NOTES – MATH 6320
SPRING 2015

KARL SCHWEDE

1. Introduction to rings, ideals and homomorphisms

Commutative algebra is the study of commutative, associative rings with unity. Throughout this class, every *ring* will be commutative, associative and with unity. There are two main historical reasons to study commutative algebra:

- Algebraic Number Theory
- Algebraic Geometry

In algebraic number theory you might study rings like $\mathbb{Z}$ or $\mathbb{Z}[17]$ or $\mathbb{Z}_p$ (p-adics). Algebraic geometry studies geometric objects where the allowable functions are polynomials. For example, in topology you study geometric objects whose geometry is measured by continuous functions. In differential geometry you study geometric objects and you use differentiable functions to measure them. In algebraic geometry you study geometric objects using algebraic functions (polynomials). In all these types of geometry, knowing the functions is the same as understanding the geometric object.

It turns out that this is surprisingly powerful for algebraic geometry, every ring is a ring of functions on some uniquely determined geometric object (including the ring $\mathbb{Z}$, as we'll see later). This lets us interpret questions from number theory in a geometric language and thus gain access to new kinds of intuition. Furthermore, it allows you to translate number theoretic questions to the case of polynomial rings, where things are frequently easier.

> *Polynomial rings with coefficients in a field (and quotients/subrings) are generally easier to study than polynomial rings with coefficients in $\mathbb{Z}$ or some other ring of integers.*

The main way we will study rings is through their ideals. Suppose R is a ring. Note that if I, J are ideals then so is their intersection $I \cap J$, their sum $I + J = \{x + y \mid x \in I, y \in J\}$, their product $I \cdot J = \{\sum_{i=1}^n x_i \cdot y_i \mid x_i \in I, y_i \in J\}$. But their union $I \cup J$ is generally *not* an ideal.

Recall the following theorem:

Theorem 1.1. *Suppose that $J \subseteq R$ is an ideal. Then there is a bijection between the sets:*

$$\{\textit{ideals of } R \textit{ containing } J\} \leftrightarrow \{\textit{ideals of } R/J\}$$

Proof. The forward $\rightarrow$ direction takes an ideal I to I/J. The inverse $\leftarrow$ direction is just $\rho^{-1}(\overline{I})$ where I is an ideal of R/J. $\square$

Definition 1.2 (Maximal ideals)**.** An ideal $I \subseteq R$ is called *maximal* if $I \neq R$ and there is no proper ideal between I and R.

Lemma 1.3. *An ideal I is maximal if and only if R/I is a field.*

Proof. The zero ring is not a field, so we can dispense with the case that $R = I$. Recall that R/I is a field if and only if the only proper ideal is $\langle 0 \rangle$. Of course, this is clearly equivalent to requiring that I is maximal by **??**. $\square$

Definition 1.4 (Prime ideals)**.** An ideal $I \subseteq R$ is called *prime* if $I \neq R$ and if $xy \in I$, for $x, y \in R$, implies that either $x \in I$ or $y \in I$.

Lemma 1.5. *An ideal I is prime if and only if R/I is an (integral) domain.*

Proof. Suppose first that I is prime. If $\overline{x}, \overline{y} \in R/I$ (corresponding to $x, y \in R$) and $\overline{x} \cdot \overline{y} = 0$, then $x \cdot y \in I$ so either $x \in I$ and $y \in I$ by the primality of I. Thus $\overline{x} = 0$ or $\overline{y} = 0$.

Conversely, if I is not prime then there exist $x, y \in R$ with $x \cdot y \in I$ but $x, y \notin I$. Hence $\overline{x} \cdot \overline{y} = 0 \in R/I$ and R/I is not an integral domain. $\square$

Example 1.6 (A ring of continuous functions)**.** Suppose that C is the ring of continuous functions $f : \mathbb{R} \longrightarrow \mathbb{R}$. These form a ring under pointwise addition and multiplication. Consider the set $I = \{f \in C \mid f(0) = 0\}$. This is an ideal of C (the sum of two functions that vanish at the origin vanishes at the origin, the product of a function that vanishes at the origin and another function still vanishes at the origin). Is it prime or maximal?

Prime: If $f \cdot g \in I$, then $0 = (f \cdot g)(0) = (f(0)) \cdot (g(0))$. Thus either f or g vanish at the origin. In particular I is prime.

Maximal: In R/I, two functions are identified whenever they agree at the origin (note $f + I = g + I$ if and only if $f - g$ vanishes at the origin). In particular, each coset of R/I looks like $\{\text{constant}\} + I$. These have the structure of the ring $\mathbb{R}$, which is a field, and hence I is maximal.

On the other hand, the ideal $J = \{f \in C \mid f(x) = 0 \text{ for all } x \in [0, 1]\}$ is not prime and hence also not maximal. To see it isn't prime, consider f and g continuous functions where f vanishes on $[0, 0.5]$ and g vanishes on $[0.5, 1]$.

Another useful fact about prime ideals is the following.

Lemma 1.7. *Suppose that $I \subseteq R$ is a prime ideal and $J, J' \subseteq R$ are other ideals, then the following are equivalent.*

(i) $J \subseteq I$ *or* $J' \subseteq I$,
(ii) $J \cap J' \subseteq I$,
(iii) $J \cdot J' \subseteq I$.

Proof. We will prove the equivalence of (i) and (ii) and leave the relation with (iii) as an exercise (or you can do it as we did in class). Of course, obviously (i) implies (ii). Now suppose that $J \cap J' \subseteq I$. Suppose $J' \notin I$ and choose $x' \in J' \setminus I$. We will show that $J \subseteq I$. Choose $x \in J$. Then $xx' \in J \cap J' \subseteq I$ and hence either $x \in I$ or $x' \in I$. But the latter situation is impossible, so $x \in I$ and hence $J \subseteq I$. We have just shown that (ii) implies (i). $\square$

Example 1.8 (A polynomial ring)**.** Consider $R = \mathbb{R}[x]$ where $\mathbb{R}$ is a field. Consider the ideal I made up of all polynomials f such that $f(0) = 0$. It is easy to see that $I = \langle x \rangle$. Furthermore I is both prime (for the same reason as the ring of continuous functions) and maximal since $R/I \cong \mathbb{R}$ is a field.

Now consider $S = \mathbb{R}[x, y]$ and I is again the ideal made up of all polynomials f such that $f(0) = 0$. In this case $I = \langle x, y \rangle$ is again both prime and maximal. Note that $J = \langle x \rangle$ is prime since $S/J \cong k[y]$ (note, S/J can be viewed as polynomials under the equivalence relation where $f \sim g$ if they agree along the line $x = 0$).

Finally, I leave it as an exercise to check that $M = \langle xy \rangle$ is the set of functions that vanish on both the x and y axes.

2. Plenty of prime ideals

Recall Zorn's lemma, which we assume as an axiom.

Theorem 2.1 (Zorn's Lemma)**.** *Suppose that X is a non-empty partially ordered set under $\leq$ that satisfies the following condition. For every ascending chain $\ldots \leq x_\lambda \leq \ldots$ (for λ in some indexing set Λ) there exists an element $z \in X$ with $z \geq$ every element in the chain. Then, X contains at least one maximal element.*

Using this, we can show that rings have plenty of maximal ideals.

Proposition 2.2. *Suppose that $I \subsetneq R$ is a proper ideal in a ring R. Then there exists a maximal ideal of R, $\mathfrak{m} \supseteq I$.*

Proof. Let X be the set of proper ideals of R which contain I, ordered under inclusion. We claim that X satisfies the condition of Zorn's lemma. Obviously X is nonempty as it contains I. Further suppose that $I \subseteq \ldots \subseteq J_\lambda \subseteq \ldots$ is an ascending chain (for λ in some indexing set Λ). Let $J = \bigcup_{\lambda \in \Lambda} J_\lambda$. We claim that J is a proper ideal.

To see it is an ideal, suppose that $x, x' \in J$, so $x \in J_\lambda$ and $x' \in J_{\lambda'}$. By symmetry we suppose that $J_\lambda \subseteq J_{\lambda'}$ so that $x, x' \in J_{\lambda'}$. Since $J_{\lambda'}$ is an ideal, $x + x' \in J_{\lambda'} \subseteq J$ which shows that J is closed under addition. If $x \in J$ and $r \in R$, then $x \in J_\lambda$ for some λ and thus so is rx. Hence $rx \in J$. This proves that J is an ideal. Finally, since each J_λ is proper, 1 is not in any J_λ and so $1 \notin J$. Hence J is also proper. It follows that Zorn's lemma is satisfied and our desired maximal ideal is guaranteed. $\square$

Corollary 2.3. Spec R *always contains at least 1 closed point assuming it is non-empty.*

Proof. Combine Lemma 6.7 and Proposition 2.2. □

3. Ring homomorphisms

We now review how ideals behave under ring homomorphisms.

Definition 3.1. For us, a homomorphism of rings $f : R \longrightarrow S$ always satisfies $f(1_R) = 1_S$.

This is justified by thinking about functions. We'll see that all ring homomorphisms are basically pullbacks of functions from one topological space to another. In this case, the constant function 1 should be pulled back to the constant function 1.

Proposition 3.2. *Suppose that $f : R \longrightarrow S$ is a ring homomorphism. Then $f^{-1}(J)$ is an ideal for every ideal $J \subseteq S$. However, if I is an ideal of R, then $f(I)$ need not be an ideal of S (unless f happens to be surjective). However, the ideal $f(I)$ generates is usually denoted by IS.*

In the special case that f is injective, or better yet that $R \subseteq S$, $f^{-1}(J)$ is frequently denoted by $J \cap R$.

Furthermore:

(a) *If $J \subseteq S$ is prime, so is $f^{-1}(J)$.*
(b) *If $J \subseteq S$ is maximal, $f^{-1}(J)$ need not be.*
(c) *If $I \subseteq R$ is prime or maximal, then $J \cdot S$ need not be, unless f is surjective.*
(d) *If $I \subseteq R$, then $I \subseteq f^{-1}(IS)$.*
(e) *If $J \subseteq S$, then $J \supseteq (f^{-1}(J))S$.*

Proof. This is left as an exercise to the reader. □

4. Exactness, tensor products, and the Hom functor

Tensor does not preserve exactness in general.

