any injective map $\iota\colon L \to N$, the induced map $L \otimes_R M \to N \otimes_R M$ is injective. First consider the case of the inclusion map $I \subset R$ where I is an ideal (not necessarily finitely generated). Assume for a contradiction that $I \otimes_R M \to M$ is not injective. Choose

$$\sum_{i=1}^{n} x_i \otimes u_i \in I \otimes_R M$$

different from zero with $\sum_{i=1}^{n} x_i u_i = 0$. Let $I_0 := \langle x_1, \ldots, x_n \rangle$. Then

$$\sum_{i=1}^{n} x_i \otimes u_i \in I_0 \otimes_R M$$

and, therefore, by assumption, it has to be zero. In particular, its image in $I \otimes_R M$ has to be zero too, which is a contradiction. Thus $I \otimes_R M \to M$ is injective for all ideals $I \subset R$.

Now we consider the more general case. Let $\iota\colon L \to N$ be an injective map. If $L \otimes_R M \to N \otimes_R M$ is not injective, then there exists

$$\sum_{i=1}^{n} u_i \otimes v_i \in L \otimes_A M$$

different from zero with

$$\sum_{i=1}^{n} \iota(u_i) \otimes v_i = 0.$$

Setting $N_0 = \sum_{i=1}^{n} \iota(u_i)R$, this would imply $L \otimes_A M \to N_0 \otimes_A M$ is not injective. So by passing to N_0 if necessary, we may assume that N is finitely generated.

Since N is finitely generated, we can find an increasing chain

$$L = L_0 \subset L_1 \subset \cdots \subset L_r = N$$

of R-modules such that each quotient L_{i+1}/L_i is generated by one element, that is, $L_{i+1}/L_i \cong R/I_i$ for some ideal I_i. Since the map $L \otimes_R M \to N \otimes_R M$ is equal to the composition of the maps $L_i \otimes_A M \to L_{i+1} \otimes_A M$, it is enough to show that $L_i \otimes_A M \to L_{i+1} \otimes_A M$ is injective for all i. We have therefore reduced the statement to the case that $L/N \cong R/I$. Now, consider the exact sequence

$$\begin{tikzcd} \mathrm{Tor}_1^R(R/I, M) = \mathrm{Tor}_1^R(L/N, M) \arrow[r] & N \otimes_R M \arrow[r] & L \otimes_R M. \end{tikzcd}$$

By assumption, $\mathrm{Tor}_1^R(R/I, M) = 0$, and so $L \otimes_A M \to N \otimes_A M$ is injective. □

11.3 Criterion for Flatness Using Equations

We want to give another criterion for flatness, in terms of equations in M, but first we need a lemma.

Lemma 11.2. *Let M and N be R-modules, let I be an indexing set, let $u_i \in M$ for all $i \in I$, and let $N = \langle v_i \mid i \in I \rangle$. Then $\sum_{i\in I} u_i \otimes v_i = 0$* [5] *if and only if there exists an indexing set J and there exists $a_{ij} \in R$ and $\widetilde{u}_j \in M$, for $i \in I$ and $j \in J$, such that*

1. *$\sum_{j\in J} a_{ij}\widetilde{u}_j = u_i$ for all $i \in I$, and;*
2. *$\sum_{i\in I} a_{ij}v_i = 0$ for all $j \in J$.*

Proof. Suppose $\sum_{j\in J} a_{ij}\widetilde{u}_j = u_i$ and $\sum_{i\in I} a_{ij}v_i = 0$, then

$$\begin{aligned}\sum_{i\in I} u_i \otimes v_i &= \sum_{i\in I}\left(\sum_{j\in J} a_{ij}\widetilde{u}_j\right) \otimes v_i \\ &= \sum_{j\in J} \widetilde{u}_j \otimes \left(\sum_{i\in I} a_{ij}v_i\right) \\ &= \sum_{j\in J} \widetilde{u}_j \otimes 0 \\ &= 0.\end{aligned}$$

Conversely, suppose $\sum_{i\in I} u_i \otimes v_i = 0$. Let

$$\begin{tikzcd} F_1 \arrow[r, "\lambda"] & F_0 \arrow[r, "\pi"] & N \arrow[r] & 0 \end{tikzcd}$$

be a presentation of N such that there is a basis $\{f_j\}_{j\in J}$ of F_1 and $\{e_i\}_{i\in I}$ of F_0 with $\lambda(f_j) = \sum_{i\in I} a_{ij}e_i$ and $\pi(e_i) = v_i$ for all $i \in I$ and $j \in J$. Now apply $M \otimes_R -$ to the presentation to get an exact sequence:

$$\begin{tikzcd} M \otimes_R F_1 \arrow[r, "1\otimes\lambda"] & M \otimes_R F_0 \arrow[r, "1\otimes\pi"] & M \otimes N \arrow[r] & 0 \end{tikzcd}$$

In these terms our assumption reads, $(1 \otimes \pi)(\sum_{i\in I} u_i \otimes e_i) = 0$, which implies $\sum_{i\in I} u_i \otimes e_i \in \ker(1 \otimes \pi)$. By the exactness of the diagram above, there exists some $\sum_{j\in J} \widetilde{u}_j \otimes f_j \in M \otimes_A F_1$ such that $(1 \otimes \lambda)(\sum_{j\in J} \widetilde{u}_j \otimes f_j) = \sum_{i\in I} u_i \otimes e_i$. So

$$\begin{aligned}\sum_{i\in I} u_i \otimes e_i &= (1 \otimes \lambda)(\sum_{j\in J} \widetilde{u}_j \otimes f_j) \\ &= \sum_{j\in J} 1(\widetilde{u}_j) \otimes \lambda(f_j) \\ &= \sum_{j\in J} \widetilde{u}_j \otimes \left(\sum_{i\in I} a_{ij}e_i\right) \\ &= \sum_{i\in I}\left(\sum_{j\in J} a_{ij}\widetilde{u}_j\right) \otimes e_i.\end{aligned}$$

This implies $u_i = \sum_{j\in J} a_{ij}\widetilde{u}_j$, since $M \otimes_R F_0$ is a free R-module with basis $\{e_i\}_{i\in I}$. To show $\sum_{i\in I} a_{ij}v_i = 0$, note that $\sum_{i\in I} a_{ij}v_i = \pi(\lambda(f_j)) = 0$. □

Proposition 11.2. *Let M be an R-module. Then M is flat if and only if the following condition is satisfied: If $\sum_{i=1}^r a_iu_i = 0$ where $a_i \in R$ and $u_i \in M$. Then there exists $a_{ij} \in R$ and $\widetilde{u}_j \in M$ such that*

1. *$\sum_{j=1}^s a_{ij}\widetilde{u}_j = u_i$ for all $i = 1, \dots, r$*
2. *$\sum_{i=1}^r a_{ij}a_i = 0$ for all $j = 1, \dots, s$.*

Proof. Assume that M is flat. Suppose

$$\sum_{i=1}^r a_iu_i = 0,$$

where $a_i \in R$ and $u_i \in M$. Set $I := \langle a_1, \dots, a_r \rangle$. Since M is flat, the map $I \otimes_R M \to M$, induced by $I \subset R$, is injective. This implies $\sum_{i=1}^r a_i \otimes u_i = 0$, and the result follows from Lemma (11.2).

Conversely, assume that the condition above is satisfied, and let $I \subset R$ be a finitely generated ideal. By Theorem (11.1), it suffices to prove that $\operatorname{Tor}_1^R(R/I, M) = 0$, or equivalently, that the induced map $I \otimes_R M \to M$ is injective. Let $\sum_{i=1}^r a_i \otimes u_i \in I \otimes_R M$ such that $\sum_i a_iu_i = 0$. Then again by Lemma (11.2), we see that $\sum_{i=1}^r a_i \otimes u_i = 0$. Thus $I \otimes_R M \to M$ is injective. □

[5] Of course, there are only finitely many indices $i \in I$ with $u_i \neq 0$ in such a sum.

Let $I = \langle a \rangle \subset R$ be a principal ideal. Then the preceding proof shows that the induced map $\langle a \rangle \otimes_R M \to M$ is injective if and only if the following condition holds: $au = 0$ for $u \in M$ implies that there exists $a_1, \dots, a_s \in A$ and $\widetilde{u}_1, \dots, \widetilde{u}_s \in M$ such that $u = \sum_{i=1}^{s} a_i \widetilde{u}_i$ and $aa_i = 0$ for all i. In other words, $\langle a \rangle \otimes_R M \to M$ is injective if and only if

$$\mathrm{Ann}_M(a) \subset \mathrm{Ann}_R(a) \cdot M.$$

Since the other inclusion is obvious, we have shown

Corollary. *Let A be a principal ideal ring. Then an R-module M is flat if and only if*

$$Ann_M(a) = Ann_A(a) \cdot M$$

for every $a \in A$. Moreover, if A is integral, then M is flat if and only if it is torsion free.

Corollary. *A $K[\varepsilon]$-module is flat if and only if $Ann_M(\varepsilon) = \varepsilon M$, i.e. the multiplication by ε induces an isomorphism $M/\varepsilon M \cong \varepsilon M$.*

11.3.1 Finitely Generated Flat Modules over Local Ring are Free

Proposition 11.3. *Let $(R, \mathfrak{m})$ be a local ring and let M be a flat R-module. Moreover, let $u_1, \dots, u_k \in M$ such that their classes $\overline{u}_1, \dots, \overline{u}_k$ in $M/\mathfrak{m}M$ are linearly independent. Then $u_1, \dots, u_k$ are linearly independent. In particular, a finitely generated R-module is flat if and only if it is free.*

Proof. We use induction on k. Let $k = 1$ and assume $au_1 = 0$ for some $a \in R$. Using Proposition (11.2), we obtain $\widetilde{u}_j \in M$ and $a_j \in R$ such that $\sum_j a_j \widetilde{u}_j = u_1$ and $aa_j = 0$ for all j. But $u_1 \notin \mathfrak{m}M$ implies $a_j \notin \mathfrak{m}$ for some j, and therefore $a = 0$.

Assume the corollary is proved for $k - 1$. Let $\sum_{i=1}^{k} a_i u_i = 0$. We use Proposition (11.2) again and obtain $\widetilde{u}_j \in M$ and $a_{ij} \in A$ such that $\sum_j a_{ij} \widetilde{u}_j = u_i$ and $\sum_i a_{ij} a_j = 0$ for all i and for all j respectively. Because $u_k \notin \mathfrak{m}M$, we have $a_{kj} \notin \mathfrak{m}$ for some j. This implies that a_k is a linear combination of $a_1, \dots, a_{k-1}$

$$a_k = \sum_{i=1}^{k-1} h_i a_i$$

for $h_i = -a_{ij}/a_{kj}$. Now we have

$$\begin{aligned} 0 &= \sum_{i=1}^{k} a_i u_i \\ &= \sum_{i=1}^{k-1} a_i u_i + a_k u_k \\ &= \sum_{i=1}^{k-1} a_i u_i + \sum_{i=1}^{k-1} h_i a_i u_k \\ &= \sum_{i=1}^{k-1} a_i (u_i + h_i u_k). \end{aligned}$$

The induction hypothesis implies that $a_1 = \cdots = a_{k-1} = 0$, and therefore $a_k = 0$ by the base case. □

11.4 More Properties of Flat Modules

Lemma 11.3. *Let M be a flat R-module, let $\{M_\lambda\}_{\lambda \in \Lambda}$ be a colletion of R-modules indexed by a set Λ, and let S be a multiplicatively closed subset of R. Then*

1. *$\bigoplus_{\lambda \in \Lambda} M_\lambda$ is flat if and only if all the M_λ are flat.*
2. *M_S is a flat R_S-module, and hence a flat R-module.*

Proof.
1. Since we have isomorophisms

$$N \otimes_R \left(\bigoplus_{\lambda \in \Lambda} M_\lambda \right) \cong \bigoplus_{\lambda \in \Lambda} (N \otimes_R M_\lambda)$$

natural in N, the functor $- \otimes_R \left(\bigoplus_{\lambda \in \Lambda} M_\lambda \right)$ is exact if and only if the functors $- \otimes_R M_\lambda$ are exact for all $\lambda \in \Lambda$.

2. Let I_S be an ideal in R_S. Since localization is exact and commutes with tensors products, we see that $I \otimes_R M \to M$ is injective implies $I_S \otimes_{R_S} M_S \to M_S$ is injective. Therefore M_S is a flat R_S-module. To see that M_S is a flat R-module, note that

$$\begin{aligned} I \otimes_R M_S &\cong I \otimes_R (R_S \otimes_{R_S} M_S) \\ &\cong (I \otimes_R R_S) \otimes_{R_S} M_S \\ &\cong I_S \otimes_{R_S} M_S. \end{aligned}$$

Thus injectivity of $I \otimes_R M_S \to M_S$ is equivalent to injectivity of $I_S \otimes_R M_S \to M_S$. □

Corollary. *Let P be a projective R-module. Then P is flat.*

Proof. First note that every free module is flat. Indeed, R is flat as an R-module and every free module is a direct sum copies of R. Thus Lemma (11.3) implies every free module is flat. Since P is projective, there exists an R-module K and a free R-module F such that $P \oplus K \cong F$. Then it follows Lemma (11.3) that P is flat since F is flat. □

11.4.1 Flat Modules are not necessarily Projective

Proposition 11.4. *$\mathbb{Q}$ is a flat $\mathbb{Z}$-module that is not projective.*

Proof. It follows from Proposition (**??**) that $\mathbb{Q}$ is a flat $\mathbb{Z}$-module, so we just need to show that $\mathbb{Q}$ is not projective. Let $\varphi \colon \bigoplus_{i \in \mathbb{N}} \mathbb{Z} \to \mathbb{Q}$ be the unique $\mathbb{Z}$-linear map defined on the standard basis $\{e_n\}$ of $\bigoplus_{i \in \mathbb{N}} \mathbb{Z}$ by

$$\varphi(e_n) = \frac{1}{n}$$

for all $n \in \mathbb{N}$, and let $\psi \colon \mathbb{Q} \to \mathbb{Q}$ be the identity map. Observe that φ is surjective since if $m/n \in \mathbb{Q}$, then $\varphi(me_n) = m/n$. However there is no $\widetilde{\psi} \colon \mathbb{Q} \to \bigoplus_{n \in \mathbb{N}} \mathbb{Z}$ such that $\psi = \varphi\widetilde{\psi}$. Indeed, observe that the injective map

$$\bigoplus_{n \in \mathbb{N}} \mathbb{Z} \to \prod_{n \in \mathbb{N}} \mathbb{Z}$$

induces the injective map

$$\mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Q}, \bigoplus_{n \in \mathbb{N}} \mathbb{Z}\right) \to \mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Q}, \prod_{n \in \mathbb{N}} \mathbb{Z}\right)$$

since $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, -)$ is a left-exact covariant functor. Therefore the injection

$$\begin{aligned} \mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Q}, \bigoplus_{n \in \mathbb{N}} \mathbb{Z}\right) &\to \mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Q}, \prod_{n \in \mathbb{N}} \mathbb{Z}\right) \\ &\cong \prod_{n \in \mathbb{N}} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) \\ &\cong 0 \end{aligned}$$

implies

$$\mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Q}, \bigoplus_{n \in \mathbb{N}} \mathbb{Z}\right) \cong 0.$$

Thus the only $\mathbb{Z}$-linear map from $\mathbb{Q}$ to $\bigoplus_{n \in \mathbb{N}} \mathbb{Z}$ is the zero map. □

11.5 Base Change

Proposition 11.5. *Let $R \to S$ be a flat ring map. If E is an injective S-module, then E is injective as an R-module.*

Proof. This is true because $\mathrm{Hom}_R(M, E) = \mathrm{Hom}_S(M \otimes_R S, E)$ and the fact that tensoring with S is exact. □

11.6 Local Criteria for Flatness

In this section we give criteria for flatness over local rings. We shall weaken the condition $\mathrm{Tor}_1^R(R/I, M) = 0$ for all $I \subset R$ to just $\mathrm{Tor}_1^R(R/\mathfrak{m}, M) = 0$ for $\mathfrak{m}$ the maximal ideal.

Proposition 11.6. *Let M be an R-module. The following conditions are equivalent:*

1. *M is a flat R-module.*

2. *$M_{\mathfrak{p}}$ is a flat $A_{\mathfrak{p}}$-module for all prime ideals $\mathfrak{p}$.*

3. *$M_{\mathfrak{m}}$ is a flat $A_{\mathfrak{m}}$-module for all maximal ideals $\mathfrak{m}$.*

Proof.

($1 \implies 2$): Let **A-Mod** denote the category of A-modules and let $\mathbf{A}_{\mathfrak{p}}$**-Mod** denote the category of $A_{\mathfrak{p}}$-modules. Then localization is full as a functor. In particular, every injective map of $A_{\mathfrak{p}}$-modules has the form $\varphi_{\mathfrak{p}} : N_{\mathfrak{p}} \to L_{\mathfrak{p}}$, where N and L are A-modules and φ is an injective map A-linear map from N to L. The map $i \otimes 1 : N \otimes_A M \to L \otimes_A M$ is also injective since M is flat as an A-module. Since localization is exact as a functor and commutes with tensor products, we have $i_{\mathfrak{p}} \otimes 1 : N_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} M_{\mathfrak{p}} \to L_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} M_{\mathfrak{p}}$ is an injective map of $A_{\mathfrak{p}}$-modules. Therefore $M_{\mathfrak{p}}$ is flat as an $A_{\mathfrak{p}}$-module.

($2 \implies 3$): Trivial.

($3 \implies 1$): Let φ denote the inclusion map $I \subset A$ be an ideal. We will show that $\operatorname{Ker}(1 \otimes \varphi) = 0$ by showing $\operatorname{Ker}(1 \otimes \varphi)_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m} \subset A$. Suppose $\mathfrak{m} \subset A$ is an arbitrary maximal ideal. By hypothesis, $M_{\mathfrak{m}}$ is a flat $A_{\mathfrak{m}}$-module. Since localization is exact as functor, the map $\varphi_{\mathfrak{m}} : I_{\mathfrak{m}} \subset A_{\mathfrak{m}}$ is injective, and since $M_{\mathfrak{m}}$ is flat as an $A_{\mathfrak{m}}$-module, the map $1 \otimes \varphi_{\mathfrak{m}} : I_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}} \to I_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}}$ is injective as well. Therefore

$$\begin{aligned} 0 &\cong \operatorname{Ker}(1 \otimes \varphi_{\mathfrak{m}}) \\ &= \operatorname{Ker}((1 \otimes \varphi)_{\mathfrak{m}}) \\ &= \operatorname{Ker}(1 \otimes \varphi)_{\mathfrak{m}}, \end{aligned}$$

which proves the claim. □

Theorem 11.4. *Let $(A, \mathfrak{m})$ and $(B, \mathfrak{n})$ be Noetherian local rings, B and A-algebra and $\mathfrak{m}B \subset \mathfrak{n}$. Let M be a finitely generated B-module. Then M is flat as an A-module if and only if $\operatorname{Tor}_1^A(A/\mathfrak{m}, M) = 0$.*

Proof. If M is flat as an A-module, then $\operatorname{Tor}_1^A(A/\mathfrak{m}, M) = 0$, by Theorem (11.1). Now assume that $\operatorname{Tor}_1^A(A/\mathfrak{m}, M) = 0$. Let $I \subset A$ be an ideal. We have to prove that $I \otimes_A M \to M$ is injective. We first claim that $\bigcap_{n=0}^{\infty} \mathfrak{m}^n \cdot (I \otimes_A M) = 0$. To see this, we consider $I \otimes_A M$ as a B-module via the B-module structure of M. It is finitely generated as a B-module, and therefore by Krull's Intersection Theorem, $\bigcap_{n=0}^{\infty} \mathfrak{n}^n \cdot (I \otimes_A M) = 0$. But $\mathfrak{m}B \subset \mathfrak{n}$ implies the claim.

Let $x \in \operatorname{Ker}(I \otimes_A M \to M)$. Then we will show that $x \in \bigcap_{n=0}^{\infty} \mathfrak{m}^n \cdot (I \otimes_A M)$ for all n. To prove this, we consider the map

$$(\mathfrak{m}^n I) \otimes_A M \to I \otimes_A M.$$

The image of this map is $\mathfrak{m}^n \cdot (I \otimes_A M)$. Using the lemma of Artin-Rees, we obtain an integer s such that $\mathfrak{m}^s \cap I \subset \mathfrak{m}^n I$. Therefore, it is enough to prove that x is in the image of

$$(\mathfrak{m}^n \cap I) \otimes_A M \to I \otimes_A M$$

for all n. From the exact sequence

$$(\mathfrak{m}^n \cap I) \otimes_A M \longrightarrow I \otimes_A M \longrightarrow (I/\mathfrak{m}^n \cap I) \otimes_A M \longrightarrow 0$$

we deduce that it is sufficient to see that x maps to 0 in $(I/\mathfrak{m}^n \cap I) \otimes_A M$. Consider the following commutative diagram:

$$\begin{tikzcd} I \otimes_A M \arrow[r, "\gamma"] \arrow[d, "\alpha"'] & (I/\mathfrak{m}^n \cap I) \otimes_A M \arrow[d, "\pi"] \\ M \arrow[r, "\beta"'] & (A/\mathfrak{m}^n) \otimes_A M \end{tikzcd}$$

We know that $\alpha(x) = 0$. Therefore, $\pi \circ \gamma(x) = 0$, and it is sufficient to prove that π is injective. To prove this, consider the following exact sequence

$$0 \longrightarrow I/(\mathfrak{m}^n \cap I) \longrightarrow A/\mathfrak{m}^n \longrightarrow A/(I + \mathfrak{m}^n) \longrightarrow 0$$

which induces an exact sequence

$$\operatorname{Tor}_1^A(A/(I + \mathfrak{m}^n), M) \longrightarrow (I/(\mathfrak{m}^n \cap I)) \otimes_A M \xrightarrow{\pi} (A/\mathfrak{m}^n) \otimes_A M.$$

We see that, finally, it suffices to prove that $\mathrm{Tor}_1^A(A/(I+\mathfrak{m}^n), M) = 0$. But $A/(I+\mathfrak{m}^n)$ is an A-module of finite length. Therefore, the following lemma proves the theorem. □

Lemma 11.5. *Let $(A,\mathfrak{m})$ be a local ring and M an A-module such that $Tor_1^A(A/\mathfrak{m}, M) = 0$. Then $Tor_1^A(P,M) = 0$ for all A-modules P of finite length.*

Proof. We use induction on the length. The case $\mathrm{length}(P) = 1$ is clear because it implies $P = A/\mathfrak{m}$. Let $N \subset P$ be a proper submodule, then we obtain the exact sequence

$$\begin{tikzcd} \mathrm{Tor}_1^A(N,M) \arrow[r] & \mathrm{Tor}_1^A(P,M) \arrow[r] & \mathrm{Tor}_1^A(P/N,M) \end{tikzcd}$$

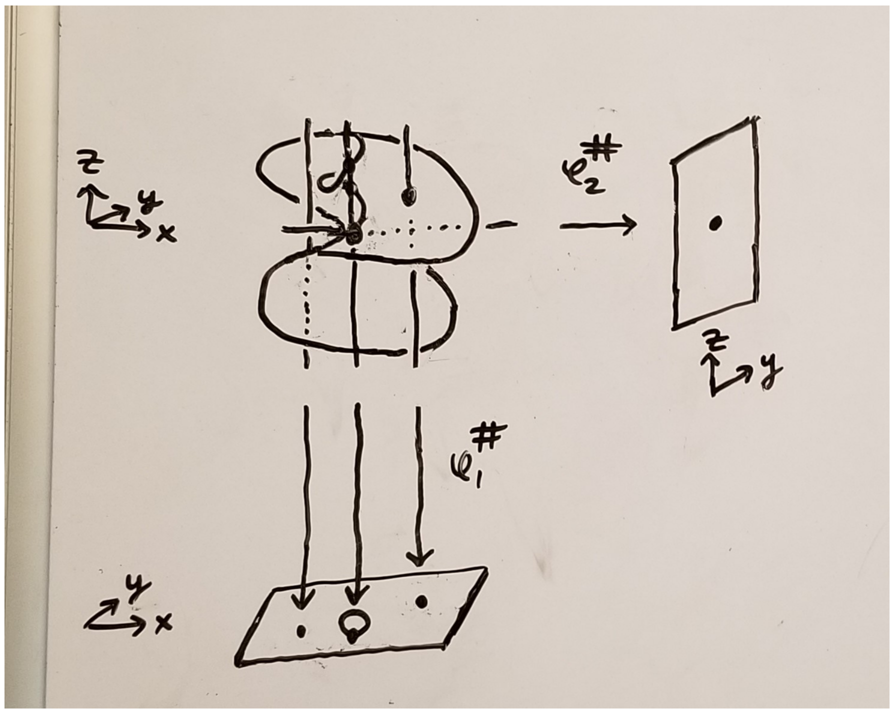
By the induction hypothesis, $\mathrm{Tor}_1^A(N,M) = 0$ and $\mathrm{Tor}_1^A(P/N,M) = 0$. This implies $\mathrm{Tor}_1^A(P,M) = 0$. □

11.7 Examples

Example 11.4. Let $A = K[x,y]$, $B = K[x,y,z]/\langle x - zy\rangle$, and $\varphi : A \to B$ be the map given by $\varphi(x) = x$ and $\varphi(y) = y$. Then $\mathrm{Spec}(A)$ corresponds tof the (x,y)-plane, and $\mathrm{Spec}(B)$ corresponds to the "blown up" (x,y)-plane. The map $\varphi : A \to B$, induces a map $\varphi^\# : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$. We calculate the inverse images of some points $\mathfrak{m}_{i,j} = \langle x - i, x - j\rangle$ in $\mathrm{Max}(A) \subset \mathrm{Spec}(A)$:

$$\left(\varphi^\#\right)^{-1}(\mathfrak{m}_{0,0}) = \langle x - zy, x, y\rangle = \langle x, y\rangle$$
$$\left(\varphi^\#\right)^{-1}(\mathfrak{m}_{1,0}) = \langle x - zy, x - 1, y\rangle = \langle 1\rangle = B$$
$$\left(\varphi^\#\right)^{-1}(\mathfrak{m}_{1,1}) = \langle x - zy, x - 1, y - 1\rangle = \langle x - 1, y - 1, z - 1\rangle$$

So there is one point which maps to $\mathfrak{m}_{1,1}$, no points which maps to $\mathfrak{m}_{1,0}$, and a whole line of points which maps to $\mathfrak{m}_{0,0}$.



On the other hand, if we let $A = K[y,z]$ and $\varphi : A \to B$ be the map given by $\varphi(y) = y$ and $\varphi(z) = z$, then it's easy to see φ is a ring isomorphism.

