Mathematics Diary

Contents

1	2023	1
	1.1 12/20/2022	
	1.2 12/21/2023 - Heights of Ideals	2
2	2024	2
	2.1 4/22/2024	5
	2.2 5/2/2024	
	2.3 5/20/2024	
	2.4 5/21/2024	
	2.5 5/29/2024	7
	2.6 6/15/2024	7

1 2023

1.1 12/20/2022

Lemma 1.1. Let (R, \mathfrak{m}, \Bbbk) be a local noetherian ring, let $J \subseteq I \subseteq \mathfrak{m}$ be ideals of R. Let E be the minimal free resolution of R/J over R, let F be the minimal free resolution of R/I over R, and let $\varphi \colon E \to F$ be a comparison map which lifts the canonical surjective map $R/J \to R/I$. Assume both $\varphi \colon E \to F$ and $\overline{\varphi} \colon E_{\Bbbk} := E \otimes_R \Bbbk \to F \otimes_R \Bbbk := F_{\Bbbk}$ are injective. Then $\Sigma(F/E)$ is the minimal free resolution of I/J over R.

Proof. Assume both $\varphi \colon E \to F$ and $\overline{\varphi} \colon E_{\mathbb{k}} := E \otimes_R \mathbb{k} \to F \otimes_R \mathbb{k} := F_{\mathbb{k}}$ are injective. Since $\varphi \colon E \to F$ is injective, we have a short exact sequence of R-complexes

$$0 \longrightarrow E \stackrel{\varphi}{\longrightarrow} F \longrightarrow F/E \longrightarrow 0 \tag{1}$$

taking homology gives us a long exact sequence

$$\cdots \longrightarrow H_{i+1}(F/E)$$

$$\downarrow H_i(E) \longrightarrow H_i(F) \longrightarrow H_i(F/E)$$

$$\downarrow H_{i-1}(E) \longrightarrow \cdots$$

Since E and F are resolutions we conclude that $H_i(F/E) = 0$ for all $i \neq 1$. Since $R/J \rightarrow R/I$ is surjective we conclude that $H_1(F/E) = I/J$. To see that F/E is free, note that tensoring the short exact sequence of graded R-modules (1) with \mathbb{k} over R gives us the long exact sequence in homology

Since E and F are free R-modules we conclude that $\operatorname{Tor}_i(F/E, \mathbb{k}) = 0$ for all $i \geq 1$. Since $\overline{\varphi} \colon E \otimes_R \mathbb{k} \to F \otimes_R \mathbb{k}$ is injective we conclude that $\operatorname{Tor}_1(F/E, \mathbb{k}) = 0$. In particular, F/E must be free. Finally, F/E is minimal since the differential d on F induces a minimal differential on F/E (i.e. $\operatorname{d}(F/E) \subseteq \mathfrak{m}(F/E)$).

Remark 1. Under the assumptions of Lemma (1.1), we see that for any R-module M connecting maps

$$\operatorname{Tor}_{i+1}^R(R/I,M) \to \operatorname{Tor}_i^R(I/J,M)$$
 and $\operatorname{Ext}_R^i(I/J,M) \to \operatorname{Ext}_R^{i+1}(R/I,M)$

are represented by the chain maps

$$F \otimes_R M \to F/E \otimes_R M$$
 and $\operatorname{Hom}_R^{\star}(F/E, M) \to \operatorname{Hom}_R^{\star}(F, M)$

respectively.

Remark 2. Note that under the assumptions we are working with, if $\overline{\varphi}$: $E_{\mathbb{k}} \to F_{\mathbb{k}}$ is injective, then already φ : $E \to F$ is injective. The converse need not hold.