Example 4.1. Indeed, consider the injection $\mathbb{Z} \xrightarrow{\times 2} \mathbb{Z}$ and let us tensor it with $\otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$. Then we have the map

$$\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \xrightarrow{(\times 2)\otimes(\mathrm{id})} \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}. \tag{4.1.1}$$

Note that first $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$. Let's convince ourselves of this explicitly, indeed each $a \otimes b = 1 \otimes ab$ and so we can represent each element of the tensor as an element of $\mathbb{Z}/2\mathbb{Z}$. Of course, there is a surjective map $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z}$ (coming from the universal property of the tensor product) and the isomorphism follows.

We return to the map and observe that $1 \otimes 1$ is sent to $2 \otimes 1 = 1 \otimes 2 = 1 \otimes 0 = 0$. In particular, the map from (4.1.1) is the zero map and hence not injective.

Tensor products do preserve a lot of other properties though.

Definition 4.2 (Short exact sequences)**.** Suppose that L, M, N are R-modules. A *short exact sequence*, denoted

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

is a pair of maps $\phi : L \longrightarrow M$ and $\psi : M \longrightarrow N$ such that ϕ is injective, ψ is surjective and $\ker \psi = \operatorname{im} \phi$.

For example, $0 \longrightarrow \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$ is a short exact sequence.

Example 4.3. The canonical example of a short exact sequence comes from picking $I \subseteq R$ an ideal and forming:

$$0 \longrightarrow I \longrightarrow R \longrightarrow R/I \longrightarrow 0.$$

Short exact sequences are special cases of exact sequences.

Definition 4.4 (Complexes Exact sequence)**.** Suppose that $\{C_i\}$ is a collection of R-modules with maps $C_i \xrightarrow{\phi_i} C_{i+1}$, written diagrammatically as:

$$\dots \xrightarrow{\phi_{i-2}} C_{i-1} \xrightarrow{\phi_{i-1}} C_i \xrightarrow{\phi_i} C_{i+1} \xrightarrow{\phi_{i+1}} C_{i+2} \xrightarrow{\phi_{i+2}} \dots$$

This is called a (cochain) complex if $\ker \phi_i \supseteq \operatorname{im} \phi_{i-1}$ for all i. It is called an *exact sequence* if $\ker \phi_i = \operatorname{im} \phi_{i-1}$ for all i.

As we have already seen, tensor products do not preserve exact sequences (since they don't preserve injections, which can be written as exact sequences $0 \longrightarrow M \longrightarrow N$). However, the following is true.

Proposition 4.5. *If* $0 \longrightarrow L \xrightarrow{a} M \xrightarrow{b} N \longrightarrow 0$ *is an exact sequence and* T *is another* R*-module, then*

$$L \otimes_R T \xrightarrow{\alpha} M \otimes_R T \xrightarrow{\beta} N \otimes_R T \longrightarrow 0$$

is also exact.

This proposition asserts that $\otimes$ is *right-exact* (it takes short exact sequences to sequences that are exact on the right).

Proof. It is easy to see that β is surjective, indeed if $n \otimes t \in N \otimes T$, then since $M \longrightarrow N$ is surjective, there exists $m \in M$ such that $b(m) = n$. Hence $m \otimes t \mapsto n \otimes t$ and it follows that β surjects.

We now need to show that $\ker \beta = \operatorname{im} \alpha$. Let $C = \operatorname{im} \alpha$, we already know that $C \subseteq \ker \beta$ and so we have a map $\gamma : (M \otimes_R T)/C \longrightarrow N \otimes_R T$. It is sufficient to show that this map is injective. Define a map

$$\sigma : N \otimes_R T \longrightarrow (M \otimes_R T)/C$$

by $n \otimes t \mapsto \overline{b_1(n) \otimes t}$ where $b_1(n)$ is *any* $m \in M$ with $b(m) = n$ and $\overline{\bullet}$ denotes the image after modding out by C. We need to show that σ is well defined. Suppose that m and m' are such that $b(m) = b(m') = n$ then we need to show that $\overline{m \otimes t} = \overline{m' \otimes t}$ (this is the same as showing that the obvious bi-linear map from the universal property is well defined). But since $b(m) = b(m')$, there exists $l \in L$ such that $a(l) = m - m'$. Therefore since $a(l) \otimes t \in C$, we see that $\overline{(m - m') \otimes t} = 0$ and $\overline{m \otimes t} = \overline{m' \otimes t}$. This shows σ is well defined. Now, $(M \otimes_R T)/C \xrightarrow{\gamma} N \otimes_R T \xrightarrow{\sigma} (M \otimes_R T)/C$ sends $\overline{m \otimes t}$ back to itself. It follows that γ is injective. $\square$

We saw another proof using the relation of $\otimes$ with Hom. Indeed, at least as fundamental as the $\otimes$ functor is the Hom functor. Suppose that M, N are R-modules. Then $\mathrm{Hom}_R(M, N)$ is the set of R-module homomorphisms $M \longrightarrow N$. It is an R-module since $r.\phi$ is defined by $(r.\phi)(m) = r\phi(m) = \phi(rm)$. In other words, r can act on either the domain or the codomain, it doesn't matter. Now suppose that $\eta : L \longrightarrow M$ is a module homomorphism. Then we have an induced R-module homomorphism:

$$\Phi : \mathrm{Hom}_R(M, N) \longrightarrow \mathrm{Hom}_R(L, N)$$

defined by $\big(\Phi(f)\big)(l) = f(\eta(l))$.

On the other and, of $\delta : N \longrightarrow O$ is an R-module homomorphism, then obtain:

$$\Psi : \mathrm{Hom}_R(M, N) \longrightarrow \mathrm{Hom}_R(M, O)$$

which is defined by $\big(\Phi(f)\big)(m) = \delta(f(m))$.

Proposition 4.6. *The functors* $\mathrm{Hom}_R(\bullet, N)$ *and* $\mathrm{Hom}_R(M, \bullet)$ *are both left-exact. In other words, if*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

is an exact sequence of R-modules, then

$$0 \longrightarrow \mathrm{Hom}_R(C, N) \xrightarrow{g'} \mathrm{Hom}_R(B, N) \xrightarrow{f'} \mathrm{Hom}_R(A, N)$$

is exact and

$$0 \longrightarrow \mathrm{Hom}_R(M, A) \xrightarrow{f''} \mathrm{Hom}_R(M, B) \xrightarrow{g''} \mathrm{Hom}_R(M, C)$$

is also exact.

Proof. For the first sequence we handle the injectivity of g' first. Suppose that $\phi \in \mathrm{Hom}_R(C, N)$ and that $B \xrightarrow{g} C \xrightarrow{\phi} N$ is zero (ie, the image of ϕ in $\mathrm{Hom}_R(B, N)$ is zero). But then since g is surjective, we must have ϕ zero as well. Next we handle $\ker f' \subseteq \operatorname{im} g'$. Suppose that $\psi \in \mathrm{Hom}_R(B, N)$ is such that $A \xrightarrow{f} B \xrightarrow{\psi} N$ is zero so that there is $\overline{\psi} : C \cong B/A \longrightarrow N$. Consider the composition $B \xrightarrow{g} B/A \xrightarrow{\overline{\psi}} N$, obviously this is the same as ψ and so $g'(\overline{\psi}) = \psi$ which shows that $\ker f' \supseteq \operatorname{im} g'$. Finally we need to show $\ker f' \supseteq \operatorname{im} g'$. Choose $\theta \in \mathrm{Hom}_R(C, N)$ and consider $g'(\theta) = \theta \circ g \in \mathrm{Hom}_R(B, N)$. Finally we consider $f'(g'(\theta)) = \theta \circ g \circ f \in \mathrm{Hom}_R(A, N)$. But $g \circ f$ is zero, and thus so is $f'(g'(\theta))$.

We now consider the second exact sequence. First suppose that $\phi \in \mathrm{Hom}_R(M, A)$, then $f''(\phi) = f \circ \phi$, ie $M \xrightarrow{\phi} A \xrightarrow{f} B$. Since f is injective, if ϕ

is nonzero, then $f \circ \phi = f''(\phi)$ is also nonzero. Next we show that $\operatorname{im} f'' \subseteq \ker g''$. Suppose that $\phi \in \operatorname{Hom}_R(M, A)$, then $f''(\phi) = f \circ \phi$. $g''(f''(\phi)) = g \circ f \circ \phi$. Since $g \circ f = 0$, $g''(f''(\phi)) = 0$ which proves what we wanted. Finally we show that $\ker g'' \subseteq \operatorname{im} f''$. Suppose $\psi \in \operatorname{Hom}_R(M, B)$ is such that $g''(\psi) = g \circ \psi = 0$. In other words

$$M \xrightarrow{\psi} B \xrightarrow{g} C$$

is zero. Since the kernel of g is equal to $f(A)$, we see that $\psi(M) \subseteq f(A)$. But f is injective and so we have a factorization of ψ

$$\psi : M \xrightarrow{\eta} A \xrightarrow{f} B.$$

But then $\psi = f''(\eta)$ which completes the proof. □

Remark 4.7. Note that in the first part of the proof, we didn't need that f was injective. In the second, we didn't need that g was surjective.

Example 4.8. We compute some Homs, first over the ring $\mathbb{Z}$. Then

$$\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) = 0$$

since if $\phi(a/b) \neq 0$, then $\phi(c \cdot (a/b)) = c\phi(a/b)$ where all terms are integers. This yields a contradiction if $\gcd(b, c) = 1$ with $b > 1$.

Also note that

$$\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/5, \mathbb{Z}) = 0$$

since the image of any such homomorphism is a finite subgroup of $\mathbb{Z}$, and the only such subgroup is $\{0\}$.

Now we work over a polynomial ring, $R = k[x, y]$. First observe that

$$\operatorname{Hom}_R(\langle x, y\rangle, \langle x, y\rangle)$$

contains the identity morphism, and all multiples of this morphism. It turns out these are the only ones (which can be verified via Macaulay2, or cleverness). In class, we verified that we can't send $x \mapsto y$ and $y \mapsto x$ and keep it a R-module homomorphism since then

$$x^2 = x\phi(y) = \phi(xy) = \phi(yx) = y\phi(x) = y^2.$$

Likewise

$$\operatorname{Hom}_R(\langle x, y\rangle, R) \cong R$$

where the inclusion homomorphism is sent to 1 (and all the others are just multiples of it).

Finally,

$$\operatorname{Hom}_R(R/\langle x, y\rangle, R) = \{0\}$$

since if $z \in R/\langle x, y\rangle, R) \cong k$ is such that $\phi(z) \neq 0$, then $0 \neq x\phi(z) = \phi(x.z) = 0$ since $xz \in \langle x, y\rangle$.

