

## CLASS NOTES

These are my notes for Math 210a as taught by Professor Richard Taylor in Fall 2022. The course is an introduction to abstract algebra, as meant to prepare for quals, and covers rings, category theory, modules, and homological algebra.

These notes are entirely written by me, and all pictures are either diagrams I made using [quiver](#) or pictures I drew during class, though credit goes to Bradley Moon for sending me content for the lectures that I missed!

Please let me know if you find any errors, typos, or unclear information in these notes - you can contact me at `atalati [at] stanford.edu`.

## TABLE OF CONTENTS

Lecture 1 :	Rings, I	page 3
Lecture 2 :	Rings, II	page 7
Lecture 3 :	Rings, III	page 12
Lecture 4 :	More on Ideals	page 17
Lecture 5 :	Rings, IV	page 21
Lecture 6 :	Fraction Rings, cont'd	page 27
Lecture 7 :	Tensor Products	page 31
Lecture 8 :	Factorization in Rings	page 37
Lecture 9 :	Factorization in Rings, II	page 41
Lecture 10:	Category Theory, I	page 45
Lecture 11:	Category Theory, II	page 50
Lecture 12:	Category Theory, III	page 55
Lecture 13:	Modules, I	page 59
Lecture 14:	Modules, II	page 64
Lecture 15:	Modules, III	page 69
Lecture 16:	Tensor Products of Modules, I	page 73
Lecture 17:	Tensor Products of Modules, II	page 77
Lecture 18:	Tensor Products of Modules, III	page 82
Lecture 19:	Finitely Generated Modules Over a PID	page 87
Lecture 20:	Finitely Generated Vector Spaces	page 92
Lecture 21:	Proof of the Structure Theorem	page 97
Lecture 22:	Additive Categories, Abelian Categories, and Sheaves	page 102
Lecture 23:	Exact Sequences in Abelian Categories	page 108
Lecture 24:	Projectives and Injectives	page 115
Lecture 25:	Maps Between Complexes	page 120
Lecture 26:	Sequences of Complexes	page 125
Lecture 27:	Sequences of Complexes, II	page 129
Lecture 28:	Right Derived Functors	page 134
Lecture 29:	Ext Functors	page 138
Lecture 30:	Tor Functors	page 141
Appendix A :	Tensor Products Review	page 145

## LECTURE 1: RINGS, I

We are going to go very quickly over rings, as presumably many people have seen this content before. If you would like a refresher on rings, there are notes on the Canvas page for review.

**Definition 1.1.** A **ring** is a set  $R$ , with two elements, 0 and 1, identified, and with two operations, denoted  $+$  and  $\cdot$ .

Furthermore,  $(R, +, 0)$  is an abelian group, where we use  $(-r)$  to denote the additive inverse of any  $r \in R$ .

Moreover,  $\cdot$  is associative and commutative, and the ring has a multiplicative identity of 1 (and it is closed under multiplication).

Finally, the distributive property holds: for any  $r, s, t \in R$ ,

$$r \cdot (s + t) = r \cdot s + r \cdot t.$$

Some people would consider the above to be the definition of “commutative rings with 1,” but for this course we will assume all rings are commutative and have 1.

**Example 1.2.** Some examples of rings are:

- the zero ring  $\{0\}$
- $\mathbb{Z}$
- $\mathbb{Q}$
- $\mathbb{R}$
- $\mathbb{C}$
- $\mathbb{Z}/n\mathbb{Z}$
- $C[0, 1]$  (continuous functions  $f : [0, 1] \rightarrow \mathbb{C}$ , where addition and multiplication are done pointwise)
- $\{(a, b) \in \mathbb{Z}^2 \mid a \equiv b \pmod{3}\}$  where addition and multiplication are done componentwise

**Exercise 1.3.** Convince yourself that:

For all  $r \in R$ ,  $-r = -1 \cdot r$ .

For all  $r \in R$ ,  $r \cdot 0 = 0$ .

If  $0 = 1 \in R$ , then  $R = \{0\}$ .

**Definition 1.4.** We say that

$$R^\times = \{r \in R \mid \exists s \in R \text{ such that } r \cdot s = 1\}$$

is the **group of units** of  $R$ .

**Exercise 1.5.** Convince yourself that for any  $r \in R$ , if such an  $s$  exists, it is unique.

**Example 1.6.** Some examples of the group of units are:

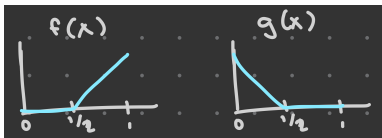
- $\mathbb{Z}^\times = \{\pm 1\}$
- $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$
- $C[0, 1]^\times =$  the set of nowhere-zero functions

**Definition 1.7.** An element  $r \in R$  is **nilpotent** if there is some positive integer  $n$  such that  $r^n = 0$ .

**Example 1.8.** In  $\mathbb{Z}/4\mathbb{Z}$ ,  $2^2 = 4 = 0$ .

**Definition 1.9.** An element  $r \in R$  is a **zero divisor** if there exists a nonzero  $s \in R$  such that  $r \cdot s = 0$ .

**Example 1.10.** In  $C[0, 1]$ , the following functions are zero divisors (we can see that  $f(x)g(x) = 0$ , but neither function is the zero function):



**Definition 1.11.** A ring  $R$  is **reduced** if 0 is the only nilpotent element.

**Definition 1.12.** A ring  $R$  is an **integral domain** if the set of zero divisors in  $R$  is exactly  $\{0\}$ .

**Definition 1.13.** A ring  $R$  is a **field** if  $R^\times = R \setminus \{0\}$ .

If  $R$  is a field then it is an integral domain (since units cannot be zero divisors - convince yourself of this).  
If  $R$  is an integral domain then it is reduced, since all nilpotent elements are zero divisors.

**Example 1.14.**

- $\mathbb{Z}$  is an integral domain
- $\mathbb{Q}$  is a field
- $\mathbb{Z}/6\mathbb{Z}$  is reduced
- $\mathbb{Z}/4\mathbb{Z}$  is *not* reduced
- $\{0\}$  is reduced (It is not a field because  $R^\times$  contains 0 and it is not an integral domain because 0 is not a zero divisor.)

**Definition 1.15.** A map  $\phi : R \rightarrow S$  is a **ring (homo)morphism** if it “preserves the ring structure” so that:

- $\phi(0) = 0$
- $\phi(1) = 1$
- for all  $r, s \in R$ ,  $\phi(r + s) = \phi(r) + \phi(s)$
- for all  $r, s \in R$ ,  $\phi(r \cdot s) = \phi(r) \cdot \phi(s)$

**Exercise 1.16.** Convince yourself that the last point implies that  $\phi(-r) = -\phi(r)$  for all  $r \in R$ .

**Example 1.17.**

- the natural inclusion  $\mathbb{Z} \hookrightarrow \mathbb{C}$
- for any point  $t \in [0, 1]$ , the map  $C[0, 1] \rightarrow \mathbb{C}$  defined by  $f \mapsto f(t)$
- the natural inclusion  $\{0\} \hookrightarrow \mathbb{Z}$  is *NOT* a ring homomorphism, since  $\phi(1) \neq 1$
- for any ring  $R$ , there is a unique homomorphism  $R \rightarrow \{0\}$  defined by  $r \mapsto 0$  for all  $r \in R$
- for any ring  $R$ , there is a unique homomorphism  $\mathbb{Z} \rightarrow R$  where:

$$\rightarrow \phi(0) = 0$$

$$\rightarrow \text{for positive } n \in \mathbb{Z}, \phi(n) = \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}$$

$$\rightarrow \text{for positive } n \in \mathbb{Z}, \phi(-n) = - \left( \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} \right)$$

**Definition 1.18.** For rings  $S$ ,  $R \subset S$  is a **subring** if  $R$  is a ring (so it is closed under addition, multiplication, and additive inverses) and  $R$  contains 0 and 1.

Some ways of constructing new rings:

**Definition 1.19.** The **product** of two rings  $R$  and  $S$  is defined to be

$$R \times S = \{(r, s) \mid r \in R, s \in S\},$$

where addition and multiplication is defined componentwise (so the additive identity is  $(0, 0)$  and the multiplicative identity is  $(1, 1)$ ).

Note that the product induces natural morphisms:

$$\begin{array}{ll} \pi_1 : R \times S \rightarrow R & \pi_2 : R \times S \rightarrow S \\ (r, s) \mapsto r & (r, s) \mapsto s \end{array}$$

However, there aren't natural morphisms in the opposite direction, for example:

**Example 1.20.** The map

$$\begin{array}{l} \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z} \\ n \mapsto (n, 0) \end{array}$$

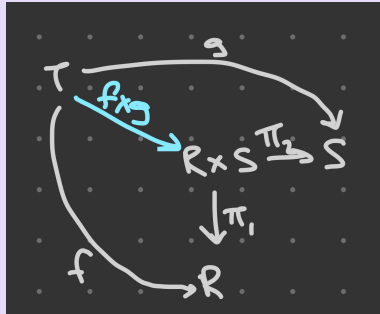
is *not* a ring morphism because 1 doesn't map to  $(1, 1)$ .

**Lemma 1.21.** If  $T$  is a ring and  $f : T \rightarrow R$  and  $g : T \rightarrow S$  are ring morphisms, then there exists a unique  $f \times g : T \rightarrow R \times S$  such that

$$\pi_1 \circ (f \times g) = f$$

$$\pi_2 \circ (f \times g) = g.$$

We say that the following diagram commutes:



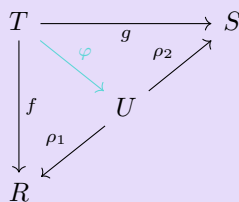
Note that the above property uniquely characterizes the product, in the sense that if we have some ring  $U$  with this property,  $U \cong R \times S$ . We will state this more rigorously and prove it next time.

## LECTURE 2: RINGS, II

As a reminder, we left of last lecture by defining a universal property of the product. We will now prove that this uniquely characterizes the product; this proof is important mainly because we will see many proofs using the same sort of argument throughout this course.

**Lemma 2.1.** Suppose there exists some ring  $U$  with morphisms  $\rho_1 : U \rightarrow R$  and  $\rho_2 : U \rightarrow S$  with the same property:

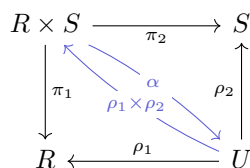
For any ring  $T$  with ring morphisms  $f : T \rightarrow R$  and  $g : T \rightarrow S$ , there exists a unique  $\varphi$  such that



this diagram commutes.

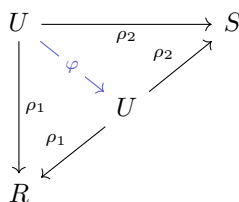
Then  $U \cong R \times S$ .

*Proof.* By applying this property of  $U$ , taking  $T = R \times S$  we get that there is a unique  $\alpha$  such that the below diagram commutes; by applying the property of  $R \times S$ , taking  $T = U$ , we get that there is a unique  $\rho_1 \times \rho_2$  such that the below diagram commutes:



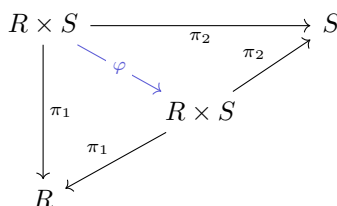
So we have homomorphisms from  $R \times S$  to  $U$  and from  $U$  to  $R \times S$ ; we need to show that they are isomorphisms.

By applying the universal property to the following commutative diagram:



we know there must be a unique  $\varphi$  that makes the diagram commute. But (check this!) taking  $\varphi = \text{id}_U$  and  $\varphi = \alpha \circ (\rho_1 \times \rho_2)$  both work, so we get that  $\alpha \circ (\rho_1 \times \rho_2) = \text{id}_U$ .

Similarly, we can apply the universal property to the following commutative diagram



and see that  $\varphi = (\rho_1 \times \rho_2) \circ \alpha$  and  $\varphi = \text{id}_{R \times S}$  both work, so by uniqueness,  $\text{id}_{R \times S} = (\rho_1 \times \rho_2) \circ \alpha$ .

Thus, these two maps are inverses of each other, so they are isomorphisms, and  $U \cong R \times S$ .  $\square$

Note that  $\alpha$  is the canonical isomorphism we would come up with when mapping  $U \rightarrow R \times S$ ; in fact, it is the unique isomorphism  $U \rightarrow R \times S$  with the property that

$$\begin{aligned}\rho_1 \circ \alpha &= \pi_1 \\ \rho_2 \circ \alpha &= \pi_2.\end{aligned}$$

We can construct larger products too:

**Definition 2.2.** For any (even infinite) index set  $I$  where we have a ring  $R_i$  for each  $i \in I$ , we can construct the product  $\prod_i R_i$  in the same way.

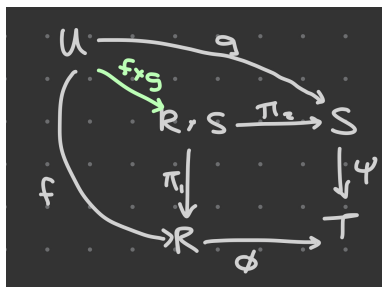
In fact, it can be shown that this larger product has all the same properties we just showed, but this is kind of tedious, so we won't show this in class.

**Definition 2.3.** For any rings  $R, S, T$  and homomorphisms  $\phi : R \rightarrow T$  and  $\psi : S \rightarrow T$ , we can form the **relative product**

$$R \times_T S = \{(r, s) \in R \times S \mid \phi(r) = \psi(s)\}.$$

This is a subring of  $R \times S$ .

The relative product has the universal property that for any ring  $U$  and homomorphisms  $f : U \rightarrow R$  and  $g : U \rightarrow S$ , such that  $\phi \circ f = \psi \circ g$ , there exists a unique  $f \times g$  such that



the above diagram commutes.

**Example 2.4.** The ring  $\{(a, b) \in \mathbb{Z}^2 \mid a \equiv b \pmod{3}\}$  that we mentioned last time is actually the relative product

$$\mathbb{Z} \times_{\mathbb{Z}/3\mathbb{Z}} \mathbb{Z}.$$

The second way of constructing new rings is polynomial rings.

This is a bit tedious to set up fully formally, but you can check the notes for a formal treatment.

If we have indeterminates  $x_i : i \in I$ , we can form monomials of the form  $x_{i_1}^{n_1} x_{i_2}^{n_2} \cdots x_{i_k}^{n_k}$ , where  $n_1, \dots, n_k$  are nonnegative integers.

**Definition 2.5.** For rings  $R$ ,  $R[x_i]_{i \in I}$  is a **polynomial ring**, and it is the set of all formal finite sums of an element of  $R$  times a monomial.

**Example 2.6.** An element of  $\mathbb{Z}[x_i]_{i \in I}$  could look like  $x_1 + 2x_1^2 x_2$ .



**Definition 2.7.** For rings  $R$ ,  $R[[x_i]]_{i \in I}$  is the set of **formal power series**, which is the same as the polynomial ring, except we allow infinite sums. This is also a ring.

Note that we always have the trivial embedding

$$\begin{aligned} R &\hookrightarrow R[[x_i]]_{i \in I} \\ r &\mapsto r \cdot 1 \end{aligned}$$

**Definition 2.8.** For any polynomial  $f(x) \in R[x]$ , we define the **degree** of  $f$  (which is  $-\infty$  or a nonnegative integer) to be:

$$\begin{aligned} \deg 0 &= -\infty \\ \deg(a_0 + a_1x + \cdots + a_dx^d) &= d \text{ if } a_d \neq 0. \end{aligned}$$

**Lemma 2.9.** If  $R$  is an integral domain, then for all  $f(x), g(x) \in R[x]$   $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$ .

When not in an integral domain, this can fail:

**Example 2.10.** In  $\mathbb{Z}/6\mathbb{Z}[x]$ ,  $\deg(2x + 1) + \deg(3x + 1) = 2$  but

$$(2x + 1)(3x + 1) = 6x^2 + 5x + 1 = 5x + 1,$$

so  $\deg((2x + 1)(3x + 1)) = 1$ .

**Lemma 2.11.** If  $R$  is an integral domain then so is  $R[x]$  and  $R[x_i]_{i \in I}$  and  $R[[x_i]]_{i \in I}$ .

All of these follow from the previous lemma, besides that in the  $R[[x_i]]_{i \in I}$  case, where our elements don't have finite degree, so we instead work with the coefficient of the *smallest* power of  $x$ .

The universal property of polynomial rings is:

Suppose  $I$  is an index set and  $S$  is a ring, and  $f : I \rightarrow S$  is any function. Moreover, suppose  $\phi : R \rightarrow S$  is a morphism. Then, there exists a unique morphism  $\psi : R[x_i]_{i \in I} \rightarrow S$  such that  $\psi|_R = \phi$  and for each  $i \in I$ ,  $\psi(x_i) = f(i)$ .

**Definition 2.12.** For any polynomial  $f(x) \in R[x]$ , if

$$f(x) = c_0 + c_1x + \cdots + c_dx^d \quad c_d \neq 0,$$

we say that  $c_d$  is the **leading term**. If the leading term is 1, we say the polynomial is **monic**.

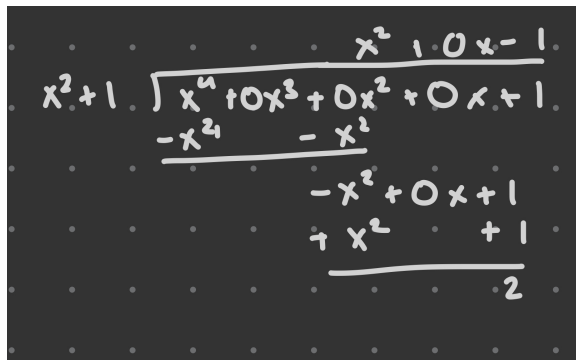
**Lemma 2.13** (“division algorithm”). If we have polynomials  $f(x), g(x) \in R[x]$  and  $g(x)$  is monic (or has a unit leading term), then there exists a unique  $q(x), r(x) \in R[x]$  such that

$$f(x) = q(x)g(x) + r(x)$$

and  $\deg(r) < \deg(g)$ .

The proof of this is just long division; we will look at an example:

**Example 2.14.** In  $\mathbb{Z}[x]$ , we can take  $f(x) = x^4 + 1$  and  $g(x) = x^2 + 1$ . Then, we have the following division:



$$\begin{array}{r}
 x^2 + 1 \overline{) x^4 + 0x^3 + 0x^2 + 0x + 1} \\
 \underline{-x^2} \phantom{+ 0x} \phantom{+ 1} \\
 -x^2 + 0x + 1 \\
 \underline{+x^2} \phantom{+ 0x} \phantom{+ 1} \\
 2
 \end{array}$$

so  $q(x) = x^2 - 1$  and  $r(x) = 2$ .

The third way to construct new rings is quotients.

To talk about quotients we first need to talk about ideals.

**Definition 2.15.** We call  $I \subset R$  an **ideal** of  $R$  if

- $0 \in I$
- for all  $r, s \in I$ ,  $r + s \in I$
- for all  $r \in R$  and  $s \in I$ ,  $rs \in I$

We denote this by saying  $I \triangleleft R$ .

**Definition 2.16.** An ideal is **proper** if  $I \subsetneq R$ .

We have the following examples of ideals:

**Example 2.17.**

- For any ring  $R$ ,  $\{0\} \triangleleft R$ ,  $R \triangleleft R$
- $(2) = \{\text{all even integers}\} \triangleleft \mathbb{Z}$
- if  $\phi : R \rightarrow S$  is a morphism and  $J \triangleleft S$ , then

$$\phi^{-1}(J) = \{r \in R \mid \phi(r) \in J\} \triangleleft R.$$

Specifically,  $\ker \phi = \phi^{-1}(0) \triangleleft R$ .

In general this is not true the other way around; for example, the image of  $(2) \triangleleft \mathbb{Z}$  in the natural inclusion  $\mathbb{Z} \hookrightarrow \mathbb{Q}$  is **not** an ideal of  $\mathbb{Q}$  since  $1/2(2) = 1$  is not an element of this image.

However, if  $\phi : R \rightarrow S$  is a *surjective* homomorphism and  $I \triangleleft R$ , then  $\phi(I) \triangleleft S$ .

**Definition 2.18.** If  $X \subset R$  is a general subset, then **the ideal generated by  $X$**  is

$$(X) = \left\{ \sum_{i=1}^n r_i x_i \mid r_i \in R, x_i \in X \right\} \triangleleft R.$$

**Exercise 2.19.** Any ideal  $I \triangleleft R$  that contains  $X$  must contain  $(X)$  as well.

## LECTURE 3: RINGS, III

Consider ideals  $I, J \triangleleft R$ . We can use these to construct the following ideals:

**Definition 3.1.** The **sum**

$$I + J = \{r + s \mid r \in I, s \in J\}$$

is an ideal and it is the smallest ideal containing  $I \cup J$ , so we can denote it  $(I \cup J)$ .

**Exercise 3.2.** The intersection  $I \cap J$  is an ideal.

**Definition 3.3.** The **product**

$$IJ = \left\{ \sum_{i=1}^n r_i s_i \mid r_i \in I, s_i \in J \right\}$$

is an ideal, and it is contained in  $I \cap J$ .

**Example 3.4.** Consider the ring  $R = \mathbb{Z}$  and the ideals  $I = (6)$  and  $J = (10)$ . Then

$$(6) + (10) = (2)$$

$$(6) \cap (10) = (30)$$

$$(6)(10) = (60)$$

**Remark 3.5.** As a heuristic, using the example of ideals of  $\mathbb{Z}$ , we can think of:

- $I \supset J$  as something like “ $I \mid J$ ”
- $I + J$  as something like “ $\gcd(I, J)$ ”
- $I \cap J$  as something like “ $\text{lcm}(I, J)$ ”
- $IJ$  as something like “ $IJ$ ”

This is a heuristic because the operations on the right are (mostly) not well-defined for ideals.

**Definition 3.6.** We call  $I, J \triangleleft R$  **comaximal** if  $I + J = R$ , or equivalently, that there exists some  $r \in I, s \in J$  such that  $r + s = 1$ .

**Remark 3.7.** As a heuristic, we can think of comaximality as something like “relatively prime.”

**Lemma 3.8.**

1. If  $I \triangleleft \mathbb{Z}$  then  $I = (n)$  for some  $n \in \mathbb{Z}$ .
2. If  $K$  is a field and  $I \triangleleft K[x]$  then  $I = (f)$  for some  $f \in K[x]$ .

*Proof.*

1. If  $I = (0)$  then it is clearly generated by one element and we are done.

If not, then  $I$  contains some nonzero element, and multiplying by  $-1$  if necessary, it contains some positive element. Let  $n > 0$  be the smallest positive element of  $I$ ; we can see that  $I \supseteq (n)$ . Then, consider any  $m \in I$ .

By the division algorithm,  $m = qn + r$ , for some  $0 \leq r < n$ . But we can see that  $r = m - qn$ , so it is an element of the ideal, which means  $r = 0$  to not contradict the minimality of  $n$ . Then, we have  $m = qn$ , so  $m \in (n)$ , and since this is true for any  $m \in I$ ,  $I = (n)$ .

2. The proof is very similar. If  $I = (0)$  then it is clearly generated by one element and we are done.

If not, then  $I$  contains some nonzero element. Let  $f(x) \neq 0$  be an element of  $I$  of minimal degree. We can make  $f(x)$  monic by multiplying by the inverse of the leading term, since  $K$  is a field. Moreover, we can see that  $I \supseteq (f)$ . Then, consider any  $g(x) \in I$ .

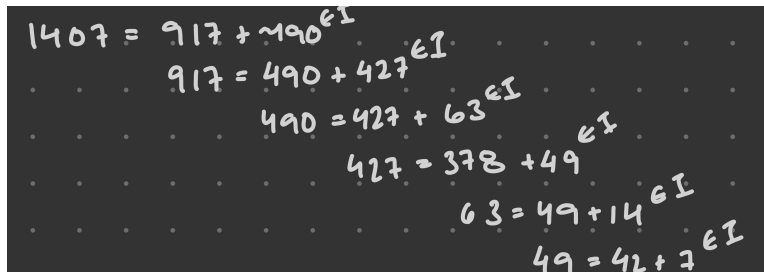
By the division algorithm,  $g = qf + r$ , with  $\deg r < \deg f$ . But we can see that  $r = g - qf$ , so it is an element of the ideal, which means  $r = 0$  to not contradict the minimality of  $f$ . Then, we have  $g = qf$ , so  $g \in (f)$ , and since this is true for any  $g \in I$ ,  $I = (f)$ .

□

Let's look at an example of the division algorithm in practice.

**Example 3.9.** Consider the ideal  $I = (1407, 917) \triangleleft \mathbb{Z}$ . What is the generator of this ideal?

We can use the Euclidean algorithm to see that:



$$\begin{aligned} 1407 &= 917 + 490 \in I \\ 917 &= 490 + 427 \in I \\ 490 &= 427 + 63 \in I \\ 427 &= 378 + 49 \in I \\ 63 &= 49 + 14 \in I \\ 49 &= 42 + 7 \in I \end{aligned}$$

so this ideal contains 7. Moreover, working back up, we can see that 1407 and 917 are both multiples of 7, so  $I = (7)$ .

Specifically, by working back up, we get that

$$7 = 89 \cdot 917 - 58 \cdot 1407.$$

Figuring out how to get 7 from the generators in this way will become useful later.

**Lemma 3.10.** Our ring  $R$  is the zero ring if and only if it has exactly one ideal.

*Proof.* It is clear that the zero ring has exactly one ideal. For the other direction, note that all rings have the ideals  $R$  and  $(0)$ . For our ring to not have more than one ideal, we must have  $R = (0)$ . □

**Lemma 3.11.** Our ring  $R$  is a field if and only if it has exactly two ideals.

*Proof.* For one direction, note that since  $R$  is a field it has at least two distinct elements, so  $R$  and  $(0)$  are two distinct ideals of  $R$ . Moreover, for any  $I \triangleleft R$ , if there is any  $s \neq 0 \in I$ , then  $s^{-1} \in R$ , so  $s^{-1}s = 1 \in I$ , and  $I = R$ .

For the other direction, we can see that if there are exactly two ideals, then this is not the zero ring, and for any  $s \neq 0 \in R$ , we must have  $(s) = R$ , so  $1 \in (s)$ , so  $1 = rs$  for some  $r \in R$ , so  $s$  has an inverse. Thus,  $R$  is a field.  $\square$

**Definition 3.12.** If  $I \triangleleft R$  then the **quotient ring** is

$$R/I = \{r + I \mid r \in R\}.$$

Then, we define addition by  $(r + I) + (s + I) = (r + s) + I$  and multiplication by  $(r + I)(s + I) = rs + I$ . The zero of our ring is  $0 + I$ , and the one is  $1 + I$ .

**Exercise 3.13.** We need to check that addition and multiplication is well-defined; that is if  $r + I = r' + I$  and  $s + I = s' + I$ , then  $(r + I)(s + I) = (r' + I)(s' + I)$ , and similarly for addition.

To do so, it is easiest to check that if  $r - r' \in I$  and  $s - s' \in I$ , then  $rs - r's' \in I$ .

**Lemma 3.14.** If  $I \triangleleft R$  and  $\phi : R \rightarrow S$  is a morphism with  $\phi(I) = \{0\}$ , then there exists a unique  $\bar{\phi} : R/I \rightarrow S$  such that  $\bar{\phi} \circ \pi = \phi$  (where  $\pi$  is the canonical projection map  $R \rightarrow R/I$ ).

$$\begin{array}{ccc} R & \xrightarrow{\phi} & S \\ \downarrow \pi & \searrow \exists! & \\ R/I & & \end{array}$$

As before, this uniquely characterizes  $R/I$ .

We can view the first isomorphism theorem as a special case of this; taking  $I = \ker \phi$ , we get the commutative diagram:

$$\begin{array}{ccc} R & \xrightarrow{\phi} & S \\ \downarrow \pi & \searrow \exists! & \\ R/\ker \phi & & \end{array}$$

**Lemma 3.15.** The ideals of the product ring  $R \times S$  are exactly  $I \times J$ , where  $I \triangleleft R$ ,  $J \triangleleft S$ .

*Proof.* It is easy to check that all such  $I \times J$  are actually ideals of  $R \times S$ . For the other direction: suppose  $K \triangleleft R \times S$ . Then for any  $(r, s) \in K$ , we can see that

$$\begin{aligned} (1, 0) \cdot (r, s) &= (r, 0) \text{ and} \\ (0, 1) \cdot (r, s) &= (0, s) \end{aligned}$$

are elements of  $K$ . Thus,  $K$  is of the form

$$(R \cap K) \times (S \cap K),$$

and we leave it as an exercise to check that  $R \cap K \triangleleft R$  and  $S \cap K \triangleleft S$ .  $\square$

**Lemma 3.16.** If  $I \triangleleft R$  then  $I[x] \triangleleft R[x]$ .

(However, in this case,  $R[x]$  has many ideals that are not of this form, as well, so this does not describe *all* ideals of  $R[x]$ .)

Note that, as we might expect:

- $(R \times S)/(I \times J) \cong R/I \times S/J$   
We can use the isomorphism  $(r, s) + I \times J \mapsto (r + I, s + J)$ .
- $R[x]/I[x] \cong (R/I)[x]$   
We can use the isomorphism  $\sum r_i x^i + I[x] \mapsto \sum (r_i + I)x^i$ .

Checking that these maps are actually isomorphisms is a bit tedious, and we leave this as an exercise.

**Lemma 3.17.** If  $I \triangleleft R$  then there is a bijection between ideals of  $R/I$  and ideals of  $R$  containing  $I$ .

We can use the map  $J \mapsto \pi(J)$ , where  $\pi$  is the natural projection map  $R \rightarrow R/I$ , and its inverse  $\bar{J} \mapsto \pi^{-1}(\bar{J})$ . We leave it as an exercise to check that this is a true bijection, or that the composites of these maps are really the corresponding identity maps.

Moreover, for any  $J \triangleleft R$  containing  $I$ , we have the isomorphism

$$R/J \cong (R/I)/\pi(J)$$

using the map  $r + J \mapsto r + I + \pi(J)$ . We leave it as an exercise to check that this is well-defined and an isomorphism.

