1 Additive Categories

Definition: A category $\mathcal{C}$ is pre-additive if its hom sets have the structure of an abelian group and composition of maps distributes over addition. Explicitly, for $X, Y, Z \in \mathcal{C}$, there exits a binary operation,

$$+ : \mathrm{Hom}\,(X, Y) \times \mathrm{Hom}\,(X, Y) \to \mathrm{Hom}\,(X, Y)$$

such that $(\mathrm{Hom}\,(X, Y), +)$ is an abelian group and, for $f, g : X \to Y$ and $h, k : Y \to Z$ we have $h \circ (f + g) = h \circ f + h \circ g$ and $(h + k) \circ f = h \circ f + k \circ f$. This is equvalent to the requirement that hom is a functor,

$$\mathrm{Hom}\,(-, -) : \mathcal{C}^{\mathrm{op}} \times \mathcal{C} \to \mathbf{AbGrp}$$

Lemma 1.1. In a pre-additive cateogory, there exists an identity element $0 \in \mathrm{Hom}\,(X, Y)$ such that $0 + f = f + 0 = f$ for $f \in \mathrm{Hom}\,(X, Y)$ and $f \circ 0 = 0$ for $f \in \mathrm{Hom}\,(Y, Z)$ and $0 \circ f = 0$ for $f \in \mathrm{Hom}\,(Z, X)$.

Proof. The hom sets are abelian groups by definiton and thus must have unique identiy elements satisfying $f + 0 = 0 + f = f$ for all $f \in \mathrm{Hom}\,(X, Y)$. Furthermore, for $f \in \mathrm{Hom}\,(Y, Z)$ we have $f \circ 0 = f \circ (0 + 0) = f \circ 0 + f \circ 0$ and thus $f \circ 0 = 0_{XZ}$. Furthermore for $f \in \mathrm{Hom}\,(Z, X)$ we know that $0 \circ f = (0 + 0) \circ f = 0 \circ f + 0 \circ f$ so $0 \circ f = 0_{ZY}$. $\square$

Definition: A biproduct of an indexed set $\{X_i\}_I$ is an object $X = \bigoplus_I X_i$ along with projection maps $\pi_i : X \to X_i$ and inclusion maps $\iota_i : X_i \to X$ such that $(X, \{\pi_i\}_I)$ is the product of $\{X_i\}_I$ and $(X, \{\iota_i\}_I)$ is the coproduct of $\{X_i\}_I$.

Proposition 1.2. Let $\mathcal{C}$ be a pre-additive category. Every finite product and finite coproduct is a biproduct. In particular, finite products and coproducts are equal.

Proof. Let $X \times Y$ be the product of X and Y. Consider the diagram,

$$\begin{tikzcd}
X \arrow[rr, "\mathrm{id}_X"] \arrow[dr, "\iota_X"] & & X \\
& X \times Y \arrow[ur, "\pi_X"] \arrow[dr, "\pi_Y"] & \\
Y \arrow[rr, "\mathrm{id}_Y"] \arrow[ur, "\iota_Y"] & & Y
\end{tikzcd}$$

where the maps $\iota_X : X \to X \times Y$ and $\iota_Y : Y \to X \times Y$ are defined via the universal property of the product applied to $(\mathrm{id}_X, 0)$ and $(0, \mathrm{id}_Y)$ respectivly where $0 \in \mathrm{Hom}\,(X, Y)$ is the identiy element of the abelian group. The universal property gives,

$$\pi_X \circ \iota_X = \mathrm{id}_X \quad \pi_Y \circ \iota_X = 0$$
$$\pi_X \circ \iota_Y = 0 \quad \pi_Y \circ \iota_Y = \mathrm{id}_Y$$

so the diagram commutes. We need to show that $X \times Y$ is universal with respect to the maps ι_X and ι_Y. Suppose we have maps $f_X : Z \to X$ and $f_Y : Z \to Y$ then define $\tilde{f} = f_X \circ \pi_X + f_Y \circ \pi_Y$.

$$\begin{tikzcd}
& X \arrow[rr, "\mathrm{id}_X"] \arrow[dl, "f_X"'] \arrow[dr, "\iota_X"] & & X \\
Z & & X \times Y \arrow[ll, dashed, "\tilde{f}"'] \arrow[ur, "\pi_X"] \arrow[dr, "\pi_Y"] & \\
& Y \arrow[rr, "\mathrm{id}_Y"] \arrow[ul, "f_Y"] \arrow[ur, "\iota_Y"] & & Y
\end{tikzcd}$$

This map satisfies the required universal property because,

$$\tilde{f} \circ \iota_X = (f_X \circ \pi_X + f_Y \circ \pi_Y) \circ \iota_X = f_X \circ \pi_X \circ \iota_X + f_Y \circ \pi_Y \circ \iota_X = f_X + 0 = f_X$$

and likewse,

$$\tilde{f} \circ \iota_Y = (f_X \circ \pi_X + f_Y \circ \pi_Y) \circ \iota_Y = f_X \circ \pi_X \circ \iota_Y + f_Y \circ \pi_Y \circ \iota_Y = 0 + f_Y = f_Y$$

Lastly, we must show that $\tilde{f}$ is unique. Suppose there exits a map $\tilde{f} : X \times Y \to Z$ such that $\tilde{f} \circ \iota_X = f_X$ and $\tilde{f} \circ \iota_Y = f_Y$. Consider the map $I : X \times Y \to X \times Y$ given by,

$$I = \iota_X \circ \pi_X + \iota_Y \circ \pi_Y$$

Therefore,

$$\pi_X \circ I = \pi_X \circ \iota_X \circ \pi_X + \pi_X \circ \iota_Y \circ \pi_Y = \pi_X + 0 = \pi_X$$

and furthermore,

$$\pi_Y \circ I = \pi_Y \circ \iota_X \circ \pi_X + \pi_Y \circ \iota_Y \circ \pi_Y = 0 + \pi_Y = \pi_Y$$

However, by the universal property of the product, there exists a unique map, namely $\mathrm{id}_{X \times Y}$, satisfying these properties. Thus, $I = \mathrm{id}_{X \times Y}$. Thus,

$$\tilde{f} = \tilde{f} \circ \mathrm{id}_{X \times Y} = \tilde{f} \circ I = \tilde{f} \circ \iota_X \circ \pi_X + \tilde{f} \circ \iota_Y \circ \pi_Y = f_X \circ \pi_X + f_Y \circ \pi_Y$$

so the map we constructed earlier is unique.

Similarly, let $X \coprod Y$ be the coproduct of X and Y. A similar argument will hold reversing all arrows. $\square$

Definition: A category is additive if it is pre-additive, has a zero object, and has all finite biproducts. The preceding dicussion implies that it is enough to check that either all finite products or all finite coproducts exit.

Definition: A functor $T : \mathcal{C} \to \mathcal{D}$ is additive if it preserves finite biproducts.

2 Abelian Categories

ABELIAN FUNCTOR

3 Categories of Modules

Definition: RING Cat and Module Cat

Lemma 3.1. A ring homomorphism $f : R \to S$ induces an additive functor

$$F : \mathbf{Mod}_R \to \mathbf{Mod}_S$$

given by $(-) \otimes_R S$ where S is an R-module under the action $r \cdot s = f(r)s$.

Proof. $\square$

Proposition 3.2. $\mathrm{GL}_n(-) : \mathbf{Ring} \to \mathbf{Grp}$ is a functor

Proof. $\square$

Proposition 3.3. $\det : \mathrm{GL}_n(-) \Longrightarrow (-)^{\times}$ is a natrual transformation.

Proof. $\square$

4 Spectra of Rings

Definition: Let A be a ring then $\mathrm{Spec}\,(A)$ is the set of prime ideals of A with the topology generated by closed sets of the form,

$$V(I) = \{\mathfrak{p} \in \mathrm{Spec}\,(A) \mid \mathfrak{p} \supset I\}$$

for each ideal $I \subset A$. This is known as the Zariski topology.

Proposition 4.1. We have the following properties of Zariski topology,

1. $V(IJ) = V(I) \cup V(J)$
2. $V(I \cap J) = V(I) \cup V(J)$
3. $V(I) \subset V(J) \iff \sqrt{I} \supset \sqrt{J}$
4. For any sequence of ideals J_i for $i \in \mathcal{I}$,

$$V\left(\sum_{i \in \mathcal{I}} J_i\right) = \bigcap_{i \in \mathcal{I}} V(J_i)$$

5. every closed set is of the form $V(I)$ for some ideal $I \subset A$.

Proof. Clearly if $\mathfrak{p} \supset I$ or $\mathfrak{p} \supset J$ then clearly $\mathfrak{p} \supset IJ$. Furthermore, if $\mathfrak{p} \not\supset I$ and $\mathfrak{p} \not\supset J$ then ther exists $a \in I$ and $b \in J$ such that $a \notin I$ and $b \notin J$ then $ab \in IJ$ and $ab \notin \mathfrak{p}$ since $\mathfrak{p}$ is prime. Therefore, $\mathfrak{p} \not\supset IJ$ so $V(IJ) = V(I) \cup V(J)$. The exact same argument holds for $V(I \cap J) = V(I) \cup V(J)$.

If $V(I) \subset V(J)$ then for each prime $\mathfrak{p} \supset I$ we have $\mathfrak{p} \supset J$. Therefore,

$$\sqrt{I} = \bigcap_{\mathfrak{p} \supset I} \mathfrak{p} \supset \bigcap_{\mathfrak{p} \supset J} \mathfrak{p} = \sqrt{J}$$

since the left is an intersection over a subset. Furthermore, if $\sqrt{I} \supset \sqrt{J}$ then clearly $V(\sqrt{I}) \subset V(\sqrt{J})$ since $\mathfrak{p} \supset \sqrt{I} \supset \sqrt{J}$ implies $\mathfrak{p} \supset \sqrt{J}$. However, $V(I) = V(\sqrt{I})$ for any ideal. Together, this implies that $V(I) \subset V(J)$.

Now consider,

$$\mathfrak{p} \supset \sum_{i \in \mathcal{I}} J_i$$

then $\mathfrak{p} \subset J_i$ for each $i \in \mathcal{I}$. Otherwise, then there exists $f_{i_1} \in J_{i_1}, \cdots f_{i_n} \in J_{i_n}$ such that, $f_{i_1} + \cdots + f_{i_n} \notin \mathfrak{p}$. Therefore, at least one $f_{i_j} \notin \mathfrak{p}$ so $J_{i_j} \not\supset J_{i_j}$ and thus $\mathfrak{p} \notin V(J_{i_j})$ so it cannot lie in the intersection. Because $V(I)$ form a basis of closed

sets, any closed set can be written as an intersection of such sets which we have shown is again of the form $V(I)$. $\square$

Proposition 4.2. A ring map $f : A \to B$ induces a continuous map of spectra, $f^* : \mathrm{Spec}\,(B) \to \mathrm{Spec}\,(A)$ via $f^*(\mathfrak{P}) = f^{-1}(\mathfrak{p})$. Furthermore, $\mathrm{Spec}\,(-) : \mathbf{Ring} \to \mathbf{Top}$ is a contravariant functor.

Proof. Let $A \to B$ be a ring map and $I \subset A$ an ideal. Consider, $\mathfrak{P} \in (f^*)^{-1}(V(I))$ i.e. $f^*(\mathfrak{p}) \in V(I)$ so $f^{-1}(\mathfrak{p}) \supset I$. Therefore, $\mathfrak{p} \supset \langle f(I) \rangle$ the ideal generated by $f(I)$ so $\mathfrak{p} \in V(\langle f(I) \rangle)$. Furthermore, if $\mathfrak{p} \in V(\langle f(I) \rangle)$ then $f^{-1}(\mathfrak{p}) \supset f^{-1}(\langle f(I) \rangle) \supset I$ so $\mathfrak{p} \in (f^*)^{-1}(V(I))$. Therefore,

$$(f^*)^{-1}(V(I)) = V(\langle f(I) \rangle)$$

so $f^* : \mathrm{Spec}\,(B) \to \mathrm{Spec}\,(A)$ is continuous. Furthermore, consider $\mathrm{id}_A : A \to A$ then $\mathrm{id}_A^*(\mathfrak{p}) = \mathrm{id}_A^{-1}(\mathfrak{p}) = \mathfrak{p}$ so $\mathrm{id}_A^* = \mathrm{id}_{\mathrm{Spec}(A)}$. Lastly, consider $f : A \to B$ and $g : B \to C$ then,

$$(g \circ f)^*(\mathfrak{P}) = (g \circ f)^{-1}(\mathfrak{P}) = f^{-1}(g^{-1}(\mathfrak{P})) = f^* \circ g^*(\mathfrak{P})$$

Therefore, $(g \circ f)^* = f^* \circ g^*$ so $\mathrm{Spec}\,(-)$ is a functor. $\square$

Definition: Let $f \in A$ then $D(f) = V((f))^C = \{\mathfrak{p} \in \mathrm{Spec}\,(A) \mid f \notin \mathfrak{p}\}$ is called a distinguished open set of $\mathrm{Spec}\,(A)$.

Proposition 4.3. The following properties of distinguished open sets hold,

1. $D(f) \cap D(g) = D(fg)$

2. given a ring map $f : A \to B$ then $(f^*)^{-1}(D(x)) = D(f(x))$.

3. The distinguished opens form a basis for the Zariski topology.

Proof. First,

$$D(f) \cap D(g) = V((f))^C \cap V((g))^C = (V((f)) \cup V((g)))^C$$
$$= V((f)(g))^C = V((fg))^C = D(fg)$$

Furthermore, if $\mathfrak{p} \in D(f) \cap D(g)$ exactly when $f \notin \mathfrak{p}$ and $g \notin \mathfrak{p}$ iff $fg \notin \mathfrak{p}$ i.e. $\mathfrak{p} \in D(fg)$ since $\mathfrak{p}$ is prime.

Let $f : A \to B$ be a ring map. Then,

$$\mathfrak{p} \in (f^*)^{-1}(D(x)) \iff f^{-1}(\mathfrak{p}) \in D(x) \iff x \notin f^{-1}(\mathfrak{p}) \iff f(x) \notin \mathfrak{p} \iff \mathfrak{p} \in D(f(x))$$

In particular, f^* is continuous.

Finally, the sets $D(f)$ form an open basis since they are closed under intersection, cover $\mathrm{Spec}\,(A)$ since $D(1) = \mathrm{Spec}\,(A)$, and for each $\mathfrak{p} \in V(I)^C$ for some ideal $I \subset A$ (any closed is of the form $V(I)$) we have $\mathfrak{p} \not\supset I$ so $\exists f \in I$ with $f \notin \mathfrak{p}$ i.e.

$$\mathfrak{p} \in D(f) \subset V(I)^C$$

since if $f \notin \mathfrak{q}$ then $\mathfrak{q} \not\supset I$. Thus the sets $D(f)$ are a basis of Zariski opens which generate the Zariski topology. $\square$

Proposition 4.4. Let A be a ring, The topological space $\mathrm{Spec}\,(A)$ is compact.

Proof. Let $\mathfrak{U}$ be an open cover of $\mathrm{Spec}\,(A)$. Since the distinguished opens form a basis of open sets, then for each $\mathfrak{p} \in \mathrm{Spec}\,(A)$ there is $f_\mathfrak{p} \in \mathrm{Spec}\,(A)$ such that $D(f_\mathfrak{p}) \subset U_\mathfrak{p}$ for some $U \in \mathfrak{U}$ and $\mathfrak{p} \in D(f_\mathfrak{p})$. Therefore,

$$\bigcup_{\mathfrak{p} \subset A} D(f_\mathfrak{p}) = \mathrm{Spec}\,(A) \implies \bigcap_{\mathfrak{p} \subset A} V((f_\mathfrak{p})) = \varnothing$$

Therefore,

$$V\left(\sum_{\mathfrak{p} \subset A} (f_\mathfrak{p})\right) = \varnothing$$

However, every proper ideal is contained in a maximal ideal so we must have,

$$\sum_{\mathfrak{p} \subset A} (f_\mathfrak{p}) = A$$

if no primes lie above it. In particular,

$$1 \in \sum_{\mathfrak{p} \subset A} (f_\mathfrak{p}) \implies a_1 f_1 + \cdots a_n f_n = 1$$

for some finite list $f_1, \cdots, f_n$ of elements, $a_i \in A$ and $f_i = f_{\mathfrak{p}_i}$. Therefore,

$$(f_1) + \cdots + (f_n) = (1) = A$$

and thus,

$$V((f_1) + \cdots + (f_n)) = \varnothing \implies V((f_1)) \cap \cdots V((f_n)) = \varnothing$$

Taking the complement,

$$D(f_1) \cup \cdots D(f_n) = \operatorname{Spec}(A)$$

and thus there exists a finite subcover, $U_1, \ldots, U_n$ since,

$$U_1 \cup \cdots U_n \supset D(f_1) \cup \cdots D(f_n) = \operatorname{Spec}(A)$$

□

5 Local Rings

Definition: A ring is local if it has a unique maximal ideal $\mathfrak{m}$. In that case, $A^\times = A \backslash \mathfrak{m}$. A ring map $f : A \to A'$ of local rings is a local map if $f(\mathfrak{m}) \subset \mathfrak{m}'$. Furthermore, the residue field is

$$k = A/\mathfrak{m}$$

Thus a local map $f : A \to A'$ induces a map $\bar{f} : k \to k'$ such that,

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d] & A' \arrow[d] \\ k \arrow[r, "\bar{f}"'] & k' \end{tikzcd}$$

Proposition 5.1. For a map of rings $\phi : A \to B$ inducing $\phi^* : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ we have $A_{\phi^*(\mathfrak{p})} \to A_{\mathfrak{P}}$ is a local map of local rings.

