IIT BOMBAY

Supervised Learning Project

Professor: Ananthnarayan Hariharan

Notes By: Aryaman Maithani

Spring 2022

Last Updated: February 15, 2024

Contents

§0. Preliminaries

§§0.1. Conventions, notations, basic definitions

1. $\mathbb{N}$ denotes the set of positive integers, $\mathbb{N}_0$ denotes the set of nonnegative integers. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ have their usual meanings.

2. For $n \in \mathbb{N}$, $[n]$ denotes the set $\{1, \dots, n\}$.

3. Rings will always be commutative and with multiplicative identity. R will denote a ring. Modules will be unital and typically denoted by N, M. We will usually consider the ring as acting on the left.
   If $a \in R$, then (a) denotes the ideal generated by R and the notation extends to more general cases in the obvious manner.

4. $\mathcal{J}(R)$ denotes the Jacobson radical, $\mathcal{N}(R)$ denotes the nilradical.

5. A local ring is a ring R with a unique maximal ideal $\mathfrak{m}$. We shall denote this by $(R, \mathfrak{m})$ or even $(R, \mathfrak{m}, k)$, where $k := R/\mathfrak{m}$ is the residue field.

6. Categories will always be typically denoted by **A**, **B**, et cetera. Categories will always be locally small, i.e., given two objects A and B in **A**, the collection of morphisms from A to B is a set.
   We shall use the notation $A \in \mathbf{A}$ to mean that A is an object of **A**.
   Given $A, B \in \mathbf{A}$, we use $\mathrm{Hom}_{\mathbf{A}}(A, B)$ to denote the set of morphisms from A to B.

7. $N \leqslant M$ indicates that N is a submodule of M.
   $N \mid M$ indicates that N is a direct summand of M, i.e., $M \cong N \oplus N'$ for some N'.

8. $I \trianglelefteq R$ indicates that I is an ideal of R.

9. A subset $S \subseteq R$ is said to be multiplicative if S satisfies the following:

   (a) $1 \in S$,

   (b) $s, t \in S \Rightarrow st \in S$.

   Localisation of M with respect to S is denoted by $S^{-1}M$.

   Special cases:

   (a) $S = \{1, a, a^2, \dots\}$ for some $a \in R$. In this case, $S^{-1}M = M_a$.

   (b) $S = R \setminus \mathfrak{p}$ for some prime $\mathfrak{p} \trianglelefteq R$. In this case, $S^{-1}M = M_{\mathfrak{p}}$.

   (c) R is an integral domain and $S = R \setminus \{0\}$. In this case, $S^{-1}R = \mathrm{Frac}(R)$. This is the field of fractions of R.

10. R-**mod** denotes the category of (left) R-modules. On rare occasions, we will use **mod**-R to indicate that we are considering the modules as right R-modules and write the multiplication by R on the right. However, note that our rings will always be commutative.

11. **Ch**(R) denotes the category of chain complexes of R-modules.

12. An R-algebra S is a ring along with a ring homomorphism $f : R \to S$.
    In this case, every module M over S can be considered an R-module via $r \cdot x = f(r) \cdot x$ for $r \in R$ and $x \in M$. (In particular, S itself is an R-module.)

13. $a \in R$ is said to be a zerodivisor if there exists $b \in R \setminus \{0\}$ such that $ab = 0$.
    $\mathscr{Z}(R)$ denotes the set of zerodivisors of R.

    More generally, given an R-module M, $a \in R$ is said to be a zerodivisor on M if there exists $x \in M \setminus \{0\}$ such that $a \cdot x = 0$.
    $\mathscr{Z}(R)$ denotes the set of zerodivisors on M.

14. Given submodules K, L of M, we define

    $$(L :_R N) := \{r \in R : rN \subseteq L\}.$$

    The above is an ideal of R.

    In particular, the annihilator is defined as

    $$\mathrm{ann}_R(N) := (0 :_R N) = \{r \in R : rN = 0\}.$$

15. Spec(R) denotes the set of prime ideals of R.

§§0.2. Localisation

We assume basic familiarity with the notion of localisation. We start by making some elementary observations. Unless otherwise stated, S will denote a multiplicative subset of a ring R.

Observation 0.2.1. Let M and N be $S^{-1}R$-modules. If $f : M \to N$ is an R-linear map, then f is also $S^{-1}R$-linear.

Indeed, note that
$$sf\left(\frac{r}{s}m\right) = f\left(s\frac{r}{s}m\right) = f(rm) = rf(m)$$
and thus, $f(\frac{r}{s}m) = \frac{r}{s}f(m)$.

Exercise 0.2.2. If $M \leqslant E$ are $S^{-1}R$-modules such that M is a direct summand of E as an R-module, then M is a direct summand of E as an $S^{-1}R$-module.

Here are two outlines to do the above: The first is to write $E = M \oplus N$ as an internal direct sum of R-modules and use the fact that E and M are $S^{-1}R$-modules to show that N is also an $S^{-1}R$-module.
Another is to use the fact that M being a direct summand means that there exists and

R-linear map $p : E \to M$ which restricts to the identity map on M. Then use Observation 0.2.1.

Let $S \subseteq R$ be a multiplicative subset, and M, N be R-modules. There is a map

$$\Phi : S^{-1} \operatorname{Hom}_R(M, N) \to \operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N),$$
$$\frac{\varphi}{s} \mapsto \left(\frac{a}{s'} \mapsto \frac{\varphi(a)}{ss'} \right)$$

of $S^{-1}R$-modules. In general, Φ is not an isomorphism. However, in the special case that $M = R$, we note that the modules are both isomorphic to $S^{-1}N$ and under this identification, Φ is simply the identity map. This gives us the following.

Proposition 0.2.3. Let $S \subseteq R$ be a multiplicative subset, and N be an R-module. Then,

$$S^{-1} \operatorname{Hom}_R(R, N) \cong \operatorname{Hom}_{S^{-1}R}(S^{-1}R, S^{-1}N)$$

as $S^{-1}R$-modules.

Recall that M is said to be finitely presented if there exists an exact sequence of the form $R^m \to R^n \to M \to 0$ for finite natural numbers $n, m \geqslant 1$.

Note that if R is Noetherian and M is finitely generated, then we can find a a surjection $R^n \twoheadrightarrow M$. As R is Noetherian, the kernel will be finitely generated and we can map R^m onto it. Thus, a finitely generated module over a Noetherian ring is finitely presented.

Proposition 0.2.4. If M is a finitely presented R-module, then for every multiplicative set $S \subseteq R$ and R-module N, Φ is an isomorphism of $S^{-1}R$-modules:

$$\Phi : S^{-1} \operatorname{Hom}_R(M, N) \cong \operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N).$$

In particular, the above isomorphism holds if R is Noetherian and M is finitely generated.

Proof. As noted, Φ is an isomorphism when $M = R$; additivity of Hom ensures that the above is true when $M = R^n$. For the general case, finite presentation of M gives us the usual sequence
$$R^m \to R^n \to M \to 0.$$

The result follows by the use of the Five Lemma on the following commutative diagram:

$$
\begin{array}{ccccccc}
0 & \longrightarrow & S^{-1}\operatorname{Hom}_R(M,N) & \longrightarrow & S^{-1}\operatorname{Hom}_R(R^n,N) & \longrightarrow & S^{-1}\operatorname{Hom}_R(R^m,N) \\
& & \downarrow{\scriptstyle \Phi} & & \downarrow{\scriptstyle \cong} & & \downarrow{\scriptstyle \cong} \\
0 & \to & \operatorname{Hom}_{S^{-1}R}(S^{-1}M,S^{-1}N) & \to & \operatorname{Hom}_{S^{-1}R}(S^{-1}R^n,S^{-1}N) & \to & \operatorname{Hom}_{S^{-1}R}(S^{-1}R^m,S^{-1}N)
\end{array}
$$

The first row above is exact since it is obtained by first applying $\mathrm{Hom}_R(-, N)$ (which is left exact) and then applying $S^{-1}(-)$ (which is exact) to Section 0.2.

The bottom row is similarly obtained by applying the functors in the opposite order.   □

§§0.3. Associated Primes of a Module

Throughout this section, R will denote a ring, and M an R-module. For $a \in R$, we denote by a_M the R-endomorphism of M given by $x \mapsto ax$.[1] We shall be as judicious as possible and state results involving "Noetherian" and "finitely generated" hypotheses only when necessary. Of course, our main interest eventually is in Noetherian rings, but many of the modules seen later will be non finitely generated.

Definition 0.3.1. A proper submodule $Q \lneq M$ is said to be primary if for every $a \in R$, the map $a_{M/Q}$ is either injective or nilpotent.

Note that $a_{M/Q}$ cannot be both injective and nilpotent since $M/Q \neq 0$ by hypothesis.

If Q is primary, then we define the ideal

$$\mathfrak{p} := \{a \in R : a_{M/Q} \text{ is nilpotent}\}.$$

Note that $R \setminus \mathfrak{p}$ is closed under multiplication since the composition of two injective maps is injective and hence, not nilpotent. Thus, $\mathfrak{p}$ is a prime ideal. We call $\mathfrak{p}$ the prime belonging to Q, and we say that Q is $\mathfrak{p}$-primary.

By considering $M = R$, we get the notion of a primary ideal: $\mathfrak{q} \subsetneq R$ is a primary ideal if $ab \in \mathfrak{q} \Rightarrow a \in \mathfrak{q}$ or $b^n \in \mathfrak{q}$ for some $n \geqslant 1$. In this case, the prime belonging to $\mathfrak{q}$ is simply $\sqrt{\mathfrak{q}}$.

Proposition 0.3.2. Let $\mathfrak{a} \trianglelefteq R$ be a proper ideal. Let $\mathfrak{m}$ be a maximal ideal such that $\mathfrak{m}^n \subseteq \mathfrak{a}$ for some $n \geqslant 1$. Then, $\mathfrak{a}$ is an $\mathfrak{m}$-primary ideal.

Proof. Let $\mathfrak{m}'$ be a maximal ideal containing $\mathfrak{a}$. Then, we have $\mathfrak{m}^n \subseteq \mathfrak{m}'$. Since $\mathfrak{m}'$ is prime, this forces $\mathfrak{m} \subseteq \mathfrak{m}'$ and maximality forces $\mathfrak{m} = \mathfrak{m}'$. Thus, $\mathfrak{m}$ is the unique maximal ideal containing $\mathfrak{a}$ and hence, $R/\mathfrak{a}$ is a local ring. Suppose $ab \in \mathfrak{a}$. If $b \in \mathfrak{m}$, then $b^n \in \mathfrak{a}$. If $b \notin \mathfrak{m}$, then b is a unit in $R/\mathfrak{a}$. But then $ab = 0$ in $R/\mathfrak{a}$ implies $a = 0$ in $R/\mathfrak{a}$, i.e., $a \in \mathfrak{a}$. Thus, $\mathfrak{a}$ is primary.

Taking radicals on $\mathfrak{m}^n \subseteq \mathfrak{a} \subseteq \mathfrak{m}$ shows that $\mathfrak{m} = \sqrt{\mathfrak{a}}$.   □

---

[1] The advantage of using this notation over μ_a is that the module is also clear.

Definition 0.3.3. Let R be a ring, and M an R-module. $\mathfrak{p} \in \text{Spec}(R)$ is said to be an associated prime of M if there exists $x \in M$ such that $\mathfrak{p} = \text{ann}_R(x)$. The set of all associated primes of M is denoted by $\text{Ass}_R(M)$.

In the notation of the above definition, we must have $x \neq 0$ since a prime ideal is a proper ideal of R. We will often drop the subscript if no confusion arises.

Proposition 0.3.4. Let M be a R-module, and $\mathfrak{p} \in \text{Spec}(R)$.

$\mathfrak{p} \in \text{Ass}_R(M)$ iff $R/\mathfrak{p}$ is isomorphic to a submodule of M.

Proof. ($\Rightarrow$) Write $\mathfrak{p} = \text{ann}_R(x)$. Define $\varphi : R \to M$ by $1 \mapsto x$. Then, $\ker(\varphi) = \mathfrak{p}$ and thus, $R/\mathfrak{p} \cong \text{im}(\varphi) \leqslant M$.

($\Leftarrow$) Let $f : R/\mathfrak{p} \hookrightarrow M$ be an injection. Composing with $R \to R/\mathfrak{p}$ gives a map $\varphi : R/\mathfrak{p} \to M$. Let $x := \varphi(1)$. Then, $\mathfrak{p} = \text{ann}_R(x)$. □

Corollary 0.3.5. If $N \leqslant M$, then $\text{Ass}_R(N) \subseteq \text{Ass}_R(M)$.

Proposition 0.3.6. If $N \leqslant M$, then

$$\text{Ass}_R(M) \subseteq \text{Ass}_R(N) \cup \text{Ass}_R(M/N).$$

Proof. Let $\mathfrak{p} = \text{ann}_R(x) \in \text{Ass}(M)$. If $Rx \cap N = 0$, then Rx can be viewed as a submodule of M/N and the result follows. Else, pick $ax \in Rx \cap N$ with $ax \neq 0$. Clearly, $\mathfrak{p} \subseteq \text{ann}_R(ax)$. Conversely, suppose that $b \in \text{ann}_R(ax)$. Then, $bax = 0$ and thus, $ba \in \mathfrak{p}$. Since $ax \neq 0$, we have $a \notin \mathfrak{p}$ and thus, $b \in \mathfrak{p}$, showing $\mathfrak{p} = \text{ann}_R(ax)$. Since $ax \in N$, we see that $\mathfrak{p} \in \text{Ass}(N)$. □

Corollary 0.3.7. If $M = \bigoplus_{i=1}^n N_i$, then

$$\text{Ass}_R(M) = \bigcup_{i=1}^n \text{Ass}_R(N_i).$$

Proof. By induction, it suffices to assume $n = 2$. As N_i are isomorphic to submodules of M, we have the inclusion $\supseteq$. For the other, note that we have an exact sequence $0 \to N_1 \to M \to N_2 \to 0$. □

Proposition 0.3.8. Let R be Noetherian, and M a <u>nonzero</u> R-module. Then, $\text{Ass}_R(M) \neq \varnothing$. Moreover,
$$\mathcal{Z}(M) = \bigcup_{\mathfrak{p} \in \text{Ass}_R(M)} \mathfrak{p}.$$
Equivalently, a_M is injective iff a does not lie in any associated prime.

Proof. Define $\mathcal{E} := \{\text{ann}_R(x) : x \in M \setminus \{0\}\}$. As $M \neq 0$, $\mathcal{E}$ is a nonempty set of proper ideals of R. Since R is Noetherian, $\mathcal{E}$ has a maximal element $I = \text{ann}_R(x)$. We now show that I is prime.

Suppose $ab \in I$ but $a \notin I$. We must show that $b \in I$. By hypothesis, $bax = 0$. Thus, $b \in \text{ann}_R(ax)$. Since $a \in I$, we have $ax \neq 0$ and thus, $\text{ann}_R(ax) \in \mathcal{E}$. But clearly, $I \subseteq \text{ann}_R(ax)$. By maximality, $I = \text{ann}_R(ax)$ and hence, $b \in I$. This shows that I is a prime and hence, $\text{Ass}(M) \neq \varnothing$.

We now prove the final statement. Note that if $a \in \mathfrak{p} \in \text{Ass}(M)$, then $a \cdot x = 0$ for some $x \neq 0$ and thus, $a \in \mathcal{Z}(M)$.
Conversely, assume that $a \in \mathcal{Z}(R)$. Then, $a \in \text{ann}_R(x)$ for some $x \neq 0$. As in the first part, we may pick a maximal element $\mathfrak{p} \in \mathcal{E}$ containing $\text{ann}_R(x)$. As seen, $\mathfrak{p}$ is prime and thus, $a \in \mathfrak{p} \in \text{Ass}(M)$. □

The above proof also shows us the following.

Porism 0.3.9. Let R be Noetherian, and M be a R-module. If $x \in M \setminus \{0\}$, then $\text{ann}_R(x)$ is contained in some associated prime, i.e., $\text{ann}_R(x) \subseteq \mathfrak{p}$ for some $\mathfrak{p} \in \text{Ass}_R(M)$.

Definition 0.3.10. An endomorphism $f \in \text{End}_R(M)$ is said to be pointwise nilpotent if for every $x \in M$, there exists $n \geqslant 1$ such that $f^n(x) = 0$.

Proposition 0.3.11. If a_M is pointwise nilpotent, a lies in every associated prime of M, i.e.,
$$\{a \in R : a_M \text{ is pointwise nilpotent}\} \subseteq \bigcap_{\mathfrak{p} \in \text{Ass}_R(M)} \mathfrak{p}.$$

If $\text{Ass}(M) = \varnothing$, then the intersection is assumed to be R, in which case the proposition has no content.

Proof. Suppose a_M is pointwise nilpotent, and $\mathfrak{p} = \text{ann}_R(x) \in \text{Ass}(M)$ is arbitrary. By assumption, there exists n such that $a^n x = 0$, i.e., $a^n \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime, we get $a \in \mathfrak{p}$. □

Proposition 0.3.12. Let $S \subseteq R$ be a multiplicative subset with $0 \notin S$. Let $\mathfrak{p}$ be maximal among all the ideals $\mathfrak{q}$ such that $\mathfrak{q} \cap S = \varnothing$. Then, $\mathfrak{p}$ is a prime ideal.

Proof. Suppose not. Pick $a, b \in R \setminus \mathfrak{p}$ with $ab \in \mathfrak{p}$. Then, $(a, \mathfrak{p})$ and $(b, \mathfrak{p})$ must intersect S by maximality of $\mathfrak{p}$. Thus, there exist $s_1, s_2 \in S$ with

$$s_1 = \lambda_1 a + p_1 \quad \text{and} \quad s_2 = \lambda_2 b + p_2$$

for $\lambda_i \in R$ and $p_i \in \mathfrak{p}$. Multiplying the elements shows that $s_1 s_2 \in S \cap \mathfrak{p}$, a contradiction. $\square$

Definition 0.3.13. For an R-module M, the support of M is defined as

$$\mathrm{Supp}_R(M) := \{\mathfrak{p} \in \mathrm{Spec}(R) : M_{\mathfrak{p}} \neq 0\}.$$

We may drop the superscript R if no confusion arises.

Proposition 0.3.14. Let M be an R-module.

$$\{a \in R : a_M \text{ is pointwise nilpotent}\} = \bigcap_{\mathfrak{p} \in \mathrm{Supp}(M)} \mathfrak{p}.$$

Note that there is no Noetherian hypothesis anywhere.

Proof. ($\subseteq$) Let a_M be pointwise nilpotent, and $\mathfrak{p} \in \mathrm{Supp}(M)$ be arbitrary. Then, there exists $x \in M$ such that $(Rx)_{\mathfrak{p}} \neq 0$. Thus, $\mathrm{ann}_R(x) \subseteq \mathfrak{p}$. Moreover, $a^n x = 0$ for some $n \geqslant 1$, by assumption. Thus, $a^n \in \mathrm{ann}_R(x) \subseteq \mathfrak{p}$ and hence, $a \in \mathfrak{p}$.

($\supseteq$) Suppose a_M is not pointwise nilpotent. Let $x \in M$ be such that $a^n x \neq 0$ for all $n \geqslant 1$. In particular, $S = \{1, a, a^2, \ldots\}$ does not intersect $\mathrm{ann}_R(x)$. Usual application of Zorn's lemma tells us that there is a maximal ideal $\mathfrak{p}$ not intersecting S and containing $\mathrm{ann}_R(x)$. By the earlier result, $\mathfrak{p}$ is prime and by construction, $(Rx)_{\mathfrak{p}} \neq 0$. Thus, $M_{\mathfrak{p}} \neq 0$ and $\mathfrak{p} \in \mathrm{Supp}(M)$. As $\mathfrak{p} \cap S = \varnothing$, $a \notin \mathfrak{p}$ and we are done. $\square$

Proposition 0.3.15. Let R be a Noetherian ring. Then,

$$\bigcap_{\mathfrak{p} \in \mathrm{Ass}_R(M)} \mathfrak{p} \subseteq \bigcap_{\mathfrak{p} \in \mathrm{Supp}_R(M)} \mathfrak{p}.$$

Proof. Let $a \in R$ be an element belonging to every associated prime. Let $\mathfrak{p} \in \mathrm{Supp}(M)$. We need to show that $a \in \mathfrak{p}$. To do that, it suffices to show that $\mathfrak{p}$ contains an associated prime $\mathfrak{q}$.

Let $x \in M$ be such that $(Rx)_{\mathfrak{p}} \neq 0$. Pick $\mathfrak{Q} \in \mathrm{Ass}_{R_{\mathfrak{p}}}((Rx)_{\mathfrak{p}})$ (this set is nonempty since $R_{\mathfrak{p}}$ is Noetherian). Write $\mathfrak{Q} = \mathrm{ann}_{R_{\mathfrak{p}}}(s^{-1}y)$ for some $y \in R \setminus \{0\}$ and $s \notin \mathfrak{p}$.
Define $\mathfrak{q} := \mathfrak{Q} \cap R$. $\mathfrak{q}$ is prime, since it is the contraction of a prime. Moreover, $\mathfrak{q}$ cannot intersect $R \setminus \mathfrak{p}$, i.e., $\mathfrak{q} \subseteq \mathfrak{p}$. To prove the result, we just need to show that $\mathfrak{q}$ is associated.

Let $q_1, \ldots, q_k$ be generators of $\mathfrak{q}$ (note that R is Noetherian). Then, $q_i s^{-1} y = 0$ for all $i \in \{1, \ldots, k\}$. Thus, there exist $s_1, \ldots, s_k \in R \setminus \mathfrak{p}$ such that $s_i q_i y = 0$ for all i. Let $t := \prod s_i \in R \setminus \mathfrak{p}$.

We claim that $\mathfrak{q} = \mathrm{ann}_R(ty)$ and hence, $\mathfrak{q}$ is associated.
($\subseteq$) Suffices to show that each q_i annihilates ty. But this is true because t is a multiple of s_i and q_i annihilates $s_i y$.
($\supseteq$) Suppose $a \in \mathrm{ann}_R(ty)$. Since t is a unit in $R_{\mathfrak{p}}$, we see that $a \in \mathrm{ann}_{R_{\mathfrak{p}}}(y) = \mathfrak{Q}$. Thus, $a \in \mathfrak{Q} \cap R = \mathfrak{q}$. $\qquad\square$

Corollary 0.3.16. Let R be a Noetherian ring, and M an R-module. Then, a_M is pointwise nilpotent iff a lies in every associated prime of M, i.e.,

$$\{a \in R : a_M \text{ is pointwise nilpotent}\} = \bigcap_{\mathfrak{p} \in \mathrm{Ass}_R(M)} \mathfrak{p}.$$

Proof. Combine Proposition 0.3.11, Proposition 0.3.14, Proposition 0.3.15. $\qquad\square$

Corollary 0.3.17. Let R be a Noetherian ring, and M be a <u>finitely generated</u> R-module (i.e., M is also Noetherian). Then, a_M is nilpotent iff a_M lies in every associated prime of M, i.e.,

$$\{a \in R : a_M \text{ is pointwise nilpotent}\} = \bigcap_{\mathfrak{p} \in \mathrm{Ass}_R(M)} \mathfrak{p}.$$

Proof. For a finitely generated module, pointwise nilpotent is same as nilpotent. $\qquad\square$

Corollary 0.3.18. If R is Noetherian, and M an R-module, then the following are equivalent:

1. $\mathrm{Ass}_R(M)$ is a singleton, i.e., M has exactly one associated prime,

2. $M \neq 0$ and for each $a \in R$, a_M is either injective or pointwise nilpotent.

In this case, $\mathfrak{p} \in \mathrm{Ass}_R(M)$ is given by $\mathfrak{p} = \{a \in R : a_M \text{ is pointwise nilpotent}\}$.

If M is also Noetherian, then "pointwise" can be omitted from the above. Thus, $\mathfrak{p} = \sqrt{\mathrm{ann}_R(M)}$.

Corollary 0.3.19. Assume that R and M are both Noetherian. A submodule $Q \leqslant M$ is primary if and only if M/Q has exactly one associated prime $\mathfrak{p}$, and in that case, Q is $\mathfrak{p}$-primary.

Example 0.3.20. Let R be a Noetherian ring. If $\mathfrak{q} \subseteq R$ is a $\mathfrak{p}$-primary ideal, then $\mathrm{Ass}_R(R/\mathfrak{q}) = \{\mathfrak{p}\}$. In particular, $\mathrm{Ass}_R(R/\mathfrak{p}) = \{\mathfrak{p}\}$.

§§0.4. Topology on a module

0.4.1 Definition

Definition 0.4.1. A topological abelian group is an abelian group $(M, +)$ with a topology such that the maps

1. $(x, y) \mapsto x + y$, and

2. $x \mapsto -x$

are continuous. Consequently, $(x, y) \mapsto x - y$ is also continuous.

By a neighbourhood of $a \in M$, we shall mean a subset $U \subseteq M$ such that a is contained in the interior of U. Equivalently, there is an open set V such that $a \in V \subseteq U$.

If $a \in M$ is a fixed element of a topological abelian group, then the map $T_a : M \to M$ defined by $x \mapsto x + a$ is continuous. Moreover, it is invertible with T_{-a} as inverse and hence, is a homeomorphism. Hence, if U is a neighbourhood of 0, then $U + a$ is a neighbourhood of a; moreover, every neighbourhood is of this. Thus, it suffices to consider neighbourhoods of 0.

Similarly, the inversion map $x \mapsto -x$ is a homeomorphism and thus, U is a neighbourhood of 0 iff $-U$ is a neighbourhood of 0.

Lemma 0.4.2. Let M be a topological abelian group. If $\{0\}$ is closed in M, then M is a Hausdorff space.

Proof. Note that the diagonal $\Delta \subseteq M \times M$ is the inverse image of $\{0\}$ under the continuous map $(x, y) \mapsto x - y$. $\square$

Lemma 0.4.3. Let N be the intersection of all neighbourhoods of 0. Then,

1. N is a subgroup.

2. $N = \overline{\{0\}}$, i.e., N is the closure of $\{0\}$.

3. M/N is Hausdorff.

4. M is Hausdorff $\Leftrightarrow N = 0$.

Proof.

1. Clearly, $0 \in N$. Suffices to show that whenever $a, b \in N$, then $a - b \in N$. From the continuity of group operations, it follows the map $M \times M \to M$ defined by $(x, y) \mapsto x - y$ is continuous. Thus, given an arbitrary neighbourhood U of 0, there exist neighbourhoods V_1 and V_2 of 0 such that

$$f(V_1 \times V_2) \subseteq U.$$

   Thus, given arbitrary $a, b \in N$ and an arbitrary neighbourhood U of 0, pick V_1 and V_2 as above. Then, $a \in V_1$ and $b \in V_2$ by assumption and hence, $a - b = f((a, b)) \in U$.

2. Suppose $a \in N$. An arbitrary neighbourhood of a is of the form $U + a$ for some neighbourhood U of 0. By the earlier part, $-a \in N$ and hence, $a \in U$. Thus, $0 \in U + a$ and hence, $a \in \overline{\{0\}}$.

   Conversely, if $a \in \overline{\{0\}}$ and U is an arbitrary neighbourhood of 0, then $a \in U$ and hence, $a \in N$.

3. By the earlier part, N is closed and thus, $\{0\}$ is closed in G/H. The result follows from the earlier lemma.

4. Trivial.   □

0.4.2   Completion via Cauchy sequences

In this subsubsection, M will denote a topological abelian group.

Definition 0.4.4. A sequence $(x_n)_{n \geq 1}$ in M is said to be a Cauchy sequence if for every neighbourhood U of 0, there exists $n_0 \geq 1$ such that

$$x_n - x_m \in U$$

for all $n, m \geq n_0$.

Two Cauchy sequences $(x_n)_n$ and $(y_n)_n$ are said to be equivalent if $x_n - y_n \to 0$ in M. The set of all equivalence classes of Cauchy sequences is denoted by $\widehat{M}$.

Note that we have a well-defined addition on $\widehat{M}$ given by

$$[(x_n)_n] + [(y_n)_n] = [(x_n + y_n)_n].$$

It is easily checked that $\widehat{M}$ is an abelian group with the above operation. We have a map $\varphi : M \to \widehat{M}$ given by $x \mapsto [(x)_n]$, i.e., x is sent to the equivalence class of the constant sequence x.

Proposition 0.4.5. $\ker(\varphi) = \bigcap U$, where U runs over all the neighbourhoods of 0.

Proof. Let $x \in M$. Note that $x \in \ker(\varphi)$ iff $(x)_n \sim (0)_n$ iff $x - 0 \to 0$ in M iff x is in every neighbourhood of U. $\square$

Using the above and Lemma 0.4.3, we get the following.

Corollary 0.4.6. φ is injective iff M is Hausdorff.

Remark 0.4.7. $\widehat{M}$ defined above has not been given a topology, it is only an abelian group. While it is possible to define a topology at this stage, we postpone this further and look at it in a special case in Section 6.

0.4.3   Fundamental system of neighbourhoods

Definition 0.4.8. We say that 0 has a fundamental system of neighbourhoods consisting of subgroups if there is a sequence of subgroups $(M_n)_{n \geqslant 0}$ with

1. $M_0 = M$,

2. $M_n \supseteq M_{n+1}$ for all $n \geqslant 0$

such that $U \subseteq M$ is a neighbourhood of 0 if and only if it contains some M_n.

Conversely, suppose that M is an abelian group (without any topology) and we are given a sequence

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$$

of subgroups. We can define a topology on M as follows: $U \subseteq M$ is open iff for every $a \in U$, there exists $n \geqslant 0$ such that $a + M_n \subseteq U$.
In other words, we are considering the basis

$$\mathcal{B} := \{a + M_n : a \in M, n \geqslant 0\}$$

and looking at the topology it generates.

Note that there is a check to be done, namely that what we have defined is actually a topology. Equivalently, we must check that $\mathcal{B}$ is actually a basis.