A useful corollary is:

**Corollary 3.18.** For any ideal  $(r, s) \triangleleft R$ ,

$$R/(r, s) \cong (R/(r))/(s + (r)) \cong (R/(s))/(r + (s)).$$

**Lemma 3.19.** If  $I, J \triangleleft R$ , then

$$R/(I \cap J) \cong R/I \times_{R/I+J} R/J.$$

We can use the isomorphism  $r + I \cap J \mapsto (r + I, r + J)$ . We leave it as an exercise to check that this is an isomorphism, noting that checking surjectivity is kind of annoying.

**Example 3.20.**

$$\mathbb{Z}/(30) \cong \mathbb{Z}/(6) \times_{\mathbb{Z}/(2)} \mathbb{Z}/(10).$$

**Lemma 3.21.** If  $I, J \triangleleft R$  are comaximal ideals, then  $I \cap J = IJ$  and then previous lemma tells us

$$R/IJ \cong R/I \cap J \cong R/I \times R/J,$$

since by definition  $I + J = R$ .

*Proof.* We must need to prove that  $IJ = I \cap J$ . We know that  $IJ \subseteq I \cap J$ , so we just need to show that for any  $x \in I \cap J$ , we can express  $x$  as some  $\sum r_i s_i$ , for  $r_i \in I$  and  $s_i \in J$ . But we know that there exists some  $r \in I$ ,  $s \in J$  such that  $r + s = 1$ , by definition of comaximality. This means that we can write

$$x = x(1) = x(r + s) = xr + xs \in IJ,$$

since this a sum of the form we want. Thus  $IJ = I \cap J$ . □

**Example 3.22.**

$$\mathbb{Z}/(35) = \mathbb{Z}/(5) \times \mathbb{Z}/(7)$$

**Lemma 3.23** (Chinese Remainder Theorem). If  $I_1, \dots, I_n \triangleleft R$  are pairwise comaximal, then  $I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$  and

$$R/I_1 \cdots I_n = R/I_1 \times \cdots \times R/I_n.$$

This just requires an inductive proof, using the previous two lemmas.



## LECTURE 4: MORE ON IDEALS

**Definition 4.1.** An ideal  $I \triangleleft R$  is **maximal** if  $I$  is a proper ideal of  $R$  and it is not strictly contained in any other proper ideal of  $R$ .

**Lemma 4.2.** An ideal  $I \triangleleft R$  is maximal if and only if  $R/I$  is a field.

*Proof.* This follows from [Lemma 3.17](#) and [Lemma 3.11](#); an ideal  $I \neq R$  is maximal if and only if  $R \neq I$  are the only two ideals of  $R$  containing  $I$ , which happens if and only if  $R/I \neq (0)$  are the only two ideals of  $R/I$ , which happens if and only if  $R$  is a field.  $\square$

**Definition 4.3.** An ideal  $I \triangleleft R$  is **prime** if  $I \neq R$  and for any  $r, s \in R$ ,  $rs \in I$  only if  $r \in I$  or  $s \in I$ .

**Example 4.4.** The prime ideals of  $\mathbb{Z}$  are  $(0)$  and  $(p)$ , where  $p$  is a prime integer.

**Lemma 4.5.** An ideal  $I \triangleleft R$  is prime if and only if  $R/I$  is an integral domain.

**Corollary 4.6.** If  $I \triangleleft R$  is maximal, it is also prime.

**Definition 4.7.** We say that  $\text{Spec } R = \{\text{prime ideals of } R\}$ .

**Lemma 4.8.** If  $\phi : R \rightarrow S$  is a ring morphism and  $J \triangleleft S$  is prime then  $\phi^{-1}(J)$  is prime in  $R$ .

*Proof.* We showed in [Example 2.17](#) that  $\phi^{-1}J$  is an ideal of  $R$ . Then, we can see that since  $\phi(1) = 1$ , then if  $1 \in \phi^{-1}(J)$  would imply that  $1 \in J$ . Since  $J$  is a prime, it is a proper ideal of  $R$ ; this implies that  $\phi^{-1}J$  is also a proper ideal of  $R$ . To see that it is prime, we can see that for any  $rs \in \phi^{-1}(J)$ ,  $\phi(r)\phi(s) \in J$ , so either  $\phi(r)$  or  $\phi(s)$  is in  $J$ . But this implies that either  $r \in \phi^{-1}\phi(r)$  or  $s \in \phi^{-1}\phi(s)$  is in  $\phi^{-1}(J)$ , so this is prime, and we are done.  $\square$

This implies that  $\phi^{-1}$  maps  $\text{Spec } S$  to  $\text{Spec } R$ .

Is there a version of the above lemma for maximal ideals?

No, we have the following example:

**Example 4.9.** Consider the natural inclusion map  $\mathbb{Z} \hookrightarrow \mathbb{Q}$ . We can see that  $(0) \in \mathbb{Q}$  is a maximal ideal, since  $\mathbb{Q}/(0) = \mathbb{Q}$  is a field. But the preimage of  $(0)$  is just  $(0) \triangleleft \mathbb{Z}$ , and  $(0)$  is not a maximal ideal of  $\mathbb{Z}$ .

**Lemma 4.10.** The prime ideals of  $R \times S$  are of the form  $I \times S$ , where  $I \triangleleft R$  is prime, or  $R \times J$ , where  $J \triangleleft S$  is prime.

*Proof.* If  $K \triangleleft R \times S$  is a prime ideal, then we know from earlier that  $K = I \times J$  where  $I \triangleleft R$  and  $J \triangleleft S$ . But then,

$$(0, 0) = (0, 1) \cdot (1, 0) \in K,$$

so either  $(0, 1) \in K$  and  $J = S$  or  $(1, 0) \in K$  and  $I = R$ . Since  $K$  must be a proper ideal, we know  $K \neq R \times S$ .

If  $J = S$ , then for any  $rs \in I$ , we can see that  $(rs, 1) \in K$ , so either  $(r, 1)$  or  $(s, 1)$  is in  $K$ , so either  $r$  or  $s$  is in  $I$ , so  $I$  is prime, and we can similarly see that  $J$  is prime in the case that  $R = I$ .  $\square$

**Lemma 4.11.** If  $I \triangleleft R$ , then there exists a bijection between prime ideals of  $R/I$  and prime ideals of  $R$  containing  $I$ , where for any  $J \triangleleft R$ ,  $J \mapsto \pi(J)$  and for any  $\bar{J} \triangleleft R/I$ ,  $\bar{J} \mapsto \pi^{-1}(\bar{J})$ , where  $\pi$  is the natural projection  $R \rightarrow R/I$ .

*Proof.* We want to show that  $\pi$  and  $\pi^{-1}$  map prime ideals to prime ideals.

We know that if  $\bar{J} \triangleleft R/I$ ,  $\pi^{-1}(\bar{J})$  is prime, since we showed this in [Lemma 4.8](#).

For the other direction, if  $J \triangleleft R$  is a prime ideal such that  $I \subseteq J$ , then if

$$(r + I)(s + I) \in \pi(J)$$

, this means we can find some  $x \in J$  such that  $\pi(x) = rs + I$ . But this implies that  $rs - x \in I \subseteq J$ , and then  $x + (rs - x) = rs \in J$ . Since  $J$  is prime, either  $r$  or  $s$  is in  $J$ , which means either  $r + I$  or  $s + I$  is in  $\pi(J)$ , as we wanted.  $\square$

Note that you *cannot* extend [Lemma 4.10](#) to arbitrary products:

**Example 4.12.** Consider the product ring  $R = \prod_{i=1}^{\infty} \mathbb{Q}$ . For a clever choice of  $\mathcal{X}$  (a collection of subsets of  $\mathbb{Z}_{\geq 0}$ ),

$$I(\mathcal{X}) = \{(r_i) \in R \mid \{i \mid r_i = 0\} \in \mathcal{X}\}$$

is prime, but it is not of the form described in [Lemma 4.10](#). We leave the details of this example as an exercise.

**Lemma 4.13.** For a ring  $R$ , the following properties are equivalent:

1. Any ideal of  $R$  is finitely generated.
2. If  $\mathcal{X}$  is a nonempty set of ideals of  $R$ , then there exists an  $I \in \mathcal{X}$  which is not properly contained in any  $I' \in \mathcal{X}$  (we say that  $I$  is a **maximal** element of  $\mathcal{X}$ ).

*Proof.* We will first show that (1)  $\implies$  (2), by contradiction.

Suppose (2) is false. That is, we can find some  $\mathcal{X}$  such that for any  $I \in \mathcal{X}$ , there is some  $I' \supsetneq I \in \mathcal{X}$ . If we pick an arbitrary  $I_1 \in \mathcal{X}$ , we can find  $I_2 \in \mathcal{X}$  strictly containing  $I_1$ , and then we can find  $I_3 \in \mathcal{X}$  strictly containing  $I_2$ , and so on, so we get the infinite chain

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots$$

Then, we can define  $I = \bigcup_{i=1}^{\infty} I_i$ , and we can see that  $I \triangleleft R$ .

But by (1), we can write  $I = (r_1, \dots, r_n)$  for some  $r_1, \dots, r_n \in R$ . But since these are a finite number of elements in  $I$ , we must be able to find some  $N$  such that  $r_1, \dots, r_n \in I_N \subset I$ . But this implies that  $I = (r_1, \dots, r_n) \subset I_N$ , so  $I = I_N$ , contradicting the fact that

$$I_N \subsetneq I_{N+1} \subset I.$$

Thus, we have reached a contradiction, and if (1) is true, (2) must also be true.

Now, we will show that (2)  $\implies$  (1).

Consider some  $I \triangleleft R$ . Let  $\mathcal{X}$  be the set

$$\mathcal{X} = \{J \triangleleft R \mid J \subseteq I, J \text{ finitely generated}\}.$$

We can see that  $(0) \in \mathcal{X}$ , so it is nonempty, and, applying (2), it must have a maximal element  $J_0$ . If  $J_0 \neq I$  then there must exist some  $r \in R$  such that  $r \in I$  but  $r \notin J_0$ , but then  $J_0 + (r)$  would be an element of  $\mathcal{X}$  strictly containing  $J_0$ . Thus, we have  $J_0 = I$ , and then  $I$  must be finitely generated.  $\square$

**Definition 4.14.** We say that  $R$  is **noetherian** if these equivalent properties hold.

**Example 4.15.**

- $\mathbb{Z}$  is noetherian
- if  $K$  is a field, then  $K$  and  $K[x]$  are noetherian
- any PID is noetherian

**Example 4.16.** The ring  $\mathbb{C}[X_1, X_2, \dots]$  is *not* noetherian because the ideal  $(X_1, X_2, \dots)$  is not finitely generated (any finite generating set will cover only finitely many of the  $X_i$ 's).

**Lemma 4.17.** If  $R$  and  $S$  are noetherian, then so is  $R \times S$ .

**Lemma 4.18.** If  $R$  is noetherian and  $I \triangleleft R$ , then  $R/I$  is noetherian.

Since we know exactly what the ideals of the product and quotient rings look like, we just need to check that these ideals are finitely generated. This follows from the fact that ideals of  $R$  and  $S$  are finitely generated, and is left as an exercise.

**Remark 4.19.** If  $R, S, T$  are noetherian rings,  $R \times_T S$  is *not necessarily* noetherian.

**Lemma 4.20** (Hilbert's Basis Theorem). If  $R$  is noetherian then so is  $R[x]$  (or  $R[x_1, \dots, x_n]$  for any finite  $n$ ).

*Proof.* We will show that any  $I \triangleleft R[x]$  is finitely generated. Consider the set

$$L_d = \left\{ r \in R \mid r \text{ is the } x^d \text{ coefficient of some } f \in I \text{ of degree } d \right\}.$$

Note that  $L_d \triangleleft R$ , and  $L_d \subseteq L_{d+1}$  since if  $f \in I$  then so is  $xf$ .

Since  $R$  is noetherian, we know that the set  $\{L_d\}$  must have some maximal element  $L_N$ , and then

$$L_N = L_{N+1} = \dots$$

But we know that each  $L_d$  is finitely generated, so we can find  $f_{d_1}, \dots, f_{d_{s_d}} \in I$  whose  $x^d$  coefficients generate  $L_d$ . (We choose this generating set to be  $x^{d-N} f_{N_1}, \dots, x^{d-N} f_{N_{s_N}}$  when  $d > N$ .) Then, consider the ideal

$$J = (f_{0_1}, \dots, f_{0_{s_0}}, f_{1_1}, \dots, f_{N_{s_N}}) \subseteq I.$$

We claim that  $I = J$ . We can see that if  $I \neq J$ , then there must be some  $g \in I - J$  of minimal degree  $d$ . But we know that, if  $g$  has leading term  $c_d x^d$ , then  $c_d \in L_d$  by definition, so there exists some  $r_i$ 's such that  $\sum_{i=1}^{s_d} r_i f_{d_i}$  has leading term  $c_d x^d$  as well. But this means

$$g - \sum_{i=1}^{s_d} r_i f_{d_i}$$

is also in  $I - J$ , and is of smaller degree, which is a contradiction.

Thus,  $I = J$ , and  $I$  is finitely generated. Since this is true for all  $I \triangleleft R[x]$ ,  $R[x]$  is noetherian. □

## LECTURE 5: RINGS, IV

**Remark 5.1.** Last time, we showed that if  $R$  is noetherian, then so is  $R[x]$ . It is also true that  $R[[x]]$  is noetherian in this case; the proof is very similar, but using the coefficient of the lowest term rather than the coefficient of the largest term.

**Definition 5.2.** A ring  $S$  is said to be **finitely generated** over  $R$  if there is a ring morphism  $\phi : R \rightarrow S$  such that we can find a *finite* subring  $X \subset S$  such that  $S$  has no proper subring strictly containing  $\phi R$  and  $X$ .

Equivalently,  $S$  is **finitely generated** if there is some finite set  $X \subset S$  such that  $X = \{x_1, \dots, x_n\}$  and we have a *surjective* homomorphism  $\psi : R[X_1, \dots, X_n] \rightarrow S$  where for  $r \in R$ ,  $\psi(r) = \phi(r)$  and  $\psi(X_i) = x_i$ .

**Remark 5.3.** If  $R$  is noetherian and  $\phi : R \rightarrow S$  is a ring morphism such that  $S$  is finitely generated over  $R$ , then  $S$  is noetherian.

*Proof.* By the second definition of “finitely generated,”  $S \cong R[X_1, \dots, X_n] / \ker \psi$ , and since  $R$  is noetherian, so is  $R[X_1, \dots, X_n]$ , and then so is  $S$  (as a quotient ring of the polynomial ring).  $\square$

The fourth way of constructing rings is the ring of fractions.

**Definition 5.4.** For a ring  $R$ , a subset  $D \subset R$  is **multiplicative** if  $1 \in D$ , and for any  $r, s \in D$ ,  $rs \in D$ .

**Remark 5.5.** For any ring morphism  $\phi : R \rightarrow S$ , and any multiplicative  $D \subset R$ ,  $\phi(D) \subset S$  is multiplicative.

*Proof.* We can see that  $\phi(1) = 1 \in \phi(D)$  and for any  $r, s \in \phi(D)$ , there is  $r', s' \in D$  such that  $\phi(r') = r$  and  $\phi(s') = s$ , so

$$rs = \phi(r')\phi(s') = \phi(r's') \in \phi(D).$$

$\square$

To define the ring of fractions, intuitively we want something like  $R \times D$ , where we are looking at (numerator, denominator) pairs. But we also want the normal fraction equivalence, so that

$$\frac{r}{d} = \frac{ra}{da},$$

for any  $r \in R$ ,  $a, d \in D$ . Remember that we intuitively consider two fractions  $r/a$  and  $s/b$  equivalent if  $rb = sa$ . To account for zero divisors, we actually use the equivalence

$$(r, a) \sim (s, b) \text{ if } c(br - as) = 0 \text{ for some } c \in D.$$

**Lemma 5.6.** The  $\sim$  defined above is an equivalence relation.

*Proof.* The part that is difficult to check is transitivity.

We want to show that if  $(r, a) \sim (s, b)$  and  $(s, b) \sim (t, c)$  then  $(r, a) \sim (t, c)$ .

We know that there is some  $d, e \in D$  such that

$$\begin{aligned}d(br - as) &= 0 \\ e(cs - bt) &= 0.\end{aligned}$$

We want to consider a linear combination of these that will cancel out the  $s$  terms, and we get that

$$\begin{aligned}ecd(br - as) + dae(cs - bt) &= 0 + 0 = 0 \\ \implies ebd(cr - at) &= 0,\end{aligned}$$

and since  $ebd \in D$ , this means that  $(r, a) \sim (t, c)$ , as we wanted!  $\square$

Note that without allowing this  $c$  term in our definition of the equivalence, we would not be able to show transitivity.

**Definition 5.7.** We denote this set of equivalence classes as  $D^{-1}R$  and we write  $r/a$  to denote  $[(r, a)]$ .

**Lemma 5.8.**  $D^{-1}R$  is a ring, with the following operations:

$$\begin{aligned}0 &= 0/1 \\ 1 &= 1/1 \\ r/a + s/b &= \frac{rb + as}{ab} \\ r/a \cdot s/b &= \frac{rs}{ab}.\end{aligned}$$

(For the latter two, note that  $ab \in D$  since  $D$  is multiplicative.)

Moreover, there is a homomorphism  $R \rightarrow D^{-1}R$  defined by  $r \mapsto r/1$ . Note that this is *not always* an injective map.

Under this homomorphism, any  $a \in D$  maps to  $a/1$  and has inverse  $1/a$ , so this homomorphism maps all of  $D$  to units in the ring of fractions.

We will not carry out the full proof - most of the proof is just checking one property after another, and should be straightforward. The longest thing is checking that  $+$  and  $\times$  are well-defined operations, so we will check now that  $+$  is well-defined.

If  $r/a = r'/a'$  and  $s/a = s'/a'$  in  $D^{-1}R$ , then we want to show that  $\frac{br+as}{ab} = \frac{b'r'+a's'}{a'b'}$ . Using our definition of equivalences, we know that there is some  $c, d \in D$  such that

$$\begin{aligned}c(a'r - ar') &= 0 \\ d(b's - bs') &= 0.\end{aligned}$$

We claim that the two sums are equivalent, and specifically that

$$cd(a'b'br + a'b'as - abb'r' - aba's') = 0.$$

But this is just

$$ca'a(d)(b's - bs') + db'b(c)(a'r - ar') = 0 + 0 = 0,$$

as we wanted. Thus, sums are well defined.

The ring of fractions also has a universal property - we can think of it as the “cheapest way” of adjusting  $R$  so that all elements of  $D$  become units.

**Lemma 5.9.** If  $D \subset R$  is multiplicative and  $\phi : R \rightarrow S$  is a morphism such that  $\phi(D) \subset S^\times$ , then there exists a unique  $\bar{\phi} : D^{-1}R \rightarrow S$  such that

$$\begin{array}{ccc} R & \xrightarrow{\phi} & S \\ \downarrow & \nearrow \bar{\phi} & \\ D^{-1}R & & \end{array}$$

commutes.

*Proof.* We claim that the map is  $\bar{\phi}(r/a) = \phi(r)(\phi(a))^{-1}$ , and leave it as an exercise to check that it is well-defined and a ring morphism.

To see that it is unique, note that if  $\psi$  is another such morphism, then since the diagram commutes, for any  $r \in R$ ,  $\psi(r/1) = \phi(r)$ . But then for any  $r/a \in D^{-1}R$ , we have that

$$\psi(r/a)\psi(a/1) = \psi(r/1) = \phi(r),$$

and since  $\psi(a/1) = \phi(a)$ , we get that

$$\psi(r/a)\phi(a) = \phi(r),$$

and since  $\phi(a)$  is a unit, we can multiply by  $(\phi(a))^{-1}$  to get

$$\psi(r/a) = \phi(r)(\phi(a))^{-1},$$

so  $\psi = \bar{\phi}$ . □

Again, this completely characterizes the ring of fractions.

**Example 5.10.**

1. If  $0 \in D$ , then  $D^{-1}R = \{0\}$ .

This is because for any  $r/a$ , we can see that  $0(1 \cdot r - a \cdot 0) = 0$ , so  $r/a \sim 0/1$ .

2. If  $D = \{r \in R \mid r \text{ not a zero divisor}\}$  (check that this is multiplicative!) then we denote  $D^{-1}R$  as  $QR$  and call it the **total quotient ring**.

In this case, the map  $R \rightarrow QR$  is injective, because if  $r/1 \sim s/1$ , this means  $c(r \times 1 - s \times 1) = 0$  for  $c$  not a zero divisor, so  $r - s = 0$ , so  $r = s$ .

- $Q\mathbb{Z} = \mathbb{Q}$
- If  $R$  is an integral domain, then  $D = R \setminus \{0\}$  and  $QR$  is a field.

This is because for any  $r/a \neq 0$ , we know that  $r \neq 0$ , so  $a/r \in QR$  as well, and we have found an inverse for  $r/a$ , so all nonzero elements are units and  $QR$  is a field.

In a sense, this makes  $QR$  the smallest field containing  $R$ ; any field containing  $R$  also contains  $QR$ .

- $Q(\mathbb{Z} \times \mathbb{Z}) = \mathbb{Q} \times \mathbb{Q}$ . We leave this as an exercise to prove.
- $Q\mathbb{C}[X]/X^2 = \mathbb{C}[X]/X^2$ .

This is because the set of elements which are not zero divisors is

$$D = \{a + bX \mid a \neq 0\},$$

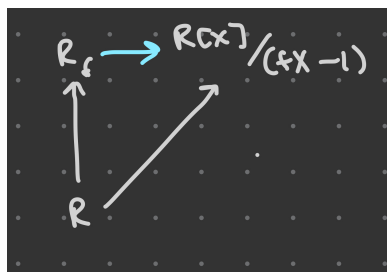
and this is already the set of units for this ring. We leave it as an exercise to check these two facts.

3. For any  $f \in R$ , the set  $\{1, f, f^2, \dots\}$  is multiplicative. In this case, we denote the ring of fractions  $R_f$  or  $R[1/f]$ .

This is isomorphic to  $R[X]/(fX - 1)$ . Why?

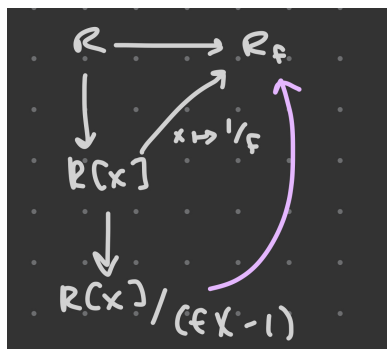
We can do some diagram chasing to prove this.

First, note that the natural map  $R \rightarrow R[X]/(fX - 1)$ , which is the inclusion map and then the projection map, maps  $f$  to a unit, since  $fX = 1 \in R[X]/(fX - 1)$ . So we can apply the universal property of  $R_f$  to get that there is a unique  $\phi : R_f \rightarrow R[X]/(fX - 1)$  such that this diagram commutes:



We can call this Diagram 1.

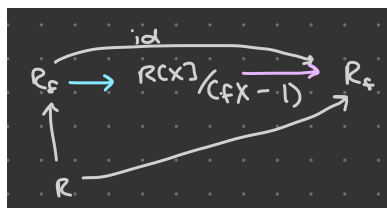
Then, if we consider the map  $R[X] \rightarrow R_f$  defined by  $X \mapsto 1/f$ , we can see that the first isomorphism theorem gives us a unique map  $\psi : R[X]/(fX - 1) \rightarrow R_f$ , which is the purple arrow in the following commutative diagram:



We can call this Diagram 2.

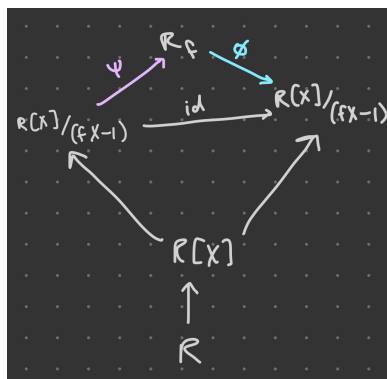
Now, we need to show that  $\phi \circ \psi = \text{id}_{R[X]/(fX-1)}$  and  $\psi \circ \phi = \text{id}_{R_f}$ . To show the latter, we can see that  $\psi \circ \phi$  makes the following diagram commute:





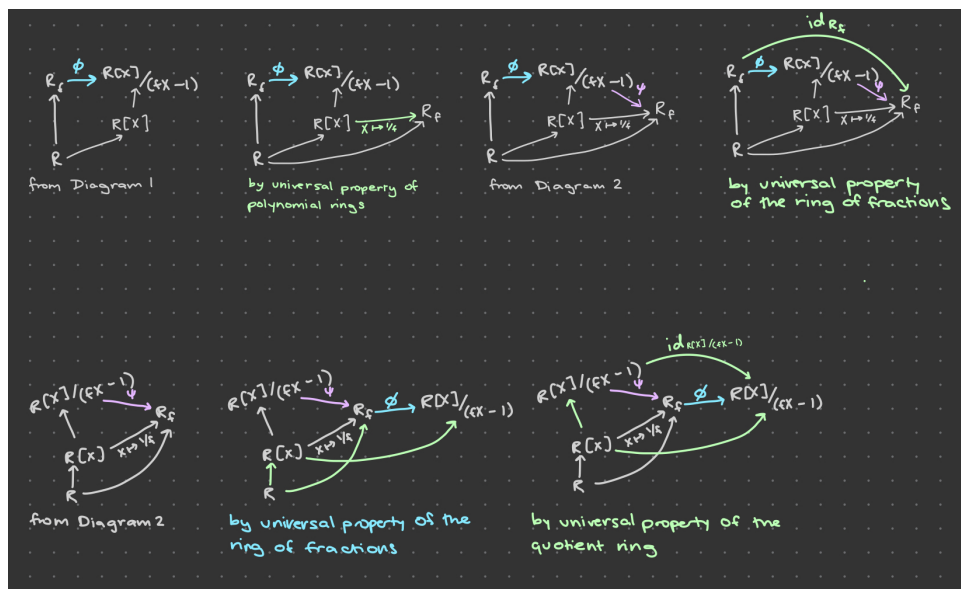
but the universal property of the ring of fractions tells us that  $\text{id}_{R_f}$  is the unique map  $R_f \rightarrow R_f$  that makes the diagram commute, so  $\psi \circ \phi = \text{id}_{R_f}$ .

Similarly, to show the former, we see that  $\phi \circ \psi$  makes the following diagram commute:



but the universal property of the quotient ring tells us that  $\text{id}_{R[X]/(fX-1)}$  is the unique map  $R[X]/(fX-1) \rightarrow R[X]/(fX-1)$  that makes this diagram commute, so  $\phi \circ \psi = \text{id}_{R[X]/(fX-1)}$ .

But how did we get the latter two commutative diagrams? We can build them up as follows:



Thus, these two are isomorphisms, as we desired.

Examples of this are:

- $\mathbb{Z}[1/n]$
- $R[[X]]_X = R((X)) = \{\sum_{i=N}^{\infty} a_i x^i \mid a_i \in R, N \in \mathbb{Z}\}$ . This is called the **Lorent series** over  $R$ .

We won't be able to cover completions in class; there will be notes uploaded to Canvas that will be important for the homework.

## LECTURE 6: FRACTION RINGS, CONT'D

Let's continue looking at examples of fraction rings:

**Example 6.1.**

4. If we have rings  $R$  and  $S$ , and multiplicative subsets  $D \subset R$  and  $E \subset S$ , then  $D \times E \subset R \times S$  is also multiplicative (this should be easy to check).

Moreover,  $(D \times E)^{-1}(R \times S) \cong D^{-1}R \times E^{-1}S$ , using the isomorphism  $(r, s)/(d, e) \mapsto (r/d, s/e)$ .

You should check that this is well-defined and an isomorphism, but this should be straightforward to do.

5. If we have a ring morphism  $\phi : R \rightarrow S$  and a multiplicative subset  $D \subset R$ , then  $\phi D \subset S$  is also multiplicative.

In the case where this map is implicitly known, people often write  $D^{-1}S$  to denote  $(\phi D)^{-1}S$ .

The diagram

$$\begin{array}{ccc} R & \xrightarrow{\phi} & S \\ \downarrow & & \downarrow \\ D^{-1}R & \xrightarrow{r/d \mapsto \phi(r)/\phi(d)} & (\phi D)^{-1}S \end{array}$$

commutes because of the universal property of the fraction ring.

We can similarly see that for any ring  $R$  and multiplicative set  $D \subset R$ ,

$$(D^{-1}R)[X] \cong D^{-1}(R[X]),$$

via the isomorphism

$$\sum_{i=0}^n (r_i/d_i) X^i \mapsto \left( \prod_{i=0}^n \frac{1}{d_i} \right) \sum_{i=0}^n r_i \left( \prod_{j \neq i} d_j \right) X^i.$$

However, we *don't* have a similar statement for formal power series: we can see that

$$\mathbb{Z}[[X]][1/2] \neq (\mathbb{Z}[1/2])[[X]],$$

as the polynomial  $1 + \frac{x}{2} + \frac{x^2}{4} + \dots$  is in  $(\mathbb{Z}[1/2])[[X]]$  but not  $\mathbb{Z}[[X]][1/2]$ .

6. If  $\wp \triangleleft R$  is a prime ideal, then  $R - \wp$  is multiplicative.

We call  $R_\wp = (R - \wp)^{-1}R$  the **localization** of  $R$  at  $\wp$ .

Note that this is slightly confusing notation, if  $f \in R$  such that  $(f)$  is prime, then  $R_f$  means (vaguely) that you are inverting  $f$ , while  $R_{(f)}$  means that you are inverting everything *but*  $f$ .