Proposition 5.2. There is a factorization,

$$\begin{tikzcd} A_{\phi^*(\mathfrak{P})} \arrow[rr] \arrow[dr] & & B_{\mathfrak{P}} \\ & A_{\phi^*(\mathfrak{P})} \otimes_A B \arrow[ur] & \end{tikzcd}$$

Lemma 5.3. Let

$$M \xrightarrow{\phi} M \xrightarrow{\psi} P$$

be an exact sequence of A-modules. Then if $S \subset A$ is mutiplicative then the localization,

$$S^{-1}M \xrightarrow{\phi} S^{-1}M \xrightarrow{\psi} S^{-1}P$$

is an exact sequence of $S^{-1}A$-modules.

Definition: Let M be an A-module and $x \in A$ we say that x is M-regular if $m \mapsto x \cdot m$ is injective.

Proposition 5.4. Let $S = \{x \in A \mid x \text{ is } A-\text{regular}\}$ then S is multiplicative and $S^{-1}A$ is the total ring of fractions of A.

6 Jacobin Radical

Definition: The radical of a ring A is the intersection of all maximal ideals,

$$\text{rad}\,(A) = \bigcap_{\mathfrak{m}} \mathfrak{m}$$

Proposition 6.1. $x \in \text{rad}\,(A) \iff \forall a \in A : 1 + ax \in A^\times$

Proof. Let $x \in \text{rad}\,(A)$ then suppose that $(1+ax)A \subsetneq A$ and thus $(1+ax)A \subset \mathfrak{m}$ for some maximal ideal. But $x \in \text{rad}\,(A) \subset \mathfrak{m}$ so $ax \in \mathfrak{m}$ and thus $1 \in \mathfrak{m}$ contradicting the fact that $\mathfrak{m}$ is proper. Thus, $(1+ax)A = A$ so $1+ax$ is a unit.

Assuming that $1+ax$ is always a unit, suppose that $x \notin \mathfrak{m}$ we would have $\bar{x} \in A/\mathfrak{m}$ is not zero and thus inveritble because $A/\mathfrak{m}$ is a field. Thus, $\exists b \in A$ such that $\bar{x}\bar{b} = \bar{1}$ and thus $1 - xb \in \mathfrak{m}$ so $1 - xb \notin A^\times$ because $\mathfrak{m}$ is proper. Thus $x \in \text{rad}\,(A)$. □

Lemma 6.2 (Nakayama)**.** Let M be an A-module of finite type then if $IM = M$ for some ideal $I \subset A$ then exists $x \in I$ such that $(1+x)M = 0$. In particular, if $I \subset \text{rad}\,(A) \implies M = (0)$.

Proof. M is finite type so there exist $m_1, \dots, m_r \in M$ such that $M = Am_1 + \cdots + m_rA$. Proceed by induction on r. For the case $r = 1$, we have $M = (m_1)$ and thus $IM = M$ implies that $Im_1 = M$ so $m_1 = xm_1$ for some $x \in I$ and thus $(1-x)m_1 = 0 \implies (1-x)M = 0$.

Suppose the lemma is true for $r-1$. The consider the module $\bar{M} = M/Am_r$ which is generated by $r-1$ elements. Then $IM = M \implies I\bar{M} = \bar{M}$. By hypothesis, $\exists x \in I : (1+x)\bar{M} = 0$ and thus $(1+x)M \subset Am_r$. Therefore, $(1+x)IM = (1+x)M \subset Im_r$ so $\exists x' \in I$ such that $(1+x)m_r = x'm_r$ and thus $(1+x-x')m_r = 0$. Next, $(1+x)(1+x-x')M \subset (1+x-x')Am_r = 0$. Thus, take $x'' = 2x - x' + x(x-x')$ and we have $(1-x')M = 0$. Thus, the lemma holds by induction. □

Corollary 6.3. Let M be an A-module and N, N' two submodules of M such that $M = N + IN'$ such that either I is nilpotent or N' a finitely generated A-module and $I \subset \text{rad}\,(A)$ then $M = N$.

Proof. Consider $\bar{M} = M/N$. From $M = N + IN'$ we have that $\bar{M} = I\bar{N}'$. We want to show that $\bar{M} = 0$ which implies that $M = N$. First,

$$\bar{M} = I\bar{N}' \subset I\bar{M} \subset \bar{M}$$

and thus $I\bar{M} = \bar{M}$ In the case that N' is finitely generated then $\bar{N}'$ and $\bar{M}$ are also finitely generated so by Nakayama, $\bar{M} = 0$. In the case that I is nilpotnent, by substitution,

$$\bar{M} = I\bar{M} = I^2\bar{M} = I^3\bar{M} = \cdots = I^n\bar{M} = 0$$

where $I^n = 0$. □

7 Noetherian and Artinian Rings

Definition: An A-module satisfies the ascending (ACC) / descending (DCC) chain condition if any increasing / decreasing sequence of submodules of M achieves a maximum / minimum.

Definition: M is Noetherian if M satisfies ACC and Artinian if M satisfies DCC.

Proposition 7.1. Let

$$0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$$

be a short exact sequence of A-modules. Then N is Noetherian / Artinian if and only if both M and P are.

Proof. □

Definition: The ring A is called Noetherian / Artinian if it is Noetherian / Artinian as an A-module.

Corollary 7.2. If A is Noetherian / Artinian then any finitely generated A-module is Noetherian / Artinian.

Proof. If M is a finitely generated A-module then $M = Am_1 + \cdots + Am_n$. Then we have the short exact sequence,

$$0 \longrightarrow N \longrightarrow A^r \longrightarrow M \longrightarrow 0$$

And use the fact that A^r is Neotherian / Artinian using the following exact sequence,

$$0 \longrightarrow A \longrightarrow A^r \longrightarrow A^{r-1} \longrightarrow 0$$

which shows that A^r is Noetherian / Artinian iff A^{r-1} is. Thus A^r is Noetherian / Artinian by induction. Thus we get that N, M are both Noetherian / Artinian. □

Lemma 7.3. A is Noetherian iff every ideal of A is finitly generated.

Proof. Take $I_1 \subset I_2 \subset I_3 \subset \cdots$. Consider the ideal,

$$I = \bigcup_i I_i$$

Therefore if I is finitly generated then each generator must appear at a finite stage so the chain terminates. Furthermore if each chain terminates then for an ideal I consider the chain

$$(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \cdots$$

where $a_i \in I \setminus (a_1, \dots, a_{i-1})$. This chain must achive a maximum meaning that it must exhaust I. $\square$

Proposition 7.4. Let A be Noetherian and S a multiplicative subset of A then $S^{-1}A$ is Noetherian.

Theorem 7.5. If A is Noetherian then $A[x]$ is Noetherian.

Proof. Take $I \subset A[x]$ and define,

$$I_n = \{a \in A \mid \exists Q(x) \in I : Q(x) = ax^n + \cdots + c\}$$

Thus we have an ascending chain,

$$I_0 \subset I_1 \subset I_2 \subset I_3 \subset \cdots$$

Thus, $I_n = (a_1, \dots, a_r)$ and take $Q_i(x) = a_i x^{n_i} + \cdots + c_i \in I$ and take $P(x) = ax^n + \cdots + c$ in I such that $a \in I_k$ for all k. We take,

$$a = \sum_{i=1}^{r} \alpha_i a_i$$

if $m > N = \sup(m_i, i = 1, \dots, r)$ Then,

$$P(x) - \sum_{i=1}^{r} \alpha_i x^{n-n_i} Q_i(x)$$

has degree less than $n - 1$ because,

$$\sum_{i=1}^{r} \alpha_r x^{n-n_i} a_i x^{n-i} = ax^n$$

Repeating this process, we can find coeficients $s_1, \dots, s_r \in A[x]$ such that,

$$P(x) - \sum_{i=1}^{N} s_i(x) Q_i(x)$$

has degree less than N. Let $A[x]_N$ denote the space of polynomials of degree less than N. Then, $I = (Q_1, Q_2, \dots, Qr) + A[x]_N \cap I$ but $A[x]_N \cong A^{n+1}$ which is Noetherian so $A[x]_N \cap I$ is a finitely generated A-module. Thus, I is finitely generated. $\square$

Lemma 7.6. If $A \to B$ is a surjective morphism of rings and A is Noetherian then B is Noetherian.

Proof. Every ascending chain in B pulls back to an ascending chain in A which must terminate. □

Definition: Let A be a ring and B an A-algebra. We say that B is finitely generated as an A-algebra if there exists elements $x_1, \dots, x_r \in B$ such that every element of B is a linear combination with coeficients in A finite products of $x_1, \dots, x_r$. In other words, there exists a surjective homomorphism of rings,

$$A[x_1, \dots, x_r] \longrightarrow B$$

Corollary 7.7. If A is Noetherian, then any finitely generated A-algebra is Noetherian.

Corollary 7.8. Any finitely generated k-algebra is Noetherian.

Proposition 7.9. Assume that we have an inclusion of rings,

$$A \subset B \subset C$$

and that A is Noetherian and C is a finitely generated A-algebra and C is a finitely generated B-module then B is a finitely generated A-algebra.

Proof. We can write,

$$C \cong A[x_1, \dots, n_m]$$

for some $x_1, \cdots, x_m \in C$ and,

$$C = Bc_1 + \cdots + Bc_\ell$$

then we may express,

$$x_i = \sum_{j=1}^{\ell} b_{ij} c_j$$

and furthermore,

$$c_i c_j = \sum_{k=1}^{\ell} b_{ijk} c_k$$

Now define,

$$B_0 = A[b_{ij}, b_{ijk}] \subset B$$

ian so and thus C is a finitely generated B_0-module but A and thus B_0 are Noetherian so any B_0-submodule of C is also finitely generated. In particular, $B \subset C$ is a finitely generated B_0-module and thus B is a finitely generated A-algebra since B_0 is. □

Theorem 7.10 (Nullstellensatz)**.** Let k be a field and E a finitely generated k-algebra. If E is a field, then E is a finite extension of k and thus is algebraic.

Proof. E is a finitely generated k-algebra and a field so $E = k[x_1, \dots, x_n]$ for $x_1, \dots, x_n \in E$. If all x are algebraic over k then $k[x_1, \dots, x_n]$ is finite-dimensional over k. Othersie, assume that $x_1, \dots, x_r$ are algebraically independent and E is algebraic over $k(x_1, \dots, x_r) = F$ and thus a finitely generated F-module. Since, $k \subset F \subset E$, by the above corollary, F must be a finitely generated k-algebra. However, if $F = k[y_1, \dots, y_m]$ with $y_i = f_i/g_i$ for $f_i, g_i \in k[x_1, \dots, x_r]$ then any element of F can be written as a polynomial in then y_i and thus as,

$$\frac{Q(x_1, \dots, x_r)}{\left(\prod_{i=1}^N g_i\right)^N}$$

with $Q \in k[x_1, \dots, x_r]$. However,

$$\prod_{i=1}^m g_i + 1 \in F \implies \frac{1}{\prod\limits_{i=1}^m g_i + 1} \in F \implies \frac{1}{\prod\limits_{i=1}^m g_i + 1} = \frac{Q(x_1, \dots, x_r)}{\left(\prod_{i=1}^N g_i\right)^N}$$

Therefore,

$$\left(\prod_{i=1}^m g_i + 1\right) \Bigg| \left(\prod_{i=1}^N g_i\right)^N$$

but the polynomials are coprime which is a contradiction. $\square$

Corollary 7.11. Let A be a finitely generated k-algebra and $\mathfrak{m}$ a maximal ideal of A then $A/\mathfrak{m}$ is a finite extension of k.

Proof. Since A is a finitely generated k-module, there exists a surjective ring maps,

$$k[x_1, \dots, x_n] \twoheadrightarrow A \twoheadrightarrow A/\mathfrak{m}$$

and thus $A/\mathfrak{m}$ is a finitely generated k-module. However, $\mathfrak{m}$ is maximal and therefore $A/\mathfrak{m}$ is a field. Therefore, by the Nullstellensatz, $A/\mathfrak{m}$ is a finite extension of E. $\square$

Remark. Let k be a field and $\bar{k}$ its algebraic closure. Consider $f_1, \dots, f_r \in k[x_1, \dots, x_m]$ and the ideal $I = (f_1, \dots, f_r) \subset k[x_1, \dots, x_m]$. Consider the zero locus,

$$Z(f_1, \dots, f_r) = \{p \in \bar{k}^m \mid f(p) = 0 \ \ \forall i\} = V$$

For $p \in V$, consder the map,

$$\begin{tikzcd} k[x_1, \dots, x_m] \arrow[rr, "\mathrm{ev}_p"] \arrow[dr] & & \bar{k} \\ & A = k[x_1, \dots, x_m]/I \arrow[ur, "\mathrm{ev}_p"'] & \end{tikzcd}$$

which factors through the quotient because $f_i(p) = 0$ and thus $\mathrm{ev}_p(I) = 0$. We know that $\mathrm{Im}(\mathrm{ev}_p)$ is contained in a finite extension of k and thus a field so $\ker \mathrm{ev}_p$ is a maximal ideal. Conversely, if $\mathfrak{m} \subset A$ is a maximal ideal then $A \to A/\mathfrak{m}$ is a finite extension of k embedded in $\bar{k}$ up to an automorphism $Gal(\bar{k}/k)$. In conclusion, there is a bijection between maximal ideals of $k[x_1, \dots, x_m]/I$ and $V(I)/Gal(\bar{k}/k)$

Definition: An ideal $\mathfrak{a} \subset A$ is irreducible if,

$$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c} \implies \mathfrak{a} = \mathfrak{b} \text{ or } \mathfrak{a} = \mathfrak{c}$$

Lemma 7.12. If $\mathfrak{p}$ is a prime ideal then $\mathfrak{p}$ is irreducible.

Proof. □

Proof. An ideal $\mathfrak{a} \subset A$ is primary if whever $xy \in \mathfrak{a}$ with $x \notin \mathfrak{a}$ then $\exists n : y^n \in \mathfrak{a}$ i.e. $y \in \sqrt{\mathfrak{a}}$. Equivalently, all zero divisors of $A/\mathfrak{a}$ are nilpotents. □

Lemma 7.13. If $\mathfrak{a}$ is primary then $\sqrt{\mathfrak{a}}$ is a prime ideal.

Proof. If $x, y \in \sqrt{\mathfrak{a}}$ then for some n, $x^n y^n \in \mathfrak{a}$ so either $x^n \in \mathfrak{a}$ or $y^{nm} \in \mathfrak{a}$ for some m. Thus, either $x \in \sqrt{a}$ or $y \in \sqrt{a}$. □

Remark. The converse is false. Take $A[x, y, z]/(xy - z^2)$ and $\mathfrak{p} = (\bar{x}, \bar{z})$ then $A/\mathfrak{p} \cong k[\bar{y}]$ is a domain so $\mathfrak{p}$ is prime. However, $\bar{x} \cdot \bar{y} = \bar{z}^2$ and $\bar{x} \notin \mathfrak{p}^2$ and $\bar{y}^m \notin \mathfrak{p}^2$ for all m. However, if $\mathfrak{m} \subset A$ is maximal then $\mathfrak{m}^m$ is primary because if $y \in A/\mathfrak{m}^m$ is a zero divisor then ...

Lemma 7.14. Let A be Noetherian then any irreducible ideal of A is primary.

Proof. Let $\mathfrak{a} \subset A$ be an irreducible ideal. Then $(0) \subset A/\mathfrak{a}$ is irreducible. Consider a zero divisor x such that $xy = 0$ with $y \neq 0$ then,

$$\mathrm{Ann}_A(x^n) = \{z \in A \mid z \cdot x^n = 0\}$$

and,

$$\mathrm{Ann}_A(x^n) \subset \mathrm{Ann}_A\left(x^{n+1}\right)$$

but since A is Noetherian, this chain must terminate so there exits m such that $\mathrm{Ann}_A(x^m) = \mathrm{Ann}_A(x^{m+1})$. I claim that $(x^n) \cap (y) = (0)$. If $ax^m = by$ then $ax^{m+1} = bxy = 0$ so $a \in \mathrm{Ann}_A(x^m) = \mathrm{Ann}_A(x^{m+1})$ but then $ax^m = 0$ proving the claim. Since (0) is irreducible and $(y) \neq 0$ we have $(x^m) = 0$ so x is nilpotent. □

Definition: We say that $I \subset A$ has a primary decomposition if we can write,

$$I = \mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_m$$

where each $\mathfrak{a}_i$ is primary.