Proposition 4.9. *A sequence* $A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ *is exact if and only if*

$$0 \longrightarrow \mathrm{Hom}_R(C, N) \xrightarrow{g'} \mathrm{Hom}_R(B, N) \xrightarrow{f'} \mathrm{Hom}_R(A, N)$$

is exact for every R*-module* N*.*

Likewise, $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C$ *is exact if and only if*

$$0 \longrightarrow \mathrm{Hom}_R(M, A) \xrightarrow{f''} \mathrm{Hom}_R(M, B) \xrightarrow{g''} \mathrm{Hom}_R(M, C)$$

is exact for every R*-module* M*.*

Proof. We have already done both of the ($\Rightarrow$) directions. So first suppose that $0 \longrightarrow \mathrm{Hom}_R(C, N) \xrightarrow{g'} \mathrm{Hom}_R(B, N) \xrightarrow{f'} \mathrm{Hom}_R(A, N)$ is exact for every R-module N. Set N to be the quotient module $C/g(B)$ and let $\psi : C \longrightarrow N$ be the canonical surjection. If g is not surjective, then ψ is nonzero and hence $g'(\psi) = \psi \circ g$ is non-zero (but that obviously is zero).

Next suppose that $\ker f' = \mathrm{im}\, g'$ for every N. We'd like to show that $\ker g = \mathrm{im}\, f$ as well. Since $f' \circ g' = 0$, by setting $N = C$ we have $f' \circ g' \circ \mathrm{id}_C = 0$. But this is just $g \circ f$. Finally, set $N = B/\mathrm{im}(A)$. Then suppose that $\phi \in \mathrm{Hom}_R(B, B/\mathrm{im}(A))$ satisfies $f'(\phi) = \phi \circ f' = 0$. In other words

$$A \xrightarrow{f} B \xrightarrow{\phi} B/\mathrm{im}(A)$$

is the zero map. Then there exists $\overline{\phi} : C \cong B/\mathrm{im}(A) \longrightarrow B/\mathrm{im}(A)$ factoring ϕ. It is easy to see that $g'(\overline{\phi}) = \phi$ which completes this part of the proof.

For the second part the proof is much easier, we begin by setting $M = R$, then the exact sequence of Homs becomes simply $0 \longrightarrow A \longrightarrow B \longrightarrow C$ which is also exact. $\square$

The functors of Hom and tensor are closely related.

Theorem 4.10 (Hom $-\otimes$ adjointness)**.** *If* L, M, N *are* R*-modules, then there is an* R*-module isomorphism:*

$$\mathrm{Hom}_R(L \otimes_R M, N) \cong \mathrm{Hom}_R(L, \mathrm{Hom}_R(M, N))$$

Proof. Given $\phi \in \mathrm{Hom}_R(L, \mathrm{Hom}_R(M, N))$ we need to construct $\Phi(\phi) \in \mathrm{Hom}_R(L, \mathrm{Hom}_R(M, N))$. We an action of ϕ on elements of $L \otimes_R M$. Given $\sum l_i \otimes m_i$ we define

$$\phi(\sum l_i \otimes m_i) = \sum (\phi(l_i))(m_i)$$

Note that each $\phi(l_i) \in \mathrm{Hom}_R(M, N)$ so it makes perfect sense to act upon m_i. Thus we have defined Φ.

To go the other way, suppose that $\psi \in \mathrm{Hom}_R(L \otimes_R M, N)$, and we will define $\Psi(\psi) \in \mathrm{Hom}_R(L, \mathrm{Hom}_R(M, N))$. So choose $l \in L$. Then $\Psi(\psi)(l) = \psi(l \otimes \_\_)$ where the blank is to be filled in from M.

We should verify that $\Psi \circ \Phi$ and $\Phi \circ \Psi$ are the identities. But I will leave this to you (I think we'll do one direction as a class). $\square$

Now we discuss a proof of the right exactness of $\otimes$ via the left exactness of Hom.

Lemma 4.11. *$\otimes_R M$ is right exact for any R-module M.*

Proof. We suppose that $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ is exact and we want to show that

$$A \otimes_R M \longrightarrow B \otimes_R M \longrightarrow C \otimes_R M \longrightarrow 0$$

is exact. It is sufficient to show that

$$0 \longrightarrow \mathrm{Hom}_R(C \otimes_R M, N) \longrightarrow \mathrm{Hom}_R(B \otimes_R M, N) \longrightarrow \mathrm{Hom}_R(A \otimes_R M, N)$$

is exact for any R-module N. But that is exact if and only if

$$0 \longrightarrow \mathrm{Hom}_R(M, \mathrm{Hom}_R(C, N)) \longrightarrow \mathrm{Hom}_R(M, \mathrm{Hom}_R(B, N)) \longrightarrow \mathrm{Hom}_R(M, \mathrm{Hom}_R(A, N))$$

is exact by the adjointness of tensor and Hom (we also need to know that the adjointness isomorphism is compatible with morphisms in the M variable, but it is, I won't check it though). But this is exact if

$$0 \longrightarrow \mathrm{Hom}_R(C, N) \longrightarrow \mathrm{Hom}_R(B, N) \longrightarrow \mathrm{Hom}_R(A, N)$$

is exact, which follows if $A \longrightarrow B \longrightarrow C \longrightarrow 0$ is exact (which it is). $\square$

Finally, I want to explain a key relation between tensor and Hom. Suppose that M, N, L are R-modules. Then it is easy to see that there is an R-module homomorphism

$$\mathrm{Hom}_R(M, N) \longrightarrow \mathrm{Hom}_R(M \otimes_R L, N \otimes_R L),$$

simply send $(\phi : M \longrightarrow N) \otimes l$ to the induced morphism $M \otimes_R L \longrightarrow N \otimes_R L$. In general this is not an isomorphism. There is another key variant of this, suppose that L is now an R-algebra, then

$$M \otimes_R L \longrightarrow N \otimes_R L$$

is a map of L-modules. In particular, we get a map

$$\mathrm{Hom}_R(M, N) \longrightarrow \mathrm{Hom}_L(M \otimes_R L, N \otimes_R L).$$

If we tensor the left side of the map by L, we get an L-linear map

$$\mathrm{Hom}_R(M, N) \otimes L \longrightarrow \mathrm{Hom}_L(M \otimes_R L, N \otimes_R L).$$

5. Nakayama's Lemma

We now switch gears entirely.

Theorem 5.1 (The determinant trick)**.** *Suppose M is an R-module generated by n-elements and $\phi \in \mathrm{Hom}_R(M, M)$. If $I \subseteq R$ is such that $\phi(M) \subseteq I \cdot M$ then there is a relation of the form*

$$\phi^n + a_1\phi^{n-1} + \cdots + a_{n-1}\phi + a_n \cdot \mathrm{id}_M = 0 \in \mathrm{Hom}_R(M, M) \tag{5.1.1}$$

where $a_i \in I^i$.

Proof. Write $M = \langle m_1, \dots, m_n \rangle$. We can write each $\phi(m_i) = \sum_{j=1}^n a_{ij} m_j$. In other words:

$$\sum_{j=1}^n (\delta_{ij} \cdot \phi - a_{ij} \cdot \mathrm{id}_M)(m_j) = 0 \in M$$

holds for each i (where δ_{ij} is the Kronekcer delta). We view this is a square matrix

$$\Delta = [(\delta_{ij} \cdot \phi - a_{ij} \cdot \mathrm{id}_M)]$$

and note that

$$\Delta \begin{bmatrix} m_1 \\ m_2 \\ \dots \\ m_n \end{bmatrix} = 0.$$

Let B be the classical adjoint matrix of Δ, and recall that $B\Delta = \det(\Delta) I_{n \times n}$ so that

$$\det(\Delta)(m_j) = 0 \in M$$

for each m_j. Since these generate M we see that $\det(\Delta) = 0 \in \mathrm{Hom}_R(M, M)$. Expanding out the determinant gives the result. $\square$

We now prove Nakayama's lemma (in fact, all of the results below are frequently referred to as Nakayama's lemma).

Theorem 5.2 (Nakayama's Lemma 1)**.** *Suppose that R is a ring, $I \subseteq R$ is an ideal and that M is a finitely generated R-module. If $M = I \cdot M$ then there exists $x \in R$ such that $x \cdot m = 0$ for all $m \in M$ and that $x - 1 \in I$.*

Proof. Set $\phi = \mathrm{id}_M$. Then by the determinant trick, $\phi(M) = M \subseteq I \cdot M$ and so there exist $a_i \in I^i$ such that

$$\mathrm{id}_M + a_1 \mathrm{id}_M + \dots + a_n \mathrm{id}_M = 0$$

In particular, $x = (1 + a_1 + \dots + a_n)$ kills every element of M. Furthermore, certainly $x - 1 \in I$. $\square$

Corollary 5.3 (Nakayama's Lemma 2)**.** *If R is local, M is an R-module and $I \subsetneq R$ is a proper ideal such that $M = I \cdot M$, then $M = 0$.*

Proof. Since I is proper, $I \subseteq \mathfrak{m}$ where $\mathfrak{m}$ is the unique maximal ideal of R. Since $x - 1 \in \subseteq \mathfrak{m}$, we see that x is not contained in $\mathfrak{m}$ and hence is a unit. But then $xm = 0$ for all $m \in M$ implies that $M = 0$. $\square$

Corollary 5.4 (Nakayama's Lemma 3)**.** *Suppose that $(R, \mathfrak{m})$ is a local ring. If $f : M \longrightarrow N$ is a map of R-modules with N finitely generated. Then f is surjective if and only if the composition*

$$\overline{f} : M \longrightarrow N \longrightarrow N/(\mathfrak{m} \cdot N)$$

is surjective.

We prove Nakayama's lemma version 3.