1.2 12/21/2023 - Heights of Ideals

Let R be a commutative ring and let \mathfrak{p} be an ideal of R. Recall the **height** of \mathfrak{p} is defined to be the supremum of lengths of chains of primes which descend from \mathfrak{p} :

$$\mathsf{ht}\,\mathfrak{p}=\mathsf{sup}\{c\in\mathbb{N}\mid\mathfrak{p}=\mathfrak{p}_0\supset\mathfrak{p}_1\supset\cdots\supset\mathfrak{p}_c\}.$$

When R is Noetherian, then Krull's principal ideal theorem states that there exists an ideal $\langle x \rangle = \langle x_1, \dots, x_c \rangle \subseteq \mathfrak{p}$ where $c = \operatorname{ht} \mathfrak{p}$ such that $\sqrt{\langle x \rangle} = \mathfrak{p}$, and that if $\langle y \rangle = \langle y_1, \dots, y_m \rangle$ is another ideal such that $\sqrt{\langle y \rangle} = \mathfrak{p}$, then we must have $c \leq m$. If I is an ideal of R, then the **height** of I is defined to be the infimum of the heights of all primes which contain I:

$$ht I = \inf\{ht \mathfrak{p} \mid \mathfrak{p} \supset I\}.$$

Lemma 1.2. Let I_1 and I_2 be ideals of R. Set $c = ht(I_1 \cap I_2)$, set $c_1 = ht I_1$, and set $c_2 = ht I_2$.

- 1. If $I_1 \subseteq I_2$, then $c_1 \le c_2$.
- 2. We have $c = \min\{c_1, c_2\}$.

Proof. 1. Let \mathfrak{p} be a prime which contains I_2 whose height is minimal among all heights of primes which contain I_2 . Since $I_1 \subseteq I_2$, we see that $I_1 \subseteq \mathfrak{p}$ also. In particular, it follows that $c_1 \leq c_2$.

2. Note that $I_1 \cap I_2 \subseteq I_1$ implies $c \le c_1$. Similarly, $I_1 \cap I_2 \subseteq I_2$ implies $c \le c_2$. It follows that $c \le \min\{c_1, c_2\}$. Conversely, let \mathfrak{p} be a prime which contains $I_1 \cap I_2$ whose height is minimal among all heights of primes which contain $I_1 \cap I_2$. Then $\mathfrak{p} \supseteq I_1 \cap I_2$ implies either $\mathfrak{p} \supseteq I_1$ or $\mathfrak{p} \supseteq I_2$ since \mathfrak{p} is a prime. In particular it follows that either $c \ge c_1$ or $c \ge c_2$ or equivalently $c \ge \min\{c_1, c_2\}$.

2 2024

$$1/20/2024 - V(Ann M) = V(Ann(0:_M x))$$

Lemma 2.1. Let R be a commutative ring, let M be an R-module, and let $x \in R$. Then

$$V(Ann(0:_M x)) = V(Ann(0:_M x^2)).$$

Proof. Note that $0 :_M x \subseteq 0 :_M x^2$ implies $Ann(0 :_M x^2) \supseteq Ann(0 :_M x)$ which implies $V(Ann(0 :_M x^2)) \subseteq V(Ann(0 :_M x))$. For the reverse inclusion, suppose $\mathfrak p$ is a prime ideal of R which contains $Ann(0 :_M x^2)$ and let $r \in Ann(0 :_M x)$. We claim that $r^2 \in Ann(0 :_M x^2)$. Indeed, if $u \in 0 :_M x^2$, then

$$x^{2}u = 0 \implies xu \in 0:_{M} x$$

$$\implies rxu = 0$$

$$\implies ru \in 0:_{M} x$$

$$\implies r^{2}u = 0.$$

Since u was arbitrary, we see that $r^2 \in \text{Ann}(0:_M x^2) \subseteq \mathfrak{p}$. However this implies $r \in \mathfrak{p}$ since \mathfrak{p} is a prime. Since r was arbitrary, we see that $\text{Ann}(0:_M x) \subseteq \mathfrak{p}$.