Lemma 7.15. A is Noetherian if and only if every nonempty set of ideals of A has a maximial element.

Proof. If A is noetherian and $S \neq \varnothing$ then if $\in S$ is not maximal there must exist $\mathfrak{a}_1 \in S$ such that $\mathfrak{a} \subsetneq \mathfrak{a}_1$ and if $\mathfrak{a}_1$ is not maximal then there must exist $\mathfrak{a}_2 \in S$ such that $\mathfrak{a} \subset \mathfrak{a}_1 \subset \mathfrak{a}_2$. Therefore, we can produce an strictly increasing chain of ideals contradicting the Noetherian assumption unless S has a maximal element. Conversely, any chain which does not terminate will give a set S with no maximal element. □

Remark. A is Artinian if and only if every nonempty set of ideals of A has a minimal element. The proof is identical.

Corollary 7.16. If A is Noetherian then any ideal has a primary decomposition.

Proof. Let S be a the set of proper ideals that cannot be written as an intersection of irreducible ideals. Assume that $S \neq \varnothing$. Because A is Noetherian, we can find $I \in S$ which is maximal in S. Since $I \in S$ then I is not irreducible so we can write $I = \mathfrak{a} \cap \mathfrak{b}$ with $\mathfrak{a}, \mathfrak{b}$ strictly above I so $\mathfrak{a}, \mathfrak{b} \notin S$ by maximality and thus $\mathfrak{a}$ and $\mathfrak{b}$ are the intersection of irreducible ideals and thus so is S which is a contradiction. Thus, every ideal of A is the intersection of irreducibles but since A is Noetherian, every irreducible is primary. $\square$

7.1 Results on Artinian Rings

Lemma 7.17. Suppose that $IJ \subset \mathfrak{p}$ where $\mathfrak{p}$ is prime then either $I \subset \mathfrak{p}$ or $J \subset \mathfrak{p}$.

Proof. Assume that $J \not\subset \mathfrak{p}$ then for each $x \in I$ take some $y \in J \setminus \mathfrak{p}$. We know that $xy \in \mathfrak{p}$ but $y \notin \mathfrak{p}$ and $\mathfrak{p}$ is prime so $x \in \mathfrak{p}$. Thus, $I \subset \mathfrak{p}$. $\square$

Corollary 7.18. If $\mathfrak{m}_1, \cdots, \mathfrak{m}_n$ are (not necessarily distinct) maximal ideals and $\mathfrak{m}$ is maximal such that $\mathfrak{m}_1, \cdots, \mathfrak{m}_n \subset \mathfrak{m}$ then $\mathfrak{m} = \mathfrak{m}_i$ for some $i \in \{1, \dots, n\}$.

Proof. Since $\mathfrak{m}$ is maximal it is also prime and thus either $\mathfrak{m}_1, \cdots, \mathfrak{m}_{n-1} \subset \mathfrak{m}$ or $\mathfrak{m}_n \subset \mathfrak{m}$. By induction, there is some $i \in \{1, \dots, n\}$ such that $\mathfrak{m}_i \subset \mathfrak{m}$. However, $\mathfrak{m}_i$ is maximal and $\mathfrak{m}$ is proper so $\mathfrak{m}_i = \mathfrak{m}$. $\square$

Proposition 7.19. Assume A is Artinian then,

1. Every prime ideal is maximal ($\dim A = 0$). In particular, $\mathrm{rad}\,(A) = \mathrm{nilrad}\,(A)$.
2. A has finitely many maximal ideals.
3. $\mathrm{rad}\,(A)$ is nilpotent.

Proof. Let $\mathfrak{p} \subset A$ be prime and $B = A/\mathfrak{p}$. Take $x \in B \setminus \{0\}$. Since $\pi : A \to B$ is a surjection, B inherits the Artinian property. We have a chain,

$$B \supset (x) \supset (x^2) \supset (x^3) \supset \cdots$$

which must become stationary at some n. Thus $(x^{n+1}) = (x^n)$ so $\exists u \in B^\times : ux^{n+1} = x^n$. Thus, $(xu - 1)x^n = 0$ but B is an integral domain since $\mathfrak{p}$ is prime so $xu = 1$ in B. Therefore, B is a field. Therefore $\mathfrak{p}$ is maximal.

Suppose that $\mathfrak{m}_1, \mathfrak{m}_2, \dots$ are maximal ideals. Consider the chain,

$$\mathfrak{m}_1 \supset \mathfrak{m}_1\mathfrak{m}_2 \supset \mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3 \supset \cdots$$

which must become stationary. Therefore, there exists a number k such that for all $n > k$,

$$\mathfrak{m}_1 \cdots \mathfrak{m}_k = \mathfrak{m}_1 \cdots \mathfrak{m}_k \mathfrak{m}_{k+1} \cdots \mathfrak{m}_n \subset \mathfrak{m}_n$$

Thus, there must be some $i \in \{1, \dots, k\}$ such that $\mathfrak{m}_i \subset \mathfrak{m}_n$ because $\mathfrak{m}_n$ is prime. This implies that $\mathfrak{m}_i = \mathfrak{m}_n$ by maximality. Thus, there are only finitly many maximal ideals.

Let $I = \text{rad}\,(A)$ and consider the chain,

$$I \supset I^2 \supset I^3 \supset \cdots$$

which must become stationary. Thus, for some $n > 0$ we have $I^n = I^{n+1}$. Consider,

$$J = \{x \in A \mid x \cdot I^n = 0\}$$

we want to show that $J = A$. Asume $J \subsetneq A$ let $J' \supsetneq J$ be minimal for ideals above J which exists because A is Artinian. Then take $x \in J' \setminus J$ so,

$$J' \supset Ax + J \supsetneq J \implies J' = Ax + J$$

by minimailty. Furthermore,

$$J \subset Ix + J \subset J'$$

so by minimality one inclusion must be equality. However if $Ix + J = J'$ then by Nakayama $J = J'$ which is false. Thus, $Ix + J = J$ so $xI \subset J$. Therefore,

$$x \cdot I^{n+1} \subset JI^n = (0)$$

which implies that,

$$x \cdot I^{n+1} = 0 \implies x \cdot I^n = 0 \implies x \in J$$

contradicting the fact that we choose $x \notin J$. Thus, $J = A$ so $1 \in J$ and thus $I^n = 0$ so I is nilpotent. $\square$

Definition: Let A be a ring.

1. We say that an A-module $M \neq (0)$ is irreducible if any submodule $N \subset M$ is either $N = (0)$ or $N = M$.
2. We say that an A-module M is of finite length if there exists a filtration

   $$M = M_0 \supset M_1 \supset \cdots \supset M_n \supset M_{n+1} = 0$$

   such that M_i / M_{i+1} is irreducible for each u. In that case $\text{length}_A\,(M) = n$. If A is not finite length then $\text{length}_A\,(M) = \infty$.

Lemma 7.20. Given ideals $I, J \subset A$ such that $I + J = A$ then,

$$A/IJ \cong (A/I) \times (A/J)$$

Proof. $\square$

Corollary 7.21. If $\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_n \subset A$ are pairwise coprime ideals i.e. $\mathfrak{a}_i + \mathfrak{a}_j = A$ for all $i \neq j$ then,

$$A/(\mathfrak{a}_1\mathfrak{a}_2 \cdots \mathfrak{a}_n) \cong \prod_{i=1}^{n} A/\mathfrak{a}_i$$

Lemma 7.22.

Proposition 7.23. A is Artinian iff $\operatorname{length}_A(A)$ is finite.

Proof. Assume that $\operatorname{length}_A(A) < \infty$ then we have a filtration

$$A \supset M_1 \supset M_2 \supset \cdots \supset M_n \supset M_{n+1} = (0)$$

with M_i/M_{i+1} irreducible. Let $\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \mathfrak{a}_3 \supset \cdots$ be a decreasing chain of ideals in A. Consider, ☐

Remark. If A is a field then $\operatorname{length}_A(M) = \dim M$.

Lemma 7.24. If we have an exact sequence of A-modules,

$$0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$$

then N has finite length $\iff$ P and M do as well and

$$\operatorname{length}_A(N) = \operatorname{length}_A(M) + \operatorname{length}_A(P)$$

Lemma 7.25. If

$$M = M_0 \supset M_1 \supset \cdots \supset M_n \supset M_{n+1} = 0$$

then M_i/M_{i+1} has finite length for all i if and only if M has finite length.

Theorem 7.26. A is Artinian $\iff$ A is Noetherian and any prime ideal is maximal.

Proof. Since A is Artinian we know that A has finite length ☐

Proposition 7.27. Let A be a Noetherian local ring with maxmal ideal $\mathfrak{m}$. Then exactly one of the two holds.

1. $\mathfrak{m}^{n+1} \subsetneq \mathfrak{m}^n$ for all $n \geq 0$.
2. $\mathfrak{m}^n = 0$ for some $n \geq 1$ and A is Artinian.

Proof. The descending chain of powers of $\mathfrak{m}$ does indeed stabilize at n then take $B = A/\mathfrak{m}^n$ which has finite length. Furthermore, by Nakayama, $\mathfrak{m}^n = 0$. Thus, A is Artinian. ☐

Proposition 7.28. An Artinian ring is isomorphic to a finite product of local Artinian rings.

Proof. Let $I = \operatorname{rad}(A)$ then $I^n = 0$ for some $n \geq 1$. Since A is Artinian, it must have a finite number of maximal ideals,

$$\mathfrak{m}_1^n \cdots \mathfrak{m}_r^n = 0$$

Since the ideal is zero,

$$A = A / \prod_{i=1}^{r} \mathfrak{m}_i^n = \prod_{i=1}^{r} A/\mathfrak{m}_i^n$$

However, $A/\mathfrak{m}_i^n$ is a local ring. Suppose that $\mathfrak{a} \subset A/\mathfrak{m}_i^n$ is maximal. The projection map $\pi : A \to A/\mathfrak{m}_i^n$ is surjective so $\pi^{-1}(\mathfrak{a})$ is maximal and contains $\mathfrak{m}_i^n$ so $\pi^{-1}(\mathfrak{a}) = \mathfrak{m}_i$. Since π is surjective, $\pi(\pi^{-1}(\mathfrak{a})) = \mathfrak{a} = \pi(\mathfrak{m})$ so the maximal ideal is unique. ◻

8 Primary Decomposition

8.1 Associated Primes

Definition: Let A be Noetherian and M an A-module we say that a prime ideal $\mathfrak{p} \subset A$ is an associated prime of M if there exists an injective map of A-modules,

$$A/\mathfrak{p} \hookrightarrow M$$

We say that $\operatorname{Ass}_A(M)$ is the set of associated primes to M.

Lemma 8.1. $\mathfrak{p} \in \operatorname{Ass}_A(M) \iff \exists m \in M : \mathfrak{p} = \operatorname{Ann}_A(m)$

Proof. If $\mathfrak{p} \in \operatorname{Ass}_A(M)$ then there is a map $\phi : A/\mathfrak{p} \to M$ and take $m = \phi(1)$. If $x \in \mathfrak{p}$ then $[x] = 0$ in $A/\mathfrak{p}$ so $x \cdot m = \phi(x \cdot 1) = 0$. Furthermore, if $x \cdot m = 0$ in M then $x \cdot \phi(1) = 0$ so $\phi(x \cdot 1) = 0 \implies x \cdot 1 = x = 0$ in $A/\mathfrak{p}$ by injectivity. Thus, $x \in \mathfrak{p}$ so $\mathfrak{p} = \operatorname{Ass}_A(M)$. Likewise, if there exists m such that $\mathfrak{p} = \operatorname{Ann}_A(m)$ then take the map $A \to M$ given by $x \mapsto xm$. Since the kernel of this map is $\mathfrak{p} = \operatorname{Ann}_A(m)$ its factors through an injective map,

$$A/\mathfrak{p} \hookrightarrow M$$

which implies that $\mathfrak{p} \in \operatorname{Ass}_A(M)$. ◻

Lemma 8.2. The set $\{\operatorname{Ann}_A(m) \mid m \in M \setminus \{0\}\} = S_M$ then any maximal element in S_M a prime ideal. In particular if $M \neq (0)$ then $\operatorname{Ass}_A(M) \neq 0$.

Proof. Let $\mathfrak{p} \in S_M$ be maximal and take $a, b \in A$ then $\mathfrak{p} = \operatorname{Ann}_A(m)$ for $m \neq 0$. Suppose $ab \in \mathfrak{p}$. If $bm = 0 \implies b \in \mathfrak{p}$ and if $bm \neq 0$ then $\operatorname{Ann}_A(m) \subset \operatorname{Ann}_A(bm) \in S_M$ so $\operatorname{Ann}_A(bm) = \mathfrak{p}$ by maximality. Therfore, $abm = 0 \implies a \in \operatorname{Ann}_A(bm) = \mathfrak{p}$. ◻

Corollary 8.3. Let A be Noetherian and M an A-module. We have the following,

1. $$M \neq (0) \iff \operatorname{Ass}_A(M) \neq \varnothing$$

2.
$$\bigcup_{\mathfrak{p} \in \mathrm{Ass}_{\mathfrak{p}}(M)} \mathfrak{p} = \{a \in A \mid \exists m \neq 0 : am = 0\}$$

Proof. Since M is Noetherian and $M \neq (0)$ then S_M has a maximal element since every chain has a maximum by the Noetherian property. Thus $\mathrm{Ass}_A(M) \neq \varnothing$. The second follows from the maximality of the associated primes in the set of annihilators and the fact that the zero divisors are those annilatred by some element and thus the union over all annihilators. □

Lemma 8.4. Let $S \subset A$ be a multiplicative subset and M and A-module. Then,

$$\mathrm{Ass}_A\left(S^{-1}M\right) = \pi^{-1}\left(\mathrm{Ass}_{S^{-1}A}\left(S^{-1}M\right)\right) = \mathrm{Ass}_A(M) \cap \{\mathfrak{p} \mid \mathfrak{p} \cap S = \varnothing\}$$

Proof. Take $\mathfrak{p} \in \mathrm{Ass}_A(S^{-1}M)$ then $\mathfrak{p} = \mathrm{Ann}_A\left(\frac{m}{1}\right) = \mathrm{Ann}_A\left(\frac{m}{s}\right)$ for any $s \in S$ since $\frac{am}{1} = 0 \iff \frac{am}{s} = 0$ in $S^{-1}M$. Suppose that $\mathfrak{p} \cap S = \varnothing$ otherwise $\exists s \in \mathfrak{p} \cap S$ which implies that $\frac{sm}{1} = 0$ so $\frac{m}{1} = 0$ but $\mathfrak{p} = \mathrm{Ann}_A(0) = A$ is not prime. The set $\{\mathrm{Ann}_A(sm) \mid s \in S\}$ has a maximal element $\mathfrak{m} = \mathrm{Ann}_A(s_0 m)$. We know that $\mathfrak{m}$ annihilates $\frac{s_0 m}{1}$ and thus $\frac{m}{1}$ so $\mathfrak{m} \subset \mathfrak{p}$. Furthermore, if $a \in \mathfrak{p} = \mathrm{Ann}_A\left(\frac{m}{1}\right)$ then $\frac{am}{1} = 0 \implies \exists s \in S : asm = 0$ so, by maximality,

$$a \in \mathrm{Ann}_A(sm) \subset \mathrm{Ann}_A(ss_0 m) = \mathrm{Ann}_A(s_0 m) = \mathfrak{m}$$

so $a \in \mathfrak{m}$. Thus, $\mathfrak{p} = \mathfrak{m} \in \mathrm{Ass}_A(M)$. Now, take $\mathfrak{p}_0 \in \mathrm{Ass}_{S^{-1}A}(S^{-1}M)$ such that,

$$\mathfrak{p}_0 = \{x \in S^{-1}A \mid x \cdot \tfrac{m}{1} = 0\}$$

for some $m \in M$. Then we have,

$$\pi^{-1}(\mathfrak{p}_0) = \mathrm{Ann}_A\left(\frac{m}{1}\right) \implies \pi^{-1}(\mathfrak{p}_0) \in \mathrm{Ass}_A\left(S^{-1}M\right)$$

□

Definition: Let M an A-module,

$$\mathrm{Supp}_A(M) = \{\mathfrak{p} \in \mathrm{Spec}(A) \mid M_{\mathfrak{p}} \neq 0\}$$

Proposition 8.5. Let M be a finitely generated A-module then $\mathrm{Supp}_A(M) = V(\mathrm{Ann}_A(M))$.