Let's look at some examples of this:

- $\mathbb{Z}_{(p)}$ , for prime  $p$ , is the set  $\{a/b \in \mathbb{Q} \mid a, b \in \mathbb{Z}, p \nmid b\}$

(where we mean  $a/b \in \mathbb{Q}$  which has a representative such that this is true; obviously we can always express  $a/b$  in a form where the denominator is a multiple of  $p$ )

- $\mathbb{Z}_{(0)} = \mathbb{Q}$
- $\mathbb{C}[X]_{(X)} = \{p/q \in \mathbb{C}[X] \mid q(0) \neq 0\}$ , which is the set of all  $f(X) \in \mathbb{C}(X)$  such that we can evaluate  $f$  at 0
- Remember that we said that if  $\wp \triangleleft S$  is prime, then  $R \times \wp \triangleleft R \times S$  is prime. Then,

$$(R \times S)_{R \times \wp} = (R \times S - R \times \wp)^{-1}(R \times S) = (R \times (S - \wp))^{-1}(R \times S).$$

Then, applying what we said about fraction rings of the product ring, this equals

$$R^{-1}R \times (S - \wp)^{-1}S = \{0\} \times S_{\wp} = S_{\wp}.$$

**Definition 6.2.** If  $I \triangleleft R$  and  $D \subset R$  is multiplicative, then

$$D^{-1}I = \{r/a \mid r \in I, a \in D\} \triangleleft D^{-1}R.$$

**Definition 6.3.** We call  $I$  **saturated** with respect to  $D$  if for any  $r \in R$  and  $a \in D$  such that  $ar \in I$ ,  $r$  is also an element of  $I$ .

**Lemma 6.4.** If  $I$  is saturated with respect to  $D$  and  $r/a \in D^{-1}I$  then  $r \in I$ .

Note that this is not true in general; we know that in general, if  $r/a \in D^{-1}I$  then there is *some* representative of  $r/a$  such that the numerator is in  $I$ , but that is not necessarily the case for the given representative  $r/a$ .

*Proof.* We know that there is some representative  $s/b = r/a$  with  $s \in I$ . Since these two are equal, there exists some  $c \in D$  such that

$$c(as - br) = 0 \implies cas = cbr.$$

But we can see that  $cas \in I$  since  $s \in I$  and  $ca \in I$ . This means that  $cbr \in I$ , and since  $cbr = (cb)r$ , with  $cb \in D$  and  $r \in R$ , this means by the definition of saturated that  $r \in I$ .  $\square$

Let  $\phi : R \rightarrow D^{-1}R$  be the natural map. Then:

**Lemma 6.5.** If  $J \triangleleft D^{-1}R$  then  $\phi^{-1}J$  is saturated with respect to  $D$  and  $D^{-1}(\phi^{-1}J) = J$ .

*Proof.* To show  $\phi^{-1}J$  is saturated with respect to  $D$ , take an arbitrary  $r \in R$ ,  $a \in D$  such that  $ar \in \phi^{-1}J$ . Applying  $\phi$ , this means that  $ar/1 \in J$ , and since  $J$  is an ideal of  $D^{-1}R$  and  $a \in D$ ,  $(1/a)(ar/1) = r/1 \in J$ . But this means that  $r \in \phi^{-1}J$ , as we desired.

Then,  $D^{-1}\phi^{-1}J$  is the set of all  $r/a$  such that  $a \in D$  and  $r \in \phi^{-1}J$ , or  $r/1 \in J$ . So

$$D^{-1}\phi^{-1}J = \{r/a \mid a \in D, r/1 \in J\}.$$

We can see that for any  $r/a \in J$ ,  $a(r/a) = r/1 \in J$ , so  $r/a \in D^{-1}\phi^{-1}J$ , and  $J \subset D^{-1}\phi^{-1}J$ .

Similarly, for any  $r/a \in D^{-1}\phi^{-1}J$ , we know that  $r/1 \in J$  and  $1/a \in D^{-1}R$ , so  $(1/a)(r/1) = r/a \in J$ , and  $D^{-1}\phi^{-1}J = J$ .  $\square$

**Lemma 6.6.** If  $I \triangleleft R$  then  $\phi^{-1}D^{-1}I$  is the smallest saturated ideal containing  $I$  (formally, all other saturated ideals containing  $I$  also contain  $\phi^{-1}D^{-1}I$ ) and  $D^{-1}\phi^{-1}D^{-1}I = D^{-1}I$ .

The proof of this is very similar to the proof of the previous lemma, so if you were confused by the previous lemma, it is recommended you do this as an exercise.

**Lemma 6.7.** There is a bijection between ideals of  $D^{-1}R$  and ideals  $I \triangleleft R$  which are saturated with respect to  $D$ , using the maps

$$J \mapsto \phi^{-1}J$$

$$D^{-1}I \leftrightarrow I.$$

This follows from the previous two lemmas.

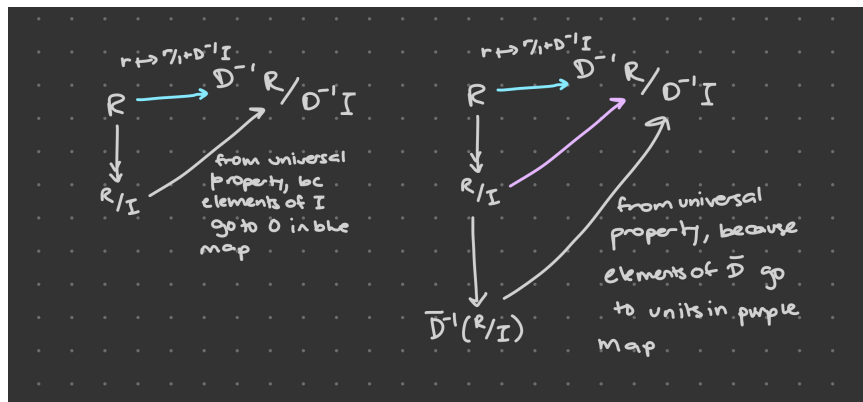
**Lemma 6.8.** If  $D \subset R$  is multiplicative and  $I \triangleleft R$ , then  $\bar{D}$ , or the image of  $D$  in  $R/I$ , is also multiplicative. There is an isomorphism

$$\bar{D}^{-1}(R/I) \cong (D^{-1}R)/(D^{-1}I),$$

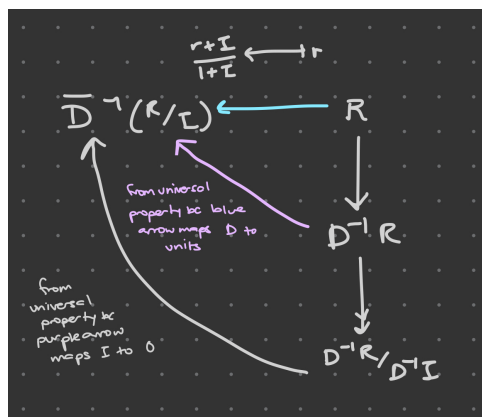
using the map  $\frac{r+I}{d+I} \mapsto r/d + D^{-1}I$ .

*Proof.* Intuitively, we can see that this is the sort of thing that we could solve from the universal property. To get a map  $\bar{D}^{-1}(R/I) \rightarrow (D^{-1}R)/(D^{-1}I)$ , we first want a map  $R/I \rightarrow (D^{-1}R)/(D^{-1}I)$  where  $\bar{D}$  maps to units, and to get this, we want a map  $R \rightarrow (D^{-1}R)/(D^{-1}I)$  where  $I$  is in the kernel.

We get the following commutative diagram:



and we can use this to explicitly compute the homomorphism and get that it is  $\frac{r+I}{d+I} \mapsto r/d + D^{-1}I$ . Similarly, in the other direction, we get the commutative diagram:



and we can use this to explicitly compute the homomorphism and get that it is  $r/d + D^{-1}I \mapsto \frac{r+I}{d+I}$ .

We can check that the composition of these maps is the identity in both directions, so this is really an isomorphism.  $\square$

**Corollary 6.9.** If  $R$  is noetherian, then so is  $D^{-1}R$ .

This follows from [Lemma 6.7](#).

**Corollary 6.10.** A prime ideal  $I \triangleleft R$  is saturated with respect to  $D$  if and only if  $I \cap D = \emptyset$ .

There is a bijection between prime ideals of  $D^{-1}R$  and prime ideal  $I$  of  $R$  with  $I \cap D = \emptyset$ , using the maps

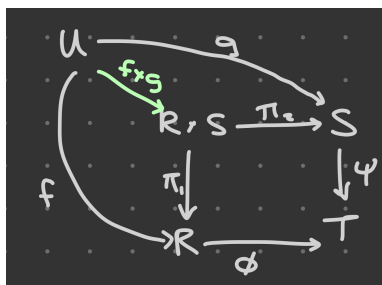
$$\begin{aligned} J &\mapsto \phi^{-1}J \\ D^{-1}I &\leftarrow I. \end{aligned}$$

This directly implies that  $\text{Spec}(D^{-1}R) \subset \text{Spec}(R)$ .

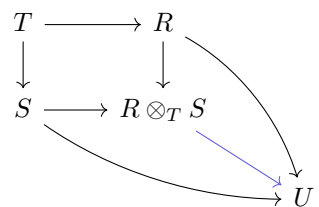
Note also that  $\text{Spec}(R_{\emptyset}) = \{I \in \text{Spec } R \mid I \subset \emptyset\}$ .

LECTURE 7: TENSOR PRODUCTS

In lecture 2, we discussed the relative product, which was a subring of  $R \times S$  with the following commutative diagram:



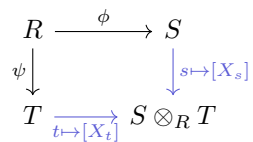
Today, we will discuss the tensor product, which in a sense extends the product in the opposite direction; we get the commutative diagram:



We will discuss what this means later in the lecture, but for now we are just presenting it as a useful way to think of the tensor product as compared to the relative product.

So how do we get the tensor product?

Let's say we have a ring  $R$ , and ring morphisms  $\phi$  and  $\psi$  to  $S$  and  $T$ , respectively. We want to construct  $S \otimes_R T$  such that the following diagram commutes:



Well, we can start with the ring  $R[X_s, Y_t]_{s \in S, t \in T}$ , so that we are trying to “add” all of  $S$  and  $T$  into the ring  $R$ . But in order to make our operations in our tensor product work the same way they did in  $R, S$ , and  $T$ , we need to mod out by the following ideal:

$$I = \left( \begin{array}{cc} X_{s_1+s_2} - X_{s_1} - X_{s_2}, & Y_{t_1+t_2} - Y_{t_1} - Y_{t_2}, \\ X_{s_1 s_2} - X_{s_1} X_{s_2}, & Y_{t_1 t_2} - Y_{t_1} Y_{t_2}, \\ X_{\phi(r)} - r, & Y_{\psi(r)} - r \end{array} \right)_{s_1, s_2 \in S, t_1, t_2 \in T, r \in R} .$$

That is, we are making sure that for all  $s_1, s_2 \in S$   $X_{s_1+s_2} = X_{s_1} + X_{s_2}$  and  $X_{s_1 s_2} = X_{s_1} X_{s_2}$ , so the  $X$ 's actually correspond to elements of  $S$ , and similarly for  $T$ . Moreover, we are making sure that for any  $r \in R$   $r \mapsto r$  in the natural map to the tensor product; this means we are making sure  $X_{\phi(r)} = r$  and  $Y_{\psi(r)} = r$ .

**Definition 7.1.** We say that the **tensor product** of  $R, S, T$  given the ring morphisms  $\phi : R \rightarrow S$  and  $\psi : R \rightarrow T$ , is

$$S \otimes_{\phi, R, \psi} T = S \otimes_R T = R[X_s, Y_t]_{s \in S, t \in T} / I,$$

where  $I$  is defined above.

Note that this depends on our choice of morphism  $\phi, \psi$  but in cases where these morphisms are implicit, we leave them out of the description of the tensor product.

**Definition 7.2.** We write  $s \otimes t \in S \otimes_R T$  to denote  $X_s Y_t \in S \otimes_R T$ .

**Remark 7.3.** For elements of the tensor product, these properties follow from the definition of  $S \otimes_R T$ :

- $(s_1 + s_2) \otimes t = s_1 \otimes t + s_2 \otimes t$
- $s \otimes (t_1 + t_2) = s \otimes t_1 + s \otimes t_2$
- $(s_1 \otimes t_1)(s_2 \otimes t_2) = s_1 s_2 \otimes t_1 t_2$
- for any  $r \in R$ , we get that

$$\phi(r)s \otimes t = X_{\phi(r)s} Y_t = X_{\phi(r)} X_s Y_t = r X_s Y_t = r(s \otimes t).$$

- for any  $r \in R$ ,  $s \otimes \psi(r)t = r(s \otimes t)$

As we might expect, the tensor product also has a universal property.

**Lemma 7.4.** If we have the commutative diagram

$$\begin{array}{ccc} R & \xrightarrow{\phi} & S \\ \psi \downarrow & & \downarrow g \\ T & \xrightarrow{f} & U \end{array}$$

then there is a unique map  $f \otimes g : S \otimes_R T \rightarrow U$  that makes the diagram

$$\begin{array}{ccccc} R & \xrightarrow{\phi} & & S & \\ \psi \downarrow & & \swarrow & & \downarrow g \\ & & S \otimes_R T & & \\ \uparrow & & \searrow & & \\ T & \xrightarrow{f} & & U & \\ & & \swarrow & & \\ & & f \otimes g & & \end{array}$$

commute.

*Proof.* We can see that since this diagram commutes, we are forced to define this map by

$$\begin{aligned} f \otimes g(r) &= f(\phi(r)) = g(\psi(r)) \\ f \otimes g(X_s) &= f(s) \\ f \otimes g(Y_t) &= g(t). \end{aligned}$$

Clearly, this gives us a ring morphism  $R[X_s, Y_t]_{s \in S, t \in T} \rightarrow U$ , so we need to show that the  $I$  we defined above is within the kernel of this map, so we can apply the universal property of the quotient map to see that this gives us a unique homomorphism  $R[X_s, Y_t]_{s \in S, t \in T}/I \rightarrow U$ , as we desired.

We can see that for any  $s_1, s_2 \in S$ ,

$$\begin{aligned} f \otimes g(X_{s_1+s_2} - X_{s_1} - X_{s_2}) &= f(s_1 + s_2) - f(s_1) - f(s_2) = 0 \\ f \otimes g(X_{s_1 s_2} - X_{s_1} X_{s_2}) &= f(s_1 s_2) - f(s_1) f(s_2) = 0, \end{aligned}$$



and for any  $r \in R$ ,

$$f \otimes g(X_{\phi(r)} - r) = f(\phi(r)) - f(\phi(r)) = 0,$$

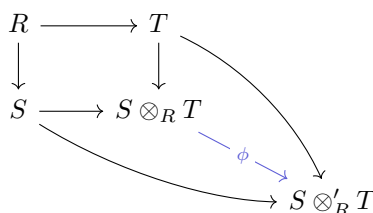
and we can similarly check these properties of the  $Y$  terms to see that the entire ideal  $I$  is in the kernel of this map, as we desired.

Thus, the  $f \otimes g$  we defined above is the unique homomorphism from  $S \otimes_R T$  to  $U$  that makes this diagram commute, as we desired.  $\square$

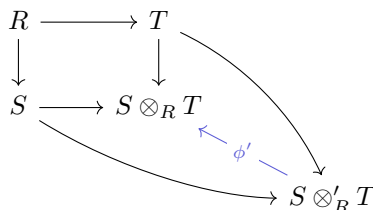
Note that the universal property of the tensor product also gives us the uniqueness of the tensor product, in the sense that

**Remark 7.5.** If we have two tensor products  $S \otimes_R T$  and  $S \otimes'_R T$  with the same universal property, then  $S \otimes_R T \cong S \otimes'_R T$ , and there is a canonical isomorphism between the two.

*Proof.* The universal property of  $S \otimes_R T$  gives us the following unique  $\phi$ :

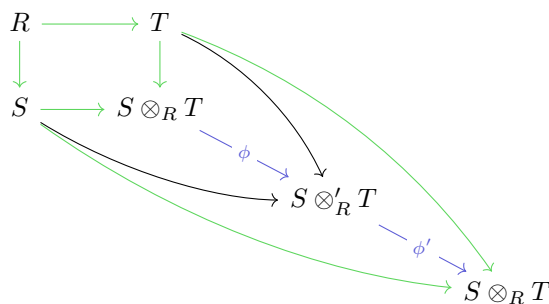


and the universal property of  $S \otimes'_R T$  gives us the following unique  $\phi'$ :



We claim that  $\phi$  and  $\phi'$  are inverses of each other. Why?

We will just show that  $\phi' \circ \phi = \text{id}_{S \otimes_R T}$ , as the other direction is identical. To do so, we combine the two commutative diagrams in the following way:



But then, by applying the universal property of  $S \otimes_R T$  to the green arrows, we get that  $\text{id}_{S \otimes_R T}$  is the unique map  $S \otimes_R T \rightarrow S \otimes_R T$  that makes the diagram commute, so  $\phi' \circ \phi = \text{id}_{S \otimes_R T}$ .

We can do the same thing in the other direction to get that these two maps are inverses of each other and therefore isomorphisms. Moreover,  $\phi$  and  $\phi'$  are the *canonical* isomorphisms in either direction, because they are the unique maps induced by the universal property.  $\square$

**Lemma 7.6.** If we have the commutative diagrams

$$\begin{array}{ccc}
 S & \xrightarrow{\alpha} & S' \\
 & \swarrow & \searrow \\
 & R & \\
 & \swarrow & \searrow \\
 & & 
 \end{array}
 \quad
 \begin{array}{ccc}
 T & \xrightarrow{\beta} & T' \\
 & \swarrow & \searrow \\
 & R & \\
 & \swarrow & \searrow \\
 & & 
 \end{array}$$

then there is a unique map  $\alpha \otimes \beta : S \otimes_R T \rightarrow S' \otimes_R T'$  defined by

$$\alpha \otimes \beta(s \otimes t) = \alpha(s) \otimes \beta(t).$$

*Proof.* We can apply the universal property of the tensor product to the following commutative diagram:

$$\begin{array}{ccccc}
 & & R & \xrightarrow{\quad} & T & \xrightarrow{\beta} & T' \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & S & \xrightarrow{\quad} & S \otimes_R T & \xrightarrow{\alpha \otimes \beta} & S' \otimes_R T' \\
 & & \downarrow \alpha & & \downarrow & & \downarrow \\
 & & S' & \xrightarrow{\quad} & S' \otimes_R T' & & 
 \end{array}$$

and then by following the diagram, we can check that

$$\alpha \otimes \beta(s \otimes t) = \alpha \otimes \beta(X_s) \alpha \otimes \beta(Y_t) = X_{\alpha(s)} Y_{\beta(t)} = \alpha(s) \otimes \beta(t).$$

□

**Definition 7.7.** We say that an element in  $S \otimes_R T$  is a **pure tensor** if we can express it in the form  $s \otimes t$ .

**Remark 7.8.** Every element of  $S \otimes_R T$  is a finite sum of pure tensors.

*Proof.* We can see that any monomial of  $R[X_s, Y_t]_{s \in S, t \in T}$  is of the form

$$r \prod_{i=1}^n X_{s_i}^{m_i} \prod_{j=1}^{n'} Y_{t_j}^{m'_j},$$

for some  $r \in R$  and some  $s_i \in S, t_i \in T$ . But in our quotient ring, we know that this is equivalent to

$$\left( \phi(r) \prod_{i=1}^n s_i^{m_i} \right) \otimes \left( \prod_{j=1}^{n'} t_j^{m'_j} \right),$$

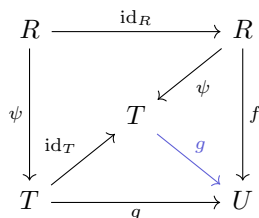
which is a pure tensor. Since every element of this polynomial ring is a finite sum of monomials, every element of our quotient must be a finite sum of pure tensors. □

**Lemma 7.9.** The tensor product  $R \otimes_R T$  is isomorphic to  $T$ , using the map  $r \otimes t \mapsto \psi(r)t$ .

*Proof.* Since we know  $R \otimes_R T$  is the unique ring with the tensor product universal property, it suffices to show the universal property also holds for  $T$ . But we know that for any  $U, f, g$  such that we have the following commutative diagram:

$$\begin{array}{ccc}
 R & \xrightarrow{\text{id}_R} & R \\
 \psi \downarrow & & \downarrow f \\
 T & \xrightarrow{g} & U
 \end{array}$$

then  $g$  is the unique map  $T \rightarrow U$  that will make the diagram

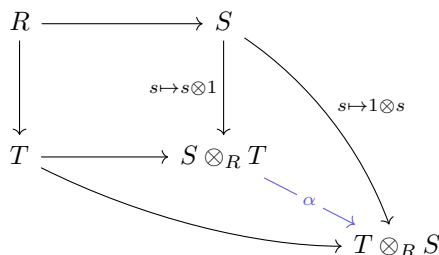


commute. Thus, the universal property holds for  $T$ , and  $R \otimes_R T \cong T$ .

We leave the proof of the definition of the isomorphism as an exercise; this just follows from the fact that it is the unique isomorphism defined in [Remark 7.5](#). □

**Lemma 7.10.** For any rings  $R, S, T$ ,  $S \otimes_R T \cong T \otimes_R S$ , and the isomorphism between them is the map  $s \otimes t \mapsto t \otimes s$ .

*Proof.* It is clear from the universal property that these are isomorphic (using the same argument as in [Remark 7.5](#)). The universal property moreover tells us that the unique isomorphism between them is the  $\alpha$  that makes this diagram commute:



Then, we can see that in order for this diagram to commute, we must have

$$\alpha(s \otimes t) = \alpha(s \otimes 1)\alpha(1 \otimes t) = (1 \otimes s)(t \otimes 1) = t \otimes s.$$

□

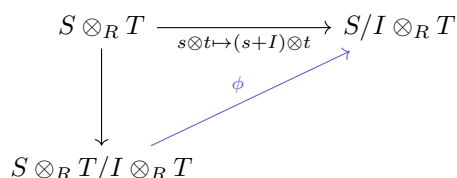
**Note 7.11.** Importantly, this means that all theorems in this section that we prove in terms of  $T$  (or the second ring in the tensor product) are also true for  $S$  (or the first ring in the tensor product). For much of this lecture, we will only state lemmas in one direction, so it is important to note they apply in both directions.

**Lemma 7.12.** If  $I \triangleleft S$  is an ideal, then we define  $I \otimes_R T$  to be the set of finite sums of pure tensors  $s \otimes t$  such that  $s \in I$ . Then,  $I \otimes_R T \triangleleft S \otimes_R T$  and

$$(S \otimes_R T)/(I \otimes_R T) \cong (S/I) \otimes_R T,$$

using the isomorphism  $s \otimes t + I \otimes_R T \mapsto (s + I) \otimes t$ .

*Proof.* Consider the map  $S \otimes_R T \rightarrow (S/I) \otimes_R T$  defined by  $s \otimes t \mapsto (s + I) \otimes t$ . We can see that any element in  $I \otimes_R T$  would map to  $0 \otimes t = 0(1 \otimes t) = 0X_1X_t = 0$ , so  $I \otimes_R T$  is in the kernel of this map, and we can apply the universal property of quotient rings to get an induced map  $\phi$  to make this diagram commute,



and we can see that  $\phi(s \otimes t + I \otimes_R T) = (s + I) \otimes t$ , as we desired. Then, in the reverse direction, we get the commutative diagram

$$\begin{array}{ccccc}
 R & \longrightarrow & S/I & \longrightarrow & S \\
 \downarrow & & \downarrow & & \downarrow \\
 T & \longrightarrow & S/I \otimes_R T & \xrightarrow{\text{green}} & S \otimes_R T \\
 & & & \searrow \psi & \downarrow \\
 & & & & S \otimes_R T / I \otimes_R T
 \end{array}$$

where the green arrow comes from applying [Lemma 7.6](#) to the inclusion map  $S/I \rightarrow S$  and the identity map  $T \rightarrow T$ , and our desired map  $\psi$  is just the composition of the green and blue maps.

We leave it as an exercise to check that these are inverses of each other.  $\square$

**Lemma 7.13.** If  $I \triangleleft R$ , then  $R/I \otimes_R T \cong T/\psi I$ .

*Proof.* We know from the previous lemma that  $R/I \otimes_R T \cong R \otimes_R T / I \otimes_R T$ , and then we can apply [Lemma 7.9](#) to see that this is isomorphic to  $T/\psi I$ .  $\square$

**Lemma 7.14.** If  $D \subset S$  is multiplicative, then  $D \otimes_R 1 = \{d \otimes 1 \mid d \in D\}$  is also multiplicative, and

$$(D^{-1}S) \otimes_R T \cong (D \otimes_R 1)^{-1}(S \otimes_R T).$$

**Lemma 7.15.** For any multiplicative  $D \subset R$ ,  $D^{-1}R \otimes_R T \cong D^{-1}T$ , using the map  $r/d \otimes t \mapsto \psi(r)t/\psi(d)$ .

**Lemma 7.16.** The tensor product  $S \otimes_R T[X]$  is isomorphic to  $(S \otimes_R T)[X]$ .

**Lemma 7.17.** For any ring  $U$ ,  $S \otimes_R (T \otimes_R U) \cong (S \otimes_R T) \otimes_R U$ , using the map  $s \otimes (t \otimes u) \mapsto (s \otimes t) \otimes u$ .

**Lemma 7.18.** For any ring  $U$ ,  $S \otimes_R (T \times U) \cong (S \otimes_R T) \times (S \otimes_R U)$ .

## LECTURE 8: FACTORIZATION IN RINGS

This week, we will cover factorization in rings, which will finish up our unit on rings.

**Definition 8.1.** If  $R$  is a ring and  $r, s \in R$ , then  $r \mid s$  (we say “ $r$  divides  $s$ ”) if  $s = rt$  for some  $t \in R$ .

**Definition 8.2.** We call  $r$  **irreducible** in  $R$  if  $r \notin R^\times$  and if  $r = st \in R$ , then either  $s \in R^\times$  or  $t \in R^\times$ .

**Example 8.3.** In  $\mathbb{Z}$ , the irreducibles are  $\pm p$  for prime  $p$ .

If  $K$  is a field then the irreducibles in  $K[X]$  are the irreducible polynomials.

**Lemma 8.4.** If  $R$  is a noetherian integral domain then for any  $r \in R$  such that  $r \neq 0$ , we can write

$$r = u \cdot \pi_1 \cdots \pi_n,$$

where  $u \in R^\times$  and each  $\pi_i$  is irreducible.

*Proof.* Let  $\mathcal{X}$  be the set of all ideals  $(r) \subset R$  where  $r$  has no such factorization.

If this is an empty set, then we are done.

If not, then since  $R$  is noetherian,  $\mathcal{X}$  has some maximal element  $(r)$ . We know that  $(r)$  is not irreducible, since then it would have a trivial factorization, so there must be some  $s, t \notin R^\times$  such that  $r = st$ .

Then,  $(r) \subseteq (s)$ , but if  $(r) = (s)$  then  $s = ur$  for some  $u \in R$ . But since we are in an integral domain, this implies  $u = t^{-1}$ , which contradicts the fact that  $t$  is not a unit. Thus, we have  $(r) \subsetneq (s)$  and similarly we get that  $(r) \subsetneq (t)$ .

Since  $(r)$  is maximal in  $\mathcal{X}$ , this means that  $(s)$  and  $(t)$  cannot be in  $\mathcal{X}$ , so we have factorizations  $s = u\pi_1 \cdots \pi_n$  and  $t = v\pi'_1 \cdots \pi'_m$ . But then,

$$r = st = uv\pi_1 \cdots \pi_n \pi'_1 \cdots \pi'_m,$$

and we have found a factorization for  $r$ , contradicting the fact that  $r$  has no such factorization.

Thus, for every  $r \in R$ , we can find such a factorization. □

**Definition 8.5.** We say that  $r, s \in R$  are **associates** if  $r = su$ , where  $u \in R^\times$ , and we denote this  $r \sim s$ .

**Example 8.6.** In  $\mathbb{Z}$ , for any prime  $p$ ,  $p \sim -p$ .

**Example 8.7.** The ring  $\mathbb{Z}$  has the property that if

$$r = u\pi_1 \cdots \pi_n = v\pi'_1 \cdots \pi'_m \in \mathbb{Z},$$

with  $u, v \in \mathbb{Z}^\times$  and  $\pi_i, \pi'_i$  irreducible, then  $m = n$ , and up to rearrangement  $\pi_i \sim \pi'_i$ .

But not all rings have this property, and even some otherwise very nice rings do not.

**Example 8.8.** In  $\mathbb{Z}[\sqrt{-5}]$  we can write

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

We claim that all of these are irreducibles and moreover that none of them are associates.

We will just show that 2 is irreducible as an example. For any factorization  $2 = (a + b\sqrt{-5})(c + d\sqrt{-5}) \in \mathbb{Z}[\sqrt{-5}]$ , we can take the norm to get that

$$4 = (a^2 + 5b^2)(c^2 + 5d^2).$$

But since  $a, b, c, d$  are integers, clearly  $b = d = 0$ , and then  $ac = \pm 2$ . But this implies that one of the factors is  $\pm 1$ , which means one of these factors is a unit, and therefore 2 is irreducible.

We leave showing that the rest of these factors are irreducibles as an exercise; after that, it is clear that they are not associates since neither  $1 + \sqrt{-5}$  or  $1 - \sqrt{-5}$  can be a multiple of 2.

**Definition 8.9.** A ring  $R$  is a **unique factorization domain** (or UFD) if it is an integral domain and

1. for any  $r \in R \setminus \{0\}$ , we can factor  $r$  as

$$r = u\pi_1 \cdots \pi_n,$$

where  $u \in R^\times$  and each  $\pi_i$  is an irreducible.

2. if

$$u\pi_1 \cdots \pi_n = v\pi'_1 \cdots \pi'_m,$$

where  $u$  and  $v$  are units and each  $\pi_i$  and  $\pi'_j$  is an irreducible, then  $n = m$  and up to rearrangement,  $\pi_i \sim \pi'_i$  for each  $i$ .

**Example 8.10.**

1.  $\mathbb{Z}$  is a UFD
2. any field is a UFD (since all nonzero elements are units)
3.  $\mathbb{Z}[\sqrt{-5}]$  is *not* a UFD

**Lemma 8.11.** If  $R$  is an integral domain and (1) holds in the definition of a UFD, then the following are equivalent:

1. a principal ideal  $(r)$  is prime if and only if  $r$  is irreducible
2. if  $\pi \in R$  is irreducible then  $(\pi)$  is prime
3. if  $\pi \in R$  is irreducible then for any  $r, s \in R$  such that  $\pi \mid rs$ , either  $\pi \mid r$  or  $\pi \mid s$
4.  $R$  is a UFD

*Proof.* Clearly, (2) and (3) are equivalent, and (1) implies (2). So to complete the equivalences we just need to show that (3) implies (4) and (4) implies (1).