Example 11.5. Let $A = K[y]$, $B = K[x,y]/\langle xy\rangle$, and $\varphi : A \to B$ be the map given by $\varphi(y) = y$. Then

$$\left(\varphi^\#\right)^{-1}(\mathfrak{m}_0) = \langle xy, y\rangle = \langle y\rangle$$
$$\left(\varphi^\#\right)^{-1}(\mathfrak{m}_1) = \langle xy, y - 1\rangle = \langle x, y - 1\rangle$$

12 Projective Modules

Definition 12.1. Let P be an R-module. We say P is **projective** if for every surjective homomorphism $\varphi\colon M \to N$ and for every homomorphism $\psi\colon P \to N$ there exists a homomorphism $\widetilde{\psi}\colon P \to M$ such that $\varphi \circ \widetilde{\psi} = \psi$. We illustrate this with the following diagram:

$$\begin{tikzcd}
 & P \arrow[dl, dashed, "\widetilde{\psi}"'] \arrow[d, "\psi"] \\
M \arrow[r, two heads, "\varphi"'] & N
\end{tikzcd}$$

An equivalent definition of being injective is given in the following proposition:

Proposition 12.1. *Let E be an R-module. Then E is projective if and only if the covariant functor $Hom_R(P, -)$ is exact.*

12.1 Properties of Projective Modules

12.1.1 Free Modules are Projective

Proposition 12.2. *Every free R-module is projective.*

Proof. Let F be a free R-module, let $\varphi\colon M \to N$ be a surjective R-module homomorphism, and let $\psi\colon F \to N$ be any R-module homomorphism. Let $\{e_i\}_{i\in I}$ be a basis for F as a free R-module. For each $i \in I$, we choose a $u_i \in M$ such that $\varphi(u_i) = \psi(e_i)$ (such a choice is possible as φ is surjective). We define $\widetilde{\psi}\colon F \to M$ to be the unique R-module homomorphism such that

$$\widetilde{\psi}(e_i) = u_i$$

for all $i \in I$. Then for all $i \in I$, we have

$$\begin{aligned}
(\varphi \circ \widetilde{\psi})(e_i) &= \varphi(\widetilde{\psi}(e_i)) \\
&= \varphi(u_i) \\
&= \psi(e_i).
\end{aligned}$$

It follows that $\varphi \circ \widetilde{\psi} = \psi$. □

12.1.2 Equivalent Conditions for being Projective

Proposition 12.3. *Let P be an R-module. The following statements are equivalent.*

1. *P is projective.*
2. *Every short exact sequence of the form*

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "\psi"] & N \arrow[r, "\varphi"] & P \arrow[r] & 0
\end{tikzcd} \tag{48}$$

   is split exact.
3. *P is a direct summand of a free R-module.*

Proof. We first show 1 implies 2. Suppose P is projective. Then there exists an R-linear map $\widetilde{\psi}\colon P \to M$ such that $\varphi \circ \widetilde{\psi} = 1_P$. In other words, $\widetilde{\psi}$ splits (48).

Next we show 2 implies 3. Suppose every short exact sequence of the form (48) is split exact. Let $\varphi\colon F \to P$ be a surjective R-linear map from a free module F to P and let K denote the kernel of this map. For instance, F could be the free module with generators δ_u for all $u \in P$, and $\varphi\colon F \to P$ could be the unique R-linear map given by $\varphi(\delta_u) = u$ for all $u \in P$. Then we have a short exact sequence

$$\begin{tikzcd}
0 \arrow[r] & K \arrow[r] & F \arrow[r] & P \arrow[r] & 0
\end{tikzcd}$$

.This short exact sequence splits by assumption, and thus we have $F \cong K \oplus P$. In other words, P is a direct summand of a free R-module.

Finally we show 3 implies 1. Suppose P is a direct summan of a free R-module, say $P \oplus K \cong F$ where F is free and K is some other R-module. Let $\pi_1\colon F \to P$ be the projection map, given by

$$\pi_1(u, v) = u$$

for all $(u, v) \in F$ and let $\iota_1 \colon P \to F$ be the inclusion map, given by

$$\iota_1(u) = (u, 0)$$

for all $u \in P$. Now we want to show that P is projective, so let $\varphi \colon M \to N$ be a surjective R-linear map and let $\psi \colon P \to N$ be any other R-linear map. Since F is free, it is also projective, and so there exists an R-linear map $\phi \colon F \to M$ such that $\varphi \circ \phi = \psi \circ \pi_1$. Define $\widetilde{\psi} \colon P \to M$ by $\widetilde{\psi} = \phi \circ \iota_1$. Then

$$\begin{aligned} \varphi \circ \widetilde{\psi} &= \varphi \circ \phi \circ \iota_1 \\ &= \psi \circ \pi_1 \circ \iota_1 \\ &= \psi \circ 1_P \\ &= \psi. \end{aligned}$$

Thus P is projective. □

12.1.3 Projective Modules over Local Ring are Free

Lemma 12.1. *Every projective R-module is free if and only if every countably generated projective R-module is free.*

Lemma 12.2. *Let M be a countably generated R-module. Suppose any direct summand N of M satisfies the following property: any element of N is contained in a free direct summand of N. Then M is free.*

Proof. Let (u_n) be a countable sequence of generators for M. Note that M is a direct summand of itself. Since $u_1 \in M$, we see that it is contained in a free direct summand of M, say F_1. Write

$$M = F_1 \oplus M_1.$$

Next, M_1 is a direct summand of M. If $M_1 = 0$, then $M = F_1$ and we are done, so (by reindexing if necessary) we may assume that $u_2 \notin F_1$. Then $u_2 \in M_1$, and so it is contained in a free direct summand of M_1, say F_2. Write

$$\begin{aligned} M &= F_1 \oplus M_1 \\ &= F_1 \oplus F_2 \oplus M_2. \end{aligned}$$

Continuining in this manner, we construct a sequence of free R-modules (F_n) such that $u_n \in F_n$ for all n. In particular, we have

$$M = \bigoplus_{n=1}^{\infty} F_n.$$

Therefore F is free. □

Lemma 12.3. *Let $A = (a_{i,j})$ be an $n \times n$ matrix over a local ring $(R, \mathfrak{m})$. If $a_{i,i}$ is a unit for all i and $a_{i,j}$ is a nonunit for all $i \neq j$, then* $\det A$ *is a unit.*

Proof. The Leibniz formula for the determinant of A is given by

$$\det A = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}.$$

Observe that if $\sigma \neq 1$, then $\prod_{i=1}^{n} a_{i,\sigma(i)} \in \mathfrak{m}$. Indeed, there exists some i such that $\sigma(i) \neq i$, and thus $a_{i,\sigma(i)} \in \mathfrak{m}$ which implies the product belongs to $\mathfrak{m}$ too. On the other hand, $\prod_{i=1}^{n} a_{i,i} \in R \backslash \mathfrak{m}$ since $R \backslash \mathfrak{m}$ is multiplicatively closed. Therefore we can express $\det A$ as a unit plus a nontunit. This implies $\det A$ is a unit. □

Lemma 12.4. *Let P be a projective module over a local ring R. Then any element of P is contained in a free direct summand of P.*

Proof. Since P is projective, it is a direct summand of some free R-module, say $F = P \oplus Q$. Let $x \in P$ be the element we wish to show is contained in a free direct summand of P. Let B be a basis of F such that the number of basis elements needed in the expression of x is minimal, say

$$x = \sum_{i=1}^{n} a_i e_i$$

for some $e_i \in B$ and $a_i \in R$. Then no a_j can be expressed as a linear combination of the other a_i. Indeed, if

$$a_j = \sum_{i \neq j} a_i b_i$$

for some $b_i \in R$, then replacing e_i by $e_i + b_ie_j$ for $i \neq j$ and leaving unchanged the other elements of B, we get a new basis for F in terms of which

$$\begin{aligned} x &= \sum_{i=1}^{n} a_ie_i \\ &= \sum_{i\neq j} a_ie_i + a_je_j \\ &= \sum_{i\neq j} a_ie_i + \left(\sum_{i\neq j} a_ib_i\right) e_j \\ &= \sum_{i\neq j} a_i(e_i + b_ie_j) \end{aligned}$$

has a shorter expression.

For each i we decompose e_i into its P and Q-components, say

$$e_i = y_i + z_i$$

where $y_i \in P$ and $z_i \in Q$. Write

$$y_i = \sum_{j=1}^{n} b_{ij}e_j + t_i \tag{49}$$

where t_i is a linear combination of elements in B other than $e_1, \dots, e_n$. To finish the proof it suffices to show that the matrix (b_{ij}) is invertible. For then the map $F \to F$ sending $e_i \mapsto y_i$ for $i = 1, \dots, n$ and fixing $B \backslash \{e_1, \dots, e_n\}$ is an isomorphism, so that $y_1, \dots, y_n$ together with $B \backslash \{e_1, \dots, e_n\}$ form a basis for F. Then the submodule N spanned by $y_1, \dots, y_n$ is a free submodule of P. Furthermore N is a direct summand of P since $N \subseteq P$ and both N and P are direct summands of F. Also $x \in N$ since $x \in P$ implies

$$\begin{aligned} x &= \sum_{i=1}^{n} a_ie_i \\ &= \sum_{i=1}^{n} a_iy_i \end{aligned}$$

So N is a free direct summand of P which contains x.

Now we prove that (b_{ij}) is invertible. Plugging (49) into

$$\sum_{i=1}^{n} a_ie_i = \sum_{i=1}^{n} a_iy_i$$

and equating coefficients gives us

$$a_j = \sum_{i=1}^{n} a_ib_{ij}.$$

But as noted above, our choice of B guarantees that no a_j can be written as a linear combination of the other a_i. Thus b_{ij} is a nonunit for $i \neq j$, and $1 - b_{ii}$ is a nonunit, so in particular b_{ii} is a unit for all i. But a matrix over a local ring having units along the diagonal and nonunits elsewhere is invertible, as its determinant is a unit. □

Theorem 12.5. *If P is a projective module over a local ring, then P is free.*

12.1.4 Local Conditions for being Projective

Proposition 12.4. *Let P be a finitely presented R-module. The following are equivalent.*

1. *P is a projective R-module.*

2. *$P_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$-module for all prime ideals $\mathfrak{p}$ in R.*

3. *$P_{\mathfrak{m}}$ is a free $R_{\mathfrak{m}}$-module for all maximal ideals $\mathfrak{m}$ in R.*

Furthermore, if R is Noetherian, then these statements are also equivalent to

4. *there is a finite set of elements $a_1, \dots, a_n \in R$ that generate the unit ideal of R such that P_{a_i} is a free R_{a_i}-module for all i.*

Proof. We first show 1 implies 2. Suppose P is a projective R-module and let $\mathfrak{m}$ be a maximal ideal. Since P is projective, it is a direct summand of a free R-module, say

$$F = P \oplus Q.$$

Since localization commutes with direct sums, this implies

$$F_{\mathfrak{p}} = P_{\mathfrak{p}} \oplus Q_{\mathfrak{p}}.$$

Thus $P_{\mathfrak{p}}$ is a direct summand of a free $R_{\mathfrak{p}}$-module. This implies $P_{\mathfrak{p}}$ is a projective $R_{\mathfrak{p}}$-module. Since projective modules over local rings are free, we see that $P_{\mathfrak{p}}$ is free.

That 2 implies 3 is clear, so we just need to show that 3 implies 1. Suppose $P_{\mathfrak{m}}$ is a free R-module for all maximal ideals $\mathfrak{m}$ in R. To show that P is projective, we need to show that for any surjective R-linear map $\varphi \colon M \to N$, then induced R-linear map

$$\mathrm{Hom}_R(P,\varphi)\colon \mathrm{Hom}_R(P,M) \to \mathrm{Hom}_R(P,N)$$

is also surjective, so let $\varphi \colon M \to N$ be a surjective R-linear map. Then observe that

$$\begin{aligned}
\mathrm{Hom}_R(P,\varphi) \text{ is surjective} &\iff \mathrm{Hom}_R(P,N)/\mathrm{Hom}_R(P,M) \cong 0 \\
&\iff (\mathrm{Hom}_R(P,N)/\mathrm{Hom}_R(P,M))_{\mathfrak{m}} \cong 0 \text{ for all maximal ideals } \mathfrak{m} \subseteq R \\
&\iff \mathrm{Hom}_R(P,N)_{\mathfrak{m}}/\mathrm{Hom}_R(P,M)_{\mathfrak{m}} \cong 0 \text{ for all maximal ideals } \mathfrak{m} \subseteq R \\
&\iff \mathrm{Hom}_{R_{\mathfrak{m}}}(P_{\mathfrak{m}},N_{\mathfrak{m}})/\mathrm{Hom}_{R_{\mathfrak{m}}}(P_{\mathfrak{m}},M_{\mathfrak{m}}) \cong 0 \text{ for all maximal ideals } \mathfrak{m} \subseteq R \\
&\iff \mathrm{Hom}_{R_{\mathfrak{m}}}(P_{\mathfrak{m}},\varphi_{\mathfrak{m}}) \text{ is surjective for all maximal ideals } \mathfrak{m} \subseteq R
\end{aligned}$$

where the last if and only if is true since $P_{\mathfrak{m}}$ is free (and hence projective) for all maximal ideals $\mathfrak{m} \subseteq R$.

Now we show 4 is equivalent to 1,2, and 3 when R is Noetherian. Suppose R is Noetherian. Then since P is finite and R is Noetherian, we see that $\operatorname{supp} P$ is finite, say

$$\operatorname{supp} P = \{\mathfrak{p}_1, \dots, \mathfrak{p}_m\}.$$

In particular, statement 2 is equivalent to $P_{\mathfrak{p}_i}$ being a free $R_{\mathfrak{p}_i}$-module for all $1 \leq i \leq m$.

□

12.2 Projective Dimension

Definition 12.2. Let A be a ring and M a finitely generated A-module. A **free resolution** of M is an exact sequence

$$\cdots \longrightarrow F_{k+1} \xrightarrow{\varphi_{k+1}} F_k \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \tag{50}$$

with finitely generated free A-modules F_i for $i \geq 0$. We say that a free resolution has **length** n if $F_k = 0$ for all $k > n$ and n is minimal with this property.

If $(A,\mathfrak{m})$ is a local ring, then a free resolution as above is called **minimal** if $\varphi_k(F_k) \subset \mathfrak{m}F_{k-1}$ for $k \geq 1$, and then $b_k(M) := \mathrm{rank}(F_k)$, $k \geq 0$, is called the kth **Betti number** of M.

Remark. What does the condition $\varphi_k(F_k) \subset \mathfrak{m}F_{k-1}$ have to do with being minimal? Let $K_i := \mathrm{Ker}(\varphi_i)$. Then (50) breaks up into exact sequences of the form

$$F_k \xrightarrow{\varphi_k} F_{k-1} \longrightarrow K_{k-2} \longrightarrow 0 \tag{51}$$

Tensoring (51) with $A/\mathfrak{m}$ gives us

$$F_k/\mathfrak{m}F_k \xrightarrow{\bar{\varphi}_k} F_{k-1}/\mathfrak{m}F_{k-1} \longrightarrow K_{k-2}/\mathfrak{m}K_{k-2} \longrightarrow 0 \tag{52}$$

The condition $\varphi_k(F_k) \subset \mathfrak{m}F_{k-1}$ forces $\dim_{A/\mathfrak{m}}(F_{k-1}/\mathfrak{m}F_{k-1}) = \dim_{A/\mathfrak{m}}(K_{k-2}/\mathfrak{m}K_{k-2}) = b_{k-1}(M)$. Applying Nakayama's lemma shows that $b_{k-1}(M)$ is the minimal number of generators of K_{k-2}.

Theorem 12.6. *Let $(A,\mathfrak{m})$ be a local Noetherian ring and M a finitely generated A-module, then M has a minimal free resolution. The rank of F_k in a minimal free resolution is independent of the resolution. If M has a minimal resolution of finite length n,*

$$0 \longrightarrow F_n \longrightarrow F_{n-1} \longrightarrow \cdots \longrightarrow F_0 \longrightarrow M \longrightarrow 0 \tag{53}$$

and if

$$0 \longrightarrow G_m \longrightarrow G_{m-1} \longrightarrow \cdots \longrightarrow G_0 \longrightarrow M \longrightarrow 0 \tag{54}$$

is any free resolution, then $m \geq n$.

Proof. Let $u_1, \dots, u_{s_0}$ be a minimal set of generators of M and consider the surjective map $\varphi_0 \colon F_0 := R^{s_0} \to M$ defined by

$$\varphi_0(a_1, \dots, a_{s_0}) = \sum_{i=1}^{s_0} a_i u_i$$

for all $(a_1, \dots, a_{s_0}) \in F_0$. Because of Nakayama's Lemma, $u_1, \dots, u_{s_0}$ induces a basis of the vector space $M/\mathfrak{m}M$, and hence φ_0 induces an isomorphism $\overline{\varphi}_0 : F_0/\mathfrak{m}F_0 \cong M/\mathfrak{m}M$. In particular, this implies $\ker\varphi_0 \subset \mathfrak{m}F_0$. Observe that $\ker\varphi_0$ is a submodule of a finitely generated module over a Noetherian ring, hence is finitely generated. As before, we can find a surjective map $\varphi_1 \colon F_1 := R^{s_1} \to K_1$, where s_1 is the minimal number of generators of K_1. Continuing in this manner, we obtain a minimal free resolution for M. To show the invariance of the Betti numbers, we consider two minimal resolutions of M:

$$\cdots \xrightarrow{\varphi_{n+1}} F_n \longrightarrow \cdots \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0 \tag{55}$$

and

$$\cdots \xrightarrow{\psi_{n+1}} G_n \longrightarrow \cdots \xrightarrow{\psi_1} G_0 \xrightarrow{\psi_0} M \longrightarrow 0 \tag{56}$$

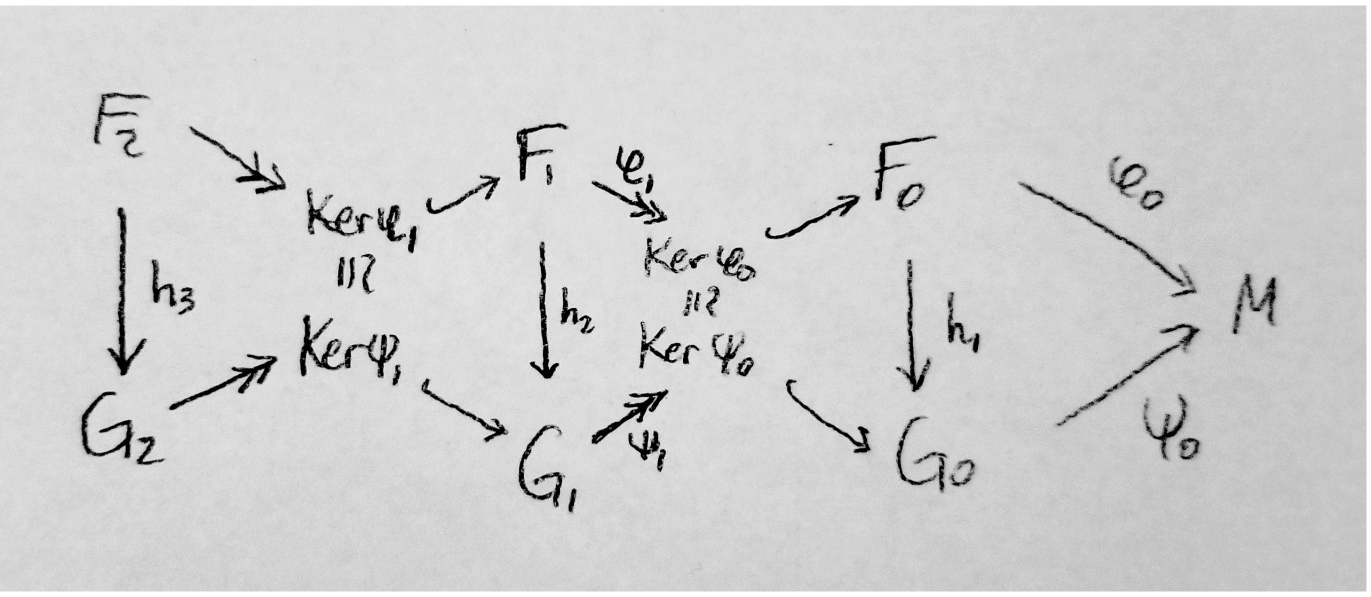
We have

$$F_0/\mathfrak{m}F_0 \cong M/\mathfrak{m}M \cong G_0/\mathfrak{m}G_0$$

and therefore $\operatorname{rank}(F_0) = \operatorname{rank}(G_0)$. Let $\{f_1, \dots, f_{s_0}\}$, respectively $\{g_1, \dots, g_{s_0}\}$ be bases of F_0, respectively G_0. As $\{\psi_0(g_i)\}$ generates M, we have

$$\varphi_0(f_i) = \sum_j a_{ij} \cdot \psi_0(g_j)$$

for some $a_{ij} \in R$. The matrix (a_{ij}) defines a map $\alpha_1 \colon F_0 \to G_0$ such that $\psi_0 \circ \alpha_1 = \varphi_0$. The induced map $\overline{\alpha}_1 : F_0/\mathfrak{m}F_0 \to G_0/\mathfrak{m}G_0$ is an isomorphism since it is a composition of isomorpisms: $\overline{\alpha}_1 = \overline{\psi}_0^{-1} \circ \overline{\varphi}_0$. In particular, we derive that $\det(a_{ij}) \neq 0 \bmod \mathfrak{m}$. This implies that $\det(a_{ij})$ is a unit in R (R is local ring) and α_1 is an isomorphism. Especially, α_1 induces an isomorphism $\ker\varphi_0 \to \ker\psi_0$. As φ_1 and ψ_1, considered as matrices, have entries in $\mathfrak{m}$, and since we have surjections $F_1 \to \ker\varphi_0$ and $G_1 \to \ker\varphi_0$, it follows, as before, that $\operatorname{rank}(F_1) = \operatorname{rank}(G_1)$. Now we can continue like this and obtain the invariance of the Betti numbers.



To prove the last statement, let

$$0 \longrightarrow F_n \longrightarrow F_{n-1} \longrightarrow \cdots \longrightarrow F_0 \longrightarrow M \longrightarrow 0 \tag{57}$$

be a minimal free resolution with $F_n \neq \langle 0 \rangle$ and

$$0 \longrightarrow G_m \longrightarrow G_{m-1} \longrightarrow \cdots \longrightarrow G_0 \longrightarrow M \longrightarrow 0 \tag{58}$$

be any free resolution. We have to prove that $m \geq n$. This can be proved in a similar way to the previous step. With the same idea, one can prove that there are injections $h_i : F_i \to G_i$ for all $i \leq n$. □

Definition 12.3. A **syzygy** between k elements $f_1, \dots, f_k$ of an A-module M is a k-tuple $(g_1, \dots, g_k) \in A^k$ satisfying

$$\sum_{i=1}^{k} g_i f_i = 0.$$

The set of syzygies between $f_1, \dots, f_k$ is a submodule of A^k. Indeed, it is the kernel of the ring homomorphism

$$\varphi : F_1 := \bigoplus_{i=1}^{k} A e_i \to M, \quad e_i \mapsto f_i,$$

where $\{e_1, \dots, e_k\}$ denotes the canonical basis of A^k. The map φ surjects onto the A-module $I := \langle f_1, \dots, f_k \rangle_A$ and

$$\mathrm{syz}(I) := \mathrm{syz}(f_1, \dots, f_k) := \mathrm{Ker}(\varphi)$$

is called the **module of syzygies** of I with respect to the generators $f_1, \dots, f_k$.

Example 12.1. Let $A = K[x, y, z, w]$ and let

$$\begin{aligned} f_1 &= xz - y^2 \\ f_2 &= yw - z^2 \\ f_3 &= xw - yz. \end{aligned}$$

There are three "trivial" syzygies of f_1, f_2 and f_3, which are given by the 3-tuples

$$\begin{aligned} m_1 &= (f_2, -f_1, 0), \\ m_2 &= (f_3, 0, -f_1), \\ m_3 &= (0, f_3, -f_2), \end{aligned}$$

but $\mathrm{syz}(f_1, f_2, f_3)$ is not generated by them. A generating set for $\mathrm{syz}(f_1, f_2, f_3)$ is given by the 3-tuples

$$\begin{aligned} n_1 &= (w, y, -z) \\ n_2 &= (z, x, -y), \end{aligned}$$

Note that

$$\begin{aligned} f_1 &= yn_1 - zn_2, \\ f_2 &= xn_1 - yn_2, \\ f_3 &= -zn_1 + wn_2. \end{aligned}$$

Remark. Let A be a Noetherian local ring. If $I = \langle f_1, \dots, f_k \rangle = \langle g_1, \dots, g_s \rangle \subset A^r$, then it is not necessarily true that $\mathrm{syz}(f_1, \dots, f_k) \cong \mathrm{syz}(g_1, \dots, g_s)$. So why are we justified in writing $\mathrm{syz}(I)$. The reason is because the modules $\mathrm{syz}(f_1, \dots, f_k)$ and $\mathrm{syz}(g_1, \dots, g_s)$ are **projectively equivalent**. This means that $\mathrm{syz}(f_1, \dots, f_k) \oplus A^m \cong A^n \oplus \mathrm{syz}(g_1, \dots, g_s)$ for some free A-modules A^m and A^n. To prove this, we first need a lemma.

Lemma 12.7. *(Schanuel's Lemma) Let A be a Noetherian ring and M a finitely generated A-module. Moreover, assume that the following sequences are exact*

$$\begin{tikzcd} 0 \arrow[r] & K_1 \arrow[r] & A^{n_1} \arrow[r, "\pi_1"] & M \arrow[r] & 0 \end{tikzcd}$$

$$\begin{tikzcd} 0 \arrow[r] & K_2 \arrow[r] & A^{n_2} \arrow[r, "\pi_2"] & M \arrow[r] & 0 \end{tikzcd}$$

Then $K_1 \oplus A^{n_2} \cong K_2 \oplus A^{n_1}$.