Proof. $M_{\mathfrak{p}} = (0)$ exactly when $(m, s) \sim (0, 1)$ for all m and s. This happens when $\exists u \in A \setminus \mathfrak{p}$ such that $um = 0$ i.e. $u \in \mathrm{Ann}_A(m)$. Thus, for each $m \in M$ we have $\mathfrak{p} \not\supset \mathrm{Ann}_A(m)$. Therefore,

$$\mathfrak{p} \in \mathrm{Supp}_A(M) \iff M_{\mathfrak{p}} \neq (0) \iff \exists m \in M : \mathfrak{p} \supset \mathrm{Ann}_A(m)$$

I claim that, $\mathfrak{p} \supset \mathrm{Ann}_A(M) \iff \exists m \in M : \mathfrak{p} \supset \mathrm{Ann}_A(m)$. If $\mathfrak{p} \supset \mathrm{Ann}_A(M)$ then,

$$\mathfrak{p} \supset \bigcap_{m \in M} \mathrm{Ann}_A(m) = \bigcap_{i=1}^{n} \mathrm{Ann}_A(m_i)$$

where $M = Am_1 + \cdots + Am_n$ which implies $\mathfrak{p} \supset \mathrm{Ann}_A(m_i)$ for some i. Also, if $\mathfrak{p} \supset \mathrm{Ann}_A(m)$ then $\mathfrak{p} \supset \mathrm{Ann}_A(m) \supset \mathrm{Ann}_A(M)$. Therefore,

$$\mathfrak{p} \in \mathrm{Supp}_A(M) \iff \mathfrak{p} \supset \mathrm{Ann}_A(M)$$

□

Remark. If M is not necessarily finitely generated, we still have,

$$\mathrm{Supp}_A(M) \subset V(\mathrm{Ann}_A(M))$$

Theorem 8.6. Let A be Noetherian and M an A-module. Then,

$$\mathrm{Ass}_A(M) \subset \mathrm{Supp}_A(M)$$

and any minimal element in $\mathrm{Supp}_A(M)$ is an associated prime.

Proof. Let $\mathfrak{p} \in \mathrm{Ass}_A(M)$ then $M_\mathfrak{p} \neq 0$ since an injective map $A/\mathfrak{p} \to M$ means that $M_\mathfrak{p} \neq 0$ since $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \neq 0$ lies inside. Pick $\mathfrak{p} \in \mathrm{Supp}_A(M)$ minimal so $M_\mathfrak{p} \neq 0$ then there exists $\mathfrak{q}_0 \in \mathrm{Ass}_{A_\mathfrak{p}}(M_\mathfrak{p}) \neq \varnothing$ so $\mathfrak{q}_0 = \mathfrak{q}A_\mathfrak{p}$ for some prime ideal $\mathfrak{q} \subset \mathfrak{p}$ so $\mathfrak{q}_0 \in \mathrm{Supp}_{A_\mathfrak{p}}(M_\mathfrak{p}) \implies (M_\mathfrak{p})_{q_0} = M_\mathfrak{q} \neq 0$. However, $\mathfrak{p}$ is minimal in $\mathrm{Supp}_A(M)$ so $\mathfrak{q} = \mathfrak{p} \implies \mathfrak{q}_0 = \mathfrak{p}A_\mathfrak{p}$ so $\mathfrak{p}A_\mathfrak{p} \in \mathrm{Ass}_{A_\mathfrak{p}}(M_\mathfrak{p})$ so $\mathfrak{p} \in \mathrm{Ass}_A(M_\mathfrak{p})$ so $\mathfrak{p} \in \mathrm{Ass}_A(M)$ by the previous lemma for $S = A \setminus \mathfrak{p}$. □

Proposition 8.7. Let A be Noetherian and M an A-module then $\mathfrak{p} \in \mathrm{Supp}_A(M)$ if and only if there exists $\mathfrak{q} \subset \mathfrak{p}$ with $\mathfrak{q} \in \mathrm{Ass}_A(M)$. Therefore,

$$\bigcap_{\mathfrak{p} \in \mathrm{Supp}_A(M)} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \mathrm{Ass}_A(M)} \mathfrak{p}$$

Proof. Take $\mathfrak{p} \in \mathrm{Supp}_A(M)$ so $M_\mathfrak{p} \neq 0$. Thus, since A is Noetherian, $\mathrm{Ass}_A(M_\mathfrak{p}) \neq \varnothing$ so there exists $\mathfrak{q} \in \mathrm{Ass}_A(M_\mathfrak{p}) = \mathrm{Ass}_A(M) \cap \{\mathfrak{q} \mid \mathfrak{q} \subset \mathfrak{p}\}$. Furthermore, if $\mathfrak{q} \subset \mathfrak{p}$ and $\mathfrak{q} \in \mathrm{Supp}_A(M)$ then $\mathfrak{q} \supset \mathrm{Ann}_A(x)$ for some $x \in M$ and thus $\mathfrak{p} \supset \mathrm{Ann}_A(x)$ so $\mathfrak{p} \in \mathrm{Supp}_A(M)$. The support is an upward set. Furthermore, if we have $\mathfrak{q} \subset \mathfrak{p}$ with $\mathfrak{q} \in \mathrm{Ass}_A(M) \subset \mathrm{Supp}_A(M)$ then $\mathfrak{p} \in \mathrm{Supp}_A(M)$. □

Lemma 8.8. Assume that we have an exact sequence,

$$0 \longrightarrow N \longrightarrow M \longrightarrow P$$

of A-modules. Then,

$$\mathrm{Ass}_A(M) \subset \mathrm{Ass}_A(N) \cup \mathrm{Ass}_A(P)$$

Proof. If $\mathfrak{p} \in \mathrm{Ass}_A(M)$ then we have an embedding

$$A/\mathfrak{p} \hookrightarrow M$$

which is injective and $\iota(A/\mathfrak{p}) \cap N = (0)$ then we get an injective map $A/\mathfrak{p} \to P$ so $\mathfrak{p} \in \mathrm{Ass}_A(P)$. If $\iota(A/\mathfrak{p}) \cap N \neq (0)$ then take nonzero $n \in \iota(A/\mathfrak{p}) \cap N$. Then $\mathrm{Ann}_A(n) = \mathrm{Ann}_A(\iota(x))$ for $x \in A/\mathfrak{p}$ nonzero. However, if $a \cdot \iota(x) = 0$ then $\iota(a \cdot x) = 0$ but ι is injective so $a \cdot x = 0$ and thus $\mathrm{Ann}_A(\iota(x)) = \mathrm{Ann}_A(x) = \mathfrak{p}$ because if $a \cdot x \in \mathfrak{p}$ for $x \notin \mathfrak{p}$ then $a \in \mathfrak{p}$. □

Proposition 8.9. Let A be Noetherian and M a finitely generated A-module. Then,

1. Ther exists a filtration $(0) = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_n = M$ such that $M_{i+1}/M \cong A/\mathfrak{p}_{i+1}$ for some $\mathfrak{p}_i \in \operatorname{Supp}_A(M)$.

2. $\operatorname{Ass}_A(M) \subset \{\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_n\}$.

Proof. Take $\mathfrak{p} \in \operatorname{Ass}_A(M)$ so we have an injection $A/\mathfrak{p} \to M$ let $M_1 \subset M$ be the image of this map so $M_1/M_0 \cong A/\mathfrak{p}_1$. Now take M/M_1 and $\mathfrak{p}_2 \in \operatorname{Ass}_A(M/M_1)$ then we have an injection $A/\mathfrak{p}_2 \to M/M_1$ so take $\bar{M}_2$ to be the image inside M/M_1 and M_2 its preimage in M. Since $M_{i+1}/M_i = A/\mathfrak{p}_i$ then

$$\mathfrak{p}_i \in \operatorname{Ass}_A(M_{i+1}/M_i) \subset \operatorname{Supp}_A(M_{i+1}/M_i) \subset \operatorname{Supp}_A(M)$$

Then we construct a sequence,

$$0 \subsetneq M_1 \subsetneq M_2 \subsetneq M_3 \subsetneq \cdots$$

However, M is Noetherian so this sequence must stabilize but it is striclty increasing when M_i is proper. Thus, $M_n = M$ for some n.

Using the filtration, we have,

$$0 \longrightarrow M_i \longrightarrow M_{i+1} \longrightarrow A/\mathfrak{p}_{i+1} \longrightarrow 0$$

Assume for induction that $\operatorname{Ass}_A(M_i) \subset \{\mathfrak{p}_1, \dots, \mathfrak{p}_i\}$ then, using the above lemma,

$$\operatorname{Ass}_A(M_{i+1}) \subset \operatorname{Ass}_A(M_i) \cup \operatorname{Ass}_A(A/\mathfrak{p}_{i+1}) \subset \{\mathfrak{p}_1, \dots, \mathfrak{p}_{i+1}\}$$

proving (2) by induction. □

Definition: An A-module M is called coprimary if $\operatorname{Ass}_A(M) = \{\mathfrak{p}\}$ and if $N \subset M$ we say that N is $\mathfrak{p}$-primary if M/N is coprimary with $\operatorname{Ass}_A(M/N) = \{\mathfrak{p}\}$.

Lemma 8.10. *M is coprimary iff any zero divisor of M is locally nilpotent i.e. if $a \cdot m = 0$ for some $m \in M \setminus \{0\}$ then $\forall m' \in M : a^n \cdot m' = 0$ for some n.*

Proof. Assume that M is coprimary, $\operatorname{Ass}_A(M) = \{\mathfrak{p}\}$. If $x \in M$ is nonzero then Ax is a nonzero submodule of M so $\operatorname{Ass}_A(Ax) = \{\mathfrak{p}\}$ since it is nonempty. Therefore, $\mathfrak{p}$ is a minimal element in $\operatorname{Supp}_A(Ax) = V(\operatorname{Ann}_A(x))$ because $Ax \cong A/\operatorname{Ann}_A(x)$. Thus, $\sqrt{\operatorname{Ann}_A(x)} = \mathfrak{p}$. If a is a zero divisor of M then $a \in \mathfrak{p}$ so $a^n \in \operatorname{Ann}_A(x)$ so a is locally nilpotent. Converely, assume that the set of zero divisors equals the set of locally nilpotent elements. Take $\mathfrak{p}$ to be the ideal of all locally nilpotents. Take $\mathfrak{q} \in \operatorname{Ass}_A(M)$ then $\mathfrak{q} = \operatorname{Ann}_A(x)$ for some x and $a \in \mathfrak{p}$ then $a^n \cdot x = 0$ for some n implies that $a^n \in \mathfrak{q}$ so $a \in \mathfrak{q}$. so $\mathfrak{p} \subset \mathfrak{q}$. Furthermore,

$$\bigcup_{\mathfrak{q} \in \operatorname{Ass}_A(M)} \mathfrak{q} = \{\text{zero divisors}\} = \mathfrak{p}$$

so for any $\mathfrak{q} \in \operatorname{Ass}_A(M)$ we have $\mathfrak{q} \subset \mathfrak{p}$. Thus, $\mathfrak{p} = \mathfrak{q}$ so $\operatorname{Ass}_A(M)$ constains a unique prime. □

Corollary 8.11. If $I \subset A$ is an ideal then $\text{Ass}_A(A/I) = \{\mathfrak{p}\}$ if and only if I is a primary ideal and in that case $\sqrt{I} = \mathfrak{p}$.

Proof. Consider $I \subset A$ and A/I is coprimary then take $x, y \in A$ such that $y \notin I$ and $\bar{x} \cdot \bar{y} = 0$ in A/I. Then $\bar{x}$ is a zero divisor of A/I so it is locally nilpotent by the above. Thus, $\bar{x}^n \cdot 1 = 0$ for some n so $x^n \in I$ so $x \in \sqrt{I}$ and thus I is primary. Furthermore,

$$\sqrt{I} = \bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \text{Supp}_A(A/I)} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \text{Ass}_A(A/I)} \mathfrak{p} = \mathfrak{p}$$

since $\text{Ass}_A(M)$ is the set of minimal primes of $\text{Supp}_A(M)$ and $\text{Ass}_A(A/I) = \mathfrak{p}$. $\square$

Corollary 8.12. Let $\mathfrak{p} \subset A$ be prime. Then $\text{Ass}_A(A/\mathfrak{p}) = \{\mathfrak{p}\}$.

Definition: Le M be an A-module and $N \subset M$ we say that N has a primary decomposition if,

$$N = Q_1 \cap Q_2 \cap \cdots \cap Q_n$$

where each Q_i is primary. Moreover, we say that this decomposition is irredundant if

1. if $i \neq j$ then $\text{Ass}_A(M/Q_i) \neq \text{Ass}_A(M/Q_j)$
2. we cannot remove any Q_j from the intersection.

Lemma 8.13. Let M be an A-module then,

1. If $Q_1, Q_2 \subset M$ are $\mathfrak{p}$-primary then $Q_1 \cap Q_2$ is $\mathfrak{p}$-primary.
2. If $N = Q_1 \cap \cdots \cap Q_n$ is a irredundant primary decomposition and for each i, Q_i is $\mathfrak{p}_i$-primary then,
$$\text{Ass}_A(M/N) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$$

Proof. Consider the injection,

$$0 \longrightarrow M/Q_1 \cap Q_2 \hookrightarrow M/Q_1 \oplus M/Q_2$$

which implies that,

$$\text{Ass}_A(M/Q_1 \cap Q_2) \subset \text{Ass}_A(M/Q_1 \oplus M/Q_2) = \text{Ass}_A(M/Q_1) \cup \text{Ass}_A(M/Q_2) = \{\mathfrak{p}\}$$

proving the first. For the second, consider the injection,

$$M/N \hookrightarrow M/Q_1 \oplus \cdots \oplus M/Q_n$$

which implies that,

$$\text{Ass}_A(M/N) \subset \text{Ass}_A(M/Q_1) \cup \cdots \cup \text{Ass}_A(M/Q_n) \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$$

We need to show that $\mathfrak{p}_i \in \text{Ass}_A(M/N)$ for each i. We have the exact sequence,

$$0 \longrightarrow N \longrightarrow Q_2 \cap \cdots \cap Q_n \longrightarrow M/Q_1$$

and therefore,

$$(Q_2 \cap \cdots \cap Q_n)/N \hookrightarrow M/Q_1$$

which implies that,

$$\operatorname{Ass}_A((Q_2 \cap \cdots \cap Q_n)/N) \subset \operatorname{Ass}_A(M/Q_1) = \{\mathfrak{p}_1\}$$

so since it is nonempy we have,

$$\{\mathfrak{p}_1\} = \operatorname{Ass}_A((Q_2 \cap \cdots \cap Q_n)/N) \subset \operatorname{Ass}_A(M/N)$$

where the inclusion holds via the exact sequence,

$$0 \longrightarrow N \longrightarrow Q_2 \cap \cdots \cap Q_n \longrightarrow M/N$$

The same argument holds for each i. $\square$

Theorem 8.14. Let M be an A-module and A Noetherian. For each $\mathfrak{p} \in \operatorname{Ass}_A(M)$, there exist $Q_\mathfrak{p} \subset M$ which are $\mathfrak{p}$-primary such that,

$$\bigcap_{\mathfrak{p} \subset \operatorname{Ass}_A(M)} Q_\mathfrak{p} = 0$$

Proof. Fix $\mathfrak{p} \in \operatorname{Ass}_A(M)$ and consider the set $S_\mathfrak{p} = \{Q \subset M \mid \mathfrak{p} \notin \operatorname{Ass}_A(Q)\} \neq \varnothing$ since we have the zero ideal. If we have a chain $\mathcal{Q} \subset S_\mathfrak{p}$ then their union,

$$U = \bigcup_{Q \in \mathcal{Q}} Q$$

is an ideal. Since A is Noetherian this union stabilizes and equals the maximal $Q \in \mathcal{Q}$. Therefore,

$$\operatorname{Ass}_A(U) = \bigcup_{Q \in \mathcal{Q}} \operatorname{Ass}_A(Q)$$

So $\mathfrak{p} \notin \operatorname{Ass}_A(U)$ so $U \in S_\mathfrak{p}$. Thus by Zorn's lemma there exists a maximal element $Q_\mathfrak{p} \in S_\mathfrak{p}$. We know,

$$\operatorname{Ann}_A(M/Q_\mathfrak{p}) \neq \varnothing$$

since we have $M/Q_\mathfrak{p} \neq (0)$. Otherwise, $M = Q_\mathfrak{p}$ which implies $\mathfrak{p} \in \operatorname{Ass}_A(Q_\mathfrak{p})$ but $Q_\mathfrak{p} \in S_\mathfrak{p}$. Let $\mathfrak{p}' \in \operatorname{Ass}_A(M/Q_\mathfrak{p})$ and suppose that $\mathfrak{p}' \neq \mathfrak{p}$ then we have,

$$A/\mathfrak{p}' \hookrightarrow M/Q_\mathfrak{p}$$

The image of this embedding is a submodule, $Q_\mathfrak{p} \subsetneq Q' \subset M$ such that $Q'/Q_\mathfrak{p} \cong A/\mathfrak{p}'$ implying that,

$$\operatorname{Ass}_A(Q'/Q_\mathfrak{p}) = \{\mathfrak{p}'\}$$

Thus we have an exact sequence,

$$0 \longrightarrow Q_\mathfrak{p} \longrightarrow Q' \longrightarrow A/\mathfrak{p} \longrightarrow 0$$

which implies that $\text{Ass}_A(Q') \subset \text{Ass}_A(Q_\mathfrak{p}) \cup \text{Ass}_A(A/\mathfrak{p}') = \text{Ass}_A(Q_\mathfrak{p}) \cup \{\mathfrak{p}'\}$. However, this contradicts the fact that $Q_\mathfrak{p}$ is maximal in $S_\mathfrak{p}$ since $Q' \in S_\mathfrak{p}$ as long as $\mathfrak{p}' \neq \mathfrak{p}$. Therefore, $\mathfrak{p}' = \mathfrak{p}$ so $\text{Ass}_A(A/Q_\mathfrak{p}) = \{\mathfrak{p}\}$. Now consider,

$$\text{Ass}_A\left(\bigcap_{\mathfrak{p}\in \text{Ass}_A(M)} Q_\mathfrak{p}\right) \subset \bigcap_{\mathfrak{p}\in \text{Ass}_A(M)} \text{Ass}_A(Q_\mathfrak{p}) = \varnothing$$

because for any $\mathfrak{p}$ we know $\mathfrak{p} \notin \text{Ass}_A(Q_\mathfrak{p})$. Therefore,

$$\bigcap_{\mathfrak{p}\in \text{Ass}_A(M)} Q_\mathfrak{p} = (0)$$

since it has no associated primes. □

Corollary 8.15. If M has finite type then any submodule has a primary decomposition.