We will first show that (3)  $\implies$  (4).

We start with an arbitrary  $u\pi_1 \cdots \pi_n = v\pi'_1 \cdots \pi'_m$ , where  $u, v \in R^\times$  and each  $\pi_i$  and  $\pi'_j$  is irreducible. We will show via induction on  $m$  that these are the same factorization.

As a base case, we can see that if  $m = 0$ , then  $u\pi_1 \cdots \pi_n$  is a unit. But any factor of a unit is also a unit (and therefore not an irreducible) so  $n = 0$ , and we are done.

For the inductive step, when  $m > 0$ , we can see that (3) implies that since  $\pi'_m$  is not a factor of  $u$ , we must have  $\pi'_m \mid \pi_i$  for some  $i$ , so there exists some  $w \in R$  such that  $\pi_i = w\pi'_m$ . Since  $\pi_i$  is irreducible, this means  $w$  must be a unit, and  $\pi'_m$  and  $\pi_i$  must be associates. We rearrange so that  $i = m$  and we get  $\pi'_m \sim \pi_n$ , and since this is an integral domain, we can then factor out the  $\pi_i$  to get

$$(uw)\pi_1 \cdots \pi_{n-1} = v\pi'_1 \cdots \pi'_{m-1}.$$

Applying our inductive assumption, we get that  $n - 1 = m - 1$  (so  $n = m$ ) and for each  $i$ ,  $\pi_i \sim \pi'_i$ , so this is a UFD.

Now we will show that (4)  $\implies$  (1).

In one direction, we consider a prime principal ideal  $(r)$ . For any  $s, t \in R$  such that  $r = st$ , we have that  $st \in (r)$ , so either  $s \in (r)$  or  $t \in (r)$ . We assume without loss of generality that  $s \in (r)$ , so that  $s = ur$  for some  $u \in R$ . But since this is an integral domain we can combine these equations to get that  $ut = 1$ , and then  $t \in R^\times$ , so  $r$  is irreducible.

For the other direction, we consider an irreducible  $r \in R$ . For any  $st \in (r)$ , we have that  $st = rx$  for some  $x \in R$ . We can write out the factorizations

$$\begin{aligned} s &= u\pi_1 \cdots \pi_n \\ t &= v\pi'_1 \cdots \pi'_m \\ u &= w\pi''_1 \cdots \pi''_p, \end{aligned}$$

so that

$$(uw)\pi_1 \cdots \pi_n \pi'_1 \cdots \pi'_m = w\pi''_1 \cdots \pi''_p r,$$

where  $r$  and all of the  $\pi$ 's are irreducible and  $u, v, w \in R^\times$ . But then, since we are in a UFD, we know that there exists some  $i$  such that  $r \sim \pi_i$  (and then  $r \mid s$  so  $s \in (r)$ ) or  $r \sim \pi'_i$  (and then  $r \mid t$  so  $t \in (r)$ ). Thus, this ideal is prime.  $\square$

**Definition 8.12.** We call  $R$  a **principal ideal domain** (or PID) if it is an integral domain and any ideal of  $R$  is principal.

**Example 8.13.**  $\mathbb{Z}$  is a PID, and when  $K$  is a field,  $K[X]$  is a PID.

**Lemma 8.14.** If  $R$  is noetherian then the following are equivalent

1.  $R$  is a PID
2.  $R$  is a UFD where each nonzero prime ideal is maximal

(Note that  $R$  being a PID implies that  $R$  is noetherian, so we can also say that if  $R$  is a general ring, then (1) is equivalent to (2) plus the property that  $R$  is noetherian.)

*Proof.* The direction (2)  $\implies$  (1) is a homework problem.

For the other direction, we will assume  $R$  is a PID and prove property (2) in [Lemma 8.11](#).

Suppose  $\pi \in R$  is an irreducible. Consider any  $rs \in (\pi)$ . Since this is a PID,  $(r, \pi) = (t)$  for some  $t \in R$ . But then  $\pi = tu$  for some  $u \in R$ , and since  $\pi$  is irreducible this means either  $t \in R^\times$  or  $u \in R^\times$ .

If  $u \in R^\times$ , then  $t \sim \pi$  so  $(t) = (\pi)$  and  $r \in (\pi)$ .

If  $t \in R^\times$ , then  $(t) = (r, \pi) = R$ , so there exists some  $x, y \in R$  such that  $rx + \pi y = 1$ . But then, multiplying by  $s$ , we get that

$$srx + s\pi y = s,$$

or  $s = (rs)x + (\pi)sy$ , so  $s$  is a multiple of  $\pi$  and  $s \in (\pi)$ .

Then, we will show that every nonzero prime ideal is maximal. If we have a prime ideal  $\wp \neq (0)$ , and any ideal  $\mathfrak{q} \neq R$  such that  $\wp \subseteq \mathfrak{q}$ , we can see that  $\mathfrak{q}$  must also be prime.

This means we have  $\wp = (\pi)$  and  $\mathfrak{q} = (\pi')$  with  $\pi, \pi'$  being irreducible. If  $(\pi) \subseteq (\pi')$  then there exists some  $u \in R$  such that  $\pi = u\pi'$ . But since  $\pi$  is irreducible, this implies that  $\pi \sim \pi'$ , and therefore  $\wp = \mathfrak{q}$ , so  $\wp$  is maximal, as we desired.  $\square$

**Example 8.15.** When  $K$  is a field,  $K[X]$  is a UFD.

We now move on to some things we can do within a UFD.

**Lemma 8.16.** Suppose  $R$  is a UFD, and  $r, s \in R$ . Then, there exists a  $\gcd(r, s) \in R$ , which is unique up to associates, such that  $\gcd(r, s) \mid r$ ,  $\gcd(r, s) \mid s$ , and for any  $t \in R$  such that  $t \mid r$  and  $t \mid s$ , we also have  $t \mid \gcd(r, s)$ .

*Proof.* Let's say that  $r = u\pi_1 \cdots \pi_n$  and  $s = v\pi'_1 \cdots \pi'_m$ . We can rearrange these irreducibles so that for any  $1 \leq i \leq p$ ,  $\pi_i \sim \pi'_i$ , and for any  $i, j > p$ ,  $\pi_i \not\sim \pi'_j$ .

Then, we define  $\gcd(r, s) = \pi_1 \cdots \pi_p$ .

We leave it as an exercise to check that the stated properties hold.  $\square$

**Definition 8.17.** If  $R$  is a UFD, then  $r, s \in R$  are **coprime** if  $\gcd(r, s) = 1$ .

**Definition 8.18.** We can define  $\gcd(r_1, \dots, r_n)$  similarly to the way we defined the gcd of two elements.

**Definition 8.19.** If  $R$  is a UFD then a polynomial  $f(X) \in R[X]$  is **primitive** if the gcd of its coefficients is 1.



## LECTURE 9: FACTORIZATION IN RINGS, II

**Lemma 9.1** (Gauss). If  $R$  is a UFD and  $f, g \in R[X]$  are primitive, then  $fg$  is also primitive.

*Proof.* We will prove the contrapositive. If  $fg$  were not primitive, then there is some irreducible  $\pi \in R$  such that  $\pi$  divides all coefficients of  $fg$ . Since  $R$  is a UFD,  $(\pi)$  must be a prime ideal of  $R$ , and then since  $R/(\pi)$  is an integral domain,  $R/(\pi)[X] = R[X]/(\pi)$  is also an integral domain.

Let  $\bar{f}$  be the image of  $f$  in  $R[X]/(\pi)$  and let  $\bar{g}$  be the image of  $g$  in  $R[X]/(\pi)$ . We know that

$$\bar{f}\bar{g} = \overline{fg} = 0 \in R[X]/(\pi),$$

and since  $R[X]/(\pi)$  is an integral domain, this means either  $\bar{f}$  or  $\bar{g}$  is 0 in this quotient, which means either  $\pi$  divides all the coefficients of  $f$  or  $\pi$  divides all the coefficients of  $g$ .

Thus, if  $fg$  is not primitive, then  $f$  and  $g$  cannot both be primitive. □

**Lemma 9.2.** If  $R$  is a UFD, then  $f(X) \in R[X]$  is irreducible if and only if either:

- $f \in R$  and  $f$  is irreducible in  $R$
- $f$  is primitive and  $f(X)$  is irreducible in  $QR[X]$  (the polynomial ring of the field of fractions of  $R$ )

*Proof.* For the first direction:

If  $f(X)$  is irreducible and  $f \in R$ , then we can see that if  $f = gh \in R$ , then either  $g$  is a unit in  $R[X]$  or  $h$  is a unit in  $R[X]$ . But we have that the units in  $R[X]$  must have degree 0 (since the degree adds when we multiply polynomials), so the units in  $R[X]$  are exactly the elements in  $R$  which have inverses in  $R$ , and we get that

$$R[X]^\times = R^\times.$$

Thus, since either  $g$  or  $h$  is a unit in  $R[X]$ , that polynomial will also be a unit in  $R$ , and therefore  $f$  is irreducible in  $R$ .

If  $f(X)$  is irreducible and  $f \notin R$ , then we can see that  $f$  must be primitive, because otherwise there is some irreducible  $\pi$  such that  $\pi$  divides all coefficients of  $f$ , and therefore  $f/\pi \in R[X]$ . Then

$$f = \pi(f/\pi),$$

and  $\pi$  is not a unit in  $R[X]$  because it is not a unit in  $R$ , and  $f/\pi$  is not a unit in  $R[X]$  because it has nonzero degree.

Thus,  $f$  is primitive. From here, let's say  $f = gh \in QR[X]$ . Then let  $a \in QR$  be the lcm of the denominators of coefficients of  $g$  divided by the gcd of the numerators of coefficients of  $g$ , so that  $g = a \cdot \tilde{g}$ , where  $\tilde{g} \in R[X]$  and is a primitive polynomial. We can similarly write  $h = b \cdot \tilde{h}$ , where  $b \in QR$  and  $\tilde{h}$  is a primitive polynomial in  $R[X]$ . Then, we have that

$$f = ab\tilde{g}\tilde{h}.$$

Since  $R$  is a UFD, we can write  $ab$  as a fraction in  $R$  in "lowest terms," where we mean that the numerator and the denominator are coprime. Then, for  $ab\tilde{g}\tilde{h}$  to be an element of  $R[X]$ , we need the denominator of  $ab$  in lowest terms to divide the gcd of the coefficients of  $\tilde{g}\tilde{h}$ . But Gauss's lemma tells us that  $\tilde{g}\tilde{h}$  is also primitive, so the denominator of  $ab$  must be a unit, and  $ab \in R$ . Then this becomes a factorization of  $f$  in  $R[X]$ , so we know that either  $\tilde{g}$  or  $\tilde{h}$  is a unit in  $R[X]$ , which means  $g$  or  $h$  is a unit in  $QR[X]$ , and  $f$  is irreducible in  $QR[X]$ .

For the other direction:

If  $f \in R$  and  $f$  is irreducible in  $R$ , then for any factorization  $f = gh \in R[X]$ , we know that since  $\deg f = \deg g + \deg h$ , the polynomials  $g$  and  $h$  must also be in  $R$ . Thus, either  $g$  or  $h$  is a unit in  $R$ , which means it is also a unit in  $R[X]$ , so  $f$  is irreducible in  $R[X]$ .

If  $f \in R[X] \setminus R$  and  $f$  is primitive and irreducible in  $QR[X]$  then for any

$$f = gh \in R[X],$$

we know that either  $g$  or  $h$  is a unit in  $QR[X]$ . We assume without loss of generality that  $g$  is the unit, and then by the same logic as before this means that  $g$  is a unit in  $QR$ . But  $g$  is also an element of  $R[X]$ , which means  $g \in R$ . Since  $f$  is primitive, this implies  $h$  is a unit in  $R$ , so it is a unit in  $R[X]$ , and  $f$  is irreducible in  $R[X]$ .  $\square$

**Theorem 9.3.** If  $R$  is a UFD then  $R[X]$  is a UFD.

**Example 9.4.** This tells us that  $\mathbb{Z}[X, Y]$  and  $\mathbb{C}[X, Y]$  are UFDs.

*Proof.* We first prove the existence of a factorization into irreducibles:

We know that for any  $f(X) \in R[X]$ , we can factor it in  $QR[X]$  (since we showed in [Example 8.15](#) that  $QR[X]$  is a UFD). Let's say we have a factorization

$$f(X) = u \cdot \pi_1 \cdots \pi_n,$$

where  $u \in QR[X]^\times = QR^\times$  and each  $\pi_i$  is an irreducible in  $QR[X]$ . Note that we can multiply  $\pi_i$  by the lcm of the denominators of its coefficients and divide  $u$  by this lcm to get the same product, but with each  $\pi_i$  being an element of  $R[X]$  and then divide  $\pi_i$  by the gcd of its coefficients and multiply  $u$  by this gcd to get the same product, but with each  $\pi_i$  being primitive. But then each  $\pi_i$  is a primitive polynomial in  $R[X]$  which is irreducible in  $QR[X]$ , and [Lemma 9.2](#) tells us that this means each  $\pi_i$  is irreducible in  $R[X]$ .

Moreover, we know that since  $R$  is a UFD we can write  $u$  in "lowest terms," and then the denominator must divide the gcd of the coefficients of  $\pi_1 \cdots \pi_n$  for the total product  $f$  to be in  $R[X]$ . But since each  $\pi_i$  is primitive, [Gauss's Lemma](#) tells us this product is primitive, so the denominator of  $u$  must be a unit, and therefore  $u \in R$ .

From here, we can just factor  $u$  as an element of  $R$  to get a factorization of  $f$  into irreducibles (this uses the fact that irreducibles in  $R$  are irreducibles in  $R[X]$ , which we just proved in [Lemma 9.2](#)).

Now that we have some factorization, we will prove the uniqueness of this factorization:

We showed in [Lemma 8.11](#) that once such a factorization exists, proving uniqueness is equivalent to showing that for any irreducible  $\pi \in R[X]$ ,  $(\pi)$  is prime. We divide this into two cases:

If  $\pi \in R$ , then we know that  $R/(\pi)$  is an integral domain since  $R$  is a UFD. This implies  $R/(\pi)[X]$  is an integral domain, and this equals  $R[X]/(\pi)$ , so  $(\pi) \triangleleft R[X]$  is prime.

If  $\pi \notin R$  then we know that  $\pi$  is primitive and  $(\pi) \triangleleft QR[X]$  is prime. Then, for any  $f, g \in R[X]$  such that  $fg \in (\pi)$ , we know that either  $f \in (\pi) \triangleleft QR[X]$  or  $g \in (\pi) \triangleleft QR[X]$ . Assume without loss of generality that  $f$  is the multiple of  $\pi$ . Then, we know that there is some  $h \in QR[X]$  such that  $f = \pi \cdot h$ . Then, as before, we write  $h = a \cdot \tilde{h}$  where  $a \in QR$  and  $\tilde{h}$  is primitive, and we note that

$$f = a\pi \cdot \tilde{h}.$$

But then  $\pi \cdot \tilde{h}$  is primitive by Gauss's lemma, so for  $f$  to be an element of  $R[X]$  we need  $a \in R$ , which means  $a\tilde{h} \in R[X]$  and  $f \in (\pi) \triangleleft R[X]$ , as we desired.  $\square$

Let's look at a few examples of polynomials, to find tricks to help us determine whether a polynomial is irreducible.

**Example 9.5.** Is  $X^3 - 3X + 1$  irreducible in  $\mathbb{Q}[X]$ ?

Note that this is primitive, so this is the same as asking about irreducibility in  $\mathbb{Z}[X]$ . Note that since this is a monic cubic, if it had non-unit factors in  $\mathbb{Z}[X]$ , they would be of the form

$$(X^2 + aX + b)(X + c) \quad a, b, c \in \mathbb{Z}.$$

Specifically we can see that  $b, c$  are integers such that  $bc = 1$ , so  $c = \pm 1$ , and this has non-unit factors only if  $\pm 1$  is a root of  $X^3 - 3X + 1$ . But we can see that  $1^3 - 3(1) + 1 = -1$  and  $(-1)^3 - 3(-1) + 1 = 3$ , so neither of these are roots, and our polynomial is irreducible.

The trick we used above was that when we look at factors of the polynomial in  $\mathbb{Z}[X]$ , there are very few options for what the coefficients could be.

**Example 9.6.** Is  $X^3 + X + 105$  irreducible in  $\mathbb{Q}[X]$ ?

Again, this is the same as asking if it is irreducible in  $\mathbb{Z}[X]$ . We could do the same thing as above, but there are lots of options for  $bc = 105$ , so this would be a lot of casework.

Instead, note that if this polynomial had non-unit factors in  $\mathbb{Z}[X]$ , then it will also have non-unit factors in  $(\mathbb{Z}/2\mathbb{Z})[X]$ . We write

$$(X^2 + aX + b)(X + c) = X^3 + X + 1 \in (\mathbb{Z}/2\mathbb{Z})[X],$$

and note that  $c$  can be either 0 or 1, meaning that either 0 or 1 would be a root of this polynomial. But we can see that  $0^3 + 0 + 1 = 1^3 + 1 + 1 = 1 \in \mathbb{Z}/2\mathbb{Z}$ , so this has no non-unit factors in  $(\mathbb{Z}/2\mathbb{Z})[X]$  and therefore it is also irreducible in  $\mathbb{Q}[X]$ .

In general, it is useful to look at our polynomial in some  $\mathbb{Z}/(m)[X]$ , as long as  $m$  and the leading coefficient of our polynomial are coprime.

**Lemma 9.7** (Eisenstein's Criterion). Suppose  $R$  is an integral domain and  $\wp$  is a prime ideal of  $R$ . Let

$$f(X) = f_0 + f_1X + \cdots + f_dX^d \in R[X].$$

Suppose moreover that  $f_d \notin \wp$ ,  $f_i \in \wp$  for each  $i < d$  and  $f_0 \notin \wp^2$ . Then,  $f$  is not the product of any two lower-degree polynomials.

**Example 9.8.** Consider  $2X + 6 \in \mathbb{Z}[X]$ .

Taking  $\wp = (3)$ , Eisenstein's criterion tells us this is not the product of any two lower-degree polynomials, but it is not irreducible because

$$2(X + 3) = 2X + 6.$$

So Eisenstein's criterion "almost" shows irreducibility; in a UFD we need to additionally check that our polynomial is primitive.

*Proof.* Suppose  $f = gh$ , where

$$\begin{aligned} g(X) &= g_0 + \cdots + g_e X^e \\ h(X) &= h_0 + \cdots + h_{d-e} X^{d-e} \end{aligned}$$

and  $e, d - e > 0$ . We can see that  $f_d = g_e h_{d-e} \notin \wp$ , so  $g_e, h_{d-e} \notin \wp$ .

Then, pick the minimal  $i, j$  such that  $g_i$  and  $h_j$  are not in  $\wp$ . We have that

$$f_{i+j} = \underbrace{g_0 h_{i+j} + \cdots + g_{i-1} h_{j+1}}_{\in \wp} + g_i h_j + \underbrace{g_{i+1} h_{i-1} + \cdots + g_{i+j} h_0}_{\in \wp}.$$

But since  $\wp$  is prime and  $g_i, h_j \notin \wp$ , we have that  $g_i h_j \notin \wp$ , which means that this sum cannot be in  $\wp$ . But this means that  $f_{i+j} = f_d$  and  $i = e, j = d - e$ .

Since those were the minimal  $i, j$  such that  $g_i, h_j \notin \wp$ , we can see that  $g_0, h_0 \in \wp$ , so  $f_0 = g_0 h_0 \in \wp^2$ , a contradiction.  $\square$

**Example 9.9.** The polynomial  $X^4 + 10X + 5$  is irreducible in  $\mathbb{Z}[X]$ .

**Corollary 9.10.** For a prime  $p$ , the  $p^{\text{th}}$  cyclotomic polynomial

$$\phi_p = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + 1 \in \mathbb{Z}[X]$$

is irreducible.

*Proof.* Note that  $\phi_p(X)$  is irreducible if and only if  $\phi_p(X + 1)$  is irreducible. But

$$\phi_p(X + 1) = \frac{(X + 1)^p - 1}{X} = X^{p-1} + pX^{p-2} + \cdots + \binom{p}{i} X^{p-i-1} + \cdots + p.$$

Applying Eisenstein's criterion with  $\wp = (p)$ , we can see that this has no factorization into lower-degree polynomials, and since this is primitive, it must be irreducible.  $\square$

## LECTURE 10: CATEGORY THEORY, I

A good reference for this part of the course is *Categories for the Working Mathematician* by Saunders Mac Lane.

**Definition 10.1.** We have a **universe**  $\mathcal{U}$  with **small sets**  $X \in \mathcal{U}$  such that

- If  $X \in Y \in \mathcal{U}$  then  $X \in \mathcal{U}$ .
- If  $X, Y \in \mathcal{U}$  then  $\{X, Y\} \in \mathcal{U}$
- If  $X \in \mathcal{U}$  then  $P(X) \in \mathcal{U}$ , where  $P(X)$  denotes the power set of  $X$ .
- $\{0, 1, 2, 3, \dots\} \in \mathcal{U}$
- If we have  $X \in \mathcal{U}$  and a function  $f : X \rightarrow \mathcal{U}$  then  $\text{im } f \in \mathcal{U}$ .

Note that the elements of  $\mathcal{U}$  are a model of ZFC, but the axioms of ZFC do not guarantee the existence of such a  $\mathcal{U}$ ; we are just assuming this exists for the sake of our course.

**Definition 10.2.** By a **category**  $\mathcal{C}$  we mean two sets  $\text{ob}(\mathcal{C}) \subset \mathcal{U}$  (of **objects**) and  $\text{mor}(\mathcal{C})$  (of **morphisms**) together with functions:

- $\text{dom} : \text{mor}(\mathcal{C}) \rightarrow \text{ob}(\mathcal{C})$  which maps a morphism to its domain
- $\text{cod} : \text{mor}(\mathcal{C}) \rightarrow \text{ob}(\mathcal{C})$  which maps a morphism to its codomain
- $\text{id} : \text{ob}(\mathcal{C}) \rightarrow \text{mor}(\mathcal{C})$  which maps an object to its identity morphism
- $\circ : \{(f, g) \in \text{mor}(\mathcal{C}) \times \text{mor}(\mathcal{C}) \mid \text{cod}(g) = \text{dom}(f)\} \rightarrow \text{mor}(\mathcal{C})$  which maps two functions to their composition

such that

1. for  $X \in \text{ob}(\mathcal{C})$ ,  $\text{dom } \text{id}_X = X = \text{cod } \text{id}_X$
2. for  $f \in \{f \in \text{mor}(\mathcal{C}) \mid \text{dom}(f) = X, \text{cod}(f) = Y\} = \text{Hom}_{\mathcal{C}}(X, Y)$ , which is denoted  $X \xrightarrow{f} Y$  or  $f : X \rightarrow Y$ , we have that
 
$$f \circ \text{id}_X = \text{id}_Y \circ f,$$
3. for  $f, g, h \in \text{mor}(\mathcal{C})$ ,  $f \circ (g \circ h) = (f \circ g) \circ h$

**Definition 10.3.** We call  $f : X \rightarrow Y$  an **isomorphism** if there exists some  $g : Y \rightarrow X$  with the property that  $f \circ g = \text{id}_Y$  and  $g \circ f = \text{id}_X$ .

**Remark 10.4.** If such a  $g$  exists, it is unique, and we call it the **inverse** of  $f$ , denoted  $f^{-1}$ .

*Proof.* If we have  $g, g'$  with this property, then

$$g \circ f \circ g' = g \circ \text{id}_Y = g$$

but

$$g \circ f \circ g' = \text{id}_X \circ g' = g',$$

so the two morphisms are the same. □

**Definition 10.5.** A morphism  $f : X \rightarrow Y$  is an **epimorphism** (or epi) if whenever we have maps

$$X \xrightarrow{f} Y \begin{array}{c} \xrightarrow{g} \\ \xrightarrow{h} \end{array} Z$$

such that  $g \circ f = h \circ f$ ,  $g = h$ . (We can think of this as similar to surjectivity.)

A morphism  $f : X \rightarrow Y$  is a **monomorphism** (or mono) if whenever we have maps

$$Z \begin{array}{c} \xrightarrow{g} \\ \xrightarrow{h} \end{array} X \xrightarrow{f} Y$$

such that  $f \circ g = f \circ h$ ,  $g = h$ . (We can think of this as similar to injectivity).

**Example 10.6.** Some examples of categories are:

1. Sets: the objects are small sets, and morphisms are functions from one small set to another.

Here, the identity, domain, codomain, and composition functions should be clear.

We can see that if  $f : X \rightarrow Y$  is surjective, then whenever  $g : Y \rightarrow Z$  and  $h : Y \rightarrow Z$  have the property that  $g \circ f = h \circ f$ , then for every  $y \in Y$ , there exists some  $x \in X$  such that  $f(x) = y$  and then  $g(y) = g(f(x)) = h(f(x)) = h(y)$ , so  $g = h$ , and this is an epimorphism. However, if  $f$  is not surjective, then there is some  $y \in Y$  that is not in the image of  $f$ , and then we can construct  $g$  and  $h$  such that  $g \circ f = h \circ f$  but  $g(y) \neq h(y)$ . Thus the epimorphisms in this category are exactly the surjective maps.

Similarly, we can see that the monomorphisms in this category are the injective maps.

2. Groups: the objects are small groups and the morphisms are group homomorphisms. As before, the epimorphisms are all surjective homomorphisms and the monomorphisms are all injective homomorphisms.
3. Rings: the objects are small rings and the morphisms are ring homomorphisms. Again, the epimorphisms are all surjective homomorphisms and the monomorphisms are all injective homomorphisms.
4. Top: the objects are small topological spaces and the morphisms are continuous functions. Again, the monomorphisms are the injective functions, but we can have epimorphisms which are not surjective: the inclusion map

$$\mathbb{Q} \hookrightarrow \mathbb{R}$$

is not surjective, but it is an epimorphism (we know that if the image of  $g$  and  $h$  agree on all the rationals, then they have to agree on all the reals because they are continuous functions and the rationals are dense in the reals).

5.  $K$ -Vect: the objects are small  $K$ -vector spaces and the morphisms are  $K$ -linear maps.
6. Ab: the objects are abelian groups, and the morphisms are group homomorphisms.

**Definition 10.7.** A **covariant functor**  $F : \mathcal{C} \rightarrow \mathcal{D}$  is a function:

$$\begin{aligned} F : \text{ob}(\mathcal{C}) &\longrightarrow \text{ob}(\mathcal{D}) \\ F : \text{mor}(\mathcal{C}) &\longrightarrow \text{mor}(\mathcal{D}) \end{aligned}$$

that preserves the category structure, in the sense that

$$\begin{aligned} F(\operatorname{dom} f) &= \operatorname{dom} F(f) \\ F(\operatorname{cod} f) &= \operatorname{cod} F(f) \\ F(\operatorname{id}_X) &= \operatorname{id}_{F(X)} \\ F(f \circ g) &= F(f) \circ F(g). \end{aligned}$$

Intuitively, we can think of  $F$  as something that “preserves arrows” in the sense that for any

$$X \xrightarrow{f} Y$$

we get

$$FX \xrightarrow{Ff} FY$$

In contrast, a **contravariant functor**  $F : \mathcal{C} \rightarrow \mathcal{D}$  reverses arrows, in the intuitive sense that for any

$$X \xrightarrow{f} Y$$

we get

$$FX \xleftarrow{Ff} FY$$

Precisely, a contravariant functor  $F$  fulfills the properties that:

$$\begin{aligned} F(\operatorname{dom} f) &= \operatorname{cod} F(f) \\ F(\operatorname{cod} f) &= \operatorname{dom} F(f) \\ F(\operatorname{id}_X) &= \operatorname{id}_{F(X)} \\ F(f \circ g) &= F(g) \circ F(f). \end{aligned}$$

**Example 10.8.** Some examples of functors are

1. The forgetful functors

$$\mathbf{K}\text{-Vect} \rightarrow \mathbf{Ab} \rightarrow \mathbf{Group} \rightarrow \mathbf{Sets},$$

in which we just “forget” some of the group structure in each map. This is a *covariant* functor.

2. The functor  $H^i : \mathbf{Top} \rightarrow \mathbf{Ab}$  defined by  $X \mapsto H^i(X, \mathbb{Z})$  which maps  $i$  to its  $i^{\text{th}}$  singular cohomology. This is a *contravariant* functor.

As a warning,  $\pi_1$  would map topological spaces *with a point identified* to its corresponding fundamental group; it is not a functor  $\mathbf{Top} \rightarrow \mathbf{Group}$  because the fundamental group of a topological space depends on your starting point.

3.  $\mathbf{GL}_n : \mathbf{Rings} \rightarrow \mathbf{Groups}$  where  $R \mapsto \mathbf{GL}_n(R)$ , or the group of  $n \times n$  invertible matrices over  $R$ , is a covariant functor.
4.  $\operatorname{id}_{\mathcal{C}} : \mathcal{C} \rightarrow \mathcal{C}$  is a covariant functor.
5. The dual map  $*_i : \mathbf{K}\text{-Vect} \rightarrow \mathbf{K}\text{-Vect}$  defined by  $V \mapsto V^*$ , where we are mapping vector spaces to their dual, is a *contravariant* functor.

**Definition 10.9.** If  $F : \mathcal{C} \rightarrow \mathcal{D}$  is a functor, then we call  $F$  **faithful** if  $F : \operatorname{Hom}_{\mathcal{C}}(X, Y) \rightarrow \operatorname{Hom}_{\mathcal{D}}(FX, FY)$  (or  $F : \operatorname{Hom}_{\mathcal{C}}(X, Y) \rightarrow \operatorname{Hom}_{\mathcal{D}}(FY, FX)$  if  $F$  is contravariant) is injective.

Similarly  $F$  is **full** if these maps are surjective.

**Example 10.10.** Looking at the examples above, we have that:

1. The forgetful functors are faithful but not full (because all group homomorphisms have corresponding set morphisms, but not all set morphisms have a preimage which preserves group structure).
4. The identity functor is fully faithful.
5. The dual functor is faithful; we know that if we have

$$V \begin{array}{c} \xrightarrow{f} \\ \xrightarrow{g} \end{array} W$$

then the image is

$$V^* \begin{array}{c} \xleftarrow{f^*} \\ \xleftarrow{g^*} \end{array} W^*$$

where  $f^*$  is defined by  $\lambda \mapsto \lambda \circ f$ . But then we have that if  $f^* = g^*$ , then for all  $\lambda$ ,  $\lambda \circ f = \lambda \circ g$ , and if there exists some  $v$  such that  $f(v) \neq g(v)$  then we can define a  $\lambda$  such that  $\lambda(f(v)) \neq \lambda(g(v))$ , which is a contradiction. Thus, we must have  $f = g$ , and this is injective.