Proof. Consider the A-module homomorphism $\pi \colon A^{n_1} \oplus A^{n_2} \to M$, given by $\pi(a, b) = \pi_1(a) + \pi_2(b)$. We will show that $\mathrm{Ker}(\pi) \cong A^{n_1} \oplus K_2$. A similar proof will show that $\mathrm{Ker}(\pi) \cong K_1 \oplus A^{n_2}$, and hence

$$A^{n_1} \oplus K_2 \cong \mathrm{Ker}(\pi) \cong K_1 \oplus A^{n_2}.$$

Let $e_1, \dots, e_{n_1}$ be a basis for A^{n_1} and let $f_1, \dots, f_{n_2}$ be a basis for A^{n_2}. Since π_2 is surjective, there exists $a_{ij} \in A$ such that

$$\pi_1(e_i) = \sum_{j=1}^{n_2} a_{ij} \pi_2(f_j).$$

for all $i = 1, \dots, n_1$. Choose such a_{ij} and let $\varphi \colon A^{n_1} \to A^{n_2}$ be the unique A-module homomorphism such that

$$\varphi(e_i) = \sum_{j=1}^{n_2} a_{ij} f_j$$

for all $i = 1, \dots, n_1$. Then $\pi_2 \circ \varphi = \pi_1$ and the set

$$F := \{(x, -\varphi(x)) \mid x \in A^{n_1}\}$$

is an A-module which is isomorphic to A^{n_1}. Viewing K_2 as

$$K_2 = \{(0, y) \mid y \in K_2\},$$

we see that $F \cap K_2 = \{(0,0)\}$, so the sum $F + K_2$ is a direct sum $F \oplus K_2$. Now suppose $(x, y) \in \mathrm{Ker}(\pi)$. Then

$$\begin{aligned} 0 &= \pi_1(x) + \pi_2(y) \\ &= (\pi_2 \circ \varphi)(x) + \pi_2(y) \\ &= \pi_2(\varphi(x)) + \pi_2(y) \\ &= \pi_2(\varphi(x) + y), \end{aligned}$$

implies $\varphi(x) + y \in \mathrm{Ker}(\pi_2)$. Moreover, we can write

$$(x, y) = (x, -\varphi(x)) + (0, \varphi(x) + y) \in F \oplus K_2 \cong A^{n_1} \oplus K_2.$$

Therefore $\mathrm{Ker}(\pi) \subseteq M \oplus K_2 \cong A^{n_1} \oplus K_2$. Conversely, suppose $(x, -\varphi(x)) + (0, y) \in M \oplus K_2$. Applying π to $(x, -\varphi(x)) + (0, y)$, we have

$$\begin{aligned} \pi((x, -\varphi(x)) + (0, y)) &= \pi((x, y - \varphi(x)) \\ &= \pi_1(x) + \pi_2(y) - \pi_2(\varphi(x)) \\ &= \pi_1(x) - \pi_1(x) \\ &= 0. \end{aligned}$$

Therefore, $A^{n_1} \oplus K_2 \cong M \oplus K_2 \subseteq \mathrm{Ker}(\pi)$. We conclude that $\mathrm{Ker}(\pi) \cong A^{n_1} \oplus K_2$. □

Corollary. *Let A be a Noetherian ring and $M = \langle f_1, \dots, f_k \rangle = \langle g_1, \dots, g_s \rangle \subset A^r$. Then $syz(f_1, \dots, f_k) \oplus A^s \cong A^r \oplus syz(g_1, \dots, g_s)$.*

12.2.1 Schanuel's Lemma

Lemma 12.8. *(Schanuel's Lemma) Let*

$$\begin{tikzcd} 0 \arrow[r] & K \arrow[r, "\iota"] & P \arrow[r, "\pi"] & M \arrow[r] & 0 \end{tikzcd}$$

and

$$\begin{tikzcd} 0 \arrow[r] & K' \arrow[r, "\iota'"] & P' \arrow[r, "\pi'"] & M \arrow[r] & 0 \end{tikzcd}$$

be two short exact sequences of R-modules where P and P' are projective R-modules. Then there is an isomorphism

$$K \oplus P' \cong K' \oplus P.$$

Proof. Consider the diagram with exact rows

$$\begin{tikzcd} 0 \arrow[r] & K \arrow[r, "\iota"] \arrow[d, dashed, "\alpha"] & P \arrow[r, "\pi"] \arrow[d, dashed, "\beta"] & M \arrow[r] \arrow[d, "1_M"] & 0 \\ 0 \arrow[r] & K' \arrow[r, "\iota'"] & P' \arrow[r, "\pi'"] & M \arrow[r] & 0 \end{tikzcd}$$

Since P is projective, there is a map $\beta \colon P \to P'$ with $\pi' \beta = \pi$; that it, the right square in the diagram commutes. A diagram chase shows that there is a map $\alpha \colon K \to K'$ making the other square commute. This commutative diagram with exact rows gives an exact sequence

$$0 \to K \xrightarrow{\theta} P \oplus K' \xrightarrow{\psi} P' \to 0$$

where $\theta \colon x \mapsto (\iota x, \alpha x)$ and $\psi \colon (u, x') \mapsto \beta u - \iota' x'$ for $x \in K$, $u \in P$, and $x' \in K'$. Exactness of this sequence is a straightforward calculation. This sequence splits because P' is projective. □

13 Associated Primes and Primary Decomposition

13.1 Radicals and Colon Ideals

13.1.1 Radical of an Ideal

Definition 13.1. Let A be a ring and let $\mathfrak{a}$ be an ideal in A. The **radical of** $\mathfrak{a}$, denoted $\sqrt{\mathfrak{a}}$, is defined to be the ideal

$$\sqrt{\mathfrak{a}} := \{a \in A \mid a^n \in I \text{ for some } n \in \mathbb{N}\}.$$

We call $\sqrt{\langle 0 \rangle}$ the **nilradical of** A.

Proposition 13.1. *Let A be a ring and let $\mathfrak{a}$ be an ideal in A. Then*

$$\sqrt{\mathfrak{a}} = \bigcap_{\substack{\mathfrak{p} \supset \mathfrak{a} \\ \textit{prime}}} \mathfrak{p}.$$

Proof. We claim that $\mathfrak{p} \supset \mathfrak{a}$ implies $\mathfrak{p} \supset \sqrt{\mathfrak{a}}$. Indeed, if $x \in \sqrt{\mathfrak{a}}$, then $x^n \in \mathfrak{a} \subset \mathfrak{p}$. But this implies $x \in \mathfrak{p}$ since $\mathfrak{p}$ is prime. Thus, we have

$$\sqrt{\mathfrak{a}} \subset \bigcap_{\substack{\mathfrak{p} \supset \mathfrak{a} \\ \text{prime}}} \mathfrak{p}.$$

For the reverse inclusion, we may assume that $\mathfrak{a} = 0$ by passing to the quotient $A/\mathfrak{a}$. Suppose that $x \in \bigcap_{\text{prime}} \mathfrak{p}$ but $x^n \neq 0$ for all $n \geq 0$. Then $A[x^{-1}]$ is nonzero and hence contains a prime ideal $\mathfrak{q}$. The preimage of $\mathfrak{q}$ in A under the natural inclusion $A \to A[x^{-1}]$ is a prime ideal which doesn't contain x. This is a contradiction. □

Proposition 13.2. *Let A be a ring and let I, J be ideals in A. Then*

1. *$\sqrt{I}$ is an ideal.*
2. *If $I \subset J$, then $\sqrt{I} \subset \sqrt{J}$.*
3. *$\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.*
4. *$\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$.*

Proof.

1. Suppose $a \in A$ and $x, y \in \sqrt{I}$, so $x^n, y^m \in I$ for some $n, m \in \mathbb{N}$. Then

$$(ax + y)^{n+m} = \sum_{i=0}^{n+m} (ax)^{n+m-i} y^i. \tag{59}$$

   Each term in (59) belongs to I, so $(ax + y)^{n+m}$ belongs to I. Therefore $ax + y$ belongs to $\sqrt{I}$.

2. Suppose $a \in \sqrt{I}$, then for some $n \in \mathbb{N}$, we have $a^n \in I \subset J$, thus $a \in \sqrt{J}$.

3. Suppose $a \in \sqrt{I \cap J}$, so $a^n \in I \cap J$ for some $n \in \mathbb{N}$. Since $a^n \in I \cap J \subset I$ and $a^n \in I \cap J \subset J$, we have $a \in \sqrt{I}$ and $a \in \sqrt{J}$. Therefore $\sqrt{I \cap J} \subset \sqrt{I} \cap \sqrt{J}$. For the reverse inclusion, suppose $a \in \sqrt{I} \cap \sqrt{J}$, so $a^n \in I$ and $a^m \in J$ for some $n, m \in \mathbb{N}$. Then $a^{\max(m,n)} \in I \cap J$ implies $a \in \sqrt{I \cap J}$. Therefore $\sqrt{I \cap J} \supset \sqrt{I} \cap \sqrt{J}$.

4. The inclusion $\sqrt{I + J} \subset \sqrt{\sqrt{I} + \sqrt{J}}$ follows from the fact that $I + J \subset \sqrt{I} + \sqrt{J}$. For the reverse inclusion, suppose $a \in \sqrt{\sqrt{I} + \sqrt{J}}$. Then $a^n = b + c$, where $b^m \in I$ and $c^k \in J$ for some $n, m, k \in \mathbb{N}$. Then $(a^n)^{(m+k)} \in I + J$, and it follows that $a \in \sqrt{I + J}$. Thus $\sqrt{I + J} \supset \sqrt{\sqrt{I} + \sqrt{J}}$.

□

Remark. Note that we do not necessarily have $\sqrt{\bigcap_{\lambda\in\Lambda} I_\lambda} = \bigcap_{\lambda\in\Lambda}\sqrt{I_\lambda}$. Indeed, consider $I_n = \langle T^n\rangle$ in $K[T]$. Then

$$\begin{aligned}\sqrt{\bigcap_{n=1}^{\infty}\langle T^n\rangle} &= \sqrt{0}\\ &= 0\\ &\neq \langle T\rangle.\\ &= \bigcap_{n=1}^{\infty}\langle T\rangle\\ &= \bigcap_{n=1}^{\infty}\sqrt{\langle T^n\rangle}.\end{aligned}$$

13.1.2 Colon Ideal

Definition 13.2. Let A be a ring and let I, J be ideals in A. The **colon ideal** $I : J$ is defined as:

$$I : J = \{a \in A \mid aJ \subseteq I\}$$

Remark. Given $a \in A$, we use the shorthand notation $I : a$ for $I : \langle a\rangle$.

Proposition 13.3. *Let A be a ring, $a, b \in A$, d be a nonzerodivisor in A, and let I, J be ideals in A. Then*

1. $(I \cap J) : a = (I : a) \cap (J : a)$,
2. $I : \langle a, b\rangle = (I : a) \cap (I : b)$,
3. $I : d = \frac{1}{d}(I \cap \langle d\rangle)$.

Proof.

1. Suppose $x \in (I \cap J) : a$, so $ax \in I \cap J$. Since $I \cap J \subset I$ and $I \cap J \subset J$, this implies $x \in I : a$ and $x \in J : a$. Therefore $(I \cap J) : f \subset (I : f) \cap (J : f)$. Now suppose $x \in (I : a) \cap (J : a)$, then $ax \in I$ and $ax \in J$, so $x \in (I \cap J) : a$, which means $(I \cap J) : f \supset (I : f) \cap (J : f)$.
2. If $x \in A$, then $x\langle a, b\rangle \subset I$ if and only if $xa \in I$ and $xb \in I$.
3. Omitted.

□

Lemma 13.1. *Let A be a ring and I_1, I_2, I_3 be ideals in A.*

1. $(I_1 \cap I_2) : I_3 = (I_1 : I_3) \cap (I_2 : I_3)$, *in particular* $I_1 : I_3 = (I_1 \cap I_2) : I_3$ *if* $I_3 \subset I_2$.
2. $(I_1 : I_2) : I_3 = I_1 : (I_2 I_3)$.
3. *If I_1 is prime and $I_2 \not\subset I_1$, then $I_1 : I_2^j = I_1$ for $j \geq 1$.*
4. *If $I_1 = \bigcap_{i=1}^r \mathfrak{p}_i$ with $\mathfrak{p}_i$ prime, then $I_1 : I_2^\infty = I_1 : I_2 = \bigcap_{I_2 \not\subset \mathfrak{p}_i} \mathfrak{p}_i$.*

Proof.

1. Is an easy exercise
2. $I_1 \subset I_1 : I_2^j$ is clear. Let $gI_2^j \subset I_1$. Since $I_2 \not\subset I_1$ and I_1 is radical, $I_2^j \not\subset I_1$ and we can find an $h \in I_2^j$ such that $h \notin I_1$ and $gh \in I_1$. Since I_1 is prime, we have $g \in I_1$.

□

13.2 Primary Ideals

Definition 13.3. Let A be a ring and let $Q \subset A$ be an ideal. We say Q is a **primary ideal** if for all $a, b \in A$, we have

$$ab \in Q \text{ and } a \notin Q \text{ implies } b^n \in Q \text{ for some } n \in \mathbb{N}.$$

Proposition 13.4. *Let A be a ring and let $Q \subset A$ be a primary ideal. Then $\sqrt{Q}$ is a prime ideal. Moreover, $\sqrt{Q}$ is the smallest prime ideal containing Q.*

Proof. Suppose $ab \in \sqrt{Q}$ and $a \notin \sqrt{Q}$. Then $(ab)^m = a^m b^m \in Q$ for some $m \in \mathbb{N}$. Since $a^m \notin Q$ and Q is primary, $(b^m)^n = b^{mn} \in Q$ for some $n \in \mathbb{N}$. This implies $b \in \sqrt{Q}$. This shows that $\sqrt{Q}$ is a prime ideal. To see that it is the smallest prime ideal, suppose $\mathfrak{p} \subset A$ is a prime ideal such that $Q \subset \mathfrak{p}$ and suppose $a \in \sqrt{Q}$. Then $a^n \in Q \subset \mathfrak{p}$ for some $n \in \mathbb{N}$. Since $\mathfrak{p}$ is a prime ideal, this implies $a \in \mathfrak{p}$. Therefore $\sqrt{Q} \subset \mathfrak{p}$. □

Example 13.1. The converse to Proposition (13.4) is false, that is, if $\mathfrak{a} \subset A$ is an ideal such that $\sqrt{\mathfrak{a}}$ is prime, then $\mathfrak{a}$ is not necessarily primary. Indeed, let $A = K[x, y]$ and $\mathfrak{a} = \langle x^2, xy \rangle$. Then $\sqrt{\mathfrak{a}} = \langle x \rangle$ is prime, but $\mathfrak{a}$ is not primary. We have $xy \in \mathfrak{a}$ and $x \notin \mathfrak{a}$, but no power of y belongs to $\mathfrak{a}$.

Definition 13.4. Let A be a ring and let $Q \subset A$ be a primary ideal. We denote $\mathfrak{p} := \sqrt{Q}$ and say Q is **$\mathfrak{p}$-primary**.

13.2.1 Intersection of $\mathfrak{p}$-Primary Ideals is Primary

Proposition 13.5. *Let A be a ring and let $Q_1, Q_2 \subset A$ be $\mathfrak{p}$-primary ideals. The $Q_1 \cap Q_2$ is a $\mathfrak{p}$-primary ideal.*

Proof. Suppose $ab \in Q_1 \cap Q_2$ and $a \notin Q_1 \cap Q_2$. Then either $a \notin Q_1$ or $a \notin Q_2$. Without loss of generality, assume $a \notin Q_2$. Then $b^n \in Q_2$ for some $n \in \mathbb{N}$. Since $\sqrt{Q_2} = \mathfrak{p}$, we have $b \in P$. But since $\mathfrak{p} = \sqrt{Q_1}$, we also have $b^m \in Q_1$ for some $m \in \mathbb{N}$. So $b^{\gcd(m,n)} \in Q_1 \cap Q_2$. □

Remark. Notice that we used the fact that these are $\mathfrak{p}$-primary ideals. If Q_1 is $\mathfrak{p}_1$-primary and Q_2 is $\mathfrak{p}_2$-primary, where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are different primes, then

$$\sqrt{Q_1 \cap Q_2} = \sqrt{Q_1} \cap \sqrt{Q_2} = \mathfrak{p}_1 \cap \mathfrak{p}_2,$$

which is not a prime ideal. Hence $Q_1 \cap Q_2$ is not primary.

13.2.2 $\mathfrak{p}$-primary ideals and colon properties

Proposition 13.6. *Let A be a ring, $\mathfrak{p} \subset A$ be a prime ideal, and $Q \subset A$ be a $\mathfrak{p}$-primary ideal.*

1. *If $x \notin Q$, then $Q : x$ is $\mathfrak{p}$-primary.*

2. *If $x \notin \mathfrak{p}$, then $Q : x = Q$*

3. *If $x \in Q$, then $Q : x = A$.*

Proof.

1. Suppose $ab \in Q : x$ and $a \notin Q : x$. Then $abx \in Q$ and $ax \notin Q$ implies $b^n \in Q$ for some $n \in \mathbb{N}$, since Q is primary. Therefore $b \in Q : x$ since $b^n x \in Q$. To see that $Q : x$ is $\mathfrak{p}$-primary, we simply note that $a \in Q : x$ implies $ax \in Q$ implies $a^n \in Q$. So $Q \subset Q : x \subset \sqrt{Q}$.

2. We certainly have $Q \subset Q : x$ since $ax \in Q$ for all $a \in Q$. For the reverse inclusion, suppose $a \in Q : x$, so $ax \in Q$. Assume $a \notin Q$. Since Q is a primary ideal, then $ax \in Q$ and $a \notin Q$ implies $x^n \in Q$ for some $n \in \mathbb{N}$. But this implies $x \in \mathfrak{p}$, which is a contradiction. Hence $a \in Q$, and thus, $Q : x \subset Q$.

3. If $a \in A$, then $ax \in Q$ since $x \in Q$. So $A \subset Q : x$. The reverse inclusion is obvious.

□

13.2.3 nth Symbolic Power

Definition 13.5. Let A be a ring and let $\mathfrak{q}$ be a prime ideal in A. The **nth symbolic power of** $\mathfrak{q}$, denoted $\mathfrak{q}^{(n)}$, is defined to be the ideal

$$\mathfrak{q}^{(n)} = \mathfrak{q}^n A_{\mathfrak{q}} \cap A = \{a \in A \mid as \in \mathfrak{q}^n \text{ for some } s \in A \backslash \mathfrak{q}\}.$$

Proposition 13.7. *Let A be a ring and let $\mathfrak{q}$ be a prime ideal in A. Then $\mathfrak{q}^{(n)}$ is the smallest $\mathfrak{q}$-primary ideal which contains $\mathfrak{q}^n$.*

Proof. It is clear that $\mathfrak{q}^n \subset \mathfrak{q}^{(n)}$. Let us show that $\mathfrak{q}^{(n)}$ is a $\mathfrak{q}$-primary ideal. Suppose $ab \in \mathfrak{q}^{(n)}$ and $a \notin \mathfrak{q}^{(n)}$. Choose $s \in A \backslash \mathfrak{q}$ such that $abs \in \mathfrak{q}^n$. Since $a \in \mathfrak{q}^{(n)}$, we must not have $bs \in A \backslash \mathfrak{q}$. In particular, this implies $b \in \mathfrak{q}$ since $A \backslash \mathfrak{q}$ is multiplicatively closed. But then $b^n \in \mathfrak{q}^n \subset \mathfrak{q}^{(n)}$. Thus $\mathfrak{q}^{(n)}$ is $\mathfrak{q}$-primary.

Now we will show that it is the smallest $\mathfrak{q}$-primary ideal which contains $\mathfrak{q}^n$. Let Q be any $\mathfrak{q}$-primary ideal which contains $\mathfrak{q}^n$ and let $a \in \mathfrak{q}^{(n)}$. Choose $s \in A \backslash \mathfrak{q}$ such that $as \in \mathfrak{q}^n \subset Q$. Since $A \backslash \mathfrak{q}$ is multiplicatively closed and since $Q \cap A \backslash \mathfrak{q} = \emptyset$, we must have $s^m \notin Q$ for all $m \in \mathbb{N}$. This implies $a \in Q$ since Q is primary. Thus $\mathfrak{q}^{(n)} \subset Q$. □

13.3 Primary Decomposition

In a Noetherian ring, any ideal can be written as a finite intersection of primary ideals (called the **primary decomposition**). Before we go over the proof, we need a definition and a lemma.

Definition 13.6. Let A be a ring and let $I \subset A$ be an ideal. We say I is **irreducible** if given two ideals $I_1, I_2 \subset A$ such that $I = I_1 \cap I_2$, then either $I = I_1$ or $I = I_2$.

Lemma 13.2. *Let A be a Noetherian ring and let $I \subset A$ be an irreducible ideal. Then I is primary.*

Proof. Suppose $ab \in I$ with $a \notin I$. There is a chain of ideals:

$$I \subset I : b \subset I : b^2 \subset \cdots$$

By the Noetherian condition we must have $I : b^n = I : b^{n+1}$ for some $n \in \mathbb{N}$. Assume $b^n \notin I$. We will show $\langle I, b^n \rangle \cap \langle I, a \rangle = I$, which is a contradiction since $b^n, a \notin I$. To show this, we only need to show $\langle b^n \rangle \cap \langle a \rangle \subset I$. Suppose $x \in \langle b^n \rangle \cap \langle a \rangle$. Then $x \in \langle a \rangle$ implies $x = ay$ and $x \in \langle b^n \rangle$ implies $x = b^n z$. Then

$$bx = b^{n+1} z = bay \in I$$

implies $z \in I : b^{n+1} = I : b^n$. Therefore $x = zb^n \in I$. □

Theorem 13.3. *Let A be a Noetherian ring and let $I \subset A$ be an ideal. Then I can be expressed as a finite intersection of primary ideals.*

Proof. First, we show that I can be expressed as a finite intersection of irreducible ideals. Assume, on the contrary, that I cannot be expressed as a finite intersection of irreducible ideals. Let S be the set of all ideals which cannot be expressed as a finite intersection of irreducible ideals. Then S is nonempty since $I \in S$. Since A is noetherian, S has a maximal element J. Since $J \in S$, it must be reducible, so we can write $J = J_1 \cap J_2$ with $J \subsetneq J_1$ and $J \subsetneq J_2$. Since J is maximal, we can express J_1 and J_2 as a finite intersection of irreducible ideals, and hence we can express J as a finite intersection of irreducible ideals, which is a contradiction. Now apply Lemma 13.2. □

Remark. It is interesting to compare this proof with the proof given in my Algebraic Number Theory notes on why every ideal in $\mathcal{O}_K$ contains a product of primes. In both cases, we needed a maximal element; one based on the index of an ideal in the ring of integers, and one based containment.

Definition 13.7. A primary decomposition $I = \bigcap_{i=1}^{n} Q_i$ is **irredundant** if for each $j \in \{1, \dots, n\}$

$$\bigcap_{i \neq j} Q_i \neq I.$$

Remark. So there are no "extraneous" factors".

Given an irredundant primary decomposition $I = \bigcap_{i=1}^{n} Q_i$, if $i \neq j$ then $\mathfrak{p}_i \neq \mathfrak{p}_j$. The reason is because if $\mathfrak{p}_i = \mathfrak{p}_j$, then by Proposition 13.5, $Q = Q_i \cap Q_j$ is a smaller primary ideal which contains I, and hence the primary decomposition for I can be replaced by removing Q_i and Q_j and replacing them with Q, which means $I = \bigcap_{i=1}^{n} Q_i$ is not irredundant. So we get a picture that looks like this:

Definition 13.8. The set of **associated primes** of I, denoted by $Ass(I)$, is defined as

$$Ass(I) = \{P \subset R \mid P \text{ prime}, P = I : f \text{ for some } f \in R\}$$

Given an irredundant primary decomposition $I = \bigcap_{i=1}^{n} Q_i$, we claim $P_i \in Ass(I)$: For any j, we can find $f_j \notin Q_j$ but which is in all the other Q_i for $i \neq j$. Then

$$I : f_j = \left(\bigcap_{i=1}^{n} Q_i \right) : f_j = \bigcap_{i=1}^{n} (Q_i : f_j) = Q_j : f_j$$

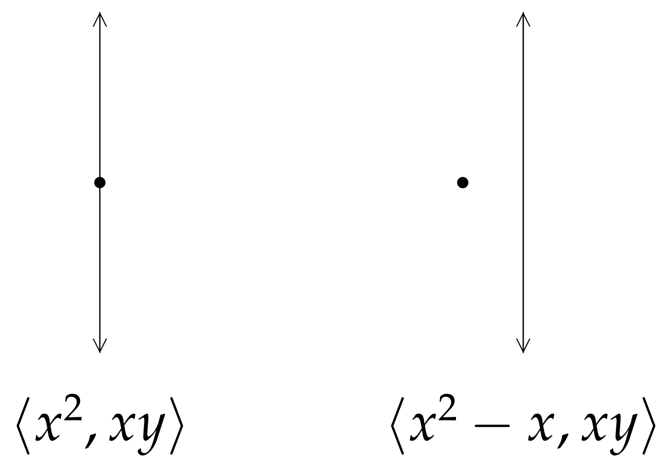
Thus, $I : f_j$ is P_j-primary. In particular $\sqrt{I : f_j} = \sqrt{Q_j : f_j} = P_j$. Also, if $P = I : f$ for some $f \in R$, then

$$P \supset Q_1 \cap Q_2 \cap \cdots \cap Q_n$$

Since P is a prime ideal, $P \supset Q_k$ for some $1 \leq k \leq n$. Then $P \supset P_k$ since P_k is the smallest prime ideal which contains Q_k.

Definition 13.9. An associated prime P_i which does not properly contain any other associated prime P_j is called a **minimal** associated prime. The non-minimal associated primes are called **embedded** associated primes.

Example 13.2. Let $I = \langle x^2, xy \rangle$. Clearly $I = \langle x^2, y \rangle \cap \langle x \rangle$.



Lemma 13.4. *(Splitting tool) Let A be a ring, $I \subset A$ an ideal, and let $I : a = I : a^2$ for some $a \in A$. Then $I = (I : a) \cap \langle I, a \rangle$.*

Proof. Since both $I : a$ and $\langle I, a \rangle$ contain I, we have $I \subset (I : a) \cap \langle I, a \rangle$. For the reverse inclusion, let $f \in (I : a) \cap \langle I, a \rangle$ and let $f = g + xa$ for some $g \in I$. Then $af = ag + xa^2 \in I$ and, therefore, $xa^2 \in I$. That is, $x \in I : a^2 = I : a$ which implies $xa \in I$ and, consequently, $f \in I$. □

Example 13.3. Let $I = \langle xy^2, y^3 \rangle$. Then $I : x = \langle y^2 \rangle = I : x^2$. Therefore, $I = \langle y^2 \rangle \cap \langle x, y^3 \rangle$.