Proof. Let $N \subset M$ be a submodule. Apply the theorem to $\bar{M} = M/N$ which has finite type so $\text{Ass}_A(M/N)$ is finite. Write, $\text{Ass}_A(M/N) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$. Therefore, there exist primary ideals Q_i such that,

$$Q_{\mathfrak{p}_1} \cap \cdots \cap Q_{\mathfrak{p}_r} = (0)$$

in M/N. Take Q_i to be the preimage of $Q_{\mathfrak{p}_i}$. Thus,

$$Q_1 \cap \cdots \cap Q_r = N$$

and

$$M/Q_i \cong \bar{M}/Q_{\mathfrak{p}_i} \implies \text{Ass}_A(M/Q_i) = \{\mathfrak{p}_i\}$$

□

9 Derived Functors

9.1 Chain Complexes

Definition: A chain complex C is a diagram,

$$\cdots \longrightarrow C_{n+1} \xrightarrow{\partial_{n+1}} C_n \xrightarrow{\partial_n} C_{n-1} \xrightarrow{\partial_{n-1}} \cdots$$

such that $\partial_n \circ \partial_{n+1} = 0$ or equivalently $\text{Im}(\partial_{n+1}) \subset \ker \partial_n$ for each n. We call ∂ the boundary map.

Similarly, a cochain complex D is equivalent but with increasing lables,

$$\cdots \longrightarrow D^{n-1} \xrightarrow{d^{n-1}} D^n \xrightarrow{d^n} D^{n+1} \xrightarrow{d^{n+1}} \cdots$$

such that $d^{n+1} \circ d^n = 0$ or equivalently $\mathrm{Im}(d^n) \subset \ker d^{n+1}$ for each n. We call d the coboundary map.

Remark. Complexes are "half exact" sequences.

Definition: A map $f : C \to D$ of (co)chain complexes is a sequnces of maps, $f_n : C_n \to D_n$ such that the diagram,

$$\begin{tikzcd}
\cdots \arrow[r] & C_{n+1} \arrow[r, "\partial_{n+1}"] \arrow[d, "f_{n+1}"] & C_n \arrow[r, "\partial_n"] \arrow[d, "f_n"] & C_{n-1} \arrow[r, "\partial_{n-1}"] \arrow[d, "f_{n-1}"] & \cdots \\
\cdots \arrow[r] & D_{n+1} \arrow[r, "\partial_{n+1}"] & D_n \arrow[r, "\partial_n"] & D_{n-1} \arrow[r, "\partial_{n-1}"] & \cdots
\end{tikzcd}$$

commutes.

Definition: Let $\mathcal{A}$ be an abelian cateogy then $\mathbf{Ch}(\mathcal{A})$ is the category of chain complexes with components in $\mathcal{A}$.

Remark. Since complexes are "half exact" sequences, we would like a way to measure how far a given complex is from being exact. This is accomplished via (co)homology.

Definition: Let C be a chain complex in $\mathbf{Ch}(\mathcal{A})$. The homology of the complex C is the sequence of $\mathcal{A}$ objects (usually abelian groups or R-modules),

$$H_n(C) = \ker \partial_n / \mathrm{Im}(\partial_{n+1})$$

We can describe this categorically via,

$$\begin{tikzcd}
C_{n+1} \arrow[r, "\partial_{n+1}"] \arrow[dr, dashed] & C_n \arrow[r, "\partial_n"] & C_{n-1} \\
& \ker \partial_n \arrow[u] \arrow[dr, dashed] & \\
& & H_n(C)
\end{tikzcd}$$

where $\partial_n \circ \partial_{n+1} = 0$ so ∂_{n+1} lifts to the kernel and $H_n(C)$ is the cokernel of this map.

Similarly, given a cochain complex D, the cohomology is the sequence

$$H^n(D) = \ker d^n / \mathrm{Im}(d^{n-1}) = 0$$

which is constructed identically.

Proposition 9.1. Taking (co)homology is a functor $H_n : \mathbf{Ch}(\mathcal{A}) \to \mathcal{A}$.

Proof. A chain map $f : C \to D$ is a diagram,

$$\begin{tikzcd}
\cdots \arrow[r] & C_{n+1} \arrow[r, "\partial_{n+1}"] \arrow[d, "f_{n+1}"] & C_n \arrow[r, "\partial_n"] \arrow[d, "f_n"] & C_{n-1} \arrow[r, "\partial_{n-1}"] \arrow[d, "f_{n-1}"] & \cdots \\
\cdots \arrow[r] & D_{n+1} \arrow[r, "\partial_{n+1}"] & D_n \arrow[r, "\partial_n"] & D_{n-1} \arrow[r, "\partial_{n-1}"] & \cdots
\end{tikzcd}$$

so if $x \in \ker \partial_n$ then $\partial_n \circ f(x) = f(\partial_n x) = 0$ so $f(x) \in \ker \partial_n$. Furthermore, if $x \in \mathrm{Im}(\partial_{n+1})$ then $f(x) \in f(\mathrm{Im}(\partial_{n+1})) = \mathrm{Im}(\partial_{n+1} \circ f_{n+1}) \subset \mathrm{Im}(\partial_{n+1})$. Therefore, $f_* : H_n(C) \to H_n(D)$ is a well-defined map taking $[x] \mapsto [f(x)]$. Clearly $\mathrm{id}_* = \mathrm{id}_{H_n}$ and $(f \circ g)_* = f_* \circ g_*$.

Categorically, (DO THIS) □

Definition: Let $f, g : C \to D$ be morphisms of chain complexes. A *chain homotopy* $p : f \implies g$ is a sequence of maps $p_n : C_n \to D_{n+1}$ such that,

$$\partial \circ p + p \circ \partial = f - g$$

or more explicitly,

$$\partial^D_{n+1} \circ p_n + p_{n-1} \circ \partial^C_n = f_n - g_n$$

in the following diagram,

$$\begin{tikzcd}
\cdots \arrow[r] & C_{n+1} \arrow[r, "\partial^C_{n+1}"] \arrow[dl, "p_{n+1}"'] \arrow[d, shift right, "f_{n+1}"'] \arrow[d, shift left, "g_{n+1}"] & C_n \arrow[r, "\partial^C_n"] \arrow[dl, "p_n"'] \arrow[d, shift right, "f_n"'] \arrow[d, shift left, "g_n"] & C_{n-1} \arrow[r] \arrow[dl, "p_{n-1}"'] \arrow[d, shift right, "f_{n-1}"'] \arrow[d, shift left, "g_{n-1}"] & \cdots \arrow[dl, "p_{n-2}"'] \\
\cdots \arrow[r] & D_{n+1} \arrow[r, "\partial^D_{n+1}"] & D_n \arrow[r, "\partial^D_n"] & D_{n-1} \arrow[r] & \cdots
\end{tikzcd}$$

Lemma 9.2. Let $f, g : C \to D$ be chain homotopic then $f_* = g_*$ on homology.

Proof. Let $p : f \implies g$ be a chain homotopy. It suffices to show that if $\alpha \in \ker \partial$ is a cycle then $(f_* - g_*)(\alpha) = 0$ which is equivalent to $(f - g)(\alpha) \in \mathrm{Im}(\partial)$ is a boundary. Suppose that $\partial\alpha = 0$. Then,

$$(f - g)(\alpha) = (\partial \circ p + p \circ \partial)(\alpha) = \partial(p(\alpha))$$

and therefore $(f - g)(\alpha)$ is a boundary. Therefore $f_* = g_*$. □

Corollary 9.3. A chain homotopy equivalence is a quasi-isomorphism i.e. an isomorphism on homology.

Theorem 9.4. Given a short exact sequence of chain complexes,

$$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{j} C \longrightarrow 0$$

we get a long exact sequence,

$$\cdots \to H_{n+1}(A) \to H_{n+1}(B) \to H_{n+1}(C) \to H_n(A) \to H_n(B) \to H_n(C) \to H_{n-1}(A) \to H_{n-1}(B) \to H_{n-1}(C) \to H_{n-2}(A) \to H_{n-2}(B) \to H_{n-2}(C) \to \cdots$$

functorially.

Proof. Consider the diagram with exact rows,

$$\begin{tikzcd}
 & \vdots \arrow[d, "\partial^A_{n+2}"] & \vdots \arrow[d, "\partial^B_{n+2}"] & \vdots \arrow[d, "\partial^C_{n+2}"] & \\
0 \arrow[r] & A_{n+1} \arrow[r, "i"] \arrow[d, "\partial^A_{n+1}"] & B_{n+1} \arrow[r, "j"] \arrow[d, "\partial^B_{n+1}"] & C_{n+1} \arrow[r] \arrow[d, "\partial^C_{n+1}"] & 0 \\
0 \arrow[r] & A_n \arrow[r, "i"] \arrow[d, "\partial^A_n"] & B_n \arrow[r, "j"] \arrow[d, "\partial^B_n"] & C_n \arrow[r] \arrow[d, "\partial^C_n"] & 0 \\
0 \arrow[r] & A_{n-1} \arrow[r, "i"] \arrow[d, "\partial^A_{n-1}"] & B_{n-1} \arrow[r, "j"] \arrow[d, "\partial^B_{n-1}"] & C_{n-1} \arrow[r] \arrow[d, "\partial^C_{n-1}"] & 0 \\
 & \vdots & \vdots & \vdots &
\end{tikzcd}$$

An application of the snake lemma gives an exact sequence,

$$0 \to \ker \partial^A_{n+2} \to \ker \partial^B_{n+2} \to \ker \partial^C_{n+2} \xrightarrow{\delta} A_n/\mathrm{Im}(\partial^A_{n+1}) \to B_n/\mathrm{Im}(\partial^B_{n+1}) \to C_n/\mathrm{Im}(\partial^C_{n+1}) \to 0$$

where I haved added the leading and trailing zeros by by the following observations. The map $B_{n+1}/\mathrm{Im}(\partial^B_{n+2}) \to C_{n+1}/\mathrm{Im}(\partial^C_{n+2})$ simply takes $[x] \mapsto [j(x)]$ and thus is clearly surjective because j is. Furthermore the map $\ker \partial^A_n \to \ker \partial^B_n$ is simply the restriction of ι which is still injective. Therefore, we can arrange these exact rows into a commutative diagram,

$$\begin{tikzcd}
 & A_{n+1}/\mathrm{Im}(\partial^A_{n+2}) \arrow[r] \arrow[d] & B_{n+1}/\mathrm{Im}(\partial^B_{n+2}) \arrow[r] \arrow[d] & C_{n+1}/\mathrm{Im}(\partial^C_{n+2}) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \ker \partial^A_n \arrow[r] & \ker \partial^B_n \arrow[r] & \ker \partial^C_n &
\end{tikzcd}$$

where the vertical maps are simply restrictions of the boundary maps whose images lie inside the respective kernels since each column is a chain complex. Another application of the snake lemma gives the exact sequence,

$$\begin{tikzcd}
\ker \partial^A_{n+1}/\mathrm{Im}(\partial^A_{n+2}) \arrow[r] & \ker \partial^B_{n+1}/\mathrm{Im}(\partial^B_{n+2}) \arrow[r] & \ker \partial^C_{n+1}/\mathrm{Im}(\partial^C_{n+2}) \arrow[dll, rounded corners, to path={ -- ([xshift=2ex]\tikztostart.east) |- node[near end, above]{\scriptstyle \delta} ([yshift=3ex]\tikztotarget.north) -- (\tikztotarget)}] \\
\ker \partial^A_{n}/\mathrm{Im}(\partial^A_{n+1}) \arrow[r] & \ker \partial^B_{n}.\mathrm{Im}(\partial^B_{n+1}) \arrow[r] & \ker \partial^C_{n}/\mathrm{Im}(\partial^C_{n+1})
\end{tikzcd}$$

Stringing together these long exact sequences (which we can do because they overlap at two points) gives the required long exact sequence. □

9.2 Injective and Projective Resolutions

Definition: P is a projective object if for any map $f : P \to X$ and epimorphism (surjection) $g : Y \to X$ the map f lifts to Y. This means there always exists a map such that the diagram,

$$\begin{tikzcd}
 & Y \arrow[d, two heads, "g"] \\
P \arrow[ur, dashed, "\tilde{f}"] \arrow[r, "f"'] & X
\end{tikzcd}$$

commutes. The slogan is: "projective objects lift over surjections".

Lemma 9.5. Any exact sequence ending in a projective object splits.

Proof. Consider the exact sequence where P is projective,

$$\begin{tikzcd}
 & & & P \arrow[dl, dashed] \arrow[d, "\mathrm{id}_P"] & \\
0 \arrow[r] & A \arrow[r] & B \arrow[r, two heads, "f"] & P \arrow[r] & 0
\end{tikzcd}$$

The induced map is a right inverse of f so the sequence is right-split. □

Definition: A projective resolution of A is an exact sequence,

$$\cdots \longrightarrow P_3 \xrightarrow{\partial_3} P_2 \xrightarrow{\partial_2} P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{p_0} A \longrightarrow 0$$

such that each P_i is projective. We will write this situation schematically as,

$$\mathbf{P}^A \xrightarrow{p_0} A \longrightarrow 0$$

Proposition 9.6. The category $\mathbf{Mod}_R$ has *enough* projectives. i.e. every R-module has a projective resolution

Proof. We will use the fact that for any R-module M there exists a free module F and a surjection $F \to M$ (take the free module on all the elements of M). Furthermore free modules are projective because any map can be defined by sending the generators to arbitrary lifts.

Let $P_0 = F$ and consider the kernel K_0 of $P_0 \to M$. Then, we can construct a free module surjecting onto K_0 call this P_1. We repeat this process inductivly to get the diagram,

$$\begin{tikzcd}
\cdots \arrow[r] & P_3 \arrow[rr, "\partial_3"] \arrow[dr] & & P_2 \arrow[rr, "\partial_2"] \arrow[dr] & & P_1 \arrow[rr, "\partial_1"] \arrow[dr] & & P_0 \arrow[r, "\epsilon"] & M \arrow[r] & 0 \\
& & K_2 \arrow[ur] \arrow[dr] & & K_1 \arrow[ur] \arrow[dr] & & K_0 \arrow[ur] \arrow[dr] & & & \\
& 0 \arrow[ur] & & 0 \arrow[ur] & & 0 \arrow[ur] & & 0 & &
\end{tikzcd}$$

where the diagonals are exact. The map $P_{n+1} \to P_n$ factors through the kernel K_n and thus goes to zero under $P_n \to P_{n-1}$. Furthermore, $P_{n+1} \to K_n$ is a surjection so the map $P_{n+1} \to P_n$ surjects onto the kernel. Thus the top row is exact. $\square$

Proposition 9.7. Every projective module is a direct factor of a free module.

Proof. Let P be projective and F be a free module surjecting onto P. Then we know that the exact sequence,

$$0 \longrightarrow \ker\phi \longrightarrow F \longrightarrow P \longrightarrow 0$$

splits because P is projective. Thus, $F \cong \ker\phi \oplus P$. $\square$

Definition: I is an injective object if for any map $f : X \to I$ and monomorphism (injection) $g : X \to Y$ the map f extends to Y. This means there always exists a map such that the diagram,

$$\begin{tikzcd}
I & X \arrow[l, "f"'] \arrow[d, hook, "g"] \\
& Y \arrow[ul, dashed, "\tilde{f}"]
\end{tikzcd}$$

commutes. The slogan is: "injective objects extend over injections."