Corollary 1. Let R be a commutative ring and let M be a finitely generated R-module. Assume that $x \in R$ acts nilpotently on M. Then

$$V(Ann(M)) = V(Ann(0:_M x)).$$

Proof. Since M is finitely generated, there exists an $n \in \mathbb{N}$ such that $M = 0 :_M x^n$. A straightforward induction on (??) gives us

$$V(Ann(M)) = V(Ann(0:_M x^n)) = V(Ann(0:_M x)).$$

1/21/2024 Some subschemes of \mathbb{P}^3

Let $R = \mathbb{k}[x, y, z, w]$. We consider three cyclic R-algebras, namely $A = R/f = R/\langle f_1, f_2, f_3 \rangle$, $B = R/g = R/\langle g_1, g_2, g_3 \rangle$, and $C = R/h = R/\langle h_1, h_2, h_3 \rangle$ where

$$f_1 = xy - zw$$
 $g_1 = xz - y^2$ $h_1 = xz - y^2$
 $f_2 = xz - yw$ $g_2 = yw - z^2$ $h_2 = x^3 - yzw$
 $f_3 = xw - yz$ $g_3 = xw - yz$ $h_3 = x^2y - z^2w$

We want a geometric picture in mind when thinking of these rings, so let $X = \operatorname{Proj} A$, $Y = \operatorname{Proj} B$, and $Z = \operatorname{Proj} C$. First let us consider X. We can see that $X(\Bbbk)$ consists of 8 distinct points in $\mathbb{P}^3(\Bbbk)$ by calculating an irreducible primary decomposition for $\langle f \rangle$. Indeed, an irredundant primary decomposition for $\langle f \rangle$ is given by $\langle f \rangle = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_8$ where

$$\mathfrak{p}_{1} = \langle y, z, w \rangle \qquad \mathfrak{p}_{5} = \langle x + y, y + z, z + w \rangle \\
\mathfrak{p}_{2} = \langle x, z, w \rangle \qquad \mathfrak{p}_{6} = \langle x + y, y - z, z + w \rangle \\
\mathfrak{p}_{3} = \langle x, y, w \rangle \qquad \mathfrak{p}_{7} = \langle x + y, y - z, z - w \rangle \\
\mathfrak{p}_{4} = \langle x, y, z \rangle \qquad \mathfrak{p}_{8} = \langle x - y, y - z, z - w \rangle.$$

These primes correspond to the points

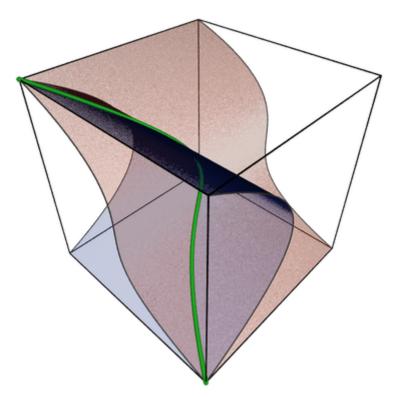
$$egin{aligned} p_1 &= [1:0:0:0] & p_5 &= [-1:1:-1:1] \ p_2 &= [0:1:0:0] & p_6 &= [1:-1:-1:1] \ p_3 &= [0:0:1:0] & p_7 &= [-1:1:1:1] \ p_4 &= [0:0:0:1] & p_8 &= [1:1:1:1] \end{aligned}$$

in $\mathbb{P}^3(\mathbb{k})$. Note that p_1, \ldots, p_8 are in linearly general position since the size 4 minors of the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & -1 & 1 & -1 & 1 \\ 0 & 1 & 0 & 0 & 1 & -1 & 1 & 1 \\ 0 & 0 & 1 & 0 & -1 & -1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

are all nonzero. In other words, viewing p_1, \ldots, p_8 as vectors in \mathbb{k}^4 , every subset of $\{p_1, \ldots, p_8\}$ of size 4 is linearly independent. The Betti diagram of A over R is given by

Next we consider Y. In fact, Y is the twisted cubic. When $\mathbb{k} = \mathbb{R}$, we can visualize $Y(\mathbb{k})$ as below:



In particular, $Y(\mathbb{k})$ is the image of the map $\mathbb{P}^1(\mathbb{k}) \to \mathbb{P}^3(\mathbb{k})$ given by $[s:t] \mapsto [s^3:s^2t:st^2:t^3]$. Note that $\langle g \rangle$ is a prime of height 2 and so $\langle g \rangle$ can be generated up to radical by two homogeneous polynomials. In particular, we have $\langle g \rangle = \sqrt{\langle g_1, g_4 \rangle}$ where $g_4 = zg_2 - wg_3$. However $\langle g \rangle$ itself cannot be generated by only two polynomials; a minimum of three polynomials are needed. We can see this in Betti diagram of B over B:

In particular, the Hilbert-Poincare series of *B* over *R* is given by

$$P(t) = \frac{1 - 3t^2 + 2t^3}{(1 - t)^4} = \frac{1 + 2t}{(1 - t)^2} = 1 + 4t + 7t^2 + 10t^3 + 13t^4 + \cdots$$

Thus Y is the set-theoretic complete intersection of $V(g_1)$ and $V(g_4)$ however it is not a scheme-theoretic or ideal-theoretic complete intersection. Note also that $\langle g \rangle$ corresponds to the ideal of size 2 minors of the matrix $\binom{x}{y} \frac{y}{z} \frac{z}{w}$. Up to linear automorphism, the twisted cubic is the only irreducible curve of degree 3 not contained in a plane. Furthermore, any 6 points in linearly general position in $\mathbb{P}^3(\mathbb{k})$ lie on a unique twisted cubic. However for a twisted cubic to pass through 7 points, the seventh must lie on the twisted cubic determined by the first 6. Consequently one can show that if W is a set of 7 points in linearly general position in $\mathbb{P}^3(\mathbb{k})$, then there are only two distinct Betti diagrams possible for the homogeneous coordinate ring of W, namely

In the first case, the points do not lie on any curve of degree 3. In the second case, the ideal *J* generated by the quadrics containing *W* is the ideal of the unique curve of degree 3 containing *W*, which is irreducible. Finally, let us write down the minimal free resolution of *B* over *R*:

$$R(-3)^{2} \xrightarrow{\begin{pmatrix} w & z \\ y & x \\ -z & -y \end{pmatrix}} R(-2)^{3} \xrightarrow{\left(xz-y^{2} & yw-z^{2} & xw-yz\right)} R \longrightarrow 0$$

Now we consider Z. The Betti diagram of C over R is given by

In particular, the Hilbert-Poincare series of *C* over *R* is given by

$$P(t) = \frac{1 - t^2 - 2t^3 + 2t^4}{(1 - t)^4} = \frac{1 + 2t + 2t^2}{(1 - t)^2} = 1 + 4t + 9t^2 + 14t^3 + 19t^4 + \cdots$$

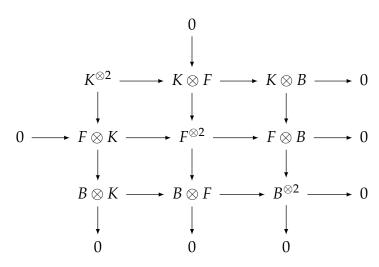
In particular, *Z* is an irreducible curve of degree 5 in $\mathbb{P}^3(\mathbb{k})$.

2.1 4/22/2024

Let A be a commutative ring and let B be an A-algebra which is finite as an A-module. Then there exists a surjection F woheadrightarrow B of A-modules where $F = A^{n+1}$ where we assume $n \ge 0$ is minimal. We are interested in the question as to whether one can lift the multiplication on B to a multiplication on F. Let K be the kernel of the map F woheadrightarrow B. In what follows, all tensors products are taken over A.

Lemma 2.2. The kernel of the map $F^{\otimes 2} \to B^{\otimes 2}$ is given by $K \otimes F + F \otimes K$.

Proof. This is easily checked via a diagram chase in the diagram below which is exact everywhere and in all directions:



Since $F^{\otimes 2}$ is free (hence projective), we can lift the composite map $F^{\otimes 2} \to B^{\otimes 2} \twoheadrightarrow B$ with respect to the map $F \twoheadrightarrow B$ to obtain an A-linear map $\mu \colon F^{\otimes 2} \to F$. Assume that A is a local noetherian ring. In this case, there exists a minimal generating set of B as an A-module of the form $\{b_0, b_1, \ldots, b_n\}$ where $b_0 = 1$. Let $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_n$ be a basis for F as a free A-module and let $F \twoheadrightarrow B$ be the A-linear map defined by $\varepsilon_i \mapsto b_i$ for all i. For each i, j, we have

$$b_i b_j = \sum_k a_{ij}^k b_k$$

where the $a_{ij}^k \in A$ need not be unique. Since the multiplication on B is unital, we can choose the a_{ij}^k such that

$$a_{j0}^k = a_{0j}^k = \begin{cases} 1 & \text{if } j = k \\ 0 & \text{else} \end{cases}$$