However, this is functor is not full because our functor is not always surjective in the case of infinite dimensional vector spaces; if we restricted this to finite dimensional vector spaces then this functor would be fully faithful.

**Definition 10.11.** A category  $\mathcal{C}$  is a **subcategory** of  $\mathcal{D}$  if  $\text{ob}(\mathcal{C}) \subset \text{ob}(\mathcal{D})$ ,  $\text{mor}(\mathcal{C}) \subset \text{mor}(\mathcal{D})$ , and  $\text{dom}$ ,  $\text{cod}$ ,  $\text{id}$ , and  $\circ$  are defined the same way in  $\mathcal{C}$  and  $\mathcal{D}$ .

As we might expect, we can compose functors, so that if we have

$$\mathcal{C} \xrightarrow{F} \mathcal{D} \xrightarrow{G} \mathcal{E}$$

then  $G \circ F : \mathcal{C} \rightarrow \mathcal{E}$  is also a functor.

Everything we've discussed above is probably somewhat familiar from defining things like groups and rings, but the following is unique to category theory:

**Definition 10.12.** If  $F, G : \mathcal{C} \rightarrow \mathcal{D}$  are functors then a **natural transformation**  $\phi : F \rightarrow G$  is a morphism  $\phi_X : FX \rightarrow GX$  for each  $X \in \text{ob}(\mathcal{C})$  such that, for any other morphism  $f : X \rightarrow Y \in \text{mor}(\mathcal{C})$ , the diagram

$$\begin{array}{ccc} FX & \xrightarrow{Ff} & FY \\ \phi_X \downarrow & & \downarrow \phi_Y \\ GX & \xrightarrow{Gf} & GY \end{array}$$

commutes.

**Example 10.13.** The determinant map  $\det : \text{GL}_n \rightarrow \text{GL}_1$  is a natural transformation because for any



ring homomorphism  $R \rightarrow S$ , we have that

$$\begin{array}{ccc} \mathrm{GL}_n(R) & \xrightarrow{\det} & \mathrm{GL}_1(R) \\ \downarrow f & & \downarrow f \\ \mathrm{GL}_n(S) & \xrightarrow{\det} & \mathrm{GL}_1(S) \end{array}$$

commutes (where the  $f$  in the diagram actually corresponds to  $\mathrm{GL}_n f$  or  $\mathrm{GL}_1 f$ , respectively, and means applying  $f$  to each entry of our matrix) because the determinant is a sort of “universal polynomial” on the elements of our matrix, so it will commute with any ring homomorphism.

We will look at more examples of natural transformations tomorrow, because it usually takes a while to wrap your head around.

## LECTURE 11: CATEGORY THEORY, II

For ease of understanding, in my notes for this lecture, I will use calligraphy letters ( $\mathcal{C}, \mathcal{D}$ ) to denote categories, capital letters ( $F$  and  $G$ ) to denote functors between categories, and bold letters ( $\phi, \psi$ ) to denote natural transformations.

**Example 11.1.** An important functor we forgot to mention last lecture is the **constant functor**  $C_y$ , for some object  $y \in \mathcal{D}$ , where for any category  $\mathcal{C}$ , we get the functor

$$\begin{aligned} C_y : \mathcal{C} &\longrightarrow \mathcal{D} \\ x &\mapsto y \\ f &\mapsto \text{id}_y \end{aligned}$$

for any  $x \in \text{ob}(\mathcal{C})$  and  $f \in \text{mor}(\mathcal{C})$ .

Now, let's continue our examples of natural transformations from last time:

**Example 11.2.**

2. We have the two functors  $\text{id} : \mathbf{K}\text{-Vect} \rightarrow \mathbf{K}\text{-Vect}$  and  $* \circ * : \mathbf{K}\text{-Vect} \rightarrow \mathbf{K}\text{-Vect}$ . What is the natural transformation between them?

(Note that we use the double dual instead of the dual because in order to have a natural transformation, we need both of our functors to be covariant or both of them to be contravariant.)

We want a natural transformation  $\mathbf{D} : \text{id} \rightarrow * \circ *$  such that for every  $V, W \in \text{ob}(\mathbf{K}\text{-Vect})$ , and  $f : V \rightarrow W \in \text{mor}(\mathbf{K}\text{-Vect})$ , we have a  $\phi_V : V \rightarrow V^{**}$  and  $\phi_W : W \rightarrow W^{**}$  such that the diagram:

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ \downarrow \mathbf{D}_V & & \downarrow \mathbf{D}_W \\ V^{**} & \xrightarrow{f^{**}} & W^{**} \end{array}$$

commutes. Remember that any  $w \in W^{**}$  is a function of  $\lambda \in W^*$ . We can see that in order to get this map to commute, we want  $\mathbf{D}_W(w)(\lambda) = \lambda(w)$ , for all  $\lambda \in W^*$ .

Then, doing a bit of algebra, we can check that we do actually get that for all  $v \in V$  and for all  $\lambda \in W^*$ ,

$$f^{**}(\mathbf{D}_V(v))(\lambda) = \mathbf{D}_W(f(v))(\lambda),$$

so this diagram commutes, as we desired.

3. For any functor  $F : \mathcal{C} \rightarrow \mathcal{D}$ , there is the identity transformation  $\mathbf{id} : F \rightarrow F$  where for any  $X \in \mathcal{C}$ ,  $\mathbf{id}_X : FX \rightarrow FX$  is the identity map.
4. For any  $f : Y \rightarrow Y' \in \text{mor}(\mathcal{D})$ ,  $\mathbf{C}_f : C_Y \rightarrow C_{Y'}$  is a natural transformation. Specifically, we have that for any  $X \in \mathcal{C}$ ,  $\mathbf{C}_{f,X} = f$ , because then for any  $g : X \rightarrow X' \in \text{mor}(\mathcal{C})$ ,

this diagram:

$$\begin{array}{ccc} C_Y X & \xrightarrow{c_Y g} & C_Y X' \\ \downarrow c_{f,X} & & \downarrow c_{f,X'} \\ C_{Y'} X & \xrightarrow{c_{Y'} g} & C_{Y'} X' \end{array}$$

becomes this:

$$\begin{array}{ccc} Y & \xrightarrow{\text{id}_Y} & Y \\ \downarrow f & & \downarrow f \\ Y' & \xrightarrow{\text{id}_{Y'}} & Y' \end{array}$$

which clearly commutes.

We can also compose natural transformations, in the way we would expect: if we have the chain

$$F \xrightarrow{\phi} G \xrightarrow{\psi} H$$

then  $\psi \circ \phi : F \rightarrow H$  is also a natural transformation.

**Definition 11.3.** We say that two functors are **equivalent** (denoted  $F \simeq G$ ) if there exist natural transformations  $\phi : F \rightarrow G$  and  $\psi : G \rightarrow F$  such that  $\psi \circ \phi = \text{id}_F$  and  $\phi \circ \psi = \text{id}_G$ .

**Exercise 11.4.** This implies that for every  $X \in \mathcal{C}$ , the maps  $\phi_X : FX \rightarrow GX$  and  $\psi_X : GX \rightarrow FX$  are mutually inverse isomorphisms.

**Example 11.5.** When restricted to finite-dimensional vector spaces,  $\text{id}_{\text{Fin-K-Vect}} \simeq * \circ *$ , because the natural transformation  $\mathbf{D}$  from before is invertible.

**Definition 11.6.** We say that  $F : \mathcal{C} \rightarrow \mathcal{D}$  is an **equivalence of categories** if there exists an inverse functor  $G : \mathcal{D} \rightarrow \mathcal{C}$  such that

$$F \circ G \simeq \text{id}_{\mathcal{D}} \text{ and } G \circ F \simeq \text{id}_{\mathcal{C}}$$

and  $F$  is covariant (this implies  $G$  is covariant).

If the above holds but  $F$  is contravariant, this is an **antiequivalence of categories**.

**Example 11.7.** The dual map  $* : \text{Fin-K-Vect} \rightarrow \text{Fin-K-Vect}$  is an antiequivalence of categories; its inverse is  $*$ .

We know this is an antiequivalence because we showed before that  $* \circ * \simeq \text{id}_{\text{Fin-K-Vect}}$ .

**Definition 11.8.** We say that  $\mathcal{C}$  is a **small category** if  $\text{ob}(\mathcal{C}), \text{mor}(\mathcal{C}) \in \mathcal{U}$ , where  $\mathcal{U}$  is our universe from the beginning of last lecture.

Let  $\mathcal{J}$  be a small category and let  $F$  be a functor  $F : \mathcal{J} \rightarrow \mathcal{C}$ .

**Definition 11.9.** By **limit** or **inverse limit** of  $F$  (denoted  $\lim F$  or  $\lim_{\leftarrow} F$ ), we mean an element  $X \in \text{ob } \mathcal{C}$  together with a natural transformation  $\phi : C_X \rightarrow F$  such that if  $X' \in \text{ob } \mathcal{C}$  and  $\psi : C_{X'} \rightarrow F$  is another natural transformation, there exists a unique  $\alpha : X' \rightarrow X \in \text{mor}(\mathcal{C})$  such that  $\psi = \phi \circ C_\alpha$ .

Remember that if  $\phi$  is a natural transformation, this means that for any  $Y, Y' \in \text{ob } \mathcal{J}$  and  $f : Y \rightarrow Y' \in \text{mor}(\mathcal{J})$ , we have that

$$\begin{array}{ccc} X & \xrightarrow{\phi_Y} & FY \\ \downarrow \text{id}_X & & \downarrow Ff \\ X & \xrightarrow{\phi_{Y'}} & FY' \end{array}$$

commutes, while the second part of this definition means that if there exists some  $X', \psi$  such that all diagrams of this form:

$$\begin{array}{ccc} X' & \xrightarrow{\psi_Y} & FY \\ & \searrow \psi_{Y'} & \downarrow Ff \\ & & FY' \end{array}$$

then there exists a unique  $\alpha$  (independent of our choice of  $Y$ ) such that the diagram

$$\begin{array}{ccccc} X' & & & & \\ & \searrow \alpha & & & \\ & & X & \xrightarrow{\phi_Y} & FY \\ & & & \searrow \phi_{Y'} & \downarrow Ff \\ & & & & FY' \end{array}$$

commutes.

**Example 11.10.**

- Suppose  $\mathcal{J}$  only has two objects, and its only morphisms are the identity morphisms for those objects:



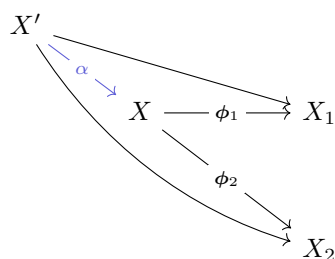
Then, any functor  $F : \mathcal{J} \rightarrow \mathcal{C}$  just has to identify some  $X_1, X_2 \in \text{ob}(\mathcal{C})$  to be the images of 1 and 2, respectively.

What is  $\lim_{\leftarrow} F$ ?

Well the only morphisms that  $\phi$  needs to commute with are the images of identity morphisms, which are still identity morphisms. So we just need some object in  $X \in \mathcal{C}$  and morphisms  $\phi_1 : X \rightarrow X_1$  and  $\phi_2 : X \rightarrow X_2$ .

Moreover, for any other  $X' \in \mathcal{C}$  with morphisms to  $X_1$  and  $X_2$ , there must be a unique  $\alpha : X' \rightarrow$

$X \in \text{mor}(\mathcal{C})$  such that the diagram



commutes.

Clearly, if  $\mathcal{C}$  was the category of rings, then  $X$  would have to be  $X_1 \times X_2$ , and the morphisms would be the corresponding projection maps.

In general, we say that if we have some small set  $I$ , we can create a category  $\mathcal{C}_I$  with its objects being elements of  $I$  and only identity morphisms. Then we say that the **product** of objects in any category is

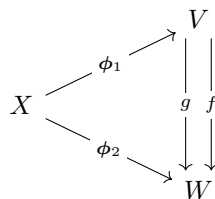
$$\prod_{i \in I} X_i = \lim_{\leftarrow} (\text{functor sending } i \mapsto X_i).$$

- Let  $\mathcal{J}$  be the category containing two objects, their identity morphisms, and two morphisms between them:



and a functor  $F : \mathcal{J} \rightarrow \mathbf{K}\text{-Vect}$ . To define this functor, we just need to pick two vector spaces  $V$  and  $W$  to be the images of the two objects, and then pick two  $K$ -linear maps  $f, g$  to be images of the two morphisms.

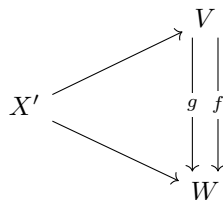
Then, an inverse limit  $(X, \phi)$  must have the property that



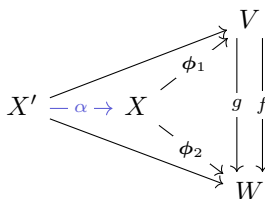
commutes, so for any  $x \in X$ ,

$$f(\phi_1(x)) = g(\phi_1(x)) = \phi_2(x).$$

Moreover, for any other  $X'$  with morphisms such that



commutes, there is a unique homomorphism  $\alpha : X' \rightarrow X$  such that



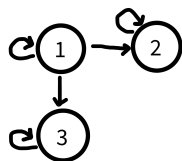
commutes.

To make this work, we take  $X = \ker(f - g)$ .

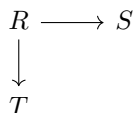
**Definition 11.11.** By a **colimit** or **direct limit** (denoted  $\text{colim } F$  or  $\varinjlim F$ ) of  $F : \mathcal{J} \rightarrow \mathcal{C}$ , we mean an object  $X \in \text{ob } \mathcal{C}$  and a natural transformation  $\phi : F \rightarrow C_X$  such that if there exists some  $X' \in \text{ob}(\mathcal{C})$  and a different natural transformation  $\psi : F \rightarrow C_{X'}$ , then there is a unique  $\alpha : X \rightarrow X' \in \text{mor}(\mathcal{C})$  such that  $\phi = C_\alpha \circ \psi$ .

This is exactly like the inverse limit, but with the arrows in the opposite direction.

**Example 11.12.** If we have a small category  $\mathcal{J}$  with three objects, their identity morphisms, and two morphisms between them:



then a functor  $F : \mathcal{J} \rightarrow \underline{\text{Rings}}$  is defined by three rings  $R, S, T$  and two ring morphisms  $R \rightarrow S$  and  $R \rightarrow T$ , so that we have the diagram:



Then, the direct limit  $\varinjlim F$  is just  $S \otimes_R T$ .

## LECTURE 12: CATEGORY THEORY, III

Let's review the definition of a **limit**.

**Reminder 12.1.** Consider any functor  $F : \mathcal{J} \rightarrow \mathcal{C}$ . Then, a limit  $\lim_{\leftarrow} F$  of this functor is an element  $X \in \text{ob}(\mathcal{C})$  along with a natural transformation  $\phi : C_X \rightarrow F$  (where  $C_X : \mathcal{J} \rightarrow \mathcal{C}$  is the functor that maps every object to  $X$  and every morphism to  $\text{id}_X$ ).

If we have any other  $X' \in \text{ob}(\mathcal{C})$  and natural transformation  $\phi' : C_{X'} \rightarrow F$ , then the definition of the limit tells us there is a unique morphism  $\alpha : X' \rightarrow X \in \text{mor}(\mathcal{C})$  such that the natural transformation  $\mathbf{C}_\alpha$  has the property that  $\phi' = \mathbf{C}_\alpha \circ \phi$ , so this diagram commutes:

$$\begin{array}{ccc} C_X & \xrightarrow{\phi} & F \\ \mathbf{C}_\alpha \uparrow & \nearrow \phi' & \\ C_{X'} & & \end{array}$$

As a reminder,  $\mathbf{C}_\alpha : C_{X'} \rightarrow C_X$  gives us a morphism  $C_{X'}J \rightarrow C_XJ$  for every  $J \in \text{ob}(\mathcal{J})$  such that, for any morphism  $f : J \rightarrow J' \in \text{mor}(\mathcal{J})$ , the diagram:

$$\begin{array}{ccc} C_{X'}J & \xrightarrow{C_{X'}f} & C_{X'}J' \\ \mathbf{C}_{\alpha,J} \downarrow & & \downarrow \mathbf{C}_{\alpha,J'} \\ C_XJ & \xrightarrow{C_Xf} & C_XJ' \end{array}$$

commutes. But we define  $\mathbf{C}_{\alpha,J}$  to be  $\alpha$  for every  $J \in \text{ob}(\mathcal{J})$ , because then we can see that since  $C_XJ = X$ ,  $C_Xf = \text{id}_X$ ,  $C_{X'}J = X'$ , and  $C_{X'}f = \text{id}_{X'}$ , so this diagram actually becomes

$$\begin{array}{ccc} X' & \xrightarrow{\text{id}_{X'}} & X' \\ \alpha \downarrow & & \downarrow \alpha \\ X & \xrightarrow{\text{id}_X} & X \end{array}$$

which clearly commutes.

Thus, when we say there is a unique  $\alpha : X' \rightarrow X$  that makes  $\mathbf{C}_\alpha$  commute with the other natural transformations, we mean that there is a unique  $\alpha : X' \rightarrow X$  such that for any  $J \in \text{ob}(\mathcal{J})$ ,  $\phi'_J = \phi_J \circ \alpha$ , where  $\phi'_J$  is a morphism  $X' \rightarrow FJ$  and  $\phi_J$  is a morphism  $X \rightarrow FJ$ .

The definition of a colimit is similar, but with arrows in the opposite direction (our  $\phi$  is now a natural transformation  $F \rightarrow C_X$ , and the unique homomorphism  $\alpha$  now maps  $X \rightarrow X'$ ).

**Lemma 12.2.** If  $(X, \phi)$  and  $(X', \phi')$  are two limits for  $F : \mathcal{J} \rightarrow \mathcal{C}$ , then there exists a unique isomorphism  $\alpha : X \rightarrow X'$  such that  $\phi' \circ \mathbf{C}_\alpha = \phi$ .

The existence of a morphism  $\alpha$  comes from the universal property of  $X'$ , and we get a similar  $\beta$  from the universal property of  $X$ . From there, it is not hard to show that  $\alpha$  and  $\beta$  are inverses.

**Lemma 12.3.** If  $(X, \phi)$  and  $(X', \phi')$  are two colimits for  $F : \mathcal{J} \rightarrow \mathcal{C}$ , then there exists a unique isomorphism  $\alpha : X \rightarrow X'$  such that  $\phi' = C_\alpha \circ \phi$ .

**Example 12.4.**

1. In the category Sets, small colimits and small limits always exist. For any functor  $F : \mathcal{J} \rightarrow \underline{\text{Sets}}$ , the limit  $\lim_{\leftarrow} F$  is subset of the Cartesian product:

$$\lim_{\leftarrow} F = \left\{ (x_J) \in \prod_{J \in \text{ob}(\mathcal{J})} FJ \mid \text{for all } f : J \rightarrow J' \in \text{mor}(\mathcal{J}), Ff(x_J) = x_{J'} \right\}.$$

This is the same inverse limit we discussed in an earlier pset.

2. In the category Rings, we also always have small colimits and small limits. The construction of limits is the same as above, but the colimit is a generalization of the tensor product, in the way we constructed it in the most recent problem set.

**Example 12.5.** Let us say  $\mathcal{J}$  has two objects (1) and (2), and just the identity morphisms for each object, and the morphism  $F : \mathcal{J} \rightarrow \mathcal{C}$  maps (1)  $\mapsto X_1$  and (2)  $\mapsto X_2$  for some  $X_1, X_2 \in \text{ob}(\mathcal{C})$ . Then, what is the direct and inverse limit for  $F$ , for some common categories  $\mathcal{C}$ ?

We have the following table:

$\mathcal{C}$	$\lim_{\leftarrow} F$	$\lim_{\rightarrow} F$
<u>Sets</u>	$X_1 \times X_2$	$X_1 \amalg X_2$ (this is the coproduct, which for sets is just the disjoint union)
<u>Rings</u>	$X_1 \times X_2$	$X_1 \otimes_{\mathbb{Z}} X_2$
<u>K-Vect</u>	$X_1 \oplus X_2$	$X_1 \oplus X_2$
<u>Groups</u>	$X_1 \times X_2$	$X_1 * X_2$ (this is the <b>free product</b> )

**Definition 12.6.** If we have two functors  $F : \mathcal{C} \rightarrow \mathcal{D}$  and  $G : \mathcal{D} \rightarrow \mathcal{C}$ , then  $F$  is a **left-adjoint for**  $G$  or  $G$  is a **right-adjoint for**  $F$  if for all  $X \in \text{ob}(\mathcal{C})$  and  $Y \in \text{ob}(\mathcal{D})$ , there exists a bijective map  $\phi_{X,Y} : \text{Hom}_{\mathcal{D}}(FX, Y) \rightarrow \text{Hom}_{\mathcal{C}}(X, GY)$  such that for all  $f : X \rightarrow X' \in \text{mor}(\mathcal{C})$ , the diagram:

$$\begin{array}{ccc} \text{Hom}_{\mathcal{D}}(FX, Y) & \xrightarrow{\phi_{X,Y}} & \text{Hom}_{\mathcal{C}}(X, GY) \\ \uparrow f' \mapsto f' \circ Ff & & \uparrow f' \mapsto f' \circ f \\ \text{Hom}_{\mathcal{D}}(FX', Y) & \xrightarrow{\phi_{X',Y}} & \text{Hom}_{\mathcal{C}}(X', GY) \end{array}$$



commutes, and similarly for all  $g : Y \rightarrow Y' \in \text{mor}(\mathcal{D})$ , the diagram:

$$\begin{array}{ccc} \text{Hom}_{\mathcal{D}}(FX, Y) & \xrightarrow{\phi_{X,Y}} & \text{Hom}_{\mathcal{C}}(X, GY) \\ \downarrow f' \mapsto g \circ f' & & \downarrow f' \mapsto Gg \circ f' \\ \text{Hom}_{\mathcal{D}}(FX, Y') & \xrightarrow{\phi_{X,Y'}} & \text{Hom}_{\mathcal{C}}(X, GY') \end{array}$$

commutes.

This relationship between the two functors is called a **adjunction**.

We can see that  $\phi_{X,Y}$  looks very similar to a natural transformation, and in fact we have an equivalent definition:

**Definition 12.7.** Let us say that we have functors  $F : \mathcal{C} \rightarrow \mathcal{D}$  and  $G : \mathcal{D} \rightarrow \mathcal{C}$  as before, and moreover that we have natural transformations  $\eta : \text{id}_{\mathcal{C}} \rightarrow G \circ F$  (so that each  $\eta_X$  is a morphism  $X \rightarrow G \circ FX$ ) and  $\mu : F \circ G \rightarrow \text{id}_{\mathcal{D}}$  (so that each  $\mu_Y$  is a morphism  $F \circ GY \rightarrow Y$ ). Then, we say that  $F$  is **left-adjoint to  $G$**  and  $G$  is **right-adjoint to  $F$**  if for any  $X \in \text{ob}(\mathcal{C})$  and  $Y \in \text{ob}(\mathcal{D})$ ,

$$\begin{aligned} \text{id}_{FX} &= \mu_{FX} \circ F\eta_X \\ \text{id}_{GY} &= G\mu_Y \circ \eta_{GY}. \end{aligned}$$

We can see that these equations make sense because  $\text{id}_{FX} \in \text{mor}(\mathcal{D})$ ,  $\eta_X \in \text{mor}(\mathcal{C})$ ,  $F$  maps  $\eta_X$  to an element of  $\text{mor}(\mathcal{D})$ , and  $FX \in \text{ob}(\mathcal{D})$  so  $\mu_{FX} \in \text{mor}(\mathcal{D})$ , and similarly for the second equation.

I am leaving it as an exercise to show that this is equivalent to the previous definition of adjunction; note that such  $\eta$  and  $\mu$  uniquely determine the adjunction between  $F$  and  $G$ .

(The above definition is slightly different from the way it was covered in lecture because I was using Wikipedia to understand it ☺)

**Example 12.8.** Let  $G : \underline{\text{Rings}} \rightarrow \underline{\text{Sets}}$  be the forgetful functor. This is a right-adjoint functor; let's look for a corresponding left-adjoint.

We want a covariant functor  $F : \underline{\text{Sets}} \rightarrow \underline{\text{Rings}}$  such that for any set  $\Omega$  and ring  $R$ ,

$$\text{Hom}_{\underline{\text{Rings}}}(F\Omega, R) \cong \text{Hom}_{\underline{\text{Sets}}}(\Omega, R).$$

We say that  $F(\Omega) = \mathbb{Z}[X_\omega]_{\omega \in \Omega}$ ; this is clearly a ring.

Then, we can see that this is an adjunction using the natural transformations  $\eta : \text{id}_{\underline{\text{Sets}}} \rightarrow G \circ F$  and  $\mu : F \circ G \rightarrow \text{id}_{\underline{\text{Rings}}}$ . This means each  $\eta_\Omega$  is a morphism  $\Omega \rightarrow \mathbb{Z}[X_\omega]$ , and we can see it must be the morphism  $\omega \mapsto X_\omega$ . Similarly, each  $\mu_R$  is a morphism  $\mathbb{Z}[X_r]_{r \in R} \rightarrow R$  and we can see it must be the morphism defined by  $X_r \mapsto r$  and  $1 \mapsto 1_R$ .

For the following two lemmas, refer to the Canvas notes on adjunctions, as we don't have time to prove them in class:

**Lemma 12.9.** Suppose we have functors  $F : \mathcal{C} \rightarrow \mathcal{D}$  and  $G : \mathcal{D} \rightarrow \mathcal{C}$ , so that  $F$  is left-adjoint to  $G$ . Then  $G$  preserves small limits and  $F$  preserves small colimits.

**Theorem 12.10.** Up to some set-theoretic considerations, the converse is true. That is, if we know (something slightly stronger than)  $G$  preserves limits, it must have a left-adjoint, and if we know (something slightly stronger than)  $F$  preserves colimits, it must have a right-adjoint.

## LECTURE 13: MODULES, I

**Definition 13.1.** We say that  $M$  is an  $R$ -**module** if  $(M, +)$  is an abelian group and  $R$  acts on  $M$  with group action  $(r, m) \mapsto r \cdot m$  such that for all  $r, s \in R, m_1, m_2 \in M$

$$\begin{aligned}(1, m) &= 1 \cdot m = m \\ (r + s) \cdot m &= r \cdot m + s \cdot m \\ r \cdot (m_1 + m_2) &= r \cdot m_1 + r \cdot m_2 \\ r \cdot (s \cdot m) &= (rs) \cdot m.\end{aligned}$$

**Example 13.2.**

1. If  $R$  is a field, then  $R$ -modules are  $R$ -vector spaces.
2. Any abelian group is a  $\mathbb{Z}$ -module, defined by the fact that

$$n \cdot m = \left( \underbrace{1 + \cdots + 1}_{n \text{ times}} \right) \cdot m = \underbrace{m + \cdots + m}_{n \text{ times}}.$$

3.  $R$  is an  $R$ -module.
4. If  $I \triangleleft R$ , then  $R/I$  is an  $R$ -module.
5. If  $\phi : R \rightarrow S$  is a ring homomorphism, then  $S$  is an  $R$ -module, defined by

$$r \cdot s = \phi(r)s.$$

6.  $\mathbb{Q}^2$  is a module over  $\mathbb{Q}[T]$ , where for  $x, y, z \in \mathbb{Q}$ ,

$$z \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} zx \\ zy \end{pmatrix}$$

and

$$T \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ -x \end{pmatrix}.$$

**Definition 13.3.** We say that  $\phi : M \rightarrow N$  is a **morphism of  $R$ -modules** or an  **$R$ -linear map** if for all  $r \in R, m, n \in M$

$$\phi(r \cdot m + n) = r\phi(m) + \phi(n).$$

Specifically, taking  $m = 0$  and  $r = 1$ , this implies that  $\phi(0) = 0$ .

**Definition 13.4.** We say that  $N$  is an  **$R$ -submodule of  $M$**  if  $N$  is a nonempty subset of  $M$  (with the same operations) and for any  $m, n \in N$  and any  $r \in R, r \cdot m + n \in N$ .

**Example 13.5.**

1. The  $R$ -submodules of  $R$  are the ideals of  $R$ .

2.  $\{0\} \subset M$  is an  $R$ -submodule of  $M$ .

**Definition 13.6.** We say that  $R\text{-Mod}$  is the category of small  $R$ -modules.

**Lemma 13.7.** The ideal  $(0)$  is an initial object and terminal object of  $R\text{-Mod}$ .

**Lemma 13.8.** For any  $R$ -modules  $M, N$ ,  $\text{Hom}_{R\text{-Mod}}(M, N)$  is an abelian group, and even an  $R$ -module. We can see that for any  $r \in R$ ,  $f, g \in \text{Hom}_{R\text{-Mod}}(M, N)$ , we can define  $r \cdot f + g$  to be the map

$$(rf + g)(m) = r \cdot f(m) + g(m).$$

Moreover, the map

$$\begin{aligned} \text{Hom}_{R\text{-Mod}}(M, N) \times \text{Hom}_{R\text{-Mod}}(N, P) &\longrightarrow \text{Hom}_{R\text{-Mod}}(M, P) \\ (f, g) &\longmapsto g \circ f \end{aligned}$$

is an  $R$ -bilinear map, in the sense that for any  $f \in \text{Hom}_{R\text{-Mod}}(M, N)$ , the map

$$\begin{aligned} \text{Hom}_{R\text{-Mod}}(N, P) &\longrightarrow \text{Hom}_{R\text{-Mod}}(M, P) \\ g &\longmapsto g \circ f \end{aligned}$$

is  $R$ -linear and for any  $g \in \text{Hom}_{R\text{-Mod}}(N, P)$ , the map

$$\begin{aligned} \text{Hom}_{R\text{-Mod}}(M, N) &\longrightarrow \text{Hom}_{R\text{-Mod}}(M, P) \\ f &\longmapsto g \circ f \end{aligned}$$

is also  $R$ -linear.