Definition: An injective resolution of A is an exact sequence,

$$0 \longrightarrow A \xrightarrow{\iota_0} I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \xrightarrow{d^2} I^3 \longrightarrow \cdots$$

such that each I^i is projective. We will write this situation schematically as,

$$0 \longrightarrow A \xrightarrow{\iota_0} \mathbf{I}_A$$

Lemma 9.8. Any exact sequence begining with an injective object splits.

Proof. Consider the exact sequence where I is projective,

$$\begin{tikzcd}
0 \arrow[r] & I \arrow[r, hook, "f"] \arrow[d, "\mathrm{id}_I"'] & A \arrow[r, two heads] \arrow[dl, dashed] & B \arrow[r] & 0 \\
& I & & &
\end{tikzcd}$$

The induced map is a left inverse of f so the sequence is left-split. $\square$

Proposition 9.9. The category $\mathbf{Mod}_R$ has *enough* injectives i.e. every R-module has an injective resolution.

Proof. If for any module M we can find and injection $M \to I$ into an injective module than we can repeat the argument for the projective case. This is true but harder; a proof can be found in Godement. $\square$

Lemma 9.10. Suppose we have the diagram,

$$\begin{tikzcd}
& P \arrow[d, "f"] \arrow[dl, dashed] & \\
A \arrow[r, "\alpha"] & B \arrow[r, "\beta"] & C
\end{tikzcd}$$

such that P is projective $\beta \circ f = 0$ and the bottom row is exact. Then there is a map $P \to A$ which makes the diagram commute.

Similarly, suppose we have the diagram,

$$\begin{tikzcd}
A \arrow[r, "\alpha"] & B \arrow[r, "\beta"] \arrow[d, "f"] & C \arrow[dl, dashed] \\
& I &
\end{tikzcd}$$

such that I is injective, $f \circ \alpha = 0$, and the top row is exact. Then there is a map $C \to I$ which makes the diagram commute.

Proof. In the first case, since $\beta \circ f = 0$ we have $\mathrm{Im}(f) \subset \ker \beta = \mathrm{Im}(\alpha)$ so we may replace B with $\mathrm{Im}(\alpha)$,

$$\begin{tikzcd}
& P \arrow[d, "f"] \arrow[dl, dashed, "\tilde{f}"] & \\
A \arrow[r, "\alpha'"] & \mathrm{Im}(\alpha) \arrow[r] & 0
\end{tikzcd}$$

and α' is surjective so we get a lift $\tilde{f}$ to A of f and $\alpha \circ \tilde{f} = f$.

Similarly, since $f \circ \alpha = 0$ then $\ker \beta = \mathrm{Im}(\alpha) \subset \ker f$. Thus, f factors through the quotient $B/\ker \alpha$ to get,

$$\begin{tikzcd}
 & B \arrow[d, "\pi"] \arrow[dr, "\beta"] & \\
0 \arrow[r] & B/\ker\beta \arrow[r, "\beta'"] \arrow[d, "\bar{f}"] & C \arrow[dl, dashed] \\
 & I &
\end{tikzcd}$$

where β' is injective so we can extend f to C over β'. Thus, f lifts over β. $\square$

Lemma 9.11. Given projective or injective resolutions of both objects A and B and a map $f : A \to B$ there exists a unque lift up to chain homotopy to a chain map on the resolutions.

Proof. Let P^A and P^B be projective resolutions of A and B respectivly. We will construct the chain map inductivly. First, we have the diagram,

$$\begin{tikzcd}
P_0^A \arrow[r] \arrow[d, dashed, "f_0"] & A \arrow[r] \arrow[d, "f"] & 0 \\
P_0^B \arrow[r] & B \arrow[r] & 0
\end{tikzcd}$$

so we have a map $P_0^A \to B$ which lifts over the surjective map $P_0^B \to B$ since P_0^A is projective. Now assume we have constructed the map up to $n-1$,

$$\begin{tikzcd}
P_{n+1}^A \arrow[r, "\partial_{n+1}^A"] \arrow[d, dashed, "f_{n+1}"] & P_n^A \arrow[r, "\partial_n^A"] \arrow[d, "f_n"] & P_{n-1}^A \arrow[d, "f_{n-1}"] \\
P_{n+1}^B \arrow[r, "\partial_{n+1}^B"] & P_n^B \arrow[r, "\partial_n^B"] & P_{n-1}^B
\end{tikzcd}$$

However, the map $(f_n \circ \partial_{n+1}^A)$ satisfies $\partial_n^B \circ (f_n \circ \partial_{n+1}^A) = f_{n-1} \circ \partial_n^A \circ \partial_{n+1}^A = 0$ by commutativity and exactness of the top row. Since the bottom row is also exact, by Lemma **??**, we get a lift to P_{n+1}^A such that the diagram commutes. Thus, we get a chain map $\mathbf{P}^A \to \mathbf{P}^B$.

Now, suppose we have two chain maps $f, g : \mathbf{P}^A \to \mathbf{P}^B$ which are lifts of f. At first, we have,

$$\begin{tikzcd}
P_1^A \arrow[r, "\partial_1^A"] & P_0^A \arrow[r, "\epsilon"] \arrow[d, shift right, "g_0"'] \arrow[d, shift left, "f_0"] \arrow[dl, dashed, "s_0"'] & A \arrow[r] \arrow[d, "f"] & 0 \\
P_1^B \arrow[r, "\partial_1^B"] & P_0^B \arrow[r, "\epsilon'"] & B \arrow[r] & 0
\end{tikzcd}$$

Because $\epsilon' \circ (f_0 - g_0) = 0$, the bottom row is exact, and P_0^A is projective, we get a lift s_0 such that $\partial_1^B \circ s_0 = f_0 - g_0$. Let $\Delta_n = f_n - g_n$. Now, suppose we have a chain homotopy up to position n and consider the diagram,

$$\begin{tikzcd}
P_{n+1}^A \arrow[r, "\partial_{n+1}^A"] \arrow[d, "\Delta_{n+1}"] & P_n^A \arrow[r, "\partial_n^A"] \arrow[d, "\Delta_n"] \arrow[dl, dashed, "s_n"] & P_{n-1}^A \arrow[r, "\partial_{n-1}^A"] \arrow[d, "\Delta_{n-1}"] \arrow[dl, "s_{n-1}"] & P_{n-2}^A \arrow[d, "\Delta_{n-2}"] \arrow[dl, "s_{n-2}"] \\
P_{n+1}^B \arrow[r, "\partial_{n+1}^B"] & P_n^B \arrow[r, "\partial_n^B"] & P_{n-1}^B \arrow[r, "\partial_{n-2}"] & P_{n-2}^B
\end{tikzcd}$$

There is a map $(\Delta_n - s_{n-1}) \circ \partial_n^A : P_n^A \to P_n^B$. Furthermore,

$$\partial_n^B \circ (\Delta_n - s_{n-1} \circ \partial_n^A) = \Delta_{n-1} \circ \partial_n^A - \partial_n^B \circ s_{n-1} \circ \partial_n^A$$

where I have used commutativity to show,

$$\partial_n^B \circ \Delta_n = \partial_n^B \circ (f_n - g_n) = f_{n-1} \circ \partial_n^A - g_{n-1} \circ \partial_n^A = \Delta_{n-1} \circ \partial_n^A$$

By the induction hypothesis, $\Delta_{n-1} = s_{n-2} \circ \partial_{n-1}^A + \partial_n^B \circ s_{n-1}$. Therefore,

$$\partial_n^B \circ (\Delta_n - s_{n-1} \circ \partial_n^A) = s_{n-2} \circ \partial_{n-1}^A \circ \partial_n^A + \partial_n^B \circ s_{n-1} \circ \partial_n^A - \partial_n^B \circ s_{n-1} \circ \partial_n^A = 0$$

because $\partial_{n-1}^A \circ \partial_n^A = 0$. Thus, we get a lift s_n of this map to P_{n+1}^B. Furthermore,

$$\partial_{n+1}^B \circ s_n + s_{n-1} \circ \partial_n^A = \Delta_n - s_{n-1} \circ \partial_n^A + s_{n-1} \circ \partial_n^A = \Delta_n$$

so we have constructed a chain homotopy up to position n. By induction, $s : \mathbf{P}^A \to \mathbf{P}^B$ is a chain homotopy between f, g. The proof for the injective case is very similar. ☐

Corollary 9.12. All projective resolutions of a given object are chain homotopic. Likewise, all injective resolutions of a given object are chain homotpic.

Proof. Let $\mathbf{P}^A \longrightarrow A \longrightarrow 0$ and $\mathbf{Q}^A \longrightarrow A \longrightarrow 0$ be two projective resolutions of A. Then the identitiy map $\mathrm{id}_A : A \to A$ gives lifts to chain maps $f : \mathbf{P}^A \to \mathbf{Q}^A$ and $g : \mathbf{Q}^A \to \mathbf{P}^A$. Then, the compositions $g \circ f : \mathbf{P}^A \to \mathbf{P}^A$ and $f \circ g : \mathbf{Q}^A \to \mathbf{Q}^A$ are lifts of the identity. The idenity chain maps are also lifts of the identiy from each resolution to itself so we must have $g \circ f \sim \mathrm{id}_{\mathbf{P}^A}$ and $f \circ g \sim \mathrm{id}_{\mathbf{Q}^A}$ via chain homotopies. Thus the two complexes are chain homotopic. ☐

Lemma 9.13 (Horseshoe)**.** If we have an exact sequence,

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

and projective resolutions $\mathbf{P}^A \longrightarrow A \longrightarrow 0$ and $\mathbf{P}^C \longrightarrow C \longrightarrow 0$ then there exists a projective resolution $\mathbf{P}^B \longrightarrow B \longrightarrow 0$ and chain maps lifting the short exact sequnce such that,

$$0 \longrightarrow \mathbf{P}^A \longrightarrow \mathbf{P}^B \longrightarrow \mathbf{P}^C \longrightarrow 0$$

is an exact sequence of chain complexes. The same is true of injective resolutions.

Proof. The proof follows from the nine lemma and can be found in Rotman. ☐

9.3 Derived Functors

Definition: Let $T : \mathcal{A} \to \mathcal{B}$ be an additive functor between abelian categories with enough projectives and injectives. Then for any object A in the category $\mathcal{A}$ we first take a projective resolution $\mathbf{P}^A \to A \to 0$ of A and also an injective resolution $0 \to A \to \mathbf{I}_A$. Then we can form two chain complexes by applying the functor T,

$$\cdots \longrightarrow T(P_3^A) \longrightarrow T(P_2^A) \longrightarrow T(P_1^A) \longrightarrow T(P_0^A) \longrightarrow 0$$

and

$$0 \longrightarrow T(I_0^A) \longrightarrow T(I_1^A) \longrightarrow T(I_2^A) \longrightarrow T(I_2^A) \longrightarrow \cdots$$

note that I have conventionally removed the A term and sent the last map to zero. These are chain complexes because additive functors preserve the zero map so the composition of two maps remains zero after we apply T. Thus we can take the (co)homology of these complexes. We define, the left and right derived functors of T,

$$L_nT(A) = H_n(T(\mathbf{P}^A)) \quad \text{and} \quad R^nT(A) = H^n(T(\mathbf{I}_A))$$

Given a map $f : A \to B$ we can lift this map to any two projective or injective resolutions of A and B,

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, "f"] & I_A^0 \arrow[r] \arrow[d] & I_A^1 \arrow[r] \arrow[d] & I_A^2 \arrow[r] \arrow[d] & I_A^3 \arrow[r] \arrow[d] & \cdots \\
0 \arrow[r] & B \arrow[r] & I_B^0 \arrow[r] & I_B^1 \arrow[r] & I_B^2 \arrow[r] & I_B^3 \arrow[r] & \cdots
\end{tikzcd}$$

If we hit this diagram with T and replace the first column with 0 then we get a commutative diagram,

$$\begin{tikzcd}
0 \arrow[r] & T(I_A^0) \arrow[r] \arrow[d] & T(I_A^1) \arrow[r] \arrow[d] & T(I_A^2) \arrow[r] \arrow[d] & T(I_A^3) \arrow[r] \arrow[d] & \cdots \\
0 \arrow[r] & T(I_B^0) \arrow[r] & T(I_B^1) \arrow[r] & T(I_B^2) \arrow[r] & T(I_B^3) \arrow[r] & \cdots
\end{tikzcd}$$

which gives a chain map $T(\mathbf{I}_A) \to T(\mathbf{I}_B)$. Such a chain map induces a map on the homology $H^n(T(\mathbf{I}_A)) \to H^n(T(\mathbf{I}_B))$ which we call the induced map

$$f_* : R^nT(A) \to R^nT(B)$$

on the derived functors.

Proposition 9.14. Derived functors are indeed functors and are well-defined up to natural isomorphism with respect to choices of resolution.

Proof. Given A we know that any two projective or injective resolutions of A are chain homotopy equivalent. Since T is an additive functior, applying T to a chain homotopy diagram gives a chain homotopy of the new complexes. Therefore, the two resolutions have isomorphic homology so $L_n T(A) = H_n(T(\mathbf{P}^A)$ and $R^n T(A) = H^n(T(\mathbf{I}_A))$ are well-defined up to isomorphisms which, one can show with far too much notation, are natural in A. Furthermore, given a map $f : A \to B$ and resolutions of both A and B we know that any two lifts of f to chain maps are chain homotopic and therefore induce the same map on homology. Thus, the induced maps,

$$f_* : L_n T(A) \to L_n T(B) \quad \text{and} \quad f_* : R^n T(A) \to R^n T(B)$$

are well-defined with respect to the choice of lift.

If we have two maps $f : A \to B$ and $g : B \to C$ then the composition of the lifted chain maps of f and g to the respective resolutions clearly compose to give a lift of $g \circ f$. Therefore, $(g \circ f)_* = g_* \circ f_*$. Furthermore, $\mathrm{id}_{\mathbf{P}^A}$ is a lift of $\mathrm{id}_A : A \to A$ so $(\mathrm{id}_A)_* = \mathrm{id}$. ☐

Proposition 9.15. If T is left-exact then $R^0 T \cong T$ and if T is right exact then $L_0 T \cong T$ naturally.

Proof. Suppose T is left-exact and take an injective resolution of A,

$$0 \longrightarrow A \longrightarrow \mathbf{I}_A$$

which is an exact sequence. Applying T and envoking left-exactness we get the exact seqeunce,

$$0 \longrightarrow T(A) \longrightarrow T(I_A^0) \xrightarrow{T(d^0)} T(I_A^1)$$

Thus, $\ker T(d^0) = T(A)$. However,

$$R^0 T(A) = \ker T(d^0)/\mathrm{Im}(0) = T(A)$$

Furthermore given a map $f : A \to B$ we get a lift,

$$\begin{tikzcd}
0 \arrow[r] & T(A) \arrow[r] \arrow[d, "T(f)"] & T(I_A^0) \arrow[r, "T(d_A^0)"] \arrow[d] & T(I_A^1) \arrow[d] \\
0 \arrow[r] & T(B) \arrow[r] & T(I_B^0) \arrow[r, "T(d_B^0)"] & T(I_B^1)
\end{tikzcd}$$

Thus, taking kernels we have the commutative square,

$$\begin{tikzcd}
T(A) \arrow[r, "\sim"] \arrow[d, "T(f)"] & \ker T(d_A^0) \subset T(I_A^0) \arrow[d] \\
T(A) \arrow[r, "\sim"] & \ker T(d_B^0) \subset T(I_A^0)
\end{tikzcd}$$

and thus $f_* : R^0T(A) \to R^0T(B)$ is identified with $T(f)$ under the isomorphisms $R^0T(A) \cong T(A)$ and $R^0T(B) \cong T(B)$.