Furthermore, since the multiplication on B is commutative, we can also choose the a_{ij}^k such $a_{ij}^k = a_{ji}^k$. With these choices of a_{ij}^k in mind, we can define a commutative and unital multiplication μ on F which lifts the multiplication on B by

$$\varepsilon_i \varepsilon_j := \sum_k a_{ij}^k \varepsilon_k.$$

Note that this multiplication need not be associative. Indeed, since the multiplication on *B* is associative, we have

$$\begin{aligned} [b_i, b_j, b_k] &= (b_i b_j) b_k - b_i (b_j b_k) \\ &= \sum_l (a_{ij}^l b_l b_k - a_{jk}^l b_i b_l) \\ &= \sum_{l,m} (a_{ij}^l a_{lk}^m - a_{jk}^l a_{il}^m) b_m. \end{aligned}$$

However this need not imply that $a_{ij}^l a_{lk}^m - a_{jk}^l a_{ik}^m = 0$ for all i, j, k, l, m (which is what we'd need in order for $[\varepsilon_i, \varepsilon_j, \varepsilon_k] = 0$).

2.2 5/2/2024

Let *R* be a noetherian ring, let *I* be an ideal of *R*, and let $r, r' \in R$. We have an *R*-linear map

$$\varphi: \langle I, r \rangle : r' \rightarrow (\langle I, r' \rangle : r) / (I : r)$$

defined as follows: if $a \in \langle I, r \rangle$: r', then we have ar' = br + x for some $b \in R$ and $x \in I$. The map is defined by sending a to the class of b in the quotient. It is straightforward to check that this is well-defined and surjective. Note if $b \in I$: r, then $ar' \in I$: r'. In particular, the kernel of φ is I: r'. Thus we've established an isomorphism

$$(\langle I, r \rangle : r') \rangle / (I : r') \cong (\langle I, r' \rangle : r) \rangle / (I : r). \tag{2}$$

In particular, if I: r' = I: r, then we must have $\langle I, r \rangle : r' = \langle I, r' \rangle : r$. Now assume that $I: r = \mathfrak{p} = \langle I, r \rangle : r'$. Then (2) implies

$$\mathfrak{p}/(I:r')\cong (\langle I,r'\rangle:r)/\mathfrak{p}.$$

Example 2.1. Let $R = \mathbb{k}[x, y, z, w]$, let $I = \langle x^2, w^2, zw, xy, yz \rangle$, let r = yw, and let r' = y. Then we have

$$I: r = \langle x, z, w \rangle$$
 $\langle I, r' \rangle : r = R$
 $I: r' = \langle x, z, w^2 \rangle$ $\langle I, r \rangle : r' = \langle x, z, w \rangle$.

Now observe that $\langle I:r,r'\rangle\subseteq\langle I,r'\rangle:r$. Indeed, if $a\in\langle I:r,r'\rangle$, then we can express it as a=b+cr' where $b\in I:r$ and $c\in R$. In particular, this means that $ar=br+cr'r\in\langle I,r'\rangle$, and hence $a\in\langle I,r'\rangle:r$.

2.3 5/20/2024

Let $A = \mathbb{k}[x] = \mathbb{k}[x_1, \dots, x_n]$, let $B = \mathbb{k}[y] = \mathbb{k}[y_1, \dots, y_m]$, and let $\varphi \colon A \to B$ be a \mathbb{k} -algebra homomorphism. Next let $Y = \operatorname{Spec} B$, let $X = \operatorname{Spec} A$, and let $f \colon Y \to X$ be given by $f(\mathfrak{q}) := \varphi^{-1}(\mathfrak{q})$ for all $\mathfrak{q} \in Y$. We want to describe how f acts all maximal ideals of B of the form $\mathfrak{n}_q = \langle y_1 - q_1, \dots, y_m - q_m \rangle$ where $q \in Y(\mathbb{k})$. To this end, for each $1 \le j \le n$ let $f_i = \varphi(x_i)$. Then we have