Example 13.4. Let $I = \langle wx, wy, wz, vx, vy, vz, ux, uy, uz, y^3 - x^2 \rangle$. Then $I : w = \langle x, y, z \rangle = I : w^2$. Therefore $I = \langle x, y, z \rangle \cap I_1$ where $I_1 = \langle w, vx, vy, vz, ux, uy, uz, y^3 - x^2 \rangle$. Then $I_1 : v = \langle w, x, y, z \rangle = I_1 : v^2$, and so $I_1 = \langle w, x, y, z \rangle \cap I_2$ where $I_2 = \langle w, v, ux, uy, uz, y^3 - x^2 \rangle$. Finally, $I_2 : u = \langle w, v, x, y, z \rangle = I_2 : u^2$, and so $I_2 = \langle w, v, x, y, z \rangle \cap \langle w, v, u, y^3 - x^2 \rangle$. So $I = \langle x, y, z \rangle \cap \langle w, x, y, z \rangle \cap \langle w, v, x, y, z \rangle \cap \langle w, v, u, y^3 - x^2 \rangle = \langle x, y, z \rangle \cap \langle w, v, u, y^3 - x^2 \rangle$.

Example 13.5. Let $A = K[x, y, z, w]$. The twisted cubic is the set-theoretic intersection of $xz - y^2$ and $z(yw - z^2) - w(xw - yz)$, but it is not a sheme-theoretic or ideal-theoretic complete intersection. To get a sense of why this is, we compute a primary decomposition of $I = \langle xz - y^2, z(yw - z^2) - w(xw - yz) \rangle$. Using Singular, we see that I is $\mathfrak{p}$-primary where $\mathfrak{p} = \langle xz - y^2, yw - z^2, xw - yz \rangle$, and thus $\sqrt{I} = \mathfrak{p}$. Therefore $\mathbf{V}(I) = \mathbf{V}(\mathfrak{p})$. On the other hand, $I \subsetneq \mathfrak{p}$.

Definition 13.10. Let A be a Noetherian ring and let I be an ideal in A.

1. The set of **associated primes** of I, denoted by $\text{Ass}(I)$, is defined as

   $$\text{Ass}(I) = \{\mathfrak{p} \subset A \mid \mathfrak{p} \text{ is prime and } \mathfrak{p} = I : a \text{ for some } a \in A\}.$$

   Elements of $\text{Ass}(\langle 0 \rangle)$ are also called **associated primes** of A.

2. Let $\mathfrak{p}, \mathfrak{q} \in \text{Ass}(I)$ and $\mathfrak{q} \subset \mathfrak{p}$. Then $\mathfrak{p}$ is called an **embedded prime ideal** of I. We define $\text{Ass}(I, \mathfrak{p}) := \{\mathfrak{q} \mid \mathfrak{q} \in \text{Ass}(I) \text{ and } \mathfrak{q} \subset \mathfrak{p}\}$.

3. I is called **equidimensional** or **pure dimensional** if all associated primes of I have the same dimension.

4. I is a **primary ideal** if, for any $a, b \in A$, $ab \in I$, and $a \notin I$, then $b \in \sqrt{I}$. Let $\mathfrak{p}$ be a prime ideal. Then a primary ideal I is called $\mathfrak{p}$-primary if $\mathfrak{p} = \sqrt{I}$.

5. A **primary decomposition** of I, that is, a decomposition $I = Q_1 \cap \cdots \cap Q_s$ with Q_i primary ideals, is called **irredundant** if no Q_i can be omitted in the decomposition and if $\sqrt{Q_i} \neq \sqrt{Q_j}$ for all $i \neq j$.

13.4 Examples

Example 13.6. Let $A = K[x,y]$ and $I = \langle x^2, xy \rangle$. Then a primary decomposition of I is given by $I = I_1 \cap I_2$, where

$$\begin{aligned} I_1 &= \langle x^2, y \rangle & \sqrt{I_1} &= \langle x, y \rangle \\ I_2 &= \langle x \rangle & \sqrt{I_2} &= \langle x \rangle \end{aligned}$$

Example 13.7. Let $A = K[x,y,u,v]$ and $I = \langle xu, xv, yu, yv \rangle$. Then a primary decomposition of I is given by $I = I_1 \cap I_2$, where

$$\begin{aligned} I_1 &= \langle x, y \rangle & \sqrt{I_1} &= \langle x, y \rangle \\ I_2 &= \langle u, v \rangle & \sqrt{I_2} &= \langle u, v \rangle \end{aligned}$$

Example 13.8. Let $A = K[x,y,u,v]$ and $I = \langle xu, yv, xv + yu \rangle$. Then a primary decomposition of I is given by $I = I_1 \cap I_2 \cap I_3$, where

$$\begin{aligned} I_1 &= \langle x, y \rangle & \sqrt{I_1} &= \langle x, y \rangle \\ I_2 &= \langle u, v \rangle & \sqrt{I_2} &= \langle u, v \rangle \\ I_3 &= \langle x^2, xy, xu, yu + xv, y^2, yv, u^2, uv, v^2 \rangle & \sqrt{I_3} &= \langle x, y, u, v \rangle \end{aligned}$$

Example 13.9. Let $A = K[x,y,u,v]$ and $I = \langle xu + yv, xv + yu \rangle$. Then a primary decomposition of I is given by $I = I_1 \cap I_2 \cap I_3 \cap I_4$, where=

$$\begin{aligned} I_1 &= \langle x, y \rangle & \sqrt{I_1} &= \langle x, y \rangle \\ I_2 &= \langle u, v \rangle & \sqrt{I_2} &= \langle u, v \rangle \\ I_3 &= \langle x + y, u - v \rangle & \sqrt{I_3} &= \langle x + y, u - v \rangle \\ I_4 &= \langle x - y, u + v \rangle & \sqrt{I_4} &= \langle x - y, u + v \rangle \end{aligned}$$

Example 13.10. Let $R = K[x,y]$ and let $I = \langle x^2 - xy, xy^2 - xy \rangle$. Using Singular, we calculate

Ring	$R = K[x,y]$
Ideal	$I = \langle x^2 - xy, xy^2 - xy \rangle$
Minimal Associated Primes	$\operatorname{MinAss} I = \{\langle x \rangle, \langle x - 1, y - 1 \rangle\}$
Associated Primes	$\operatorname{Ass} I = \{\langle x \rangle, \langle x, y \rangle, \langle x - 1, y - 1 \rangle\}$
Primary Decomposition	$I = \langle x \rangle \cap \langle x^2, y \rangle \cap \langle x - 1, y - 1 \rangle$

Now observe that $\dim I = 1$ and $y - 1$ belongs to a minimal associated prime of I, yet $\dim(\langle I, y - 1 \rangle) = 0$. On the other hand, x also belongs to a minimal associated prime of I, and $\dim(\langle I, x \rangle) = 1$. The difference between $y - 1$ and x here is that $y - 1$ belongs to the minimal associated prime $\langle x - 1, y - 1 \rangle$ whereas x belongs to the minimal associated prime $\langle x \rangle$.

Now if we localize at the maximal ideal $\mathfrak{m} = \langle x, y \rangle$, then the table above transforms as follows:

Ring	$R_{\mathfrak{m}} = K[x,y]_{\langle x,y \rangle}$
Ideal	$I_{\mathfrak{m}} = \langle x^2, xy \rangle$
Minimal Associated Primes	$\operatorname{MinAss} I = \{\langle x \rangle\}$
Associated Primes	$\operatorname{Ass} I = \{\langle x \rangle, \langle x, y \rangle\}$
Primary Decomposition	$I = \langle x \rangle \cap \langle x^2, y \rangle$

What happened here is that we now have $\langle x - 1, y - 1 \rangle_{\mathfrak{m}} = R_{\mathfrak{m}}$, since both $x - 1$ and $y - 1$ are units. Thus it is becomes an irrelevant factor.

13.5 Associated Primes

Definition 13.11. Let R be a ring, $\mathfrak{p} \subset R$ a prime ideal, and M an R-module. We say $\mathfrak{p}$ is an **associated prime of** M if $\mathfrak{p} = 0 : u$ for some $u \in M$. The set of all associated primes of M is written $\text{Ass}(M)$.

Theorem 13.5. *Let A be a Noetherian ring and let M be a finitely generated A-module.*

1. *$Ass(M)$ is a finite, nonempty set of primes, each containing $Ann(M)$. The set $Ass(M)$ includes all primes minimal among primes containing $Ann(M)$.*

2. *The union of associated primes of M consists of 0 and the set of zerodivisors on M.*

3. *The formation of the set $Ass(M)$ commutes with localization at an arbitrary multiplicately closed set, in the sense that*
$$Ass_{S^{-1}A}(S^{-1}M) = \{S^{-1}\mathfrak{p} \mid \mathfrak{p} \in Ass(M) \text{ and } \mathfrak{p} \cap S = \varnothing\}.$$

Lemma 13.6. *(Prime Avoidance) If $I \subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$, with $\mathfrak{p}_i$ prime, then $I \subseteq \mathfrak{p}_i$ for some i.*

Proof. We prove the contrapositive: $I \not\subseteq \mathfrak{p}_i$ for all i implies $I \not\subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$. Induct on n, the base case is trivial. We now suppose that $I \not\subseteq \mathfrak{p}_i$ for all i and $I \subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$, and arrive at a contradiction. From our inductive hypothesis, for each i, $I \not\subseteq \bigcup_{j \neq i} \mathfrak{p}_j$. In particular, for each i there is an x_i which is in I but is not in $\bigcup_{j \neq i} \mathfrak{p}_j$. Notice that if $x_i \notin \mathfrak{p}_i$ then $x_i \notin \bigcup_{j=1}^{n} \mathfrak{p}_j$, and we have an immediate contradiction. So suppose for every i that $x_i \in \mathfrak{p}_i$. Consider the element
$$x = \sum_{i=1}^{n} x_1 \cdots \hat{x}_i \cdots x_n.$$
By construction, $x \in I$. We claim that $x \notin \bigcup_{i=1}^{n} \mathfrak{p}_i$. To see this, observe that $x_1 \cdots \hat{x}_i \cdots x_n \notin \mathfrak{p}_i$, because for each index $k \neq i$, x_k is not in $\bigcup_{j \neq k} \mathfrak{p}_j$, so in particular is not in $\mathfrak{p}_i$. Since $\mathfrak{p}_i$ is prime, this proves that $x_1 \cdots \hat{x}_i \cdots x_n \notin \mathfrak{p}_i$. But every other monomial of x is in $\mathfrak{p}_i$, since every other monomial contains x_i. This shows that $x \notin \mathfrak{p}_i$ for any i, hence $x \notin \bigcup_{j=1}^{n} \mathfrak{p}_j$, a contradiction. □

Finitely generated modules over Noetherian rings are distinguished for two reasons:

1. Every zerodivisor of M is contained in an associated prime ideal: Let x be a nonzerodivisor of M. This means there is a nonzero $m \in M$ such that $xm = 0$. Then x belongs to the ideal $0 : m = \{a \in A \mid am = 0\}$. In a Noetherian ring, we have primary decomposition. So
$$x \in 0 : m = Q_1 \cap Q_2 \cap \cdots \cap Q_k \subseteq \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \cdots \cap \mathfrak{p}_k$$
where each $\mathfrak{p}_i = (0 : m) : d_i = 0 : d_i m$ for some $d_i \in A$. That is, each $\mathfrak{p}_i$ is an associated prime ideal of M.

2. The number of associated prime ideals of M is finite. So if I is an ideal which consists of zero-divisors of M, then
$$I \subseteq \bigcup_{\mathfrak{p} \in \text{Ass}(M)} \mathfrak{p}.$$
and by the Lemma (14.1), we must have $I \subseteq \mathfrak{p}_i$ for some i. Writing $\mathfrak{p}_i = 0 : m_i$, the assignment $1 \mapsto m_i$ induces a non-zero homomorphism $\varphi : A/I \to M$.

Example 13.11. Let $A = K[x,y]$ and $M = K[x,y]/\langle xy \rangle$. Then $\text{Ass}(M) = \{\langle x \rangle, \langle y \rangle\}$ and $\text{Supp}(M) = \mathbf{V}(\langle xy \rangle)$. Clearly $\text{Supp}(M)$ is much bigger than $\text{Ass}(M)$. For example, $\langle x - a, y \rangle \in \text{Supp}(M)$ but $\langle x - a, y \rangle \notin \text{Ass}(M)$ for all $a \in K$. Consider the filtration
$$0 = M_0 \subset M_1 \subset M_2 \subset M_3 = M,$$
where $M_1 = \langle x \rangle / \langle xy \rangle$ and $M_2 = \langle x, y \rangle / \langle xy \rangle$. The factors of this filtration are
$$M_3/M_2 \cong K[x,y]/\langle x,y \rangle,$$
$$M_2/M_1 \cong K[x,y]/\langle x \rangle,$$
$$M_1/M_0 \cong K[x,y]/\langle y \rangle.$$

Proposition 13.8. *Let*
$$0 \to M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \to 0$$
be a short exact sequence of R-modules. Then
$$\text{Ass}(M') \subset \text{Ass}(M) \subset \text{Ass}(M') \cup \text{Ass}(M'')$$

Proof. We first show $\operatorname{Ass}(M') \subset \operatorname{Ass}(M)$. Let $\mathfrak{p} \in \operatorname{Ass}(M')$. Choose $u' \in M'$ such that $\mathfrak{p} = 0 : u'$. We claim that $\mathfrak{p} = 0 : \varphi(u')$. Indeed, if $a \in \mathfrak{p}$, then

$$\begin{aligned} a\varphi(u') &= \varphi(au') \\ &= \varphi(0) \\ &= 0 \end{aligned}$$

implies $a \in 0 : \varphi(u')$ and hence $\mathfrak{p} \subset 0 : \varphi(u')$. Conversely, if $a \in 0 : \varphi(u')$, then

$$\begin{aligned} 0 &= a\varphi(u') \\ &= \varphi(au') \end{aligned}$$

implies $au' = 0$ since φ is injective, which implies $a \in \mathfrak{p}$ since $\mathfrak{p} = 0 : u'$. Therefore $\mathfrak{p} \supset 0 : \varphi(u')$, and so $\mathfrak{p} \in \operatorname{Ass}(M)$. This implies $\operatorname{Ass}(M') \subset \operatorname{Ass}(M)$.

We now show $\operatorname{Ass}(M) \subset \operatorname{Ass}(M') \cup \operatorname{Ass}(M'')$. Let $\mathfrak{p} \in \operatorname{Ass}(M)$. Choose $u \in M$ such that $\mathfrak{p} = 0 : u$.

Case 1: Assume that $Ru \cap M' \neq 0$. Choose an a nonzero element in $Ru \cap M'$, say au for some $a \in R$. Since $au \neq 0$, we must have $a \notin \mathfrak{p}$ since $0 : u = \mathfrak{p}$. Thus

$$\begin{aligned} 0 : au &= (0 : u) : a \\ &= \mathfrak{p} : a \\ &= \mathfrak{p}, \end{aligned}$$

which implies $\mathfrak{p} \in \operatorname{Ass}(M')$, hence $\operatorname{Ass}(M) \subset \operatorname{Ass}(M')$.

Case 2: Assume that $Ru \cap M' = 0$. We claim that $\mathfrak{p} = 0 : \psi(u)$. First note that $\mathfrak{p} \subset 0 : \psi(u)$ follows from the argument above, so it suffices to show $\mathfrak{p} \supset 0 : \psi(u)$. Let $a \in 0 : \psi(u)$. Then

$$\begin{aligned} 0 &= a\psi(u) \\ &= \psi(au) \end{aligned}$$

implies $au \in \ker \psi = M'$. Since $Ru \cap M' = 0$, this implies $au = 0$, and consequently $a \in \mathfrak{p}$. It follows that $\mathfrak{p} \supset 0 : \psi(u)$. □

Proposition 13.9. *Let R be a Noetherian ring and let M be a finitely-generated R-module. Then there exists a finite filtration*

$$0 = M_0 \subset M_1 \subset \cdots \subset M_k = M$$

such that the successive quotients M_{i+1}/M_i are isomorphic to various $R/\mathfrak{p}_i$ with the $\mathfrak{p}_i \subset R$ prime.

Proof. Let $M' \subset M$ be maximal among submodules for which such a filtration (ending with M') exists. We would like to show that $M' = M$. Now M' is well-defined since 0 has such a filtration and M is Noetherian.

There is a filtration

$$0 = M_0 \subset M_1 \subset \cdots \subset M_l = M' \subset M$$

where the successive quotients, *except* possibly the last M/M', are of the form $R/\mathfrak{p}_i$ for $\mathfrak{p}_i$ prime. If $M' = M$, we are done. Otherwise, consider the quotient $M/M' \neq 0$. There is an associated prime of M/M'. So there is a prime $\mathfrak{p}$ which is the annihilator of $x \in M/M'$. This means that there is an injection

$$R/\mathfrak{p} \hookrightarrow M/M'.$$

Now, take M_{l+1} as the inverse image in M of $R/\mathfrak{p} \subset M/M'$. Then we can consider the finite filtration

$$0 = M_0 \subset M_1 \subset \cdots \subset M_{l+1},$$

all of whose successive quotients are of the form $R/\mathfrak{p}_i$; this is because $M_{l+1}/M_l = M_{l+1}/M'$ is of this form by construction. We have thus extended this filtration one step further, a contradiction since M' was assumed to be maximal. □

14 Depth

14.0.1 Prime Avoidance

Lemma 14.1. *(Prime Avoidance) If $I \subseteq \bigcup_{i=1}^n \mathfrak{p}_i$, with $\mathfrak{p}_i$ prime, then $I \subseteq \mathfrak{p}_i$ for some i.*

Proof. We prove the contrapositive: $I \not\subseteq \mathfrak{p}_i$ for all i implies $I \not\subseteq \bigcup_{i=1}^n \mathfrak{p}_i$. Induct on n, the base case is trivial. We now suppose that $I \not\subseteq \mathfrak{p}_i$ for all i and $I \subseteq \bigcup_{i=1}^n \mathfrak{p}_i$, and arrive at a contradiction. From our inductive hypothesis, for each i, $I \not\subseteq \bigcup_{j \neq i} \mathfrak{p}_j$. In particular, for each i there is an x_i which is in I but is not in $\bigcup_{j \neq i} \mathfrak{p}_j$. Notice that if $x_i \notin \mathfrak{p}_i$ then $x_i \notin \bigcup_{j=1}^n \mathfrak{p}_j$, and we have an immediate contradiction. So suppose for every i that $x_i \in \mathfrak{p}_i$. Consider the element

$$x = \sum_{i=1}^n x_1 \cdots \hat{x}_i \cdots x_n.$$

By construction, $x \in I$. We claim that $x \notin \bigcup_{i=1}^n \mathfrak{p}_i$. To see this, observe that $x_1 \cdots \hat{x}_i \cdots x_n \notin \mathfrak{p}_i$, because for each index $k \neq i$, x_k is not in $\bigcup_{j \neq k} \mathfrak{p}_j$, so in particular is not in $\mathfrak{p}_i$. Since $\mathfrak{p}_i$ is prime, this proves that $x_1 \cdots \hat{x}_i \cdots x_n \notin \mathfrak{p}_i$. But every other monomial of x is in $\mathfrak{p}_i$, since every other monomial contains x_i. This shows that $x \notin \mathfrak{p}_i$ for any i, hence $x \notin \bigcup_{j=1}^n \mathfrak{p}_j$, a contradiction. □

14.0.2 Support

Definition 14.1. Let M be an R-module. The **support** of M is the set

$$\operatorname{Supp} M = \{\mathfrak{p} \in \operatorname{Spec} R \mid M_\mathfrak{p} \neq 0\}$$

Lemma 14.2. *Let M be an R-module. Then we have*

$$\operatorname{Supp} M \subseteq \mathrm{V}(\operatorname{Ann} M).$$

If moreover, M is finitely-generated, then

$$\operatorname{Supp} M \supseteq \mathrm{V}(\operatorname{Ann} M).$$

Proof. Let $\mathfrak{p} \in \operatorname{Supp} M$ and assume for a contradiciton that $\mathfrak{p} \notin \mathrm{V}(\operatorname{Ann} M)$, so $\mathfrak{p} \not\supseteq \operatorname{Ann} M$. Choose $s \in \operatorname{Ann} M$ such that $x \notin \mathfrak{p}$. Then $M_\mathfrak{p} = 0$ since given any $u/t \in M_\mathfrak{p}$, we have

$$\begin{aligned} \frac{u}{t} &= \frac{su}{st} \\ &= \frac{0}{st} \\ &= 0. \end{aligned}$$

This is a contradiction as $\mathfrak{p} \in \operatorname{Supp} M$ which means $M_\mathfrak{p} \neq 0$. Thus $\mathfrak{p} \in \mathrm{V}(\operatorname{Ann} M)$ and since $\mathfrak{p}$ is arbitrary, this implies

$$\operatorname{Supp} M \subseteq \mathrm{V}(\operatorname{Ann} M).$$

Now we prove the second part of the lemma: suppose M is finitely-generated, say by $u_1, \dots, u_n \in M$, and let $\mathfrak{p} \in \mathrm{V}(\operatorname{Ann} M)$, so $\mathfrak{p} \supseteq \operatorname{Ann} M$. Assume for a contradiction that $\mathfrak{p} \notin \operatorname{Supp} M$, so $M_\mathfrak{p} = 0$. Choose $s_i \in R \backslash \mathfrak{p}$ such that $s_i u_i = 0$ for all $1 \leq i \leq n$ and denote $s = s_1 s_2 \cdots s_n$. Then $s \in R \backslash \mathfrak{p}$ and $s \in \operatorname{Ann} M$ since

$$\begin{aligned} su_i &= s_1 s_2 \cdots s_n u_i \\ &= s_1 \cdots s_{i-1} s_{i+1} \cdots s_n (s_i u_i) \\ &= s_1 \cdots s_{i-1} s_{i+1} \cdots s_n \cdot 0 \\ &= 0 \end{aligned}$$

for all $1 \leq i \leq n$. This contradicts the fact that $\mathfrak{p} \supseteq \operatorname{Ann} M$. Thus $\mathfrak{p} \in \operatorname{Supp} M$ and since $\mathfrak{p}$ is arbitary, this implies

$$\operatorname{Supp} M \supseteq \mathrm{V}(\operatorname{Ann} M).$$

□

14.1 Depth

Finite modules over Noetherian rings are distinguished for two reasons: First, every zerodivisor of M is contained in an associated prime ideal. Indeed, let x be a zerodivisor of M. This means there is a nonzero $u \in M$ such that $xu = 0$. Then x belongs to the ideal

$$0 :_R u = \{a \in R \mid au = 0\}.$$

In a Noetherian ring, we have primary decomposition. So

$$\begin{aligned} x &\in 0 :_R u \\ &= Q_1 \cap \cdots \cap Q_m \\ &\subseteq \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m, \end{aligned}$$

where

$$\begin{aligned} \mathfrak{p}_i &= (0 :_R u) : d_i \\ &= 0 :_R d_i u. \end{aligned}$$

for some $d_i \in R$. That is, each $\mathfrak{p}_i$ is an associated prime ideal of M.

Secondly, the number of associated prime ideals of M is finite. So if I is an ideal which consists of zerodivisors of M, then

$$I \subseteq \bigcup_{\mathfrak{p} \in \mathrm{Ass}(M)} \mathfrak{p}.$$

and by the Lemma (14.1), we must have $I \subseteq \mathfrak{p}_i$ for some i. Writing $\mathfrak{p}_i = 0 :_R u_i$, the assignment $1 \mapsto u_i$ induces a nonzero homomorphism $\varphi \colon R/I \to M$.

Proposition 14.1. *Let M and N be R-modules.*

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

Proof. 1. Suppose $\operatorname{Ann} M$ contains an N-regular element. Choose $x \in \operatorname{Ann} M$ to be such an element and let $\varphi \in \operatorname{Hom}_R(M, N)$. Then

$$\begin{aligned} x\varphi(u) &= \varphi(xu) \\ &= \varphi(0) \\ &= 0 \end{aligned}$$

implies $\varphi(u) = 0$ for all $u \in M$. Therefore $\varphi = 0$.

2. Suppose R is Noetherian, M, N are finite, and $\operatorname{Hom}_R(M, N) = 0$. Assume for a contradiction that $\operatorname{Ann} M$ consists of zerodivisors of N. Then by the remarks above, $\operatorname{Ann} M \subset \mathfrak{p}$ for some associated prime ideal $\mathfrak{p}$ of N. By Lemma (14.2), $\mathfrak{p} \in \operatorname{Supp} M$; so $M_{\mathfrak{p}} \neq 0$. In fact, Nakayama's Lemma tells us that $M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}} \neq 0$. Since $M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}}$ is just a direct sum of copies of $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$, one has an epimorphism

$$M_{\mathfrak{p}} \to M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}} \to R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}.$$

Now observe that $\mathfrak{p}R_{\mathfrak{p}} \in \operatorname{Ass} N_{\mathfrak{p}}$, and thus we can compose this epimorphism with a nonzero homomorphism to obtain a nonzero homomorphism,

$$M_{\mathfrak{p}} \to R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} \to N_{\mathfrak{p}}.$$

Thus

$$\begin{aligned} 0 &\neq \operatorname{Hom}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}}, N_{\mathfrak{p}}) \\ &= \operatorname{Hom}_R(M, N)_{\mathfrak{p}}, \end{aligned}$$

which is a contradiction. □

Example 14.1. Let $A = \mathbb{Q}[x, y]$, $N = \mathbb{Q}[x, y]/\langle x \rangle$, and $M = \mathbb{Q}[x, y]/\langle x^2, yx \rangle$. Clearly there exists a nonzero morphism from N to M. For example, $N \xrightarrow{\cdot x} M$ is a homomorphism from N to M. However, we want to construct a homomorphism from N to M using the techniques of Proposition (14.1). Set $I := \operatorname{Ann}(N) = \langle x \rangle$. There are two associated primes of M, namely $\mathfrak{p} := \langle x, y \rangle$ and $\mathfrak{q} := \langle x \rangle$, both contain I, and $0 : \overline{x} = \mathfrak{p}$ and $0 : \overline{y} = \mathfrak{q}$. We have $N_{\mathfrak{q}} \cong \mathbb{Q}(y)$, $N_{\mathfrak{p}} \cong \mathbb{Q}[y]_{\langle y \rangle}$, $A_{\mathfrak{q}}/\mathfrak{q}A_{\mathfrak{q}} \cong \mathbb{Q}(y)$, and $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \cong \mathbb{Q}$. The morphism $N_{\mathfrak{p}} \to M_{\mathfrak{p}}$ is given by $f/g \mapsto xf/g$ where $f, g \in \mathbb{Q}[y]$ and $g(0) \neq 0$. The morphism $N_{\mathfrak{q}} \to M_{\mathfrak{q}}$ is given by $f/g \mapsto yf/g$ where $f, g \in \mathbb{Q}(y)$ and $g \neq 0$.