Proof. Note that $M \in \mathcal{B}$ and thus, the union of all elements of $\mathcal{B}$ is indeed M. Now, suppose that

$$x \in (a + M_n) \cap (b + M_m)$$

for some $a, b \in M$ and $n, m \geqslant 0$. Without loss of generality, we may assume $m \geqslant n$. Thus, $M_m \subseteq M_n$.
Note that $x + M_m$ is an element of $\mathcal{B}$ containing x. We claim that

$$(x + M_m) \subseteq (a + M_n) \cap (b + M_m).$$

Indeed, if $y \in x + M_m$, then

$$y - a = (y - x) + (x - a) \in M_m + M_n = M_n$$

and similarly, $y - b \in M_m$, as desired. $\qquad\square$

Thus, we have shown that this gives M a topology. As one would desire, more is true, namely that M is a topological abelian group with this topology.

Proof. First, we consider the map $f : M \to M$ given by $x \mapsto -x$. Let $U \subseteq M$ be open. We must show that $f^{-1}(U) = -U$ is open. But this is true simply because if $B \in \mathcal{B}$, then $-B \in \mathcal{B}$ as well.

Now, consider the map $g : M \to M$ given by $(x, y) \mapsto x + y$. Let $U \subseteq M$ be open and let $(x, y) \in f^{-1}(U)$. Put $a := f(x, y)$. Then, U contains a set of the form $a + M_n$. We claim that

$$(x + M_n) \times (y + M_n) \subseteq f^{-1}(U).$$

Indeed, if $(x', y') \in (x + M_n) \times (y + M_n)$, then

$$f(x', y') = x' + y' = a + (x' - x) + (y' - y) \in a + M_n \subseteq f^{-1}(U). \qquad\square$$

Lastly, one checks that $(M_n)_{n \geqslant 0}$ is a fundamental system of neighbourhoods. We leave this to the reader.

Remark 0.4.9. Note that each M_n is clearly open in this topology. Moreover, each M_n is also closed, being the complement of the open set $\bigcup_{x \notin M_n} (x + M_n)$.

§1. Injective modules and Injective hull

§§1.1. Essential extensions

Definition 1.1.1. Let R be a ring, and $M \leqslant E$ be R-modules. E is said to be an essential extension of M if for every $x \in E \setminus \{0\}$, there exists $r \in R$ such that $r \cdot x \in M \setminus \{0\}$.

Remark 1.1.2. The above definition is equivalent to demanding that every nonzero submodule of E intersects M nontrivially.

Example 1.1.3. Every module is an essential extension of itself.

Example 1.1.4. Let R be an integral domain, and $K = \mathrm{Frac}(R)$ its field of fractions. Then, $R \leqslant K$ is an essential extension of R-modules.

Proposition 1.1.5 (Transitivity of essentialness)**.** Let $L \leqslant M \leqslant N$ be R-modules. The following are equivalent.

(i) $L \leqslant M$ and $M \leqslant N$ are essential extensions.

(ii) $L \leqslant N$ is an essential extension.

Proof. (i) $\Rightarrow$ (ii): Let $n \in N \setminus \{0\}$. Then, there exists $r_1 \in R$ such that $r_1 \cdot n \in M \setminus \{0\}$. In turn, there exists $r_2 \in R$ such that $r_2 \cdot (r_1 \cdot n) \in L \setminus \{0\}$. Thus, $(r_1 r_2) \cdot n \in L \setminus \{0\}$, as desired.

(ii) $\Rightarrow$ (i): Let $n \in N \setminus \{0\}$. Then, there exists $r \in R$ such that $r \cdot n \in L \setminus \{0\}$. Since $L \setminus \{0\} \subseteq M \setminus \{0\}$, this proves that $M \leqslant N$ is essential.
Similarly, if $m \in M \setminus \{0\}$, then $m \in N \setminus \{0\}$ and essentialness of $L \leqslant N$ finishes the proof. $\square$

Proposition 1.1.6. Let $M \leqslant E$ be R-modules. Consider the set

$$\mathcal{E} := \{N \leqslant E : N \text{ is an essential extension of } M\}$$

and order it by inclusion. Then, $\mathcal{E}$ has a maximal element.

Proof. Note that $\mathcal{E} \neq \varnothing$ since $M \in \mathcal{E}$. We use Zorn's lemma to prove that $\mathcal{E}$ has a maximal

element. As usual, it suffices to show that whenever $\{N_\alpha\}_{\alpha \in \Lambda}$ is a chain in $\mathcal{E}$, then

$$N := \bigcup_{\alpha \in \Lambda} N_\alpha$$

is an element of M.

But this follows easily because if $x \in N \setminus \{0\}$, then $x \in N_\alpha \setminus \{0\}$ for some α. Using the essentialness of $M \leqslant N_\alpha$ finishes the proof. $\qquad \square$

Proposition 1.1.7. If $N_1 \leqslant M_1$ and $N_2 \leqslant M_2$ are essential, then so is $N_1 \oplus N_2 \leqslant M_1 \oplus M_2$.

Proof. Let $(x, y) \in M_1 \oplus M_2$ be nonzero. Without loss of generality, $x \neq 0$. Then, there exists $r \in R$ such that $r \cdot x \in N_1 \setminus \{0\}$. Thus, $r \cdot (x, y) \in N_1 \oplus N_2$ is nonzero. $\qquad \square$

§§1.2. Injective modules

Definition 1.2.1. And R-module E is said to be injective if it satisfies the following lifting property: Given any injection $f : N \to M$ and a map $\alpha : N \to E$, there exists a map $\beta : M \to E$ such that $\alpha = \beta \circ f$.

$$0 \longrightarrow M \longrightarrow N$$
$$\Big\downarrow \quad \swarrow_{\exists}$$
$$E \qquad \qquad .$$

In terms of Hom, the above is precisely saying that the "restriction" map $\operatorname{Hom}_R(M, E) \xrightarrow{f^*} \operatorname{Hom}_R(N, E)$ is surjective. Indeed, this is what one means by a lift. Note that the contravariant $\operatorname{Hom}_R(-, E)$ functor is always left exact. Thus, we have shown the following.

Proposition 1.2.2. E is an injective R-module iff $\operatorname{Hom}_R(-, E)$ is exact.

Proposition 1.2.3. Let $S \subseteq R$ be a multiplicative set, and let E be an $S^{-1}R$-module. E is injective as an R-module iff E is injective as an $S^{-1}R$-module.

Proof. ($\Rightarrow$) Assume E is an injective R-module. Suppose we have a diagram of $S^{-1}R$-

modules and maps as

$$0 \longrightarrow N \lhook\joinrel\longrightarrow M$$
$$\alpha \downarrow$$
$$E$$.

By injectivity of E as an R-module, there exists a desired lift $M \to E$. By Observation 0.2.1, it follows that this map is $S^{-1}R$-linear.

($\Longleftarrow$) Assume E is an injective $S^{-1}R$-module. Suppose we have a diagram of $S^{-1}R$-modules and maps as

$$0 \longrightarrow N \lhook\joinrel\longrightarrow M$$
$$\alpha \downarrow$$
$$E$$.

Then, we get a diagram as

$$0 \longrightarrow N \lhook\joinrel\longrightarrow M$$
$$\downarrow \qquad\qquad \downarrow$$
$$0 \longrightarrow S^{-1}N \lhook\joinrel\longrightarrow S^{-1}M$$
$$S^{-1}\alpha \downarrow$$
$$E$$,

where the vertical maps are the localisation maps. Note that $S^{-1}E = E$ and that the composite $N \to S^{-1}N \xrightarrow{S^{-1}\alpha} E$ is equal to α. The lower part of the diagram consists of $S^{-1}R$-modules and maps and hence, there exists a lift $S^{-1}M \to E$ of $S^{-1}\alpha$. Composing this with $M \to S^{-1}M$ gives the desired map. $\square$

Theorem 1.2.4 (Baer's Criterion). A right R-module E is injective iff for every right ideal J of R, every map $J \to E$ can be extended to a map $R \to E$.

Proof. ($\Longrightarrow$) This follows simply from the definition of injective.

($\Longleftarrow$) Suppose we are given a diagram as

$$0 \longrightarrow N \lhook\joinrel\longrightarrow M$$
$$\alpha \downarrow$$
$$E$$.

We shall assume that N is simply an R-submodule of M. Define the poset $\mathcal{E}$ to consist of all pairs (N', α') where N' is an R-submodule and $\alpha' : N' \to E$ is a map such that

$$N \leqslant N' \leqslant M \quad \text{and} \quad \alpha'|_N = \alpha.$$

This has the obvious partial order defined by $(N', \alpha') \leqslant (N'', \alpha'')$ if

$$N' \subseteq N'' \quad \text{and} \quad \alpha''|_{N''} = \alpha'.$$

Note that $\mathcal{E}$ is nonempty since $(N, \alpha) \in \mathcal{E}$. It is also clear that every chain has an upper bound, by the usual trick of unions. Thus, by Zorn's lemma, there is a maximal extension

$$\alpha' : N' \to E.$$

We now show that $N' = M$. To the contrary, suppose that $N' \neq M$ and pick $x \in M \setminus N'$. Let $J := (x :_R N') \trianglelefteq R$.

By assumption, the composite $J \xrightarrow{x} N' \xrightarrow{\alpha'} E$ extends to a map $R \to E$. Consider the submodule

$$N'' := N' + Rx \subseteq M$$

and define $\alpha'' : N'' \to E$ by

$$\alpha''(a + rx) = \alpha'(a') + f(r), \quad a' \in N' \text{ and } r \in R.$$

This is well-defined because we have $\alpha'(r)x = f(r)$ for $xr \in N' \cap Rx$. But now, we have $(N'', \alpha'') > (N', \alpha')$ contradicting the maximality. Thus, we must have $N' = M$. □

Proposition 1.2.5. If $(E_i)_{i \in I}$ is a family of injective modules, then $\prod_{i \in I} E_i$ is injective. In particular, a finite direct sum of injective modules is injective.

Proof. The last statement follows from the first since finite products and direct sums coincide.

Let $N \leqslant M$ be R-modules, and $f : N \to \prod_{i \in I} E_i$ be an R-linear map. Composing with the canonical projections $\prod E_i \to E_j$, we get R-linear maps $f_i : N \to E_i$ for all i. By injectivity, these lift to maps $\widetilde{f_i} : M \to E_i$ for all i. By the universal property of products, we get a map $\widetilde{f} : M \to \prod_{i \in I} E_i$. It is simple to check that $\widetilde{f}|_N = f$. □

Proposition 1.2.6. Suppose R is Noetherian and $(E_i)_{i \in I}$ is a family of injective modules. Then $\bigoplus_{i \in I} E_i$ is injective.

Proof. We use Baer's Criterion 1.2.4. Let $J \trianglelefteq R$ be an ideal and $f : J \to \bigoplus_i E_i$ be R-linear. As R is Noetherian, J is finitely generated by say $r_1, \ldots, r_n \in J$. Each $f(r_i)$ is contained in a submodule of $\bigoplus_i E_i$ which is a direct sum of finitely many E_i. In turn, $f(J)$ is contained in a finite such direct sum. Now, by the previous corollary, this sum is injective and we may get the desired lift $R \to \bigoplus_i E_i$. □

Remark 1.2.7. We shall see later (Example 1.2.18) that the Noetherian hypothesis above cannot be dropped. In fact, we shall show that given *any* non-Noetherian ring, there exists a (countable!) family of injective modules whose direct sum is not injective.

Proposition 1.2.8. Any direct summand of an injective module is injective.

Sketch. Let E be injective and write $E = I \oplus I'$. We wish to show that I is injective. As usual, assume $N \leqslant M$ and $f : N \to I$ is R-linear. Then, we have a map $N \to E$ given by the composition $N \to I \to E$. By injectivity of E, this lifts to a map $M \to E$. Compose this with $E \to I$ to get a map $M \to I$. Verify that this extends f. $\square$

We recall the following adjointness between tensor and Hom. We shall briefly consider modules on the right to give a precise formulation of the general adjointness. Recall that M is an S-R bimodule if M is a left S-module and a right R-module such that $s \cdot (m \cdot r) = (s \cdot m) \cdot r$ for all $s \in S$, $m \in M$, $r \in R$. Note that every (left) R-module is also an R-R bimodule with the right action being given by $m \cdot r := r \cdot m$.

Theorem 1.2.9 (Tensor-Hom Adjointness). Let R and S be rings. If B is an S-R bimodule and C a right R-module, then $\mathrm{Hom}_R(B, C)$ is a naturally a right S-module by the rule $(f \cdot s)(b) := f(sb)$ for $f \in \mathrm{Hom}_R(B, C)$, $s \in S$, and $b \in B$.
The functor $\mathrm{Hom}_R(B, -) : \mathbf{mod}\text{-}R \to \mathbf{mod}\text{-}S$ is right adjoint to $\otimes_S B$.
That is, for every S-module A and R-module C, there is a natural isomorphism

$$\tau : \mathrm{Hom}_R(A \otimes_S B, C) \xrightarrow{\cong} \mathrm{Hom}_S(A, \mathrm{Hom}_R(B, C))$$

of S-modules.

Remark 1.2.10. Note that as a special case (since we are working with commutative rings), we may always take $S = R$. In this case, the theorem is saying that given any R-module B, the functor $- \otimes_R B : \mathbf{mod}\text{-}R \to \mathbf{mod}\text{-}R$ is left adjoint to $\mathrm{Hom}_{\mathbf{mod}\text{-}R}(B, -)$.

Sketch. The proof follows essentially from the definition of the tensor product. We define τ as follows: Given an R-linear map $f : A \otimes_S B \to C$, we define $(\tau f)(a)$ to be the map $b \mapsto f(a \otimes b)$.
Conversely, given an R-linear map $g : A \to \mathrm{Hom}_R(B, C)$, we define $\sigma(g)$ to be the map defined by the bilinear form $a \otimes b \mapsto g(a)(b)$.
Then, one verifies that τ and σ are inverses of each other and that τ is natural. $\square$

Corollary 1.2.11. If S is an R-algebra and E is an injective R-module, then $\text{Hom}_R(S, E)$ is an injective S-module.

Proof. We wish to show that $\text{Hom}_S(-, \text{Hom}_R(S, E))$ preserves short exact sequences of S-modules. By adjointness, this is true iff $\text{Hom}_R(- \otimes_S S, E)$ preserves short exact sequences of S-modules. But this is true since $- \otimes_S S$ is the identity functor and $\text{Hom}_R(-, E)$ is exact by virtue of E being injective.   □

Definition 1.2.12. Let R be a ring, and M an R-module. For $a \in R$, let $\mu_a \in \text{End}_R(M)$ denote the map $x \mapsto ax$.
M is said to be divisible if μ_a is surjective for each $a \notin \mathcal{Z}(R)$.
M is said to be torsionfree if μ_a is injective for each $a \notin \mathcal{Z}(R)$.

The reader may look at Section 4.4 to see how the above two definitions relate to injectivity. The first few results from there are stated below, and the reader may prove them as an exercise. The proofs are elementary and are given in that section.

Exercise 1.2.13. Let R be a domain, and E be an R-module.

1. If E is injective, then E is divisible.

2. If E is divisible and torsionfree, then E is injective.

3. If R is a PID and E is divisible, then E is injective. In particular, for $R = \mathbb{Z}$, the notion for injective and divisible modules coincide.

Exercise 1.2.14. Give examples to show that

1. a divisible module need not be injective,

2. an injective module need not be torsionfree.

Example 1.2.15. Using the above exercises, we have some examples and nonexamples.

1. Let R be a domain which is not a field. Then, R is not an injective R-module.

2. Let R be a domain and $K = \text{Frac}(R)$. Then, K is an injective R-module (since it is divisible and torsionfree).

3. The quotient of a divisible module is divisible.

4. Thus, if $R = \mathbb{Z}$ (or more generally a PID), the quotient of an injective module is injective.

5. $\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module. More generally, K/R is an injective R-module whenever R is a PID and $K = \mathrm{Frac}(R)$.

Let M be an arbitrary $\mathbb{Z}$-module. Then, we may map a free module $\bigoplus_i \mathbb{Z}$ onto M, i.e., we can write $M \cong (\bigoplus_i \mathbb{Z})/N$. In turn, we have

$$M \cong \frac{\bigoplus_i \mathbb{Z}}{N} \hookrightarrow \frac{\bigoplus_i \mathbb{Q}}{N}.$$

As $\mathbb{Z}$ is Noetherian, the rightmost module is Noetherian (using Proposition 1.2.6 and the above examples). Thus, we have proven the following result.

Proposition 1.2.16. Every $\mathbb{Z}$-module can be embedded in an injective $\mathbb{Z}$-module, i.e., given any $\mathbb{Z}$-module M, there exists an inclusion $M \hookrightarrow E$ where E is an injective $\mathbb{Z}$-module.

Using the above, we may replace $\mathbb{Z}$ by R.

Theorem 1.2.17. Let R be an arbitrary ring.

The category of R-modules has enough injectives, i.e., given any R-module M, there exists an inclusion $M \hookrightarrow E$ where E is an injective R-module.

Proof. Note that R is a $\mathbb{Z}$-algebra in a canonical way.
Considering M as a $\mathbb{Z}$-module, we get an injection $\varphi : M \hookrightarrow E$, where E is an injective $\mathbb{Z}$-module.
This induces a map $\Phi : M \to \mathrm{Hom}_{\mathbb{Z}}(R, E)$ given by $x \mapsto (r \mapsto \varphi(rx))$. If $x \neq 0$, then $\varphi(x) \neq 0$ and thus, $\Phi(x)(1) \neq 0$. Thus, Φ is an injection.
By Corollary 1.2.11, $\mathrm{Hom}_{\mathbb{Z}}(R, E)$ is an injective module and we are done. $\square$

Example 1.2.18. We now prove the converse to Proposition 1.2.6: Suppose R is not Noetherian. Then, there exists a family $(E_n)_{n \geqslant 1}$ of injective R-modules such that $\bigoplus_{n \geqslant 1} E_n$ is not injective.

As R is not Noetherian, we can find ideals

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots .$$

For each n, fix an injective module E_n and a map $R/I_n \hookrightarrow E_n$. (This can be done in view of Theorem 1.2.17.)

Define $I := \bigcup_{n \geqslant 1} I$ and $E := \bigoplus_{n \geqslant 1} E_n$. We wish to show that E is not injective. We do so by constructing an R-linear map $I \to E$ that cannot be extended to $R \to E$. (Note that I is indeed an ideal.)

For each $n \geqslant 1$, we have a map $f_n : I \to E_n$ given by the composition

$$I \hookrightarrow R \twoheadrightarrow R/I_n \hookrightarrow E_n.$$

Thus, we get a map $f : I \to \prod_{n \geqslant 1} E_n$. We claim that the image actually lies in the direct sum $\bigoplus_{n \geqslant 1} E_n$. Indeed, let $x \in I$. Let there exists $N \geqslant 1$ such that $x \in I_n$ for all $n \geqslant N$. But this means that the image of x in R/I_n is nonzero only for finitely many n, as desired.

Thus, we have obtained a map $f : I \to E$. For the sake of contradiction, assume that this lifts to an R-linear map $F : I \to E$. Let $e := F(1)$. Then, we have

$$F(r) = re$$

for all $r \in R$. As noted, e is an element of the direct sum $\bigoplus_{n \geqslant 1} E_n$. Thus, there exists $N \geqslant 2$ such that the n-th component of e is 0 for all $n \geqslant N$. In turn, the same is true for $F(r)$ for every $r \in R$. Now, choose $r \in I_{N+1} \setminus I_N$. Since $r \notin I_N$, the image of r under the composition $I \hookrightarrow R \twoheadrightarrow R/I_N$ is nonzero. Thus, the N-th component of $F(r)$ must be nonzero, a contradiction.

Recall that a short exact sequence

$$0 \to M \xrightarrow{f} L \xrightarrow{g} N \to 0$$

is said to split if there exists a map $f' : L \to M$ such that $f'f = \mathrm{id}_M$. A consequence of this is that $f(M)$ becomes a direct summand of L.

Corollary 1.2.19. For an R-module E, the following are equivalent:

(i) E is injective.

(ii) Every short exact sequence $0 \to E \to M \to N \to 0$ splits.

(iii) Whenever $E \hookrightarrow M$, we have $E \mid M$.

Proof. (i) $\Rightarrow$ (ii): Use injectivity of E to lift $\mathrm{id}_E : E \to E$ to a map $f' : M \to E$.

(ii) $\Rightarrow$ (i): By Theorem 1.2.17, there exists an injective module I such that $0 \to E \hookrightarrow I \to N \to 0$ is exact. By hypothesis, E is a direct summand of I. By Proposition 1.2.8, E is injective.

(ii) $\Leftrightarrow$ (iii) is left as an exercise. $\square$

Corollary 1.2.20. Let E be an injective R-module, and $0 \to E \to M \to N \to 0$ an exact sequence. M is injective iff N is so.

Proof. By the previous corollary, we may write $M \cong E \oplus N$. The result follows from Proposition 1.2.5 and Proposition 1.2.8.   □

§§1.3. Injective hull

Suppose $M \leqslant E$ is an essential extension, and $i : M \hookrightarrow I$ is an injection where I is injective. Then, by injectivity, we see that i extends to a map $i' : E \to I$. Note that $\ker(i') \cap E = \ker(i) = 0$. Since E is an essential extension, this forces $\ker(i') = 0$ (see Remark 1.1.2). Thus, E embeds inside I as well.

As an example, consider R to be a domain, $M = R$, and $E = K = \text{Frac}(R)$. In this case, note that not only is K is an essential extension of R but also that K is injective. Thus, the preceding paragraph shows that K is a minimal injective module containing R.

Definition 1.3.1. Let R be a ring, and $M \leqslant E$ be R-modules. E is said to be an injective hull of M if

1. E is an injective R-module,

2. E is an essential extension of M.

Remark 1.3.2. As is usual, we will not differentiate between inclusions and injections. Thus, an injective hull should be thought of as a module E along with an injection $f : M \hookrightarrow E$ such that E is injective and $f(M) \leqslant E$ is essential.

In some sense, we are saying that E is a minimal injective module containing M. In another sense, we would like to say that E is a maximal essential extension of M. To this end, we first prove an intermediary result.

Proposition 1.3.3. An R-module E is injective if and only if there is no proper essential extension of E.

Proof. ($\Rightarrow$) Let E be injective, and $E \leqslant M$ be essential. By Corollary 1.2.19, we may write $M = E \oplus F$, where this sum is an internal direct sum. This forces $E \cap F = 0$. As $E \leqslant M$ is essential, we must have $F = 0$ and thus, $M = E$.

($\Leftarrow$) Suppose E has no proper essential extensions. By Theorem 1.2.17, let I be an injective module such that $E \leqslant I$. If $E = I$, then we are done. Else, I is a proper extension of E and hence, is not essential. Thus, the poset

$$\mathcal{E} = \{N \leqslant I : N \neq 0 \text{ and } N \cap E = 0\}$$

is nonempty (ordering is by inclusion). The usual application of Zorn's lemma gives us a maximal element $N \in \mathcal{E}$. Note that E embeds within I/N as

$$E \cong \frac{E}{E \cap N} \cong \frac{E + N}{N} \hookrightarrow \frac{I}{N}.$$

By maximality of N, the above extension is essential. Since E has no proper extensions, we get $E \cong I/N$ via the above inclusion. This means $E + N = I$. We had $E \cap N = 0$ by construction and thus, E is a direct summand of I and hence, is injective by Proposition 1.2.8. $\square$

Theorem 1.3.4. Let R be a ring, and $M \leqslant E$ be R-modules. The following are equivalent:

 (i) E is an injective hull of M.

 (ii) E is a minimal injective R-module containing M.

 (iii) E is a maximal essential extension of M.

Proof. (i) $\Rightarrow$ (ii): Assume (i). By hypothesis, E is injective. As seen before, given any injection $M \hookrightarrow I$ with I injective, the injection extends to an injection $E \hookrightarrow I$. This proves the minimality.

(ii) $\Rightarrow$ (iii): Assume (ii). By Proposition 1.1.6, we can find a maximal $N \leqslant E$ such that $M \leqslant N$ is essential.

Claim. N has no proper extensions.

Assuming the claim, we see that N is injective by Proposition 1.3.3. By minimality of E, we get that $N = E$ and thus, E is an essential extension. Being a maximal essential again follows from Proposition 1.3.3.

The proof of the claim is not difficult: if $f : N \leqslant L$ is essential, then so is $M \leqslant L$. Since E is injective, we saw earlier that this gives $L \hookrightarrow E$. But maximality of N then forces $f(N) = L$.

(iii) $\Rightarrow$ (i): Assume (iii). We need to show that E is injective. Suppose not. Then, there is a proper essential extension $E \hookrightarrow L$, by Proposition 1.3.3. But then by transitivity, $M \hookrightarrow L$ is an essential extension which contradicts maximality of E. $\square$

Theorem 1.3.5. Let R be a ring, and M be an R-module. Then, there exists an injective hull $M \hookrightarrow E$, which is unique up to isomorphism.

Proof. Let I be an injective module with $M \hookrightarrow I$ (cf. Theorem 1.2.17). The proof of (ii) $\Rightarrow$ (iii) in Theorem 1.3.4 shows that there is a maximal essential extension E of M contained in I. This is an injective hull.

Now, if E' is also an injective hull of M, then using injectivity of E' and essentialness of E gives inclusions $M \hookrightarrow E \hookrightarrow E'$. But E is a maximal essential extension of M and thus, the last inclusion is an isomorphism. $\square$

Definition 1.3.6. Let R be a ring, and M be an R-module. The injective hull of M is denoted by $E_R(M)$.

Example 1.3.7. If R is domain, then $E_R(R) = \text{Frac}(R)$.

§§1.4. Injective Modules over Noetherian rings

In this subsection we see that injective modules over Noetherian rings satisfy a nice unique decomposition theorem as one would like. Every injective module can be written as a direct sum of indecomposable injectives modules in a unique way. Moreover, one knows exactly what the indecomposable injective modules are. Also note that we had already seen that an arbitrary direct sum of injective modules (over a Noetherian ring) is injective (Proposition 1.2.6). We had also seen that the converse is true (Example 1.2.18). In this section, we employ the use of associated primes. The reader is encouraged to review Section 0.3.

Proposition 1.4.1. Let R be a Noetherian ring, and M an R-module. Then, $\text{Ass}_R(E_R(M)) = \text{Ass}_R(M)$. In particular, $\text{Ass}_R(E_R(R/\mathfrak{p})) = \{\mathfrak{p}\}$.

Proof. Since $M \leqslant E_R(M)$, we have $\text{Ass}(M) \subseteq \text{Ass}(E_R(M))$, by Corollary 0.3.5.

Conversely, if $\mathfrak{p} \in \text{Ass}(E_R(M))$, then $R/\mathfrak{p} \hookrightarrow E_R(M)$. Since $M \hookrightarrow E_R(M)$ is essential, we see that $N := M \cap (R/\mathfrak{p}) \neq 0$. Thus,

$$\varnothing \neq \text{Ass}(N) \subseteq \text{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}.$$

(Using Proposition 0.3.8, Corollary 0.3.5, Example 0.3.20.) Thus, $\{\mathfrak{p}\} = \text{Ass}(N) \subseteq \text{Ass}(M)$.

The last statement follows from Example 0.3.20. □

Definition 1.4.2. A <u>nonzero</u> R-module M is said to be decomposable if M can be written as an internal direct sum of nonzero submodules, and is said to be indecomposable otherwise.

Note that an indecomposable module is nonzero by assumption.

Theorem 1.4.3 (Matlis). Let R be a Noetherian ring, and E an R-module. Then,

1. E is an indecomposable injective R-module iff $E \cong E_R(R/\mathfrak{p})$ for some $\mathfrak{p} \in \text{Spec}(R)$,

2. $E_R(R/\mathfrak{p}) \not\cong E_R(R/\mathfrak{q})$ if $\mathfrak{p}$ and $\mathfrak{q}$ are distinct prime ideals of R, and

> 3. every injective R-module can be written as a (possibly infinite) direct sum of indecomposable R-modules.

Proof.

1. ($\Rightarrow$) Let E be an indecomposable injective R-module. Then, $E \neq 0$ and thus, we may pick $\mathfrak{p} \in \mathrm{Ass}(M)$ (Proposition 0.3.8). By Proposition 0.3.4, there is an injection $R/\mathfrak{p} \hookrightarrow E$. As E is injective, we get $E_R(R/\mathfrak{p}) \hookrightarrow E$. As $E_R(R/\mathfrak{p})$ is injective, Corollary 1.2.19 tells us that $E_R(R/\mathfrak{p}) \mid E$ and hence, $E \cong E_R(R/\mathfrak{p})$ since E is indecomposable.

   ($\Leftarrow$) Let $\mathfrak{p} \in \mathrm{Spec}(R)$. We need to prove that $E := E_R(R/\mathfrak{p})$ is indecomposable. Suppose $E = E_1 \oplus E_2$ is an internal direct sum. We have the map $i : R/\mathfrak{p} \hookrightarrow E = E_1 \oplus E_2$. Let $i(\bar{1}) = (y_1, y_2)$. Then,

$$\mathfrak{p} = \mathrm{ann}_R((y_1, y_2)) = \mathrm{ann}_R(y_1) \cap \mathrm{ann}_R(y_2).$$

   As $\mathfrak{p}$ is prime, the above implies (without loss of generality) that $\mathrm{ann}_R(y_1) = \mathfrak{p} \subseteq \mathrm{ann}_R(y_2)$. Thus, $R/\mathfrak{p}$ embeds into E_1 via the projection $E \to E_1$. But E_1 is injective (since $E_1 \mid E$) and E is essential over $R/\mathfrak{p}$. This forces $E \hookrightarrow E_1$, such that the embedding restricts to $R/\mathfrak{p} \hookrightarrow E_1$. Thus, the natural projection $E \to E_1$ is one-one and $E_1 = E$.

2. Follows from Proposition 1.4.1 since $\{\mathfrak{p}\} = \mathrm{Ass}(R/\mathfrak{p}) = \mathrm{Ass}(E_R(R/\mathfrak{p}))$.