**Definition 13.9.** We say that

$$M \oplus N = \{(m, n) \mid m \in M, n \in N\},$$

with the operations defined as

$$r \cdot (m, n) + (m', n') = (r \cdot m + m', r \cdot n + n').$$

We have the natural inclusion and projection maps

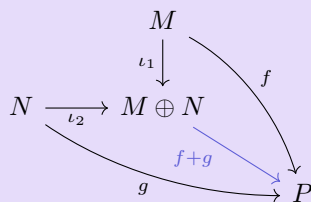
$$\begin{aligned} \iota_1 : M &\hookrightarrow M \oplus N, & \iota_2 : N &\hookrightarrow M \oplus N \\ \pi_1 : M \oplus N &\twoheadrightarrow M, & \pi_2 : M \oplus N &\twoheadrightarrow N, \end{aligned}$$

and we can see that

$$\begin{aligned} \pi_1 \circ \iota_1 &= \text{id}_M, & \pi_2 \circ \iota_2 &= \text{id}_N \\ \pi_2 \circ \iota_1 &= 0, & \pi_1 \circ \iota_2 &= 0 \\ \iota_1 \circ \pi_1 + \iota_2 \circ \pi_2 &= \text{id}_{M \oplus N}. \end{aligned}$$

**Lemma 13.10.** If  $f : M \rightarrow P$  and  $g : N \rightarrow P$  are morphisms of  $R$ -modules, there exists a unique  $R$ -module morphism  $f + g : M \oplus N \rightarrow P$  such that  $(f + g) \circ \iota_1 = f$  and  $(f + g) \circ \iota_2 = g$ , so there is a

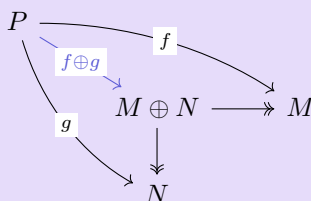
unique  $f + g$  that makes



commute.

This is the universal property of the **coproduct**.

If we have  $R$ -module morphisms  $f : P \rightarrow M$  and  $g : P \rightarrow N$ , then there exists a unique  $f \oplus g : P \rightarrow M \oplus N$  that makes the diagram



commute.

This is the universal property of the **product**.

Note that  $M \oplus N$  is both the **product** and **coproduct** of  $M$  and  $N$ ; this is true for any finite number of modules.

**Lemma 13.11.** If  $f : M \rightarrow N$  is a  $R$ -Mod morphism, then

$$\ker(f) = \{m \in M \mid f(m) = 0\}$$

is an  $R$ -submodule of  $M$ , and

$$\text{im}(f) = \{f(m) \mid m \in M\},$$

which is an  $R$ -submodule of  $N$ .

**Lemma 13.12.** If  $N$  is an  $R$ -submodule of  $M$ , then the quotient abelian group  $M/N$  is also an  $R$ -module.

We have the projection morphism

$$\begin{aligned} \pi : M &\twoheadrightarrow M/N \\ m &\mapsto m + N. \end{aligned}$$

For any morphism  $f : M \rightarrow N$ , we say that  $\text{coker } f = N/\text{im } f$ .

Then,  $M/N = \text{coker}(N \hookrightarrow M)$  and  $\text{im } f = \ker(N \rightarrow \text{coker } f)$ .

If  $f : N \hookrightarrow M$  (so  $f$  is injective), then

$$N \cong \ker(M \twoheadrightarrow \text{coker } f),$$

and if  $f : N \twoheadrightarrow M$  (so  $f$  is surjective), then

$$M \cong \text{coker}(\ker f \twoheadrightarrow N).$$

**Definition 13.13.** We say that a pair of maps

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

is **exact** at  $N$  if  $\text{im}(f) = \ker(g)$  (so  $g \circ f = 0$  and  $g(n) = 0$  implies  $n \in \text{im } f$ ).

A chain

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$$

is **short exact** if it is exact at  $M, N$ , and  $P$ , so  $M \hookrightarrow N$  and  $N \twoheadrightarrow P$ .

**Lemma 13.14.** Our category  $\mathbf{R}\text{-Mod}$  is an abelian category.

For any small sets  $I$  and  $R$ -modules  $M_i$ , the **product** or **direct product** is

$$\prod_{i \in I} M_i = \{(m_i) \mid m_i \in M_i\}$$

and the **coproduct** or **direct sum** is

$$\bigoplus_{i \in I} M_i = \left\{ (m_i) \in \prod_{i \in I} M_i \mid m_i = 0 \text{ for all but finitely many } i's \right\}.$$

$\mathbf{R}\text{-Mod}$  also contains all its small limits and colimits. For any functor  $F : \mathcal{J} \rightarrow \mathbf{R}\text{-Mod}$ , we have

$$\lim_{\leftarrow} F = \left\{ (m_j) \in \prod_{j \in \text{ob}(\mathcal{J})} F_j \mid \text{for all } \phi : i \rightarrow j \in \text{mor}(\mathcal{J}), F\phi(m_i) = m_j \right\}$$

and if we let  $N$  be the module generated by

$$\left\{ (m_j) \in \prod_{j \in \text{ob}(\mathcal{J})} F_j \mid \text{there exists } \phi \in \text{mor}(\mathcal{J}) \text{ such that } (m_j) = \iota_i(m_i) - \iota_j(F\phi(m_i)) \right\},$$

then

$$\lim_{\rightarrow} F = \left( \bigoplus_{j \in \text{ob}(\mathcal{J})} F(j) \right) / N.$$

**Example 13.15.** Let  $\Omega$  be a small set. Then we let

$$F_R(\Omega) = \bigoplus_{\omega \in \Omega} R.$$

We can see that every element of  $F_R(\Omega)$  can be thought of as a function  $f : \Omega \rightarrow R$  such that  $f(\omega) = 0$  for all but finitely many  $\omega \in \Omega$ .

As an example, the function

$$e_\omega(\omega') = \begin{cases} 1 & \text{if } \omega' = \omega \\ 0 & \text{otherwise} \end{cases}$$

is an element of  $F_R(\omega)$ , which looks something like  $(0, \dots, 0, 1, 0, \dots, 0)$ .

Since each element in  $F_R(\Omega)$  can be expressed as

$$\sum_{\omega \in \Omega} r_\omega e_\omega$$

for some  $r_\omega \in R$  (and the  $e_\omega$ 's are linearly independent), we can say that  $\{e_\omega\}$  is a basis for  $F_R(\Omega)$  and this is a **free module on  $\Omega$** .

**Lemma 13.16.** If we think of  $F_R$  as a functor  $\underline{\text{Sets}} \rightarrow \text{R-Mod}$ , then it is left-adjoint to the forgetful functor  $\text{R-Mod} \rightarrow \underline{\text{Sets}}$ .

*Proof.* First, we can see that for any  $\Omega \in \underline{\text{Sets}}$  and  $M \in \text{R-Mod}$ ,

$$\text{Hom}_{\text{R-Mod}}(F_R(\Omega), M) \cong \text{Hom}_{\underline{\text{Sets}}}(\Omega, M),$$

via the bijections

$$\begin{array}{ccc} \phi & \longmapsto & (\omega \mapsto \phi(e_\omega)) \\ \left( (r_\omega) \mapsto \sum_{\omega \in \Omega} r_\omega \psi(\omega) \right) & \longleftarrow & \psi \end{array}$$

□

## LECTURE 14: MODULES, II

Last lecture, we left off describing the free module on  $\Omega$ , for any set  $\Omega$ .

We said that the function  $F_R(\Omega)$  is a left-adjoint for the forgetful functor, which implies that for any set morphism  $\Omega \rightarrow M$ , where  $M$  is an  $R$ -module, there exists a unique  $R$ -module morphism  $F_R(\Omega) \rightarrow M$  that makes the diagram

$$\begin{array}{ccc} F_R(\Omega) & \xrightarrow{\quad} & M \\ & \swarrow \quad \searrow & \\ & \Omega & \end{array}$$

commute.

**Definition 14.1.** We say that  $M$  is **free** if  $M \cong F_R(\Omega)$  for some  $\Omega$ .

This implies there is some  $\mathcal{B} \subset M$  such that  $F_R(\mathcal{B}) \cong M$ , using the isomorphism  $e_b \mapsto b$ . We call  $\mathcal{B}$  a **basis** for  $M$ .

Note that saying  $F_R(\mathcal{B}) \cong M$  is equivalent to saying that every  $m \in M$  can be expressed uniquely as a sum of the form

$$\sum_{i=1}^n r_i b_i \quad b_i \in \mathcal{B}, r_i \in R.$$

**Example 14.2.**

1. Since we know that any vector space has a basis, any module over a field is free.
2.  $\mathbb{Q}$  is not free as a  $\mathbb{Z}$  module, because it cannot be generated by a single element, and any two elements in  $\mathbb{Q}$  are linearly dependent.

$\mathbb{Z}/2\mathbb{Z}$  is not free as a  $\mathbb{Z}$ -module, because  $\{0\}$  and  $\{1\}$  are the only one-element sets, and both of these are linearly dependent sets since  $1 \cdot 0 = 0$  and  $2 \cdot 1 = 2 = 0$ .

Intuitively, it is very unlikely that an arbitrary module over a general ring is free. Also, it is fine for a free module to have an infinite basis, but because we are taking the direct sum (not the direct product) over this basis, we need all the elements of the module to be expressed as linear combinations of finitely many basis elements.

**Proposition 14.3.** If  $F_R(\Omega) \cong F_R(\Omega')$  then  $\Omega$  and  $\Omega'$  can be put in bijection.

We will not prove this in class, but the trick is to show that for a maximal ideal  $\mathfrak{m} \triangleleft R$ ,  $F_R(\Omega) \cong F_R(\Omega')$  implies  $F_{R/\mathfrak{m}}(\Omega) \cong F_{R/\mathfrak{m}}(\Omega')$ , and since  $R/\mathfrak{m}$  is a field, we are now working within vector spaces, where we know this result is true.

With the above proposition, we can now have the following definition:

**Definition 14.4.** If  $M$  is free, we can define the **rank** of  $M$  to be  $\#\Omega$ , for any set  $\Omega$  such that  $M \cong F_R(\Omega)$ .



**Definition 14.5.** If  $\Omega \subset M$  is an arbitrary subset, we say that the **submodule generated by  $\Omega$**  is

$$\langle \Omega \rangle = \text{im}(F_R(\Omega) \rightarrow M) = \left\{ \sum_{i=1}^n r_i \omega_i \mid r_i \in R, \omega_i \in \Omega \right\}.$$

**Proposition 14.6.** If  $N$  is a submodule of  $M$  containing  $\Omega$ , then  $\langle \Omega \rangle \subset N$ .

**Proposition 14.7.** If  $N_1, N_2 \subset M$  are submodules then  $N_1 \cap N_2$  is also a submodule, and it is the largest submodule contained in both  $N_1$  and  $N_2$ . Also,

$$N_1 + N_2 = \{n_1 + n_2 \mid n_i \in N_i\}$$

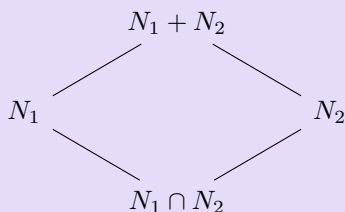
is a submodule, and it is the smallest submodule containing  $N_1$  and  $N_2$ .

**Proposition 14.8.** Analogous to ideals,

$$N_1 + N_2 / N_2 \cong N_1 / N_1 \cap N_2,$$

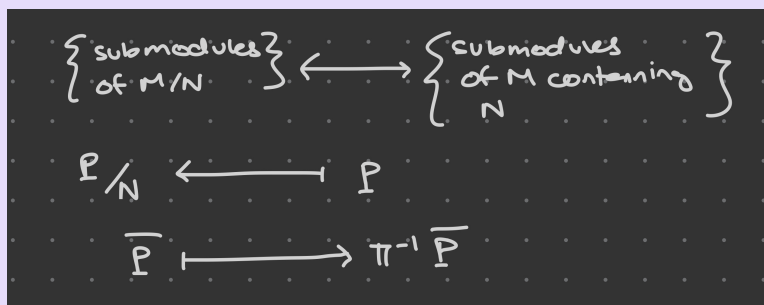
using the isomorphism  $n + N_2 \longleftrightarrow n + N_1 \cap N_2$ .

We can visualize this via the diamond



where pairs of parallel lines represent quotients that are isomorphic.

**Proposition 14.9.** If  $N \subset M$  is a submodule, there exists a bijection



where  $\pi$  is the projection map  $M \rightarrow M/N$ .

**Definition 14.10.** We say that the **dual** of  $M$  is

$$M^* = \text{Hom}_R(M, R).$$

This is not as nice as the dual in vector spaces, for example:

**Example 14.11.** If we consider  $\mathbb{Z}/2\mathbb{Z}$  as a  $\mathbb{Z}$ -module, then

$$(\mathbb{Z}/2\mathbb{Z})^* = \text{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}).$$

But we know that any such homomorphism  $f$  has the property that  $f(0) = 0$  and if  $f(1) = a$  then  $2a = 2f(1) = f(2) = f(0) = 0$ , so  $a = 0$ . Thus, in this case the dual is just  $\{0\}$ .

**Definition 14.12.** We say that the **endomorphisms** of  $M$  are

$$\text{End}_R(M) = \text{Hom}_R(M, M).$$

**Proposition 14.13.** If  $M$  is an  $R$ -module and  $T \in \text{End}_R(M)$ , then  $M$  becomes an  $R[X]$  module via the operation

$$(f_0 + f_1X + \cdots + f_dX^d) \cdot m = f_0m + f_1Tm + f_2T^2m + \cdots + f_dT^dm.$$

**Proposition 14.14.** If  $I \triangleleft R$  then

$$IM = \left\{ \sum_{i=1}^n r_i m_i \mid r_i \in I, m_i \in M \right\}$$

is submodule of  $M$ .

**Example 14.15.** If we have the ideal  $(2) \triangleleft R$  then

$$(2)(\mathbb{Z} \oplus \mathbb{Z}) = 2\mathbb{Z} \oplus 2\mathbb{Z}.$$

**Definition 14.16.** If  $\Omega \subset M$  is a subset of an  $R$ -module, then the **annihilator in  $R$  of  $\Omega$**  is

$$\text{Ann}_R(\Omega) = \{r \in R \mid r\omega = 0 \text{ for all } \omega \in \Omega\} \triangleleft R.$$

**Example 14.17.**  $\text{Ann}_R(R/I) = I$ .

**Example 14.18.** Consider  $\mathbb{Q}^2$  as a  $\mathbb{Q}[X]$ -module where  $X$  acts by  $T$ , where

$$T \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ -x \end{pmatrix}.$$

What is  $\text{Ann}_{\mathbb{Q}[X]}(\mathbb{Q}^2)$ ?

We know that

$$\text{Ann}_{\mathbb{Q}[X]}(\mathbb{Q}^2) = \{f \in \mathbb{Q}[X] \mid f(T) = 0\} \triangleleft \mathbb{Q}[X].$$

We can see that  $X^2 + 1 \in \text{Ann}_{\mathbb{Q}[X]}(\mathbb{Q}^2)$ , and moreover we can see that if  $f \in \text{Ann}_{\mathbb{Q}[X]}(\mathbb{Q}^2)$ , then by the division algorithm we can write

$$f(X) = q(X)(X^2 + 1) + (aX + b)$$

for some rationals  $a, b$ . But this implies  $aX + b \in \text{Ann}_{\mathbb{Q}[X]}(\mathbb{Q}^2)$ , so for all  $x, y \in \mathbb{Q}$ ,

$$(aT + b) \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ay + bx \\ -ax + by \end{pmatrix} = 0.$$

Since we want this to be true for all rational  $x, y$ , we can take an arbitrary one, such as  $x = 1, y = 0$  and see that we need  $\begin{pmatrix} b \\ -a \end{pmatrix} = 0$ , which implies  $a$  and  $b$  are both 0, and  $f$  is a multiple of  $X^2 + 1$ .

Thus,  $\text{Ann}_{\mathbb{Q}[X]}(\mathbb{Q}^2) = (X^2 + 1) \triangleleft \mathbb{Q}[X]$ .

**Lemma 14.19.** If  $M$  is an  $R$ -module then the following are equivalent:

1. every submodule of  $M$  is finitely generated
2. any nonempty set of submodules of  $M$  contains a maximal element

The proof is exactly the same as for ideals.

**Definition 14.20.** If the above conditions hold, then we say  $M$  is **noetherian**.

**Lemma 14.21.**  $R$  is noetherian as an  $R$ -module if and only if  $R$  is noetherian as a ring.

This is just because the submodules of  $R$  are the ideals of  $R$ .

**Lemma 14.22.** All submodules and quotient modules of noetherian modules are noetherian.

This follows from property (2) of being noetherian.

**Lemma 14.23.** If  $M/N$  and  $N$  are noetherian, so is  $M$ .

*Proof.* Let  $P \subset M$  be a submodule. Then  $N \cap P$  is a submodule of  $N$ , so it is finitely generated; we can say

$$N \cap P = \langle n_1, \dots, n_r \rangle.$$

Similarly, there is a map  $P/N \cap P \hookrightarrow M/N$ , so since  $M/N$  is noetherian, we can say

$$P/N \cap P = \langle m_1 + N \cap P, \dots, m_s + N \cap P \rangle.$$

Then, we claim

$$P = \langle n_1, \dots, n_r, m_1, \dots, m_s \rangle.$$

To see this, for any  $p \in P$ , we know that since  $P/N \cap P$  is finitely generated by  $\langle m_i \rangle$ , we can find some  $r_i \in R$  such that

$$p - \sum_{i=1}^s r_i m_i \in N \cap P,$$

and then since this difference is in  $N \cap P$ , which is generated by  $\langle n_i \rangle$ , we know there is some  $r_j \in R$  such that

$$p = \sum_{j=1}^r r_j n_j + \sum_{i=1}^s r_i m_i.$$

□

**Lemma 14.24.** If  $M, N$  are noetherian, then  $M \oplus N$  is noetherian.

We know that  $M \oplus N/N \cong M$ , so this follows from the previous lemma.

**Lemma 14.25.** If  $R$  is noetherian and  $M$  is a finitely generated  $R$ -module then  $M$  is noetherian.

*Proof.* We know since  $M$  is finitely generated that there is some finite set  $\Omega$  such that  $F_R(\Omega) \twoheadrightarrow M$ , so  $M$  is a submodule of  $F_R(\Omega)$ . But  $F_R(\Omega)$  is a direct sum of finitely many copies of  $R$ , so by the previous lemma it is noetherian, and then we know that a submodule of a noetherian module is also noetherian, so  $M$  must be noetherian.  $\square$

If  $D \subset R$  is multiplicative, then we can define an equivalence relation on  $M \times D$  by

$$(m, d) \sim (n, e) \iff f(em - dn) \text{ for some } f \in D.$$

Then  $D^{-1}M$  is the set of equivalence classes  $m/d = [(m, d)]$ .

We leave it as an exercise to check that the operations are well-defined and this is a  $D^{-1}R$ -module.

Then,

$$\begin{aligned} M &\longrightarrow D^{-1}M \\ m &\longmapsto m/1 \end{aligned}$$

is a morphism of  $R$ -modules.

For a prime ideal  $\varphi \triangleleft R$ , we use  $M_\varphi$  to denote  $(R - \varphi)^{-1}M$ .

For an element  $f \in R$ , we use  $M_f$  to denote  $\{1, f, f^2, \dots\}^{-1}M$ .

**Definition 14.26.** We say that a submodule  $N \subset M$  is **saturated with respect to  $D$**  if for any  $m \in M$ ,  $d \in D$  such that  $dm \in N$ , this implies  $m \in N$ .

**Definition 14.27.** The  **$D$ -saturation of  $N$**  is the set

$$\{m \in M \mid \text{there exists } d \in D \text{ such that } dm \in N\},$$

and it is the smallest saturated submodule containing  $N$ .

## LECTURE 15: MODULES, III

Last time, we left off talking about fractions and saturations of modules.

**Example 15.1.** Consider the ring  $R = \mathbb{Z}$  and  $D = \mathbb{Z} - (3)$ .

If we look at  $\mathbb{Z}/(2)$  as a  $\mathbb{Z}$ -module, then

$$D^{-1}(\mathbb{Z}/(2)) \cong \{0\}$$

because  $2 \in D$  so for any  $\frac{a+(2)}{b}$ , this is congruent to  $\frac{2a+(2)}{2b} = \frac{0+(2)}{b}$ .

If we look at  $\mathbb{Z}/(3)$  as a  $\mathbb{Z}$ -module, then

$$D^{-1}(\mathbb{Z}/(3)) \cong \mathbb{Z}/(3).$$

To see this, consider the map

$$\begin{aligned} \mathbb{Z}/(3) &\longrightarrow D^{-1}(\mathbb{Z}/(3)) \\ a + (3) &\longmapsto \frac{a + (3)}{1}. \end{aligned}$$

This is injective because if  $\frac{a+(3)}{1} = \frac{0}{1}$ , then there exists some  $d \in D$  such that  $d(a + (3)) = 0 + (3)$ , but since  $d$  is not a multiple of 3, we get that  $a = 0$ . It is surjective because for any  $\frac{a+(3)}{d}$ , we can take  $b = ad^{-1} \in \mathbb{Z}/3\mathbb{Z}$  (since this is a field, so we can take inverses), and we get that

$$b + (3) \mapsto \frac{b + (3)}{1} = \frac{ad^{-1} + (3)}{1} = \frac{a + (3)}{d}.$$

What is the  $D$ -saturation of  $(3)/(6) \subset \mathbb{Z}/(6)$ , as  $\mathbb{Z}$ -modules?

By definition, this is the set

$$\{a + (6) \mid \text{there exists } d \in D \text{ with } da + (6) \in (3)/(6)\},$$

but we know that  $3 \nmid d$  for any  $d \in D$ , so since  $3 \mid ad$ , we get that  $3 \mid a$ , so this is just the original submodule  $(3)/(6)$ .

What is the  $D$ -saturation of  $(2)/(6) \subset \mathbb{Z}/(6)$ ?

By definition, this is the set

$$\{a + (6) \mid \text{there exists } d \in D \text{ with } da + (6) \in (2)/(6)\}.$$

But we can always take  $d = 2$  to make  $da + (6) \in (2) + (6)$ , so this is the entire set  $\mathbb{Z}/(6)$ .

Let  $\iota$  be the injective map  $M \rightarrow D^{-1}M$ ,  $m \mapsto m/d$ . This is an  $R$ -linear map.

We have a universal property of the fraction module:

**Lemma 15.2.** If  $N$  is a  $D^{-1}R$ -module and  $f : M \rightarrow N$  is  $R$ -linear, then there exists a unique  $D^{-1}R$ -

linear map  $\tilde{f} : D^{-1}M \rightarrow N$  with  $\tilde{f} \circ \iota = f$ ; that is, there is a unique  $\tilde{f}$  that makes this diagram commute:

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \iota \downarrow & \nearrow \tilde{f} & \\ D^{-1}M & & \end{array}$$

*Proof.* We can see that if such a map exists, then it must map  $\tilde{f}(m/1) = f(m)$ , and since it is  $D^{-1}R$ -linear, it must map  $\tilde{f}(m/d) = 1/df(m)$ .

What remains is to check that this map is well-defined and a module homomorphism; we leave this as an exercise.  $\square$

**Definition 15.3.** If  $f : M \rightarrow N$  is a morphism of  $R$ -modules, then  $D^{-1}f : D^{-1}M \rightarrow D^{-1}N$  is the map defined by  $m/d \mapsto f(m)/d$ , and it is a morphism of  $D^{-1}R$ -modules.

We have a bunch of lemmas, where we leave the proofs as short exercises (some of these will be homework problems).

**Lemma 15.4.**  $D^{-1}(M/N) \cong (D^{-1}M)/(D^{-1}N)$ , via the map  $\frac{m+N}{d} \mapsto m/d + D^{-1}N$ .

**Lemma 15.5.**  $D^{-1}(M \oplus N) = D^{-1}M \oplus D^{-1}N$ .

**Lemma 15.6.**  $D^{-1}$  commutes with any small colimit and any finite limit.

Note that  $D^{-1}$  does not commute with any (infinite) limit: the map

$$\begin{aligned} \left( \prod_{i=1}^{\infty} \mathbb{Z} \right)_{(0)} &\longrightarrow \prod_{i=1}^{\infty} \mathbb{Z}_{(0)} = \prod_{i=1}^{\infty} \mathbb{Q} \\ \frac{(m_i)}{d} &\longmapsto \left( \frac{m_i}{d} \right) \end{aligned}$$

is injective but not surjective, because we can have unbounded fractions on the RHS but only bounded fractions on the LHS.

**Lemma 15.7.**  $D^{-1}F_R(\Omega) \cong F_{D^{-1}R}(\Omega)$ .

**Lemma 15.8.** If  $I \triangleleft R$ , then  $D^{-1}(IM) \cong (D^{-1}I)(D^{-1}M)$ .

**Lemma 15.9.** If  $M \xrightarrow{f} N \xrightarrow{g} P$  is exact at  $N$  then

$$D^{-1}M \xrightarrow{D^{-1}f} D^{-1}N \xrightarrow{D^{-1}g} D^{-1}P$$

is exact at  $D^{-1}N$ .

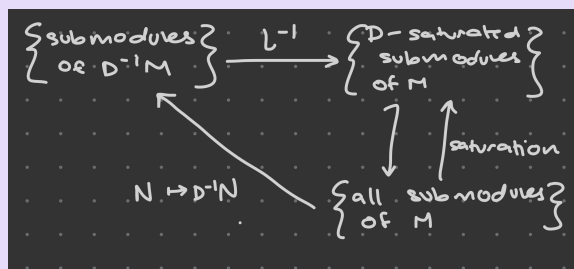
**Lemma 15.10.** If  $0 \rightarrow M \rightarrow N \rightarrow P \rightarrow 0$  is short exact then so is

$$0 \rightarrow D^{-1}M \rightarrow D^{-1}N \rightarrow D^{-1}P \rightarrow 0.$$

**Lemma 15.11.** If we have a  $R$ -module morphism  $f : M \rightarrow N$ , then

$$\begin{aligned} \ker(D^{-1}f) &= D^{-1}(\ker f) \\ \text{coker}(D^{-1}f) &= D^{-1}(\text{coker } f). \end{aligned}$$

**Lemma 15.12.** Remember that  $\iota : M \rightarrow D^{-1}M$  is the injective map defined before. Then, the diagram:



commutes, and  $\iota^{-1}$  is a bijection between these two sets.

Here, the fact that  $\iota^{-1}$  commutes follows from the fact that the diagram commutes, because we can show via diagram-chasing that this means  $\iota^{-1}$  must be injective and surjective.

The following lemma requires more advanced techniques to prove than just an exercise; it may be a homework problem later on:

**Lemma 15.13.** If  $R$  is noetherian and  $M$  is finitely generated over  $R$ , then

$$D^{-1} \text{Hom}_R(M, N) \cong \text{Hom}_{D^{-1}R}(D^{-1}M, D^{-1}N).$$

**Example 15.14.** If we take  $R = \mathbb{Z}$  and  $D = \mathbb{Z} - (3)$ , we get that

$$D^{-1}(\mathbb{Z}/(6)) = D^{-1}(\mathbb{Z}/(2) \oplus \mathbb{Z}/(3)).$$

But then, applying [Lemma 15.5](#), we get that this equals

$$D^{-1}(\mathbb{Z}/(6)) = D^{-1}(\mathbb{Z}/(2)) \oplus D^{-1}(\mathbb{Z}/(3)),$$

and applying what we found before, we get

$$D^{-1}(\mathbb{Z}/(6)) = 0 \oplus \mathbb{Z}/(3) = \mathbb{Z}/(3).$$

**Example 15.15.** Using the same methods as for finding  $D^{-1}(\mathbb{Z}/(3))$ , we get that

$$D^{-1}(\mathbb{Z}/(9)) = \mathbb{Z}/(9).$$

**Definition 15.16.** Suppose  $\phi : R \rightarrow S$  is a ring morphism. Then, if  $M$  is an  $R$ -module, we think of the **tensor product**  $S \otimes_{\phi, R} M$  as a way of making  $M$  into an  $S$ -module.

Specifically, we consider the  $S$ -module  $F_S(M)$ , and define  $N$  to be the submodule

$$N = \langle e_n + e_m - e_{m+n}, e_{rm} - \phi(r)e_m \mid r \in R, m, n \in M \rangle.$$

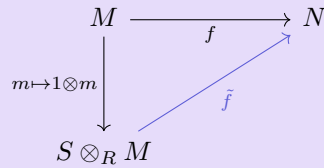
Then, we can say that

$$S \otimes_R M \cong F_S(M)/N,$$

where  $s \otimes m \mapsto se_m$  and  $m \mapsto 1 \otimes m \mapsto e_m$ .

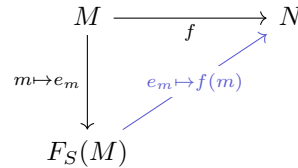
For this tensor product, it is usually easier to work with the universal property:

**Lemma 15.17.** If  $N$  is any  $S$ -module and  $f : M \rightarrow N$  is an  $R$ -linear map (so  $f(rm_1 + m_2) = \phi(r)f(m_1) + f(m_2)$ ), then there exists a unique  $S$ -linear map  $\tilde{f} : S \otimes_R M \rightarrow N$  such that



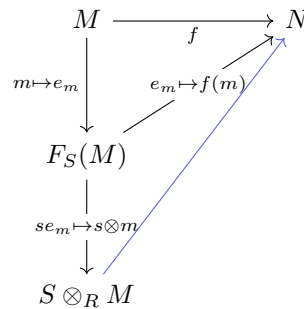
commutes and  $\tilde{f}(s \otimes m) = sf(m)$ .

*Proof.* We start with the diagram



where the map  $m \mapsto e_m$  is a set morphism, and the purple arrow is a  $S$ -module morphism which comes from the fact that  $F_S$  is a left-adjoint for the forgetful functor.