Lemma 14.3. *Let M and N be R-modules and let $\mathbf{x} = x_1, \dots, x_n$ be a weak N-sequence contained in* $\operatorname{Ann} M$. *Then*

$$\operatorname{Hom}_R(M, N/\mathbf{x}N) \cong \operatorname{Ext}^n_R(M, N).$$

Proof. We use induction on n, starting form the vacuous case $n = 0$. Let $n \geq 1$, and set $\mathbf{x}' = x_1, \dots, x_{n-1}$. Then the induction hypothesis implies that

$$\operatorname{Ext}^{n-1}_R(M, N) \cong \operatorname{Hom}_R(M, N/\mathbf{x}'N).$$

As x_n is $(N/\mathbf{x}'N)$-regular, we must have $\operatorname{Ext}^{n-1}_R(M, N/\mathbf{x}'N) = 0$ by Prop (14.1). Therefore the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & N/\mathbf{x}'N \arrow[r, "\cdot x_n"] & N/\mathbf{x}'N \arrow[r] & N/\mathbf{x}N \arrow[r] & 0 \end{tikzcd}$$

yields an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{Ext}^{n-1}_R(M, N/\mathbf{x}N) \arrow[r] & \operatorname{Ext}^n_R(M, N/\mathbf{x}'N) \arrow[r, "\overline{x}_n"] & \operatorname{Ext}^n_R(M, N/\mathbf{x}'N) \end{tikzcd}$$

The map φ is multiplication by x_n inherited from $M/\mathbf{x}'M$: That is, after choosing an injective resolution of $M/\mathbf{x}'M$ with modules labeled I_i and morphisms labeled $\varphi_i : I_i \to I_{i+1}$, then an element in $\operatorname{Ext}^n_A(N, M/\mathbf{x}'M)$ is represented by a map $\psi_n : N \to I_n$ such that $\varphi_n \circ \psi_n = 0$. Then the map φ sends the representative ψ_n in $\operatorname{Ext}^n_A(N, M/\mathbf{x}'M)$ to the representative $x_n\psi_n$ in $\operatorname{Ext}^n_A(N, M/\mathbf{x}'M)$, but

$$\begin{aligned} (x_n\psi_n)(n) &= x_n\psi_n(n) \\ &= \psi_n(x_n n) \\ &= \psi_n(0) \\ &= 0, \end{aligned}$$

for all $n \in N$. Therefore φ is the zero map. Hence ψ is an isomorphism. It's now easy to show that we get the sequence of isomorphism:

$$\operatorname{Hom}_A(N, M/\mathbf{x}M) \cong \operatorname{Ext}^0_A(N, M/\mathbf{x}M) \cong \operatorname{Ext}^1_A(N, M/\mathbf{x}'M) \cong \cdots \cong \operatorname{Ext}^n_A(N, M)$$

□

Let A be a Noetherian ring, I an ideal, M a finite A-module with $M \neq IM$, and $\mathbf{x} = x_1, \dots, x_n$ a maximal M-sequence in I. From Prop (14.1) and Lemma (14.3), we have, since I contains an $M/\langle x_1, \dots, x_{i-1}\rangle M$-regular element for $i = 1, \dots, n$,

$$\operatorname{Ext}^{i-1}_A(A/I, M) \cong \operatorname{Hom}_A(A/I, M/\langle x_1, \dots, x_{i-1}\rangle M) \neq 0.$$

We have therefore proved

Theorem 14.4. *(Rees). Let A be a Noetherian ring, M be a finite A-module, and I an ideal such that $IM \neq M$. Then all maximal M-sequences in I have the same length n given by*

$$n = min\{i \mid Ext^i_A(A/I, M) \neq 0\}.$$

Definition 14.2. Let A be a ring, $I \subset A$ and ideal and M an A-module. If $M \neq IM$, then the maximal length n of an M-sequence $a_1, \dots, a_n \in I$ is called the I-**depth** of M and denoted by $\operatorname{depth}(I, M)$. If $M = IM$ then the I-depth of M is by convention ∞. If $(A, \mathfrak{m})$ is a local ring, then the $\mathfrak{m}$-depth of M is simply called the **depth** of M, that is, $\operatorname{depth}(M) := \operatorname{depth}(\mathfrak{m}, M)$.

Example 14.2.

1. Let K be a field and $K[x_1, \dots, x_n]$ the polynomial ring. Then

   $$\operatorname{depth}(\langle x_1, \dots, x_n\rangle, K[x_1, \dots, x_n]) \geq n,$$

   since $x_1, \dots, x_n$ is an $\langle x_1, \dots, x_n\rangle$-sequence (and we shall see later that it is $= n$).

2. Let A be a ring, $I \subset A$ an ideal and M an A-module. Then the I-depth of M is 0 if and only if every element of I is a zerodivisor for M. Hence, $\operatorname{depth}(I, M) = 0$ if and only if I is contained in some associated prime ideal of M. In particular, for a local ring $(A, \mathfrak{m})$, we have $\operatorname{depth}(\mathfrak{m}, A/\mathfrak{m}) = 0$.

Recall that if $M = IM$, then we set the I-depth of M to be ∞. This is consistent with Theorem (14.4) because $\operatorname{depth}(I, M) = \infty$ if and only if $\operatorname{Ext}^i_A(A/I, M) = 0$ for all i. For if $IM = M$, then $\operatorname{supp}(M) \cap \operatorname{supp}(A/I) = \{\mathfrak{p} \mid \mathfrak{p} \supset I \text{ and } M_{\mathfrak{p}} \neq 0\} = \emptyset$, by Nakayama's lemma, hence

$$\operatorname{supp}(\operatorname{Ext}^i_A(A/I, M) \subset \operatorname{supp}(M) \cap \operatorname{supp}(A/I) = \emptyset;$$

conversely, if $\operatorname{Ext}^i_A(A/I, M) = 0$ for all i, then Theorem (14.4) gives $IM = M$.

Proposition 14.2. *Let A be a Noetherian ring, I and ideal in A, and*

$$\begin{tikzcd} 0 \arrow[r] & U \arrow[r] & M \arrow[r] & N \arrow[r] & 0 \end{tikzcd}$$

an exact sequence of finite A-modules. Then

1. *$depth(I, M) \geq min\{depth(I, U), depth(I, N)\}$.*
2. *$depth(I, U) \geq min\{depth(I, M), depth(I, N) + 1\}$.*
3. *$depth(I, N) \geq min\{depth(I, U) - 1, depth(I, M)\}$.*

Proof. Let $k = \operatorname{depth}(I, U)$, $m = \operatorname{depth}(I, M)$, and $n = \operatorname{depth}(I, N)$. The given exact sequence induces a long exact sequence

$$\begin{tikzcd} & \cdots \arrow[r] & Ext^{i-1}_A(A/I,N) \arrow[dll] \\ Ext^{i}_A(A/I,U) \arrow[r] & Ext^{i}_A(A/I,M) \arrow[r] & Ext^{i}_A(A/I,N) \arrow[dll] \\ Ext^{i+1}_A(A/I,U) \arrow[r] & \cdots & \end{tikzcd}$$

From the long exact sequence above, we deduce the following:

- If $k < n$, then $\operatorname{Ext}^i_A(A/I, M) \cong \operatorname{Ext}^i_A(A/I, N)$ for all $i > k$. This implies $m = n$.
- If $k > n + 1$, then $\operatorname{Ext}^i_A(A/I, M) \cong \operatorname{Ext}^i_A(A/I, U)$ for all $i > n + 1$. This implies $m = k$.
- If $k = n + 1$, then $\operatorname{Ext}^i_A(A/I, M) \cong \operatorname{Ext}^i_A(A/I, U)$ for all $i > n + 1$. This implies $m \leq n$.
- If $k = n$, then $\operatorname{Ext}^i_A(A/I, M) \cong 0$ for all $i > n$. Moreover, $\operatorname{Ext}^n_A(A/I, M) \ncong 0$, since $\operatorname{Ext}^n_A(A/I, N) \ncong 0$ and $\operatorname{Ext}^n_A(A/I, U) \cong 0$. This implies $m = n = k$.

□

Proposition 14.3. *Let A be a Noetherian ring, I, J ideals of A, and M a finite A-module. Then*

1. *$grade(I, M) = inf\{depth M_{\mathfrak{p}} \mid \mathfrak{p} \supset I\}$.*
2. *$grade(I, M) = grade(\sqrt{I}, M)$,*
3. *$grade(I \cap J, M) = min\{grade(I, M), grade(J, M)\}$*
4. *If $\mathbf{x} = x_1, \ldots, x_n$ is an M-sequence in I, then $grade(I/\langle \mathbf{x} \rangle, M/\mathbf{x}M) = grade(I, M/\mathbf{x}M) = grade(I, M) - n$.*
5. *If N is a finite A-module with $suppN = V(I)$, then $grade(I, M) = inf\{i \mid Ext^i_A(N, M) \neq 0\}$.*

Proof.

1. It is evident from the definition that $\operatorname{grade}(I, M) \leq \operatorname{grade}(\mathfrak{p}, M) \leq \operatorname{depth} M_{\mathfrak{p}}$ for $\mathfrak{p} \supset I$. Suppose $IM \neq M$ and choose a maximal M-sequence $\mathbf{x}$ in I. Since I consists of zero-divisors of $M/\mathbf{x}M$, there exists $\mathfrak{p} \in \operatorname{Ass}(M/\mathbf{x}M)$ with $\mathfrak{p} \supset I$. Since $\mathfrak{p}A_{\mathfrak{p}} \in \operatorname{Ass}(M/\mathbf{x}M)_{\mathfrak{p}}$ and $(M/\mathbf{x}M)_{\mathfrak{p}} \cong M_{\mathfrak{p}}/\mathbf{x}M_{\mathfrak{p}}$, the ideal $\mathfrak{p}A_{\mathfrak{p}}$ consists of zero-divisors of $M_{\mathfrak{p}}/\mathbf{x}M_{\mathfrak{p}}$, and $\mathbf{x}$ (as a sequence in $A_{\mathfrak{p}}$) is a maximal $M_{\mathfrak{p}}$-sequence.
2. Factor I into its primary decomposition $I = Q_1 \cap Q_2 \cap \cdots \cap Q_k$. Then $\sqrt{I} = \sqrt{Q_1} \cap \sqrt{Q_2} \cap \cdots \cap \sqrt{Q_k}$. Any prime $\mathfrak{p}$ which contains I, must contain one of the $\sqrt{Q_i}$, and therefore must contain $\sqrt{I}$.

3. Factor I and J into their primary decompositions $I = Q_1 \cap Q_2 \cap \cdots \cap Q_k$ and $J = P_1 \cap P_2 \cap \cdots \cap P_\ell$ with corresponding primes $\mathfrak{q}_1, \mathfrak{q}_2 \ldots, \mathfrak{q}_k$ and $\mathfrak{p}_1, \mathfrak{p}_2, \ldots \mathfrak{p}_\ell$ respectively. For similar reasons as above, we must have $\mathrm{grade}(I \cap J, M) = \mathrm{depth} M_{\mathfrak{p}}$ for some $\mathfrak{p} \in \{\mathfrak{q}_1, \mathfrak{q}_2 \ldots, \mathfrak{q}_k, \mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_\ell\}$.

4. Set $\overline{A} = A/\langle \mathbf{x} \rangle$, $\overline{I} = I/\langle \mathbf{x} \rangle$, and $\overline{M} = M/\mathbf{x}M$. First observe that $IM = M \iff I\overline{M} = \overline{M} \iff \overline{IM} = \overline{M}$. Furthermore, $y_1, \ldots, y_n \in I$ form an $\overline{M}$-sequence if and only if $\overline{y}_1, \ldots, \overline{y}_n \in \overline{I}$ form such a sequence. This shows that $\mathrm{grade}(I/\langle \mathbf{x} \rangle, M/\mathbf{x}M) = \mathrm{grade}(I, M/\mathbf{x}M)$.

□

Let $(A, \mathfrak{m})$ be Noetherian local and M a finite A-module. All the minimal elements of $\mathrm{Supp}M$ belong to $\mathrm{Ass}M$. Therefore if $x \in \mathfrak{m}$ is an M-regular element, then $x \notin \mathfrak{p}$ for all minimal elements of $\mathrm{Supp}M$: Suppose $x \in \mathfrak{p}$ where $\mathfrak{p} = 0 : m$ for some nonzero $m \in M$. Then $x \in \mathfrak{p}$ implies $xm = 0$, which is a contradiction since x is M-regular. Therefore $\dim M/xM \leq \dim M - 1$: A longest chain containing $\mathrm{Ann}M$ must start with a minimal prime of $\mathrm{Supp}M$, but a longest chain containing $\mathrm{Ann}M \cup \langle x \rangle$ does not start with a minimal prime of $\mathrm{Supp}M$.

Proposition 14.4. *Let $(A, \mathfrak{m})$ be Noetherian local and $M \neq 0$ a finite A-module. Then $\mathrm{depth}M \leq \dim A/\mathfrak{p}$ for all $\mathfrak{p} \in \mathrm{Ass}M$.*

Lemma 14.5. *Let A be a Noetherian ring, M a finitely generated A-module, and $I \subset A$ an ideal with $IM \neq M$. Then the following are equivalent:*

1. *$\mathrm{Ext}^i_A(N, M) = 0$ for all $i < n$ and all finitely generated A-modules N with $\mathrm{supp}(N) \subset V(I)$.*

2. *$\mathrm{Ext}^i_A(A/I, M) = 0$ for all $i < n$.*

3. *$\mathrm{Ext}^i_A(N, M) = 0$ for all $i < n$ and some finitely generated A-module N with $\mathrm{supp}(N) = V(I)$.*

4. *I contains an M-sequence of length n.*

Proof. (1) implies (2) is obvious since $\mathrm{supp}(A/I) = V(I)$. Also, (2) implies (3) is obvious since A/I is some finitely generated A-module with $\mathrm{supp}(A/I) = V(I)$. To prove (3) implies (4), let $n > 0$ and assume first that I contains only zero divisors of M, that is, I is contained in an associated prime ideal $\mathfrak{p} = 0 : m$, where m is some nonzero element in M. Then the map $A/\mathfrak{p} \to M$, defined by $1 \mapsto m$, is injective. Localizing a $\mathfrak{p}$, we obtain that $\mathrm{Hom}_{A_\mathfrak{p}}(k, M_\mathfrak{p}) \neq 0$, where $k = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$. Now $\mathfrak{p} \in V(I) = \mathrm{supp}(N)$, that is, $N_\mathfrak{p} \neq 0$, and hence, $N_\mathfrak{p}/\mathfrak{p}N_\mathfrak{p} = N \otimes_A k \neq 0$ (Lemma of Nakayama). This implies that $\mathrm{Hom}_k(N \otimes_A k, k) \neq 0$ and, therefore, we have a non-trivial $A_\mathfrak{p}$-linear map

$$N_\mathfrak{p} \to N \otimes_A k \to k \to M_\mathfrak{p},$$

that is, $\mathrm{Hom}(N_\mathfrak{p}, M_\mathfrak{p}) \neq 0$. This implies that $\mathrm{Hom}_A(N, M) \neq 0$, which contradicts (3) for $i = 0$. So we proved that I contains an M-regular element f. By assumption, $M/IM \neq 0$, hence if $n = 1$ we are done. If $n > 1$, then we obtain from the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r, "f"] & M \arrow[r] & M/fM \arrow[r] & 0 \end{tikzcd}$$

that $\mathrm{Ext}^i_A(N, M/fM) = 0$ for $i < n - 1$. Using induction, this implies that I contains an (M/fM)-regular sequence $f_2, \ldots, f_n$.

To prove (4) implies (1), let $f_1, \ldots, f_n \in I$ be an M-sequence and consider again the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r, "f_1"] & M \arrow[r] & M/f_1M \arrow[r] & 0 \end{tikzcd}$$

Applying the function $\mathrm{Ext}^i_A(N, -)$ to this sequence gives the exact sequence

$$\begin{tikzcd} \cdots \arrow[r] & \mathrm{Ext}^i_A(N, M) \arrow[r, "f_1"] & \mathrm{Ext}^i_A(N, M) \arrow[r] & \mathrm{Ext}^i_A(N, M/f_1M) \arrow[r] & \cdots \end{tikzcd}$$

If $n = 1$, then we consider the first part of this sequence

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Hom}_A(N, M) \arrow[r, "f_1"] & \mathrm{Hom}_A(N, M) \end{tikzcd}$$

If $n > 1$, then we use induction to obtain $\mathrm{Ext}^i_A(N, M/f_1M) = 0$ for $i < n - 1$. This implies

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Ext}^i_A(N, M) \arrow[r, "f_1"] & \mathrm{Ext}^i_A(N, M) \end{tikzcd}$$

is exact for $i < n$. Now $\mathrm{Ext}^i_A(N, M)$ is annihilated by elements of $\mathrm{Ann}(N)$. On the other hand, by assumption, we have

$$\mathrm{supp}(N) = V(\mathrm{Ann}(N)) \subset V(I).$$

This implies that $I \subset \sqrt{\mathrm{Ann}(N)}$. Therefore, a sufficiently large power of f_1 annihilates $\mathrm{Ext}^i_A(N, M)$. But we already saw that f_1 is a nonzerodivisor for $\mathrm{Ext}^i_A(N, M)$ and, consequently, $\mathrm{Ext}^i_A(N, M) = 0$ for $i < n$. □

14.2 Koszul Complex and Depth

This subsection is for readers who are familiar with tools and techniques from homological algebra.

Theorem 14.6. *Let R be a Noetherian ring, let $I = \langle x_1, \ldots, x_n \rangle = \langle \underline{x} \rangle$ an ideal of R, and let M a finitely-generated R-module such that $M \neq IM$. Set $\delta = sup\{i \mid \mathrm{H}_i(\underline{x}, M) \neq 0\}$. Then all maximal M-sequences in I have length $n - \delta$. In particular,*

$$\mathrm{depth}(I, M) = n - \sup\{i \mid \mathrm{H}_i(\underline{x}, M) \neq 0\}.$$

Proof. First suppose that every element in I is a zerodivisor for M. Then I is contained in an associated prime of M, say $\mathfrak{p}$ where $\mathfrak{p} = 0 : u$ for some nonzero $u \in M$. In particular, we have $Iu = 0$, hence $u \in 0 :_M I = \mathrm{H}_n(\underline{x}, M)$. It follows that $\mathrm{H}_n(\underline{x}, M) \neq 0$, so $\delta = n$. Thus every maximal M-sequence has length $0 = n - \delta$ in this case.

Now suppose that $y_1, \ldots, y_q \in I$ is a maximal M-sequence in I. We shall prove $\delta = n - q$ by induction on q. The base case $q = 0$ was shown above, so assume that $q > 0$. Consider the short exact sequence of R-modules

$$0 \to M \xrightarrow{y_1} M \to M/y_1M \to 0.$$

This short exact sequence of R-modules induces a short exact sequence of R-complexes

$$0 \to \mathcal{K}(\underline{x}, M) \xrightarrow{y_1} \mathcal{K}(\underline{x}, M) \to \mathcal{K}(\underline{x}, M/y_1M) \to 0.$$

Taking the long exact sequence in homology and using the fact that y_1 kills $\mathrm{H}(\underline{x}, M)$, we obtain following short exact sequence of R-modules

$$0 \to \mathrm{H}_{i+1}(\underline{x}, M) \to \mathrm{H}_{i+1}(\underline{x}, M/y_1M) \to \mathrm{H}_i(\underline{x}, M) \to 0 \tag{60}$$

for all $i \in \mathbb{Z}$. Note that $y_2, \ldots, y_q$ is a maximal M/y_1M sequence. Also note that $I(M/y_1M) \neq M/y_1M$ since $M \neq IM$. Thus we have by induction that $\mathrm{H}_{i+1}(\underline{x}, M/y_1M) = 0$ for all $i > n - (q-1)$ and $\mathrm{H}_{n-q+1}(\underline{x}, M/y_1M) \neq 0$. Using this together with the short exact sequence (60) gives us $\mathrm{H}_i(\underline{x}, M) = 0$ for all $i > n - q$ and $\mathrm{H}_{n-q}(\underline{x}, M) \neq 0$. In other words, $\delta = n - q$. □

Remark. It's worth pointing out that we obtain slightly more than what's stated in the theorem above; namely from (60) we obtain $\mathrm{H}_{\delta+1}(\underline{x}, M/y_1M) \cong \mathrm{H}_\delta(\underline{x}, M)$. An inductive argument then gives us

$$\begin{aligned}
\mathrm{H}_\delta(\underline{x}, M) &\cong \mathrm{H}_n(\underline{x}, M/\underline{y}M) \\
&\cong 0 :_{M/\underline{y}M} I \\
&= \mathrm{Hom}_R(R/I, M/\underline{y}M) \\
&\cong \mathrm{Ext}^0_R(R/I, M/\underline{y}M) \\
&\cong \mathrm{Ext}^q_R(R/I, M).
\end{aligned}$$

The last isomorphism will be explained in the next section.

Theorem 14.7. *Let M be a nonzero R-module and let $\underline{x} = x_1, \ldots, x_n$ be a sequence in R.*

1. *If $\underline{x}$ is an M-sequence, then $\mathrm{H}_i(\underline{x}, M) = 0$ for all $i > 0$.*

2. *Suppose $(R, \mathfrak{m})$ is local with $\underline{x} \in \mathfrak{m}$. If M is finitely-generated and $\mathrm{H}_1(\underline{x}, M) = 0$, then $\underline{x}$ is an M-sequence.*

Proof. 1. We prove this by induction on n. For the base case, suppose $n = 1$. Then since $\mathrm{H}_1(x_1, M) = 0 :_M x_1$, we see that $\mathrm{H}_1(x_1, M) = 0$ if and only if x_1 is M-regular. This establishes the base case. For the induction step, assume $n > 1$ and that we've shown the theorem to be true for all M-sequences of length $m < n$. Let $\underline{x} = x_1, \ldots, x_n$ be an M-sequence of length n and let $\underline{x}' = x_1, \ldots, x_{n-1}$ be an M-sequence of length $n-1$ obtained by removing x_n from $\underline{x}$. The multiplication by x_n map from $\mathcal{K}(\underline{x}', M)$ to itself induces a short exact sequence of R-complexes

$$0 \to \mathcal{K}(\underline{x}', M) \to \mathrm{C}(x_n) \to \Sigma\mathcal{K}(\underline{x}', M) \to 0, \tag{61}$$

where $\mathrm{C}(x_n)$ is the mapping cone with respect to the multiplication by x_n map. Since $\mathrm{C}(x_n) \cong \mathcal{K}(\underline{x}, M)$ and since the connecting map induced by (61) is just multiplication by x_n, we we obtain a long exact sequence in homology

$$\cdots \to \mathrm{H}_i(\underline{x}', M) \to \mathrm{H}_i(\underline{x}, M) \to \mathrm{H}_{i-1}(\underline{x}', M) \xrightarrow{x_n} \mathrm{H}_{i-1}(\underline{x}', M) \to \cdots. \tag{62}$$

Since $\underline{x}'$ is an M-sequence of length $n-1$, we have by induction $\mathrm{H}_i(\underline{x}', M) = 0$ for all $i > 0$. This together with the long exact sequence in homology (62) implies $\mathrm{H}_i(\underline{x}, M) = 0$ for all $i > 1$. The vanishing of $\mathrm{H}_1(\underline{x}, M)$ follows from taking $i = 1$ in (62) together with the fact that $\mathrm{H}_0(\underline{x}', M) \cong M/x'M$ and x_n is $(M/\underline{x}'M)$-regular.

2. We prove this by induction on n. The base case $n = 1$ is proved similarly as in the base case in 1. For the induction step, suppose that we've shown the theorem to be true for all sequences in $\mathfrak{m}$ of length $m < n$ for some $n > 1$. Let $\underline{x} = x_1, \dots, x_n \in \mathfrak{m}$ be a sequence in $\mathfrak{m}$ of length n and suppose that $\mathrm{H}_1(\underline{x}, M) = 0$. As in 1, let let $\underline{x}' = x_1, \dots, x_{n-1}$ be a sequence in $\mathfrak{m}$ of length $n-1$ obtained by removing x_n from $\underline{x}$. By the same argument as in 1, we obtain a long exact sequence in homology

$$\cdots \to \mathrm{H}_{i+1}(\underline{x}, M) \to \mathrm{H}_i(\underline{x}', M) \xrightarrow{x_n} \mathrm{H}_i(\underline{x}', M) \to \mathrm{H}_i(\underline{x}, M) \to \cdots. \tag{63}$$

In particular, since $\mathrm{H}_1(\underline{x}, M) = 0$, we have a surjective map $\mathrm{H}_1(\underline{x}', M) \xrightarrow{x_n} \mathrm{H}_1(\underline{x}', M)$. By Nakayama's lemma, this implies $\mathrm{H}_1(\underline{x}', M) = 0$. Using induction, we obtain that $\underline{x}'$ is an M-sequence. Finally, using the fact that $\mathrm{H}_1(\underline{x}, M) = 0$ together with the long exact sequence in (63) we see that $\mathrm{H}_0(\underline{x}', M) \xrightarrow{x_n} \mathrm{H}_0(\underline{x}', M)$ is injective. Since $\mathrm{H}_0(\underline{x}', M) \cong M/x'M$, it follows that $\underline{x}$ is an M-sequence. □

Corollary. *Let $(R, \mathfrak{m})$ be a local ring, let $I = \langle x_1, \dots, x_n \rangle = \langle \underline{x} \rangle$ be a proper ideal of R, and let M be a nonzero finitely-generated R-module. Suppose $\underline{y} = y_1, \dots, y_n$ is an M-sequence of length n contained in I. Then $\underline{x}$ is an M-sequence.*

Proof. Since $\underline{y}$ is an M-sequence of length n contained in the ideal I which is generated by n elements, we must have $\operatorname{depth}(I, M) = n$. In particular, this implies $\mathrm{H}_1(\underline{x}, M) = 0$. Therefore $\underline{x}$ must be an M-sequence, by Theorem (14.7).