Likewise, suppose that T is right-exact and take a projective resolution of A,

$$\mathbf{P}_0^A \longrightarrow A \longrightarrow 0$$

which is an exact sequence. Applying T and envoking right-exactness we get the exact sequence,

$$T(P_1^A) \xrightarrow{T(\partial_1)} T(P_0^A) \longrightarrow T(A) \longrightarrow 0$$

Thus, $T(A) = T(P_0^A)/\mathrm{Im}(T(P_1^A))$. However,

$$L_0T(A) = \ker T(\partial_0)/\mathrm{Im}(T(\partial_1)) = \ker T(P_0^A)/\mathrm{Im}(T(P_1^A)) = T(A)$$

Furthermore given a map $f : A \to B$ we get a lift,

$$\begin{tikzcd}
T(P_1^A) \arrow[r, "T(\partial_1^A)"] \arrow[d] & T(P_0^A) \arrow[r] \arrow[d] & T(A) \arrow[r] \arrow[d, "T(f)"] & 0 \\
T(P_1^B) \arrow[r, "T(\partial_1^B)"] & T(P_0^B) \arrow[r] & T(B) \arrow[r] & 0
\end{tikzcd}$$

Thus, taking cokernels we have the commutative square,

$$\begin{tikzcd}
T(P_0^A)/\mathrm{Im}(T(P_1^A)) \arrow[r, "\sim"] \arrow[d] & T(A) \arrow[d, "T(f)"] \\
T(P_0^A)/\mathrm{Im}(T(P_1^A)) \arrow[r, "\sim"] & T(B)
\end{tikzcd}$$

and thus $f_* : L_0T(A) \to L_0T(B)$ is identified with $T(f)$ under the isomorphisms $L_0T(A) \cong T(A)$ and $L_0T(B) \cong T(B)$. $\square$

Theorem 9.16. Given an exact sequence,

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

and and additive functor $T : \mathcal{A} \to \mathcal{B}$ we get a long exact sequence,

$$\begin{tikzcd}
\cdots \arrow[r] & L_3T(A) \arrow[r] & L_3T(B) \arrow[r] & L_3T(C) \arrow[r] & L_2T(A) \arrow[r] & L_2T(B) \arrow[r] & L_2T(C) \arrow[dlllll, rounded corners] \\
& L_1T(A) \arrow[r] & L_1T(B) \arrow[r] & L_1T(C) \arrow[r] & L_0T(A) \arrow[r] & L_0T(B) \arrow[r] & L_0T(C) \arrow[r] & 0
\end{tikzcd}$$

of left-derived functors and a long exact sequence,

$$\begin{tikzcd}
0 \arrow[r] & R^0T(A) \arrow[r] & R^0T(B) \arrow[r] & R^0T(C) \arrow[r] & R^1T(A) \arrow[r] & R^1T(B) \arrow[r] & R^1T(C) \arrow[dlllll, rounded corners] \\
& R^2T(A) \arrow[r] & R^2T(B) \arrow[r] & R^2T(C) \arrow[r] & R^3T(A) \arrow[r] & R^3T(B) \arrow[r] & R^3T(C) \arrow[r] & \cdots
\end{tikzcd}$$

of right-derived functors. Furthermore, a morphism of short exact sequences will induce a morphisms of the long exact sequences.

Proof. By the Horseshoe lemma, there exists an exact sequence of projective resolutions of A, B, and C respectivly,

$$0 \longrightarrow \mathbf{P}^A \longrightarrow \mathbf{P}^B \longrightarrow \mathbf{P}^C \longrightarrow 0$$

Each row of this sequence of chain maps is a short exact sequence of projectives and thus split. However, additive functors preserve splitting so the sequence of chain complexes,

$$0 \longrightarrow T(\mathbf{P}^A) \longrightarrow T(\mathbf{P}^B) \longrightarrow T(\mathbf{P}^C) \longrightarrow 0$$

is short exact. Finally, this short exact sequence of chain complexes gives rise to a long exact sequence of homology which are exactly the left-derived functors.

Similarly, by the Horseshoe lemma, there exists an exact sequence of injective resolutions of A, B, and C respectivly,

$$0 \longrightarrow \mathbf{I}^A \longrightarrow \mathbf{I}^B \longrightarrow \mathbf{I}^C \longrightarrow 0$$

Each row of this sequence of chain maps is a short exact sequence of injectives and thus split. However, additive functors preserve splitting so the sequence of chain complexes,

$$0 \longrightarrow T(\mathbf{I}^A) \longrightarrow T(\mathbf{I}^B) \longrightarrow T(\mathbf{I}^C) \longrightarrow 0$$

is short exact. Finally, this short exact sequence of chain complexes gives rise to a long exact sequence of homology which are exactly the right-derived functors. $\square$

Remark. In practice, we will only are about left-derived functors of right-exact functors and right-derived functors of left-exact functors because for the long exact sequences to be of use we need to have T applied to the original objects appear in it somewhere.

Proposition 9.17. Let $T : \mathcal{A} \to \mathcal{B}$ be an additive functor between abelian categories with enough projectives and injectives. If I is projective then $R^nT(I) = 0$ and if P is projective then $L_nT(P) = 0$ for all $n > 0$.

Proof. If I is injective then

$$0 \longrightarrow I \longrightarrow I \longrightarrow 0$$

is an injective resolution of I where $I^0 = I$ and $I^n = 0$ for $n > 0$. Thus, for $n > 0$, $R^nT(I) = \ker T(d^n)/\mathrm{Im}(T(d^{n-1})) = 0$ because $d^n = 0$.

If P is projective then,

$$0 \longrightarrow P \longrightarrow P \longrightarrow 0$$

is an injective resolution of P where $P_0 = P$ and $P_n = 0$ for $n > 0$. Thus, for $n > 0$, $L_nT(P) = \ker T(\partial_n)/\mathrm{Im}(T(\partial_{n+1})) = 0$ because $\partial_n = 0$. $\square$

9.4 Ext and Tor

Proposition 9.18 (Tensor-Hom Adjunction)**.**

$$\mathrm{Hom}_A(M \otimes N, P) = \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P))$$

That is, the functor $(-) \otimes_R N$ is a left-adjoint of the functor $\mathrm{Hom}_R(N, -)$.

Remark. Since $(-) \otimes_R N$ is a left-adjoint it is cocontinuous and thus right-exact. Furthermore, $\mathrm{Hom}(R, N) -$ is a right-adjoint so it is continuous and thus left-exact. However, we will prove these facts explicitly without too much appeal to abstract nonsense.

Lemma 9.19. The functor $(-) \otimes_R N$ is right-exact.

Proof. Let

$$K \xrightarrow{i} L \xrightarrow{j} M \longrightarrow 0$$

be exact. Consider the sequence,

$$K \otimes N \xrightarrow{i \otimes \mathrm{id}_N} L \otimes N \xrightarrow{j \otimes \mathrm{id}_N} M \otimes N \longrightarrow 0$$

Construct a map $\phi : M \times N \to L \otimes N/(i \otimes \mathrm{id}_N)(K \otimes M)$ by $\phi(m, n) = \ell \otimes n$ where $j(\ell) = m$ where I have used the fact that j is surjective. If $\ell, \ell' \in L$ where $j(\ell) = j(\ell')$ then,

$$\ell \otimes n - \ell' \otimes n = (\ell - \ell') \otimes n$$

However, $\ell - \ell' \in \ker j = \mathrm{Im}(i)$ so take $k \in K$ such that $i(k) = \ell - \ell'$. Thus,

$$\ell \otimes n - \ell' \otimes n = i(k) \otimes n = (i \otimes \mathrm{id}_N)(k \otimes n) = 0$$

in the quotient. By the universal property of the tensor product, there exists a linear map,

$$\tilde{\phi} : M \otimes N \to L \otimes N/(i \otimes \mathrm{id}_N)(K \otimes M)$$

Furthermore, $\tilde{\phi}$ is the inverse map to $\jmath \otimes \mathrm{id}_N$ on the quotient. Therefore, $\ker j \otimes \mathrm{id}_N$ is exactly $\mathrm{Im}(i \otimes \mathrm{id})$. ☐

Definition: Define, $\mathrm{Tor}_n^R(-, N)$ to be the n^{th} left-derived functor of $(-) \otimes_R N$.

Proposition 9.20. Tor is symmetric, $\mathrm{Tor}_n^R(M, N) \cong \mathrm{Tor}_n^R(N, M)$.

Proposition 9.21. Properties of the Tor functor,

1. If M or N is projective then $\mathrm{Tor}_n^R(M, N) = 0$ for $n > 0$.
2. $\mathrm{Tor}_n^R(\bigoplus_\alpha M_\alpha, N) \cong \bigoplus_\alpha \mathrm{Tor}_n^R(M_\alpha, N)$

3. If $r \in R$ is not a zero divisor, then,

$$\mathrm{Tor}_1^R(R/(r), N) \cong \{n \in N \mid rn = 0\}$$

the r-torsion of N and,

$$\mathrm{Tor}_n^R(R/(r), N) = 0$$

for $n > 1$.

4. If R is a PID then $\mathrm{Tor}_n^R(M, N) = 0$ for $n > 1$.

Proof. I will sketch each:

1. If M is projective then $\mathrm{Tor}_n^R(M, N) = 0$ for $n > 0$ by Proposition **??**. Otherwise use symmetry.

2. This follows from the fact that direct sum and tensor product commute.

3. (DO THIS)

4. If R is a PID then submodules of free modules are free. Therefore given any R-module M we can chose a projective resolution,

$$0 \longrightarrow K \longrightarrow F \longrightarrow M \longrightarrow 0$$

where $F \to M$ is the surjection of a free R-module and $K \to F$ is the inclusion of the kernel which is also free since $K \subset F$ and F is a free R-module. Thus, the left derived functors vanish after $n = 1$ since $P_n^M = 0$ for $n > 1$ and thus the kernels of the boundary maps are zero.

□

Proposition 9.22. Given a short exact sequence of R-modules,

$$0 \longrightarrow K \longrightarrow L \longrightarrow M \longrightarrow 0$$

then we get a long exact sequence,

$$\cdots \longrightarrow \mathrm{Tor}_1^R(K, N) \longrightarrow \mathrm{Tor}_1^R(L, N) \longrightarrow \mathrm{Tor}_1^R(M, N) \longrightarrow K \otimes N \longrightarrow L \otimes N \longrightarrow M \otimes N \longrightarrow 0$$

Lemma 9.23. The functor $\mathrm{Hom}(A, -)$ is left-exact.

Proof. $\mathrm{Hom}(A, -)$ is a continuous functor and therefore preserves kernels. □

Lemma 9.24. The functor $\mathrm{Hom}(P, -)$ is exact if and only if P is projective. Similarly, the functor $\mathrm{Hom}(-, I)$ is exact if and only if I in injective.

Proof. Since $\mathrm{Hom}(P, -)$ is always left-exact, we need only that $\mathrm{Hom}(P, -)$ takes surjections to surjections. Thus if $f : A \to B$ is a surjection, we need that any map $g : P \to B$ can lift to a map $\tilde{g} : P \to A$ such that $f \circ \tilde{g} = g$.

$$\begin{tikzcd} & P \arrow[dl, dashed, "\tilde{g}"'] \arrow[d, "g"] \\ A \arrow[r, "f"] & B \end{tikzcd}$$

This is exactly the definition of P being projective. The injective case is similar. $\square$

Definition: Let M be an R-module. Define $\mathrm{Ext}_R^n(M,-)$ to be the n^{th} right-derived functor of $\mathrm{Hom}_R(M,-)$.

Proposition 9.25. Properties of the Ext functor,

1. $\mathrm{Ext}_R^n(A,B) = 0$ for $n > 0$ if either A is projective or B is injective.
2. $$\mathrm{Ext}_R^n\left(\bigoplus_\alpha A_\alpha, B\right) \cong \prod_\alpha \mathrm{Ext}_R^n(A_\alpha, B)$$ $$\mathrm{Ext}_R^n\left(A, \prod_\beta B_\beta\right) \cong \prod_\beta \mathrm{Ext}_R^n(A, B_\beta)$$
3. If R is a PID then $\mathrm{Ext}_R^n(A,B) = 0$ for $n > 1$.

Proof. I will sketch each:

1. If P is projective then $\mathrm{Hom}_R(P,-)$ is exact so its derived functors are trivial. If I is injective then $\mathrm{Ext}_R^n(A,I) = 0$ by Lemma **??**.
2. This follows from the fact that $\mathrm{Hom}(A,-)$ is contious and thus commutes with products so a resolution of the product is sent to a complex of products. Furthermore, $\mathrm{Hom}(-,B)$ takes colimts to limits and thus $$\mathrm{Hom}\left(\bigoplus_\alpha A_\alpha, -\right) \cong \prod_\alpha \mathrm{Hom}(A_\alpha, -)$$ and its derived functors will also be products since it takes each injective to a product.
3. (DO THIS)

$\square$

Proposition 9.26. Given a short exact sequence of R-modules,

$$0 \longrightarrow K \longrightarrow L \longrightarrow M \longrightarrow 0$$

then we get a long exact sequence,

$$0 \to \mathrm{Hom}_R(N,K) \to \mathrm{Hom}_R(N,L) \to \mathrm{Hom}_R(N,M) \to \mathrm{Ext}_R^1(N,K) \to \mathrm{Ext}_R^1(N,L) \to \cdots$$

10 Flatness

Definition: An A-module Q is said to to be A-flat if $(-) \otimes_A Q$ is exact. Thus, Q is A-flat iff $\mathrm{Tor}_n^A(-, Q) = 0$ for $n > 0$. Furthermore if $\mathrm{Tor}_1^A(-, Q) = 0$ then $(-) \otimes_A Q$ is exact by the long exact sequence. Thus, Q is A-flat iff $\mathrm{Tor}_1^A(-, Q) = 0$.

Proposition 10.1.
$$\mathrm{Tor}_n^A\left(\varinjlim M_i, P\right) = \varinjlim \mathrm{Tor}_n^A(M_i, P)$$

Proof. The functor $\varinjlim$ is exact. Furthermore,

$$\begin{aligned}\mathrm{Hom}_A\left((\varinjlim M_i) \otimes_A P, N\right) &= \mathrm{Hom}_A\left(\varinjlim M_i, \mathrm{Hom}_A(P, N)\right) = \varprojlim \mathrm{Hom}_A(M_i, \mathrm{Hom}_A(P, N)) \\ &= \varprojlim \mathrm{Hom}_A(M_i \otimes_A P, N) = \mathrm{Hom}_A\left(\varinjlim (M_i \otimes_A P), N\right)\end{aligned}$$

Then since the Yonenda embedding is injective,

$$(\varinjlim M_i) \otimes_A P = \varinjlim (M_i \otimes_A P)$$

□

Proposition 10.2. If Q is projective then Q is A-flat.

Proof. Since Q is projective $\mathrm{Tor}_n^A(-, Q) = 0$ for $n > 0$. □

Proposition 10.3. Let M be an A-module then the following are equivalent.

1. The A-module M is A-flat.
2. The functor $(-) \otimes_A M$ preserves monomorphisms.
3. Every finitely generated ideal $I \subset A$ satisfies $I \otimes_A M = IM$.
4. $\mathrm{Tor}_1^A(M, A/I) = 0$ for all finitely generated ideals $I \subset A$.
5. $\mathrm{Tor}_1^A(M, N) = 0$ for any finitely generated A-module N.
6. For all $a_i \in A$ and $x_i \in M$ with $\sum_{i=1}^r a_i x_i = 0$ there exists $b_{ij} \in A$ such that $\sum_{i=1}^r b_{ij} = 0$ for all j and there exist $y_i \in M$ such that $x_i = \sum_{j=1}^s b_{ij} y_j$.

Proposition 10.4. Let B be an A-algebra which is flat as an A-module and M is a B-flat B-module then M is an A-flat A-module.

Proof. Let S be an A-module. Then,

$$S \otimes_A M = S \otimes_A (B \otimes_B M) = (S \otimes_A B) \otimes_B M$$

However, $(-) \otimes_A B$ and $(-) \otimes_B M$ are exact so the composition $(-) \otimes_A M$ is exact. □

Proposition 10.5. Suppose B is an A-algebra then if M is A-flat then $B \otimes_A M$ is B-flat.

Proof. Suppose S is a B-module then,

$$S \otimes_B (B \otimes_A M) = (S \otimes_B B) \otimes_A M = S \otimes_A M$$

However, $(-) \otimes_A M$ is exact so $(-) \otimes_B (B \otimes_A M)$ is exact. □

Proposition 10.6. If $S \subset A$ is multiplicative then $S^{-1}A$ is A-flat.