3. Define

$$\mathfrak{E} := \{\{E_i\}_{i \in I} : \{E_i\}_{i \in I} \text{ is a collection of indecomposable injective submodules}$$
$$\text{of } E \text{ such that their sum is direct}\}.$$

   The proof of (i) shows us that $E_R(R/\mathfrak{p}) \hookrightarrow E$ for any $\mathfrak{p} \in \mathrm{Ass}(E)$. Since $E_R(R/\mathfrak{p})$ is indecomposable, we see that $\{E_R(R/\mathfrak{p})\} \in \mathfrak{E}$ and thus, $\mathfrak{E} \neq \varnothing$. Zorn's lemma now gives us a maximal collection $\{E_i\}_{i \in I} \in \mathfrak{E}$.

   Let $I := \bigoplus_{i \in I} E_i$. If $I = E$, we are done. Thus, assume $I \neq E$. By Proposition 1.2.6, I is injective and thus, $I \mid E$. Write $E = I \oplus N$ for $N \neq 0$ and note that N is also injective. Picking $\mathfrak{p} \in N$, we see that there is a copy of $E_R(R/\mathfrak{p})$ sitting inside N. But then, $\{E_i\}_{i \in I} \cup \{E_R(R/\mathfrak{p})\}$ is a strictly larger element of $\mathfrak{E}$.

$\square$

Corollary 1.4.4. Let E be an injective R-module with R Noetherian. Then,

$$E \cong \bigoplus_{\mathfrak{p} \in \mathrm{Ass}_R(E)} E_R(R/\mathfrak{p})^{a(\mathfrak{p})} \tag{1.1}$$

for nonzero cardinals $a(\mathfrak{p})$.

The fact that the cardinals are nonzero actually follows from the proof of the previous result. We shall see later that the cardinals $\mathfrak{a}(\mathfrak{p})$ are uniquely determined and do not depend on the choice of decomposition.

Recall that given a prime ideal $\mathfrak{p} \in \mathrm{Spec}(R)$, there are two ways to get a corresponding field:

1. Form the quotient ring $R/\mathfrak{p}$. This is a integral domain. Consider its field of fractions $\mathrm{Frac}(R/\mathfrak{p})$.

2. Form the localisation $R_\mathfrak{p}$. This is a local ring with maximal ideal $\mathfrak{p}R_\mathfrak{p}$. Consider its residue field $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$.

One can check that both these operations lead to the same field, which we shall denote by $\kappa(\mathfrak{p})$. Note that localisation and quotients commute and thus,

$$(R/\mathfrak{p})_\mathfrak{p} \cong R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} = \kappa(\mathfrak{p}).$$

Theorem 1.4.5. Let R be a Noetherian ring, $\mathfrak{p} \in \mathrm{Spec}(R)$ a prime ideal. Then,

$$E_R(R/\mathfrak{p}) = E_{R_\mathfrak{p}}(\kappa(\mathfrak{p})).$$

Proof. We first show that $E := E_R(R/\mathfrak{p})$ is indeed an R-module. Let $s \in R \setminus \mathfrak{p}$. We must show that the multiplication map by s is an automorphism of E. Note that $\mathrm{Ass}(E) = \{\mathfrak{p}\}$ by Proposition 1.4.1. By Proposition 0.3.8, we see that s is not a zero divisor on E and hence, $sE \cong E$ is injective. But $sE \subseteq E$ and thus, $sE \mid E$. E is indecomposable by Theorem 1.4.3 and hence, $sE = E$.

The map $R/\mathfrak{p} \hookrightarrow E$ factors as

$$R/\mathfrak{p} \hookrightarrow \kappa(\mathfrak{p}) \hookrightarrow E,$$

since $R/\mathfrak{p} \hookrightarrow \kappa(\mathfrak{p})$ is an essential extension as ($R/\mathfrak{p}$-modules and hence) R-modules. Since $R \hookrightarrow E$ is an essential extension of R-modules, so is $\kappa(\mathfrak{p}) \hookrightarrow E$. A fortiori, it is an essential extension of $R_\mathfrak{p}$-modules. To finish the proof, we need to show that E is an injective $R_\mathfrak{p}$-module.

Note that we have the $R_\mathfrak{p}$-module isomorphisms

$$E \cong \mathrm{Hom}_{R_\mathfrak{p}}(R_\mathfrak{p}, E) \cong \mathrm{Hom}_{R_\mathfrak{p}}(R_\mathfrak{p}, \mathrm{Hom}_R(R_\mathfrak{p}, E)).$$

By Tensor-Hom Adjointness 1.2.9, we have $\mathrm{Hom}_{R_\mathfrak{p}}(R_\mathfrak{p}, \mathrm{Hom}_R(R_\mathfrak{p}, E)) \cong \mathrm{Hom}_R(R_\mathfrak{p}, E)$ which is an injective $R_\mathfrak{p}$-module by Corollary 1.2.11. $\qquad\square$

Remark 1.4.6. Recall that localisation at a prime is localisation with respect to its complement. Moreover, if $S \subseteq T$ are multiplicative subsets of R, and M is a $T^{-1}R$ module, then localising with respect to S does not change anything (since elements of S already act as units). In other words, $M \cong S^{-1}(M)$ is also an $S^{-1}R$ module.

Applying to the case where $\mathfrak{q} \subseteq \mathfrak{p}$ are primes, we see that any $R_\mathfrak{q}$-module is also an $R_\mathfrak{p}$ module.

Corollary 1.4.7. Let R be a Noetherian ring, $\mathfrak{q}$ and $\mathfrak{p}$ be primes in R with $\mathfrak{q} \subseteq \mathfrak{p}$. Then,

$$E_R(R/\mathfrak{q}) \cong E_{R_\mathfrak{p}}(R_\mathfrak{p}/\mathfrak{q}R_\mathfrak{p}).$$

In particular, $E_R(R/\mathfrak{q})$ is an indecomposable injective $R_\mathfrak{p}$-module.

Proof. If $a \in R \setminus \mathfrak{p}$, then a is not in $\mathfrak{q}$ and thus, a is not a zerodivisor on $R/\mathfrak{q}$. Thus, the localisation map $R/\mathfrak{q} \hookrightarrow (R/\mathfrak{q})_\mathfrak{p}$ is injective. Note that $(R/\mathfrak{q})_\mathfrak{p} \cong R_\mathfrak{p}/\mathfrak{q}R_\mathfrak{p}$. Thus, we have an injection

$$R/\mathfrak{q} \hookrightarrow E_{R_\mathfrak{p}}(R_\mathfrak{p}/\mathfrak{q}R_\mathfrak{p})$$

of R-modules. In turn, we have an injection

$$E_R(R/\mathfrak{q}) \hookrightarrow E_{R_\mathfrak{p}}(R_\mathfrak{p}/\mathfrak{q}R_\mathfrak{p})$$

of R-modules. (Note that the right module above is injective over R by Proposition 1.2.3.)

By injectivity, the above splits. In view of Theorem 1.4.5 and Remark 1.4.6, we see that the left module is also an $R_\mathfrak{p}$-module. Using Exercise 0.2.2, we see that the above splitting is also as $R_\mathfrak{p}$-modules. Since $E_{R_\mathfrak{p}}(R_\mathfrak{p}/\mathfrak{q}R_\mathfrak{p})$ is an indecomposable module (by Matlis 1.4.3), we see that the above inclusion is actually an isomorphism. □

Theorem 1.4.8. Let R be a Noetherian ring, $I \subseteq \mathfrak{p} \subseteq R$ be ideals, $\mathfrak{p} \in \mathrm{Spec}(R)$. Let $E := E_R(R/\mathfrak{p})$. Then,

$$E_{R/I}(R/\mathfrak{p}) \cong \mathrm{Hom}_R(R/I, E_R(R/\mathfrak{p})) \cong (0 :_E I).$$

The last isomorphism is the natural one: Giving a map from R/I is the same as giving a map from R which vanishes on I. In turn, giving a map from R is the same as giving an element in the codomain.

Proof. We know that $\mathrm{Hom}_R(R/I, E)$ is an injective R/I-module. We now show that it is (isomorphic to) an essential extension of $R/\mathfrak{p}$.
As noted earlier, we have $\mathrm{Hom}_R(R/I, E) \cong (0 :_E I) \subseteq E$. Identify $R/\mathfrak{p}$ with a subset of E under $R/\mathfrak{p} \hookrightarrow E$. As $I \subseteq \mathfrak{p}$, we see that $R/\mathfrak{p} \subseteq (0 :_E I)$. By Transitivity of essentialness 1.1.5, $R/\mathfrak{p} \hookrightarrow (0 :_E I)$ is essential, as desired. □

Corollary 1.4.9. Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring, and $E := E_R(k)$ be the injective hull of k over R. Then for any proper ideal I in R, $E_{R/I}(k) \cong (0 :_E I)$.

Remark 1.4.10. The above corollary says the following: Suppose that we have computed the injective hull E of k over R. Then, for any ideal I, the injective hull over R/I can be simply obtained the submodule of E which is annihilated by I.

Our goal now is to show that the exponents $\mathfrak{a}(\mathfrak{p})$ in (1.1) are uniquely determined.

Proposition 1.4.11. Let R be a Noetherian ring, $\mathfrak{p}$ and $\mathfrak{q}$ prime ideals in R. Then,

1.
$$[E_R(R/\mathfrak{q})]_{\mathfrak{p}} = \begin{cases} 0 & \text{if } \mathfrak{q} \not\subseteq \mathfrak{p}, \\ E_R(R/\mathfrak{q}) & \text{if } \mathfrak{q} \subseteq \mathfrak{p}. \end{cases}$$

2.
$$\operatorname{Hom}_{R_{\mathfrak{p}}}(\kappa(\mathfrak{p}), E_R(R/\mathfrak{q})_{\mathfrak{p}}) = \begin{cases} \kappa(\mathfrak{p}) & \text{if } \mathfrak{p} = \mathfrak{q}, \\ 0 & \text{if } \mathfrak{p} \neq \mathfrak{q}. \end{cases}$$

Proof. For brevity, define $E := E_R(R/\mathfrak{q})$.

1. As noted in Theorem 1.4.5, $E = E_R(R/\mathfrak{q})$ is an $R_{\mathfrak{q}}$ module. By Remark 1.4.6, it follows that $E_{\mathfrak{p}} = E$ if $\mathfrak{p} \supseteq \mathfrak{q}$.

   Now, suppose $\mathfrak{q}$ is not a subset of $\mathfrak{p}$. Pick $\mathfrak{a} \in \mathfrak{q} \setminus \mathfrak{p}$. Note that $\operatorname{Ass}_R(E_R(R/\mathfrak{q})) = \{\mathfrak{q}\}$ and thus, $\mathfrak{a}$ is pointwise nilpotent (Corollary 0.3.18) on E, i.e., given any $x \in E$, there exists $n = n(x) \geqslant 1$ such that $\mathfrak{a}^n x = 0$. Since $\mathfrak{a} \notin \mathfrak{p}$, it follows that $\frac{x}{1} = 0$ in $E_{\mathfrak{p}}$, as desired.

2. If $\mathfrak{q}$ is not contained in $\mathfrak{p}$, then the first part tells us directly that the Hom is 0. Thus, assume $\mathfrak{q} \subseteq \mathfrak{p}$.

   For $\mathfrak{q} = \mathfrak{p}$, we note

$$\begin{aligned} \operatorname{Hom}_{R_{\mathfrak{p}}}(\kappa(\mathfrak{p}), E_{\mathfrak{p}}) &\cong \operatorname{Hom}_{R_{\mathfrak{p}}}(\kappa(\mathfrak{p}), E_R(R/\mathfrak{p})) \\ &\cong \operatorname{Hom}_{R_{\mathfrak{p}}}(\kappa(\mathfrak{p}), E_{R_{\mathfrak{p}}}(\kappa(\mathfrak{p}))) \\ &\cong E_{\kappa(\mathfrak{p})}(\kappa(\mathfrak{p})) \\ &= \kappa(\mathfrak{p}). \end{aligned}$$

   Theorem 1.4.5

   Theorem 1.4.8

   Now, assume $\mathfrak{q} \subsetneq \mathfrak{p}$. By Proposition 0.2.4, we see that

$$\operatorname{Hom}_{R_{\mathfrak{p}}}(\kappa(\mathfrak{p}), E_R(R/\mathfrak{q})_{\mathfrak{p}}) \cong [\operatorname{Hom}_R(R/\mathfrak{p}, E_R(R/\mathfrak{q}))]_{\mathfrak{p}}.$$

Thus, it is enough to prove that $\text{Hom}_R(R/\mathfrak{p}, E_R(R/\mathfrak{q})) = 0$.
Suppose $f \in \text{Hom}_R(R/\mathfrak{p}, E)$. Then $\mathfrak{p}f(\bar{1}) = 0$, i.e., $\mathfrak{p} \subseteq \text{ann}_R(f(\bar{1}))$. On the other hand, since $\text{Ass}(E) = \{\mathfrak{q}\}$, Porism 0.3.9 shows that $\text{ann}_R(x) \subseteq \mathfrak{q}$ for all $x \in E \setminus \{0\}$. Since $\mathfrak{p} \not\subseteq \mathfrak{q}$, it follows that $f(\bar{1}) = 0$ and we are done. $\square$

Corollary 1.4.12. Let I be an injective module over a Noetherian ring R. For every $\mathfrak{p} \in \text{Spec}(R)$, $I_\mathfrak{p}$ is an injective $R_\mathfrak{p}$-module. Furthermore, the map $I \to I_\mathfrak{p}$ is surjective.

Proof. By Matlis 1.4.3, decompose I as in (1.1). Then,

$$I_\mathfrak{p} \cong \bigoplus_{\mathfrak{q} \in \text{Ass}(I), \mathfrak{q} \subseteq \mathfrak{p}} E_R(R/\mathfrak{q})^{a(\mathfrak{q})}.$$

By Corollary 1.4.7, the result follows. $\square$

Corollary 1.4.13. Let R be a Noetherian ring and I be an injective R-module. Suppose $I \cong \bigoplus_{\mathfrak{p} \in \text{Spec}(R)} E_R(R/\mathfrak{p})^{a(\mathfrak{p})}$. Then, $a(\mathfrak{p}) = \dim_{\kappa(\mathfrak{p})}(\text{Hom}_{R_\mathfrak{p}}(\kappa(\mathfrak{p}), I_\mathfrak{p}))$.

Remark 1.4.14. The previous corollary is saying that given a decomposition of I as a direct sum of $E_R(R/\mathfrak{p})$, the exponent is uniquely determined. Existence of a decomposition was given by Matlis 1.4.3. Combining the two statements gives us the existence and uniqueness of the decomposition.

§2. Some Homological Algebra

§§2.1. Injective Resolutions

Theorem 1.2.17 told us that given any module M, we can find an injective module I^0 and an injection $M \xrightarrow{\varepsilon} I^0$. This gives us a short exact sequence

$$0 \to M \xrightarrow{\varepsilon} I^0 \to \operatorname{coker}(\varepsilon) \to 0.$$

Now, using Theorem 1.2.17 again gives us an injection $\operatorname{coker}(\varepsilon) \hookrightarrow I^1$. Composing this with $I^0 \twoheadrightarrow \operatorname{coker}(\varepsilon)$ gives us a map $I^0 \xrightarrow{\partial^0} I^1$. Thus, we now have an exact sequence

$$0 \to M \xrightarrow{\varepsilon} I^0 \xrightarrow{\partial^0} I^1 \to \operatorname{coker}(\partial^0) \to 0.$$

Continuing in this way, we get a sequence of injective modules $(I^n)_{n \geqslant 0}$ and module homomorphisms $\partial^n : I^n \to I^{n+1}$ such that the augmented complex

$$0 \to M \xrightarrow{\varepsilon} I^0 \xrightarrow{\partial^0} I^1 \xrightarrow{\partial^1} I^2 \xrightarrow{\partial^2} \cdots$$

is exact.

Definition 2.1.1. Let R be a ring, and M be an R-module. An injective resolution of M is an exact sequence

$$0 \to M \xrightarrow{\varepsilon} I^0 \xrightarrow{\partial^0} I^1 \xrightarrow{\partial^1} I^2 \xrightarrow{\partial^2} \cdots,$$

where each I^n is an injective module.

The content of the beginning discussion is the following.

Proposition 2.1.2. Every module has an injective resolution.

§§2.2. δ-Functors

For this subsection, we work in slight generality. In what follows, **A** and **B** will be abelian categories. Standard examples of abelian categories are R-**mod** and **Ch**(R). If the reader is unfamiliar with abelian categories, they might as well assume that the categories are one of these two.
Recall that a functor $F : \mathbf{A} \to \mathbf{B}$ is said to be additive if $F(f + g) = F(f) + F(g)$.

Definition 2.2.1. A (covariant) cohomological δ-functor between **A** and **B** is a collection of additive functors $T^n : \mathbf{A} \to \mathbf{B}$ for $n \geqslant 0$, together with morphisms

$$\delta^n : T^n(C) \to T^{n+1}(A)$$

defined for each short exact sequence $0 \to A \to B \to C \to 0$ in **A**. We make the convention that $T^n = 0$ for $n < 0$. We impose the following two conditions:

1. For each short exact sequence as above, there is a long exact sequence

$$\cdots \to T^{n-1}(C) \xrightarrow{\delta} T^n(A) \to T^n(B) \to T^n(C) \xrightarrow{\delta} T^{n+1}(A) \to \cdots .$$

   In particular, T^0 is left exact.

2. For each morphism of short exact sequences from $0 \to A' \to B' \to C' \to 0$ to $0 \to A \to B \to C \to 0$, the δs give a commutative diagram

$$
\begin{array}{ccc}
T^n(C') & \xrightarrow{\ \delta\ } & T^{n+1}(A') \\
\downarrow & & \downarrow \\
T^n(C) & \xrightarrow[\ \delta\ ]{} & T^{n+1}(A)
\end{array}\ .
$$

Definition 2.2.2. A morphism $S \to T$ between δ-functors is a system of natural transformations $S^n \to T^n$ that commute with δ.

A cohomological δ-functor S is universal if, given any δ-functor T and a natural transformation $\varphi^0 : S^0 \to T^0$, there is a unique morphism $S \to T$ of δ-functors that extends φ^0.

Remark 2.2.3. The statement about "commuting with δ" simply means that the squares in the corresponding ladder of long exact sequences commute. To elaborate more: Let

$$0 \to A \to B \to C \to 0$$

be an exact sequence in **A**. Since T and S are δ-functors, and $(\varphi^n)_n$ natural transformations, we have the ladder as

$$
\begin{array}{ccccccccc}
\cdots \xrightarrow{\ \delta\ } & S^n(A) & \longrightarrow & S^n(B) & \longrightarrow & S^n(C) & \xrightarrow{\ \delta\ } & S^{n+1}(A) & \longrightarrow \cdots \\
& \downarrow{\scriptstyle \varphi^n(A)} & & \downarrow{\scriptstyle \varphi^n(B)} & & \downarrow{\scriptstyle \varphi^n(C)} & & \downarrow{\scriptstyle \varphi^{n+1}(A)} & \\
\cdots \xrightarrow[\ \delta\ ]{} & T^n(A) & \longrightarrow & T^n(B) & \longrightarrow & T^n(C) & \xrightarrow[\ \delta\ ]{} & T^{n+1}(A) & \longrightarrow \cdots
\end{array}\ .
$$

The two left squares commute simply by virtue of φ^n being natural transformations. The rightmost square commutes by our requirement of φ commuting with δ.

Exercise 2.2.4. If $F : \mathbf{A} \to \mathbf{B}$ is an exact functor, show that $T^0 = F$ and $T^n = 0$ for $n \neq 0$ defines a universal δ-functor.

Solution. That it defines a δ-functor is clear, with $\delta^n = 0$ for all n (here is where we use exactness). Let us now show that it is is universal. To this end, let S be a δ-functor, and $f^0 : S^0 \to T^0$ be a natural transformation.

Note that an extension, if it exists, is necessarily unique since $T^n(A) = 0$ for all $n \geqslant 1$ and all objects $A \in \mathbf{A}$. Thus, each f^n is forced to be the zero transformation. Now, we must check that this does define a morphism of δ-functors. This f also commutes with δ since both are 0. $\qquad\square$

Remark 2.2.5. As expected, a consequence of the universal property of the universal δ-functor is as follows: Suppose T^* and S^* are universal δ-functors with $T^0 \cong S^0$, i.e., there is a natural transformation $\varphi^0 : T^0 \to S^0$. Then, $T^* \cong S^*$, i.e., there is an isomorphism $T^* \to S^*$ of δ-functors.

Definition 2.2.6. A family $(F^n)_{n \geqslant 0}$ of additive functors $F^n : \mathbf{A} \to \mathbf{B}$ is said to vanish on enough injectives if for every object $A \in \mathbf{A}$, there exists an injective object $I \in \mathbf{A}$ and a monomorphism $A \hookrightarrow I$ such that $F^n(I) = 0$ for all $n \geqslant 1$.

Note that $F^0(I) = 0$ is *not* necessary.

Example 2.2.7. Let F be a left exact functor, and $\mathcal{R}^*F$ denote its right derived functor. Then, it is a simple consequence of the definition that $\mathcal{R}^nF(I) = 0$ for all injectives I and all $n \geqslant 1$. Thus, $\mathcal{R}^*F$ vanishes on enough injectives (in fact, on all injectives) in view of Theorem 1.2.17.

Proposition 2.2.8. Let $F^* : \mathbf{A} \to \mathbf{B}$ be a δ-functor that vanishes on enough injectives. Then, F^* is a universal δ-functor.

Proof. Suppose T^* is a δ-functor and that a natural transformation $\varphi^0 : F^0 \to T^0$ is given. We need to show that φ^0 admits a unique extension to a morphism $\varphi^* : F^* \to T^*$ of δ-functors. Fix $n \geqslant 0$ and suppose inductively that $\varphi^i : F^i \to T^i$ are defined for $0 \leqslant i \leqslant n$ such that they commute with the appropriate δ^*. For each A in $\mathbf{A}$, fix an exact sequence $0 \to A \to I \to C \to 0$ with I injective and $F^n(I) = 0$ for $n > 0$. This can be done by our assumption of F^* vanishing on enough injectives. Now, we have a commutative diagram

with exact rows given by

$$
\begin{array}{ccccccc}
F^n(I) & \longrightarrow & F^n(C) & \xrightarrow{\ \delta\ } & F^{n+1}(A) & \longrightarrow & 0 \\
& & \downarrow{\scriptstyle \varphi^n(I)} & & \downarrow{\scriptstyle \varphi^n(C)} & & \\
T^n(I) & \longrightarrow & T^n(C) & \xrightarrow[\delta]{} & T^{n+1}(A) & &
\end{array}
\tag{2.1}
$$

The 0 in the first row is because $F^{n+1}(I) = 0$. (Note that $n = 0$ is allowed and so we are not commenting on $F^n(I)$.) A diagram chase now reveals that there is a *unique* map $\varphi^{n+1}(A) : F^{n+1}(A) \to T^{n+1}(A)$ making the above diagram commute. We will now show that φ^{n+1} defined as above is a natural transformation that commutes with δ^*.

Natural transformation. Let $f : A' \to A$ be a morphism. As fixed earlier, we have an exact sequence $0 \to A' \to I' \to C' \to 0$. By injectivity, we get a map $g : I' \to I$ and then, this induces a map $h : C' \to C$ such that the following diagram is commutative with exact rows.

$$
\begin{array}{ccccccc}
0 & \longrightarrow & A' & \longrightarrow & I' & \longrightarrow & C' & \longrightarrow & 0 \\
& & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\
0 & \longrightarrow & A & \longrightarrow & I & \longrightarrow & C & \longrightarrow & 0
\end{array}
\tag{2.2}
$$

To see that φ^n commutes with f, we note that in the following diagram, each small quadrilateral commutes.

$$\tag{2.3}$$

(The top and bottom trapezia commute since F^* and T^* are δ-functors. The left and right ones commute by construction of φ^{n+1}. The middle square commutes since φ^n is a natural transformation, by inductive hypothesis.)
A diagram chase reveals that

$$
T^{n+1}(f) \circ \varphi^{n+1}(A') \circ \delta = \varphi^{n+1}(A) \circ F^{n+1}(f) \circ \delta
$$

Since δ is epic, we can cancel it above to see that φ "commutes" with f, i.e., φ is a natural transformation. (In fact, taking $A = A'$ and $f = \mathrm{id}_A$ also shows that $\varphi_n(A')$ does not depend on choice of I and C.)

Commuting with δ. Suppose we are given a short exact sequence $0 \to A' \to A \to A'' \to 0$. As before, we have maps and an injective I' such that the following diagram is commutative with exact rows.

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & A' & \longrightarrow & A' & \longrightarrow & A'' & \longrightarrow & 0 \\
 & & \| & & \downarrow f & & \downarrow g & & \\
0 & \longrightarrow & A' & \longrightarrow & I' & \longrightarrow & C' & \longrightarrow & 0
\end{array}
\tag{2.4}
$$

This yields a diagram

$$
\begin{array}{ccccc}
F^n(A'') & \xrightarrow{F^n(g)} & F^n(C') & \xrightarrow{\delta} & F^{n+1}(A') \\
\downarrow{\varphi^n} & & \downarrow{\varphi^n} & & \downarrow{\varphi^{n+1}} \cdot \\
T^n(A'') & \xrightarrow[T^n(g)]{} & T^n(C') & \xrightarrow[\delta]{} & T^{n+1}(A')
\end{array}
$$

The left square commutes since φ^n is a natural transformation by inductive hypothesis. The right square commutes since that is how we defined φ^{n+1} (see (2.1)). Thus, the outer rectangle commutes. On the other hand, the naturality of δ tells us that the horizontal composite $\delta \circ F^n(g)$ is simply the δ map $F^n(A'') \to F^{n+1}(A')$ corresponding to the first row of (2.4) and similarly for T^*. Thus, the outer rectangle commuting shows us that φ^{n+1} commutes with δ, as desired. $\qquad\square$

§§2.3. Introduction to colimits

Recall that a partially ordered set (poset) $(\Lambda, \leqslant)$ is a set Λ with a binary relation $\leqslant$ which is reflexive, antisymmetric, and transitive. We shall assume that all our posets are nonempty. Λ can be considered as a category in the following way:

1. the objects are elements of Λ,

2. there is a unique arrow $a \to b$ whenever $a \leqslant b$,

3. the composition is the forced one.

Λ is said to be (upwards) directed if for all $a, b \in \Lambda$, there exists $c \in \Lambda$ such that $a \leqslant c$ and $b \leqslant c$.

We now define what a colimit is, in the general setting, but we shall soon turn to the situation where the index category is a directed poset.

**Definition 2.3.1.** Let I and $\mathbf{C}$ be categories, and $F : I \to \mathbf{C}$ be a functor.

A co-cone (N, ψ) of F is an object N of C together with a family of morphisms $\psi_i : F(i) \to N$ for every object i of I, such that for every morphism $f : i \to j$ in I, we have $\psi_j \circ F(f) = \psi_i$.

A colimit of F is a co-cone (L, φ) of F such that for any co-cone (N, ψ) of F, there is a unique morphism $u : L \to N$ such that $u \circ \varphi_i = \psi_i$ for all $i \in I$.

To ease our mind, let us immediately see an example when I the simplest interesting example: the poset $(\mathbb{N}_0, \leqslant)$. Giving a functor $F : I \to \mathbf{C}$ is the same as giving a diagram (in $\mathbf{C}$) of the form

$$C(0) \xrightarrow{f(0)} C(1) \xrightarrow{f(1)} C(2) \xrightarrow{f(2)} \cdots .$$

A limit will be an object L along with morphism $\varphi(i) : C(i) \to L$ such that each (of the infinitely many) triangle commutes:
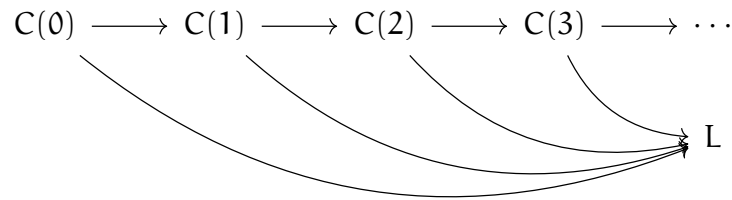
The universal property states that given any commutative diagram of the above form after replacing L with some N, there exists a unique morphism $L \to N$ making the diagram below commute for all $i \geqslant 0$.
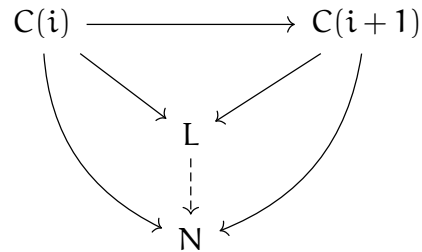
Exercise 2.3.2. Show that if a colimit of F exists, then it is unique up to unique isomorphism.

In view of the above exercise, we can talk about *the* colimit. This is denoted by $\operatorname{colim}_{i \in I} F(i)$. If I is a directed poset considered as a category, then the colimit is called a direct limit and denoted by $\varinjlim_{i \in I} F(i)$.

Example 2.3.3. We also have a familiar example of colimit: direct sums. Indeed, if I is an arbitrary (nonempty) set, then I can be made a poset by giving it the discrete order, i.e., $x \leqslant y \Leftrightarrow x = y$. In this case, the colimit of $F : I \to \mathbf{A}$ is simply the direct sum $\bigoplus_{i \in I} F(i)$. Note that if I is not a singleton, then the poset is not directed.

Proposition 2.3.4. Let I be a small category, i.e., the collection of objects forms a set. Let $\mathbf{A}$ be either R-**mod** or $\mathbf{R}$ for some ring R. Then, given any functor $F : I \to \mathbf{A}$, the colimit $\mathrm{colim}_{i \in I} F(i)$ exists.

Proof. Construct the following two direct sums:

$$\bigoplus_{\varphi : i \to j} F(i) \quad \text{and} \quad \bigoplus_{i \in I} F(i),$$

where the first direct sum is taken over all morphisms in I.