Proof. Certainly if f is surjective so is $\overline{f}$. Conversely suppose that $\overline{f}$. The fact that $\overline{f}$ is surjective implies that $f(M) + (\mathfrak{m} \cdot N) = N$. It follows that $\mathfrak{m} \cdot (N/f(M)) = (\mathfrak{m} \cdot N + f(M))/f(M) = N/f(M)$. Thus $N/f(M) = 0$ and so f is surjective. ☐

Corollary 5.5 (Nakayama's Lemma 4)**.** *Suppose that* $(R, \mathfrak{m}, k = R/\mathfrak{m})$ *is a local ring,* M *is a finite* R*-module and* $\overline{M} = M/(\mathfrak{m} \cdot M)$*. Then* $\overline{M}$ *is a finite dimensional vector space of dimension* n*. Furthermore,*

(a) *If* $\overline{m}_1, \ldots, \overline{m}_n$ *are a* k*-basis for* $\overline{M}$*, then any set of pre-images* $m_1, \ldots, m_n$ *form a minimal generating set for* M*.*
(b) *Every minimal generating set for* M *is obtained in this way, and so they all have* n *elements.*

Proof. We begin with the proof of (a). It is easy to see that the m_i are a generating set, indeed consider the map $R^n \longrightarrow M$ which sends e_i to m_i. Then this map is certainly surjective by Nakayama's Lemma 3. We just need to show that this set is minimal. However, if it was not minimal, we could remove an element, and still have a generating set. Without loss of generality let us remove m_n. But then $R^{n-1} \longrightarrow M$ would be surjective and thus so would $k^{n-1} \cong (R/\mathfrak{m})^{n-1} \longrightarrow \overline{M}$, which is impossible since $\overline{M}$ has dimension M.

Now suppose that $m_1, \ldots, m_l$ is another generating set for M with $l > n$ (the case of $l < n$ is ruled out by the argument immediately above). It follows that some set of n elements within $\{\overline{m}_1, \ldots, \overline{m}_l\}$ span $\overline{M}$, say $\overline{m}_1, \ldots, \overline{m}_l$ span the vector space $\overline{M}$. Hence $m_1, \ldots, m_n$ also generate M and so every minimal generating set of M is obtained this way. ☐

6. The spectrum of a ring

Definition 6.1 (Spec)**.** For a ring R the *(prime) spectrum* of R, denoted $\operatorname{Spec} R$, is the set of all prime ideals of R. The set of all maximal ideals is denoted by $\mathfrak{m}\text{-}\operatorname{Spec} R$.

Example 6.2 (Spec of PIDs)**.**

- If k is a field, then $\operatorname{Spec} k$ is a singleton, the ideal generated by zero.
- $\operatorname{Spec} \mathbb{Z}$ is the set $\{\langle p \rangle \mid p \in \mathbb{Z}_{>0} \text{ prime}\} \cup \{\langle 0 \rangle\}$.
- For $\operatorname{Spec}(R = \mathbb{C}[x])$, since $\mathbb{C}[x]$ is a PID, we observe that the prime ideals are just $\langle f \rangle$ where f is irreducible or zero. Since $\mathbb{C}$ is algebraically closed, the irreducible elements are linear polynomials. In particular,
$$\operatorname{Spec} R = \{\langle x - \alpha \rangle \mid \alpha \in \mathbb{C}\} \cup \{\langle 0 \rangle\}.$$
This can be identified with $\mathbb{C}$ unioned with another point $\langle 0 \rangle$.
- For $\operatorname{Spec}(R = \mathbb{R}[x])$, a similar analysis yields:
$$\operatorname{Spec} R = \{\langle x - \alpha \rangle \mid \alpha \in \mathbb{R}\} \cup \{\langle x^2 + bx + c \rangle \mid b, c \in \mathbb{R}, x^2 + bx + c \text{ is irreducible}\} \cup \{\langle 0 \rangle\}.$$
In this case, $\operatorname{Spec} \mathbb{R}[x]$ can be viewed as the set of conjugate pairs of $\mathbb{C}$, unioned with another point $\langle 0 \rangle$.

Our next goal is to give $\operatorname{Spec} R$ the structure of a topological space. Suppose that I is an ideal of R. Then we set $V(I) \subseteq \operatorname{Spec} R$ to be the set of prime ideals containing I.

Lemma 6.3. (a) *If I, J are ideals, then $V(I \cap J) = V(I) \cup V(J)$.*
(b) *If $\{I_\lambda\}_{\lambda \in \Lambda}$ is a family of ideals then $V\big(\sum_{\lambda\in\Lambda} I_\lambda\big) = \bigcap_{\lambda \in \Lambda} V(I_\lambda)$.*

Proof. For (a), suppose that a prime ideal P contains $I \cap J$. Then P contains I or J by Lemma 1.7. The reverse direction just reverses this.

For (b), suppose that $P \supseteq \sum_{\lambda\in\Lambda} I_\lambda$, then obviously P contains every ideal in the sum. For the reverse direction, if P contains each I_λ then it contains the sum. $\square$

Hence we declare a subset $Y \subseteq \operatorname{Spec} R$ to be *closed* if $Y = V(I)$.

Theorem 6.4. *With notation as above, the closed sets form a topology on* $\operatorname{Spec} R$. *This is called the* Zarsiki topology.

This *very weak* topology is very far from Hausdorff. Indeed, a point (prime ideal) $P \in \operatorname{Spec} R$ is closed if and only if P is a maximal ideal. On $\operatorname{Spec} \mathbb{Z}$, ignoring the point $\langle 0 \rangle$, this is just the finite complement topology.

Proposition 6.5. *Suppose that $f : R \longrightarrow S$ is a ring homomorphism. Then the map $Q \mapsto f^{-1}(Q)$, $\phi : \operatorname{Spec} S \longrightarrow \operatorname{Spec} R$ is continuous.*

Proof. Suppose that I is an ideal of R. We need to show that $\phi^{-1}(V(I))$ is closed. The obvious thing to hope is that $\phi^{-1}(V(I)) = V(IS)$. Indeed, suppose that $P \in V(I) \subseteq \operatorname{Spec} R$ so that $P \supseteq I$. Suppose that $Q \in \operatorname{Spec} S$ is such that $\phi(Q) = P$ (in other words, that $f^{-1}(Q) = P$). Certainly $P \cdot S \subseteq Q$ and so $I \cdot S \subseteq Q$ and thus $\phi^{-1}(V(I)) \subseteq V(IS)$.

Now suppose that $Q \in V(IS) \subseteq \operatorname{Spec} S$ so that $Q \supseteq IS$. Consider $P = f^{-1}(Q) = \phi(Q)$ and observe that $P \supseteq I$. Thus $V(IS) \subseteq \phi^{-1}(V(I))$. $\square$

Example 6.6. Consider the map $f : \mathbb{C}[x] \longrightarrow \mathbb{C}[t]$ which sends x to $t^2 - 1$ and fixes $\mathbb{C}$. Let's consider the induced map on the prime spectra (note that both spectra are the same, copies of $\mathbb{C}$ with an extra zero point). Denote the map $\phi : \operatorname{Spec} \mathbb{C}[t] \longrightarrow \operatorname{Spec} \mathbb{C}[x]$. From here on out, since f is injective, we can replace x by t^2.

The zero ideal $\langle 0 \rangle$ is sent to the zero ideal (since ϕ is injective) so that isn't interesting. Now consider the prime ideal $P = \langle t - \alpha \rangle \subseteq \mathbb{C}[t]$. We ask what is $\phi(P)$. There is a unique prime ideal $Q \subseteq \mathbb{C}[t^2 - 1]$ with $Q = P \cap \mathbb{C}[t]$. Since the prime ideals of $\mathbb{C}[x] = \mathbb{C}[t^2 - 1]$ all look like $\langle (t^2 - 1) - \beta \rangle$, we need $(t^2 - 1) - \beta \in \langle t - \alpha \rangle$ (and this β is unique). Of course, $t^2 - \alpha^2 \in \langle t - \alpha \rangle$ and so we see that $1 + \beta = \alpha^2$ or in other words that $\beta = \alpha^2 - 1$.

In conclusion, the point $\langle t - \alpha \rangle$ (corresponding to α) is sent to $\langle x - (\alpha^2 - 1) \rangle$ (which corresponds to $\alpha^2 - 1$). If we identify the map ϕ with the map $\mathbb{C} \longrightarrow \mathbb{C}$ which sends α to $\alpha^2 - 1$, then f is just the pullback of this morphism (on polynomials).

Lemma 6.7. *Given any $P \in \operatorname{Spec} R$, the topological closure $\overline{\{P\}}$ is equal to $V(P)$. In particular, the closed points of* $\operatorname{Spec} R$ *are exactly the maximal ideals.*

Proof. The smallest $V(I)$ that contains P is simply $V(P)$. (Note if $P \in V(I)$, then $P \supseteq I$, larger ideals give smaller V's). The result follows immediately. $\square$

7. Multiplicative sets and localization

Suppose that R is a ring.

Definition 7.1 (Multiplicative set)**.** A multiplicative set $W \subseteq R$ is a set such that $1 \in W$ and such that W is closed under multiplication.

Example 7.2. Suppose that R is an integral domain, then $W = R \setminus \{0\}$ is a multiplicative set. Alternately, if $t \in R$, then $\{1, t, t^2, t^3, \ldots\}$ is a multiplicative set.

Lemma 7.3. *Suppose that $P \subseteq R$ is a prime ideal, then $R \setminus P$ is a multiplicative set.*

Proof. If $a, b \in W := R \setminus P$, then $ab \notin P$ and hence $ab \in W$. Of course $1 \in W$ since $1 \notin P$. $\square$

Definition-Proposition 7.4. *Consider the set $R \times W$ under the following equivalence relation. $(r, w) \sim (r', w')$ if there exists $v \in W$ such that $rw'v = r'wv$. We denote the equivalence classes under this operation by $W^{-1}R$. For simplicity, we write $[(r, w)] \in W^{-1}R$ as r/w.*

Then $W^{-1}R$ is a ring with the following addition and multiplication.

$$\begin{array}{rcl} (r/w) + (r'/w') & = & \frac{rw'+r'w}{ww'} \\ (r/w) \cdot (r'/w') & = & \frac{rr'}{ww'} \end{array}$$

Furthermore, there is a canonical ring homomorphism $\ell : R \longrightarrow W^{-1}R$ which sends r to $r/1$.

Proof. This is an exercise for the reader. $\square$

Obviously if R is an integral domain and $W = R \setminus \{0\}$ then $W^{-1}R$ is a field, the smallest field containing R (up to isomorphism).

We make a couple trivial (but useful) observations.

Lemma 7.5. (a) *An element $r/w \in W^{-1}R$ is equal to $0 = 0/1$ if and only if there exists $v \in W$ such that $vr = 0$.*

(b) *If an element $r/w \in W^{-1}R$ is equal to $1 = 1/1$, then $vr \in W$ for some $v \in W$.*

Proof. For (a), if $r/w = 0/1$, then there exists $v \in W$ such that $vr = 0w = 0$. The converse reverses this. For (b), if $r/w = 1$, then $vr = vw \in W$ for some $v \in V$. $\square$

Example 7.6. The map $\ell : R \longrightarrow W^{-1}R$ need not be injective in general. For instance, if $0 \in W$, then $W^{-1}R$ is the zero ring.