□

14.3 Ext and Depth

Proposition 14.5. *Let R be a Noetherian local ring, let N be a finitely-generated R-module, and let I be an ideal of R such that $IN \neq N$, and let n be a positive integer. Then the following are equivalent:*

1. *$\operatorname{Ext}^i_R(M, N) = 0$ for all $i < n$ and all finitely-generated R-modules M with $\operatorname{Supp} M \subseteq \mathrm{V}(I)$.*
2. *$\operatorname{Ext}^i_R(R/I, N) = 0$ for all $i < n$.*
3. *$\operatorname{Ext}^i_R(M, N) = 0$ for all $i < n$ for some finitely-generated R-module M with $\operatorname{Supp} M = \mathrm{V}(I)$.*
4. *I contains an N-sequence of length n.*

Remark. Note that if M is a finitely-generated R-module, then $\operatorname{Supp} M = \mathrm{V}(\operatorname{Ann} M)$. Thus we have several equivalent statements:

$$\begin{aligned} M_{\mathfrak{p}} \neq 0 \text{ implies } \mathfrak{p} \supseteq I \text{ for all } \mathfrak{p} \in \operatorname{Spec} R &\iff \operatorname{Supp} M \subseteq \mathrm{V}(I) \\ &\iff \mathrm{V}(\operatorname{Ann} M) \subseteq \mathrm{V}(I) \\ &\iff \sqrt{\operatorname{Ann} M} \supseteq \sqrt{I} \\ &\iff \sqrt{\operatorname{Ann} M} \supseteq I \\ &\iff \text{if } x \in I \text{ then } x^k M = 0 \text{ for some } k \in \mathbb{N}. \end{aligned}$$

Proof. That 1 implies 2 implies 3 is clear. Let us prove 3 implies 4. Assume for a contradiction that I consists of zero divisors of N. We will show $\operatorname{Hom}_R(M, N) \neq 0$ which will contradict 3 by taking $i = 0$. Since I consists of zero divisors of N, we see that

$$I \subseteq \bigcup_{\mathfrak{p} \in \operatorname{Ass} N} \mathfrak{p}.$$

It follows from the fact that $\operatorname{Ass} N$ is finite and prime avoidance that I be contained in some associated prime of N, say $I \subseteq \mathfrak{p}$. It follows that there is an injective R-linear map $R/\mathfrak{p} \rightarrowtail N$. By localizing at $\mathfrak{p}$ we obtain an injective $R_{\mathfrak{p}}$-linear map $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} \rightarrowtail N_{\mathfrak{p}}$. Also $M_{\mathfrak{p}} \neq 0$ since $\mathfrak{p} \in \mathrm{V}(I) = \operatorname{Supp} M$, and by Nakayama's lemma, we must also have $M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}} \neq 0$. Note that $M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}}$ is just an $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$-vector space, thus we can certainly find a surjective

$(R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p})$-linear map $M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p} \twoheadrightarrow R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$, and hence an $R_\mathfrak{p}$-linear map when viewing these as $R_\mathfrak{p}$-modules. Altogether we obtain a sequence of $R_\mathfrak{p}$-linear maps

$$M_\mathfrak{p} \twoheadrightarrow M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p} \twoheadrightarrow R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} \rightarrowtail N_\mathfrak{p}.$$

In particular, we see that

$$\begin{aligned} 0 &\neq \operatorname{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}) \\ &= \operatorname{Hom}_R(M, N)_\mathfrak{p}, \end{aligned}$$

which is a contradiction.

Thus I must contain an N-regular element, say $x_1 \in I$. By assumption, $N/IN \neq 0$, hence if $n = 1$, then we are done. Otherwise, assume $n > 1$. From the exact sequence

$$0 \to N \xrightarrow{x_1} N \to N/x_1N \to 0$$

we obtain a long exact sequence in Ext

$$\cdots \to \operatorname{Ext}_R^i(M, N) \to \operatorname{Ext}_R^i(M, N/x_1N) \to \operatorname{Ext}_R^{i+1}(M, N) \to \cdots,$$

which implies $\operatorname{Ext}_R^i(M, N/x_1N) = 0$ for all $i < n - 1$. Using induction, this implies that I contains an (N/x_1N)-sequence of length $n - 1$, say $x_2, \dots, x_n$. In particular, we see that $x_1, x_2, \dots, x_n$ is an N-sequence of length n.

Now we prove 4 implies 1. Suppose M is a finitely-generated R-module with $\operatorname{Supp} M \subseteq \mathrm{V}(I)$. We will prove by induction on n that for any finitely-generated R-module N, if I contains an N-sequence of length n, then $\operatorname{Ext}_R^i(M, N) = 0$ for all $i < n$. For the base case $n = 1$, suppose $x \in I$ is an N-regular element. In this case, we just need to show that $\operatorname{Hom}_R(M, N) = 0$. Note that since M is finitely-generated, we have $\operatorname{Supp} M = \mathrm{V}(\operatorname{Ann} M)$. Thus we we see that $\mathrm{V}(\operatorname{Ann} M) = \operatorname{Supp} M \subseteq \mathrm{V}(I)$, and this implies $\sqrt{\operatorname{Ann} M} \supseteq I$. In particular, some power of x kills M, say $x^k M = 0$. Thus if $\varphi \in \operatorname{Hom}_R(M, N)$, then for all $u \in M$, we have

$$\begin{aligned} x^k \varphi(u) &= \varphi(x^k u) \\ &= \varphi(0) \\ &= 0, \end{aligned}$$

which implies $\varphi(u) = 0$ since x is N-regular. Thus $\varphi = 0$ and hence $\operatorname{Hom}_R(M, N) = 0$.

For the induction step, suppose $n > 1$ and suppose that for any finitely-generated R-module N' such that I contains an N'-sequence of length $n - 1$, we have $\operatorname{Ext}_R^i(M, N') = 0$ for all $i < n - 1$. Let N be an R-module such that I contains an N-sequence of length n, say $x_1, \dots, x_n \in I$. Again, since $\sqrt{\operatorname{Ann} M} \supseteq I$, some power of x_1 kills M, say $x_1^k M = 0$. From the exact sequence

$$0 \to N \xrightarrow{x_1^k} N \to N/x_1^kN \to 0$$

we obtain a long exact sequence in Ext

$$\cdots \to \operatorname{Ext}_R^{i-1}(M, N/x_1^kN) \to \operatorname{Ext}_R^i(M, N) \xrightarrow{\cdot x_1^k} \operatorname{Ext}_R^i(M, N) \to \operatorname{Ext}_R^i(M, N/x_1^kN) \to \cdots. \tag{64}$$

Note that x_1^k kills $\operatorname{Ext}_R(M, N)$. To see this, let (E, d) be an injective resolution of N over R. Then for any $\varphi \in \operatorname{Hom}_R^\star(M, E)$, we have $x_1^k \varphi = 0$ by the same argument as in the base case. It follows that x_1^k kills $\operatorname{Hom}_R^\star(M, E)$. In particular, we have

$$\begin{aligned} x_1^k \operatorname{Ext}_R(M, N) &= x_1^k \mathrm{H}(\operatorname{Hom}_R^\star(M, E)) \\ &\rightarrowtail \mathrm{H}(x_1^k \operatorname{Hom}_R^\star(M, E)) \\ &= \mathrm{H}(0) \\ &= 0. \end{aligned}$$

Thus x_1^k kills $\operatorname{Ext}_R(M, N)$ as claimed. It follows that the long exact sequence in homology (64) breaks up into short exact sequences of R-modules

$$0 \to \operatorname{Ext}_R^i(M, N) \to \operatorname{Ext}_R^i(M, N/x_1^kN) \to \operatorname{Ext}_R^{i+1}(M, N) \to 0 \tag{65}$$

for all $i \in \mathbb{Z}$. Now recall that if $x_1, x_2, \dots, x_n$ is an N-sequence, then $x_1^k, x_2, \dots, x_n$ is also an N-sequence. In particular, I contains an (N/x_1^kN)-sequence of length $n - 1$. Thus, using induction (with $N' = N/x_1^kN$), we have $\operatorname{Ext}_R^{i+1}(M, N/x_1^kN) = 0$ for all $i + 1 < n$. Using this together with the short exact sequence (65) gives us $\operatorname{Ext}_R^i(M, N) = 0$ for all $i < n$. □

Keep the same notation as in Proposition (14.5). Then the proposition above tells us that

$$\operatorname{depth}(I,N) = \inf\{i \mid \operatorname{Ext}^i_R(R/I,N) \neq 0\}.$$

Indeed, denote $q = \operatorname{depth}(I,N)$. Then I contains an N-sequence of length q which implies $\operatorname{Ext}^i_R(R/I,N) = 0$ for all $i < q$. On the other hand, any maximal N-sequence contained in I must also have length q, so we must have $\operatorname{Ext}^q_R(R/I,N) \neq 0$ (otherwise there would be an N-sequence in I of length $q+1$). In fact, we get more than just this from Proposition (14.5). Indeed, if $\sqrt{I}N \neq N$, then Proposition (14.5) also implies

$$\begin{aligned}\operatorname{depth}(I,N) &= \inf\{i \mid \operatorname{Ext}^i_R(R/\sqrt{I},N) \neq 0\}.\\ &= \operatorname{depth}(\sqrt{I},N).\end{aligned}$$

More generally, if J is any ideal of R such that $\sqrt{J} = \sqrt{I}$, then $\operatorname{depth}(I,N) = \operatorname{depth}(J,N)$.

Note also that just as in the Koszul case, we obtain more than what's stated in the theorem above. In particular, denote $y = x_1^k$ in (65) and let $q = \operatorname{depth}(I,N)$. Then (65) gives us an isomorphism

$$\operatorname{Ext}^q_R(M,N) \cong \operatorname{Ext}^{q-1}_R(M,N/yN).$$

This explains Remark (14.2) in the last section.

15 Cohen-Macaulay Modules

Definition 15.1. Let $(R,\mathfrak{m})$ be a Noetherian local ring and let M be a finitely-generated R-module. We say M is a **Cohen-Macaulay module** if $M = 0$ or $M \neq 0$ and

$$\operatorname{depth} M = \dim M.$$

If $\operatorname{depth} M = \dim R$, then M is called **maximal Cohen-Macaulay**. We say R is a **Cohen-Macaulay ring** if it is a Cohen-Macaulay R-module.

Lemma 15.1. *Let $(R,\mathfrak{m})$ be a Noetherian local ring and let M and N be nonzero finitely-generated R-modules. Then $\operatorname{Ext}^i_R(M,N) \cong 0$ for all $i < \operatorname{depth} N - \dim M$.*

Proof. Denote $q = \operatorname{depth} N$ and $d = \dim M$. We prove the lemma by induction on d. If $d = 0$, then $\sqrt{\operatorname{Ann} M} = \mathfrak{m}$. Therefore $\operatorname{Ext}^i_R(M,N) \cong 0$ for all $i < q$ by Lemma (15.2). Now assume that $d > 0$. Choose a filtration of M, say

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

wher $M_j/M_{j+1} \cong R/\mathfrak{p}_j$ for suitable prime ideals $\mathfrak{p}_j$. Now it is sufficient to prove $\operatorname{Ext}^i_R(M_j/M_{j+1},N) \cong 0$ for all j and $i < q - d$ because this implies $\operatorname{Ext}^i_R(M,N) \cong 0$. Since $\dim(M_j/M_{j+1}) \leq \dim M$ for all j, we may as well assume that $M = R/\mathfrak{p}$ for a prime ideal $\mathfrak{p}$. Since $\dim(R/\mathfrak{p}) > 0$, we must have $\mathfrak{m} \supset \mathfrak{p}$ where the inclusion containment is proper. Therefore we can choose an $x \in \mathfrak{m}$ which is not in $\mathfrak{p}$. Consider the short exact sequence

$$0 \to R/\mathfrak{p} \xrightarrow{x} R/\mathfrak{p} \to R/\langle \mathfrak{p}, x\rangle \to 0. \tag{66}$$

This short exact sequence (66) gives rise to the following long exact sequence in Ext

$$\cdots \to \operatorname{Ext}^i_R(R/\langle \mathfrak{p},x\rangle,N) \to \operatorname{Ext}^i_R(R/\mathfrak{p},N) \xrightarrow{x} \operatorname{Ext}^i_R(R/\mathfrak{p},N) \to \operatorname{Ext}^{i+1}_R(R/\langle \mathfrak{p},x\rangle,N) \to \cdots \tag{67}$$

Since $\dim(R/\langle \mathfrak{p},x\rangle) < d$, we obtain by induction on d that $\operatorname{Ext}^i_R(R/\langle \mathfrak{p},x\rangle,N) \cong 0$ for all $i < q - d + 1$. Using this together with the long exact sequence (67), we find find that the map

$$\operatorname{Ext}^i_R(R/\mathfrak{p},N) \xrightarrow{x} \operatorname{Ext}^i_R(R/\mathfrak{p},N)$$

is surjective for all $i < q - d$ which implies $\operatorname{Ext}^i_R(R/\mathfrak{p},N) \cong 0$ for all $i < q - d$ by Nakayama's lemma. □

Lemma 15.2. *Let $(A,\mathfrak{m})$ be a local Cohen-Macaulay ring of dimension d, M be a maximal Cohen-Macaulay module of finite injective dimension, and N a finitely generated module of depth e. Then*

$$Ext^i_A(N,M) = 0 \textit{ for } i > depth(M) - depth(N) = d - e.$$

Proof. We do induction on e. □

Proposition 15.1. *Let R be a local Cohen-Macaulay ring of dimension d, and let N be a maximal Cohen-Macaulay module of finite injective dimension.*

1. *If M is a finitely generated R-module of depth q, then $\operatorname{Ext}^i_R(M,N) \cong 0$ for $i > d-q$.*
2. *If x is a nonzerodivisor on M, then x is a nonzerodivisor on $Hom_A(N,M)$. If N is also a maximal Cohen-Macaulay module, then*
$$Hom_A(N,M)/xHom_A(N,M) \cong Hom_{A/x}(N/xN, M/xM)$$
by the homomorphism taking the class of a map $\varphi : N \to M$ to the map $N/xN \to M/xM$ induced by φ.

Proof. We do induction on q. By Proposition (16.7), the injective dimension of N is d, so that $\operatorname{Ext}^i_R(M,N) \cong 0$ for any M if $i > d$. This gives the case $e = 0$. Now suppose $e > 0$, and let x be a nonzerodivisor on N that lies in the maximal ideal of A. From the short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r, "\cdot x"] & N \arrow[r] & N/xN \arrow[r] & 0 \end{tikzcd}$$

we get a long exact sequence

$$\begin{tikzcd} \cdots \arrow[r] & \operatorname{Ext}^j_A(N,M) \arrow[r, "\cdot x"] & \operatorname{Ext}^j_A(N,M) \arrow[r] & \operatorname{Ext}^{j+1}_A(N/xN,M) \arrow[r] & \cdots \end{tikzcd}$$

The module N/xN has depth $e-1$, so by induction $\operatorname{Ext}^{j+1}_A(N/xN,M)$ vanishes if $j+1 > d-(e-1)$, that is, if $j > d-e$. By Nakayama's lemma, $\operatorname{Ext}^j_A(N,M)$ vanishes if $j > d-e$.

1. We do induction on e. By Proposition (16.7), the injective dimension of M is d, so that $\operatorname{Ext}^j_A(N,M) = 0$ for any N if $j > d$. This gives the case $e = 0$. Now suppose $e > 0$, and let x be a nonzerodivisor on N that lies in the maximal ideal of A. From the short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r, "\cdot x"] & N \arrow[r] & N/xN \arrow[r] & 0 \end{tikzcd}$$

we get a long exact sequence

$$\begin{tikzcd} \cdots \arrow[r] & \operatorname{Ext}^j_A(N,M) \arrow[r, "\cdot x"] & \operatorname{Ext}^j_A(N,M) \arrow[r] & \operatorname{Ext}^{j+1}_A(N/xN,M) \arrow[r] & \cdots \end{tikzcd}$$

The module N/xN has depth $e-1$, so by induction $\operatorname{Ext}^{j+1}_A(N/xN,M)$ vanishes if $j+1 > d-(e-1)$, that is, if $j > d-e$. By Nakayama's lemma, $\operatorname{Ext}^j_A(N,M)$ vanishes if $j > d-e$.

2. From the short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r, "\cdot x"] & M \arrow[r] & M/xM \arrow[r] & 0 \end{tikzcd}$$

we derive a long exact sequence beginning

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{Hom}_A(N,M) \arrow[r, "\cdot x"] & \operatorname{Hom}_A(N,M) \arrow[r] & \operatorname{Hom}_A(N,M/xM) \arrow[r] & \operatorname{Ext}^1_A(N,M) \arrow[r] & \cdots \end{tikzcd}$$

Thus x is a nonzerodivisor on $\operatorname{Hom}_A(N,M)$. If N is a maximal Cohen-Macaulay module then $\operatorname{depth}(N) = d$, so $\operatorname{Ext}^1_A(N,M) = 0$ by part 1. Every homomorphism $N \to M/xM$ factors uniquely through N/xN, so $\operatorname{Hom}_A(N,M/xM) = \operatorname{Hom}_A(N/xN,M/xM)$. The short exact sequence above thus becomes

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{Hom}_A(N,M) \arrow[r, "\cdot x"] & \operatorname{Hom}_A(N,M) \arrow[r] & \operatorname{Hom}_A(N/xN,M/xM) \arrow[r] & 0 \end{tikzcd}$$

Since $\operatorname{Hom}_A(M/xM,N/xN) = \operatorname{Hom}_{A/x}(N/xN,M/xM)$, this proves part 2.

□

Proposition 15.2. *Let $(A,\mathfrak{m})$ be a Noetherian local ring and let M be a finitely generated A-module. Then $dim(A/\mathfrak{p}) \geq depth(M)$ for all $\mathfrak{p} \in Ass(M)$.*

Proof. Let $\mathfrak{p} \in \operatorname{Ass}(M)$, that is, $\mathfrak{p} = 0 : m$ for some nonzero m in M. This implies that $\operatorname{Hom}(A/\mathfrak{p},M) \neq 0$, because $1 \mapsto m$ defines a non-trivial homomorphism. Hence, by Lemma (15.2), we obtain $0 \geq \operatorname{depth}(M) - \dim(A/\mathfrak{p})$. □

Theorem 15.3. *Let $(A,\mathfrak{m})$ be a Noetherian local ring, $M \neq 0$ a finitely generated A-module, and $x \in A$.*

1. *Let M be Cohen-Macaulay. Then $dim(A/\mathfrak{p}) = dim(M)$ for all $\mathfrak{p} \in Ass(M)$.*
2. *If $dim(M/xM) = dim(M) - 1$, then x is M-regular.*
3. *Let $x_1, \ldots, x_r \in \mathfrak{m}$ be an M-sequence. Then M is Cohen-Macaulay if and only if $M/\langle x_1, \ldots, x_r \rangle M$ is Cohen-Macaulay.*
4. *If M is Cohen-Macaulay, then $M_\mathfrak{p}$ is Cohen-Macualay for all prime ideal $\mathfrak{p}$ and $depth(\mathfrak{p}, M) = depth_{A_\mathfrak{p}}(M_\mathfrak{p})$ if $M_\mathfrak{p} \neq 0$.*

Proof.

1. For all associated primes $\mathfrak{p}$ of M, we have
$$\operatorname{depth}(M) \leq \dim(A/\mathfrak{p}) \leq \dim(M).$$
Thus $\dim(A/\mathfrak{p}) = \dim(M)$ for all $\mathfrak{p} \in \operatorname{Ass}(M)$ since $\operatorname{depth}(M) = \dim(M)$.
2. Observe that
$$\begin{aligned} \dim(A/\langle x, \operatorname{Ann}(M) \rangle) &= \dim(M/xM) \\ &< \dim(M) \\ &= \dim(A/\mathfrak{p}) \end{aligned}$$
implies $x \notin \mathfrak{p}$ for all $\mathfrak{p} \in \operatorname{Ass}(M)$. Therefore x is M-regular.
3. We have
$$\begin{aligned} \operatorname{depth}(M/\langle x_1, \ldots, x_r \rangle M) &= \operatorname{depth}(M) - r \\ &= \dim(M) - r \\ &= \dim(M/\langle x_1, \ldots, x_r \rangle M). \end{aligned}$$

□

15.1 Auslander-Buchsbaum Formula

We want to prove the Auslander-Buchsbaum formula, which is of fundamental importance for modules which allow a finite projective resolution. First we need a definition and a lemma.

Definition 15.2. Let $(A, \mathfrak{m})$ be a Noetherian local ring and let M be a finitely generated A-module. We say M has finite **projective dimension** if there exists an exact sequence (a free resolution)

$$0 \longrightarrow F_n \xrightarrow{\varphi_n} F_{n-1} \xrightarrow{\varphi_{n-1}} \cdots \longrightarrow F_0 \xrightarrow{\varphi_0} M \longrightarrow 0 \tag{68}$$

with finitely generated free A-modules F_i. The integer n is called the **length** of the resolution. The minimal length of a free resolution is called the **projective dimension** of M, and is denoted $\operatorname{pd}_A(M)$.

Lemma 15.4. *Let $(R, \mathfrak{m})$ be a Noetherian local ring and let*

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

be a short exact sequence of R-modules. Then

$$\operatorname{depth} M_2 \geq \min(\operatorname{depth} M_1, \operatorname{depth} M_3).$$

If the inequality is strict, then

$$\operatorname{depth} M_1 = \operatorname{depth} M_3 + 1.$$

Proof. First assume all three modules have positive depth. Observe that we can find a common nonzerodivisor $x \in \mathfrak{m}$ of M_1, M_2 and M_3. Indeed, the set of all zerodivisors of M_j is

$$\bigcup_{\mathfrak{p} \in \operatorname{Ass}(M_j)} \mathfrak{p}.$$

Assuming for a contradiction that we cannot find a common nonzerodivisor $x \in \mathfrak{m}$ of M_1,M_2, and M_3, then we would have

$$\bigcup_{\substack{\mathfrak{p} \in \operatorname{Ass}(M_j) \\ j=1,2,3}} \mathfrak{p} = \mathfrak{m}.$$

Since the number associated primes is finite, we must have $\mathfrak{m} = \mathfrak{p}$ for some $\mathfrak{p} \in \operatorname{Ass}(M_j)$ and $j \in \{1,2,3\}$, by prime avoidance. However this is a contradiction, since it would imply that every $x \in \mathfrak{m}$ is a zerodivisor for M_j. Thus we can find a common nonzerodivisor $x \in \mathfrak{m}$ of M_1, M_2, and M_3.

Since x is M_3-regular, we obtain a short exact sequence

$$0 \to M_1/xM_1 \to M_2/xM_2 \to M_3/xM_3 \to 0$$

Since depth drops by one when we divide by x, we see that the proof of the lemma can be reduced to the case that the depth of one of the M_j is zero.

Case 1: Suppose that $\operatorname{depth} M_1 = 0$. Then $\operatorname{depth} M_2 = 0$, because any nonzerodivisor of M_2 is a nonzerodivisor of M_1. The lemma is proved in this case.

Case 2: Suppose that $\operatorname{depth} M_2 = 0$ and assume for a contradiction that $\operatorname{depth} M_1 > 0$ and $\operatorname{depth} M_3 > 0$. Let $x \in \mathfrak{m}$ be a common nonzerodivisor of M_1 and M_3. From the snake lemma we obtain that x is a nonzerodivisor for M_2 too. This is a contradiction.

Case 3: Suppose that $\operatorname{depth} M_3 = 0$. If $\operatorname{depth} M_2 > 0$, let $x \in \mathfrak{m}$ be a nonzerodivisor of M_2. This is also a nonzero divisor for M_1, and therefore $\operatorname{depth} M_1 > 0$. Using the snake lemma, we obtain an injective map

$$\ker(M_3 \xrightarrow{x} M_3) \rightarrowtail M_1/xM_1.$$

As $\operatorname{depth} M_3 = 0$, we have $\ker(M_3 \xrightarrow{x} M_3) \neq 0$. Any nonzerodivisor of M_1/xM_1 would give a nonzerodivisor of $\ker(M_3 \xrightarrow{x} M_3)$. But this is not possible, and therefore $\operatorname{depth} M_1 = 1$. □

We are now ready to state the Auslander-Buchsbaum Formula.

Theorem 15.5. *(Auslander-Buchsbaum Formula) Let $(R, \mathfrak{m})$ be a Noetherian local ring and let M be a finitely generated R-module of finite projective dimension. Then*

$$\operatorname{depth} M + \operatorname{pd}_R M = \operatorname{depth} R.$$

Proof. Denote $q_M = \operatorname{depth} M$, $q_R = \operatorname{depth} R$, and $p = \operatorname{pd}_R M$. The proof is by induction on q_R. First assume $q_R = 0$. Then $\mathfrak{m}$ consists of zerodivisors. In particular,

$$\mathfrak{m} \subseteq \bigcup_{\mathfrak{p} \in \operatorname{Ass} R} \mathfrak{p},$$

and since the number of associated primes of R is finite (R is Noetherian!), we must have $\mathfrak{m} = \mathfrak{p}$ for some associated prime by prime avoidance. Therefore, there exists a nonzero $x \in R$ such that $x\mathfrak{m} = 0$. Choose such an $x \in R$ and let (F, d) be a minimal free resolution of M over R of finite length n. If $n > 0$, then by minimality of the resolution, we have

$$\begin{aligned} \mathrm{d}_n(xF_n) &= x\mathrm{d}_n(F_n) \\ &\subseteq x\mathfrak{m}F_{n-1} \\ &= 0. \end{aligned}$$

This implies $xF_n = 0$ since d_n is injective, and thus $F_n = 0$ since F_n is free. This contradicts the minimality of the resolution. In particular, we must have $n = 0$, which implies $F_0 \cong M$. In other words, we have $p = 0$ and $q_M = q_R$.

Now we assume $q_R > 0$ and $q_M > 0$. Let $x \in \mathfrak{m}$ be a common nonzerodivisor of both M and R (such an element exists since both M and R have positive depth). Then the projective dimension is constant if we divide by x, that is,

$$\operatorname{pd}_{R/x}(M/xM) = \operatorname{pd}_R M,$$

but the depth drops by one. This is because the sequence if (F, d) is a minimal free resolution of M over R, then $(F/xF, \overline{\mathrm{d}})$ is a minimal free resolution of M/xM over R/xR as long as x is both M-regular and R-regular. It follows from the induction hypothesis, that

$$\begin{aligned} \mathrm{pd}_R\, M + \mathrm{depth}_R\, M &= \mathrm{pd}_{R/x}(M/xM) + \mathrm{depth}_{R/x}(M/xM) + 1 \\ &= \mathrm{depth}_{R/x}(R/x) + 1 \\ &= \mathrm{depth}_R\, R. \end{aligned}$$

Finally, assume $q_R > 0$ and $q_M = 0$. Then $p > 0$, because otherwise M would be free and we would have $q_M = q_R > 0$, which is a contradiction. Let

$$0 \to N \to F \to M \to 0$$

be a short exact sequence of R-modules where F is a finitely-generated free R-module and where $0 \neq N \subseteq \mathfrak{m}F$. We apply Lemma (15.4) and obtain depth $N = 1$. Therefore by the previous case, we have

$$\begin{aligned} \mathrm{depth}\, M + \mathrm{pd}_R\, M &= \mathrm{depth}\, N - 1 + \mathrm{pd}_R\, N + 1 \\ &= \mathrm{depth}\, N + \mathrm{pd}_R\, N \\ &= \mathrm{depth}\, R. \end{aligned}$$

□

Example 15.1. Let $R = K[x,y,z]_{\langle x,y,z \rangle}$ and let $I = \langle xz, yz \rangle$. The minimal free resolution of R/I over R is given by

$$\begin{tikzcd} 0 \arrow[r] & R \arrow[r, "\begin{pmatrix} -y \\ x \end{pmatrix}"] & R^2 \arrow[r, "\begin{pmatrix} xz & yz \end{pmatrix}"] & R \arrow[r] & 0 \end{tikzcd}$$

In particular, $\mathrm{pd}_R(R/I) = 2$, and hence $\mathrm{depth}(R/I) = 1$ since depth $R = 3$. On the other hand, we know that $\dim(R/I) \geq 2$, since

$$\langle \overline{x}, \overline{y}, \overline{z} \rangle \supset \langle \overline{y}, \overline{z} \rangle \supset \langle \overline{z} \rangle$$

gives a chain of prime ideals of length 2. Therefore R/I is not a Cohen-Macaulay R-module.