For each such morphism $\varphi : i \to j$ in I, we have the map $F(\varphi) : F(i) \to F(j)$. This gives us a map

$$\Phi : \bigoplus_{\varphi : i \to j} F(i) \to \bigoplus_{i \in I} F(i).$$

(Note that we may have multiple arrows between two objects of I. This leads to multiple copies of $F(i)$ on the left.) Similarly, since we have the maps $\mathrm{id}_{F(i)} : F(i) \to F(i)$ for every $\varphi : i \to j$, we get a map

$$\Psi : \bigoplus_{\varphi : i \to j} F(i) \to \bigoplus_{i \in I} F(i).$$

$\mathrm{coker}(\Phi - \Psi)$ gives the desired colimit. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \square$

Remark 2.3.5. The above construction works for any small category I. In the special case that I is a directed poset, we have a better alternate description as follows: Let $F : I \to \mathbf{A}$ be a functor. Construct the disjoint $\coprod_{i \in I} F(i)$ and go modulo the following equivalence relation $\sim$: if $x_i \in A_i$ and $x_j \in A_j$, then $x_i \sim x_j$ iff there exists $k \in I$ with $i \leqslant k$ and $j \leqslant k$ such that

$$F(i \to k)(x_i) = F(j \to k)(x_j),$$

i.e., x_i and x_j "become equal in some higher $F(k)$".

Thus, the (object of the) colimit is given by

$$L := \coprod_{i \in I} F(i)/\sim.$$

The maps $\varphi_i : F(i) \to L$ are the the obvious inclusions $F(i) \hookrightarrow \coprod_{i \in I} F(i)$ followed by the projection $\coprod_{i \in I} F(i) \to L$.

Example 2.3.6. Consider the poset $I = \mathbb{N}$ with the order given by divisibility, i.e., $i \leqslant j$ iff i divides j. Consider the functor $F : I \to \mathbb{Z}\text{-}\mathbf{mod}$ given by

$$F(i) = \mathbb{Z}$$

for all $i \in I$. Moreover, if $i \to j$ is a map, then $F(i \to j)$ is multiplication by $\frac{j}{i}$.

It is easy to check that F is indeed a functor since $\frac{i}{i} = 1$ and $\frac{j}{i} \cdot \frac{k}{j} = \frac{k}{i}$.

We claim that the colimit of F is $\mathbb{Q}$ with the map $\varphi_i : F(i) \to \mathbb{Q}$ is division by i.

First, we check that $(\mathbb{Q}, \varphi)$ is actually a co-cone. To this end, if $i \to j$ is a morphism, then given $x \in \mathbb{Z}$, we have

$$(\varphi_j \circ F(i \to j))(x) = \varphi_j \left(\frac{jx}{i} \right) = \frac{x}{i} = \varphi_i(x).$$

The check of the universal property is left as an exercise. We are essentially using the fact that $\mathbb{Q}$ is a localisation of $\mathbb{Z}$ with respect to $\mathbb{N}$.

Remark 2.3.7. More generally, any localisation can be viewed as a colimit. However, this will be as a colimit of a category which is more general than a directed poset. It will be the colimit of a *filtered category*, which is not something we need to define and so we do not. We outline the construction below.

Let $S \subseteq R$ be a multiplicative subset and M be an R-module. Consider S as a category where the objects are elements of S and

$$\mathrm{Hom}_S(s_1, s_2) = \{s \in S : ss_1 = s_2\}.$$

Composition is given by multiplication. 1 acts as identity. (Note that it is possible that $\mathrm{Hom}_S(s_1, s_2) = \varnothing$ for some s_1 and s_2. That is okay.)

For $s \in S$, let $\mu_s : M \to M$ denote multiplication by s. Then, we define the functor $F : S \to R\text{-}\mathbf{mod}$ by

$$F(s) = M \quad \text{and} \quad F(s_1 \xrightarrow{s} s_2) = \mu_s.$$

As before, it is easy to see that F is actually a functor. Lastly, the colimit is given by $S^{-1}M$ with the maps $\varphi_s : M \to S^{-1}M$ being $x \mapsto \frac{x}{s}$.

§3. I-**power torsion**

§§3.1. Definition

In what follows, R will be a commutative ring with 1, M an R-module, and $I \subseteq R$ an ideal of R.

Definition 3.1.1. Given a R-module M, and an ideal $I \subseteq R$, we define

$$\Gamma_I(M) := \{x \in M : I^k x = 0 \text{ for some } k \geqslant 1\}.$$

If $I = (a)$, we denote Γ_I by Γ_a.

Remark 3.1.2. Note that

$$\Gamma_I(M) = \bigcup_{k \geqslant 1} \left(0 :_M I^k\right) = \bigcup_{k \geqslant 1} \text{ann}_M(I^k).$$

is a submodule of M.

Proposition 3.1.3. Let $a \in R$, and M be an R-module. a is a nonzerodivisor on M iff $\Gamma_a(M) = 0$.

Proof. ($\Rightarrow$) Suppose a is a nonzerodivisor on M. If $x \neq 0$, then $ax \neq 0$ since a is a nonzerodivisor. Inductively, this gives us that $a^n x \neq 0$ for all $n \geqslant 1$. Thus, $\Gamma_a(M) = 0$.

($\Leftarrow$) Suppose $x \in M \setminus \{0\}$. Then, $x \notin \Gamma_a(M)$. In particular, $ax \neq 0$, as desired.   □

Proposition 3.1.4. Let $a \in R$, and M be an R-module. Then, the kernel of the natural map $M \xrightarrow{\varphi} M_a$ is equal to $\Gamma_a(M)$.

Proof. For $x \in M$, note that

$$x \in \ker(\varphi) \Leftrightarrow a^n x = 0 \text{ for some } n \Leftrightarrow x \in \Gamma_a(M).$$ □

Example 3.1.5. It is not necessary that $\Gamma_I(M/\Gamma_I(M)) = 0$.

Consider $R = M = k[X_1, X_2, X_3, \ldots]/(X_1, X_2^2, X_3^3, \ldots, X_i X_j \text{ for } i \neq j)$.
Let x_i denote the image of X_i in the ring R. Let $\mathfrak{m} = (x_1, x_2, \ldots)$.

Claim. $\mathfrak{m} = \Gamma_\mathfrak{m}(R)$.

This is easy to see since $m^n x_n = 0$. Thus, $x_n \in \Gamma_m(R)$ for all n. In turn, $m \subseteq \Gamma_m(R)$. The latter is a proper ideal since m is not nilpotent. Thus, maximality of m forces equality.

Thus, $k = R/\Gamma_m(R)$. However, note that $mk = 0$, i.e., every element of m annihilates every element of k. Thus, $\Gamma_m(k) = k \neq 0$. Thus,

$$\Gamma_m(R/\Gamma_m(R)) \neq 0.$$

The above does not happen if one of R or M is Noetherian.

Proposition 3.1.6. Let M be an R-module. Let $I \subseteq R$ be an ideal. If either R is a Noetherian ring, or M is a Noetherian R-module, then $\Gamma_I(M/\Gamma_I(M)) = 0$.

Proof. Note that given any $x \in M$, the hypothesis of one of R or M being Noetherian implies that $I^k x$ is a finitely generated submodule of M.

Let $N := \Gamma_I(M)$. Let $x \in M$ be such that $\overline{x} \in \Gamma_I(M/N)$. Thus, there is some $k \geqslant 1$ such that $I^k \overline{x} = 0$ or $I^k x \subseteq N$. Thus, every element of $I^k x$ is annihilated by some power of I. Since $I^k x$ is finitely generated, one can find $n \gg 0$ such that I^n that kills $I^k x$. Thus, $I^{n+k} x = 0$ and $x \in \Gamma_I(M)$, as desired. □

Definition 3.1.7. M is said to be I-torsion if $\Gamma_I(M) = M$.
M is said to be I-torsionfree if $\Gamma_I(M) = 0$.

Observation 3.1.8. If N is a submodule of M, then $\Gamma_I(N)$ is a submodule of $\Gamma_I(M)$. More precisely, $N \cap \Gamma_I(M) = \Gamma_I(N)$.

Observation 3.1.9. If $J \subseteq I$ and $x \in M$, then $J^k x \subseteq I^k x$ for all x. Thus, $\Gamma_I(M) \subseteq \Gamma_J(M)$. In particular,

$$M \text{ is J-torsionfree} \Rightarrow M \text{ is I-torsionfree},$$
$$M \text{ is I-torsion} \Rightarrow M \text{ is J-torsion}.$$

Moreover, $\Gamma_0(M) = M$ and $\Gamma_R(M) = 0$ for all M.

Proposition 3.1.10. Let $I, J \subseteq R$ be ideals of R. Let M be an R-module. Then,

(i) $\Gamma_{I+J}(M) = \Gamma_I(M) \cap \Gamma_J(M)$,

(ii) $\Gamma_I(M) + \Gamma_J(M) \subseteq \Gamma_{IJ}(M)$,

(iii) $\Gamma_I(\Gamma_J(M)) = \Gamma_I(M) \cap \Gamma_J(M) = \Gamma_{I+J}(M)$.

Proof. Using Observation 3.1.8, we see that (iii) follows from (i). By Observation 3.1.9, it follows that $\Gamma_{I+J}(M) \subseteq \Gamma_I(M) \cap \Gamma_J(M)$ and $\Gamma_I(M) + \Gamma_J(M) \subseteq \Gamma_{IJ}(M)$. We only need to prove $\Gamma_I(M) \cap \Gamma_J(M) \subseteq \Gamma_{I+J}(M)$.

Let $x \in \Gamma_I(M) \cap \Gamma_J(M)$. Pick $k \gg 0$ such that $I^k x = J^k x = 0$. Then, $(I + J)^{2k} x = 0$. $\qquad\square$

Example 3.1.11. We give an example to show that the inclusion $\Gamma_I(M) + \Gamma_J(M) \subseteq \Gamma_{IJ}(M)$ can be strict.

Let $R = k[x, y]$, $I = (x)$, $J = (y)$, and $M = R/IJ$. Then, $\Gamma_{IJ}(M) = M$, $\Gamma_I(M) = (y)$, and $\Gamma_J(M) = (x)$.

Proposition 3.1.12. Suppose $J \subseteq I$ are ideals such that $I^n \subseteq J$ for some $n \geqslant 1$. Then, $\Gamma_I(M) = \Gamma_J(M)$.

Proof. By Observation 3.1.9, we have

$$\Gamma_I(M) \subseteq \Gamma_J(M) \subseteq \Gamma_{I^n}(M).$$

Since a power of I^n is also a power of I, it follows that $\Gamma_{I^n}(M) \subseteq \Gamma_I(M)$ and we are done. $\qquad\square$

Corollary 3.1.13. If R is Noetherian, then $\Gamma_I = \Gamma_{\sqrt{I}}$.

Proof. $I \subseteq \sqrt{I}$ is true for any ideal in any ring. Since R is Noetherian, there exists n such that $(\sqrt{I})^n \subseteq I$ and the result follows. $\qquad\square$

Corollary 3.1.14. Let R be Noetherian, and $I, J \trianglelefteq R$. $\Gamma_I = \Gamma_J$ iff $\sqrt{I} = \sqrt{J}$.

By $\Gamma_I = \Gamma_J$, we mean that $\Gamma_I(M) = \Gamma_J(M)$ for all modules M.

Proof. ($\Longleftarrow$) If $\sqrt{I} = \sqrt{J}$, then $\Gamma_I = \Gamma_{\sqrt{I}} = \Gamma_{\sqrt{J}} = \Gamma_J$.

($\Longrightarrow$) Suppose $\sqrt{I} \neq \sqrt{J}$. We wish to show that $\Gamma_I \neq \Gamma_J$. Without loss of generality, there exists $a \in \sqrt{I} \setminus \sqrt{J}$.

Consider the module $M = R/J$. Evidently, M is J-torsion as $\Gamma_J(M) = M$. However, M is

not I-torsion. Indeed, for every $k \geqslant 1$, we have $\mathfrak{a}^k \in I^k$. Since $\mathfrak{a} \notin \sqrt{J}$, we have that $\mathfrak{a}^k \notin J$ for all k. Thus, $I^k \cdot \bar{1} \neq 0$ for all $k \geqslant 1$. $\qquad\square$

Example 3.1.15. The above is not true without the Noetherian hypothesis. We may consider the setup of Example 3.1.5 again. Note that $\mathfrak{m} = \sqrt{0}$ but $\Gamma_0(R) = R \neq \mathfrak{m} = \Gamma_{\mathfrak{m}}(R)$.

§§3.2. Functorial properties

Let R-**mod** denote the category of R-modules, and $\Gamma_I(R\text{-}\mathbf{mod})$ the full subcategory of R-**mod** whose objects are I-torsion modules.

Observation 3.2.1. Note that $\Gamma_I(R\text{-}\mathbf{mod})$ is closed under submodules and quotients, i.e., is closed under kernels and cokernels. The direct sum of I-torsion modules is again I-torsion. Thus, $\Gamma_I(R\text{-}\mathbf{mod})$ is an abelian category.

Observation 3.2.2. Let $f : M \to N$ be an R-linear map. Suppose $x \in M$ is annihilated by I^k for some k. Then,
$$I^k f(x) = f(I^k x) = 0.$$
Thus, $f(x) \in \Gamma_I(N)$. In other words, $f(\Gamma_I(M)) \subseteq \Gamma_I(N)$.

Definition 3.2.3. In view of the above observation, we let Γ_I denote the obvious functor from R-**mod** to $\Gamma_I(R\text{-}\mathbf{mod})$.

Let $\iota : \Gamma_I(R\text{-}\mathbf{mod}) \to R\text{-}\mathbf{mod}$ denote the inclusion functor.

Observation 3.2.4. Note that Γ_I is an additive functor (as addition of maps commutes with restriction).
Also, $\Gamma_I(\Gamma_I(M)) = M$ for all $M \in R\text{-}\mathbf{mod}$.

Proposition 3.2.5. Γ_I preserves injective maps.

Proof. By Observation 3.2.2, we see that $\Gamma_I(f)$ is simply a restriction of f. Thus, if f were injective, so is $\Gamma_I(f)$. $\qquad\square$

Remark 3.2.6. Note that preserving injective maps is weaker than being left exact. The next proposition will tell us that Γ_I is indeed left exact.

Proposition 3.2.7. Γ_I is right adjoint to ι and hence, is left exact.

Proof. This again follows from Observation 3.2.2: If M were I-torsion to begin with, then we see that any map from M lands within $\Gamma_I(N)$. Thus, there is a natural isomorphism

$$\mathrm{Hom}_{R\text{-}\mathbf{mod}}(\iota(M), N) \cong \mathrm{Hom}_{\Gamma_I(R\text{-}\mathbf{mod})}(M, \Gamma_I(N)).$$ $\square$

We give an alternate proof below that $\Gamma := \Gamma_I$ is a left exact functor.

Proof. Let

$$0 \to L \xrightarrow{f} M \xrightarrow{g} N \tag{3.1}$$

be an exact sequence.

$\Gamma(f)$ is injective by Proposition 3.2.5. We need to show that $\mathrm{im}(\Gamma(f)) = \ker(\Gamma(g))$. To this end, let $m \in \ker(\Gamma(g))$. Then

$$g(m) = \Gamma(g)(m) = 0.$$

By exactness of (3.1), it follows that there exists $l \in L$ such that $f(l) = m$. We wish to show that $l \in \Gamma(L)$.

Since $m \in \Gamma(M)$, there exists $k \geqslant 1$ such that $I^k m = 0$. For $i \in I^k$, we have

$$f(il) = if(l) = im = 0.$$

Since f is an injection, it follows that $il = 0$ and thus $I^k l = 0$, as desired. $\square$

Corollary 3.2.8. Γ_I preserves injectives.

Proof. ι is exact and Γ_I is a right adjoint to ι. $\square$

Remark 3.2.9. Note that the above is saying that if E is an injective R-module, then $\Gamma_I(E)$ is an injective object in the category $\Gamma_I(R\text{-}\mathbf{mod})$. This is not saying that $\Gamma_I(E)$ is an injective R-module.

We will now like to show that $\Gamma_I(E)$ is actually an injective R-module when R is Noetherian (and we will do so without using Corollary 3.2.8). Γ_I being additive tells us that Γ_I preserves finite direct sums. It is not difficult to see $\Gamma_I(-)$ actually preserves arbitrary direct sums. Thus, in view of Theorem 1.4.3, it suffices to study $\Gamma_I(E_R(R/\mathfrak{p}))$ for $\mathfrak{p} \in \mathrm{Spec}(R)$.

Proposition 3.2.10. Let R be Noetherian. Fix $\mathfrak{p} \in \mathrm{Spec}(R)$ and set $E := E_R(R/\mathfrak{p})$. For $a \in R$, let $\mu_a \in \mathrm{End}_R(E)$ be the map $x \mapsto ax$.

1. If $a \notin \mathfrak{p}$, then μ_a is an isomorphism.

2. If $a \in \mathfrak{p}$, then for every $y \in E$, there exists $n \geqslant 1$ such that $a^n y = 0$.

Proof. Note that $\mathrm{Ass}(E) = \{\mathfrak{p}\}$.

1. If $a \notin \mathfrak{p}$, then a is not a zerodivisor on E, i.e., μ_a is injective. Thus, $\mu_a(E) \cong E$ is injective. Since $\mu_a(E)$ is an injective submodule of E, it splits off E. But E is indecomposable. This forces $\mu_a(E) = E$, as desired.

2. Let $y \in E$. There is nothing to prove if $y = 0$. Assume $y \neq 0$. Then, $\varnothing \neq \mathrm{Ass}(Ry) \subseteq \{\mathfrak{p}\}$. Thus, $\sqrt{\mathrm{ann}_R(y)} = \mathfrak{p}$. Thus, y is killed by some power of $\mathfrak{p}$ and hence, of a. $\square$

Porism 3.2.11. $E_R(R/\mathfrak{p})$ is $\mathfrak{p}$-torsion.

Corollary 3.2.12. Let $I \subseteq R$ be an ideal, and $\mathfrak{p} \in \mathrm{Spec}(R)$.

$$\Gamma_I(E_R(R/\mathfrak{p})) = \begin{cases} E_R(R/\mathfrak{p}) & I \subseteq \mathfrak{p}, \\ 0 & I \not\subseteq \mathfrak{p}. \end{cases}$$

In words: $E_R(R/\mathfrak{p})$ is I-torsion if $I \subseteq \mathfrak{p}$ and I-torsionfree otherwise.

Proof. By Porism 3.2.11, the result is clear if $I \subseteq \mathfrak{p}$. Conversely, if there exists $a \in I \setminus \mathfrak{p}$, then μ_a is injective, by Proposition 3.2.10. Thus, so is each μ_a^n. Hence, if $0 \neq y \in E_R(R/\mathfrak{p})$. Then, $0 \neq a^n y \in I^n y$. $\square$

Corollary 3.2.13. Let R be a Noetherian ring, and E an injective R-module. Then, $\Gamma_I(E)$ is an injective R-module.

Proof.

$$\Gamma_I \left(\bigoplus_{\mathfrak{p}} E_R(R/\mathfrak{p})^{a(\mathfrak{p})} \right) = \bigoplus_{\mathfrak{p} \supseteq I} E_R(R/\mathfrak{p})^{a(\mathfrak{p})}.$$ $\square$

Example 3.2.14. Let us see Γ_I is not right exact. Suffices to show that Γ_I does not preserve surjections. Consider $R = \mathbb{Z}$ and $I = p\mathbb{Z}$ for any integer $p \geqslant 2$. We have the surjective quotient map

$$\mathbb{Z} \to \mathbb{Z}/p.$$

Applying Γ_I gives us
$$0 \to \mathbb{Z}/p,$$
which is clearly not surjective.

More generally, we may choose R to be any domain which is not a field, and I to be any nonzero proper ideal and consider the map $R \to R/I$.

§§3.3. Localisation

In what follows, S will be a multiplicative subset of R.

If $N \leqslant M$ are R-modules, note that $S^{-1}N$ is an $S^{-1}R$-submodule of $S^{-1}M$ given as

$$S^{-1}N = \left\{ \frac{x}{s} : x \in N, s \in S \right\}.$$

We record a simple property below.

Proposition 3.3.1. $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$ for ideals $I, J \subseteq R$.

Recall that if J is an ideal of R, and M an R-module, then we define the R-submodule $\text{ann}_M(J)$ of M by
$$\text{ann}_M(J) := \{x \in M : jx = 0 \text{ for all } j \in J\}.$$

Proposition 3.3.2. Let J be a finitely generated ideal of R. Then,

$$S^{-1}(\text{ann}_M(J)) = \text{ann}_{S^{-1}M}(S^{-1}J).$$

Proof. ($\subseteq$) Let $\frac{x}{s} \in S^{-1}(\text{ann}_M(J))$, where $x \in \text{ann}_M(J)$ and $s \in S$. (This is how an arbitrary element of $S^{-1}(\text{ann}_M(J))$ looks.)

Then, given an arbitrary $\frac{j}{t} \in S^{-1}J$ (where $j \in J$ and $t \in S$), we have

$$\frac{j}{t}\frac{x}{s} = \frac{jx}{ts} = \frac{0}{ts} = 0.$$

Thus, $\frac{x}{s} \in \text{ann}_{S^{-1}M}(S^{-1}J)$.

($\supseteq$) Let $\frac{x}{s} \in \text{ann}_{S^{-1}M}(S^{-1}J)$, where $x \in M$ and $s \in S$.
Fix $j \in J$. By assumption, we have

$$\frac{j}{1}\frac{x}{s} = 0.$$

Thus, there exists $s_j \in S$ such that

$$s_j j x = 0 \quad \text{or} \quad j(s_j x) = 0.$$

Now, let $j_1, \ldots, j_n$ generate J and set $s_0 := s_{j_1} \cdots s_{j_n} \in S$. Then we have

$$j(s_0 x) = 0$$

for all $j \in J$, i.e., $s_0 x \in \mathrm{ann}_M(J)$. In turn, we have

$$\frac{x}{s} = \frac{s_0 x}{s_0 s} \in S^{-1}(\mathrm{ann}_M(J)),$$

as desired. $\square$

Proposition 3.3.3. Let

$$M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots$$

be an increasing chain of R-submodules of M. Then,

$$S^{-1}\left(\bigcup_{n \geqslant 0} M_n \right) = \bigcup_{n \geqslant 0} S^{-1} M_n.$$

Proof. Easy check. $\square$

Corollary 3.3.4. Let R be a Noetherian ring, $I \subseteq R$ an ideal, $S \subseteq R$ a multiplicative subset, and M an R-module. Then,

$$S^{-1}\Gamma_I(M) = \Gamma_{S^{-1}I}(S^{-1}M).$$

Proof. Note that we have

$$\begin{aligned}
S^{-1}\Gamma_I(M) &= S^{-1}\left(\bigcup_{k \geqslant 1} \mathrm{ann}_M(I^k) \right) && \text{\textit{Proposition 3.3.3}} \\
&= \bigcup_{k \geqslant 1} \left(S^{-1} \mathrm{ann}_M(I^k) \right) && \text{\textit{Proposition 3.3.2}} \\
&= \bigcup_{k \geqslant 1} \mathrm{ann}_{S^{-1}M}(S^{-1}(I^k)) && \text{\textit{Proposition 3.3.1}} \\
&= \bigcup_{k \geqslant 1} \mathrm{ann}_{S^{-1}M}((S^{-1}I)^k) && \\
&= \Gamma_{S^{-1}I}(S^{-1}M),
\end{aligned}$$

as desired. $\square$

Example 3.3.5. Let R be Noetherian. Specialising to the case where $S = \{1, a, a^2, \ldots\}$ for some $a \in R$, we have

$$(\Gamma_I(M))_a = \Gamma_{I_a}(M_a).$$

Now, we have the localisation map

$$\Gamma_I(M) \to \Gamma_{I_a}(M_a).$$

By Proposition 3.1.4, we see that the kernel of the above map is $\Gamma_a(\Gamma_I(M))$. By Proposition 3.1.10, we see that this kernel is $\Gamma_{(I,a)}(M)$. Thus, we have an exact sequence as

$$0 \to \Gamma_{(I,a)}(M) \to \Gamma_I(M) \to \Gamma_{I_a}(M_a).$$

§§3.4. Restriction of scalars

In this section, R and S are rings, and $f : R \to S$ is a ring homomorphism. M will be an S-module, which we shall consider as an R-module via the rule

$$r \cdot m := f(r) \cdot m$$

for $r \in R$ and $m \in M$. We may denote this module by f^*M or M_R to remind us that we are viewing M as an R-module.

Given an ideal $J \trianglelefteq S$, we have an ideal $f^{-1}(J)$ of R.
Conversely, given an ideal $I \trianglelefteq R$, we may extend to an ideal $f(I)S$ of S.

Proposition 3.4.1. Let $J \subseteq S$ be an ideal, and M be an S-module. We have

$$\Gamma_J(M) \subseteq \Gamma_{f^{-1}(J)}(f^*M).$$

Furthermore, if f is a surjection, then equality holds.

Note that technically, the left object is an S-module and the right is an R-module. However, it makes sense to talk about the above inclusions both sets above are subsets of M. Alternately, the S-module may be treated as an R-module.

Proof. Put $I := f^{-1}(J)$ and let $x \in \Gamma_I(M) \, \Gamma_{f^{-1}(I)}(f^*M)$ be arbitrary. Let k be such that $J^k x = 0$. Note that $f(I) \subseteq J$ and thus, $f(I^k) \subseteq J^k$. Thus, given $r \in I^k$, we have $r \cdot x \in J^k x = \{0\}$.

Now, if f is a surjection, then $f(I) = J$ and consequently $f(I^k) = J^k$ from the reverse inclusion follows. $\qquad\square$

Example 3.4.2. The above inclusion can be strict if f is not onto. Consider $R = \mathbb{Z}$, $S = \mathbb{Z}[x]$, and f to be the inclusion map. Consider $M = S$ as a module over itself. Let $J = (x)S$. Thus, $I = f^{-1}(J) = 0$. Thus, $\Gamma_J(M) = 0$ and $\Gamma_{f^{-1}(J)}(f^*M) = S$.

Question. What if f is an epimorphism (but not necessarily surjective, for example, a localisation map), i.e., if $g, h : S \to S'$ are ring maps with $gf = hf$, then $g = h$?

Proposition 3.4.3. Let $I \subseteq R$ be an ideal, and M be an S-module. Then,

$$\Gamma_I(f^*M) = \Gamma_{f(I)S}(M).$$

Proof. Let $J := f(I)S$.

($\subseteq$) Let $x \in \Gamma_I(f^*M)$. Pick $k \geqslant 1$ such that $I^k x = 0$. Note that J^k is additively generated by elements of the form $f(i)s$, where $i \in I^k$ and $s \in S$. For such an element, we have

$$f(i)s \cdot x = s \cdot (f(i) \cdot x) = 0.$$

($\supseteq$) Conversely, let $x \in \Gamma_J(M)$ and $k \geqslant 1$ be such that $J^k x = 0$. We have $f(I^k) \subseteq J^k$. Thus, given $i \in I^k$, we have

$$i \cdot x = f(i) \cdot x \in J^k x = 0. \qquad \square$$

§§3.5. **Extension of scalars**

In this section, R and S are rings, and $f : R \to S$ is a ring homomorphism. M will be an R-module. We define the R-module $M^S := S \otimes_R M$ which we shall consider as an S-module via the rule

$$s \cdot (s' \otimes m) := (ss') \otimes m,$$

for $s, s' \in S$ and $m \in M$ (and extending it linearly).

As before, given ideals $I \trianglelefteq R$ and $J \trianglelefteq S$, we get ideals $f(I)S \trianglelefteq S$ and $f^{-1}(J) \trianglelefteq R$.

Remark 3.5.1. If $N \leqslant M$ are R-module, then there are two ways one way wish to interpret N^S. The first is the honest tensor product $S \otimes_R N$. The other is the additive subgroup of $S \otimes_R M$ generated by elements of the form $s \otimes n$ for $s \in S$ and $n \in N$.
The unfortunate issue is that they are **not** isomorphic in general.

Consider the example of $R = \mathbb{Z}$, $S = \mathbb{Z}/2$, f being the quotient, $M = \mathbb{Z}$, $N = 2\mathbb{Z}$. Note that $M \cong N$ as $\mathbb{Z}$-modules and thus, the tensor products $S \otimes_{\mathbb{Z}} M$ and $S \otimes_{\mathbb{Z}} N$ are both isomorphic to $\mathbb{Z}/2$. However, the submodule interpretation gives us the 0-module since then we have

$$\overline{x} \otimes (2y) = (2\overline{x}) \otimes y = 0$$

for all $\overline{x} \in \mathbb{Z}/2$ and $y \in \mathbb{Z}$.

In essence, this is just capturing the fact that tensoring is not left exact in general, i.e., if $0 \to N \xrightarrow{i} M$ is exact, it does not mean that $0 \to N^S \xrightarrow{i^S} M^S$ is so. In fact, the second interpretation of N^S as a submodule of M^S is precisely the submodule $i^S(N^S)$. The failure of i^S being injective shows that N^S need not be isomorphic to $i^S(N^S)$.

However, if S is a flat R-algebra, then this does not happen.

Proposition 3.5.2. Let M be an R-module, and $I \subseteq R$ an ideal. Let N denote the submodule which is the image $S \otimes_R \Gamma_I(M)$ inside M^S. Then,

$$N \subseteq \Gamma_{f(I)S}(M^S).$$

Or, interpreting appropriately, we have

$$S \otimes_R \Gamma_I(M) \subseteq \Gamma_{f(I)S}(M^S).$$

Proof. Let $\sum s_\alpha \otimes m_\alpha \in N$, with $m_\alpha \in \Gamma_I(M)$. As the summation is finite, we may fix $k \geqslant 1$ such that $I^k m_\alpha = 0$ for all α. Let $J := f(I)S$. As before, J^k is generated additively by elements of the form $f(i)s$ with $i \in I^k$ and $s \in S$. For such an element, we have

$$(f(i)s) \cdot \left(\sum s_\alpha \otimes m_\alpha \right) = \sum (f(i)ss_\alpha) \otimes m_\alpha = \sum (ss_\alpha) \otimes (i \cdot m_\alpha) = 0. \qquad \square$$

Example 3.5.3. The inclusion above can be strict even if f is surjective. Consider $R = \mathbb{Z}$, $S = \mathbb{Z}/4$, f to be the quotient map, $M = \mathbb{Z}$, and $I = 2\mathbb{Z}$. Then, $\Gamma_I(\mathbb{Z}) = 0$. On the other hand,

$$\Gamma_{f(I)S}(M^S) = \Gamma_{2\mathbb{Z}/4}(\mathbb{Z}/4) = \mathbb{Z}/4 \neq 0.$$

Example 3.5.4. In the other direction, one may consider an ideal $J \subseteq S$ and ask if there is any inclusion between

$$S \otimes_R \Gamma_{f^{-1}(J)}(M) \quad \text{and} \quad \Gamma_J(M^S),$$

where the left module is interpreted as the submodule of M^S.