Then, we get that



by the universal property of the quotient module, as long as everything in the kernel of  $F_S(M) \rightarrow S \otimes_R M$  is also in the kernel of  $F_S(M) \rightarrow N$ .  $\square$



## LECTURE 16: TENSOR PRODUCTS OF MODULES, I

Last time, we left off describing the tensor product  $S \otimes_{\phi, R} M$ . We showed the literal definition of the tensor product and the universal property; we can also describe the tensor product as:

**Definition 16.1.** We consider forgetful functor  $\phi^* : \mathbf{S}\text{-Mod} \rightarrow \mathbf{R}\text{-Mod}$ ,  $N \mapsto N$ , where  $r \in R$  acts on  $N$  by  $r \cdot n = \phi(r) \cdot n$ .

We can say that the functor  $S \otimes_{\phi, R}$  (where  $M \mapsto S \otimes_{\phi, R} M$ ) is the left-adjoint of the forgetful functor, so

$$\mathrm{Hom}(S \otimes_{\phi, R} M, N) \cong \mathrm{Hom}_R(M, \phi^* N).$$

We have the following lemmas about the tensor product, some of which will be homework problems:

**Lemma 16.2.** For an ideal  $I \triangleleft R$ , we have

$$R/I \otimes_{\phi, R} M \cong M/IM,$$

where  $\phi$  is a ring homomorphism  $R \rightarrow R/I$ .

**Lemma 16.3.** For a multiplicative subset  $D \subset R$ , we have

$$(D^{-1}R) \otimes_{\phi, R} M \cong D^{-1}M,$$

where  $\phi$  is a ring homomorphism  $R \rightarrow D^{-1}R$ .

**Lemma 16.4.** For rings  $R, S, T$ ,

$$T \otimes_S (S \otimes_{\phi, R} M) \cong T \otimes_R M.$$

We can check the above three lemmas by check that that the expression on the RHS has the universal property of the tensor product on the LHS.

**Lemma 16.5.**

$$S \otimes_{\phi, R} (M \oplus N) \cong (S \otimes_{\phi, R} M) \oplus (S \otimes_{\phi, R} N).$$

This uses the functor definition of  $S \otimes_{\phi, R}$ , since it is a left adjoint, which preserves coproducts.

**Lemma 16.6.** For any small set  $\Omega$ ,

$$S \otimes_{\phi, R} F_R(\Omega) \cong F_S(\Omega).$$

**Lemma 16.7.** If  $f : M \rightarrow N$  is a morphism of  $R$ -modules, there exists a unique morphism of  $S$  modules  $1 \otimes f : S \otimes_{\phi, R} M \rightarrow S \otimes_{\phi, R} N$  that makes the diagram:

$$\begin{array}{ccc} M & \xrightarrow{m \mapsto 1 \otimes f(m)} & S \otimes_R N \\ \downarrow & \searrow^{1 \otimes f} & \\ S \otimes_R M & & \end{array}$$

commute; specifically, this is the map  $(1 \otimes f)(s \otimes m) = s \otimes f(m)$ .

Note that this is different from the universal property, because the universal property gives us an  $S$ -linear map  $S \otimes_{\phi, R} M \rightarrow N$ .

**Lemma 16.8.** Suppose we have ring morphisms  $\phi : R \rightarrow S$  and  $\psi : R \rightarrow T$ . Then, we can consider the tensor product of rings  $S \otimes_R^{\text{ring}} T$  and the tensor product of  $R$ -modules  $S \otimes_R^{\text{mod}} T$ , which turns  $T$  as an  $R$ -module into an  $S$ -module. These two are isomorphic as  $S$ -modules, using the map  $s \otimes t \mapsto s \otimes t$ .

*Proof.* Our instinct would be to use the universal property of the ring tensor product, applied to the map  $T \rightarrow S \otimes_R^{\text{mod}} T$ , to get an induced map  $S \otimes_R^{\text{ring}} T \rightarrow S \otimes_R^{\text{mod}} T$ . However,  $T \rightarrow S \otimes_R^{\text{mod}} T$  is a morphism of  $S$ -modules, not necessarily a ring morphism, and in particular we don't know that  $S \otimes_R^{\text{mod}} T$  is a ring at all.

So we begin by trying to make  $S \otimes_R^{\text{mod}} T$  into a ring, by defining a multiplication operation. To do so, we first note that within the  $R$ -module  $T$ , we can think of “multiplication by  $t \in T$ ” as an element of  $\text{End}_R(T)$ . That is, we have the morphism of  $R$ -modules

$$\begin{aligned} T &\longrightarrow \text{End}_R(T) \\ t &\longmapsto (t' \mapsto tt'). \end{aligned}$$

Then, we can extend this into the  $R$ -module morphism

$$\begin{array}{ccc} T & \longrightarrow & \text{End}_R(T) & \longrightarrow & \text{End}_R(S \otimes_R^{\text{mod}} T) \\ t & \longrightarrow & & \longrightarrow & (s \otimes t' \mapsto s \otimes tt') \end{array}$$

We will call this extension  $f$ , and leave it as an exercise to check that  $f$  is actually an  $R$ -linear map.

But then, by the universal property of the module tensor product ([Lemma 15.17](#)), this induces an  $S$ -linear map  $S \otimes_R^{\text{mod}} T \rightarrow \text{End}_R(S \otimes_R^{\text{mod}} T)$ , so the diagram

$$\begin{array}{ccccc} T & \xrightarrow{\quad f \quad} & \text{End}_R(T) & \longrightarrow & \text{End}_R(S \otimes_R^{\text{mod}} T) \\ \downarrow t \mapsto 1 \otimes t & & & & \uparrow \tilde{f} \\ S \otimes_R^{\text{mod}} T & & & & \end{array}$$

commutes. We also know that  $\tilde{f}(s \otimes t) = sf(t)$ , so

$$\tilde{f}(s \otimes t)(s' \otimes t') = s(s' \otimes tt') = ss' \otimes tt'.$$

Using this, we can define multiplication in  $S \otimes_R^{\text{mod}} T$  as, for  $x, y \in S \otimes_R^{\text{mod}} T$ ,

$$x \cdot y = \tilde{f}(x)(y).$$

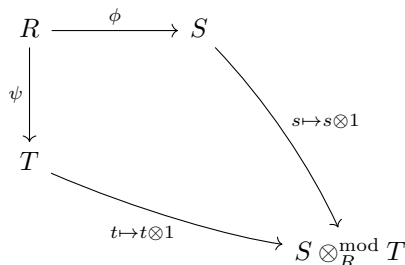
We leave it as an exercise to check that  $S \otimes_R^{\text{mod}} T$  now has all the properties of a ring (specifically, that multiplication is commutative and associative and that the distributive property holds).

Then, we claim that the natural map  $T \rightarrow S \otimes_R^{\text{mod}} T$  is a ring morphism. As a reminder, this map is defined as  $t \mapsto 1 \otimes t$ , and then we can see that for any  $t_1, t_2 \in T$ ,

$$\begin{aligned} t_1 + t_2 &\mapsto 1 \otimes t_1 + t_2 = (1 \otimes t_1) + (1 \otimes t_2) \\ t_1 t_2 &\mapsto 1 \otimes t_1 t_2 = (1 \otimes t_1)(1 \otimes t_2), \end{aligned}$$

so this is a ring morphism, as we wanted. We similarly have the ring morphism  $S \rightarrow S \otimes_R^{\text{mod}} T$  defined by  $s \mapsto s \otimes 1$ , and we can also check that this has the desired properties of a ring morphism.

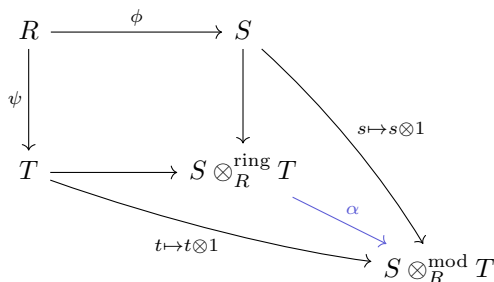
In order to apply the universal property of the ring tensor product, we want the diagram



to commute. We can see that going to the right and then down gives us  $\phi(r) \otimes 1$ , while going down and then to the right gives us  $1 \otimes \psi(r)$ . But these are equal, because by definition of the module tensor product and the way  $R$  acts on  $T$ ,

$$\phi(r) \otimes 1 = 1 \otimes r \cdot 1 = 1 \otimes \psi(r).$$

Thus, this diagram commutes, and we can apply the universal property of the ring tensor product to get the induced map



and we can check that because this diagram commutes,  $\alpha$  is the map  $s \otimes t \mapsto s \otimes t$ .

We leave it as an exercise to check this map is  $S$ -linear and invertible; this implies  $S \otimes_R^{\text{ring}} T \cong S \otimes_R^{\text{mod}} T$ , as we wanted.  $\square$

We now turn to talking about multilinear algebra.

**Definition 16.9.** If we have  $R$ -modules  $M_1, \dots, M_a$  and  $P$ , then we say

$$\psi : M_1 \times \dots \times M_a \longrightarrow P$$

is **multilinear** if for any set of  $m_i \in M_i$  and any  $j$ , the map  $M_j \rightarrow P$  defined by

$$m \mapsto \psi(m_1, \dots, m_{j-1}, m, m_{j+1}, \dots, m_a)$$

is  $R$ -linear.

Specifically, this means that  $\psi$  is a set morphism from the set-theoretic product  $M_1 \times \dots \times M_a$  to  $P$ , but if we hold almost all the coordinates constant, the resulting map  $M_i \rightarrow P$  is an  $R$ -module morphism.

**Example 16.10.** If we take  $R = \mathbb{R}$  and  $M = \mathbb{R}^3$ , then the cross product

$$\begin{aligned}
 \mathbb{R}^3 \times \mathbb{R}^3 &\longrightarrow \mathbb{R}^3 \\
 (x, y) &\longmapsto x \times y
 \end{aligned}$$

is a multilinear map, and so is the dot product

$$\begin{aligned}\mathbb{R}^3 \times \mathbb{R}^3 &\longrightarrow \mathbb{R} \\ (x, y) &\longmapsto x \cdot y.\end{aligned}$$

## LECTURE 17: TENSOR PRODUCTS OF MODULES, II

Last time, we left off talking about multilinear maps. We will continue our discussion of those today.

**Definition 17.1.** If  $\psi : M_1 \times \cdots \times M_a$  is a multilinear map, we call  $\psi$  **symmetric** if  $M_1, \dots, M_a = M$  and if for any  $\sigma \in S_a$  (the symmetric group of order  $a$ ),

$$\psi(m_1, \dots, m_a) = \psi(m_{\sigma_1}, \dots, m_{\sigma_a}).$$

**Example 17.2.** The dot product is a symmetric multilinear map.

**Definition 17.3.** We call  $\psi$  **alternating** if  $M_1, \dots, M_a = M$  and if  $m_i = m_j$  for some  $i \neq j$  implies

$$\psi(m_1, \dots, m_a) = 0.$$

**Definition 17.4.** The cross product is an alternating multilinear map.

**Lemma 17.5.** If  $\psi$  is an alternating multilinear map and if  $\sigma \in S_a$  then

$$\psi(m_{\sigma_1}, \dots, m_{\sigma_a}) = (-1)^\sigma \psi(m_{\sigma_1}, \dots, m_{\sigma_a}),$$

so permuting the elements changes the sign of the output based on the sign of the permutation.

If  $2 \in R^\times$  then the converse is true.

*Proof.* We just need to show that a transposition (swapping  $m_i$  and  $m_j$ ) will flip the sign of the output. We will just show this for the example of swapping  $m_1$  and  $m_2$ :

Since  $\psi$  is alternating, we know that

$$0 = \psi(m_1 + m_2, m_1 + m_2, m_3, \dots, m_a)$$

and then since  $\psi$  is multilinear, we get that

$$\begin{aligned} 0 &= \psi(m_1 + m_2, m_1 + m_2, m_3, \dots, m_a) \\ &= \psi(m_1, m_1 + m_2, m_3, \dots, m_a) + \psi(m_2, m_1 + m_2, m_3, \dots, m_a) \\ &= \psi(m_1, m_1, m_3, \dots, m_a) + \psi(m_1, m_2, m_3, \dots, m_a) + \psi(m_2, m_1, m_3, \dots, m_a) + \psi(m_2, m_2, m_3, \dots, m_a). \end{aligned}$$

But since  $\psi$  is alternating, the first and last terms of this sum are 0, so we get that

$$\psi(m_1, m_2, m_3, \dots, m_a) = -\psi(m_2, m_1, m_3, \dots, m_a).$$

For the converse, we will again just consider the example where  $m_1 = m_2$ . Since  $\psi$  is anti-symmetric, we know that swapping  $m_1$  and  $m_2$  will give us the opposite sign, so we get that

$$\psi(m_1, m_1, m_3, \dots, m_a) = -\psi(m_1, m_1, m_3, \dots, m_a).$$

Adding  $\psi(m_1, m_1, m_3, \dots, m_a)$  to both sides gives us

$$2\psi(m_1, m_1, m_3, \dots, m_a) = 0$$

and when we can multiply both sides by  $2^{-1}$ , we get

$$\psi(m_1, m_1, m_3, \dots, m_a) = 0,$$

as we desired. □

**Definition 17.6.** We say that  $\text{Bil}_R(M_1 \times M_2, P)$  is the set of all bilinear maps  $M_1 \times M_2 \rightarrow P$ . This is an  $R$ -module when we define

$$(r\psi + \phi)(m_1, m_2) = r\psi(m_1, m_2) + \phi(m_1, m_2).$$

We leave it as an exercise to check that this has all the properties of an  $R$ -module.

Similarly, we define  $\text{Mult}_R(M_1 \times \cdots \times M_a, P)$  is the set of all multilinear maps  $M_1 \times \cdots \times M_a \rightarrow P$ , and it can be made into an  $R$ -module in a similar way.

**Lemma 17.7.** The  $R$ -modules  $\text{Bil}_R(M_1 \times M_2, P)$  and  $\text{Hom}_R(M_1, \text{Hom}_R(M_2, P))$  are isomorphic.

*Proof.* We have the maps

$$\psi \mapsto (m_1 \mapsto (m_2 \mapsto \psi(m_1, m_2)))$$

and

$$((m_1, m_2) \mapsto f(m_1)(m_2)) \longleftarrow f,$$

and we leave it as an exercise to check that the images of these maps are in the desired sets, these are  $R$ -module morphisms, and they are inverses of each other.  $\square$

We are now in a position to define the tensor product of modules. We define these via the following universal property:

**Lemma 17.8.** For any  $R$ -modules  $M_1 \times \cdots \times M_a$ , there is an  $R$ -module  $M_1 \otimes \cdots \otimes M_a$  and a universal multilinear map

$$\begin{aligned} M_1 \times \cdots \times M_a &\longrightarrow M_1 \otimes \cdots \otimes M_a \\ (m_1, \dots, m_a) &\longmapsto m_1 \otimes \cdots \otimes m_a. \end{aligned}$$

By “universal,” we mean that if  $\psi : M_1 \times \cdots \times M_a \rightarrow P$  is multilinear, then there exists a unique  $R$ -linear map  $\tilde{\psi} : M_1 \otimes \cdots \otimes M_a \rightarrow P$  such that

$$\begin{array}{ccc} M_1 \times \cdots \times M_a & \xrightarrow{\psi} & P \\ \downarrow & \nearrow \tilde{\psi} & \\ M_1 \otimes \cdots \otimes M_a & & \end{array}$$

commutes.

*Proof.* As in our previous construction of the tensor product, we first consider the free module  $F_R(M_1 \times \cdots \times M_a)$ . We know since  $F_R$  is a left-adjoint to the forgetful functor that there exists a unique  $R$ -module morphism  $f : F_R(M_1 \times \cdots \times M_a) \rightarrow P$  such that

$$\begin{array}{ccc} M_1 \times \cdots \times M_a & \xrightarrow{\psi} & P \\ \downarrow & \nearrow f & \\ F(M_1 \times \cdots \times M_a) & & \end{array}$$

commutes.

But we know that since  $\psi$  is multilinear, for any  $m_j \in M_j$ ,  $m'_i \in M_i$ , and  $r \in R$ ,

$$f(e_{(m_1, \dots, m_i + rm'_i, \dots, m_a)}) = f(e_{(m_1, \dots, m_a)} + re_{(m_1, \dots, m'_i, \dots, m_a)}).$$

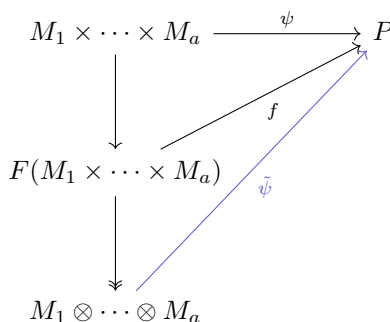
Let  $N$  be the submodule of  $F_R(M_1 \times \dots \times M_a)$  defined by

$$N = \langle e_{(m_1, \dots, m_i + rm'_i, \dots, m_a)} - e_{(m_1, \dots, m_a)} - re_{(m_1, \dots, m'_i, \dots, m_a)} \rangle_{m_j \in M_j, m'_i \in M_i, r \in R}.$$

Then, we define the **tensor product of  $M_1, \dots, M_a$  over  $R$**  to be

$$M_1 \otimes \dots \otimes M_a = F_R(M_1 \times \dots \times M_a) / N.$$

Since  $N$  is in the kernel of  $f$  by definition, we can use the universal property of the quotient to get a unique ring morphism  $\tilde{\psi} : M_1 \otimes \dots \otimes M_a \rightarrow P$  such that

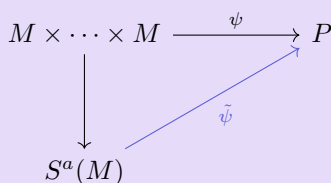


commutes. □

The pure tensors here are the images of elements of the form  $(m_1, \dots, m_a)$ , and they are denoted  $m_1 \otimes \dots \otimes m_a$ .

**Lemma 17.9.** There exists a universal symmetric multilinear map  $\underbrace{M \times \dots \times M}_{a \text{ times}} \rightarrow S^a(M)$ .

Here, “universal” means that if  $\psi : M \times \dots \times M \rightarrow P$  is a symmetric multilinear map then, there exists an  $R$ -linear map  $\tilde{\psi} : S^a(M) \rightarrow P$  such that



commutes.

We define  $S^a(M)$  almost identically to the tensor product in the previous lemma, but we also mod out by

$$\langle e_{(m_1, \dots, m_a)} - e_{(m_{\sigma_1}, \dots, m_{\sigma_a})} \rangle_{m_i \in M_i, \sigma \in S_a}$$

to preserve the symmetric property.

The pure tensors of this module are also denoted  $m_1 \otimes \dots \otimes m_a$ .

**Lemma 17.10.** There exists a universal alternating multilinear map  $\underbrace{M \times \dots \times M}_{a \text{ times}} \rightarrow \wedge^a(M)$ .

Here, “universal” means that if  $\psi : M \times \dots \times M \rightarrow P$  is a symmetric multilinear map then, there exists

an  $R$ -linear map  $\tilde{\psi} : \bigwedge^a(M) \rightarrow P$  such that

$$\begin{array}{ccc} M \times \cdots \times M & \xrightarrow{\psi} & P \\ \downarrow & \nearrow \tilde{\psi} & \\ \bigwedge^a(M) & & \end{array}$$

commutes.

Again,  $\bigwedge^a(M)$  is defined similarly to the tensor product, but we also mod out by

$$\langle e_{(m_1, \dots, m_i, \dots, m_j, \dots, m_a)} + e_{(m_1, \dots, m_j, \dots, m_i, \dots, m_a)} \rangle.$$

The pure tensors of this module are denoted  $m_1 \wedge \cdots \wedge m_a$ .

Lets look at some properties of module tensor products.

**Proposition 17.11.** Suppose that for  $1 \leq i \leq a$ , we have  $R$ -linear maps  $f_i : M_i \rightarrow N_i$ . Then there is a unique  $R$ -linear map

$$\begin{aligned} f_1 \otimes \cdots \otimes f_a : M_1 \otimes \cdots \otimes M_a &\longrightarrow N_1 \otimes \cdots \otimes N_a \\ m_1 \otimes \cdots \otimes m_a &\longmapsto f_1(m_1) \otimes \cdots \otimes f_a(m_a). \end{aligned}$$

*Proof.* We can see that if such a map exists, it must be unique, since we have defined the map on the pure tensors, and these span the tensor product.

Thus, we just need to show the existence of this map. To do so, we first look for a multilinear map  $\psi : M_1 \times \cdots \times M_a \rightarrow N_1 \otimes \cdots \otimes N_a$ , so that we can apply the universal property. Clearly, this map must be

$$\psi(m_1, \dots, m_a) = f_1(m_1) \otimes \cdots \otimes f_a(m_a).$$

Is this multilinear?

Well, we can see that

$$\psi(m_1, \dots, m_i + rm'_i, \dots, m_a) = f_1(m_1) \otimes \cdots \otimes f_i(m_i + rm'_i) \otimes \cdots \otimes f_a(m_a).$$

Since  $f_i$  is  $R$ -linear, we can expand this into

$$f_1(m_1) \otimes \cdots \otimes f_i(m_i) + rf_i(m'_i) \otimes \cdots \otimes f_a(m_a),$$

and then by definition of the tensor product, this is equal to

$$f_1(m_1) \otimes \cdots \otimes f_i(m_i) \otimes \cdots \otimes f_a(m_a) + r(f_1(m_1) \otimes \cdots \otimes f_i(m'_i) \otimes \cdots \otimes f_a(m_a)),$$

so this is a multilinear map!

Thus, we can apply the universal property of the tensor product to get an induced  $R$ -linear map  $M_1 \otimes \cdots \otimes M_a \rightarrow N_1 \otimes \cdots \otimes N_a$  with the desired properties.  $\square$

**Proposition 17.12.** If  $f : M \rightarrow N$  is  $R$ -linear, there exists a unique  $R$ -linear map

$$\begin{aligned} S^a(f) : S^a(M) &\longrightarrow S^a(N) \\ m_1 \otimes \cdots \otimes m_a &\longmapsto f(m_1) \otimes \cdots \otimes f(m_a), \end{aligned}$$



and there exists a unique  $R$ -linear map

$$\begin{aligned}\wedge^a(f) : \wedge^a(M) &\longrightarrow \wedge^a(N) \\ m_1 \otimes \cdots \otimes m_a &\longmapsto f(m_1) \wedge \cdots \wedge f(m_a).\end{aligned}$$

As a side note, we can't always expect that tensor products act according to our intuition:

**Example 17.13.** Consider the ring  $R = \mathbb{C}[X, Y]$ . We can see that there are no nonzero zero divisors in the ideal  $(X, Y) \triangleleft \mathbb{C}[X, Y]$ , but we claim that there is some  $z \neq 0 \in (X, Y) \otimes_R (X, Y)$  such that  $Xz = Yz = 0$ .

**Proposition 17.14.** For any permutation  $\sigma \in S_a$ , there is an  $R$ -linear isomorphism

$$\begin{aligned}\sigma^* : M_1 \otimes \cdots \otimes M_a &\longrightarrow M_{\sigma_1} \otimes \cdots \otimes M_{\sigma_a} \\ m_1 \otimes \cdots \otimes m_a &\longmapsto m_{\sigma_1} \otimes \cdots \otimes m_{\sigma_a}\end{aligned}$$

*Proof.* First, we need to show that such an  $R$ -linear map exists. We again induce it from the multilinear map

$$\begin{aligned}M_1 \times \cdots \times M_a &\longrightarrow M_{\sigma_1} \otimes \cdots \otimes M_{\sigma_a} \\ (m_1, \dots, m_a) &\longmapsto m_{\sigma_1} \otimes \cdots \otimes m_{\sigma_a}\end{aligned}$$

We leave it as an exercise to check that this is multilinear.

Then, to check that it is an isomorphism, we will show that  $(\sigma^{-1})^* = (\sigma^*)^{-1}$ .

To do so, first check that  $\text{id}^* = \text{id}$ .

Then, check that for any transposition  $\tau$ ,

$$(\sigma\tau)^* = \tau^* \sigma^*.$$

It is sufficient to show that this holds for pure tensors.

Together, these imply that

$$(\sigma)^*(\sigma^{-1})^* = (\sigma^{-1}\sigma)^* = \text{id}^* = \text{id},$$

so this is an isomorphism. □

**Proposition 17.15.**

$$M_1 \otimes \cdots \otimes M_a \cong (M_1 \otimes \cdots \otimes M_b) \otimes (M_{b+1} \otimes \cdots \otimes M_a).$$

*Proof.* We start with the multilinear map

$$M_1 \times \cdots \times M_a \longrightarrow (M_1 \otimes \cdots \otimes M_b) \otimes (M_{b+1} \otimes \cdots \otimes M_a)$$

defined by

$$(m_1, \dots, m_a) \mapsto (m_1 \otimes \cdots \otimes m_b) \otimes (m_{b+1} \otimes \cdots \otimes m_a).$$

and we get an induced map from the tensor product. What remains is to show that this map is invertible; we will finish showing this next lecture. □

## LECTURE 18: TENSOR PRODUCTS OF MODULES, III

We continue with our proof of [Proposition 17.15](#) that we left off last lecture.

*Proof, cont'd.* We want to find a bilinear map

$$(M_1 \otimes \cdots \otimes M_b) \times (M_{b+1} \otimes \cdots \otimes M_a) \longrightarrow M_1 \otimes \cdots \otimes M_a$$

which is the inverse of our map in the previous direction.

Recall [Lemma 17.7](#) tells us that the bilinear maps are in isomorphism with

$$\text{Hom}_R(M_1 \otimes \cdots \otimes M_b, \text{Hom}_R(M_{b+1} \otimes \cdots \otimes M_a, M_1 \otimes \cdots \otimes M_a)).$$

We want to find a map in this homomorphism set such that

$$m_1 \otimes \cdots \otimes m_b \longmapsto (m_{b+1} \otimes \cdots \otimes m_a \mapsto m_1 \otimes \cdots \otimes m_a).$$

We know that for a given  $m_1, \dots, m_b$ , we can apply the universal property of the tensor product to the multilinear map

$$\begin{aligned} M_{b+1} \times \cdots \times M_a &\longrightarrow M_1 \otimes \cdots \otimes M_a \\ (m_{b+1}, \dots, m_a) &\longmapsto m_1 \otimes \cdots \otimes m_a \end{aligned}$$

to get that there is a unique  $R$ -linear map  $f_{(m_1, \dots, m_b)}$  such that the diagram

$$\begin{array}{ccc} & \xrightarrow{(m_{b+1}, \dots, m_a) \mapsto m_1 \otimes \cdots \otimes m_a} & \\ M_{b+1} \times \cdots \times M_a & & M_1 \otimes \cdots \otimes M_a \\ \downarrow & \nearrow f_{(m_1, \dots, m_b)} & \\ M_{b+1} \otimes \cdots \otimes M_a & & \end{array}$$

commutes. So we've found a linear map that matches the inner part of our homomorphism.

To get the entire homomorphism, consider the map

$$\begin{aligned} f : M_1 \times \cdots \times M_b &\longrightarrow \text{Hom}_R(M_{b+1} \otimes \cdots \otimes M_a, M_1 \otimes \cdots \otimes M_a) \\ (m_1, \dots, m_b) &\longmapsto f_{(m_1, \dots, m_b)}. \end{aligned}$$

We want this to be a multilinear map so that we can induce an  $R$ -linear map from the tensor product.

We will just check that it is linear on  $M_1$ ; it is sufficient to check the behavior on pure tensors. We can see that

$$\begin{aligned} f_{(rm_1+m'_1, \dots, m_b)}(m_{b+1} \otimes \cdots \otimes m_a) &= (rm_1 + m'_1) \otimes m_2 \otimes \cdots \otimes m_b \otimes m_{b+1} \otimes \cdots \otimes m_a \\ &= r(m_1 \otimes m_2 \otimes \cdots \otimes m_b \otimes m_{b+1} \otimes \cdots \otimes m_a) + (m'_1 \otimes m_2 \otimes \cdots \otimes m_b \otimes m_{b+1} \otimes \cdots \otimes m_a) \\ &= rf_{(m_1, \dots, m_b)}(m_{b+1} \otimes \cdots \otimes m_a) + f_{(m'_1, \dots, m_b)}(m_{b+1} \otimes \cdots \otimes m_a), \end{aligned}$$

as we desired. So this is a multilinear map, and we can apply the universal property once more to get the induced map

$$\begin{array}{ccc} & \xrightarrow{f} & \\ M_1 \times \cdots \times M_b & & \text{Hom}_R(M_{b+1} \otimes \cdots \otimes M_a, M_1 \otimes \cdots \otimes M_a) \\ \downarrow & \nearrow \bar{f} & \\ M_1 \otimes \cdots \otimes M_b & & \end{array}$$

which is  $R$ -linear.

Then, we go back from our double homomorphism to a bilinear map, by defining  $\phi(x, y) = \tilde{f}(x)(y)$ , and finally we get our induced map

$$\begin{aligned} \tilde{\phi} : (M_1 \otimes \cdots \otimes M_b) \otimes (M_{b+1} \otimes \cdots \otimes M_a) &\longrightarrow M_1 \otimes \cdots \otimes M_a \\ (m_1 \otimes \cdots \otimes m_b) \otimes (m_{b+1} \otimes \cdots \otimes m_a) &\longmapsto m_1 \otimes \cdots \otimes m_a \end{aligned}$$

which is  $R$ -linear.

We leave it as an exercise to check that the map we just constructed is truly an inverse of the map we constructed in the opposite direction.  $\square$

**Proposition 18.1.** If  $\phi : R \rightarrow S$  is a ring morphism and if  $M$  is an  $R$ -module, then  $S \otimes_R M$ , meaning turning  $M$  into an  $S$ -module, and  $S \otimes_R M$ , meaning the tensor product of  $R$ -modules, are isomorphic as  $R$ -modules.

It is easy to find a map from the module tensor product  $S \otimes_R M$  to the ring-module tensor product  $S \otimes_R M$ , but it is harder to find the inverse of this map.

**Proposition 18.2.** For any  $R$ -morphisms  $M, N, P$ ,

$$M \otimes (N \oplus P) \cong (M \otimes N) \oplus (M \otimes P),$$

via the map

$$m \otimes (n, p) \mapsto (m \otimes n, m \otimes p).$$

**Proposition 18.3.** For any sets  $X, Y$ ,

$$F_R(X) \otimes F_R(Y) \cong F_R(X \times Y),$$

via the map  $e_x \otimes e_y \longmapsto e_{(x,y)}$ .