For a slightly more interesting example, set $R = k[x, y]/\langle xy\rangle$ and fix $W = \{1, x, x^2, x^3, \ldots\}$. Then observe that $y/1 = 0 \in W^{-1}R$ since $xy = 0 \cdot 1$. It is in fact possible to show that $W^{-1}R = k[x, x^{-1}]$.

Example 7.7. If R is an integral domain and $f \in R$ is non-zero, the $W^{-1}R = R[f^{-1}] = R[x]/\langle xf - 1\rangle$. Hopefully you proved that this is true on the homework.

Theorem 7.8 (Universal property of localization)**.** *Suppose that R is a ring, W is a multiplicative set and $f : R \longrightarrow S$ is a ring homomorphism such that $f(w)$ is invertible in S for each $w \in W$. Then there is a unique factorization of f making the diagram commute:*

$$\begin{tikzcd} R \arrow[rr, "f"] \arrow[dr, "\ell"'] & & S \\ & W^{-1}R \arrow[ur, dotted, "\phi"'] & \end{tikzcd}$$

Proof. We prove the existence of such a factorization. Obviously we want $\phi(x/w) = f(x)/f(w)$. There is the question of whether or not this is well defined, so suppose that $x/w = x'/w'$ so that $vxw' = vx'w$ for some $v \in V$. Then $f(v)f(x)f(w') = f(v)f(x')f(w)$ and so since $f(v), f(w)$ and $f(w')$ are invertible, we see that

$$f(x)/f(w) = f(x')/f(w')$$

which proves that ϕ is well defined. □

Let us now describe what localization does to extension of ideals.

Lemma 7.9. *Suppose that $I \subseteq R$ is an ideal and $W \subseteq R$ is a multiplicative set. Then we can characterize the extension*

$$I(W^{-1}R) = \{x/w \in W^{-1}R \mid x \in I\}$$

Proof. Obviously the containment $\supseteq$ holds since $(x/1) \cdot (1/w) \in I(W^{-1}R)$ for all $x \in I$ and $w \in W$. For the reverse containment, suppose that

$$\sum_i^n (x_i/1) \cdot (1/w_i) \in I(W^{-1}R)$$

is an arbitrary element. But

$$\sum_{i=1}^n (x_i/1) \cdot (1/w_i) = \frac{\sum_{i=1}^n x_i \widehat{w_i}}{\prod_{i=1}^n w_i} \in \{x/w \in W^{-1}R \mid x \in I\}.$$

□

Localization has a very controllable impact on the prime spectrum.

Proposition 7.10. *Suppose that R is a ring and $W \subseteq R$ is a multiplicative set. There is a canonical bijection:*

$$\left\{ \begin{array}{c} \textit{Primes } P \in \operatorname{Spec} R \\ \textit{such that } P \cap W = \emptyset. \end{array} \right\} \leftrightarrow \Big\{ \textit{Primes in } W^{-1}R \Big\}.$$

The bijection is simply

$$P \mapsto P(W^{-1}R).$$

Proof. Suppose P is such that $P \cap W = \emptyset$. First we show that $P(W^{-1}R)$ is prime. Suppose that $(r/w)(r'/w') \in P(W^{-1}R)$. This means that $\frac{rr'}{ww'} \in \{x/w \in W^{-1}R \mid x \in I\}$. Hence $\frac{rr'}{ww'} = x/u$ for some $x \in P$ and $u \in W$. It follows that there exists $v \in W$ such that $uvrr' = vww'x$. In particular, $uvrr' \in P$. But $u, v \notin P$ so $rr' \in P$ so that $r \in P$ or $r' \in P$. In the first case, $r/w \in P(W^{-1}R)$ and in the second $r'/w' \in P(W^{-1}R)$. This proves that $P(W^{-1}R)$ is prime or equal to $W^{-1}R$. Finally, if $1 = 1/1 \in P(W^{-1}R)$ then $vx \in W$ for some $v \in W$ and $x \in P$, which is impossible because $vx \in P$ since P is prime.

Now suppose that $Q \subseteq W^{-1}R$ is prime, set $P = \ell^{-1}(Q)$, a prime in R. We will show that $P(W^{-1}R) = Q$ which will show that our proposed bijection is at least surjective. Certainly $P(W^{-1}R) \subseteq Q$ so now choose $x/w \in Q \subseteq W^{-1}R$. Then $(w/1)(x/w) = x/1 \in Q$ and so $x \in P$. Hence $x/w \in P(W^{-1}R)$ which proves the other containment.

Finally, we prove injectivity. Suppose $P, P' \in \operatorname{Spec} R$ both have trivial intersection with W and that $P(W^{-1}R) = P'(W^{-1}R)$. In particular, for every $x \in P$, there exists $x' \in P'$ and $w' \in W$ such that $x/1 = x'/w'$. Then $vw'x = vx'$ for some $v \in W$ and so $vw'x \in P'$. Note that then $x \in P'$ since $vw' \in W$ and so not in P'. This proves that $P \subseteq P'$ which completes the proof by symmetry. $\square$

Corollary 7.11. *The primes of R that do not contain $x \in R$ are in bijective correspondence with the primes of $R_x = \{1, x, x^2, \ldots\}^{-1}R$. In other words,* $\operatorname{Spec} R_x$ *corresponds to* $(\operatorname{Spec} R) \setminus V(x)$.

Example 7.12. Suppose that R is a ring and $\langle x_1, x_2, \ldots \rangle = I \subseteq R$ is an ideal. We know $Z = V(I)$ is a closed subset of $X = \operatorname{Spec} R$ so that $X \setminus Z$ is open. It turns out that $X \setminus Z$ is covered by *affine* charts, $X_i = \operatorname{Spec}\{1, x_i, x_i^2, \ldots\}^{-1}R = \operatorname{Spec} R_{x_i}$ for each i, here $X_i = X \setminus V(x_i)$. Indeed, suppose that $P \in X = \operatorname{Spec} R$. If P is in $Z = V(I)$, then P contains each x_i, and so it does not correspond to any point in any of the X_i by Proposition 7.10. On the other hand, if P is not in Z, then P does not contain some x_i, and so P corresponds to a point in X_i.

Note that $X_i \cap X_j$ corresponds to $\operatorname{Spec}\{1, x_i x_j, x_i^2 x_j^2, \ldots\}^{-1}R$.

Example 7.13. Suppose that $P \subseteq R$ is a prime ideal and set $W = R \setminus P$. Then $W^{-1}R$ has a unique maximal prime ideal, $P(W^{-1}R)$. In this case, $W^{-1}R$ is denoted by R_P.

Definition 7.14. A *local ring* is a ring with a unique maximal ideal. For example each R_P is a local ring.

Geometrically, local rings some how contain only the data of functions passing through the unique maximal ideal (which is a point in the Spec).

8. Modules, localization of modules, and tensor products

We begin by introducing tensor products. Suppose that R is a ring and that M and N are R-modules.

Suppose we wish to multiply elements of m and n, formally, and consider the resulting as an R-module. The tensor product lets us do exactly that. In particular, the tensor product $M \otimes_R N$ is generated by elements $m \otimes n$. Note that in order for it to be a module, it has to be closed under addition, and so we

(i) have to allow finite sums $\sum_{i=1}^t m_i \otimes n_i$.

We also want our multiplication to be distributive, and so we must have

(ii) $(m + m') \otimes n = m \otimes n + m' \otimes n$ and $m \otimes (n + n') = m \otimes n + m \otimes n'$.

Finally, we need to describe our action of R on this product. We have

(iii) $(rm) \otimes n = m \otimes (rn) = r.(m \otimes n)$. In other words, only elements of R can move over the tensor product.

Elements of r of course must also distribute across sums:

(iv) $r. \sum_{i=1}^t m_i \otimes n_i = \sum_{i=1}^t (rm_i) \otimes n_i$

Formally, the tensor product $M \otimes_R N$ is the free Abelian group generated by all ordered pairs $m \otimes n := (m, n) \in M \times N$ modulo the relations generated by properties (ii) and (iii) above. It is an R-module if one distributes R across sums linearly as in (iv).

Proposition 8.1 (Universal property of the tensor product)**.** *If $f : M \oplus N \longrightarrow L$ is a bilinear map of R-modules, then then there exists a unique R-linear $\phi : M \otimes N \longrightarrow L$ such that $\phi(m \otimes n) = f(m, n)$. Note that the obvious map $M \oplus N \longrightarrow M \otimes N$ is bi-linear.*

Now suppose that $N = S$ is an R-algebra (a ring with map $R \longrightarrow S$). Then we will frequently form the tensor product $M \otimes_R S$. This is both an R-module and an S-module (S acts on S and extends linearly).

Definition 8.2 (Localization of a module)**.** Suppose now that R is a ring, W is a multiplicative system and M is an R-module. Then the localization $W^{-1}M$ is the set of pairs $(m, w) \in M \times W$ modulo the equivalence relation $(m, w) \sim (m', w')$ if there exists $v \in W$ such that $vw'm = vwm'$. Equivalence classes $[(m, w)]$ are denoted by m/w. $W^{-1}M$ becomes a $W^{-1}R$-module with the following addition and $W^{-1}R$-action.

$$\begin{array}{rcl} m/w + m'/w' & = & \frac{w'm+wm'}{ww'} \\ (r/w).(m/w') & = & rm/(ww') \end{array}$$

Proposition 8.3. *Suppose R is a ring, M is an R-module and W is a multiplicative system. Then:*

$$W^{-1}R \otimes_R M \cong W^{-1}M.$$

even as $W^{-1}R$-modules.

Proof of Proposition 8.3. The tensor product $W^{-1}R \otimes_R M$ is very simple as tensor products go. Indeed, notice that

$$\begin{array}{rl} & (r/w \otimes m) + (r'/w' \otimes m') \\ = & (\frac{rw'}{ww'} \otimes m) + (\frac{r'w}{ww'} \otimes m') \\ = & (\frac{1}{ww'} \otimes (rw'm)) + (\frac{1}{ww'} \otimes (r'wm')) \\ = & \frac{1}{ww'} \otimes (rw'm + r'wm'). \end{array}$$

It follows that every element of $W^{-1}R \otimes_R M$ can be expressed as $\frac{1}{w} \otimes m$. Since it is easy to see that the map $W^{-1}R \oplus M \longrightarrow W^{-1}M$, $(r/w, m) \mapsto rm/w$ is bilinear, by the universal property of the tensor product, we have a map

$$\phi : W^{-1}R \otimes M \longrightarrow W^{-1}M.$$

We need to show it is an isomorphism. Certainly it is surjective, so now choose $\frac{1}{w} \otimes m \in W^{-1}R$ and suppose that $\phi(\frac{1}{w} \otimes m) = m/w = 0$. Hence there exists $v \in W$ such that $vm = 0$. But then

$$\frac{1}{w} \otimes m = \frac{v}{wv} \otimes m = \frac{1}{wv} \otimes vm = \frac{1}{wv} \otimes 0 = 0.$$

Checking that the map is a $W^{-1}R$-module homomorphism is routine and will be left to the reader. □

There is one really useful fact about localization of modules.