We now give two examples to show that neither inclusion is true.

Firstly, we may consider the previous example with $J = 2\mathbb{Z}/4\mathbb{Z}$ to see that the right module is a strict superset.

Secondly, we may consider $R = \mathbb{Z}$, $S = \mathbb{Z}[x]$, f the inclusion map, $M = \mathbb{Z}$, and $J = (x)$. Then, $f^{-1}(J) = (0)$. Thus, the left module is $\mathbb{Z}[x]$ whereas the right is 0.

§§3.6. Derived functors

Since Γ_I is a left exact functor, it makes sense to talk about its derived functor.

Definition 3.6.1. For $n \geqslant 1$, let Γ_I^n denote the n-th derived functor of Γ_I.

Define $\Gamma_I^0 := \Gamma_I$.

Remark 3.6.2. Recall how a derived functor: Given an R-module M, fix an injective resolution

$$0 \to M \to I^0 \to I^1 \to I^2 \to \cdots .$$

Applying Γ_I, we form the cochain

$$0 \to \Gamma_I(I^0) \to \Gamma_I(I^1) \to \cdots . \tag{3.2}$$

The cohomology at the n-th stage is $\Gamma_I^n(M)$. As usual, this is functorial and independent of the resolution $I^\bullet$.

Proposition 3.6.3. Let M be any R-module. Then, $\Gamma_I^n(M)$ is an I-torsion module for all $n \geqslant 0$.

Proof. The modules in (3.2) are all I-torsion. Since $\Gamma_I(R\text{-}\mathbf{mod})$ is closed under subquotients (Observation 3.2.1), the result follows. $\square$

§4. Injective hull over polynomial rings

§§4.1. Definitions and Notations

k will denote an arbitrary field. n will denote a positive integer. R_n will denote the polynomial ring $k[X_1, \ldots, X_n]$ with the usual operations.

Definition 4.1.1. E_n is the R_n-module defined as follows: As a set, $E_n = k[X_1^{-1}, \ldots, X_n^{-1}]$, i.e., polynomial in $X_1, \ldots, X_n^{-1}$ with k-coefficients. The scalar multiplication is defined on monomials by

$$X_i \cdot (X_1^{-b_1} \cdots X_n^{-b_n}) := \begin{cases} X^{-b_1} \cdots X^{-(b_i-1)} \cdots X_n^{-b_n} & \text{if } b_i \geqslant 1, \\ 0 & \text{else.} \end{cases}$$

Remark 4.1.2. Note that the above has the effect of the following multiplication on monomials:

$$(X_1^{a_1} \cdots X_n^{a_n}) \cdot (X_1^{-b_1} \cdots X_n^{-b_n}) := \begin{cases} X^{-(b_1-a_1)} \cdots X_n^{-(b_n-a_n)} & \text{if } b_i \geqslant a_i \text{ for all } i, \\ 0 & \text{else.} \end{cases}$$

In words: multiply the monomials in the expected manner, that is the actual product if the result is indeed in E_n, else it is 0.

Definition 4.1.3. Let R be a ring, and E an R-module. E is said to be an injective R-module if for every ideal $J \subseteq R$, every R-linear map $J \to E$ extends to an R-linear map $R \to E$.

Remark 4.1.4. The usual definition for E being injective is that for every inclusion $N \hookrightarrow M$ of R-modules, the restriction map $\operatorname{Hom}_R(M, E) \to \operatorname{Hom}_R(N, E)$ is surjective. The above definition says that it suffices to look at the inclusions $J \hookrightarrow R$. The equivalence is known as Baer's criterion.

Remark 4.1.5. One can show that the injective hull is defined uniquely up to isomorphism. Thus, we shall use the article "the" instead of "an" henceforth.

Note that k is an R_n-module viewed as the quotient $R_n/(X_1, \ldots, X_n)$. Thus, the action of R_n on k is given by each X_i acting trivially on k. This lets one identify k as an R_n-submodule of E_n.

Proposition 4.1.6. $k \subseteq E_n$ is an essential extension.

Proof. Let $n \geqslant 1$. Let $R_0 := k$ and $E_0 := R_0$. Note that $k \subseteq E_0$ is an essential extension. We now proceed by induction.

Let $p \in E_n \setminus \{0\}$ be arbitrary. We may write

$$p = p_0 + p_1 X_n^{-1} + \cdots p_k X_n^{-k}$$

for some $p_0, \ldots, p_k \in E_{n-1}$ with $k \geqslant 0$ and $p_k \neq 0$. Then,

$$X_n^k \cdot p = p_k \in R_{n-1} \setminus \{0\}.$$

By induction, we may multiply the above with an element of R_{n-1} and get a nonzero element of k. $\qquad \square$

§§4.2. One variable case

Note that $k[X]$ is a PID and thus, to show that $k[X^{-1}]$ is injective, it suffices to show that $k[X^{-1}]$ is divisible (Proposition 4.4.2). For ease of notation, we let $R = k[X]$ and $E = k[X^{-1}]$ with the R-module structure on E being as earlier.

Proposition 4.2.1. E is a divisible R-module.

Corollary 4.2.2. E is the injective hull of k.

Proof of Proposition 4.2.1. For $f \in R$, let $\mu_f \in \mathrm{End}_R(E)$ denote the map $p \mapsto f \cdot p$.

First note that μ_{X^k} is surjective for all $k \geqslant 0$. Indeed,

$$X^k \cdot (b_0 X^{-k} + b_1 X^{-k-1} + \cdots b_m X^{-k-m}) = b_0 + b_1 X^{-1} + \cdots + b_m X^{-m}.$$

Now, given $0 \neq f \in R$, we may write $f = X^k g$ for some $k \geqslant 0$ and $g \in R$ such that $g(0) \neq 0$, i.e., g has nonzero constant term.[2] As μ_{X^k} is surjective by the above, it suffices to assume that $f(0) \neq 0$. In fact, we may assume $f(0) = 1$ and write

$$f = 1 + a_1 X + \cdots + a_k X^k. \tag{4.1}$$

Now, note that $f \cdot 1 = 1$. Thus, $1 \in \mathrm{im}(\mu_f)$. Next,

$$f \cdot X^{-1} = (1 + a_1) + X^{-1}.$$

----

[2]We have simply pulled out the largest power of X.

The first term in parenthesis is already in $\mathrm{im}(\mu_f)$ as it is a k-multiple of 1. Thus, $X^{-1} \in \mathrm{im}(\mu_f)$. More generally, if $n \geqslant 1$, then

$$f \cdot X^{-n} = b_0 + b_1 X^{-1} + \cdots + b_{n-1} X^{-(n-1)} + X^{-n}$$

for some $b_i \in k$. Thus, inductively, we see that $X^{-n} \in \mathrm{im}(\mu_f)$ for all $n \geqslant 1$. As $\{X^{-n} : n \geqslant 0\}$ is a k-spanning set for E, we have shown that μ_f is surjective, as desired. $\square$

Remark 4.2.3. My original proof of the last part was a bit different. I had shown the following: Let f be as in (4.1) and assume $n \geqslant k$. Let $E[n]$ denote the k-vector subspace of E spanned by $\{1, \ldots, X^{-n}\}$. Then, one notes that μ_f restricts to a k-endomorphism $E[n]$. This is because any multiplication $X^a \cdot X^{-b}$, if nonzero, results in a monomial X^{-c} with $c \leqslant b$. In fact, if $a > 0$, then $c < b$.

Now, with respect to the basis $\{1, \ldots, X^{-n}\}$ of $E[n]$, the matrix of μ_f is upper triangular with 1s along the diagonal. This is a consequence of the last line of the previous paragraph. Thus, the matrix obtained is invertible. As every $q \in E$ is contained in some $E[n]$ (with $n \geqslant k$), this finished the proof.

The proof given above can actually be shortened to not involve taking the case $f = X^k$ separately. We do this in more generality for higher variables.

§§4.3. More variables

In this section, we show that E_n is an R_n-divisible module for any $n \geqslant 1$. However, note that this does not let us conclude that E_n is an injective R_n-module since R_n is not a PID for $n \geqslant 2$.

We introduce some notations.

1. $[n] := \{1, \ldots, n\}$ for $n \in \mathbb{N}$.

2. An element $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$ is called a multi-index.

3. $|\alpha| := \alpha_1 + \cdots + \alpha_n$.

4. We define the total order $<_{\text{lex}}$ on $\mathbb{N}_0^n$ by

$$\alpha <_{\text{lex}} \beta \Leftrightarrow \text{there exists } i \in [n] \text{ such that } \alpha_i < \beta_i \text{ and } \alpha_j = \beta_j \text{ for all } j < i$$

5. We define the total order $<$ on $\mathbb{N}_0^n$ by

$$\alpha < \beta \Leftrightarrow |\alpha| < |\beta|, \text{ or}$$
$$|\alpha| = |\beta| \text{ and } \alpha <_{\text{lex}} \beta.$$

6. For $\alpha, \beta \in \mathbb{N}_0^n$, we define

$$X^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n} \in R_n \quad \text{and} \quad X^{-\beta} = X_1^{-\beta_1} \cdots X_n^{-\beta_n} \in E_n.$$

Note that there is a natural way to define $\beta - \alpha$ as an element of $\mathbb{Z}^n$. Under the above definition, the multiplication on E_n can be written as:

$$X^\alpha \cdot X^{-\beta} = \begin{cases} X^{-(\beta - \alpha)} & \text{if } \beta - \alpha \in \mathbb{N}_0^n, \\ 0 & \text{else.} \end{cases}$$

Due to this, we may sometimes write $X^{-\beta}$ even if $\beta \in \mathbb{Z}^n$, with the understanding that this element is 0 if $\beta \notin \mathbb{N}_0^n$.

Remark 4.3.1. Note that $\alpha < \beta \Rightarrow \alpha + \gamma < \beta + \gamma$ for all $\alpha, \beta, \gamma \in \mathbb{N}_0^n$. However, $\alpha < \beta$ does not imply that $\beta - \alpha \in \mathbb{N}_0^n$.

Remark 4.3.2. Multi-indices and monomials in R_n have a one-to-one correspondence via $\alpha \leftrightarrow X^\alpha$. Similarly, so do multi-indices and monomials in E_n. Using this, we may compare two monomials in R_n (resp. E_n) as well.

Note that this means that $X^{-\beta_1}$ will be called smaller than $X^{-\beta_2}$ if $\beta_1 < \beta_2$. Explicitly, X_1^{-1} is smaller than X_1^{-2}.

Remark 4.3.3. $<$ is a well-order on $\mathbb{N}_0^n$. Thus, we may give inductive proofs.

Proposition 4.3.4. E_n is a divisible R_n-module.

Proof. Suppose not. Then there is some $0 \neq f \in R_n$ such that μ_f is not surjective. Pick β smallest such that $X^{-\beta}$ is not in $\operatorname{im}(\mu_f)$. Let X^α be the smallest monomial appearing in f. Without loss of generality, the coefficient of X^α is 1. Thus, we may write

$$f = X^\alpha + \sum_{\alpha' > \alpha} c_{\alpha'} X^{\alpha'}$$

for $c_{\alpha'} \in k$.

Then,

$$f \cdot X^{-(\alpha + \beta)} = X^{-\beta} + \sum_{\alpha' > \alpha} c_{\alpha'} X^{-(\beta + \alpha - \alpha')}.$$

Note that the monomials on the summation on the right are smaller than $X^{-\beta}$ since $\alpha < \alpha'$. Thus those monomials are in $\operatorname{im}(\mu_f)$. But then,

$$X^{-\beta} = f \cdot X^{-(\alpha + \beta)} - \sum_{\alpha' > \alpha} c_{\alpha'} X^{-(\beta + \alpha - \alpha')} \in \operatorname{im}(\mu_f). \qquad \square$$

§§4.4. Divisibility and Injectivity

We now look at some proofs of how injectivity and divisibility are related.

Proposition 4.4.1. Let E an injective R-module. Then, E is divisible.

Proof. Let $r \neq R \setminus \mathcal{Z}(R)$ and $x \in E$ be arbitrary. As $r \notin \mathcal{Z}(R)$, the ideal rR has basis $\{r\}$. Thus, we get an R-linear map $f : rR \to E$ defined by $r \mapsto x$. As E is injective, f extends to an R-linear map $F : R \to E$. Thus,

$$x = f(r) = F(r) = rF(1) = \mu_r(F(1)),$$

showing that μ_r is surjective. □

Proposition 4.4.2. Let R be a PID, and E a divisible R-module. Then, E is injective.

Proof. Let $J \subseteq R$ be an ideal, and $f : J \to R$ be R-linear. If $J = 0$, then zero map $0 : R \to E$ works as an extension. Thus, assume that $J = rR$ for some $r \neq 0$. (J is singly generated as R is a PID.)

Let $y := f(r) \in E$. As E is divisible and $r \neq 0$, there exists $x \in E$ such that $rx = y$. Define $F : R \to E$ by $1 \mapsto x$. Then, for $rs \in rR$, we see that

$$F(rs) = rsF(1) = srx = sy = sf(r) = f(rs).$$

That is, $F|_J = f$, as desired. □

Note that there are possibly multiple $x \in E$ that solve $rx = y$. Choosing any x gives a valid choice of F. The reason is that J was singly generated and thus, we only need to check compatibility with r. If R is not a PID, then it is not so simple.

Proposition 4.4.3. Let R be any domain, and E be a divisible and torsionfree R-module. Then, E is injective.

Proof. As before, we assume that $J \neq 0$ is an ideal of R and $f : J \to E$ is R-linear. Let $j \in J \setminus \{0\}$. By hypothesis, $\mu_j : E \to E$ is an isomorphism. We claim that the element

$$x_j := \mu_j^{-1}(f(j)) \in E$$

is independent of $j \in J \setminus \{0\}$.

Note that x_j is defined to be the unique solution to

$$jx_j = f(j).$$

(To emphasise: existence is guaranteed by divisibility and uniqueness by torsionfreeness.)

Let $i \in J \setminus \{0\}$ be arbitrary. Note that

$$ijx_j = if(j) = f(ij) = jf(i) = jix_i.$$

Thus,

$$ij(x_i - x_j) = 0.$$

As R is a domain and E is torsionfree, the above forces $x_i = x_j$, as desired.

Now, denoting this element by x, we simply define $F : R \to E$ by $1 \mapsto x$. Note that if $j \in J \setminus \{0\}$, then

$$F(j) = jF(1) = jx = f(j),$$

as desired. (Clearly, $F(0) = 0 = f(0)$ as well.) $\square$

Remark 4.4.4. To summarise, we have shown that for an arbitrary domain, we have

$$\text{injective} \Rightarrow \text{divisible},$$
$$\text{divisible and torsionfree} \Rightarrow \text{injective}.$$

Whereas for a PID, we have
$$\text{injective} \Leftrightarrow \text{divisible}.$$

Example 4.4.5. Let $R = \mathbb{Z}$, and $E = \mathbb{Q}/\mathbb{Z}$. $\mathbb{Q}$ is a divisible R-module and thus, so is E. Thus, E is injective (since $\mathbb{Z}$ is a PID) but E is not torsionfree.

Example 4.4.6. We now show that "divisible $\Rightarrow$ injective" is indeed not true.

Let $R = \mathbb{Z}[x]$ and $E = \mathbb{Q}(x)/\mathbb{Z}[x]$. Note that E is divisible since $\mathbb{Q}(x)$ is so. Let $J = (2, x)R \subseteq R$. Define the map $f : J \to E$ by

$$2 \mapsto 0,$$
$$x \mapsto [1/2],$$

where $[\cdot]$ denotes the class modulo $\mathbb{Z}[x]$. Note that $\{2, x\}$ is not an R-basis of J and thus, we must check that f above is well-defined. We must check that whenever $f, g \in R$ are such that $2f + xg = 0$, then $f \cdot 0 + g \cdot [1/2] = 0$. This is easy to see. Indeed, if

$$2f = -xg,$$

then $2 \mid g$. (Note that 2 is a prime in R and does not divide $-x$.)
Thus, we may write $g = 2h$ for some $h \in R$ but then

$$f \cdot 0 + g \cdot [1/2] = 2h \cdot [1/2] = h \cdot [1] = 0.$$

We contend that there is no extension $F : R \to E$ of f. We look at the equations that $F(1)$ would have to satisfy. We have

$$2F(1) = F(2) = 0,$$
$$xF(1) = F(x) = [1/2].$$

The first equation tells us that $F(1) = [\frac{1}{2}h(x)]$ for some $h(x) \in \mathbb{Z}[x]$. By the second, we have that

$$x\left[\frac{1}{2}h(x)\right] = \left[\frac{1}{2}\right] \quad \text{or} \quad \frac{1}{2}(xh(x) - 1) \in \mathbb{Z}[x].$$

Evaluating the above at $x = 0$ gives us that $1/2 \in \mathbb{Z}$, a contradiction.

The calculation in the proof of Proposition 4.4.3 tells us the following.

Proposition 4.4.7. Let R be a ring, $J \subseteq R$ an ideal, E an R-module, and $f \in \mathrm{Hom}_R(J, E)$. There exists an extension $F : R \to E$ iff there exists $x \in E$ such that $j \cdot x = f(j)$ for all $j \in J$.

Note that there is no domain assumption.

Proof. ($\Rightarrow$) Take $x = F(1)$.

($\Leftarrow$) Defining F by $1 \mapsto x$ does the job. $\qquad\square$

In fact, the proof given in Example 4.4.6 was essentially to show that there is no $y \in E$ that solves both $2 \cdot y = f(2)$ and $x \cdot y = f(x)$. Note that divisibility told us one may *individually* solve $2 \cdot y_1 = f(2)$ and $x \cdot y_2 = f(x)$ for $y_1, y_2 \in E$. However, there is no *common* solution.

Note that if $j_1 \cdot x = f(j_1)$ and $j_2 \cdot x = f(j_2)$, then for $r_1, r_2 \in R$, we have

$$f(r_1 j_1 + r_2 j_2) = r_1 f(j_1) + r_2 f(j_2) = r_1 j_1 \cdot x + r_2 j_2 \cdot x = (r_1 j_1 + r_2 j_2) \cdot x.$$

Thus, we get the following corollary.

Corollary 4.4.8. Let R be a ring, $J \subseteq R$ an ideal, E an R-module, and $f \in \mathrm{Hom}_R(J, E)$. Suppose J is generated by S.
There exists an extension $F : R \to E$ iff there exists $x \in E$ such that $s \cdot x = f(s)$ for all $s \in S$.

Thus, we have reduced our system of simultaneous equations to a generating set. In particular, if R is Noetherian, then S can be chosen to be finite.

Proposition 4.4.9. Let R be a domain. Suppose E is a divisible R-module, and $J \subseteq R$ is an ideal. Assume J contains a nonzerodivisor $j_0 \in J$ on E. Then, any R-linear map $f : J \to E$ can be extended to a map $R \to E$.

Proof. In view of Proposition 4.4.7, we wish to solve for simultaneously solve for an $x \in E$ such that $j \cdot x = f(j)$ for all $j \in J$. By hypothesis, there exists a unique $x \in E$ such that $j_0 \cdot x = f(j_0)$. We now show that this x works for every $j \in J$. Indeed, as before we have

$$j_0 \cdot f(j) = j \cdot f(j_0) = j_0 \cdot (j \cdot x).$$

Now, we may cancel j_0 to get $f(j) = j \cdot x$ for every $j \in J$. □

Remark 4.4.10. Note that in our earlier case of $R_n = k[X_1, \ldots, X_n]$ and $E_n = k[X_1^{-1}, \ldots, X_n^{-1}]$, we see that any $f \in R_n$ with a nonzero constant term is a nonzerodivisor on E_n. Conversely, if $f(\mathbf{0}) = 0$, then f annihilates k.

Thus, to use prove injectivity of E_n, we only need to show that we can extend maps from ideals J contained in the maximal ideal $(X_1, \ldots, X_n)$.

Here's a modified version of Baer's criterion.

Proposition 4.4.11. Let R be a Noetherian ring, and E be a module such that the following holds: For every proper ideal $I \subsetneq R$ and every R-linear map $f : I \to E$, there exists an ideal $J \supsetneq I$ such that f can be extended to an R-linear map $J \to E$.

Then, E is injective.

Proof. Suppose E is not injective. Then, by Baer's criterion, there exists an ideal I and a R-linear map $f : I \to E$ which cannot be extended to a map $R \to E$. Since R is Noetherian, we may choose I to be maximal with respect to this property. Note that $I \neq R$ since otherwise f itself is the desired extension. Then, by hypothesis, f can be extended to map $F : J \to R$ for some strictly larger ideal $J \supsetneq I$. By the maximality of I, F can extended to a map $\widetilde{F} : R \to E$. But then $\widetilde{F}$ extends f, contrary to our assumption. □

We record the usual trick of expanding $f(j_1 j_2)$ in two ways below.

Proposition 4.4.12 (Compatibility condition). Let $f : J \to M$ be an R-linear map, where J is an ideal of R. Then, for $r, s \in J$, we have

$$r \cdot f(s) = s \cdot f(r). \tag{CC}$$

Observation 4.4.13. Let us consider the case of two variables: $R = k[X, Y]$ and $E = k[X^{-1}, Y^{-1}]$. Suppose $\varphi : (X, Y) \to E$ is an R-linear map. We wish to show that φ can be extended to R.

Write

$$\varphi(X) = \sum_{\beta \in \mathbb{N}_0^2} b_\beta X^{-\beta},$$

$$\varphi(Y) = \sum_{\beta \in \mathbb{N}_0^2} c_\beta X^{-\beta}.$$

Note that

$$X \cdot \varphi(Y) = \sum_{\substack{\beta_1 \geqslant 1 \\ \beta_2 \geqslant 0}} c_{\beta_1, \beta_2} X^{1-\beta_1} Y^{-\beta_2}$$

$$= \sum_{\beta \in \mathbb{N}_0^2} c_{1+\beta_1, \beta_2} X^{-\beta_1} Y^{-\beta_2}.$$

Similarly,

$$Y \cdot \varphi(X) = \sum_{\beta \in \mathbb{N}_0^2} b_{\beta_1, 1+\beta_2} X^{-\beta_1} Y^{-\beta_2}.$$

Now, by (CC), we get

$$c_{1+\beta_1, \beta_2} = b_{\beta_1, 1+\beta_2}$$

for all $(\beta_1, \beta_2) \in \mathbb{N}_0^2$.

This lets us get a simultaneous solution as desired by Corollary 4.4.8. More precisely, we first define

$$p := \sum_{\beta \in \mathbb{N}_0^2} b_\beta X^{-(\beta_1+1)} Y^{-\beta_2}.$$

Evidently, we have $X \cdot p = \varphi(X)$. Moreover, we have

$$Y \cdot p = \sum_{\substack{\beta_1 \geqslant 0 \\ \beta_2 \geqslant 1}} b_{\beta_1, \beta_2} X^{-(\beta_1+1)} Y^{-(\beta_2-1)}$$

$$= \sum_{\beta \in \mathbb{N}_0^2} b_{\beta_1, \beta_2+1} X^{-(\beta_1+1)} Y^{-\beta_2}$$

$$= \sum_{\beta \in \mathbb{N}_0^2} c_{1+\beta_1, \beta_2} X^{-(\beta_1+1)} Y^{-\beta_2}$$

$$= \sum_{\substack{\beta_1 \geqslant 1 \\ \beta_2 \geqslant 0}} c_\beta X^{-\beta}.$$

Note that the above is *almost* $\varphi(Y)$. More precisely, $\varepsilon := \varphi(Y) - Y \cdot p$ is given by

$$\varepsilon = \sum_{\beta_2 \geqslant 0} c_{0,\beta_2} Y^{-\beta_2}.$$

Now, if we define $\delta := \sum_{\beta_2 \geqslant 0} c_{0,\beta_2} Y^{-(\beta_2+1)}$, then $Y \cdot \delta = \varepsilon$ and $X \cdot \delta = 0$. This means that the corrected term $q := p + \delta$ satisfies

$$X \cdot q = \varphi(X) \quad \text{and} \quad Y \cdot q = \varphi(Y).$$

Thus, by Corollary 4.4.8, the result follows.

Observation 4.4.14. The above can be extended to $R_3 = k[X, Y, Z]$ and E_3 as well. In this case, writing

$$\varphi(X) = \sum_{\beta \in \mathbb{N}_0^3} b_\beta X^{-\beta}$$

$$\varphi(Y) = \sum_{\beta \in \mathbb{N}_0^3} c_\beta X^{-\beta},$$

$$\varphi(Z) = \sum_{\beta \in \mathbb{N}_0^3} d_\beta X^{-\beta},$$

we will get compatibility conditions as

$$b_{\beta_1,\beta_2+1,\beta_3} = c_{\beta_1+1,\beta_2,\beta_3},$$
$$c_{\beta_1,\beta_2,\beta_3+1} = d_{\beta_1,\beta_2+1,\beta_3},$$
$$d_{\beta_1+1,\beta_2,\beta_3} = b_{\beta_1,\beta_2,\beta_3+1},$$

for all $(\beta_1, \beta_2, \beta_3) \in \mathbb{N}_0^3$. For convenience, let $e_1 := (1,0,0)$, and similarly define e_2 and e_3.

As before, our first candidate for a common solution will be

$$p := \sum_{\beta \in \mathbb{N}_0^3} b_\beta X^{-(\beta+e_1)}.$$

Then, $X \cdot p = \varphi(X)$ but $Y \cdot p$ differs from $\varphi(Y)$. The terms corresponding to $\beta_1 = 0$ will not appear in $Y \cdot p$. Thus, we modify our solution to

$$p' := p + \sum_{\substack{\beta \in \mathbb{N}_0^3 \\ \beta_1 = 0}} c_\beta X^{-(\beta+e_2)}.$$

As before, X annihilates the additional term added and $Y \cdot p' = \varphi(Y)$. Lastly, we add $\sum_{\beta_3 \geqslant 0} d_\beta X^{-(0,0,\beta_3)}$ to correct the term for Z.

It is now clear how one may proceed in higher variables to obtain similar results. The only trouble is notational. We state the result without proving it.

Proposition 4.4.15. Let R_n and E_n be as in Definition 4.1.1, and define $\mathfrak{m} := (X_1, \ldots, X_n)$. Suppose $f : \mathfrak{m} \to E_n$ is R_n-linear. Then, f extends to an R_n-linear map $F : R_n \to E_n$.

§5. Čech cohomology

Definition 5.0.1. Let R be a ring, and $a \in R$. Define the cocomplex $\check{C}^\bullet(a)$ by

$$0 \to R \to R_a \to 0,$$

concentrated in degrees 0 and 1.

The map $R \to R_a$ is the natural localisation map $r \mapsto r/1$.

Recall that given cocomplexes $C^\bullet$ and $D^\bullet$, the tensor product $C^\bullet \otimes_R D^\bullet$ is the cocomplex whose n-th term is

$$[C^\bullet \otimes_R D^\bullet]^n := \bigoplus_{p+q=n} C^p \otimes_R D^q,$$

with the coboundary map given on simple tensors $c^p \otimes d^q \in C^p \otimes_R D^q$ by

$$\partial(c^p \otimes d^q) := \partial(c^p) \otimes d^q + (-1)^p c^p \otimes \partial(d^q).$$

Definition 5.0.2. Given elements $a_1, \ldots, a_n$, define the Čech cocomplex $\check{C}^\bullet(a_1, \ldots, a_n)$ by

$$\check{C}^\bullet(a_1) \otimes_R \cdots \otimes_R \check{C}^\bullet(a_n).$$

Note that we have natural isomorphisms

$$R_a \otimes_R R_b \cong (R_a)_b \cong R_{ab}$$

of R-modules.

For notational sake, let e_a denote $1/1$ in R_a. Similarly, let e_{ab} denote $1/1$ in R_{ab}, et cetera.

Example 5.0.3. Let us write out $\check{C}(a, b)$ and $\check{C}(a, b, c)$. The modules are given as:

$$0 \to R \to R_a \oplus R_b \to R_{ab} \to 0,$$
$$0 \to R \to R_a \oplus R_b \oplus R_c \to R_{ab} \oplus R_{bc} \oplus R_{ac} \to R_{abc} \to 0.$$

This makes the general picture of $\check{C}(a_1, \ldots, a_n)$ clear, as far as the modules are concerned. It looks something like

$$0 \to R \xrightarrow{\partial^0} \bigoplus_{1 \leqslant i \leqslant n} R_{a_i} \xrightarrow{\partial^1} \bigoplus_{1 \leqslant i_1 < i_2 \leqslant n} R_{a_{i_1} a_{i_2}} \xrightarrow{\partial^2} \cdots \to \bigoplus_{1 \leqslant i \leqslant n} R_{a_1 \cdots \widehat{a_i} \cdots a_n} \xrightarrow{\partial^{n-1}} R_{a_1 \cdots a_n} \to 0.$$

$$(5.1)$$

∂_0 is given by $1 \mapsto (e_{a_1}, \ldots, e_{a_n})$. ∂^{n-1} is "given by"

$$e_{a_1 \cdots \widehat{a_i} \cdots a_n} \mapsto \pm e_{a_1 \cdots a_n},$$

where the sign depends on i and n.

Remark 5.0.4. Note that e_a is not an R-basis for R_a. Indeed, $1/a$ is not generally in the R-submodule generated by $\{e_a\}$.