$$\varphi^{-1}(\mathfrak{n}_q)=\mathfrak{m}_p$$

where $p = (f_1(q), \dots, f_n(q))$ and where $\mathfrak{m}_p = \langle x_1 - p_1, \dots, x_n - p_n \rangle$. Indeed, observe that

$$\varphi(\mathfrak{m}_{p}) = \langle \varphi(x_{1}) - p_{1}, \dots, \varphi(x_{n}) - p_{n} \rangle$$

$$= \langle f_{1} - f_{1}(\mathbf{q}), \dots, f_{n} - f_{n}(\mathbf{q}) \rangle$$

$$\subseteq \mathfrak{n}_{q}.$$

2.4 5/21/2024

Let R be a commutative ring, let M_1 and M_2 be R-modules, and set $T = \operatorname{Tor}^R(M_1, M_2)$. We can turn T into an R-complex as follows: choose projective resolutions F^1 of M_1 and F^2 of M_2 over R. Then $d \otimes 1$: $F^1 \otimes_R F^2 \to F^1 \otimes_R F^2$ is a chain map of degree -1, thus it induces a map in homology $d \otimes 1$: $T \to T$. Furthermore $(d \otimes 1)^2 = 0$ and so $d \otimes 1$ gives T an R-complex structure. There are map γ_i^{31} : $T_i^{31} \to T_{i-1}^{31}$ defined to be the composite

$$T_i^{31} \to T_i^{32} \to T_{i-1}^{12} \to T_{i-1}^{13} = T_{i-1}^{31}.$$

Similarly, we define $\gamma_i^{32} \colon T_i^{32} \to T_{i-1}^{32}$ to be the composite

$$T_i^{32} \to T_{i-1}^{12} \to T_{i-1}^{13} \to T_{i-1}^{23} = T_{i-1}^{32},$$

and we define $\gamma_i^{21} : T_i^{21} \to T_{i-1}^{21}$ to be the composite

$$T_i^{21} \to T_i^{31} \to T_i^{32} \to T_{i-1}^{12} = T_{i-1}^{21}$$

Actually I just realized these are all just the zero map.

2.5 5/29/2024

Proposition 2.1. Let R be a regular local ring, let I be an ideal of R, let F be the minimal free resolution of R/I over R, and let $S = S_R(F)$ be the symmetric DG algebra of F over R. There exists a surjective chain map $\pi: S \to F$ which splits the inclusion map $F \hookrightarrow S$.

Proof. It suffices to show that $\operatorname{Ext}_R^1(S/F,F)=0$. Note that the underlying graded R-module of S/F is just $S^{\geq 2}$. In particular, S/F is semi-projective, thus $\operatorname{Hom}_R^{\star}(S/F,-)$ preserves quasi-isomorphisms. It follows that

$$\operatorname{Ext}_{R}^{1}(S/F, F) = \operatorname{Ext}_{R}^{1}(S/F, R/I) = 0,$$

where the last part follows from the fact that R/I sits in homological degree 0 but $(S/F)_i = 0$ for all $i \le 1$.

Remark 3. Note that giving a surjective chain map $\pi: S \to F$ which splits the inclusion map is equivalent to giving chain maps $\pi^n: F^{\otimes n} \to F$ for each $n \geq 2$ such that each π^n is strictly commutative and such that for all $1 \leq i \leq n$ and for all $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n \in F_+$ we have

$$\pi^n(a_1,\ldots,a_{i-1},1,a_i,\ldots,a_n)=\pi^{n-1}(a_1,\ldots,a_{i-1},a_i,\ldots,a_n).$$

For instance, if a_1, a_2, a_3 are homogeneous elements in F with $|a_1| = 1$ and $|a_2|, |a_3| \ge 2$, then we have

$$d\pi^{3}(a_{1}, a_{2}, a_{3}) = r_{1}\pi^{2}(a_{2}, a_{3}) - \pi^{3}(a_{1}, da_{2}, a_{3}) + \pi^{3}(a_{1}, a_{2}, da_{3}),$$

where $r_1 = da_1$.