Lemma 8.4. *Suppose that $\phi : M \longrightarrow N$ is an injective map of R-modules and $W \subseteq R$ is a multiplicative system, then the induced map*

$$\phi' : W^{-1}M \longrightarrow W^{-1}N$$

is also injective. Equivalently the induced map, $W^{-1}R \otimes_R M \longrightarrow W^{-1}R \otimes_R N$ is injective.

Proof. Ok, what do I mean by ϕ'? $\phi'(m/w) = \phi(m)/w$ (what else could it be?) Suppose that $\phi'(m/w) = \phi(m)/w = 0$. Hence there exists $v \in W$ such that $v\phi(m) = 0$. But $v\phi(m) = \phi(vm)$ so that $vm = 0$ since ϕ is injective. But then $0 = m/v \in W^{-1}M$. □

It is actually really uncommon that tensoring preserves injectivity (as we'll see in the next section). Modules L such that if $M \longrightarrow N$ is injective, then so is $L \otimes M \longrightarrow L \otimes N$ are called *flat*. Thus $W^{-1}R$ is a flat R-module.

What we have just done is a great example of a special type of tensor product called *extension of scalars*. Suppose M is an R-module, $R \longrightarrow S$ is a ring homomorphism, and we really want to make M into an S-module. The most obvious thing to do is $M \otimes_R S$. Then S can act on this tensor product on the right. For example, $\mathbb{R}[x] \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C}[x]$. Likewise $\mathbb{Z}[x] \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})[x]$.

Theorem 8.5. *Suppose that k is an algebraically closed field, and that R and S are two finite generated k algebras (in other words, $R = k[x_1, \dots, x_m]/I$ and $S = k[y_1, \dots, y_n]/J$. Then there is a natural bijection between m-$\operatorname{Spec} R \otimes_k S$, the maximal ideals of the ring $R \otimes_k S$, with $(m\text{-}\operatorname{Spec} R) \times (m\text{-}\operatorname{Spec} S)$.*

Proof. Consider maps $f : R \longrightarrow R \otimes_k S$ and $g : S \longrightarrow R \otimes_k S$ which sends $r \mapsto r \otimes 1$ and $s \mapsto 1 \otimes s$ respectively. This gives us a map $(f^{\#} \times g^{\#}) :$ m-$\operatorname{Spec}(R \otimes_k S) \longrightarrow (\text{m-}\operatorname{Spec} R) \times (\text{m-}\operatorname{Spec} S)$. We will call this map φ. We need to show it is bijective. We will use the letter A to denote the ring $R \otimes_k S$.

First we prove a lemma.

Lemma 8.6. *If $\mathfrak{m}$ is a maximal ideal of R and $\mathfrak{n}$ is a maximal ideal of S, then $\mathfrak{c} := \langle f(\mathfrak{m}) \rangle + \langle g(\mathfrak{n}) \rangle = \mathfrak{m}A + \mathfrak{n}A$ is a maximal ideal of A.*

Proof. Consider the map $f : R \longrightarrow A$ and apply the functor $R/\mathfrak{m} \otimes_R \bullet$, we obtain

$$f' : R/\mathfrak{m} \longrightarrow R/\mathfrak{m} \otimes_R (R \otimes_k S) \cong (R/\mathfrak{m} \otimes_R R) \otimes_k S \cong R/\mathfrak{m} \otimes_k S \cong S \cong A/(\mathfrak{m}A)$$

This map is injective because S is a free k-module (in fact every module over a vector space is free). Now consider the map $\rho \circ g : S \longrightarrow A \longrightarrow A/(\mathfrak{m}A)$ which is an isomorphism by above and tensor with $\bullet \otimes_S S/\mathfrak{n}$ and obtain the isomorphism

$$g'' : S/\mathfrak{n} \xrightarrow{\overline{\rho \circ g}} A/(\mathfrak{m}A) \otimes_S S/\mathfrak{n} \cong (R/\mathfrak{m} \otimes_k S/\mathfrak{n}) \cong k \cong A/(\mathfrak{m}A + \mathfrak{n}A)$$

Thus $A/(\mathfrak{m}A + \mathfrak{n}A)$ is a field and so $\mathfrak{m}A + \mathfrak{n}A$ is maximal. Now we return to our main proof. ☐

We continue our proof of Theorem 8.5. We first prove the injectivity so suppose that $\mathfrak{a}$ and $\mathfrak{b}$ are maximal ideals of $R \otimes_k S$ and that $\varphi(\mathfrak{a}) = \varphi(\mathfrak{b})$ (so $f^{-1}(\mathfrak{a}) = f^{-1}(\mathfrak{b})$ and likewise $g^{-1}(\mathfrak{a}) = g^{-1}(\mathfrak{b})$). Consider the ideal $\langle f(f^{-1}(\mathfrak{a})) \rangle + \langle g(g^{-1}(\mathfrak{a})) \rangle = \langle f(f^{-1}(\mathfrak{b})) \rangle + \langle g(g^{-1}(\mathfrak{b})) \rangle$. This is a maximal ideal, by the Lemma, contained inside both $\mathfrak{a}$ and $\mathfrak{b}$ and so the injectivity of φ is done.

Now we prove the surjectivity of φ. But this is easy since given $\mathfrak{m}$ and $\mathfrak{n}$ and constructing $\mathfrak{c}$ as in the lemma, it is clear that $f^{-1}(\mathfrak{c}) \supseteq \mathfrak{m}$ (and so we must have equality) and likewise for $\mathfrak{n}$. ☐

Example 8.7. When not working of finite type over an algebraically closed field, the above theorem fails. For example, $\mathbb{C}$ is a finitely generated $\mathbb{R}$-module, and $\operatorname{Spec} \mathbb{C}$ is a singleton. However, $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ has two points in its prime spectrum (this kind of behavior can also happen in number theoretic settings).

Example 8.8. $k[x] \otimes_k k[y] \cong k[x, y]$ (this is easy to see explicitly as well). Note that the Cartesian product only works for the maximal ideals.

We have a universal property for a tensor product of rings as well.

Proposition 8.9. *Suppose that A is a ring and that R and S are A-algebras (rings with maps $A \longrightarrow R$, $A \longrightarrow S$). Then for every other ring C with maps $f : R \longrightarrow C$ and $g : S \longrightarrow C$ making the diagram commute*

$$\begin{tikzcd}
C & & \\
& R \otimes_A S \arrow[ul, dotted, "\phi"'] & R \arrow[l, dotted] \arrow[ull, bend right] \\
& S \arrow[u, dotted] \arrow[uul, bend left] & A \arrow[l] \arrow[u]
\end{tikzcd}$$

there exists a unique map of rings ϕ as above making the diagram commute.

Proof. This follows easily from the other universal (bilinear) property for modules we already mentioned. $\square$

If we dualize the diagram, we have the following picture.

$$\begin{tikzcd}
\operatorname{Spec} C \arrow[dr, dotted] \arrow[drr, bend left] \arrow[ddr, bend right] & & \\
& \operatorname{Spec}(R \otimes_A S) \arrow[r, dotted] \arrow[d, dotted] & \operatorname{Spec} R \arrow[d] \\
& \operatorname{Spec} S \arrow[r] & \operatorname{Spec} A
\end{tikzcd}$$

The dual of the universal property is exactly the universal property of the fiber product for topological spaces (this works well for the $\mathfrak{m}$-Spec when we are finite type over an algebraically closed field A, in which case the fiber product is all pairs whose image is the same in $\operatorname{Spec} A$).

9. Localization and Hom

Definition 9.1. Recall an R-module L is called flat if $\bullet \otimes_R L$ is an exact functor (ie, it preserve injectivity). Remember $W^{-1}R$ is a flat R-module for any multiplicative set W.

Proposition 9.2. *If M is a finitely presented R-module (meaning it can be generated by finitely many elements subject to finitely many relations), N is any R-module and S is a flat R-algebra (in particular, it is an R-algebra which is flat as an R-module), then*

$$\operatorname{Hom}_R(M, N) \otimes_R S \longrightarrow \operatorname{Hom}_S(M \otimes_R S, N \otimes_R S)$$

is an isomorphism.

Proof. Since M is finitely presented, we can write an exact sequence

$$R^m \longrightarrow R^n \longrightarrow M \longrightarrow 0$$

Since S is flat, the functors $\mathrm{Hom}_R(\bullet, N) \otimes_R S$ and $\mathrm{Hom}_R(\bullet \otimes_R S, N \otimes_R S)$ are both left-exact. Hence we have the following diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}_R(M, N) \otimes_R S \arrow[r] \arrow[d, "f"'] & \mathrm{Hom}_R(R^m, N) \otimes_R S \arrow[r] \arrow[d, "g"'] & \mathrm{Hom}_R(R^m, N) \otimes_R S \arrow[d, "h"'] \\
0 \arrow[r] & \mathrm{Hom}_S(M \otimes_R S, N \otimes_R S) \arrow[r] \arrow[d, leftrightarrow, "\sim"] & \mathrm{Hom}_S(R^m \otimes_R S, N \otimes_R S) \arrow[r] \arrow[d, leftrightarrow, "\sim"] & \mathrm{Hom}_S(R^n \otimes_R S, N \otimes_R S) \arrow[d, leftrightarrow, "\sim"] \\
0 \arrow[r] & \mathrm{Hom}_S(M \otimes_R S, N \otimes_R S) \arrow[r] & \mathrm{Hom}_S(S^m, N \otimes_R S) \arrow[r] & \mathrm{Hom}_S(S^n, N \otimes_R S)
\end{tikzcd}$$

The bottom row of isomorphisms just comes from the fact that $R^a \otimes_R S = S^a$.