Proposition 5.0.5. The zeroth cohomology $H^0(\check{C}(a_1, \ldots, a_n))$ is given as

$$H^0(\check{C}(a_1, \ldots, a_n)) = \Gamma_{a_1}(R) \cap \cdots \cap \Gamma_{a_n}(R) = \Gamma_{(a_1, \ldots, a_n)}(R).$$

Proof. Follows from Proposition 3.1.4 and Proposition 3.1.10. $\square$

Corollary 5.0.6. If R is a domain, and $a_1, \ldots, a_n \in R$ are nonzero, then $H^0(\check{C}(a_1, \ldots, a_n)) = 0$. More generally, if $a_1, \ldots, a_n$ are nonzerodivisors, then $H^0(\check{C}(a_1, \ldots, a_n)) = 0$.

Similarly, if $(a_1, \ldots, a_n) = R$, then $H^0(\check{C}(a_1, \ldots, a_n)) = 0$.

Proposition 5.0.7. Let $a_1, \ldots, a_n \in R$. For each $i \in \{1, \ldots, n\}$, let N_i denote the image of $R_{a_1 \cdots \widehat{a_i} \cdots a_n}$ in $R_{a_1 \cdots a_n}$. Then,

$$H^n(\check{C}(a_1, \ldots, a_n)) = R_{a_1 \cdots a_n} / (N_1 + \cdots + N_n).$$

Of course, the above proposition is not saying anything since the above is quite literally the definition of (co)homology. However, we now note a particular example.

Example 5.0.8. Consider $R = k[X]$ and $a = X$. In this case, note that the Čech cocomplex $\check{C}(X)$ is given as

$$0 \to k[X] \hookrightarrow k\left[X, \frac{1}{X}\right] \to 0.$$

As $k[X]$ is an integral domain and $X \neq 0$, it follows that the localisation map above is an inclusion, i.e., $H^0(\check{C}(X)) = 0$. For the first cohomology, note that

$$H^1(\check{C}(X)) = \frac{k\left[X, \frac{1}{X}\right]}{k[X]}.$$

Let us analyse the above quotient. Elements of $k[X, \frac{1}{X}]$ are elements of the form

$$\frac{a_{-m}}{X^m} + \cdots + \frac{a_{-1}}{X} + a_0 + \cdots + a_n X^n.$$

Quotienting by $k[X]$ will only leave us with the "principal" (or "negative" part). More precisely, each equivalence class of the quotient will contain a unique representative of the form $\frac{a_{-m}}{X^m} + \cdots + \frac{a_{-1}}{X}$. Furthermore, adding two representatives gives us the representative of the sum. Finally, looking at the action of X^k on such an element, we see that

$$X^k \cdot \left(\frac{a_{-m}}{X^m} + \cdots + \frac{a_{-1}}{X} \right) = \sum_{k < i \leqslant m} \frac{a_{-i}}{X^{i-k}}.$$

This resembles the familiar module $E_1 = k[X^{-1}]$ from Definition 4.1.1! More precisely, this is $k[X^{-1}]/k$.

In fact, this generalises quite easily to case of $R = R_n$. In that case, we have

$$H_n(\check{C}(X_1, \ldots, X_n)) \cong X_1^{-1} \cdots X_n^{-1} E_n.$$

Let us try to see the above in the case of $n = 2$. Write $R = k[X, Y]$ and take $(a_1, a_2) = (X, Y)$. Note that R_{XY} are sums of the form

$$\sum_{a,b \in \mathbb{Z}} ?X^a Y^b,$$

where the coefficients are in k.
Thus, we have elements like $\frac{1}{XY} + \frac{1}{X} + \frac{1}{Y} + X$.

On the other hand, the image of $R_X \oplus R_Y$ only consists of polynomials of the form

$$\sum_{a,b \in \mathbb{N}_0} ?X^a Y^b + \sum_{a<0} ?X^a + \sum_{b<0} ?Y^b.$$

Thus, there are no polynomials involving terms with both X and Y having negative exponent. Again, it is easy to see that the quotient is E_2/k.

For the general case, we may define a map $R_{X_1 \cdots X_n} \to E_n$ by

$$\sum_{\alpha \in \mathbb{Z}^n} a_\alpha X^\alpha \mapsto \sum_{\alpha \in (-\mathbb{N}_0)^n} a_\alpha X^\alpha.$$

Composing this with the quotient map $E_n \to E_n/k$ gives us an onto map $R_{X_1 \cdots X_n} \to E_n/k$. The kernel of this contains precisely of those polynomials which have monomials of the form X^α with at least one α_i nonnegative. This is exactly the image of ∂^{n-1}, in the notation of (5.1).

Example 5.0.9. Let us now compute all cohomologies for polynomials rings in few variables. The rings appearing below will be integral domains. The advantage in that case is that we can think of the localisations as submodules of the quotient field of R (and all the localisation maps are actually inclusions).

$n = 1 : R = k[X]$. $\check{C}(X)$ is given as

$$0 \to k[X] \to k\left[X, \frac{1}{X}\right] \to 0.$$

As discussed, we have

$$H^0(\check{C}(X)) = 0 \quad \text{and} \quad H^1(\check{C}(X)) = k[X^{-1}]/k.$$

$n = 2 : R = k[X]$. $\check{C}(X, Y)$ is given as

$$0 \to k[X, Y] \xrightarrow{\partial^0} k\left[X, Y, \frac{1}{X}\right] \oplus k\left[X, Y, \frac{1}{Y}\right] \xrightarrow{\partial^1} k\left[X, Y, \frac{1}{XY}\right] \to 0.$$

We already know that $H^0 = 0$ and $H^2 = k[X^{-1}, Y^{-1}]/k$ for the above. We claim that $H^1 = 0$. Indeed, note that

$$\partial^1(f, g) = -f + g.$$

Thus, if $\partial^1(f, g) = 0$, then

$$f = g \in k\left[X, Y, \frac{1}{X}\right] \cap k\left[X, Y, \frac{1}{Y}\right] = k[X, Y].$$

Thus, $(f, g) = \partial^0(f) \in \text{im}(\partial^0)$, as desired.

$n = 3 : R = k[X, Y, Z]$ and the complex is "given by"

$$0 \to R \xrightarrow{\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}} R_X \oplus R_Y \oplus R_Z \xrightarrow{\begin{bmatrix} -1 & 1 & 0 \\ -1 & 0 & 1 \\ 0 & -1 & 1 \end{bmatrix}} R_{XY} \oplus R_{XZ} \oplus R_{YZ} \xrightarrow{[1 \; -1 \; 1]} R_{XYZ} \to 0.$$

Note that the modules appearing above are not free R-modules, even though we are using matrices to denote the maps. The above says that for $(f, g, h) \in R_X \oplus R_Y \oplus R_Z$, we have

$$\partial^1(f, g, h) = (-f + g, -f + h, -g + h).$$

Thus, if $(f, g, h) \in \ker(\partial^1)$, then

$$f = g = h \in R_X \cap R_Y \cap R_Z = R.$$

As before, we have $(f, g, h) = \partial^0(f) \in \mathrm{im}(\partial^0)$. Thus, $H^1(\check{C}(X, Y, Z)) = 0$.

Now, let $(f, g, h) \in R_{XY} \oplus R_{XZ} \oplus R_{YZ}$ be in the kernel of ∂^2. Then,

$$f = g - h \in R_{XY} \cap (R_{XZ} + R_{YZ}) = R_X + R_Y.$$

(The sum and intersection above makes sense by working in the field $k(X, Y, Z)$, as remarked earlier.)

Similarly, $g \in R_X + R_Z$ and $h \in R_Y + R_Z$. Thus, we can write

$$
\begin{aligned}
f &= -f_1 + f_2, \\
g &= -g_1 + g_2, \\
h &= -h_1 + h_2,
\end{aligned}
$$

for $f_1, g_1 \in R_X$, $f_2, h_1 \in R_Y$, and $g_2, h_2 \in R_3$.

Now, using the fact that $f - g + h = 0$, we get

$$(-f_1 + g_1) + (f_2 - h_1) + (-g_2 + h_2) = 0.$$

The terms are grouped so that the terms are in R_X, R_Y, and R_Z, respectively. This shows that all the terms are actually polynomials. (Since $R_X \cap (R_Y + R_Z) = R$, etc.)

Note that we have freedom in choosing f_1, g_1, h_1 in the sense that we may change the value by an element of R and accordingly fix f_2, g_2, h_2. Since $-f_1 + g_1$ is a polynomial, we may as well adjust the terms so that $-f_1 + g_1 = 0$. Now, f_2 is fixed. But $f_2 - h_1$ is a polynomial and thus we may fix h_1 such that $f_2 - h_1 = 0$. This also then forces $g_2 = h_2$. Thus, we are left with

$$(f, g, h) = (-f_1 + h_1, -f_1 + g_2, -h_1 + g_2) = \partial^1(f_1, h_1, g_2) \in \mathrm{im}(\partial^1).$$

This shows that $H^2(\check{C}(X, Y, Z)) = 0$ as well.

§6. Completions

§§6.1. Filtered rings and modules

Definition 6.1.1. A filtered ring R is a ring R together with a family $(R_n)_{n \geqslant 0}$ of subgroups of R satisfying the conditions:

1. $R_0 = R$,

2. $R_{n+1} \subseteq R_n$ for all $n \geqslant 0$,

3. $R_m R_n \subseteq R_{m+n}$ for all $m, n \geqslant 0$.

Putting $m = 0$ in the last condition gives $RR_n \subseteq R_n$ for all $n \geqslant 0$. Thus, $(R_n)_{n \geqslant 0}$ is a (decreasing) family of ideals.

Example 6.1.2.   1. For any ring R, setting $R_0 = R$ and $R_n = 0$ for $n > 0$ gives a filtration on R. This is called the trivial filtration.

2. Let R be an arbitrary ring and $I \trianglelefteq R$ be an ideal. Then, $R_n := I^n$ for $n \geqslant 0$ gives the I-adic filtration on R.

3. If $(R_n)_n$ is a filtration on R and S a subring of R, then $(S \cap R_n)_n$ is a filtration on S, called the induced filtration on S.

Definition 6.1.3. Let R be a filtered ring. A filtered R-module M is an R-module M together with a family $(M_n)_{n \geqslant 0}$ of additive groups of M satisfying

1. $M_0 = M$,

2. $M_{n+1} \subseteq M_n$ for all $n \geqslant 0$,

3. $R_m M_n \subseteq M_{m+n}$ for all $n, m \geqslant 0$.

As before, putting $m = 0$ in the last point shows that each M_n is an R-submodule.

1. A filtered ring is a filtered module over itself (with the filtration being the same).

2. Corresponding to the trivial filtration on R, we have the trivial filtration on any (usual) R-module M given by $M_0 = M$ and $M_n = 0$ for $n > 0$.

3. Similarly, defining $M_n := I^n M$ gives the I-adic filtration on M (corresponding to the I-adic filtration on R).

4. More generally, given a filtered ring R and an ordinary R-module M, we can define a filtration on M by $M_n := R_n M$. This gives M the structure of a filtered R-module.

5. Let M be a filtered R-module and N be an R-submodule of M. Then, we have an

induced filtration on N and M/N given as

$$(N \cap M_n)_{n \geqslant 0} \quad \text{and} \quad \left(\frac{N + M_n}{N} \right)_{n \geqslant 0},$$

respectively.

Definition 6.1.4. Let M and N be filtered modules over a filtered ring R. A map $f : M \to N$ is called a homomorphism (map) of filtered modules if f is R-linear and $f(M_n) \subseteq N_n$ for all $n \geqslant 0$.

Example 6.1.5.   1. Let R be a filtered ring, and $f : M \to N$ be an (ordinary) R-module homomorphism. If M and N are given the filtrations $(R_n M)_{n \geqslant 0}$ and $(R_n N)_{n \geqslant 0}$ respectively, then f is a homomorphism of filtered modules.
   In particular, this is true for I-filtrations.

   2. Let M be a filtered R-module and N be an R-submodule. Then, the projection $p : M \to M/N$ is a homomorphism of filtered modules. Indeed, the filtration of M/N is given precisely as $(p(M_n))_{n \geqslant 0}$.

Definition 6.1.6. A graded ring R is a ring which can be written as a direct sum of subgroups $(R_n)_{n \geqslant 0}$ such that $R_m R_n \subseteq R_{m+n}$ for all $n, m \geqslant 0$.

A nonzero element of R_n is said to be a homogeneous element of degree n.

Remark 6.1.7. Note that we are not demanding $R_0 = R$ above. In fact, if $R_0 = 0$, then we would have $R_n = 0$ for all $n > 0$. This is called the trivial gradation on R.

Observation 6.1.8. R_0 is a subring of R. Indeed, it is clear that R_0 is closed under sums and products (put $m = n = 0$ in the definition).
We must show that $1 \in R_0$.

By assumption, we may write

$$1 = r_0 + r_1 + \cdots + r_m$$

for some $m \geqslant 0$ with $r_i \in R_i$.

Multiplying both sides with r_i above gives

$$r_i = r_i r_0 + r_i r_1 + \cdots r_i r_m.$$

Comparing degrees of homogeneous elements on both sides shows that $r_0 r_i = r_i$ for all $0 \leqslant i \leqslant m$. Finally, we get

$$r_0 = r_0 \cdot \sum r_i = \sum r_0 r_i = \sum r_i = 1.$$

Corollary 6.1.9. If R is a graded ring with grading $(R_n)_{n \geqslant 0}$, then

1. R_0 is a subring,

2. R is an R_0-module,

3. R_n is an R_0-submodule for all $n \geqslant 0$.

Proof. Only the last assertion needs to be proven. This follows by putting $m = 0$ in the definition of a graded ring. $\square$

Example 6.1.10. The motivating example is that of a polynomial ring. Consider $R = k[X_1, \ldots, X_n]$, where k is a field. Define R_n to be the k-vector space generated by monomials of the form X^α with $|\alpha| = n$. Then, $(R_n)_{n \geqslant 0}$ defines a gradation on R.

Example 6.1.11. Given a ring R, and an R-module M, one forms the tensor algebra of M over R to be the R-algebra
$$T^*(M) = \bigoplus_{p \geqslant 0} T^p(M),$$
with $T^0(M) := R$ and $T^p(M) = M^{\otimes p}$ for $p \geqslant 1$. Multiplication is defined on pure tensors by
$$(x_1 \otimes \cdots \otimes x_p) \cdot (y_1 \otimes \cdots \otimes y_q) := x_1 \otimes \cdots \otimes x_p \otimes y_1 \otimes \cdots \otimes y_q.$$
This gives $T^*(M)$ the structure of a graded ring (which is also an R-algebra). However, this is **not** a commutative ring in general. Going modulo the ideal generated by elements of the form $x \otimes y - y \otimes x$ for $x, y \in M$ gives a graded commutative ring.

Note that R and M were not assumed to be graded here.

Definition 6.1.12. Let R be a graded ring. An R-module M is called a graded R-module if M can be expressed as a direct sum of subgroups $(M_n)_{n \geqslant 0}$ such that $R_m M_n \subseteq M_{m+n}$ for all $m, n \geqslant 0$.

An R-submodule N of M is said to be a graded submodule if N is the (internal) direct sum of $(N \cap M_n)_{n \geqslant 0}$.

Remark 6.1.13. Note that in the above M_n need **not** be an R-submodule of M. However, putting $m = 0$ shows that each M_n will be an R_0-submodule of M.

Example 6.1.14. Every graded ring is a graded module over itself (with the same gradation).

To check that the reader is following what is happening so far, they may verify the following proposition as an exercise.

Exercise 6.1.15. Let R be a graded and M a graded R-module. Let $N \leqslant M$ be an R-submodule. Show that the following are equivalent:

1. N is a graded submodule.

2. N is generated (as an R-module) by homogeneous elements.

3. If $x \in N$ and $x = x_0 + x_1 + \cdots x_n$, where $x_i \in M_i$, then $x_i \in N_i$ for all i.

The last point is saying that if some element belongs to N, then each of its homogeneous components also belongs to N.

Exercise 6.1.16. Let R be a graded ring and N be a graded submodule of M. Show that M/N has a graded R-module structure with gradation given by

$$\left(\frac{N + M_n}{N} \right)_{n \geqslant 0}.$$

Moreover, $(N + M_n)/N \cong M_n/N_n$ for all $n \geqslant 0$.

Definition 6.1.17. Let M and N be graded modules over a graded ring R. Let $f : M \to N$ be a map of R-modules. f is called a homomorphism (map) of graded modules if $f(M_n) \subseteq N_n$ for all $n \geqslant 0$.

Definition 6.1.18. Let R be a filtered ring with filtration $(R_n)_{n \geqslant 0}$. Let

$$\mathrm{gr}_n(R) := R_n/R_{n+1} \quad \text{and} \quad \mathrm{gr}(R) := \bigoplus_{n \geqslant 0} \mathrm{gr}_n(R).$$

Then, $gr(R)$ has a natural multiplication structure given by

$$(a + R_{m+1})(b + R_{n+1}) = ab + R_{m+n+1}$$

for $a \in R_m$ and $b \in R_n$. This makes R into a graded ring. This ring is called the associated graded ring of R.

Remark 6.1.19. Note that if $a \in R_m$ and $b \in R_n$, then

$$aR_{n+1} \subseteq R_{m+n+1}, \ bR_{m+1} \subseteq R_{m+n+1}, \ R_{m+1}R_{n+1} \subseteq R_{m+n+2} \subseteq R_{m+n+1}.$$

This is why the product defined above is well-defined. The ring axioms then are easily verified.

$gr_n(R) \, gr_m(R) \subseteq gr_{m+n}(R)$ is also clear from construction.

Example 6.1.20. Let R be any ring, and $t \in R$ be a nonzerodivisor. Consider the (t)-adic filtration on R. In this case,

$$gr_n(R) = (t^n)/(t^{n+1}),$$
$$gr(R) = R/(t) \oplus (t)/(t^2) \oplus (t^2)/(t^3) \oplus \cdots.$$

We observe that $gr(R)$ is naturally isomorphic to the polynomial ring $\frac{R}{(t)}[X]$.

To see this, first note that we have the identity ring homomorphism $R/(t) \to gr_0(R)$. (By definition, we have $gr_0(R) = R_0/R_1$.)

By the universal property of polynomial rings, extending this map to a ring homomorphism $\frac{R}{(t)}[X] \to gr(R)$ is the same as giving an element of $gr(R)$ and mapping X to it. We map X to the image of t in $gr_1(R) = (t)/(t^2)$. This gives us a ring homomorphism $\varphi : \frac{R}{(t)}[X] \to gr(R)$.

This is surjective as $\bar{r}X^n$ maps to $rt^n + (t^{n+1})$ and thus, the image contains $gr_n(R)$ for all $n \geqslant 0$.

We now show that $\ker(\varphi) = 0$. Let $\sum \bar{r_i}X^i \in \ker(\varphi)$, where $\bar{r_i}$ denotes the image of $r_i \in R$ in $R/(t)$.

Applying φ gives us that $r_i t^i \in (t^{i+1})$ for all i. Thus, we can write

$$r_i t^i = s_i t^{i+1}$$

for some s_i. Since t is a nonzerodivisor, we may cancel t^i to get $r_i = s_i t \in (t)$, i.e., $\bar{r_i} = 0$, as desired.

Example 6.1.21. Let $R = k[\![X_1, \ldots, X_n]\!]$ denote the n-variable power series ring over a field k, and $\mathfrak{m} := (X_1, \ldots, X_n)$. Consider the $\mathfrak{m}$-adic filtration on R. Note that $f \in \mathfrak{m}^d$ iff $\mathrm{ord}(f) \geqslant d$. (The order $\mathrm{ord}(f)$ of a nonzero power series to defined to be the minimum of $|\alpha|$ taking over all α such that X^α appears in f.)

Moreover, as a k-vector space, R_d/R_{d+1} is isomorphic to the space of all homogeneous polynomials of degree d. It is a quick check from here to see that

$$\mathrm{gr}(R) \cong k[X_1, \ldots, X_n],$$

the polynomial ring.

Definition 6.1.22. Let R be a filtered ring and M a filtered R-module. Let

$$\mathrm{gr}_n(M) := M_n/M_{n+1} \quad \text{and} \quad \mathrm{gr}(M) := \bigoplus_{n \geqslant 0} \mathrm{gr}_n(M).$$

Then, $\mathrm{gr}(M)$ has the structure of a <u>graded</u> $\mathrm{gr}(R)$-module given by

$$(a + R_{m+1})(x + M_{n+1}) = ax + M_{m+n+1}$$

for $a \in R_m$ and $x \in M_n$. This module is called the associated graded module of M.

Definition 6.1.23. Let R be a filtered ring, M, N filtered R-modules, and $f : M \to N$ a map of filtered R-modules. Then, there is a natural map

$$\mathrm{gr}(f) : \mathrm{gr}(M) \to \mathrm{gr}(N)$$

given on $\mathrm{gr}_n(M)$ by

$$m + M_{n+1} \mapsto f(m) + N_{n+1}$$

for $m \in M_n$.

Remark 6.1.24. As $f(M_{n+1}) \subseteq N_{n+1}$, the above map is well-defined.

The explicit definition leads to an easy proof of the following proposition.

Proposition 6.1.25. With notations as in Definition 6.1.23, we have the following.

1. $\mathrm{gr}(f)$ is a map of graded R-modules.
2. $\mathrm{gr}(\mathrm{id}_M) = \mathrm{id}_{\mathrm{gr}(M)}$.

3. If $h : N \to K$ is a map of filtered R-modules, then $gr(h \circ f) = gr(h) \circ gr(f)$.

Example 6.1.26. Let $R = \mathbb{Z}$, $I = (n)$ for some fixed $n > 1$. Let $M = N = \mathbb{Z}$. We have the R-linear map $f : M \to N$ given by $x \mapsto nx$. Giving the I-adic filtration to each of R, M, N yields that f is also a filtered map. Thus, we get a map $gr(f) : gr(M) \to gr(N)$. It is clear that $gr(f)$ is the zero map, even though f was a nonzero map. In fact, f was injective.

Proposition 6.1.27. Let R be a filtered, M, N filtered R-modules, and $f : M \to N$ a map of filtered R-modules. Suppose that $\bigcap_{n \geqslant 0} M_n = 0$.
If $gr(f)$ is injective, then f is injective.

Proof. By assumption, the restriction $gr_n(f) : M_n/M_{n+1} \to N_n/N_{n+1}$ is injective for all n. Thus, if $f(x_n) \in N_{n+1}$ for some $x_n \in M_n$, then $x_n \in M_n$. In other words,

$$f^{-1}(N_{n+1}) \cap M_n \subseteq M_{n+1}.$$

Moreover, note that

$$f^{-1}(N_0) \subseteq M_0.$$

Indeed, if $f(x_0 + \cdots + x_n) \in N_0$, then $f(x_1) = \cdots = f(x_n) = 0$ and hence, $x_i = 0$ for $i > 0$.

The above inclusions inductively give us that

$$f^{-1}(N_n) \subseteq M_n$$

for all $n \geqslant 0$. In turn,

$$f^{-1}(0) \subseteq f^{-1}\left(\bigcap_{n \geqslant 0} N_n\right) = \bigcap_{n \geqslant 0} f^{-1}(N_n) \subseteq \bigcap_{n \geqslant 0} M_n = (0). \qquad \square$$

Remark 6.1.28. The above is not true if "injective" is replace with "surjective".

Proposition 6.1.29. Let R be a graded ring with gradation $(R_n)_{n \geqslant 0}$. The following are equivalent:

  (i) R is Noetherian.

  (ii) R_0 is Noetherian and R is a finitely generated R_0-algebra.

Proof. (ii) $\Rightarrow$ (i) is a consequence of Hilbert's basis theorem. We prove the other direction.

Assume R is Noetherian. Note that $R_+ = \bigoplus_{n>1} R_n$ is an ideal of R with $R_0 \cong R/R_+$. Thus, R_0 is Noetherian.

As R is Noetherian, R_+ is finitely generated. Using Exercise 6.1.15, we may choose a finite generating set consisting of homogeneous elements, say $\{r_1, \ldots, r_n\}$, where r_i has degree n_i. Let R' be the R_0-subalgebra of R generated by $\{r_i\}_i$. We show by induction that $R_n \subseteq R'$ for all n.

Clearly, $R_0 \subseteq R'$. Fix $n \geqslant 0$ and suppose that $R_k \subseteq R'$ for all $k \leqslant n$. Let $r \in R_{n+1} \subseteq R_+$ be arbitrary. Then, we can write

$$r = \sum \lambda_i r_i.$$

After expanding each λ_i in terms of its homogeneous components and comparing the degree $n+1$ component, we may assume that λ_i is homogeneous of degree $n + 1 - n_i$. Note that $n_i \geqslant 1$ for all i and thus, $n + 1 - n_i \leqslant n$. By induction, $\lambda_i \in R'$. In turn, $r \in R'$.   □

Remark 6.1.30. Note that under the above hypothesis, R need not be a finitely generated R_0-module. Indeed, consider the example of $R = k[X]$ with the usual grading.

Definition 6.1.31. Let M be a filtered R-module, and $I \trianglelefteq R$ an ideal. The filtration $(M_n)_{n \geqslant 0}$ is called an I-filtration if $IM_n \subseteq M_{n+1}$ for all $n \geqslant 0$.
Furthermore, if there exists m such that $IM_n = M_{n+1}$ for all $n \geqslant m$, then the filtration is said to be I-stable.

Example 6.1.32. The I-adic filtration is I-stable.

Proposition 6.1.33. Let M be a finitely generated filtered R-module over a Noetherian ring R with an I-filtration. The following conditions are equivalent.

1. The filtration on M is I-stable.

2. If $R^* = \bigoplus_{n \geqslant 0} I^n$ and $M^* = \bigoplus_{n \geqslant 0} M_n$, the graded R^*-module M^* is finitely generated.

Note that the direct sums above are *external* direct sums. Note that $(M_n)_{n \geqslant 0}$ here is a filtration and not a gradation. The filtration on M being an I-filtration is what lets us define the graded module structure above.

Proof. Set $N_n := M_0 \oplus \cdots \oplus M_n$. Note that each M_i is finitely generated over R and hence, so is each N_n. For $n \geqslant 0$, define the R^*-submodule M_n^* of M^* by

$$M_n^* := M_0 \oplus \cdots \oplus M_n \oplus IM_n \oplus I^2 M_n \oplus \cdots.$$

Since N_n is a finitely generated R-module, we see that M_n^* is a finitely generated R^*-module.

Hence, $M = \bigcup_{n \geqslant 0} M_n^*$ is finitely generated over R^* iff $M^* = M_m^*$ for some m iff $M_{m+k} = I^k M_m$ for some m and all $k \geqslant 1$. The last condition is precisely the definition of $(M_n)_{n \geqslant 0}$ being I-stable.   □

Proposition 6.1.34 (Artin-Rees Lemma)**.** Let M be a filtered R-module with an I-stable filtration. Assume R is Noetherian and M is a finitely generated R-module. Then, the filtration induced by M on a submodule $N \leqslant M$ is also I-stable.

Proof. Recall that the filtration on N is given by $N_n := M \cap N_n$. Define the objects

$$R^* := \bigoplus_n I^n, \ M^* := \bigoplus_n M_n, \ N^* := \bigoplus_n N_n.$$

As R is Noetherian, I is finitely generated. In turn, R^* is a finitely generated R-algebra. By Proposition 6.1.29, it follows that R^* is Noetherian. By Proposition 6.1.33, it follows that M^* is finitely generated. Since R^* is Noetherian, this implies that N^* is also finitely generated. By Proposition 6.1.33 again, the filtration on N is I-stable.   □

Corollary 6.1.35. Let R be a Noetherian ring, $I \trianglelefteq R$ an ideal, and M a finitely generated R-module, and N a submodule of R. Then there exists $m \geqslant 0$ such that

$$I^k(I^m M \cap N) = I^{m+k} M \cap N$$

for all $k \geqslant 1$.

Proof. Apply Artin-Rees Lemma 6.1.34 to the I-adic filtration on M.   □

§§6.2. Completion

Dual to colimits (Section 2.3), one may define the limit of a functor. As before, one may look at poset categories. The reader is encouraged to formulate the definition of a limit in the general setting, by flipping the arrows. For the purpose of our exposition, it suffices to restrict to a particular case that we define below.

Definition 6.2.1. An inverse system of R-modules if a collection of R-modules $(M_n)_{n \geqslant 0}$ and homomorphisms $(\theta_n)_{n \geqslant 1}$, where $\theta_n : M_n \to M_{n-1}$.
If θ_n is surjective for all n, then the system is said to be a surjective system.

The inverse limit of this system is an R-module M together with R-homomorphisms $(f_i)_{i \geqslant 1}$, where $f_i : M \to M_i$ are such that $\theta_{i+1} \circ f_{i+1} = f_i$ for all $i \geqslant 0$, and M is *universal* for this property, i.e., if M' is another R-module with maps $g_i : M' \to M_i$ satisfying $\theta_{i+1} g_{i+1} = g_i$, then there exists a unique R-linear map $\lambda : M' \to M$ with $f_i \lambda = g_i$ for all $i \geqslant 0$.

Example 6.2.2. If we have a filtration

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots,$$

then we have an inverse system $(M/M_n)_{n \geqslant 0}$ with

$$\theta_{n+1} : M/M_{n+1} \to M/M_n$$

being the natural map $x + M_{n+1} \mapsto x + M_n$.

Moreover, this is a *surjective system*.

Proposition 6.2.3. The inverse limit of $((M_n), (\theta_n))$ exists and is unique up to unique isomorphism.

Proof. We only prove existence. The uniqueness follows from the universal properties as usual.

Define $N := \prod_{i \geqslant 0} M_i$ and let $\pi_i : N \to M_i$ denote projection onto the i-th coordinate. Consider the submodule $M \subseteq N$ consisting of coherent sequences, i.e., sequences $(x_i)_{i \geqslant 0} \in N$ satisfying

$$\theta_{i+1}(x_{i+1}) = x_i \quad \text{for all } i \geqslant 0.$$

Define $f_i : M \to N_i$ to be $\pi_i|_M$. Then, $(M, (f_i))$ is the inverse limit. $\square$

The inverse limit is denoted by

$$\varprojlim_n M_n.$$

An element $(x_n)_{n \geqslant 0}$ of the inverse limit may also be written as

$$(\ldots, x_2, x_1, x_0).$$

Example 6.2.4. Let $R = k$ be a field. For $n \geqslant 0$, consider the R-module $M_n := k[X]/(X^n)$. There is a natural map $\theta_{n+1} : M_{n+1} \to M_n$ induced by the quotient map. Note that elements of M_{n+1} have a canonical representative given by a polynomial of

degree at most n. Moreover, θ_{n+1} simply truncates the X^n term. Using this, identify $\varprojlim_n M_n$ as $k[\![X]\!]$.