2.6 6/15/2024

Today we prove the following result:

Proposition 2.2. Let R be a noetherian ring and let M and N be R-modules such that M is finitely generated. Then

$$\operatorname{Ass}(\operatorname{Hom}_R(M,N)) = \operatorname{Supp} M \cap \operatorname{Ass} N.$$

Proof. Let \mathfrak{p} be an associated prime of $\operatorname{Hom}_R(M,N)$. Thus there exists an R-linear map $\varphi \colon M \to N$ such that $\mathfrak{p} = 0 \colon \varphi = \{a \in R \mid a\varphi = 0\}$. Let u_1, \ldots, u_m be generators of M as an R-module and let $v_1, \ldots, v_m \in N$ be their respective images under φ . Then note that $a\varphi = 0$ if and only if $av_i = 0$ for all $1 \le i \le m$.

$$a \in \mathfrak{p} \iff a\varphi = 0$$

 $\iff av_i = 0 \text{ for all } i$
 $\iff a \in \bigcap_{i=1}^m 0 : v_i.$

In particular we see that $\mathfrak{p} = \bigcap_{i=1}^m 0 : v_i$. Since \mathfrak{p} is prime, we see that $\mathfrak{p} = 0 : v_i$ for some i, or in other words, \mathfrak{p} is an associated prime of N. Next, assume for a contradiction that $M_{\mathfrak{p}} = 0$. Then for each i there exists an $s_i \in R \setminus \mathfrak{p}$ such that $s_i u_i = 0$. However this implies $s = s_1 \cdots s_n$ is in \mathfrak{p} since $sv_i = \varphi(su_i) = 0$ for all i, which is a contradiction. Therefore \mathfrak{p} is in the support of M. Thus far we have shown

$$Ass(Hom_R(M, N)) \subseteq Supp M \cap Ass N.$$

For the converse direction, suppose $\mathfrak p$ is in the support of M and is an associated prime of N, so $M_{\mathfrak p} \neq 0$ and $\mathfrak p = 0 : v$ for some $v \in N$. Since $M_{\mathfrak p} \neq 0$, there exists an i such that $0 : u_i \subseteq \mathfrak p = 0 : v$. By reordering if

necessary, we may assume that $0: u_1 \subseteq \mathfrak{p} = 0: v$. One would like to define an R-linear map $\varphi: M \to N$ such that $\varphi(u_1) = v$, but it's not clear how we should define it on the u_i for all $2 \le i \le m$. Let us cut to the chase and show how one usually proves this result: we have

```
\mathfrak{p} \in \mathrm{Ass}(\mathrm{Hom}_R(M,N)) \iff \mathfrak{p}_{\mathfrak{p}} \in \mathrm{Ass}(\mathrm{Hom}_R(M,N)_{\mathfrak{p}})
\iff \mathfrak{p}_{\mathfrak{p}} \in \mathrm{Ass}(\mathrm{Hom}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}},N_{\mathfrak{p}}))
\iff \mathrm{Hom}_{R_{\mathfrak{p}}}(\kappa(\mathfrak{p}),\mathrm{Hom}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}},N_{\mathfrak{p}})) \neq 0
\iff \mathrm{Hom}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}},N_{\mathfrak{p}}) \neq 0
\iff M_{\mathfrak{p}} \neq 0 \text{ and } \mathrm{Hom}_{R_{\mathfrak{p}}}(\kappa(\mathfrak{p}),N_{\mathfrak{p}}) \neq 0
\iff \mathfrak{p} \in \mathrm{Supp}\,M \cap \mathrm{Ass}\,N,
```

where in the second last if and only if we used the fact that $M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}}$ is a finite dimensional $\kappa(\mathfrak{p})$ (so it is a direct sum of $\kappa(\mathfrak{p})$'s). Note that we needed Nakayama's lemma for the statement $M_{\mathfrak{p}} \neq 0$ if and only if $M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}} \neq 0$, hence why we needed a noetherian hypothesis on R.