It is now straightforward to verify that the maps g and h are isomorphisms. Indeed, they are both homomorphisms from free modules and so you just need to decide where each basis element goes in each case (note $\mathrm{Hom}_R(R^a, M) = M^a$ as well). It follows that f is an isomorphism as well (it is two different ways to interpret the kernel of the same map). $\square$

Using the fact that localization can be written in terms of (flat) tensor product, we have that:

Corollary 9.3. *Suppose R is a ring, A is a finitely presented R-module and B is any R-module. If $W \subseteq R$ is any multiplicative set, then*

$$W^{-1}\,\mathrm{Hom}_R(A, B) \cong \mathrm{Hom}_{W^{-1}R}(W^{-1}A, W^{-1}B).$$

10. Noetherian rings

Definition 10.1. Suppose R is a ring. We say that R is *Noetherian* if its ideals satisfy the ascending chain condition. That is, if

$$I_1 \subseteq I_2 \subseteq \ldots$$

is an ascending chain of ideals, then $I_n = I_{n+1}$ for all $n \gg 0$.

Likewise we say that R is *Artinian* if its ideals satisfy the descending chain condition. That is if

$$I_1 \supseteq I_2 \supseteq \ldots$$

is a descending chain of ideals, then $I_n = I_{n+1}$ for all $n \gg 0$.

Lemma 10.2. *R is Noetherian if and only if every ideal of R is finitely generated.*

Proof. I leave it to you to write it down carefully. $\square$

Example 10.3. Clearly a field is both Artinian and Noetherian, but of course most rings we encounter are not Artinian. For instance $k[x]$ and $\mathbb{Z}$ are Noetherian but not Artinian.

Proposition 10.4. *Every Artinian ring is Noetherian (this is* NOT *true for modules).*

Proof. This is left as an exercise. (It will be a homework problem). $\square$

Next we prove Hilbert's basis theorem.

Theorem 10.5 (Hilbert's basis theorem)**.** *If R is Noetherian, then so is $R[x]$.*

Proof. Let $J \subseteq R[x]$ be an ideal. We need to show that J is finitely generated. Set $J_n = \{r \in R | rx^n + r_{n-1}x^{n-1} + \ldots + r_0 \in J \text{ for some } r_i \in R\}$. We note that J_n is an ideal of R. Furthermore, $J_n \subseteq J_{n+1}$ (since we can multiply elements of J by x and stay in J). Hence $J_n = J_{n+1}$ for all $n \geq n_0$.

For each $0 \leq i \leq n_0$ write $J_i = \langle r_{i,1}, \ldots r_{i,d}\rangle$ (we can use the same d for all if we desire). Choose $f_{i,j} \in J$ of degree i whose leading coefficient is $r_{i,j}$. We will show that $\langle \ldots, f_{i,j}, \ldots\rangle = J$. Now choose $f \in J$. We will show that $f \in \langle \ldots, f_{i,j}, \ldots\rangle$ by induction on $\deg f$ (degree 0 being obvious). Indeed, write $f = rx^n + \ldots$. Note that $r \in J_n$ and hence there exists $g \in \langle \ldots, f_{i,j}, \ldots\rangle$ with $g = rx^n + \ldots$. Thus $f - g \in J$ has lower degree and we are done. □

Corollary 10.6. *Finitely generated algebras over $\mathbb{Z}$ or a field k are Noetherian.*

Now we move on to modules.

Definition 10.7. We say that an R-module M is *Noetherian* if its submodules satisfy the ascending chain condition.

Note that submodules (and quotient modules) of Noetherian modules are clearly Noetherian.

Lemma 10.8. *M is Noetherian if and only if every submodule of M is finitely generated as an R-module.*

Proof. Obviously a Noetherian module is finitely generated. And if every submodule is finitely generated, the ascending chain condition holds by the usual argument. □

Lemma 10.9. *If $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ is a short exact sequence then B is Noetherian if and only if A and C are Noetherian.*

Proof. We only need to handle the ($\Rightarrow$) direction, the other containment is obvious. Suppose that $M \subseteq B$ is a submodule. Then $g(M)$ is a finitely generated submodule of C. Likewise, $f^{-1}(M) \subseteq A$ is finitely generated. But notice $0 \longrightarrow f^{-1}(M) \longrightarrow M \longrightarrow g(M) \longrightarrow 0$ is exact and so M is finitely generated by the homework problem. □

Corollary 10.10. *If R is a Noetherian ring, then R^n is a Noetherian module for every $n \geq 0$.*

Proof. We have short exact sequences $0 \longrightarrow R^i \longrightarrow R^{i+j} \longrightarrow R^j \longrightarrow 0$ and induction. □

Proposition 10.11. *Suppose R is a Noetherian ring. Then an R-module M is finitely generated if and only if it is Noetherian. In particular, every submodule of a finitely generated module over a Noetherian ring is finitely generated.*

Proof. We only have to show that if M is finitely generated then it is Noetherian. First since M is finitely generated there exists a surjection $R^n \longrightarrow M$. But then M is a quotient of a Noetherian module and hence Noetherian. $\square$

11. Homological algebra

We have so far seen several functors which are left or right exact, but not *exact*. For instance

- $\mathrm{Hom}_R(M, \_\_)$ is left exact
- $\mathrm{Hom}_R(\_\_, N)$ is left exact (although contravariant)
- $\otimes$ is right exact

It turns out there is a nice way to handle all these failures of exactness. Through the use of derived functors.

First a formality.

Definition 11.1. Suppose that $B^\bullet = \ldots \to B^{-1} \to B^0 \to B^1 \to B^2 \to \ldots$ is a complex (ie, $\ker(B_i \longrightarrow B_{i+1}) \supseteq \mathrm{im}(B_{i-1} \longrightarrow B_i)$). We define the ith cohomology of $B^\bullet$ to be

$$\mathbf{h}^i(B^\bullet) = \ker(B_i \longrightarrow B_{i+1}) / \mathrm{im}(B_{i-1} \longrightarrow B_i)$$

11.1. Tor.

Definition 11.2 (Projective resolutions)**.** Suppose R is a ring and M is an R-module. A projective resolution of M is a series of projective (ie free) modules P_i, $i = 0, -1, -2, \ldots$ and maps

$$\ldots \xrightarrow{f_n} P^{-n} \xrightarrow{f_{n-1}} P^{-n+1} \xrightarrow{f_{n-2}} \ldots \xrightarrow{f_2} P^{-2} \xrightarrow{f_1} P^{-1} \xrightarrow{f_0} P^0 \to M \longrightarrow 0$$

making the above sequence exact. Such a sequence could be infinite. Since every module is a quotient of a free (and hence projective) module, every module has a projective resolution (although not a unique one).

Definition 11.3 (Tor)**.** Suppose that $P^\bullet \longrightarrow M$ is a projective resolution of M. Note that for any module C, $P^\bullet \otimes C$ is a complex. We define $\mathrm{Tor}_i(M, C)$ to be $\mathbf{h}^i(P^\bullet \otimes C)$. It is not obvious that this is independent of the choice of projective resolution, but it is true (maybe we'll do this on a worksheet later).

It is easy to see that:

Lemma 11.4. $\mathrm{Tor}_0(M, C) \cong M \otimes C$. *Furthermore, if M is projective then* $\mathrm{Tor}_i(M, C) = 0$ *for all $i > 0$.*

One other fact that is useful, but which we won't prove in lecture is that

Lemma 11.5. $\mathrm{Tor}_i(M, C) \cong \mathrm{Tor}_i(C, M)$.

Now suppose that $0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$ is a short exact sequence. We form a projective resolutions of L and N to form the following:

$$\begin{tikzcd}
 & \cdots \arrow[d] & & \cdots \arrow[d] & \\
 & P'^{-2} \arrow[d] & & P''^{-2} \arrow[d] & \\
 & P'^{-1} \arrow[d] & & P''^{-1} \arrow[d] & \\
 & P'^{0} \arrow[d] & & P''^{0} \arrow[d] & \\
0 \arrow[r] & L \arrow[r] & M \arrow[r] & N \arrow[r] & 0
\end{tikzcd}$$

We set $P_i = P_i' \oplus P_i''$ with the canonical short exact sequences $0 \longrightarrow P_i' \longrightarrow P_i \longrightarrow P_i'' \longrightarrow 0$. We claim that these combine to form a commutative diagram

$$\begin{tikzcd}
 & \cdots \arrow[d] & \cdots \arrow[d] & \cdots \arrow[d] & \\
0 \arrow[r] & P'^{-2} \arrow[r] \arrow[d] & P^{-2} \arrow[r] \arrow[d] & P''^{-2} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & P'^{-1} \arrow[r] \arrow[d] & P^{-1} \arrow[r] \arrow[d] & P''^{-1} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & P'^{0} \arrow[r] \arrow[d] & P^{0} \arrow[r] \arrow[d] & P''^{0} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & L \arrow[r] & M \arrow[r] & N \arrow[r] & 0
\end{tikzcd}$$

where the columns form projective resolutions. This is pretty easy.