More generally, consider R to be any ring, fix $k \geqslant 1$, and define $R' := R[X_1, \ldots, X_k]$, $\mathfrak{m} := (X_1, \ldots, X_k)$. If $M_n := R'/\mathfrak{m}^n$, then we have

$$\varprojlim_n M_n \cong R[\![X_1, \ldots, X_k]\!].$$

Definition 6.2.5. Let M be a filtered R-module. The filtration $(M_n)_{n \geqslant 0}$ on M defines a topological group structure on M (recall Section 0.4) for which $(M_n)_{n \geqslant 0}$ is a fundamental system of neighbourhoods of $\{0\}$. This is called the topology induced by the filtration $(M_n)_n$.

Note that R is also now a topological space due to the filtration $(R_n)_{n \geqslant 0}$. For $a, b \in R$, we have

$$(a + R_n)(b + R_n) \subseteq ab + R_n$$

for all $n \geqslant 0$. This implies that multiplication on R is continuous. Furthermore, if $x \in M$, then

$$(a + R_n)(x + M_n) \subseteq ax + M_n.$$

Thus, the scalar multiplication $R \times M \to M$ is also continuous. This means that R is a topological ring and M a topological R-module.

Proposition 6.2.6. Let N be a submodule of the filtered module M. In the topology on M induced by the filtration, we have

$$\overline{N} = \bigcap_{n \geqslant 0} (N + M_n).$$

Proof. Let $x \in M$. $x \notin \overline{N}$ iff there exists some neighbourhood of x not intersecting N iff there exists $n \geqslant 0$ such that $(x + M_n) \cap N = \varnothing$, i.e., $x \notin N + M_n$ for some n. $\square$

Corollary 6.2.7. The topology defined by the filtration is Hausdorff if and only if $\bigcap_{n \geqslant 0} M_n = \{0\}$.

Proof. Use Lemma 0.4.3. $\square$

Recall that in Section 0.4.2, we had defined the completion of an arbitrary topological abelian group using Cauchy sequences. In our case of the topology being defined via

filtrations, we see that the definition of Cauchy sequences can be formulated by using just $(M_n)_n$ instead of an arbitrary neighbourhood U. Moreover, two Cauchy sequences $(x_n)_n$ and $(y_n)_n$ are equivalent iff for each m there exists n_0 such that $x_n - y_n \in M_m$ for all $n \geqslant n_0$.

Note that if $(x_n)_n$ is a Cauchy sequence and $r \in R$, then $(rx_n)_n$ is a Cauchy sequence. (Use the filtered structure.)

Moreover, the equivalence class of this product depends only on the equivalence class of $(x_n)_n$. Thus, $\widehat{M}$ is also an R-module. (So far, we have not defined any topology on $\widehat{M}$.)

We now show the completion can also be obtained as a direct limit.

Proposition 6.2.8. Let M be a filtered R-module with filtration $(M_n)_{n \geqslant 0}$ and the topology induced by this filtration. Then,

$$\widehat{M} \cong \varprojlim_n M/M_n,$$

as R-modules.

Proof. We shall use the construction of $\widetilde{M} := \lim_n M/M_n$ as defined in Proposition 6.2.3 and the construction of $\widehat{M}$ as in Section 0.4.2.

We define a map

$$\alpha : \varprojlim_n M/M_n \to \widehat{M}$$

as follows: Let $y \in \widetilde{M}$ with $y = (y_n)_n$ being a coherent sequence. For each n, choose $x_n \in M$ such that $\overline{x_n} = y_n$. Note that $x_n - x_m \in M_m$ for all $n \geqslant m$ and thus, $(x_n)_n$ is a Cauchy sequence.

Similarly, if we had chosen another sequence $(x'_n)_n$ such that $\overline{x'_n} = y_n$ for all n, then we would have $x'_n - x_n \in M_m$ for all m and all $n \geqslant m$. Thus, the two Cauchy sequences are equivalent and we get a well-defined map

$$\alpha(y) := [(x_n)_n].$$

α is easily seen to be R-linear. We show that α is an isomorphism.

Suppose $y = (y_n)_n \in \ker(\alpha)$. Then, $(x_n)_n$ is equivalent to $(0)_n$, i.e., $x_n \to 0$. Thus, for every m there exists n_0 such that $x_n \in M_m$ for all $n \geqslant n_0$. Thus, we may find $n > m$ such that $x_n \in M_m$. Note that by construction, we have that the image of $x_n + M_n$ under the compositions

$$M/M_n \xrightarrow{\theta_n} \cdots \xrightarrow{\theta_{m+1}} M/M_m$$

is $x_n + M_m$. On the other hand, by the coherence condition, it equals $x_m + M_m$. Thus, $x_m - x_n \in M_m$. As $x_n \in M_m$, we get $x_m \in M_m$. We have shown that $x_m \in M_m$ for all $m \geqslant 0$. Thus, $y = 0$.

To see that α is surjective, given Cauchy sequence $(z_n)_n$ in M, we can inductively pick a subsequence $(x_n)_n$ such that $x_{n+1} - x_n \in M_n$ for all n. If $y_n := x_n + M$, then $y := (y_n)_n$ satisfies $\alpha(y) = [(z_n)_n]$. □

Remark 6.2.9. From this point on, we shall work with topologies induced by filtrations. We shall interchangeably use the description of $\widehat{M}$ in terms of (equivalence classes) of Cauchy sequences and in terms of coherent sequences.

There is a map $M \to \widehat{M}$ given by

$$x \mapsto (x + M_n)_n.$$

Observation 6.2.10. The natural map $\varphi : M \to \widehat{M}$ is injective iff $\bigcap_{n \geqslant 0} M_n = 0$. In turn, this is equivalent to M being Hausdorff (Corollary 6.2.7).

Indeed, $x \in \ker(\varphi)$ iff $x \in M_n$ for all $n \geqslant 0$.

Definition 6.2.11. M is said to be complete if the natural map $M \to \widehat{M}$ is an isomorphism.

Note that in such a case, the kernel must be zero, i.e., $\bigcap_{n \geqslant 0} M_n = 0$, i.e., M is Hausdorff.

Remark 6.2.12. Note that if R is a ring, then $\widehat{R}$ as defined above is an R-module. However, note that $\widehat{R}$ is also quite naturally a ring with multiplication being the natural one (in either interpretation – via Cauchy sequences or coherent sequences – there is a natural product which is indeed well-defined).

Along with the natural map $R \to \widehat{R}$, we see that $\widehat{R}$ is an R-algebra.

Definition 6.2.13. Given inverse systems (M'_n, θ'_n) and (M_n, θ_n), a morphism of inverse systems
$$f : (M'_n)_n \to (M_n)_n$$
is a family of maps $f_n : M'_n \to M_n$ for $n \geqslant 0$ such that the following diagram commutes for all n:

$$
\begin{array}{ccc}
M'_{n+1} & \xrightarrow{f_{n+1}} & M_{n+1} \\
\theta'_{n+1} \downarrow & & \downarrow \theta_{n+1} \\
M'_n & \xrightarrow{f_n} & M_n
\end{array}
$$

A sequence of inverse system morphisms

$$0 \to (M'_n) \xrightarrow{f} (M_n) \xrightarrow{g} (M''_n) \to 0$$

is said to be exact if the corresponding sequence is exact for each n.

Given a morphism as above, one can "take limits on both sides" and get an induced map

$$\varprojlim_n M'_n \to \varprojlim_n M_n$$

defined by

$$(x'_n)_n \mapsto (f_n(x'_n))_n.$$

The diagram commuting ensures that the sequence on the right is coherent.

Proposition 6.2.14. Suppose we have an exact sequence

$$0 \to (A_n) \xrightarrow{f} (B_n) \xrightarrow{g} (C_n) \to 0$$

of inverse systems. Then, the sequence

$$0 \to \varprojlim_n A_n \to \varprojlim_n B_n \to \varprojlim_n C_n$$

is exact. Furthermore, if $(A_n)_n$ is a surjective system, then

$$0 \to \varprojlim_n A_n \to \varprojlim_n B_n \to \varprojlim_n C_n \to 0$$

is exact.

Proof. Let $A := \prod_n A_n$ and define $d^A : A \to A$ by

$$(a_n) \mapsto (a_n - \theta_{n+1}(a_{n+1}))_n.$$

Note that $\ker(d^A) = \varprojlim A_n$. Define B, C, d^B, d^C similarly. We now have a commutative diagram with exact rows as follows

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d^A} & & \downarrow{\scriptstyle d^B} & & \downarrow{\scriptstyle d^C} & & \\
0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0
\end{array}
$$

This gives us an exact sequence

$$0 \to \ker(d^A) \to \ker(d^B) \to \ker(d^C) \to \operatorname{coker}(d^A),$$

as desired. Finally, if $(A_n)_n$ is a surjective system, we need to show that d^A is surjective. But this is simple because we just need to inductively solve

$$x_n - \theta_{n+1}(x_{n+1}) = a_n. \qquad \square$$

Corollary 6.2.15. Let

$$0 \to M' \to M \xrightarrow{p} M'' \to 0$$

be an exact sequence and $(M_n)_n$ a filtration of M with induced filtrations on M' and M''. If completions are taken with respect to these filtrations, then the sequence

$$0 \to \widehat{M'} \to \widehat{M} \to \widehat{M''} \to 0$$

is exact.

Proof. Apply Proposition 6.2.14 to

$$0 \to \frac{M'}{M' \cap M_n} \to \frac{M}{M_n} \to \frac{M''}{p(M_n)} \to 0. \qquad \square$$

Corollary 6.2.16. Given a filtration $(M_n)_n$ on M, $\widehat{M_n}$ can be realised as submodule of $\widehat{M}$ and

$$\widehat{M}/\widehat{M_n} \cong M/M_n. \tag{6.1}$$

Proof. Fix n. Using Corollary 6.2.15 on $M' = M_n$ and $M'' = M/M_n$ shows us that

$$\widehat{M}/\widehat{M_n} \cong \widehat{M''}.$$

On the other hand, note that the filtration on M'' is given as $\left(\frac{M_m + M_n}{M_n}\right)_m$. For $m \geqslant n$, we have $(M_m + M_n)/M_n = 0$. Thus, the topology on M'' is the discrete one and hence, $M'' \cong \widehat{M''}$ (as Cauchy sequences are eventually constant and two Cauchy sequences are equivalent iff they are eventually equal). Thus, we have

$$\widehat{M}/\widehat{M_n} \cong M'' = M/M_n. \qquad \square$$

Note that the identification of $\widehat{M_n}$ as a submodule of $\widehat{M}$ is in the natural way: a Cauchy sequence in M_n remains a Cauchy sequence in M, and this defines a map on the equivalence classes also. The exactness property tells us that if two Cauchy sequences were inequivalent in M_n, then they continue to be so in M. The isomorphism above is the natural one: We have the natural maps $M \to \widehat{M} \to \widehat{M}/\widehat{M_n}$ and the kernel of this composition is M_n.

It is also straightforward to see that $(\widehat{M_n})_n$ defines a filtration on $\widehat{M}$. Thus, $\widehat{M}$ itself can now be regarded as a topological abelian group.

Corollary 6.2.17. Under the filtration $(\widehat{M_n})_n$ of $\widehat{M}$, we have

$$\widehat{\widehat{M}} \cong \widehat{M}.$$

Proof. Take limits in (6.1).   □

 Here is a summary of what we have done:

We started with a filtered ring R **and a filtered** R**-module** M.
Using the filtration $(M_n)_{n \geqslant 0}$**, we can defined a topology on** M**. In particular, this gives a topology on** R **as well.**
We see that R **is a topological ring, and** M **a topological** R**-module.**
Then, we constructed a new R**-module** $\widehat{M}$**, which we called the completion of** $\widehat{M}$**. This could be constructed in two ways:**

1. **equivalence classes of Cauchy sequences in** M,

2. **coherent sequences in** $\prod_{n \geqslant 0} M/M_n$**.**

In either case, we only saw how to get a module (without any topology). Then, we saw that there is a natural filtration on $\widehat{M}$ **given by** $(\widehat{M_n})_{n \geqslant 0}$**.**
This makes $\widehat{M}$ **into a topological** R**-module. One could repeat the same thing again but we saw that** $\widehat{M} \cong \widehat{\widehat{M}}$**. In particular, this shows that** $\widehat{M}$ **is complete, and thus, every Cauchy sequence in** $\widehat{M}$ **converges.**

Observation 6.2.18. Let M be a filtered R-module. Let $(x_n)_{n \geqslant 0}$ be a sequence such that $x_n \in M_n$ for all $n \geqslant 0$. Then,

$$x_0 + x_1 + x_2 + \cdots$$

converges in $\widehat{M}$. (To be precise, we mean the image of x_i under the natural map $M \to \widehat{M}$, which is not an inclusion unless $\bigcap_n M_n = 0$.)

Indeed, for $n \geqslant m$, we have

$$x_m + x_{m+1} + \cdots + x_n \in M_m.$$

Thus, the sequence of partial sums is Cauchy in M and hence has a limit in $\widehat{M}$.

In particular, if we consider R with the I-adic filtration, then we see that

$$1 + a + a^2 + \cdots$$

has a limit in $\widehat{R}$ for any $a \in I$.

Also, note that if $a \in I$, then $a^n \in I^n$ and hence, $\lim_{n \to \infty} a^n = 0$. Thus, taking limits on both sides of

$$(1 - a)(1 + a + \cdots + a^n) = 1 - a^{n+1}$$

shows that $1 + a + a^2 + \cdots$ is the inverse of $1 - a$ in $\widehat{R}$.

We now make some general remarks. Our first aim is to observe a scenario where two different filtrations given the same topology. As a motivational example, the reader may recall that two norms $\| \cdot \|_1, \| \cdot \|_2$ on a real vector space are said to be equivalent if there exists constants $c, C > 0$ such that $c\|x\|_1 \leqslant \|x\|_2 \leqslant C\|x\|_1$ for all vectors x. It is an easy check that equivalent norms induce the same topology.

Definition 6.2.19. Let R be a filtered ring and M be an R-module. Two filtrations $(M_n)_n$ and $(M'_n)_n$ on M are said to be equivalent if there exists an integer $k \geqslant 0$ such that

$$M_{n+k} \subseteq M'_n \quad \text{and} \quad M'_{n+k} \subseteq M_n$$

for all $n \geqslant 0$.

Note that the above is equivalent to asking for the existence of two integers $k_1, k_2 \geqslant 0$ such that

$$M_{n+k_1} \subseteq M'_n \quad \text{and} \quad M'_{n+k_2} \subseteq M_n$$

for all $n \geqslant 0$.

One direction (getting k_1 and k_2 from k) is trivial.
For the other, note that taking $k = \max\{k_1, k_2\}$ does the job since

$$M_{n+k} = M_{n+k-k_1+k_1} \subseteq M'_{n+k-k_1} \subseteq M'_n$$

and similarly, $M'_{n+k} \subseteq M_n$.

Proposition 6.2.20. Equivalent filtrations induce the same topology. Furthermore, the completions with respect to these filtrations are isomorphic.

Proof. Let the notations be as before. We first show that the topologies induced are the same. It suffices to consider open neighbourhoods of 0. Let U be an open neighbourhood of 0 with respect to the $(M_n)_n$-topology. We show that U is open in the $(M'_n)_n$ topology.

Fix $y \in U$. Then U contains $y + M_n$ for some $n \geqslant 0$. Note that

$$y + M'_{n+k} \subseteq y + M_n.$$

As $y + M'_{n+k}$ is open in the (M'_n)-topology and $y \in U$ was arbitrary, we are done.

We now show that the completions are isomorphic. Let

$$M_1 := \varprojlim_n M/M_n \quad \text{and} \quad M_2 := \varprojlim_n M/M'_n.$$

Define $\Phi : M_1 \to M_2$ by

$$(\ldots, x_2 + M_2, x_1 + M_1, x_0 + M_0) \mapsto (\ldots, x_{k+2} + M'_2, x_{k+1} + M'_1, x_k + M'_0).$$

The map above is well-defined since $M_{n+k} \subseteq M'_n$ for all $n \geqslant 0$. Similarly, define $\Psi : M_2 \to M_1$ by

$$(\ldots, x_2 + M'_2, x_1 + M'_1, x_0 + M'_0) \mapsto (\ldots, x_{k+2} + M_2, x_{k+1} + M_1, x_k + M_0).$$

Then, $\Psi \circ \Phi$ is given by

$$(\ldots, x_2 + M_2, x_1 + M_1, x_0 + M_0) \mapsto (\ldots, x_{2k+2} + M_2, x_{2k+1} + M_1, x_{2k} + M_0).$$

Note that since the sequence on the left is a coherent sequence (by definition of the inverse limit), we have $x_{2k+n} + M_n = x_n + M_n$ and thus, the above map is indeed the identity map. Similarly, so is $\Phi \circ \Psi$ and we are done. $\square$

Corollary 6.2.21. Let R be a Noetherian, M a finitely generated R-module, and N a submodule of M. If I is an ideal in R, then the two filtrations on N, viz. $(I^n N)_{n \geqslant 0}$ and $(N \cap I^n M)_{n \geqslant 0}$ are equivalent. Consequently, the completions of N with respect to these topologies are the same.

Proof. Firstly, note that
$$I^n N \subseteq N \cap I^n M$$
for all $n \geqslant 0$.

We must show that there exists k such that
$$N \cap I^{n+k} M \subseteq I^n N.$$

By Corollary 6.1.35, there exists $k \geqslant 0$ such that
$$N \cap I^{n+k} M = I^n (N \cap I^m M) \subseteq I^n N$$
for all $n \geqslant 0$, as desired. $\square$

§§6.3. I-adic filtration

Let R be a ring, M an R-module, and $I \trianglelefteq R$ an ideal of R.

Recall that we have the I-*adic* filtrations $R_n := I^n$ and $M_n := I^n M$ defined on R and M, respectively. With these filtrations, R is a filtered ring and M is a filtered R-module.

Definition 6.3.1. The topology defined on M be the I-adic filtration is called the I-adic topology and the completion is called the I-adic completion.

Example 6.3.2. Let $R = k[X]$ with k a field and $I = (X)$. Then, $\widehat{R} = \varprojlim_n R/(X^n)$. By Example 6.2.4, we see that this is $k[\![X]\!]$.

More generally, the completion of $k[X_1, \ldots, X_k]$ with respect to the $(X_1, \ldots, X_n)$-adic topology is $k[\![X_1, \ldots, X_k]\!]$.

Example 6.3.3. Let $R = \mathbb{Z}$ and $I = (p)$, where $p \geqslant 2$ is a prime. Then, the completion $\widehat{R} = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ is called the ring of p-adic integers.

Let $\widehat{R}$ and $\widehat{M}$ denote the I-adic completions of R and M, respectively. Then, we have a well-defined map $\widehat{R} \times \widehat{M} \to \widehat{M}$ given by

$$[(a_n)_n] \cdot [(x_n)_n] := [(a_n x_n)_n].$$

The above makes $\widehat{M}$ into an $\widehat{R}$-module.

Note that if M and N are R-module and $f : M \to N$ is any R-linear homomorphism, then $f(I^n M) \subseteq I^n f(M)$ for all $n \geqslant 0$. This induces an R-linear map $f_n : M/I^n M \to N/I^n N$ such that

$$
\begin{array}{ccc}
M/I^{n+1}M & \xrightarrow{f_{n+1}} & N/I^{n+1}N \\
\downarrow & & \downarrow \\
M/I^n M & \xrightarrow{\quad f_n \quad} & N/I^n N
\end{array}
$$

commutes for all n.

In other words, f is a morphism of the appropriate inverse systems. As seen before, this induces a map $\widehat{f} : \widehat{M} \to \widehat{N}$.

Proposition 6.3.4. Let R be a Noetherian ring, and $I \trianglelefteq R$ an ideal. Let $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ be an exact sequence of finitely generated R-modules. Then, the I-adic completions form an exact sequence of $\widehat{R}$ modules

$$0 \to \widehat{A} \xrightarrow{\widehat{f}} \widehat{B} \xrightarrow{\widehat{g}} \widehat{C} \to 0.$$

Proof. We wish to use Proposition 6.2.14. First, consider the filtrations on A and C *induced* from that of B. As usual, we may as well assume that f is an inclusion and $C = B/A$ with

g being the canonical quotient map. Then, the induced filtration on A is $(A \cap I^n B)_{n \geqslant 0}$ and that on C is $((A + I^n B)/A)_{n \geqslant 0}$. Let the completions with respect to these filtrations be $\widehat{A}'$ and $\widehat{C}'$. Then, Proposition 6.2.14 tells us that

$$0 \to \widehat{A}' \to \widehat{B} \to \widehat{C}' \to 0$$

is exact.

Now, note that $(A + I^n B)/A$ is equal to $I^n(B/A) = I^n C$. Thus, $\widehat{C} = \widehat{C}'$.
On the other hand, by Corollary 6.2.21, we have $\widehat{A}' \cong \widehat{A}$. Moreover, the isomorphism is such that we have a commutative ladder as

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \widehat{A}' & \longrightarrow & \widehat{B} & \longrightarrow & \widehat{C}' & \longrightarrow & 0 \\
& & \downarrow{\scriptstyle\cong} & & \| & & \| & & \\
0 & \longrightarrow & \widehat{A} & \longrightarrow & \widehat{B} & \longrightarrow & \widehat{C} & \longrightarrow & 0
\end{array}
\;,
$$

which proves the statement. $\qquad\square$

Remark 6.3.5. In the above proof, the Noetherian and finitely generated hypothesis was only required for invoking Artin-Rees. In particular, $\widehat{g}$ being surjective did not require either hypothesis.

Let M be an R-module and I and ideal in R. Recall that we had natural maps $R \to \widehat{R}$ and $M \to \widehat{M}$. This gives us R-linear maps

$$\widehat{R} \otimes_R M \to \widehat{R} \otimes_R \widehat{M} \to \widehat{R} \otimes_{\widehat{R}} \widehat{M} \cong \widehat{M}.$$

Let ϕ_M denote the composition $\widehat{R} \otimes_R M \to \widehat{M}$. On simple tensors, it is given by

$$(a_n + R_n)_n \otimes x \mapsto (a_n x + M_n)_n,$$

where we describing the modules in terms of coherent sequences. (To check their understanding, the reader may quickly reason why the sequence on the right is indeed a coherent sequence.)

Proposition 6.3.6. Let R be a ring, and M a finitely generated R-module. Then, the map $\phi_M : \widehat{R} \otimes_R M \to \widehat{M}$ is surjective. If, further, R is Noetherian, then ϕ_M is an isomorphism.

Proof. Clearly, $\phi_R : \widehat{R} \otimes_R R \to \widehat{R}$ is an isomorphism. Also, the natural maps make the following diagram commute

$$
\begin{array}{ccc}
(\widehat{R} \otimes_R M) \oplus (\widehat{R} \otimes_R N) & \overset{\cong}{\longrightarrow} & \widehat{R} \otimes_R (M \oplus N) \\
{\scriptstyle \phi_M \oplus \phi_N}\downarrow & & \downarrow{\scriptstyle \phi_{M \oplus N}} \\
\widehat{M} \oplus \widehat{N} & \underset{\cong}{\longrightarrow} & \widehat{M \oplus N}
\end{array}
\;.
$$

Thus, ϕ_M is an isomorphism when M is a finite rank free module.

Now, if M is an arbitrary finitely generated R-module, then there is an exact sequence

$$0 \to N \xrightarrow{f} F \xrightarrow{g} M \to 0,$$

where F is free of finite rank. This gives us a commutative diagram as

$$
\begin{array}{ccccccc}
\widehat{R} \otimes_R N & \longrightarrow & \widehat{R} \otimes_R F & \longrightarrow & \widehat{R} \otimes_R M & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \\
0 \longrightarrow \widehat{N} & \underset{\widehat{f}}{\longrightarrow} & \widehat{F} & \underset{\widehat{g}}{\longrightarrow} & \widehat{M} & \longrightarrow & 0
\end{array}
$$

The top row is exact since tensor is right-exact. The proof of Proposition 6.3.4 shows that $\widehat{g}$ is surjective (cf. Remark 6.3.5). Since ϕ_F is an isomorphism, it follows that ϕ_M is surjective.

Assume now that R is Noetherian. Then, Proposition 6.3.4 tells us that the bottom row is exact. Moreover, $\widehat{N}$ is also finitely generated and hence, ϕ_N is surjective. This now implies that ϕ_M is injective (by a diagram chase). □

Recall that an R-module F is said to be flat if $- \otimes_R F$ is an exact functor. Also recall that this functor is always right exact. Thus, flatness is equivalent to showing that whenever $N \xrightarrow{f} M$ is an injection, so is the induced map $N \otimes_R F \xrightarrow{f_*} M \otimes_R F$.
It is relatively simple to show that one may relax the condition to N and M being just finitely generated, i.e., F is flat iff whenever N and M are finitely generated R-modules and $N \xrightarrow{f} M$ is an injection, then so is the induced map $N \otimes_R F \xrightarrow{f_*} M \otimes_R F$.

Thus, the above result then gives us the following.

Corollary 6.3.7. Let R be a Noetherian ring, $I \trianglelefteq R$ an ideal in R. Then, the I-adic completion $\widehat{R}$ is a flat R-algebra.

Corollary 6.3.8. Let R be a Noetherian ring, $I \trianglelefteq R$ an ideal in R, and $\widehat{R}$ the I-adic completion. If $a \in R$ is nonzerodivisor on R, then it is also a nonzerodivisor on $\widehat{R}$.

Proof. Consider the homothety $\mu_a : R \to R$ given by $b \mapsto ab$. Then, the induced map $\widehat{\mu_a} : \widehat{R} \to \widehat{R}$ is multiplication by a. Since a was a nonzerodivisor on R, μ_a was injective and in turn, so is $\widehat{\mu_a}$ and hence, a is a nonzerodivisor on $\widehat{R}$. □

Remark 6.3.9. If R is a domain, it is **not** necessary that $\widehat{R}$ is also a domain.

Proposition 6.3.10. Let R be a Noetherian ring, $I \trianglelefteq R$ an ideal in R, and $\widehat{R}$ the I-adic completion. Then,

1. $\widehat{I} \cong \widehat{R} \otimes_R I \cong \widehat{R}I$,

2. $\widehat{I^n} \cong (\widehat{I})^n$ for all $n \geqslant 0$, i.e., completion and taking powers commute,

3. $I^n/I^{n+1} \cong \widehat{I^n}/\widehat{I^{n+1}}$ for all $n \geqslant 0$,

4. $\widehat{I}$ is contained in the Jacobson radical of $\widehat{R}$.

Proof.

1. Since R is Noetherian, I is finitely generated and

$$\phi_I : \widehat{R} \otimes_R I \to \widehat{I}$$

is an isomorphism (Proposition 6.3.6). Since $\widehat{R}$ is flat, the natural map

$$\widehat{R} \otimes_R I \to \widehat{R} \otimes_R R$$

is an injection with image $\widehat{R}I$.

2. Apply the earlier part to I^n to get

$$\widehat{I^n} \cong \widehat{R}I^n = (\widehat{R}I)^n \cong (\widehat{I})^n.$$

3. We had seen natural isomorphisms $R/I^n \cong \widehat{R}/\widehat{I^n}$ in Corollary 6.2.16. Using the third isomorphism theorem gives us the desired isomorphism.

4. Let $a \in \widehat{I}$. It suffices to show that $1 - ra$ is a unit for any $r \in \widehat{R}$. Note that ra is again an element of $\widehat{I}$ and thus, it suffices to show that $1 - a$ is a unit. As in Observation 6.2.18, we see that

$$1 + a + a^2 + \cdots$$

is the inverse of $1 - a$. $\qquad\square$

Corollary 6.3.11. Let $(R, \mathfrak{m})$ be a Noetherian local ring. Then, the $\mathfrak{m}$-adic completion $\widehat{R}$ is also a local ring with unique maximal ideal $\widehat{\mathfrak{m}}$.

It is also true that $\widehat{R}$ is Noetherian, see Corollary 6.5.5.

Proof. $\widehat{R}/\widehat{\mathfrak{m}} \cong R/\mathfrak{m}$ and thus, $\widehat{\mathfrak{m}}$ is indeed maximal. Furthermore, $\widehat{\mathfrak{m}}$ is contained in the Jacobson radical. Thus, $\widehat{\mathfrak{m}}$ must be equal to the Jacobson radical and be the unique maximal ideal of $\widehat{R}$. $\qquad\square$

Theorem 6.3.12 (Krull's Intersection Theorem). Let R be a Noetherian ring, M be a finitely generated R-module, I an ideal of R, and define $N := \bigcap_{n \geq 0} I^n M$.

If $x \in M$ is annihilated by some element of $1 + I$, then $x \in N$.

Moreover, there exists $a \in I$ such that $(1 + a)N = 0$.

Remark 6.3.13. Note that if $\widehat{M}$ is the I-adic completion of M, then N above is precisely the kernel of the natural map $M \to \widehat{M}$.

Proof. If $a \in I$ and $x \in M$ are such that $(1 - a)x = 0$, then

$$x = ax = a^2 x = a^3 x = \cdots \in I^n M$$

for all $n \geq 0$.

Note that by Artin-Rees Lemma 6.1.34, there exists $n \geq 1$ such that

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

for all $k \geq 0$. In particular, taking $k = 1$ shows that $N \subseteq IN$ and hence, $N = IN$. Thus, there exists some $a \in I$ such that $(1 - a)N = 0$. This finishes the proof. $\qquad\square$

Corollary 6.3.14. Let R be a Noetherian domain, and $I \subsetneq R$ be a proper ideal of R. Then, $\bigcap_{n \geq 0} I^n = 0$.