Example 15.2. Let $R = K[x,y,z]_{\langle x,y,z \rangle}$ and let $I = \langle xy, xz, yz \rangle$. The minimal free resolution of R/I over R is given by

$$\begin{tikzcd} 0 \arrow[r] & R^2 \arrow[r, "\begin{pmatrix} 0 & -z \\ -y & y \\ x & 0 \end{pmatrix}"] & R^3 \arrow[r, "\begin{pmatrix} xy & xz & yz \end{pmatrix}"] & R \arrow[r] & 0 \end{tikzcd}$$

So $\mathrm{pd}_R(R/I) = 2$, and hence $\mathrm{depth}(R/I) = 1$ since depth $R = 3$. We also have $\dim(R/I) = 1$, so R/I is a Cohen-Macaulay R-module.

16 Duality Canonical Modules, and Gorenstein Rings

Let K be a field and let R be a local zero-dimensional ring that is finite-dimensional as a K-algebra. If we wish to imitate the usual duality theory for vector spaces, we might at first try to work with the functor $\mathrm{Hom}_R(-, R)$. But this is often very badly behaved; for example, it does not usually preserve exact sequences, and if we do it twice we do not get the identity, that is,

$$\mathrm{Hom}_R(\mathrm{Hom}_R(M, R), R) \ncong M$$

in general. For instance, consider the following example. For instance, consider the case where $M = R/I$ where I is an ideal of R. Then since $\mathrm{Hom}_R(R/I, R) \cong \mathrm{Ann}\, I$, we have

$$\begin{aligned} \mathrm{Hom}_R(\mathrm{Hom}_R(R/I, R), R) &\cong \mathrm{Hom}_R(\mathrm{Ann}(R/I), R) \\ &= \mathrm{Hom}_R(I, R). \end{aligned}$$

The following example shows that we may not have $\mathrm{Hom}_R(I, R) \cong R/I$.

Example 16.1. Let $R = K[x,y]/\langle x^2, xy^2, y^3\rangle$ and let $I = \langle \overline{y}\rangle$. Then we have

$$\begin{aligned}\operatorname{Hom}_R(R/I, R) &\cong \operatorname{Ann} I \\ &= \langle \overline{xy}, \overline{y}^2\rangle.\end{aligned}$$

Now let's calculate $\operatorname{Hom}_R(\langle \overline{xy}, \overline{y}^2\rangle, R)$. Well any $\varphi \in \operatorname{Hom}_R(\langle \overline{xy}, \overline{y}^2\rangle, R)$ is completely determined by where it maps the generators $\overline{xy}$ and $\overline{y}^2$, but we must keep in mind that φ can't send these elements to *any* two elements in R. For example, we cannot have $\overline{xy} \mapsto \overline{y}$ since

$$\begin{aligned}\varphi(\overline{xxy}) &= \varphi(0) \\ &= 0 \\ &\neq \overline{xy} \\ &= \overline{x}\varphi(\overline{xy}).\end{aligned}$$

It is straightforward to check that both $\overline{xy}$ and $\overline{y}^2$ can be mapped to any K-linear combination of $\overline{xy}$ and $\overline{y}^2$. Thus as a K-vector space, we have $\operatorname{Hom}_R(\langle \overline{xy}, \overline{y}^2\rangle, R) \cong K^4$. On the other hand, as a K-vector space, we have $R/I \cong K^3$.

A good duality theory may be defined in a different way: If M is a finitely generated R-module, we provisionally define the dual of M to be

$$D(M) = \operatorname{Hom}_K(M, K)$$

The vector space $D(M)$ is naturally an R-module by the action

$$(a\varphi)(u) = \varphi(au)$$

for all $a \in R$, $\varphi \in D(M)$, and $u \in M$.

Example 16.2. Returning to Example (16.7), we see that $D(A/I) = K\varphi_x + K\varphi_{xy}$, where $\varphi_x(x) = 1$, $\varphi_x(xy) = 0$ and $\varphi_{xy}(x) = 0$ and $\varphi_{xy}(xy) = 1$. Then $x \cdot \varphi_x = 0$ since

$$\begin{aligned}x \cdot \varphi_x(xy) &= \varphi_x(x^2y) \\ &= \varphi_x(0) \\ &= 0\end{aligned}$$

and

$$\begin{aligned}x \cdot \varphi_x(x) &= \varphi_x(x^2) \\ &= \varphi_x(0) \\ &= 0.\end{aligned}$$

Similarly, one can show that $x \cdot \varphi_{xy} = 0$, $y \cdot \varphi_x = 0$, and $y \cdot \varphi_{xy} = \varphi_x$.

16.1 Dualizing Functors

Definition 16.1. Let D be a contravariant functor from the category of R-modules to itself. We say D is a **dualizing functor** if it is exact and D^2 is naturally isomorphic to the identity functor.

With D defined above, we see that D a contravariant functor from the category of finitely generated A-modules to itself. Since M is finite-dimensional over K, the natural map $M \to D(D(M))$ sending $m \in M$ to the functional $\widehat{m} : \varphi \mapsto \varphi(m)$, for $\varphi \in \operatorname{Hom}_K(M, K)$ is an isomorphism of vector spaces. In fact, it is an isomophism of A-modules. Indeed, we have $\widehat{am} = a \cdot \widehat{m}$ since

$$\begin{aligned}(a \cdot \widehat{m})(\varphi) &= \widehat{m}\,(a \cdot \varphi) \\ &= (a \cdot \varphi)\,(m) \\ &= \varphi\,(am) \\ &= \widehat{am}(\varphi)\end{aligned}$$

for all $\varphi \in D(M)$. Since K is a field, D is **exact** in the sense that it takes exact sequences to exact sequences (with arrows reversed). Thus D is a **dualizing functor** on the category of finitely generated A-modules.

To get an idea of how D acts, note first that if $\mathfrak{p}$ is a maximal ideal of A, then any dualizing functor D takes the simple module $A/\mathfrak{p}$ to itself. Indeed, $D(A/\mathfrak{p})$ must be simple, because else it would have a proper factor module M and $D(M)$ would be a proper submodule of $A/\mathfrak{p}$. As A is local, it has only one simple module, and thus

$D(A/\mathfrak{p}) \cong A/\mathfrak{p}$. Since D takes exact sequences to exact sequences, reversing the arrows, D "turns composition series upside down" in the sense that if

$$0 \subset M_1 \subset \cdots \subset M_n \subset M$$

is a chain of modules with simple quotients $M_i/M_{i-1} \cong A/\mathfrak{p}$, then

$$D(M) \supset D(M_n) \supset \cdots \supset D(M_1) \supset D(0) = 0$$

is a chain of surjections whose kernels N_i are simple. In particular, for any module of finite length, then length of $D(M)$ equals the length of M.

A central role in the theory of modules over a local ring $(A, \mathfrak{p})$ is played by what might be thought of as the **top** of a module M, defined to be the quotient $\mathrm{Top}(M) := M/\mathfrak{p}M$; Nakayama's lemma shows that this quotient controls the generators of M. It could be defined categorically as the largest quotient of M that is a direct sum of simple modules. That is,

$$M/\mathfrak{p}M = \bigoplus_i (A/\mathfrak{p})\,.$$

The dual notion is that of the **socle** of M, denoted $\mathrm{Soc}(M)$: It is defined as the annihilator in M of the maximal ideal $\mathfrak{p}$, or equivalently, as the sum of all the simple submodules of M. Note that since the top of A is $A/\mathfrak{p}$, a simple module, the socle of $D(A)$ must be a simple module as well.

Example 16.3. Let $A = K[x,y]/\langle x^2, y^3\rangle$. Then $\mathrm{Soc}(A) = Kxy^2$ and $\mathrm{Top}(A) = K$. To calculate $D(A)$, we first write A as a K-vector space:

$$A = K + Kx + Ky + Kxy + Ky^2 + Kxy^2.$$

Then a dual basis for $D(A)$ is given by

$$D(A) = K\varphi_1 + K\varphi_x + K\varphi_y + K\varphi_{xy} + K\varphi_{y^2} + K\varphi_{xy^2}.$$

Then one can check that $\mathrm{Soc}(D(A)) = K\varphi_1$ and $\mathrm{Top}(D(A)) = K\varphi_{xy^2}$.

Remark. This remark is for those who are familiar with the Koszul Complex construction. Let $(A, \mathfrak{p})$ be a local ring and suppose $\mathfrak{p} = \langle x_1, \ldots, x_n\rangle$. Then

$$H_n(K(x_1, \ldots, x_n; M) \cong \mathrm{Soc}(M)$$
$$H_0(K(x_1, \ldots, x_n; M) \cong \mathrm{Top}(M)$$

Any dualizing functor preserves endomorphism rings; more generally, $\mathrm{Hom}_A(D(M), D(N)) \cong \mathrm{Hom}_A(N, M)$. In particular, $D(A)$ is a module with endomorphism ring A. To see this, consider the mappings given by applying D :

$$\mathrm{Hom}_A(M,N) \to \mathrm{Hom}_A(D(N), D(M)) \to \mathrm{Hom}_A(M,N) \to \mathrm{Hom}_A(D(N), D(M)).$$

Since $D^2 \cong 1$, the composite of two successive maps in this sequence is an isomorphism, so each of the maps is an isomorphism too. For instance, suppose $\varphi \in \mathrm{Hom}_A(M,N)$ was in the first map, that is, $D(\varphi) = 0$. Then $D^2(\varphi) = 0$ implies $\varphi = 0$ since D^2 is an isomorphism, which shows the map $D : \mathrm{Hom}_A(M,N) \to \mathrm{Hom}_A(D(N), D(M))$ is injective. Next, suppose $\varphi \in \mathrm{Hom}_A(D(N), D(M))$. Since D^2 is an isomorphism, there exists a $\psi \in \mathrm{Hom}_A(D(N), D(M)$ such that $D^2(\psi) = \varphi$. Then $D(\psi) \in \mathrm{Hom}_A(M,N)$ and $D(D(\psi)) = \varphi$, which shows the map $D : \mathrm{Hom}_A(M,N) \to \mathrm{Hom}_A(D(N), D(M))$ is surjective.

16.2 Canonical module of a local zero-dimensional ring

Proposition 16.1. *Let $(R, \mathfrak{m})$ be a local zero-dimensional ring. If E is any dualizing functor from the category of finitely generated R-modules to itself, then there is an isomorphism of functors $E(-) \cong \mathrm{Hom}_R(-, E(R))$. Further, $E(R)$ is isomorphic to the injective hull of $R/\mathfrak{m}$. Thus there is up to isomorphism at most one dualizing functor.*

Proof. Since $E^2 \cong 1$ as functors, the map $\mathrm{Hom}_R(M,N) \to \mathrm{Hom}_R(E(N), E(M))$ given by $\varphi \mapsto E(\varphi)$ is an isomorphism. Thus, there is an isomorphism, functorial in M,

$$\begin{aligned} E(M) &\cong \mathrm{Hom}_R(R, E(M)) \\ &\cong \mathrm{Hom}_R(E(E(M)), E(R)) \\ &\cong \mathrm{Hom}_R(M, E(R)) \end{aligned}$$

This proves the first statement.

Since R is projective, $E(R)$ is injective. As we observed above, R has a simple top, so $E(R)$ has a simple socle. Because R is zero-dimensional, every module contains simple submodules. The socle of a module M contains all the simple submodules of M, and thus meets every submodule of M; that is, it is an essential submodule of M. Since $R/\mathfrak{m}$ appears as an essential submodule of $E(R)$, we see that $E(R)$ is an injective hull of $R/\mathfrak{m}$. □

With Proposition (16.1) for justification, we define the **canonical module** ω_R of a local zero-dimensional ring R to be the injective hull of the residue class field of R. By Proposition (16.1), any **dualizing functor** D on the category of finitely generated A-modules must be $D(M) := \operatorname{Hom}_A(M, \omega_A)$, and in fact this functor is always dualizing.

Proposition 16.2. *Let $(A, \mathfrak{m})$ be a local zero-dimensional ring. Then the functor $M \mapsto D(M) := Hom_A(M, \omega_A)$ is a dualizing functor on the category of finitely generated A-modules.*

Proof. The

$$\operatorname{Hom}_A(M, N) \to \operatorname{Hom}_A(D(N), D(M))$$

is given by $\lambda \mapsto \lambda^\star$, where $\lambda^\star(\varphi) = \varphi \circ \lambda$, $\lambda \in \operatorname{Hom}_A(M, N)$ and $\varphi \in D(N)$. Then $(a\lambda + b\mu)^\star = a\lambda^\star + b\mu^\star$ for all $a, b \in A$ and $\lambda, \mu \in \operatorname{Hom}_A(M, N)$ shows D is A-linear. Also, D is exact because ω_A is injective. Thus it suffices to show that D^2 is isomorphic to the identity. Let $\alpha : 1 \to D^2$ be the natural transformation given by maps

$$\alpha_M : M \to \operatorname{Hom}_A(\operatorname{Hom}_A(M, \omega_A), \omega_A)$$

given by mapping $m \mapsto \widehat{m}$ where $m \in M$ and $\widehat{m}$ is the homomorphism taking $\varphi \in \operatorname{Hom}_A(M, \omega_A)$ to $\varphi(m)$. We shall show that α is an isomorphism by showing that each α_M is an isomorphism.

We do induction on the length of M. First suppose that the length is 1, so that $M = A/\mathfrak{p}$, where $\mathfrak{p}$ is the maximal ideal of A. Since ω_A is the injective hull of $A/\mathfrak{p}$, the socle of ω_A is $A/\mathfrak{p}$, and we have $\operatorname{Hom}_A(A/\mathfrak{p}, \omega_A) = A/\mathfrak{p}$, generated by any nonzero map $A/\mathfrak{p} \to \omega_A$. Thus $\operatorname{Hom}_A(\operatorname{Hom}_A(A/\mathfrak{p}, \omega_A), \omega_A) = A/\mathfrak{p}$, generated by any nonzero map. But if $1 \in A/\mathfrak{p}$ is the identity, then the map induced by 1 takes the inclusion $A/\mathfrak{p} \hookrightarrow \omega_A$ to the image of 1 under that inclusion, and is thus nonzero, so $\alpha_{A/\mathfrak{p}}$ is an isomorphism.

If the length of M is greater than 1, let M' be any proper submodule and let $M'' = M/M'$. By the naturality of α and the exactness of D^2 it follows that there is a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r] \arrow[d, "\alpha'_M"] & M \arrow[r] \arrow[d, "\alpha_M"] & M'' \arrow[r] \arrow[d, "\alpha'_M"] & 0 \\
0 \arrow[r] & D^2(M') \arrow[r] & D^2(M) \arrow[r] & D^2(M'') \arrow[r] & 0
\end{tikzcd}$$

Both M' and M'' have lengths stricly less than the length of M, so the left-hand and right-hand vertical maps are isomorphisms by induction. It follows by an easy diagram chase that the middle map α_M is an isomorphism too. □

Corollary. *Let A be a local Artinian ring. Then the annihilator of ω_A is 0; the length of ω_A is the same as the length of A; and the endomorphism ring of ω_A is A.*

Proof. The dualizing functor preserves annihilators, lengths, and endomorphism rings, and takes A to ω_A. □

Proposition 16.3. *Let A be a zero-dimensional local ring. Suppose that for some local ring B, A is a B-algebra that is finitely generated as a B-module and the maximal ideal of B maps into that of A. If E is the injective hull of the residue class field of B, then*

$$\omega_A = Hom_B(A, E).$$

In particular, if B is also zero-dimensional, then $\omega_A = Hom_B(A, \omega_B)$.

Proof. $\operatorname{Hom}_B(A, E)$ is an injective A-module (see my notes on injective modules for a proof of this). To show that it is the injective hull of the residue class field k of A, it suffices to show that it is an essential extension of the residue class field k of A. Let $\mathfrak{p}$ be the maximal ideal of A, and $\mathfrak{p}_B$ be the maximal ideal of B. The preimage of $\mathfrak{p}$ is a maximal ideal in B which contains $\mathfrak{p}_B$, so it must be $\mathfrak{p}_B$. Therefore there is an induced homomorphism of the residue class field k_B of B to k. As k is a finite dimensional vector space over k_B, we have $k = \omega_k \cong \operatorname{Hom}_{k_B}(k, k_B)$ as k-modules.

Let $S \subset \operatorname{Hom}_B(A, E)$ be the A-submodule of homomorphisms whose kernel contains $\mathfrak{p}$, or equivalently, such that $\mathfrak{p}\varphi = 0$. The module S is the socle of $\operatorname{Hom}_B(A, E)$ as an A-module. If $\varphi \in S$, then since $\mathfrak{p}_B A \subset \mathfrak{p}$, the image of φ is annihilated by $\mathfrak{p}_B$; that is, the image of φ is in the socle of E as a B-module, and since E is the injective hull of k_B, this is k_B. Since the homomorphisms in S all factor through the projection $A \to A/\mathfrak{p} = k$, we have $S \cong \operatorname{Hom}_B(k, k_B) \cong k$.

If $\varphi : A \to E$ is any B-module homomorphism, then since $\mathfrak{p}$ is nilpotent, φ is annihilated by a power of $\mathfrak{p}$, and thus there is a multiple $a\varphi \neq 0$ that is annihilated by $\mathfrak{p}$. Thus S is an essential A-submodule of $\operatorname{Hom}_B(A, E)$, as required. □

16.3 Zero Dimensional Local Gorenstein Rings

Definition 16.2. A zero-dimensional local ring A is **Gorenstein** if $A \cong \omega_A$.

Example 16.4. Let $A = K[x,y]/\langle x^2, y^3 \rangle$. Then both A and $D(A)$ are graded K-modules, with homogeneous components being

$$\begin{aligned} A_0 &= K & D(A)_0 &= K\varphi_1 \\ A_1 &= K\overline{x} + K\overline{y} & (S_{I_\Delta^{\mathrm{sq}}})_2 &= K\varphi_x + K\varphi_y \\ A_2 &= K\overline{xy} + K\overline{y}^2 & (S_{I_\Delta^{\mathrm{sq}}})_1 &= K\varphi_{xy} + K\varphi_{y^2} \\ A_3 &= K\overline{xy}^2 & (S_{I_\Delta^{\mathrm{sq}}})_0 &= K\varphi_{xy^2} \end{aligned}$$

where

$$\varphi_{\mathbf{x}^\alpha}\left(\overline{\mathbf{x}}^\beta\right) = \begin{cases} 1 & \text{if } \alpha = \beta \\ 0 & \text{else .} \end{cases}$$

One can check that $A \cong D(A)$ by the map

$$\begin{aligned} 1 &\mapsto \varphi_{xy^2} \\ x &\mapsto \varphi_{y^2} \\ y &\mapsto \varphi_{xy} \\ xy &\mapsto \varphi_y \\ y^2 &\mapsto \varphi_x \\ xy^2 &\mapsto \varphi_1 \end{aligned}$$

So A is a Gorenstein ring.

Proposition 16.4. *Let $(A, \mathfrak{m})$ be a zero-dimensional local ring. The following are equivalent.*

1. *A is Gorenstein.*
2. *A is injective as an A-module.*
3. *The socle of A is simple.*
4. *ω_A can be generated by one element.*

Proof.

$(1 \implies 2)$: ω_A is injective as an A-module, so if $A \cong \omega_A$, then A is injective as an A-module.

$(2 \implies 3)$: As A is a local ring, it is indecomposable as an A-module (Proof: Suppose $A \cong I \oplus J$ for two proper submodules $I, J \subset A$ (i.e. ideals). This implies there exists $x \in I$ and $y \in J$ such that $x + y = 1$. But since $\mathfrak{m}$ is the unique maximal ideal of A, we have $I \subset \mathfrak{m}$ and $J \subset \mathfrak{m}$, and so $1 = x + y \in \mathfrak{m}$ leads to a contradiction.) Since

$$\mathrm{Soc}(A) \subset \bigcup_{n=1}^{\infty} 0 :_A \mathfrak{m}^n = A$$

is an essential extension, if A is injective as an A-module, then it must be the injective hull of its socle. The injective hull of a direct sum is the direct sum of the injective hulls of the summands, so the socle must be simple.

$(3 \implies 4)$: If the socle of A is simple, that is, isomorphic to $A/\mathfrak{m}$, then the "top" of the dual of A, that is the top of ω_A, which is $\omega_A/\mathfrak{m}\omega_A$, is simple. By Nakayama's lemma ω_A can be generated by one element.

$(4 \implies 1)$: If ω_A is generated by one element then it is a homomorphic image of A. But A and ω_A have the same length by Proposition (16.2), so $A \cong \omega_A$. □

Example 16.5. Let $A = K[x,y,z]/\langle x^2, y^2, xz, yz, z^2 - xy \rangle$. Then A is a 0-dimensional Gorenstein ring that is not a complete intersection ring. In more detail: a basis for A as a K-vector space is

$$A = K + Kx + Ky + Kz + Kz^2$$

The ring A is Gorenstein because the socle has dimension 1 as K-vector space, namely $\mathrm{Soc}(A) = Kz^2$. Finally, A is not a complete intersection because it has 3 generators and a minimal set of 5 relations.

Most of the common methods of constructing Gorenstein rings work just as well in the case where A is not zero-dimensional, and we shall postpone them for a moment. However, one technique, Macaulay's method of **inverse systems**, is principally of interest in the zero-dimensional case.

Let $S = K[x_1, \ldots, x_r]$. For each $d \geq 0$, let S_d be the vector space of forms of degree d in the x_i. Let $T = K[x_1^{-1}, \ldots, x_r^{-1}] \subset K(A) = K(x_1, \ldots, x_r)$ be the polynomial ring on the inverses of the x_i. We make T into an S-module as follows: Let x^α be a monomial in A and x^β be a monomial in T, where $\alpha = (\alpha_1, \ldots, \alpha_r) \in \mathbb{Z}^r_{\geq 0}$ and $\beta = (\beta_1, \ldots, \beta_r) \in \mathbb{Z}^r_{\leq 0}$. Then

$$x^\alpha \cdot x^\beta = \begin{cases} 0 & \text{if } \alpha_i > \beta_i \text{ for some } i \\ x^{\alpha+\beta} & \text{else.} \end{cases}$$

Theorem 16.1. *With the notation above, there is a one-to-one inclusion reversing correspondence between finitely generated S-modules $M \subset T$ and ideal $I \subset S$ such that $I \subset \langle x_1, \ldots, x_r \rangle$ and A/I is a local zero-dimensional ring, given by*

$$M \mapsto (0 :_S M), \textit{ the annihilator of } M \textit{ in } S.$$
$$I \mapsto (0 :_T I), \textit{ the submodule of } T \textit{ annihilated by } I.$$

Proof. The S-module T may be identified with the graded dual $\bigoplus_d \operatorname{Hom}_K(S_d, K)$ of S; indeed the dual basis vector to $x^\alpha \in S_d$ is $x^{-\alpha} \in T$. Moreover, the graded dual is the injective hull of $K = S/\langle x_1, \ldots, x_r \rangle$ as an S-module. □

16.4 Canonical Modules and Gorenstein Rings in Higher Dimension

Definition 16.3. Let A be a local Cohen-Macaulay ring. A finitely generated A-module ω_A is a **canonical module for** A if there is a nonzerodivisor $x \in A$ such that $\omega_A / x\omega_A$ is a canonical module for $A/\langle x \rangle$. The ring A is **Gorenstein** if A is itself a canonical module; that is, A is Gorenstein if there is a nonzerodivisor $x \in A$ such that $A/\langle x \rangle$ is Gorenstein.

The induction in this definition terminates because $\dim(A/\langle x \rangle) = \dim(A) - 1$. We may easily unwind the induction, and say that ω_A is a canonical module if some maximal regular sequence $x_1, \ldots, x_d$ on A is also an ω_A-sequence, and $\omega_A / \langle x_1, \ldots, x_d \rangle \omega_A$ is the injective hull of the residue class field of $A/\langle x_1, \ldots, x_d \rangle$. Similarly, A is Gorenstein if and only if $A/\langle x_1, \ldots, x_d \rangle$ is a zero-dimensional Gorenstein ring for some maximal regular sequence $x_1, \ldots, x_d$. By Nakayama's lemma and Proposition (16.4), this is the case if and only if A has a canonical module generated by one element.

For a simple example, consider the case when A is a regular local ring. We claim that A has a canonical module, and in fact $\omega_A = A$. When $\dim(A) = 0$ the result is obvious, since A is a field. For the general case we do inductino on the dimension. If we choose x in the maximal ideal of A, but not its square, then x is a nonzerodivisor and A/x is again a regular local ring, so A/x is a canonical module for A/x . Therefore A is a canonical module for A, by defintion.

There are three problems with these notions. First, it is not at all obvious from the definitions that they are independent of the nonzero divisor x that was chosen. Second, something called a canonical module should at least be unique, and uniqueness is not clear either. Our first goal is to show that this independence and uniqueness do hold.

The third problem is that it is not obvious that a canonical module should even exist. Here we are not quite so lucky: There are local Cohen-Macaulay rings with no canonical module. However, our second goal will be to establish that canonical modules do exist for any Cohen-Macaulay rings that are homomorphic images of regular local rings (and a little more generally). This includes complete local rings and virtually all other rings of interest in algebraic geometry and number theory.

Example 16.6. Let $A = K[x,y,z]_{\langle x,y,z \rangle} / \langle xy, xz, yz \rangle$. Then $x + y + z$ is a nonzerodivisor in A, and

$$A/\langle x+y+z \rangle = K[x,y,z]_{\langle x,y,z \rangle} / \langle x+y+z, xy, xz, yz \rangle \cong K[y,z]_{\langle y,z \rangle} / \langle y^2, yz, z^2 \rangle = K + Ky + Kz,$$

which does not have a simple socle, so this is not Gorenstein.

Example 16.7. Let $A = K[x,y,z]_{\langle x,y,z \rangle} / \langle x+y+z, xz, yz \rangle$. Then $x + y + z$ is a nonzerodivisor in A, and

$$A/\langle x+y+z \rangle = K[x,y,z]_{\langle x,y,z \rangle} / \langle x+y+z, xy, xz, yz \rangle \cong K[y,z]_{\langle y,z \rangle} / \langle y^2, yz, z^2 \rangle = K + Ky + Kz,$$

which does not have a simple socle, so this is not Gorenstein.