Now apply the functor $\otimes_R C$ for some module C to the resolutions $P^\bullet = \dots P^2 \to P^1 \to P^0$ (likewise with $P'^\bullet$ and $P''^\bullet$). We obtain

$$\begin{tikzcd}
 & \dots \arrow[d] & \dots \arrow[d] & \dots \arrow[d] & \\
0 \arrow[r] & P'^{-2} \otimes C \arrow[r] \arrow[d] & P^{-2} \otimes C \arrow[r] \arrow[d] & P''^{-2} \otimes C \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & P'^{-1} \otimes C \arrow[r] \arrow[d] & P^{-1} \otimes C \arrow[r] \arrow[d] & P''^{-1} \otimes C \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & P'^{0} \otimes C \arrow[r] \arrow[d] & P^{0} \otimes C \arrow[r] \arrow[d] & P''^{0} \otimes C \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & 0
\end{tikzcd}$$

We now apply the snake lemma, first to the diagram

$$\begin{tikzcd}
 & P'^{-1} \otimes C/\operatorname{im}(P'^{-2} \otimes C) \arrow[r] \arrow[d] & P^{-1} \otimes C/\operatorname{im}(P^{-2} \otimes C) \arrow[r] \arrow[d] & P''^{-1} \otimes C/\operatorname{im}(P''^{-2} \otimes C) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & P'^{0} \otimes C \arrow[r] & P^{0} \otimes C \arrow[r] & P''^{0} \otimes C \arrow[r] & 0
\end{tikzcd}$$

The cokernel below the bottom row is simply

$$L \otimes C \longrightarrow M \otimes C \longrightarrow N \otimes C \longrightarrow 0$$

but this snakes up and connects with the kernels above the top row, which are

$$\operatorname{Tor}_1(L, C) \longrightarrow \operatorname{Tor}_1(M, C) \longrightarrow \operatorname{Tor}_1(N, C)$$

connecting these we get a long exact sequence

$$\operatorname{Tor}_1(L, C) \longrightarrow \operatorname{Tor}_1(M, C) \longrightarrow \operatorname{Tor}_1(N, C) \longrightarrow L \otimes C \longrightarrow M \otimes C \longrightarrow N \otimes C \longrightarrow 0.$$

But we don't stop now. We next consider the diagram:

$$\begin{tikzcd}
 & P'^{-2} \otimes C/\operatorname{im}(P'^{-3} \otimes C) \arrow[r] \arrow[d] & P^{-2} \otimes C/\operatorname{im}(P^{-3} \otimes C) \arrow[r] \arrow[d] & P''^{-2} \otimes C/\operatorname{im}(P''^{-3} \otimes C) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \ker(P'^{-1} \otimes C \to P'^{0} \otimes C) \arrow[r] & \ker(P^{-1} \otimes C \to P^{0} \otimes C) \arrow[r] & \ker(P''^{-1} \otimes C \to P''^{0} \otimes C) &
\end{tikzcd}$$

applying the snake lemma again gets us to the long exact sequence

$$\begin{array}{ccccccc}
 & & & & \dots & \longrightarrow & \\
\operatorname{Tor}_2(L, C) & \longrightarrow & \operatorname{Tor}_2(M, C) & \longrightarrow & \operatorname{Tor}_2(N, C) & \longrightarrow & \\
\operatorname{Tor}_1(L, C) & \longrightarrow & \operatorname{Tor}_1(M, C) & \longrightarrow & \operatorname{Tor}_1(N, C) & \longrightarrow & \\
L \otimes C & \longrightarrow & M \otimes C & \longrightarrow & N \otimes C & \longrightarrow & 0.
\end{array}$$

11.2. **Ext.** We first consider the functor $\operatorname{Hom}_R(\_\_, C)$.

Definition 11.6. If $P^\bullet$ is a projective resolution of M, then we define $\operatorname{Ext}^i(M, C)$ to be $\mathbf{h}^i(\operatorname{Hom}_R(P^\bullet, C))$, the ith cohomology of the complex $\operatorname{Hom}_R(P^\bullet, C)$.

Given a short exact sequence

$$0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$$

as above, we again form projective resolutions

$$\begin{array}{ccccccccc}
 & & \cdots & & \cdots & & \cdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P'^{-2} & \longrightarrow & P^{-2} & \longrightarrow & P''^{-2} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P'^{-1} & \longrightarrow & P^{-1} & \longrightarrow & P''^{-1} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P'^{0} & \longrightarrow & P^{0} & \longrightarrow & P''^{0} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & L & \longrightarrow & M & \longrightarrow & N & \longrightarrow & 0
\end{array}$$

and apply the functor $\operatorname{Hom}_R(\_\_, C)$ to the projective resolutions to obtain:

$$\begin{array}{ccccccccc}
 & & \cdots & & \cdots & & \cdots & & \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longleftarrow & \operatorname{Hom}_R(P'^{-2}, C) & \longleftarrow & \operatorname{Hom}_R(P^{-2}, C) & \longleftarrow & \operatorname{Hom}_R(P''^{-2}, C) & \longleftarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longleftarrow & \operatorname{Hom}_R(P'^{-1}, C) & \longleftarrow & \operatorname{Hom}_R(P^{-1}, C) & \longleftarrow & \operatorname{Hom}_R(P''^{-1}, C) & \longleftarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longleftarrow & \operatorname{Hom}_R(P'^{0}, C) & \longleftarrow & \operatorname{Hom}_R(P^{0}, C) & \longleftarrow & \operatorname{Hom}_R(P''^{0}, C) & \longleftarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longleftarrow & 0 & \longleftarrow & 0 & \longleftarrow & 0 & \longleftarrow & 0
\end{array}$$

Applying the same snake lemma formalisms again, we note that we have diagrams

$$\begin{array}{ccccccc}
\ker\begin{pmatrix}\operatorname{Hom}_R(P'^{-i-1}, C) \\ \longrightarrow \\ \operatorname{Hom}_R(P'^{-i-2}, C)\end{pmatrix} & \longleftarrow & \ker\begin{pmatrix}\operatorname{Hom}_R(P^{-i-1}, C) \\ \longrightarrow \\ \operatorname{Hom}_R(P^{-i-2}, C)\end{pmatrix} & \longleftarrow & \ker\begin{pmatrix}\operatorname{Hom}_R(P''^{-i-1}, C) \\ \longrightarrow \\ \operatorname{Hom}_R(P''^{-i-2}, C)\end{pmatrix} & \longleftarrow & 0 \\
\uparrow & & \uparrow & & \uparrow & & \\
0 \leftarrow \operatorname{Hom}_R(P'^{-i}, C)/\operatorname{im}(\operatorname{Hom}_R(P'^{-i+1}, C)) & \leftarrow & \operatorname{Hom}_R(P^{-i}, C)/\operatorname{im}(\operatorname{Hom}_R(P^{-i+1}, C)) & \leftarrow & \operatorname{Hom}_R(P''^{-i}, C)/\operatorname{im}(\operatorname{Hom}_R(P''^{-i+1}, C)) & &
\end{array}$$

The snake lemma yields the following long exact sequence.

$$\begin{array}{rcccc} 0 \longrightarrow & \mathrm{Hom}_R(N, C) & \longrightarrow & \mathrm{Hom}_R(M, C) & \longrightarrow & \mathrm{Hom}_R(L, C) \\ \longrightarrow & \mathrm{Ext}^1_R(N, C) & \longrightarrow & \mathrm{Ext}^1_R(M, C) & \longrightarrow & \mathrm{Ext}^1_R(L, C) \\ \longrightarrow & \mathrm{Ext}^2_R(N, C) & \longrightarrow & \dots & & \end{array}$$

However, there isn't just one Ext functor... We also have $\mathrm{Hom}_R(B, \_\_)$. Projective resolutions just aren't good enough any more. We need

Definition 11.7 (Injective resolutions)**.** Suppose that M is a module. We say that

$$\Big(0 \longrightarrow M \longrightarrow I^\bullet\Big) = \Big(0 \longrightarrow M \longrightarrow I^0 \longrightarrow I^1 \longrightarrow I^2 \longrightarrow\Big)$$

is an injective resolution if each I^i is an injective module and the above sequence is a long exact sequence. It is a non-trivial fact that injective resolutions exist (to show it, it is enough to show that for every module N, there is an injective module and an injection $N \hookrightarrow I$, we may do this in a worksheet/homework).

Definition 11.8. Fix $I^\bullet$ to be an injective resolution of a module M and let $\mathrm{Hom}_R(B, I^\bullet)$ be the corresponding complex. Then we define $\mathrm{Ext}^i_R(B, M)$ to be $\mathbf{h}^i(\mathrm{Hom}_R(B, I^\bullet))$.

There are a couple key facts we won't prove in lecture.

- This Ext is also independent of the choice of injective resolution.
- This Ext agrees with the other Ext we defined (which is really useful!) In other words

$$\mathbf{h}^i(\mathrm{Hom}_R(B, I^\bullet)) \cong \mathbf{h}^i(\mathrm{Hom}_R(P^\bullet, M))$$

  where $I^\bullet$ is an injective resolution of M and $P^\bullet$ is a projective resolution of B.

Again, given $0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$ we can form injective resolutions of L and N and take the direct sum to get an injective resolution of M and so have

$$\begin{tikzcd} & \dots & \dots & \dots & \\ 0 \arrow[r] & I'^2 \arrow[r] \arrow[u] & I^2 \arrow[r] \arrow[u] & I''^2 \arrow[r] \arrow[u] & 0 \\ 0 \arrow[r] & I'^1 \arrow[r] \arrow[u] & I^1 \arrow[r] \arrow[u] & I''^1 \arrow[r] \arrow[u] & 0 \\ 0 \arrow[r] & I'^0 \arrow[r] \arrow[u] & I^0 \arrow[r] \arrow[u] & I''^0 \arrow[r] \arrow[u] & 0 \\ 0 \arrow[r] & L \arrow[r] \arrow[u] & M \arrow[r] \arrow[u] & N \arrow[r] \arrow[u] & 0 \end{tikzcd}$$

We can apply the covariant functor $\mathrm{Hom}_R(B, \_\_)$ to the I parts and obtain:

$$\begin{tikzcd}
 & \cdots & \cdots & \cdots & \\
0 \arrow[r] & \mathrm{Hom}_R(B, I'^2) \arrow[r] \arrow[u] & \mathrm{Hom}_R(B, I^2) \arrow[r] \arrow[u] & \mathrm{Hom}_R(B, I''^2) \arrow[r] \arrow[u] & 0 \\
0 \arrow[r] & \mathrm{Hom}_R(B, I'^1) \arrow[r] \arrow[u] & \mathrm{Hom}_R(B, I^1) \arrow[r] \arrow[u] & \mathrm{Hom}_R(B, I''^1) \arrow[r] \arrow[u] & 0 \\
0 \arrow[r] & \mathrm{Hom}_R(B, I'^0) \arrow[r] \arrow[u] & \mathrm{Hom}_R(B, I^0) \arrow[r] \arrow[u] & \mathrm{Hom}_R(B, I''^0) \arrow[r] \arrow[u] & 0 \\
0 \arrow[r] & 0 \arrow[r] \arrow[u] & 0 \arrow[r] \arrow[u] & 0 \arrow[r] \arrow[u] & 0
\end{tikzcd}$$

The rows are exact and the columns are complexes. Using the snake lemma as before gives us a long exact sequence

$$\begin{array}{ccccccc}
0 & \to & \mathrm{Hom}_R(B, L) & \to & \mathrm{Hom}_R(B, M) & \to & \mathrm{Hom}_R(B, N) \\
 & \to & \mathrm{Ext}^1_R(B, L) & \to & \mathrm{Ext}^1_R(B, M) & \to & \mathrm{Ext}^1_R(B, N) \\
 & \to & \mathrm{Ext}^2_R(B, L) & \to & \mathrm{Ext}^2_R(B, M) & \to & \mathrm{Ext}^2_R(B, N) \\
 & \to & \cdots & & & &
\end{array}$$