Proof. Notice that if M is an A-module then $S^{-1}M \cong M \otimes_A S^{-1}A$ and localization is exact so $(-) \otimes_A S^{-1}A$ is exact. □

Proposition 10.7. Let M, N be A-modules and assume B is a flat A-algebra then,

$$\mathrm{Tor}_i^B (M \otimes_A B, N \otimes_A B) \cong \mathrm{Tor}_i^A (M, N) \otimes_A B$$

and similarly,

$$\mathrm{Ext}_B^i (M \otimes_A B, N \otimes_A B) \cong \mathrm{Ext}_A^i (M, N) \otimes_A B$$

Proof. Let $\mathbf{P} \to N \to 0$ be a projective resolution of N. Because B is A-flat then $\mathbf{P} \otimes_A B \to N \otimes_A B \to 0$ is a projective resolution. Thus,

$$\begin{aligned}\mathrm{Tor}_i^B (M \otimes_A B, N \otimes_A B) &= H_i((M \otimes_A B) \otimes_B (\mathbf{P} \otimes_A B)) \\ &= H_i((M \otimes_A \mathbf{P}) \otimes_A B) = \mathrm{Tor}_i^A (M, N) \otimes_A B\end{aligned}$$

where again I have used the exactness of $(-) \otimes_A B$ to pull it out of the homology since it preserves kernels and images. □

Proposition 10.8. Let A be a local ring and M a finitely generated A-module. Then the following are equivalent,

1. M is free
2. M is projective
3. M is flat

Proof. The first and second implications are true in general. Suppose $\mathfrak{m} \subset A$ is the maximal ideal and $k = A/\mathfrak{m}$. Then $M \otimes_A k = M/(\mathfrak{m}M)$ is a finite-dimensional k-vectorspace. There exist $x_1, \dots, x_r \in M$ such that their image $\bar{x}_1, \dots, \bar{x}_r \in M$ is a basis of $M \otimes_A k$. Consider the span map $\phi : A^r \to M$ then $\phi \otimes \mathrm{id} : k^r \to M \otimes_A k = M/(\mathfrak{m}M)$ is surjective so $\mathrm{Im}(\phi) + \mathfrak{m}M = M$. By Nakayama, $M = \mathrm{Im}(\phi)$. □

Lemma 10.9. Let $\phi : A \to B$ be a ring map. Take $\mathfrak{P} \in \mathrm{Spec}\,(A)$ and $\mathfrak{p} = \phi^{-1}(\mathfrak{P})$ and N an A-module. Then,

$$\mathrm{Tor}_i^{A_\mathfrak{p}} (B_\mathfrak{P}, N_\mathfrak{p}) = \mathrm{Tor}_i^A (B, N)_\mathfrak{P}$$

Proposition 10.10. Let $\phi : A \to B$ be a ring map then the following are equivalent,

1. B is A-flat

2. $B_{\mathfrak{P}}$ is $A_{\mathfrak{p}}$-flat for all primes $\mathfrak{p} = \phi^{-1}(\mathfrak{P})$

3. $B_{\mathfrak{P}}$ is $A_{\mathfrak{p}}$-flat for all maximal ideals $\mathfrak{p} = \phi^{-1}(\mathfrak{P})$

Proof. First, $B_{\mathfrak{p}} = B \otimes_A A_{\mathfrak{p}}$ which is clearly flat over $A_{\mathfrak{p}}$ by change of base. Furthermore, $B_{\mathfrak{P}}$ is flat over $B_{\mathfrak{p}}$ because $B_{\mathfrak{P}} = S^{-1}B_{\mathfrak{p}}$ for $S = B_{\mathfrak{p}} \setminus \mathfrak{P}B_{\mathfrak{p}}$. By transitivity, $B_{\mathfrak{P}}$ is $A_{\mathfrak{p}}$-flat. Clearly, the second implies the third. Take $Q = \operatorname{Tor}_i^A(B, N)$ using the above lemma,

$$Q_{\mathfrak{P}} = \operatorname{Tor}_i^{A_{\mathfrak{p}}}(B_{\mathfrak{P}}, N_{\mathfrak{p}}) = 0$$

because $B_{\mathfrak{P}}$ is $A_{\mathfrak{p}}$-flat. Thus, $\forall \mathfrak{P} \in \operatorname{Spec}(A)$ which are maximal we have $Q_{\mathfrak{P}} = 0$ which implies that $Q = 0$. ☐

Definition: Let M be an A-module. We say that M is *faithfully flat* over A if the sequence,

$$N \longrightarrow P \longrightarrow Q$$

is exact if and only if the sequence,

$$N \otimes_A M \longrightarrow P \otimes_A M \longrightarrow Q \otimes_A M$$

is exact.

Theorem 10.11. Let M be an A-module. Then the following are equivalent,

1. M is faithfully flat over A

2. M is A-flat and for any A-module $N \neq 0$ we have $N \otimes_A M \neq 0$.

3. M is A-flat an $\forall m \subset A$ maximal we have $M \neq \mathfrak{m}M$.

Proof. Faithfully flat implies flatness. Furhtermore, consider the sequence

$$0 \to N \to 0$$

If $M \otimes_A N = 0$ then clearly the sequence

$$0 \to M \otimes_A N \to 0$$

is exact. Thus,

$$0 \to N \to 0$$

must be exact so $N = 0$.

Now suppose 2. and let,

$$N \xrightarrow{f} P \xrightarrow{g} Q$$

be a sequence such that,

$$N \otimes_A M \longrightarrow P \otimes_A M \longrightarrow Q \otimes_A M$$

is exact. However, $g \circ f = 0$ by exactness and the flatness of M. Furthermore,

$$\ker g \otimes_A \mathrm{id}_M = \ker g \otimes_A M \qquad \mathrm{Im}(f \otimes_A \mathrm{id}_M) = \mathrm{Im}(f) \otimes_A M$$

by flatness. However, exactness implies that $\ker g \otimes_A M = \mathrm{Im}(f) \otimes_A M$ which implies that $(\ker g / \mathrm{Im}(f)) \otimes_A M = 0$ so $\ker g = \mathrm{Im}(f)$ because $(-) \otimes_A M$ is injective. Furthermore, assuming 2. take $\mathfrak{m} \subset A$ maximal then $M \otimes A/\mathfrak{m} \neq 0$ implies that $M \neq \mathfrak{m}M$. Now assume 3. and take $N \neq 0$ with $x \in N$ nonzero. Let $I = \mathrm{Ann}_A(x) \subset \mathfrak{m}$ for some maximal ideal. Consider the map $\iota : A/I \xrightarrow{\sim} Ax \subset N$. Then $A/\mathfrak{m} \otimes_A M \neq 0$ implies tht $A/I \otimes M \neq 0$ so $Ax \otimes_A M \neq 0$ by 3. Then $Ax \otimes_A M$ embedds inside $N \otimes_A M$ because M is A-flat. Thus $N \otimes_A M \neq 0$. $\square$

Corollary 10.12. Let A and B be local rings and $A \to B$ a local map. Let M be a nontrivial finitely generated B-module, then M if A-flat $\iff$ M of faithfully flat over A.

Proof. Consider the maximal ideal $\mathfrak{m}_B \subset B$ then M is A-flat implies that $M \otimes_B B/\mathfrak{m}_B \neq 0$ by Nakayama, $M \otimes_B B/\mathfrak{m}_A B \neq 0$. However, this equals $M \otimes_A A/\mathfrak{m}_A$ which must be nonzero so $M \neq \mathfrak{m}_A M$. Thus, by above, M is faithfully flat. $\square$

Proposition 10.13. Let $A \to B$ be a map of rings. If M is faithfully flat over A then $M_B = M \otimes_A B$ is faithfully flat over B.

Proposition 10.14. Let M be a B-module and $A \to B$ a map of rings. Suppose that M is faithfully flat over B and faithfully flat over A then B is faithfully flat over A.

Proposition 10.15. Let $\phi : A \to B$ be a map of rings with B faithfully flat over A then,

1. For any A-module N, the canonical map,

$$N \to N \otimes_A B$$

is injective. In particular, ϕ is injective.

2. For any ideal $I \subset A$, we have $IB \cap A = I$.

3. $\phi^{-1} : \mathrm{Spec}\,(B) \to \mathrm{Spec}\,(A)$ is surjective.

Proof. Let $x \neq 0$ take $x \otimes 1 \neq 0$ since $Ax \otimes_A B \neq 0$ because B is faithfully flat. Thus, $x \mapsto x \otimes 1$ is injective, Now consider the map,

$$A/I \to A/I \otimes_A B = B/IB$$

which is injective by the above argument. Thus we have a diagram,

$$\begin{tikzcd} A/I \arrow[r, "\tilde{\phi}"] & A/I \otimes_A B \arrow[d] \\ A \arrow[u] \arrow[r, "\bar{\phi}"] & B/IB \end{tikzcd}$$

Then $IB \cap A = \ker \bar{\phi}$ and $\ker \tilde{\phi} = \ker \bar{\phi}/I = IB \cap A/I = 0$. Thus $IB \cap A = I$. Furthermore, consider $\phi^{-1} : \mathrm{Spec}\,(B) \to \mathrm{Spec}\,(A)$ and take $\mathfrak{p} \in \mathrm{Spec}\,(A)$. Consider,

$$A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \otimes_A B \neq 0$$

which is nonzero because B is faithfully flat. Thus $B_\mathfrak{p} \supsetneq \mathfrak{p}B_\mathfrak{p}$ which implies that there exists $\mathfrak{m}$ a maximal ideal of $B_\mathfrak{p}$ containing $\mathfrak{p}B_\mathfrak{p}$. Furthermore, $\mathfrak{m} \cap A_\mathfrak{p} \supset \mathfrak{p}A_\mathfrak{p}$ which implies that $\mathfrak{m} \cap A_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$. Then $\mathfrak{P} = \mathfrak{m} \cap B$ so

$$\mathfrak{P} \cap A = \mathfrak{m} \cap A = (\mathfrak{m} \cap A_\mathfrak{p}) \cap A = (\mathfrak{p}A_\mathfrak{p}) \cap A = \mathfrak{p}$$

□

Proposition 10.16. Let B be a faithfully flat A-algebra and M an A-module then,

1. M is flat (resp. faithfully flat) over $A \iff M_B$ is flat (resp. faithfully flat) over B.

2. If A is local and M is a finitly generated A-module then M is free over $A \iff M_B$ is free over B.

Proof. The □

Theorem 10.17. Let $\varphi : A \to B$ be a ring map thn the following are equivalent,

1. B is faithfully flat over A i.e. φ is faithfully flat.

2. φ is flat and $\mathrm{Spec}\,(B) \to \mathrm{Spec}\,(A)$ is a surjection.

3. φ is flat and for any maximal ideal $\mathfrak{m}$ of A there exists a maximal ideal $\mathfrak{m}'$ of B such that $\varphi^{-1}(\mathfrak{m}') = \mathfrak{m}$.

11 Integral Domains

Definition: Take $A \subset B$ and $x \in B$. We say that x is integral over A if it satisfies a monic polynomial $p \in A[X]$ with $p(x) = 0$.

Definition: We say, for $A \subset B$, that B is integral over A if every $x \in B$ is integral over A.

Proposition 11.1. The following are equivalent,

1. $x \in B$ is integral over A

2. $A[x] \subset B$ is a finitely generated A-module.

3. $A[x] \subset C \subset B$ where C is finitely generated over A and a subring of B.

4. There exists a faithfull $A[x]$-module M of finite type over A.

Proof. If $x \in B$ is integral with $t \in A[X]$ then any polynomial $p(X) \in A[X]$ can be reduced to $p = tq + r$ with lower degree than t. Thus, we have a surjective map $A[x_0, \ldots, x_d] \to A[x]$. Now suppose that $A[x] \subset C \subset B$ for some finitely generated A-module. Then $x \in A[x] \subset C$ so the map $m_x : C \to C$ given by multiplication by x is given by some matrix M in an A-basis of C. Then $(M - xI_n)$ is the zero map so $\det(M - xI_n) = 0$. This says that x solves a monic polynomial $p(X) = \det(M - XI_n)$ which has coefficients in A. □

Corollary 11.2. For $A \subset B$ if $y_1, \ldots, y_n \in B$ are integral over A then $A[y_1, \ldots, y_n]$ is a finite A-module and is integral over A.

Corollary 11.3. For $A \subset B$ then the set C of elements of B which are integral over A is a subring of B constaining C.

Proof. Clearly $C \supset A$. If $x, y \in C$ then $A[x, y]$ is a finite A-module so $A[x, y] \subset C$ and thus $xy, x + y \in C$. □

Corollary 11.4. For $A \subset B \subset C$ if C is integral over B and B is integral over A then C is integral over A.

Corollary 11.5. Suppose $A \subset B$ is such that B is a finitely generated A-algebra then B is integral over A if and only if B is finite over A.

Proof. If B is a finite A-module then it is integral by above. Since B is finitely generated over A then $B = A[y_1, \ldots, y_n]$ and y_i are integral over A so B is finite over A. □

Definition: Let $A \subset B$ then the set,

$$C = \{x \in B \mid x \text{ is integral over } A\}$$

is called the integral closure of A inside B.

Definition: If A is a domain we say that A is integrally closed if $x \in \mathrm{Frac}(A)$ is integral over A implies that $x \in A$. That is, A is equal to its integral closure inside $\mathrm{Frac}(A)$.

Corollary 11.6. Let $A \subset B$ be domains such that A is integrally closed then the integral closure of A inside B is integrally closed.

Proof. □

Remark. Let $A \subset B \subset C$ with A Noetherian and C finitely generated A-algebra ad C is finitely generated over B then B is a finitely generated A-algebra.

Lemma 11.7. Suppose B is integral over A and B is a domain then A is a field if and only if B is a field.

Proof. Suppose that A is a field and take $x \in B$ with $x \neq 0$. We know that x is integral over A so x solves some monic,

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

for $a_i \in A$. If $a_0 = 0$ then since B is a domain we may eliminate a factor of x. Assume that $a_0 \neq 0$ then,

$$x(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1) = -a_0$$

but $a_0 \neq 0$ and A is a field so a_0 is invertible. Thus,

$$x\tfrac{1}{-a_0}(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1) = 1$$

so x is invertible. Thus B is a field.

Now assume that B is a field. For any nonzero $a \in A$ we must have $a^{-1} \in B$ since B is a field. However, B is integral over A so there must exist a monic polynomial such that,

$$a^{-n} + a_{n-1}a^{-(n-1)} + \cdots + a_1 a^{-1} + a_0 = 0$$

which implies that,

$$a^{-1} + a_{n-1} + \cdots + a_1 a^{n-2} + a_0 a^{n-1} = 0$$

However,

$$a_{n-1} + \cdots + a_1 a^{n-2} + a_0 a^{n-1} \in A$$

and thus $a^{-1} \in A$ so A is a field. □

Corollary 11.8. Suppose B is integral over A with $\varphi : A \to B$ then the map $\phi^{-1} : \mathrm{Spec}\,(B) \to \mathrm{Spec}\,(A)$ satisfies the property that $\mathfrak{P} \subset B$ is maximal if and only if $\mathfrak{p} = \varphi^{-1}(\mathfrak{P})$ is maximal.

Proof. $B/\mathfrak{P}$ is integral over $A/\mathfrak{p}$ with the map $A/\mathfrak{p} \hookrightarrow B/\mathfrak{P}$ and both are domains. Therefore $A/\mathfrak{p}$ is a field if and only if $B/\mathfrak{P}$ is a field and thus $\mathfrak{p}$ is maximal if and only if $\mathfrak{P}$ if maximal. □

Definition: Given a ring map $\varphi : A \to B$ we say that φ has the going up property if whenever $\mathfrak{p} \subset \mathfrak{p}' \in \mathrm{Spec}\,(A)$ and we have $\mathfrak{P} \mapsto \mathfrak{p}$ then there exists $\mathfrak{P}' \in \mathrm{Spec}\,(B)$ above $\mathfrak{P}$ such that $\mathfrak{P}' \mapsto \mathfrak{p}'$. Similarly, φ has the going down property if whenever we have $\mathfrak{P}' \mapsto \mathfrak{p}'$ then there exists $\mathfrak{P} \in \mathrm{Spec}\,(B)$ inside $\mathfrak{P}'$ such that $\mathfrak{P} \mapsto \mathfrak{p}$.

Theorem 11.9. If $\varphi : A \to B$ is flat then φ has the going down property.

Proof. Take $\mathfrak{p} \subset \mathfrak{p}'$ in $\mathrm{Spec}\,(A)$ and take $\mathfrak{P}' \in \mathrm{Spec}\,(B)$ such that $\varphi^{-1}(\mathfrak{P}') = \mathfrak{p}'$. Consider the localization $\mathrm{Spec}\,(A_{\mathfrak{p}'})$ which is exactly the subset of $\mathrm{Spec}\,(A)$ which lies below $\mathfrak{p}'$. Furthermore, $B_{\mathfrak{p}'}$ is flat over $A_{\mathfrak{p}'}$ and $B_{\mathfrak{P}'}$ is flat over $A_{\mathfrak{p}'}$ so $A_{\mathfrak{p}'} \to B_{\mathfrak{P}'}$ is local and flat so faithfully flat. Thus the map $\mathrm{Spec}\,(B_{\mathfrak{P}'}) \to \mathrm{Spec}\,(A_{\mathfrak{p}'})$ is surjective. Thus for any prime below $\mathfrak{p}'$ we get a prime below $\mathfrak{P}'$ mapping to it. □

Theorem 11.10 (Cohen)**.** Let $A \subset B$ and B is integral over A then the following hold,

1. The map $\mathrm{Spec}\,(B) \to \mathrm{Spec}\,(A)$ is surjective.
2. There is no inclusion relatons between two prime ideals of B above the same ideal of A.
3. The going up property holds.
4. If A is local with maximal ideal $\mathfrak{p}$ the maximal ideals of B are exactly those prime ideals with preimage $\mathfrak{p}$.
5. If A and B are integral domains then the going down property holds.
6. If A and B are integral domains with $K = \mathrm{Frac}\,(A)$. Suppose L is a normal extension of K and B is the integral closure of A inside L then two prime ideals of B lieing over the same prime ideal of A are conjugated by an automorphism of L/K.