16.5 Maximal Cohen-Macaulay Modules

Proposition 16.5. *Let R be a local ring of dimension d, and let M be a finitely-generated R-module. The following conditions are equivalent:*

1. *Every system of parameters in R is an M-sequence.*
2. *Some system of parameters in R is an M-sequence.*
3. $\operatorname{depth} M = d$

*If these conditions are satisfied, we say that M is a **maximal Cohen-Maculay module over** R. Every element outside the minimal primes of R is a nonzerodivisor on M.*

Proof. The implications 1 implies 2 implies 3 are immediate from the definitions. Let us show 3 implies 1. Suppose $\operatorname{depth} M = d$. If $x_1, \dots, x_d$ is a system of parameters, then $Q = \langle x_1, \dots, x_d \rangle$ is $\mathfrak{m}$-primary. In particular, $\sqrt{Q} = \mathfrak{m}$. Therefore

$$\begin{aligned} \operatorname{depth}(Q, M) &= \operatorname{depth}(\sqrt{Q}, M) \\ &= \operatorname{depth}(\mathfrak{m}, M) \\ &= \operatorname{depth} M \\ &= d, \end{aligned}$$

which implies $x_1, \dots, x_d$ is an M-regular sequence.

To prove the last statement, note that if x_1 is not in any minimal prime of R, then $\dim(R/x_1) = \dim R - 1$, so a system of parameters mod x_1 may be lifted to a system of parameters for R beginning with x_1. Thus, x_1 is a nonzerodivisor on M. □

Corollary. *Let $(A, \mathfrak{m})$ be a local ring of dimension d, $Q = \langle x_1, \dots, x_d \rangle$ and $\mathfrak{m}$-primary ideal, and M a maximal Cohen-Macaulay module over A. Then*

$$Gr_{\mathfrak{q}}(M) \cong Gr_{\mathfrak{q}}(A) \otimes_A M.$$

In case A is zero-dimensional, all finitely generated modules are maximal Cohen-Macaulay modules. On the other hand, if A is a regular local ring, then by the Auslander-Buchsbaum formula, the maximal Cohen-Macaulay A-modules are exactly the free A-modules.

More generally, if A is a finitely generated module over some regular local ring S of dimension d, then by the Auslander-Buchsbaum theorem, the maximal Cohen-Macaulay modules over A are those A-modules that are free as S-modules. Thus maximal Cohen-Macaulay modules may be thought of as representations of A as a ring of matrices over a regular local ring–as such they generalize the objects studied in integral representation theory of finite groups under the name **lattices**. We shall exploit the following example. If $B = A/J$ is a homomorphic image of A such that B is again Cohen-Macaulay of dimension d as a ring, then B is a Cohen-Macaulay A-module.

16.6 Modules of Finite Injective Dimension

Proposition 16.6. *Let R be a ring, let N be an R-module, let $x \in R$ be an R-regular and an N-regular element, and let (E, d) be a minimal injective resolution of N over R. Set $\widetilde{E} = \bigoplus_i 0 :_{E_i} x \cong \operatorname{Hom}^\star_R(R/x, E)$. Then $\Sigma\widetilde{E}$ is an injective resolution of N/xN over R/x. Thus*

$$\operatorname{id}_{R/x}(N/xN) = \operatorname{id}_R(N) - 1.$$

Furthermore, let M be an R-module which is annihilated by x, then

$$\operatorname{Ext}^{i+1}_R(M, N) \cong \operatorname{Ext}^i_{R/x}(M, N/xN)$$

for all $i \geq 0$.

Proof. By Lemma (10.3), we see that each $\widetilde{E}^i$ is an injective (R/x)-module. Furthermore, note that E^0 is an essential extension of N since E is a *minimal* injective resolution of N over R. In particular, since

$$\widetilde{E}^0 \cap N = 0 :_N x = 0,$$

we see that $\widetilde{E}^0 = 0$. It remains to show that $\mathrm{H}^0(\Sigma\widetilde{E}) \cong N/xN$ and $\mathrm{H}^i(\Sigma\widetilde{E}) \cong 0$ for all $i \geq 1$, or equivalently, that $\mathrm{H}^1(\widetilde{E}) \cong N/xN$ and $\mathrm{H}^i(\widetilde{E}) \cong 0$ for all $i \geq 2$. Note that $\mathrm{H}(\widetilde{E}) = \operatorname{Ext}_R(R/x, N)$ by definition. Computing this homology using the short exact sequence

$$0 \to R \xrightarrow{x} R \to R/x \to 0$$

gives us $\mathrm{Ext}^1_R(R/x,N) \cong N/xN$ and $\mathrm{Ext}^i_R(R/x,N) \cong 0$ for all $i \geq 2$. It follows that $\Sigma\widetilde{E}$ is an injective resolution of N/xN over R/x. To see that $\Sigma\widetilde{E}$ is minimal, note that $\ker \widetilde{\mathrm{d}}^n$ is the intersection of the essential submodule $\ker \mathrm{d}^n$ with $\widetilde{E}^n$, and is thus essential in $\widetilde{E}^n$. It follows at once that

$$\mathrm{id}_{R/x}(N/xN) = \mathrm{id}_R(N) - 1.$$

For the latter part of the proposition, note that every map from M to an E^i has image killed by x, so

$$\begin{aligned}\mathrm{Hom}^\star_R(M,E) &= \mathrm{Hom}^\star_R(M,\widetilde{E})\\ &= \mathrm{Hom}^\star_{R/x}(M,\widetilde{E})\\ &= \Sigma^{-1}\mathrm{Hom}^\star_{R/x}(M,\Sigma\widetilde{E})\end{aligned}$$

Taking homology gives us the last statement of the proposition. □

Remark. Recall that if $(R,\mathfrak{m})$ is a local ring, M is a finitely-generated R-module, and $x \in \mathfrak{m}$ is an R-regular and M-regular element, then $\mathrm{pd}_{R/x}(M/xM) = \mathrm{pd}_R(M)$. The idea behind that proof is as follows: we start with a minimal projective resolution P of M over R and denote $p = \mathrm{pd}\, M$. Then one shows that P/xP is a minimal projective resolution of M/xM over R/xR. They key here however is that $(P/xP)_p = P_p/xP_p \neq 0$ by Nakayama's lemma.

To exploit this result, we need to know the modules of finite injective dimension over a zero-dimensional ring.

Proposition 16.7. *Let R be a local Cohen-Macaulay ring and let M be a maximal Cohen-Macaulay module of finite injective dimension. Then $\mathrm{id}_R(M) = \dim\, R$. Moreover, if $\dim\, R = 0$, then M is a direct sum of copies of ω_R, and $M \cong \omega_R$ if and only if $\mathrm{End}_R(M) = R$.*

Proof. Suppose first that $\dim\, R = 0$ and let $D = \mathrm{Hom}_R(-,\omega_R)$ be the dualizing functor. Applying D to an injective resolution of M we see that $D(M)$ is a module of finite projective dimension, and is thus free by the Auslander-Buchsbaum formula. Applying D again we see that $M \cong D^2(M)$ is a direct sum of copies of $D(R) = \omega_R$. Using D, we see that the endomorphism ring of ω_R^n is the same as the endomorphism ring of R^n. Thus it is equal to R if and only if $n = 1$.

Now suppose $\dim R = d$ is arbitrary. Choose an R-regular sequence $x_1,\ldots,x_d$ that is also an M-regular sequence. Then by Proposition (16.6), together with an induction argument, we conclude that

$$\begin{aligned}\mathrm{id}_R(M) &= d + \mathrm{id}_{R/\langle x_1,\ldots,x_d\rangle}(M/\langle x_1,\ldots,x_d\rangle M)\\ &= d + 0\\ &= d.\end{aligned}$$

□

Proposition 16.8. *Let $(R,\mathfrak{m})$ be a local Cohen-Macaulay ring of dimension d and let N be a maximal Cohen-Macaulay module of finite injective dimension.*

1. *Let M be a finitely-generated R-module of depth q, then $\mathrm{Ext}^i_R(M,N) \cong 0$ for $i > d - q$.*

2. *Let x be an N-regular element. Then x is a $\mathrm{Hom}_R(M,N)$-regular element. Furthermore, if M is also a maximal Cohen-Macaulay module, then*

$$\mathrm{Hom}_R(M,N)/x\mathrm{Hom}_R(M,N) \cong \mathrm{Hom}_{R/x}(M/xM,N/xN)$$

by the homomorphism taking the class of a map $\varphi : N \to M$ to the map $N/xN \to M/xM$ induced by φ.

Proof. 1. We do induction on q. By Proposition (16.7), the injective dimension of N is d, so that $\mathrm{Ext}^i_R(M,N) \cong 0$ for any N if $i > d$. This gives the case where $q = 0$. Now suppose $q > 0$ and let $x \in \mathfrak{m}$ be an M-regular element. From the short exact sequence

$$0 \to M \xrightarrow{x} M \to M/xM \to 0$$

we get a long exact sequence in Ext

$$\cdots \to \mathrm{Ext}^i_R(M,N) \xrightarrow{x} \mathrm{Ext}^i_R(M,N) \to \mathrm{Ext}^{i+1}_R(M/xM,N) \to \cdots$$

The module M/xM has depth $q-1$, so by induction $\mathrm{Ext}^{i+1}_R(M/xM,N)$ vanishes if $i+1 > d-(q-1)$, that is, if $i > d-q$. By Nakayama's lemma, we conclude that $\mathrm{Ext}^i_R(M,N)$ vanishes if $i > d-q$.

2. From the short exact sequence

$$0 \to N \xrightarrow{x} N \to N/xN \to 0,$$

we derive a long exact sequence in Ext beginning

$$0 \to \operatorname{Hom}_R(M,N) \xrightarrow{x} \operatorname{Hom}_R(M,N) \to \operatorname{Hom}_R(M,N/xN) \to \operatorname{Ext}^1_R(M,N) \to \cdots$$

Thus x is $\operatorname{Hom}_R(M,N)$-regular. Now assume that M is maximal Cohen-Macaulay, so $q = d$. Then $\operatorname{Ext}^1_R(M,N) \cong 0$ by part 1. Every R-linear map $M \to N/xN$ factors uniquely through M/xM, so $\operatorname{Hom}_R(M,N/xN) = \operatorname{Hom}_R(M/xM,N/xN)$. The short exact sequence above thus becomes

$$0 \to \operatorname{Hom}_R(M,N) \xrightarrow{x} \operatorname{Hom}_R(M,N) \to \operatorname{Hom}_R(M/xM,N/xN) \to 0$$

Finally since $\operatorname{Hom}_R(M/xM,N/xN) = \operatorname{Hom}_{R/x}(M/xM,N/xN)$, we obtain part 2. □

Proposition 16.9. *Let $(R,\mathfrak{m})$ be a local ring, and let M and N be finitely generated R-modules, and let $x \in \mathfrak{m}$ be an N-regular element. If $\varphi\colon M \to N$ is an R-linear map and $\overline{\varphi}\colon M/xM \to N/xN$ is the map induced by φ, then*

1. *If $\overline{\varphi}$ is surjective, then φ is surjective.*

2. *If $\overline{\varphi}$ is injective, then φ is injective.*

In particular, if $\overline{\varphi}$ is an isomorphism, then φ is an isomorphism.

Proof. 1. Suppose $\overline{\varphi}$ is surjective. Then $N = \varphi(M) + xN$. By Nakayama's lemma, this implies $N = \varphi(M)$. Thus φ is surjective.

2. Suppose $\overline{\varphi}$ is injective. Let $L = \ker\varphi$. Since L goes to zero in N/xN, we must have $L \subseteq xM$. On the other hand, since x is a nonzerodivisor on the image of φ, we must have $L :_M x = L$. To see this, note that $v \in L :_M x$ implies $xv \in L$, thus

$$0 = \varphi(xv) = x\varphi(v),$$

then x being a nonzerodivisor on the image of φ implies $\varphi(v) = 0$, or $v \in L$. So $L :_M x = L$ and $L \subseteq xM$ implies $xL = L$, and hence $L = 0$ by Nakayama's lemma. □

Theorem 16.2. *Let R be a local Cohen-Macaulay ring of dimension d, and let W be a finitely generated R-module of depth q. Then W is a canonical module for R if and only if*

1. $\operatorname{depth} W = \dim R$.

2. *W is a module of finite injective dimension (necessarily equal to d).*

3. $\operatorname{End}_R W = R$

Proof. First suppose that W is a canonical module. We do induction on the dimension of R. Suppose $d = 0$. Then condition 1 is vacuous, since $q \leq d$. Also, condition 2 is satisfied because $W = \omega_R$ is injective. Lastly, condition 3 follows because, by duality

$$\begin{aligned}\operatorname{End}_R(\omega_R) &\cong \operatorname{End}_R(D(\omega_R)) \\ &\cong \operatorname{End}_R R \\ &\cong R.\end{aligned}$$

Now suppose $d > 0$, and let x be a nonzerodivisor. By hypothesis, W/xW is a canonical module over R/x, and by induction it satisfies conditions 1,2, and 3 as an (R/x)-module. Since x is a nonzerodivisor on W and W/xW has depth $d-1$, condition 1 is satisfied. By Proposition (16.6), W has finite injective dimension, in particular

$$d - 1 = \operatorname{id}_{R/x}(W/xW) = \operatorname{id}_R W - 1.$$

Let $S = \operatorname{End}_R W$, and consider the homothety map $\varphi\colon R \to S$ sending each element $a \in R$ to the map $\mathrm{m}_a \in \operatorname{End}_R W$, where $\mathrm{m}_a(w) = aw$ for all $w \in W$. We must show that φ is an isomorphism. By Proposition (16.8), x is a nonzerodivisor on S, and $S/xS = \operatorname{End}_{R/x}(W/xW) = R/x$. Thus by induction the map φ induces an isomorhpism $R/x \to S/xS$. It follows from Proposition (16.6) that φ is an isomorphism.

Next suppose that W is an R-module satisfying conditions 1,2, and 3. Again, we do induction on d. In case $d = 0$ we must show that $W = \omega_R$. By Proposition (16.7), this follows from conditions 2 and 3. Now suppose that $d > 0$, and let x be a nonzerodivisor in R. The element x is also a nonzerodivisor on W by Proposition (16.5), so W/xW has depth $d-1$ over R/x. By Proposition (16.6), $\operatorname{id}_{R/x}(W/xW) < \infty$, and by Proposition (16.8),

$$\operatorname{End}_{R/x}(W/xW) = \operatorname{End}_R(W)/x\operatorname{End}_R(W) = R/x.$$

Thus, W/xW is a canonical module for R/x by induction, and W is a canonical module for R. □

16.7 Uniqueness and (Often) Existence

These results imply a strong uniqueness result.

Corollary. *(Uniqueness of canonical modules). Let R be a local Cohen-Macualay ring of dimension d with a canonical module W, and let M be a finitely-generated maximal Cohen-Macaulay R-module of finite injective dimension. Then M is a direct sum of copies of W. In particular, any two canonical module of R are isomorphic.*

Proof. We do induction on d, the case $d = 0$ being Proposition (16.7). If $x \in R$ is a nonzerodivisor, then x is a nonzerodivisor on W and on M, and $M/xM \cong (W/xW)^n$ for some n by induction. By Proposition (16.9), there is an isomorphism $M \cong W^n$. □

Corollary. *(Uniqueness of canonical modules). Let A be a local Cohen-Macualay ring with a canonical module W. If M is any finitely generated maximal Cohen-Macaulay A-module of finite injective dimension, then M is a direct sum of copies of W. In particular, any two canonical module of A are isomorphic.*

Proof. We do induction on $\dim(A)$, the case $\dim(A) = 0$ being Proposition (16.7). If $x \in A$ is a nonzerodivisor, then x is a nonzerodivisor on W and on M, and $M/xM \cong (W/xW)^n$ for some n by induction. By Proposition (16.9), there is an isomorphism $M \cong W^n$. □

Henceforth, we shall write ω_A for a canonical module of A (if one exists). We now come to the question of existence. We have already seen that if R is a regular local ring, then R has canonical module $\omega_R = R$. We shall now show that if A is a homomorhpic image of a local ring with a canonical module, then A has a canonical module too.

Theorem 16.3. *(Construction of canonical modules). Let $(R, \mathfrak{m})$ be a local Cohen-Macaulay ring with canonical module ω_R. If A is a local R-algebra that is finitely generated as an R-module, and A is Cohen-Macaulay, then A has a canonical module. In fact, if $c = \dim(R) - \dim(A)$, then*

$$\omega_A \cong \mathit{Ext}^c_R(A, \omega_R)$$

Proof. We shall do induction on $\dim(A)$. First suppose that $\dim(A) = 0$. In this case, c is the dimension of R. The annihilator of A contains a power of the maximal ideal of R, say $\mathfrak{m}^n$. Since $\operatorname{depth}(\mathfrak{m}^n, R) = \operatorname{depth}(\mathfrak{m})$, we may choose a regular sequence $x_1, \ldots, x_c$ of length c in the annihilator of A. Let $R' = R/\langle x_1, \ldots, x_c\rangle$. Then R' is a local Cohen-Macaulay ring of dimension 0, and A is a finitely generated R'-module.

By definition, $\omega_R/\langle x_1, \ldots, x_c\rangle\omega_R$ is a canonical module for R', for which we shall write $\omega_{R'}$. By Proposition (16.6), applied c times,

$$\operatorname{Ext}^c_R(A, \omega_R) \cong \operatorname{Ext}^0_{R'}(A, \omega_{R'}) = \operatorname{Hom}_{R'}(A, \omega_{R'}).$$

By Proposition (16.3), this is a canonical module for A, as required.

Now suppose $\dim(A) > 0$. It suffices to show that if x is a nonzerodivisor on A, then x is a nonzerodivisor on $\operatorname{Ext}^c_R(A, \omega_R)$ and $\operatorname{Ext}^c_R(A, \omega_R)/x\operatorname{Ext}^c_R(A, \omega_R)$ is a canonical module for A/x. The short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "\cdot x"] & A \arrow[r] & A/x \arrow[r] & 0 \end{tikzcd}$$

gives rise to a long exact sequence in Ext of which a part is

$$\begin{tikzcd} \cdots \arrow[r] & \operatorname{Ext}^c_R(A/x, \omega_R) \arrow[r] & \operatorname{Ext}^c_R(A, \omega_R) \arrow[r, "\cdot x"] & \operatorname{Ext}^c_R(A, \omega_R) \arrow[r] & \operatorname{Ext}^{c+1}_R(A/x, \omega_R) \arrow[r] & \operatorname{Ext}^{c+1}_R(A, \omega_R) \arrow[r] & \cdots \end{tikzcd}$$

By induction, $\operatorname{Ext}^{c+1}_R(A/x, \omega_R)$ is a canonical module for A/x, so it suffices to show that the outer terms are 0, which we may do as follows:

Set $I = \operatorname{Ann}_R(A)$. The ring A/x is annihilated by $\langle I, x\rangle$, which has depth $c+1$ in R. Thus, $\operatorname{Ext}^c_R(A/x, \omega_R) = 0$. The ring A, being Cohen-Macaulay, has depth equal to $\dim(R) - c$, so $\operatorname{Ext}^{c+1}_R(A, \omega_R) = 0$ by Proposition (16.8). □

17 Category Theory

ZFC stands for Zermelo-Frankel + Axiom of Choice. There are $9 + 1$ axioms in ZFC. We also consider NGB (Von Neumann-Gödel-Bernays).

17.1 Definition of a Category

Definition 17.1. A **category** $\mathcal{C}$ consists of:

- A class $\mathrm{Ob}(\mathcal{C})$ of **objects**. If $x \in \mathrm{Ob}(\mathcal{C})$, we simply write $x \in \mathcal{C}$.
- Given $x, y \in \mathcal{C}$, there's a class $\mathrm{Mor}_{\mathcal{C}}(x, y)$ of **morphisms**, whose elements are called **morphisms** or **arrows** from x to y. If $f \in \mathrm{Mor}_{\mathcal{C}}(x, y)$, we write $f \colon x \to y$.
- Given $f \colon x \to y$ and $g \colon y \to z$, there is a morphism called their **composite** and is denoted $g \circ f \colon x \to z$. To clean notation, we sometimes denote the composite as gf.

$$\begin{tikzcd}
& y \arrow[dr, "g"] & \\
x \arrow[ur, "f"] \arrow[rr, "g\circ f"'] & & z
\end{tikzcd}$$

- Composition is associative: $(h \circ g) \circ f = h \circ (g \circ f)$ if either side is well-defined.

$$\begin{tikzcd}
\bullet \arrow[r, "g"] \arrow[dr, "h\circ f"] & \bullet \arrow[d, "h"] \\
\bullet \arrow[u, "f"] \arrow[ur, "g\circ f"] \arrow[r, "h\circ(g\circ f)=(h\circ g)\circ f"'] & \bullet
\end{tikzcd}$$

- For any $x \in \mathcal{C}$, there is an **identity morphism** $1_x \colon x \to x$

$$\begin{tikzcd}
x \arrow[loop above, "1_x"]
\end{tikzcd}$$

- We have the **left and right unity laws**:

$$1_x \circ f = f \text{ for any } f \colon y \to x$$
$$g \circ 1_x = g \text{ for any } g \colon x \to y$$

17.1.1 Functors exactness

Proposition 17.1. *Let $\mathcal{F}$ and $\mathcal{G}$ be two functors from the category of R-modules to itself, let $\tau \colon \mathcal{F} \to \mathcal{G}$ be a natural isomorphism, and let*

$$M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3$$

be exact at M_2. Then

$$\mathcal{F}(M_1) \xrightarrow{\mathcal{F}(\varphi_1)} \mathcal{F}(M_2) \xrightarrow{\mathcal{F}(\varphi_1)} \mathcal{F}(M_3) \tag{69}$$

is exact at $\mathcal{F}(M_2)$ if and only if

$$\mathcal{G}(M_1) \xrightarrow{\mathcal{G}(\varphi_1)} \mathcal{G}(M_2) \xrightarrow{\mathcal{G}(\varphi_1)} \mathcal{G}(M_3)$$

is exact at $\mathcal{G}(M_2)$.

Proof. The natural transformation $\tau \colon \mathcal{F} \to \mathcal{G}$ gives us the commutative diagram

$$\begin{tikzcd}
\mathcal{F}(M_1) \arrow[r, "\mathcal{F}(\varphi_1)"] \arrow[d, "\tau_{M_1}"] & \mathcal{F}(M_2) \arrow[r, "\mathcal{F}(\varphi_1)"] \arrow[d, "\tau_{M_2}"] & \mathcal{F}(M_3) \arrow[d, "\tau_{M_3}"] \\
\mathcal{G}(M_1) \arrow[r, "\mathcal{G}(\varphi_1)"] & \mathcal{G}(M_2) \arrow[r, "\mathcal{G}(\varphi_1)"] & \mathcal{G}(M_3)
\end{tikzcd}$$

The proposition follows trivially from the 3×3 lemma. □

17.2 Colimits

Definition 17.2. Let X be a set. A **preorder** on X is a binary relation that is reflexive and transitive.

Definition 17.3. Let $(I, \leq)$ be a preordered set. A system (M_i, μ_{ij}) of R-modules over I consists of a family of R-modules $\{M_i\}_{i \in I}$ indexed by I and a family of R-module maps $\{\mu_{ij} \colon M_i \to M_j\}_{i \leq j}$ such that for all $i \leq j \leq k$,

$$\mu_{ii} = 1_{M_i} \quad \text{and} \quad \mu_{ik} = \mu_{jk}\mu_{ij}.$$

We say (M, μ_{ij}) is a **directed system** if I is a directed set.

Lemma 17.1. *Let (M_i, μ_{ij}) be a system of R-modules over the preordered set I. The colimit of the system (M_i, μ_{ij}) is the quotient R-modules*

$$\bigoplus_{i \in I} M_i / \langle \{(\iota_i(u_i) - \iota_j(\mu_{ij}(u_i)) \mid u_i \in M_i \text{ and } i \in I\} \rangle,$$

where $\iota_i \colon M_i \to \bigoplus_{i \in I} M_i$ is the natural inclusion. We denote the colimit $M = \operatorname{colim}_i M_i$. We denote $\pi \colon \bigoplus_{i \in I} M_i \to M$ the projection map and $\phi_i = \pi \circ \iota_i \colon M_i \to M$.

Proof. Note that $\phi_i = \phi_j \circ \mu_{ij}$ in the above construction. Indeed, let $u_i \in M_i$. Then

$$\begin{aligned}(\phi_j \mu_{ij})(u_i) &= (\pi \iota_j \mu_{ij})(u_i) \\ &= \pi(\iota_j(\mu_{ij}(u_i))) \\ &= \pi(\iota_i(u_i)) \\ &= (\pi \iota_i)(u_i) \\ &= \varphi_i(u_i).\end{aligned}$$

To show the pair (M, ϕ_i) is the colimit we have to show it satisfies the universal property: for any other such pair (Y, ψ_i) with $\psi_i \colon M_i \to Y$ and $\psi_i = \psi_j \circ \mu_{ij}$, there is a unique R-module homomorphism $g \colon M \to Y$ such that the following diagram commutes:

$$\begin{tikzcd}
M_i \arrow[rr, "\mu_{ij}"] \arrow[dr, "\phi_i"] \arrow[ddr, bend right, "\psi_i"'] & & M_j \arrow[dl, "\phi_j"'] \arrow[ddl, bend left, "\psi_j"] \\
& M \arrow[d, "g"] & \\
& Y &
\end{tikzcd}$$

and this is clear because we can define g by taking the map ψ_i on the sumand M_i in the direct sum $\bigoplus M_i$. □

Lemma 17.2. *Let (M_i, μ_{ij}) be a system of R-modules over the preordered set I. Assume that I is directed. The colimit of the system (M_i, μ_{ij}) is canonically isomorphic to the module M defined as follows:*

1. *as a set let*

   $$M = \left(\coprod_{i \in I} M_i \right) / \sim$$

   where for $u \in M_i$ and $u' \in M_{i'}$ we have

   $$u \sim u' \text{ if and only if } \mu_{ij}(u) = \mu_{i'j}(u') \text{ for some } j \geq i, i'$$

2. *as an abelian group for $u \in M_i$ and $u' \in M_{i'}$ we define the sum of the classes of u and u' in M to be the class of $\mu_{ij}(u) + \mu_{i'j}(u')$ where $j \in I$ is any index with $i \leq j$ and $i' \leq j$, and*

3. *as an R-module define $u \in M_i$ and $a \in R$ the product of a and the class of u in M to be the class of au in M.*

The canonical maps $\phi_i \colon M_i \to M$ are induced by the canonical maps $M_i \to \coprod_{i \in I} M_i$.

17.3 Adjoint Functors