Proof. I does not contain -1 and thus, $1 + I$ does not contain 0. Thus, every element of $1 + I$ is a nonzerodivisor. $\qquad\square$

Corollary 6.3.15. Let M be a finitely generated module over a Noetherian ring R and let $I \subseteq \mathcal{J}(R)$ be an ideal contained in the Jacobson radical of R. Then, $\bigcap_{n \geq 0} I^n M = 0$, i.e., the I-adic topology on M is Hausdorff.

Proof. Every element of $1 + I$ is a unit. $\qquad\square$

Corollary 6.3.16. Let M be a finitely generated module over a Noetherian local ring $(R, \mathfrak{m})$. Then, the $\mathfrak{m}$-adic topology on M is Hausdorff. In particular, the $\mathfrak{m}$-adic topology on R is Hausdorff.

Algebraically: $\bigcap_{n \geq 0} \mathfrak{m}^n = 0$.

Proof. We have $\mathfrak{m} = \mathcal{J}(R)$. Use Corollary 6.3.15. $\qquad\square$

Corollary 6.3.17. Let R be a Noetherian ring, M be a finitely generated R-module, and $I \subseteq \mathcal{J}(R)$ be an ideal. Every submodule of M is closed in the I-adic topology. In particular, every ideal of R is closed in the I-adic topology.

Proof. Let $N \leqslant M$ be a submodule. By Corollary 6.3.15, M/N is Hausdorff and thus, $\{\bar{0}\} \subseteq M/N$ is closed. Note that the canonical map $\pi : M \to M/N$ is continuous and thus, $N = \pi^{-1}(\{\bar{0}\})$ is closed in M. $\qquad\square$

Example 6.3.18. Let us show that Krull's Intersection Theorem 6.3.12 is not true without the Noetherian hypothesis. Let $R = \mathcal{C}^\infty(\mathbb{R})$ be the ring of infinitely differentiable real-valued functions defined on $\mathbb{R}$. R is a commutative ring under pointwise addition and multiplication.

Consider the ideal I of functions vanishing at 0, i.e., I is the kernel of the ring homomorphism $R \to \mathbb{R}$ given by $f \mapsto f(0)$.

Note that if $g \in 1 + I$, then g is strictly positive on an interval around 0. Thus, if $f \in R$ is annihilated by g, then f vanishes on a neighbourhood of 0. In particular, f defined below is not annihilated by any element of $1 + I$.

$$f(x) := \begin{cases} \exp\left(-\frac{1}{x^2}\right) & x \neq 0, \\ 0 & x = 0. \end{cases}$$

It is an exercise in analysis to check that $f \in R$.

We claim that $f \in \bigcap_{n \geqslant 0} I^n$. By definition, it is clear that $f \in I$ since $f(0) = 0$. For $n \geqslant 1$, define $f_n \in I$ by

$$f_n(x) := \begin{cases} \exp\left(-\frac{1}{nx^2}\right) & x \neq 0, \\ 0 & x = 0. \end{cases}$$

Now, $f = f_n^n \in I^n$, as desired.

§§6.4. An application to Prime Avoidance

We first recall a standard fact from commutative algebra.

Theorem 6.4.1 (Prime Avoidance)**.** Let R be a ring, and $\mathfrak{a} \trianglelefteq R$ an ideal. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be prime ideals of R. If $\mathfrak{a} \subseteq \bigcup_{i=1}^n \mathfrak{p}_i$, then $\mathfrak{a} \subseteq \mathfrak{p}_j$ for some $j \in [n]$.

Proof. The statement is clear for $n = 1$. We prove it for $n \geqslant 2$ by induction.

We prove the contrapositive, i.e., assume that $\mathfrak{a} \not\subseteq \mathfrak{p}_i$ for all i. We construct an element of $\mathfrak{a}$ which is not in the union $\bigcup_{i=1}^n \mathfrak{p}_i$.

By inductive hypothesis, for each $j \in [n]$, we can find an element

$$x_j \in \mathfrak{a} \setminus \bigcup_{i:i\neq j} \mathfrak{p}_i.$$

Then, consider the element

$$x = x_1 \cdots x_{n-1} + x_n.$$

Clearly, $x \in \mathfrak{a}$. We show that x is not in any $\mathfrak{p}_j$.

If $x \in \mathfrak{p}_j$ for some $j \in [n-1]$, then $x_n \in \mathfrak{p}_j$, contrary to construction.
If $x \in \mathfrak{p}_n$, then $x_1 \cdots x_{n-1} \in \mathfrak{p}_n$, contrary to the assumption that $\mathfrak{p}_n$ is prime. $\qquad\square$

Looking at the above proof, one sees that one can actually make a stronger statement.

Porism 6.4.2 (Prime Avoidance refined)**.** Let R be a ring, and $E \subseteq R$ be an additive subgroup of R which is also closed under multiplication.
Let $I_1, \ldots, I_n$ be ideals of R such that I_i is prime for $i \geqslant 3$.
If $E \subseteq \bigcup_{i=1}^n I_i$, then $I \subseteq I_j$ for some $j \in [n]$.

We now wish to prove a version with countably many primes (and not just finitely many) under some more topological hypothesis.

Let R be a ring, and $I \trianglelefteq R$ an ideal. Assume that $\bigcap_{n\geqslant 1} I^n = 0$, i.e., the I-adic topology on R is Hausdorff. Then, one can define a metric on R by

$$d_I(x,y) = \inf\{2^{-n} : x - y \in I^n\}.$$

Note that if $x \neq y$, then the set on the right is finite and we have $d(x,y) > 0$. Clearly, we also have $d(x,x) = 0$ and $d(x,y) = d(y,x)$. Now, if $x,y,z \in R$ satisfy $x - y \in I^n$ and $y - z \in I^m$ for $m \geqslant n$, then we have

$$x - z = (x-y) + (y-z) \in I^n + I^m = I^n.$$

Using the above, we conclude the following.

Proposition 6.4.3. d_I is a metric on R. In fact, d_I is an ultrametric, i.e.,

$$d_I(x,z) \leqslant \max\{d_I(x,y), d_I(y,z)\}$$

for all $x,y,z \in R$.

Notation. For $x \in R$ and $r > 0$, let $B_I(r) := \{x \in R : d_I(0, x) < r\}$.

Fix $n \geqslant 1$. Let r be such that $2^{-(n+1)} < r < 2^{-n}$. Then, $B_I(r)$ contains I^{n+1} as $d_I(0, x) \leqslant 2^{-(n+1)}$ for any $x \in I^{n+1}$. Conversely, if $x \in B_I(r)$, then $d_I(0, x) \leqslant 2^{-(n+1)}$ which implies that $x \in I^{n+1}$. Thus, we have shown that

$$B_I(r) = I^{n+1}.$$

Note that the metric is translation invariant. The r-neighbourhood of x is simply $x + B_I(r)$. This discussion essentially leads to the following.

Proposition 6.4.4. The I-adic and d_I-induced topologies on R coincide.

Before moving on to the promised applications, we recall a theorem from topology.

Theorem 6.4.5 (Baire's Category Theorem). Let X be a complete metric space. Then, X cannot be written as a countable union of closed sets with empty interior.

As usual, $\overline{X_i}$ above denotes the closure of X_i.

Definition 6.4.6. A complete local ring is a local ring $(R, \mathfrak{m})$ which is complete with respect to the $\mathfrak{m}$-adic topology.

Note that in particular, the topology is Hausdorff and thus, our previous discussion of R being a metric space (with the $d_\mathfrak{m}$ metric) applies.

Theorem 6.4.7. Let $(R, \mathfrak{m})$ be a Noetherian local ring. Let $(\mathfrak{p}_i)_{i \geqslant 1}$ be a family of prime ideals of R, $\mathfrak{a}$ an ideal of R, and $r \in R$. Let $r + \mathfrak{a}$ denote the additive coset of $\mathfrak{a}$.

If $r + \mathfrak{a} \subseteq \bigcup_{i \geqslant 1} \mathfrak{p}_i$, then $r + \mathfrak{a} \subseteq \mathfrak{p}_j$ for some $j \geqslant 1$ (and in turn, $rR + \mathfrak{a} \subseteq \mathfrak{p}_j$).

Proof. Note that $\mathfrak{a}$ is closed in R by Corollary 6.3.17 and hence, $r + \mathfrak{a}$ is a complete metric space with

$$r + \mathfrak{a} = \bigcup_{i \geqslant 1} ((r + \mathfrak{a}) \cap \mathfrak{p}_i).$$

Note that each $\mathfrak{p}_i$ is also closed in R and thus, the union on the right is of closed sets. By Baire's Category Theorem 6.4.5, we may fix $j \geqslant 1$ and pick an element c in the interior of $(r + \mathfrak{a}) \cap \mathfrak{p}_j$. (This is interior within $r + \mathfrak{a}$.)

By our preceding discussion, we see that an open ball (in R) around c is of the form $c + \mathfrak{m}^n$ for some $n \geqslant 0$. Thus, there exists $n \geqslant 1$ such that

$$(r + \mathfrak{a}) \cap (c + \mathfrak{m}^n) \subseteq (r + \mathfrak{a}) \cap \mathfrak{p}_j. \tag{6.2}$$

Claim. $\mathfrak{a} \cap \mathfrak{m}^n \subseteq \mathfrak{p}_j$.

Proof of Claim. Let $x \in \mathfrak{a} \cap \mathfrak{m}^n$. Define $y := x + c$.
Note that

$$y = x + c = r + (x + (r - c)) \in r + \mathfrak{a},$$

since $c \in r + \mathfrak{a}$ by construction and $x \in \mathfrak{a}$.

Similarly, $y \in c + \mathfrak{m}^n$ since $x \in \mathfrak{m}^n$.

Thus, by (6.2), it follows that $y \in \mathfrak{p}_j$. $c \in \mathfrak{p}_j$ by construction and thus, $x = y - c \in \mathfrak{p}_j$.   □

As $\mathfrak{p}_j$ is prime, we see that $\mathfrak{a} \cap \mathfrak{m}^n \subseteq \mathfrak{p}_j$ implies that either $\mathfrak{a} \subseteq \mathfrak{p}_j$ or $\mathfrak{m}^n \subseteq \mathfrak{p}_j$.
In the latter case, it follows that $\mathfrak{m} = \mathfrak{p}_j$ and the claim is clear since r cannot be a union (as it is contained in a union of prime ideals) and thus, $rR + \mathfrak{a}$ is a proper ideal and hence, must be contained in the (unique) maximal ideal $\mathfrak{m}$.
In the former case, we have $c \in \mathfrak{p}_j$ and $r - c \in \mathfrak{a} \subseteq \mathfrak{p}_j$, from which is follows that $r \in \mathfrak{p}_j$ as well.   □

The special case of $r = 0$ above gives us the more familiar prime avoidance-esque result.

Corollary 6.4.8. Let R be a complete local ring, $(\mathfrak{p}_i)_{i \geqslant 1}$ be a family of prime ideals of R, and I an ideal of R.

If $\mathfrak{a} \subseteq \bigcup_{i \geqslant 1} \mathfrak{p}_i$, then $\mathfrak{a} \subseteq \mathfrak{p}_j$ for some $j \geqslant 1$.

§§6.5. Associated graded rings

Let R be a ring, M an R-module, and I an ideal in R. Consider the R-adic filtrations on M and R and the corresponding graded module $\mathrm{gr}_I(M)$ over $\mathrm{gr}_I(R)$ (recall Definition 6.1.18 and Definition 6.1.22).
We shall discuss relations between the $\mathrm{gr}_I(R)$-module $\mathrm{gr}_I(M)$ and the R-module M. At times, we do not need to assume the I-adic filtration on M. Rather, just being an I-filtration or an I-stable filtration is sufficient (recall Definition 6.1.31). In such cases, the associated graded module is denoted $\mathrm{gr}(M)$. Note that we still have that M is a filtered module with respect to the I-adic filtration on R.

Proposition 6.5.1. Let R be a Noetherian ring, M a finitely generated R-module, and I an ideal in R. Let $(M_n)_{n \geqslant 0}$ be an I-stable filtration on M. Then,

  (i) $\mathrm{gr}_I(R)$ is Noetherian,

 (ii) $\mathrm{gr}_I(R) \cong \mathrm{gr}_{\widehat{I}}(\widehat{R})$ as graded rings,

(iii) $\mathrm{gr}(M)$ is a finitely generated $\mathrm{gr}_I(R)$-module.

Proof.

(i) Let $I = (a_1, \ldots, a_n)$. Then, the set $\{a_1 + I^2, \ldots, a_n + I^2\} \subseteq I/I^2$ generates $\mathrm{gr}_I(R)$ as an algebra over R/I. Since R/I is Noetherian, the same is true for $\mathrm{gr}_I(R)$ by Proposition 6.1.29.

(ii) Use Proposition 6.3.10 (see the proofs to check that the isomorphisms $I^n/I^{n+1} \cong \widehat{I}^n/\widehat{I}^{n+1}$ are suitably natural).

(iii) Fix m such that $I^r M = M_{m+r}$ for all $r \geqslant 1$. Then, $\mathrm{gr}(M)$ is generated by $\bigoplus_{n=0}^{m} M_n/M_{n+1}$ over $\mathrm{gr}_I(R)$.

Note that each M_n/M_{n+1} is a Noetherian R-module and annihilated by I. Thus, each M_n/M_{n+1} is a finitely generated R/I-module. In turn, $\mathrm{gr}_I(M)$ is a finitely generated $\mathrm{gr}_I(R)$-module. $\square$

Proposition 6.5.2. Let M and N be filtered R-modules, and $\phi : M \to N$ a homomorphism of filtered modules.
Let $\mathrm{gr}(\phi) : \mathrm{gr}(M) \to \mathrm{gr}(N)$ and $\widehat{\phi} : \widehat{M} \to \widehat{N}$ be as usual.
If $\mathrm{gr}(\phi)$ is injective (resp. surjective), then $\widehat{\phi}$ is injective (resp. surjective).

Proof. As ϕ is a filtered homomorphism, we have $\phi(M_n) \subseteq N_n$. Thus, we have a natural commutative ladder as shown below.

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \dfrac{M_n}{M_{n+1}} & \longrightarrow & \dfrac{M}{M_{n+1}} & \longrightarrow & \dfrac{M}{M_n} & \longrightarrow & 0 \\
& & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle \phi_{n+1}} & & \downarrow{\scriptstyle \phi_n} & & \\
0 & \longrightarrow & \dfrac{N_n}{N_{n+1}} & \longrightarrow & \dfrac{N}{N_{n+1}} & \longrightarrow & \dfrac{N}{N_n} & \longrightarrow & 0
\end{array}
$$

This give us an exact sequence

$$\ker(f_n) \to \ker(\phi_{n+1}) \to \ker(\phi_n) \to \mathrm{coker}(f_n) \to \mathrm{coker}(\phi_{n+1}) \to \mathrm{coker}(\phi_n). \qquad (6.3)$$

Suppose that $\mathrm{gr}(\phi)$ is injective (resp. surjective). We first prove by induction that each ϕ_n is injective (resp. surjective). For $n = 0$, we see that ϕ_0 is the 0 map between 0 modules. For $n = 1$, note that $\phi_1 = f_0$. Now, let $n \geqslant 1$. By inductive hypothesis, we have $\ker(\phi_n) = 0$ (resp. $\mathrm{coker}(\phi_n) = 0$). As $\mathrm{gr}(\phi)$ is injective (resp. surjective), we also have that $\ker(f_n) = 0$ (resp. $\mathrm{coker}(f_n) = 0$). Thus, exactness of (6.3) gives us that $\ker(\phi_{n+1}) = 0$ (resp. $\mathrm{coker}(\phi_{n+1}) = 0$).

We have now shown that ϕ_n is injective (resp. surjective) for all n. By Proposition 6.2.14, the theorem now follows. $\square$

Theorem 6.5.3. Let R be a ring, I an ideal in R. Give R the I-adic filtration and let M be a filtered R-module with an I-filtration $(M_n)_{n \geqslant 0}$.
Assume that R is complete in the I-adic topology and $\bigcap_{n \geqslant 0} M_n = 0$. If $gr(M)$ is a finitely generated $gr_I(R)$-module, then M is a finitely generated R-module.

Proof. Consider a finite generating set of $gr(M)$ over $gr_I(R)$ consisting of homogeneous elements, say $\{y_1, \ldots, y_t\}$. Let $n_i := \deg(y_i)$ and choose $x_i \in M_{n_i}$ such that $x_i + M_{n_i+1} = y_i$, for all $i \in [t]$.

Let $F := R^{\oplus t}$, and define the filtration on F by

$$F_n := \{(a_1, \ldots, a_t) : a_i \in I^{n-n_i} \text{ for all } i \in [t]\}$$

for $n \geqslant 0$. (We are using the convention that $I^k = R$ for $k \leqslant 0$.) Under this filtration, the map $\phi : F \to M$ defined by

$$(a_1, \ldots, a_t) \mapsto \sum_{i \in [t]} a_i x_i$$

is a homomorphism of filtered R-modules.

The associated homomorphism $gr(\phi) : gr(F) \to gr(M)$ is surjective as $\{y_i\}_i$ generates $gr(M)$. Thus, by Proposition 6.5.2, we see that $\widehat{\phi} : \widehat{F} \to \widehat{M}$ is surjective. Note that we have the commutative diagram

$$
\begin{array}{ccc}
F & \xrightarrow{\phi} & M \\
\scriptstyle f \downarrow & & \downarrow \scriptstyle g \\
\widehat{F} & \xrightarrow[\widehat{\phi}]{} & \widehat{M}
\end{array}
$$

f is an isomorphism since R is complete and F is a finite direct sum of copies of R. g is injective since $\bigcap_{n \geqslant 0} M_n = 0$. $\widehat{\phi}$ is surjective by the discussion above. In turn, ϕ is surjective and thus, M is finitely generated by $\{x_1, \ldots, x_t\}$. $\square$

Corollary 6.5.4. With the same hypothesis as above, if $gr_I(M)$ is a Noetherian $gr_I(R)$-module, then M is a Noetherian R-module.

Proof. Let $N \leqslant M$ be a submodule. We show that N is finitely generated.

Consider the induced filtration on N given by $N_n := N \cap M_n$. Then, $(N_n)_{n \geqslant 0}$ is also an I-filtration and we have injections $N_n/N_{n+1} \to M_n/M_{n+1}$ for $n \geqslant 0$. In turn, we have an injection $gr(N) \to gr(M)$. Since $gr(M)$ is a Noetherian $gr_I(R)$-module, $gr(N)$ is also a Noetherian $gr_I(R)$-module. By Theorem 6.5.3, N is finitely generated. $\square$

Corollary 6.5.5. Let R be a Noetherian ring and I an ideal in R. Then, the I-adic completion $\widehat{R}$ is Noetherian.

Proof. As R is Noetherian, so is $\mathrm{gr}_I(R)$, by Proposition 6.5.1. Since $\mathrm{gr}_I(R) \cong \mathrm{gr}_{\widehat{I}}(\widehat{R})$, it follows that $\mathrm{gr}_{\widehat{I}}(\widehat{R})$ is Noetherian. Since $\widehat{R}$ is complete, we have $\bigcap_{n \geqslant 0} \widehat{I}^n = 0$. By Corollary 6.5.4, it follows that $\widehat{R}$ is Noetherian. □

Corollary 6.5.6. If R is Noetherian, then the power series ring $R[\![X_1, \ldots, X_n]\!]$ is Noetherian.

Proof. Consider the $(X_1, \ldots, X_n)$-adic completion of the Noetherian ring $R[X_1, \ldots, X_n]$. □

Combing Corollary 6.5.5 and Corollary 6.3.11, we get the following.

Corollary 6.5.7. Let $(R, \mathfrak{m})$ be a Noetherian local ring. Then, the $\mathfrak{m}$-adic completion $\widehat{R}$ is also a local Noetherian ring with unique maximal ideal $\widehat{\mathfrak{m}}$.

Proposition 6.5.8. Let R be a Noetherian ring and $I \trianglelefteq R$ an ideal of R. Suppose that R is Hausdorff in the I-adic topology. (By Corollary 6.3.15, a particular example is if $I \subseteq \mathcal{J}(R)$.) If $\mathrm{gr}_I(R)$ is a domain, then R is a domain.

Proof. Let $a, b \in R \setminus \{0\}$. By hypothesis, $\bigcap_{n \geqslant 0} I^n = 0$. Pick $n, m \geqslant 0$ such that $a \in I^m \setminus I^{m+1}$ and $b \in I^n \setminus I^{n+1}$.
Then, $\overline{a} := a + I^{m+1}$ and $\overline{b} := b + I^{n+1}$ are nonzero elements of $\mathrm{gr}_I(R)$. By assumption, $\overline{a} \cdot \overline{b} \neq 0$ in $\mathrm{gr}_I(R)$. In turn, $ab \neq 0$ in R, as desired. □

Recall that by a complete local ring, we mean a local ring $(R, \mathfrak{m}, k)$ such that R is complete in the $\mathfrak{m}$-adic topology.
Given a polynomial $f = \sum a_i X^i \in R[X]$, we shall use the notation $\overline{f}$ to denote the polynomial $\sum \overline{a_i} X^i \in k[X]$.

Theorem 6.5.9 (Hensel's Lemma). Let $(R, \mathfrak{m}, k)$ be a complete local ring. Let $f \in R[X]$ be a monic polynomial, and $\alpha, \beta \in k[X]$ be relatively prime monic polynomials such that

$$\overline{f} = \alpha\beta$$

in $k[X]$.

Then, there exist monic polynomials $g, h \in R[X]$ such that

1. $f = gh$ in $R[X]$,

2. $\bar{g} = \alpha$ and $\deg(g) = \deg(\alpha)$,

3. $\bar{h} = \beta$ and $\deg(h) = \deg(\beta)$.

In other words, we can lift the factorisation from $k[X]$ to $R[X]$ such that the lifts have the same degree. See Example 6.5.10 to note that the coprime hypothesis cannot be dropped.

Proof. Let the degrees of α and β be a and b, respectively. We shall construct sequences of polynomials $(g_n)_{n \geqslant 1}$ and $(h_n)_{n \geqslant 1}$ in $R[X]$, such that for all $n \geqslant 1$, we have

(P1) $\deg(g_n) \leqslant a$ and $\deg(h_n) \leqslant b$,

(P2) $\overline{g_n} = \alpha$ and $\overline{h_n} = \beta$,

(P3) $f - g_n h_n \in \mathfrak{m}^n R[X]$,

(P4) $g_n - g_{n-1} \in \mathfrak{m}^{n-1} R[X]$ and $h_n - h_{n-1} \in \mathfrak{m}^{n-1} R[X]$.

Assuming the construction for now, let us see how this gives the desired result.
Note that by (P1), each g_n is of the form $c_n^{(0)} + c_n^{(1)} X + \cdots + c_n^{(a)} X^a$.
By (P4), we see that each of $(c_n^{(0)})_{n \geqslant 1}, \ldots, (c_n^{(a)})_{n \geqslant 1}$ is a Cauchy sequence. By taking limits coefficient-wise, we get $g := \lim_n g_n \in R[X]$.
Similarly, we get $h := \lim_n h_n$.

We now show that $f = gh$ by showing that $f - gh \in \mathfrak{m}^n R[X]$ for all $n \geqslant 1$. (By completeness, we have $\bigcap_{n \geqslant 1} \mathfrak{m}^n = 0$.)
Fix $n \geqslant 1$. Since $g_m \to g$ and $h_m \to h$ coefficient-wise, we can fix $m \gg 0$ such that $g_m - g \in \mathfrak{m}^n R[X]$ and $h_m - h \in \mathfrak{m}^n R[X]$. In turn,

$$f - gh = (f - g_m h_m) + g_m (h_m - h) + (g_m - g)h.$$

All the bracketed terms above are in $\mathfrak{m}^n R[X]$, as desired.
Taking $n = 1$ in the above also shows that $\bar{g} = \overline{g_1} = \alpha$ and $\bar{h} = \beta$. Since $\deg(g) \leqslant a$ and $\deg(h) \leqslant b$ but $\deg(g) + \deg(h) = \deg(f) = a + b$, it follows that $\deg(g) = \deg(\alpha)$ and $\deg(h) = \deg(\beta)$.
Lastly, by f being monic, we see that the leading coefficients of g and h are inverses of each other. Since α is monic, the coefficients are of the form $(1 + a)$ and $(1 + a)^{-1}$ for $a \in \mathfrak{m}$. By appropriate scaling, we may assume that g and h are monic and still continue to have $\bar{g} = \alpha$ and $\bar{h} = \beta$. Thus, we have the desired lifts.

We now simply have to construct the sequences with the above desired properties. We define these sequences inductively.

$n = 1$: Pick coefficient-wise lifts g_1 and h_1 of α and β, respectively. (P1) and (P2) are satisfied trivially and (P4) is not to be checked. Moreover, $\overline{f - g_1 h_1} = \alpha\beta - \alpha\beta = 0$ and thus, $f - g_1 h_1 \in \mathfrak{m} R[X]$, satisfying (P3).

Assume now that $n \geqslant 1$ and that g_n and h_n have been constructed satisfying (P1) - (P4). Let $d := a + b = \deg(f)$. Then, we can write

$$f - g_n h_n = \sum_{i=0}^{d} \lambda_i X^i$$

for $\lambda_i \in \mathfrak{m}^n$.

Since α and β are relatively prime, for each $i \in [d]$, we can find polynomials $u_i, v_i \in R[X]$ of degrees at most b and a respectively, such that

$$X^i = \overline{u_i}\alpha + \overline{v_i}\beta$$

in $k[X]$. Since $\alpha = \overline{g_n}$ and $\beta = \overline{h_n}$, we get

$$X^i - u_i g_n - v_i h_n \in \mathfrak{m}R[X].$$

Define

$$g_{n+1} := g_n + \sum_i \lambda_i v_i,$$

$$h_{n+1} := h_n + \sum_i \lambda_i u_i.$$

Clearly, we have $\deg(g_{n+1}) \leqslant a$ and $\deg(h_{n+1}) \leqslant b$. As the λ_i are all in $\mathfrak{m}^n$, we see that (P2) and (P4) are also satisfied (for $n + 1$). To check (P3), note that

$$f - g_{n+1}h_{n+1} = f - (g_n + \sum_i \lambda_i v_i)(h_n + \sum_i \lambda_i u_i)$$

$$= f - g_n h_n - g_n \sum_i \lambda_i u_i - h_n \sum_i \lambda_i v_i - \sum_{i,j} \lambda_i \lambda_j v_i u_j$$

$$= \sum_i \lambda_i X^i - g_n \sum_i \lambda_i u_i - h_n \sum_i \lambda_i v_i - \sum_{i,j} \lambda_i \lambda_j v_i u_j$$

$$= \sum_i \lambda_i (X^i - g_n v_i - h_n u_i) - \sum_{i,j} \lambda_i \lambda_j v_i u_j.$$

Each term above is in $\mathfrak{m}^{n+1}R[X]$, as desired. $\qquad \square$

Example 6.5.10. We now show that the hypothesis of α and β being coprime in Hensel's Lemma 6.5.9 is not unnecessary.

Consider the local ring $R = \mathbb{Q}[\![t]\!]$ with maximal ideal $\mathfrak{m} = (t)$ and residue field $k = \mathbb{Q}$. Note that R is indeed complete in the $\mathfrak{m}$-adic topology.

Consider $f = X^2 - t \in R[X]$. Then, $\bar{f} = X^2 = X \cdot X$ in $\mathbb{Q}[X]$. Now, if there exist g and h as in the theorem, then f has a root in R. But there is no power series $a \in \mathbb{Q}[\![t]\!]$ such that $a^2 = t$.

Corollary 6.5.11. Let $(R, \mathfrak{m}, k)$ be a complete local ring. Let $f \in R[X]$ be a monic polynomial such that $\bar{f} \in k[X]$ has a simple root $\xi \in k$. Then, f has a simple root $a \in R$ such that $\bar{a} = \xi$.

Proof. By hypothesis, we can factorise $\bar{f}$ as $(X - \xi)\beta(X)$. ξ being a simple root tells us that $X - \xi$ and $\beta(X)$ are coprime. Using Hensel's Lemma 6.5.9 gives us the desired result. $\quad\square$

Corollary 6.5.12 (Implicit Function Theorem)**.** Let k be a field, and $R = k[\![X_1, \ldots, X_t]\!] = k[\![\mathbf{X}]\!]$ be the power series ring in t variables over k. Let

$$f(z) = z^n + a_1(\mathbf{X})z^{n-1} + \cdots + a_n(\mathbf{X}) \in R[z]$$

be a monic polynomial such that

$$z^n + a_1(\mathbf{0})z^{n-1} + \cdots + a_n(\mathbf{0}) \in k[z]$$

has a simple root $\xi \in k$. Then, there exists some $g(\mathbf{X}) \in R$ with $g(\mathbf{0}) = \xi$ and $f(g(\mathbf{X})) = 0$.

Proof. Simply apply Corollary 6.5.11 to the complete local ring $(k[\![\mathbf{X}]\!], (\mathbf{X}), k)$. (Note that the image of $a(\mathbf{X}) \in k[\![\mathbf{X}]\!]$ under the quotient map $R \to k$ is precisely $a(\mathbf{0})$.) $\quad\square$

Corollary 6.5.13. Let $R = k[\![X_1, \ldots, X_t]\!]$ be a power series ring over a field, and d an integer relatively prime to $\mathrm{char}(k)$. Let $a(\mathbf{X}) \in R$ be such that $a(\mathbf{0})$ is nonzero and is a d-th power in k. Then, $a(\mathbf{X})$ is a d-th power in R.

Proof. Consider $f(z) = z^d - a(\mathbf{X})$ and use the earlier corollary. Note that $\bar{f}(z) = z^d - a(\mathbf{0})$ has a root by hypothesis. The root is simple by the derivative test (here is where we use that $\gcd(d, \mathrm{char}(k)) = 1$ and $a(\mathbf{0}) \neq 0$). $\quad\square$

Example 6.5.14. Let us look at a concrete example of the previous corollary. Let k be a field of characteristic different from 2. Then, $a(X) = 1 + X \in k[\![X]\!]$ and $d = 2$ satisfy the hypothesis. Thus, $\sqrt{1 + X}$ makes sense as a power series. More precisely, there exists a power series $b \in k[\![X]\!]$ such that $b^2 = 1 + X$.