Similarly,

$$S^a(F_R(X)) \cong F_R(S^a(X)),$$

via the map  $e_1 \otimes \cdots \otimes e_a \longmapsto e_{[(x_1, \dots, x_a)]}$ .

**Proposition 18.4.** Suppose  $<$  is a total order on  $X$ . Then, we define

$$\wedge_{<}^a(X) = \{(x_1, \dots, x_a) \mid x_i \in X, x_i < x_j \forall i < j\}.$$

Then we have

$$\wedge^a(F_R(X)) \cong F_R(\wedge_{<}^a(X)),$$

via the map

$$e_{x_1} \wedge \cdots \wedge e_{x_a} \longmapsto \begin{cases} 0 & x_i = x_j \text{ for } i \neq j \\ (-)^\sigma e_{(x_{\sigma_1}, \dots, x_{\sigma_a})} & \text{otherwise,} \end{cases}$$

where  $\sigma$  is the permutation that puts the  $x_i$ 's in increasing order.

**Example 18.5.** Let  $X = \{1, \dots, a\}$  with the standard ordering. Then,  $F_R(X) = R^{\oplus a}$ .

Then, the above proposition tells us that

$$\bigwedge^a(R^{\oplus a}) \cong F_R(\bigwedge^a_{<}(X)),$$

but we can see that the only element in  $\bigwedge^a_{<}(X)$  is  $(1, 2, \dots, a)$ , so we get that

$$\bigwedge^a(R^{\oplus a}) \cong R.$$

Similarly, we can see that

$$\bigwedge^{a-1}(R^{\oplus a}) \cong F_R(\bigwedge^{a-1}_{<}(X)) = R^{\oplus a}.$$

**Proposition 18.6.** There exists an  $R$ -linear map  $\phi : M \rightarrow \text{Hom}_R(\bigwedge^a M, \bigwedge^{a+1} M)$  defined by

$$\phi(m)(m_1 \wedge \dots \wedge m_a) = m_1 \wedge \dots \wedge m_a \wedge m.$$

Moreover, for any  $R$ -module morphism  $f : M \rightarrow N$ ,  $\bigwedge^{a+1} f \circ \phi(m) = \phi(f(m)) \circ \bigwedge^a(f)$ ; both of these equal the map

$$\begin{aligned} \bigwedge^a M &\longrightarrow \bigwedge^{a+1} N \\ m_1 \wedge \dots \wedge m_a &\longmapsto f(m_1) \wedge \dots \wedge f(m_a) \wedge f(m). \end{aligned}$$

**Proposition 18.7.** Remember that

$$\text{End}_R(R^{\oplus a}) \cong M_{a \times a}(R),$$

where  $M_{a \times a}(R)$  is the set of  $a \times a$  matrices over  $R$ .

For any map  $f \in \text{End}_R(R^{\oplus a})$ , there is an induced map  $\bigwedge^a f : \bigwedge^a(R^{\oplus a}) \rightarrow \bigwedge^a(R^{\oplus a})$  that maps any basis element  $e \neq 0 \mapsto (\det f)e$ .

We leave it as an exercise to check that this is well-defined and  $R$ -linear; this uses the fact that we can express each  $f e_i$  as  $\sum_j b_{ij} e_j$  for some  $b_{ij} \in R$ , and then

$$\det f = \sum_{\sigma \in S_a} (-1)^\sigma b_{1\sigma_1} \dots b_{a\sigma_a}.$$

**Proposition 18.8.** For any  $f \in \text{End}_R(R^{\oplus a})$ , we can construct the commutative diagram

$$\begin{array}{ccc} R^{\oplus a} & \longrightarrow & \text{Hom}_R(\bigwedge^{a-1} R^{\oplus a}, \bigwedge^a R^{\oplus a}) \\ & & \downarrow \\ & & \boxed{g \mapsto g \circ \bigwedge^{a-1} f} \\ & & \downarrow \\ R^{\oplus a} & \longrightarrow & \text{Hom}_R(\bigwedge^{a-1} R^{\oplus a}, \bigwedge^a R^{\oplus a}) \end{array}$$

where the horizontal maps are

$$r \mapsto (r_1 \wedge \dots \wedge r_{a-1} \mapsto r_1 \wedge \dots \wedge r_{a-1} \wedge r),$$

and we can use bases to show that the horizontal maps are actually isomorphisms.

Then,  $\text{adj } f$  or the **adjugate** of  $f$  is the unique map  $R^{\oplus a} \rightarrow R^{\oplus a}$  that makes the diagram

$$\begin{array}{ccc} R^{\oplus a} & \longrightarrow & \text{Hom}_R(\wedge^{a-1} R^{\oplus a}, \wedge^a R^{\oplus a}) \\ \downarrow \text{adj } f & & \downarrow g \mapsto g \circ \wedge^{a-1} f \\ R^{\oplus a} & \longrightarrow & \text{Hom}_R(\wedge^{a-1} R^{\oplus a}, \wedge^a R^{\oplus a}) \end{array}$$

commute.

We leave it as an exercise to show that  $\text{adj } f$  is the map such that

$$\text{adj } f \circ f = (\det f) \text{id}_{R^{\oplus a}} .$$

Recall that if  $f \in \text{End}_R(R^{\oplus a})$ , we can make it into a map in  $\text{End}_{R[T]}(R[T]^{\oplus a})$ , using the fact that

$$R[T]^{\oplus a} = R[T] \otimes_R R^{\oplus a},$$

and then mapping  $f$  to  $1 \otimes f \in R[T] \otimes_R R^{\oplus a}$ .

**Definition 18.9.** Using this, we say that the **characteristic polynomial** of  $f$  is the polynomial

$$\text{ch}_f(T) = c_f(T) = \det \left( T \text{id}_{R[T]^{\oplus a}} - 1 \otimes f \right) \in R[T].$$

**Lemma 18.10** (Cayley-Hamilton Theorem). For any  $f \in \text{End}_R(R^{\oplus a})$ ,

$$c_f(f) = 0.$$

*Proof.* Remember that

$$\det(T \text{id} - f) = \text{adj}(T \text{id} - f) \circ (T \text{id} - f),$$

and we can consider the adjugate as some polynomial

$$B_0 + B_1 T + B_2 T^2 + \dots + B_d T^d, \quad B_i \in \text{End}_R(R^{\oplus a}).$$

But then applying the composition gives us that polynomial

$$c_f(T) = \sum_{i=0}^d (B_{i-1} - B_i \circ f) T^i,$$

and we can evaluate this at  $f$  to get

$$c_f(f) = \sum_{i=0}^d (B_{i-1} f^i - B_i f^{i+1}) = \sum_i (B_{i-1} f^i - B_{i-1} f^i) = 0.$$

□

**Corollary 18.11** (Nakayama’s Lemma). Suppose  $M$  is a finitely generated  $R$ -module,  $I \triangleleft R$ , and  $IM = M$ . Then, there exists some  $r \in I$  such that  $(1 + r)M = (0)$ .

*Proof.* Let us say  $M$  is generated by  $\{m_1, \dots, m_a\}$ . Then, there is a surjection  $R^{\oplus a} \rightarrow M$  and we get the commutative diagram

$$\begin{array}{ccc} R^{\oplus a} & \longrightarrow & M \\ \downarrow A & & \downarrow \text{id} \\ R^{\oplus a} & \longrightarrow & M \end{array}$$

where  $A$  is some element of  $\text{End}_R(R^{\oplus a})$  that makes the diagram commute.

But then, we can see that the diagram should still commute if we apply any polynomial to both vertical arrows, so in particular

$$\begin{array}{ccc} R^{\oplus a} & \longrightarrow & M \\ \downarrow c_A(A) & & \downarrow c_A(1) \\ R^{\oplus a} & \longrightarrow & M \end{array}$$

commutes. But the Cayley-Hamilton theorem tells us that  $c_A(A) = 0$ , so

$$c_A(1)M = (0).$$

Since  $c_A(T)$  is of the form  $T^a + c_1T^{a+1} + \dots + c_dT^{a+d}$ , we get that  $c_1, \dots, c_d \in I$ , so

$$c_A(1) \in 1 + I,$$

as we desired. □

**Corollary 18.12.** If  $M$  is torsion-free and finitely generated over  $R$ , and  $I \triangleleft R$  is a proper ideal of  $R$  such that  $IM = M$ , then  $M = (0)$ .

*Proof.* We know from Nakayama's Lemma that we can find some  $r \in I$  such that  $(1+r)M = 0$ , but since  $r \in I$  and  $1 \notin I$ ,  $1+r \notin I$ , and in particular this means it cannot be zero. But if  $M$  is torsion free, multiplying by a nonzero element cannot make it zero unless it was already just  $(0)$ . □

**Corollary 18.13.** Suppose we are in the same scenario as in Nakayama's Lemma, but  $I$  is a subset of all maximal ideals of  $R$ . Then,  $M = (0)$ .

*Proof.* This implies that  $1+r$  is not in any maximal ideals of  $R$ , which means  $1+r$  is a unit, so if  $(1+r)M = (0)$  then  $M = (0)$ . □

**Corollary 18.14.** Suppose  $M$  is finitely generated over  $R$ , and we have found  $m_1, \dots, m_a \in M$  such that  $M = \langle m_1, \dots, m_a, IM \rangle$ , where  $I \triangleleft R$  and  $I$  is a subset of all maximal ideals of  $R$ .

Then,  $M = \langle m_1, \dots, m_a \rangle$ .

## LECTURE 19: FINITELY GENERATED MODULES OVER A PID

We begin today by stating the structure theorem for finitely generated modules over a PID. The proof of this theorem is kind of involved, so we will spend the next two lectures looking at examples of why this theorem is useful, before returning to its proof.

**Theorem 19.1.** Suppose  $R$  is a PID and  $N \subset R^{\oplus n}$  is a submodule. Then,  $N$  must be free, and we can find a basis  $\{e_1, \dots, e_n\}$  of  $R^{\oplus n}$  and elements

$$a_1 \mid a_2 \mid \dots \mid a_m \neq 0 \in R$$

such that  $\{a_i e_i\}$  is a basis of  $N$ .

Moreover, these  $a_i$ 's are unique up to associates.

**Corollary 19.2** (structure theorem for finitely generated modules over a PID). If  $R$  is a PID and  $M$  is a finitely generated  $R$ -module, then there exists

$$a_1 \mid a_2 \mid \dots \mid a_m \neq 0 \in R,$$

where none of the  $a_i$ 's are units, such that

$$M \cong R^{\oplus d} \oplus \bigoplus_{i=1}^m (R/(a_i)).$$

Moreover,  $d, m$ , and the  $a_i$ 's are uniquely determined by  $M$ .

Note that we call the  $R/a_i$  terms the **invariant factors** of  $M$ .

*Proof.* If  $M$  is finitely generated by  $n$  elements, then we know that  $M \subset R^{\oplus n}$  and there is a projection map  $\pi : R^{\oplus n} \rightarrow M$  such that

$$M \cong R^{\oplus n} / \ker \pi.$$

But [Theorem 19.1](#) tells us that

$$R^{\oplus n} / \ker \pi \cong \bigoplus_{i=1}^m (R/(a_i)),$$

and then we account for the fact that the first  $d$  such  $a_i$ 's may be units in  $R$  to get that

$$M \cong R^{\oplus d} \oplus \bigoplus_{i=d+1}^m (R/(a_i)),$$

as we wanted. □

Now, we can apply the following lemma, which is a weaker version of the Chinese remainder theorem for modules:

**Lemma 19.3.** For ideals  $(a), (b) \triangleleft R$ , if  $(a)$  and  $(b)$  are comaximal, then

$$R/(ab) \cong R/(a) \oplus R/(b)$$

as  $R$ -modules.

This gives us the following version of the structure theorem:

**Corollary 19.4.** If  $R$  is a PID and  $M$  is a finitely-generated  $R$ -module, then there exists a function  $n(\pi)$  which maps irreducibles of  $R$  to nonnegative integers, such that  $n(\pi) = 0$  for all but finitely many  $\pi$ , and multiplicities  $m_i(\pi)$ , such that

$$M \cong R^{\oplus d} \oplus \bigoplus_{\substack{\pi \in R \\ \text{irreducible}}} \bigoplus_{i=1}^{n(\pi)} R/(\pi^{m_i(\pi)}),$$

where  $d$ ,  $n(\pi)$ , and  $m_i(\pi)$  are uniquely determined by  $M$ .

*Proof.* In words, this corollary is saying we can express the invariant factors of  $M$  as the product of  $R/I$ 's, where the  $I$ 's are all powers of prime ideals of  $R$ .

To do so, we note that since a PID is a UFD, we can express each  $a_i$  in the form

$$\prod_{\substack{\pi \in R \\ \text{irreducible}}} \pi^{m_i(\pi)},$$

up to associates, and where all but finitely many  $m_i(\pi)$ 's are just 0. But then, [Lemma 19.3](#) tells us that

$$R/(a_i) \cong \prod_{\substack{\pi \in R \\ \text{irreducible}}} R/(\pi^{m_i(\pi)}),$$

and the statement of the corollary follows.  $\square$

**Example 19.5.** Find all abelian groups  $M$  that can fit into a short exact sequence of the form

$$0 \longrightarrow \mathbb{Z} \oplus \mathbb{Z}/(5) \longrightarrow M \longrightarrow \mathbb{Z} \oplus \mathbb{Z}/(10) \longrightarrow 0.$$

The structure theorem tells us that  $M \cong \mathbb{Z}^{\oplus d} \oplus \bigoplus_{i=1}^m \mathbb{Z}/(a_i)$ , for some  $d, m, \{a_i\}$ . Can we find any restrictions on what  $d, m$ , and the  $a_i$ 's must be?

Well, we can see that

$$M_{(0)} = \mathbb{Q}^{\oplus d},$$

since we can interchange localizing and direct sums, and  $(\mathbb{Z}/(a_i))_{(0)} = (0)$  since  $a_i$  is in our denominator set. Moreover, as we showed in the homework, localizing preserves exactness, so

$$0 \longrightarrow \mathbb{Q} \xrightarrow{f} \mathbb{Q}^{\oplus d} \xrightarrow{g} \mathbb{Q} \longrightarrow 0$$

must be a short exact sequence.

But since  $f$  must be injective,  $\text{im } f \cong \mathbb{Q}$ , and since  $g$  must be surjective,  $\text{im } g \cong \mathbb{Q}$ . But this means  $\mathbb{Q}^{\oplus d} / \ker g = \text{im } g = \mathbb{Q}$ , and since  $\ker g = \text{im } f = \mathbb{Q}$ , we get that  $d = 2$ .

Thus,  $M \cong \mathbb{Z}^{\oplus 2} \oplus \bigoplus_{i=1}^m \mathbb{Z}/(a_i)$  for some  $m, \{a_i\}$ . Can we find restrictions on these values?

We define

$$M^{\text{tor}} = \{m \in M \mid \exists a \neq 0 \in R \text{ such that } am = 0\}.$$

It should be straightforward to check that this is a submodule of  $M$ , and we call this the **torsion submodule** of  $M$ .

Then, we can see that  $M^{\text{tor}} \cong \bigoplus_{i=1}^m R/(a_i)$ , since any element of  $R/(a_i)$  is killed by  $a_i$ , but  $R$  is an integral domain so any nonzero element of  $R$  cannot be in the torsion submodule.



We leave it as an exercise to check that taking the torsion submodule preserves left exactness but not necessarily right exactness (intuitively, since every torsion element has to map to a torsion element to preserve  $R$ -linearity, but it isn't necessary for  $R$ -linearity that the preimage of a torsion element is torsion).

Thus, we have the left-exact sequence

$$0 \longrightarrow \mathbb{Z}/(5) \xrightarrow{f} M^{\text{tor}} \xrightarrow{g} \mathbb{Z}/(10)$$

We can see that since  $M^{\text{tor}}$  is a finite group, and  $\text{im } f = \mathbb{Z}/(5)$  must be a submodule of  $M^{\text{tor}}$ , we get that  $\#M^{\text{tor}}$  must be a multiple of 5. Similarly, since  $\text{im } g = M^{\text{tor}}/\ker g = M^{\text{tor}}/(\mathbb{Z}/(5))$  must be a submodule of  $\mathbb{Z}/(10)$ , we get that  $\#M^{\text{tor}}/5$  must be a factor of 10, so

$$5 \mid \#M^{\text{tor}} \mid 50.$$

By the fundamental theorem of finite abelian groups, this means our options for  $M^{\text{tor}}$  are

$$\mathbb{Z}/(5), \mathbb{Z}/(10), \mathbb{Z}/(5) \oplus \mathbb{Z}/(5), \mathbb{Z}/(25), \mathbb{Z}/(5) \oplus \mathbb{Z}/(10), \text{ or } \mathbb{Z}/(50).$$

Let's try all these possibilities, and see which ones work.

We begin with  $M = \mathbb{Z}^{\oplus 2} \oplus \mathbb{Z}/(5)$ , so we want a short exact sequence

$$0 \longrightarrow \mathbb{Z} \oplus \mathbb{Z}/(5) \longrightarrow \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}/(5) \longrightarrow \mathbb{Z} \oplus \mathbb{Z}/(10) \longrightarrow 0$$

We recall that the torsion submodule  $\mathbb{Z}/(5)$  has to inject into the torsion submodule  $\mathbb{Z}/(5)$ , so we can use a bit of trial and error from there to get the maps

$$\begin{aligned} (a, b) &\longmapsto (10a, 0, b) \\ (x, y, z) &\longmapsto (y, x \bmod 10) \end{aligned}$$

(We leave it as an exercise to check this is short exact.) So  $M = \mathbb{Z}^{\oplus 2} \oplus \mathbb{Z}/(5)$  works!

I encourage you at this point to pause and try the rest of these sequences on your own, and come back to the lecture notes if you get stuck - it's not super interesting to read 5 more versions of very similar exact sequences, but it is a good exercise to make sure you can come up with these maps, and make sure they are actually  $R$ -linear and exact at each module, yourself.

Next, we check  $M = \mathbb{Z}^{\oplus 2} \oplus \mathbb{Z}/(10)$ , so we want a short exact sequence

$$0 \longrightarrow \mathbb{Z} \oplus \mathbb{Z}/(5) \longrightarrow \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}/(10) \longrightarrow \mathbb{Z} \oplus \mathbb{Z}/(10) \longrightarrow 0$$

We recall that the torsion submodule  $\mathbb{Z}/(5)$  has to inject into the torsion submodule  $\mathbb{Z}/(10)$ , so we can use a bit of trial and error from there, recalling we want cokernel equal to  $\mathbb{Z} \oplus \mathbb{Z}/(10)$ , to get the maps

$$\begin{aligned} (a, b) &\longmapsto (5a, 0, 2b) \\ (x, y, z) &\longmapsto (y, 5(z \bmod 2) + 2(x \bmod 5)) \end{aligned}$$

(We leave it as an exercise to check this is short exact.) So  $M = \mathbb{Z}^{\oplus 2} \oplus \mathbb{Z}/(10)$  works as well!

Next, we check  $M = \mathbb{Z}^{\oplus 2} \oplus \mathbb{Z}/(5) \oplus \mathbb{Z}/(5)$ , so we want a short exact sequence

$$0 \longrightarrow \mathbb{Z} \oplus \mathbb{Z}/(5) \longrightarrow \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}/(5) \oplus \mathbb{Z}/(5) \longrightarrow \mathbb{Z} \oplus \mathbb{Z}/(10) \longrightarrow 0$$

We get the maps

$$\begin{aligned} (a, b) &\longmapsto (2a, 0, b, 0) \\ (x, y, z, w) &\longmapsto (y, 2w + 5(x \bmod 2)) \end{aligned}$$

(We leave it as an exercise to check this is short exact.) So  $M = \mathbb{Z}^{\oplus 2} \oplus \mathbb{Z}/(5) \oplus \mathbb{Z}/(5)$  works!

Next, we check  $M = \mathbb{Z}^{\oplus 2} \oplus \mathbb{Z}/(25)$ , so we want a short exact sequence

$$0 \longrightarrow \mathbb{Z} \oplus \mathbb{Z}/(5) \longrightarrow \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}/(25) \longrightarrow \mathbb{Z} \oplus \mathbb{Z}/(10) \longrightarrow 0$$

We get the maps

$$\begin{aligned} (a, b) &\longmapsto (2a, 0, 5b) \\ (x, y, z) &\longmapsto (y, 5x + 2(z \bmod 5)) \end{aligned}$$

(We leave it as an exercise to check this is short exact.) So  $M = \mathbb{Z}^{\oplus 2} \oplus \mathbb{Z}/(25)$  works!

Next, we check  $M = \mathbb{Z}^{\oplus 2} \oplus \mathbb{Z}/(5) \oplus \mathbb{Z}/(10)$ , so we want a short exact sequence

$$0 \longrightarrow \mathbb{Z} \oplus \mathbb{Z}/(5) \longrightarrow \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}/(5) \oplus \mathbb{Z}/(10) \longrightarrow \mathbb{Z} \oplus \mathbb{Z}/(10) \longrightarrow 0$$

We get the maps

$$\begin{aligned} (a, b) &\longmapsto (a, 0, b, 0) \\ (x, y, z, w) &\longmapsto (y, w) \end{aligned}$$

(We leave it as an exercise to check this is short exact.) So  $M = \mathbb{Z}^{\oplus 2} \oplus \mathbb{Z}/(5) \oplus \mathbb{Z}/(10)$  works!

Finally, we check  $M = \mathbb{Z}^{\oplus 2} \oplus \mathbb{Z}/(50)$ , so we want a short exact sequence

$$0 \longrightarrow \mathbb{Z} \oplus \mathbb{Z}/(5) \longrightarrow \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}/(50) \longrightarrow \mathbb{Z} \oplus \mathbb{Z}/(10) \longrightarrow 0$$

We get the maps

$$\begin{aligned} (a, b) &\longmapsto (a, 0, 10b) \\ (x, y, z) &\longmapsto (y, z \bmod 10) \end{aligned}$$

(We leave it as an exercise to check this is short exact.) So  $M = \mathbb{Z}^{\oplus 2} \oplus \mathbb{Z}/(50)$  works!

Thus, we have found all 6 abelian groups  $M$  that fit into a short exact sequence of this form.

Note that it is not the case in general that all the  $M$ 's that have the correct  $d$  and correct size of  $M^{\text{tor}}$  fit into the exact sequence, but it is usually the case that most such  $M$ 's fit, and if it doesn't fit, there is usually an explicit reason why. For example, if  $M$  had more generators than the sum of the number of generators of its neighbors, then there would be no way to fit it into the short exact sequence.

**Example 19.6.** Suppose  $K$  is a field and  $V$  is a finite-dimensional  $K$ -vector space. Suppose also that we have  $T \in \text{End}_K(V)$ .

As we've done before, we can make  $V$  into a finitely generated  $K[X]$  module where  $X$  acts via  $T$ , so  $(\sum a_i X^i)v = \sum a_i T^i(v)$ .

Then, the structure theorem of finitely generated modules over a PID tells us that

$$V \cong K[X]^{\oplus d} \oplus \bigoplus_{i=1}^m K[X]/(a_i),$$

where  $a_1 \mid a_2 \mid \cdots \mid a_m \neq 0 \in K[X]$ ,  $\deg a_i > 0$ , and each  $a_i$  is monic (since we can just multiply by the inverse of the leading term). Moreover,  $d$  and the  $a_i$ 's are uniquely determined by  $V$ .

However, since  $V$  is finite-dimensional over  $K$ , while  $K[X]$  is infinite-dimensional over  $K$ , we get that  $d = 0$ , so

$$V \cong \bigoplus_{i=1}^m K[X]/(a_i),$$

and

$$\dim V = \sum_{i=1}^m \deg a_i,$$

since  $\{1, \dots, X^{\deg a_i - 1}\}$  serves as a basis for  $K[X]/(a_i)$  as a  $K$ -vector space.

Note that in the above, we are dealing with an isomorphism of  $K[X]$  modules, and then the endomorphism  $T$  on the left side maps to the endomorphism  $v \mapsto Xv$  on the right side.

Also, for any other  $V' \cong \bigoplus_{i=1}^{m'} K[X]/(a'_i)$ , where  $T'$  is the endomorphism we used to make  $V'$  a  $K[X]$ -module, there exists an isomorphism

$$f : V \xrightarrow{\sim} V' \text{ with } f \circ T = T' \circ f$$

if and only if  $V \cong V'$  as a  $K[X]$ -module (the existence of an isomorphism implies they're isomorphic as  $K$ -vector spaces, and the fact that it commutes with  $T$  and  $T'$  implies they're isomorphic as  $K[X]$ -modules). This happens if and only if  $m = m'$  and  $a_i = a'_i$  for all  $i$ .

## LECTURE 20: FINITELY GENERATED VECTOR SPACES

Today, we continue our example from last time of finitely generated vector spaces  $V$ , where we make  $V$  into a  $K[X]$  module where  $X$  acts as  $T \in \text{End}_K(V)$ , and then

$$V \cong \bigoplus_{i=1}^m K[X]/(a_i)$$

as a  $K[X]$ -module.

We also mentioned that for each  $K[X]/(a_i)$ , the basis is  $\{1, X, X^2, \dots, X^{\deg a_i - 1}\}$ , and then the basis for  $V$  combines all these bases, so that  $\dim V = \sum_{i=1}^m \deg a_i$ .

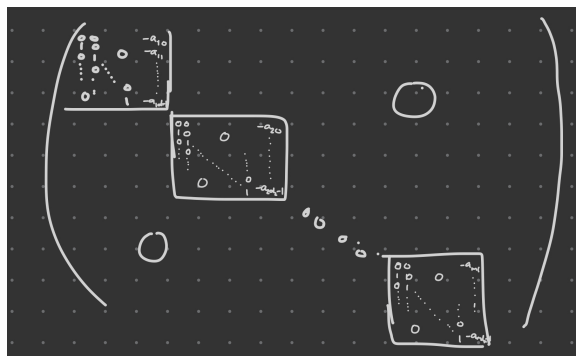
What is the matrix for  $T$  with respect to this basis?

We know that  $T$  corresponds to multiplication by  $X$ , so we can see that, over a singular  $K[X]/(a)$ , where  $a(X) = a_1 + \dots + a_{d-1}X^{d-1} + X^d$ , the matrix would be

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & & 0 & -a_2 \\ \vdots & 0 & \ddots & 0 & \vdots \\ \vdots & & & 1 & -a_{d-1} \end{pmatrix}$$

since each  $X^i$  would get mapped to the next basis element  $X^{i+1}$ , but then  $X^{d-1}$  would get mapped to  $X^d = -a_1 + \dots + (-a_{d-1})X^{d-1}$  when we take it mod  $a(X)$ .

Then, we can combine this over our direct sum to get that, for this basis of  $V$ , our endomorphism  $T$  has the following matrix:



This is known as the **rational canonical form** of  $T$ .

**Proposition 20.1.** For each such  $T$ , its rational canonical form is unique.

*Proof.* Based on the matrix in rational canonical form, we can define the polynomials  $a_i(X) = a_{i0} + \dots + a_{id_{i-1}}X^{d_{i-1}} + X^{d_i}$ , and for  $T$  to be in rational canonical form, we need  $a_1 \mid a_2 \mid \dots \mid a_m$ , which means we can then express  $V$  as

$$K[X]/(a_1) \oplus \dots \oplus K[X]/(a_m).$$

Thus, if there were two rational canonical forms for  $T$ , there would be two such ways to factor  $V$ , when we express it as a  $K[X]$ -module where  $X$  acts by  $T$ , and this contradicts the uniqueness part of the structure theorem for finitely generated modules over a PID.  $\square$

**Proposition 20.2.** For such  $T$ ,  $\text{ch}_T(X) = a_1(X) \cdots a_m(X)$ .

**Proposition 20.3.** There exists a monic polynomial  $m_T(X)$  where  $m_T(T) = 0$  and if  $f(T) = 0$  then  $m_T \mid f$ . This is called the **minimal polynomial of  $T$** .

*Proof.* Consider the annihilator of  $V$ ; we can see that this is the set

$$\text{Ann}_{K[X]}(V) = \{f \in K[X] \mid f(T) = 0\},$$

and it is an ideal of  $K[X]$ .

But since  $K[X]$  is a PID, this ideal must be equal to some  $(m_T) \triangleleft R[X]$ , and then  $m_T$  is our desired minimal polynomial.  $\square$

Moreover, we can see that since such a polynomial exists, it must be equal to the gcd of  $a_1, \dots, a_m$ , and since all other  $a_i$ 's are factors of  $a_m$ , we get that

$$m_T(X) = a_m(X).$$

**Definition 20.4.** If we have two endomorphisms  $A, B \in M_{n \times n}K$ , we say that  $A$  and  $B$  are **similar** if there exists  $g \in \text{GL}_n(K)$  such that

$$B = gAg^{-1}.$$

Note that this happens if and only if  $(K^{\oplus n}, A) \cong (K^{\oplus n}, B)$ , which happens if and only if  $A$  and  $B$  have the same invariant factors.

Thus, we can divide such endomorphisms into conjugacy classes of similar matrices. Let's try this with a few examples.

**Example 20.5.** Determine the conjugacy classes of  $\text{GL}_3(\mathbb{F}_2)$ .

As we just mentioned, the conjugacy classes are determined by the invariant factors, so we want to find all possible invariant factors for  $\mathbb{F}_2^3$  as a  $\mathbb{F}_2[X]$ -module.

This means we are looking for monic polynomials  $a_1 \mid \cdots \mid a_m \in (\mathbb{Z}/2\mathbb{Z})[X]$  where  $\deg a_1 \geq 1$  and  $\deg a_1 + \cdots + \deg a_m = 3$ .

But we are also looking for invertible matrices, and we note that a matrix is invertible if and only if

$$0 \neq \det(T) = \text{ch}_T(0) = a_1(0) \cdots a_m(0).$$

Thus, we want to pick our invariant factors such that  $a_m$  is not a multiple of  $X$ .

We proceed via casework on the size of  $m$ .

When  $m = 1$ , we are looking for monic degree-3 polynomials with constant term 1. Thus, we get the following options

$$\begin{aligned} &\{x^3 + 1\} \\ &\{x^3 + x^2 + 1\} \\ &\{x^3 + x + 1\} \\ &\{x^3 + x^2 + x + 1\}. \end{aligned}$$

When  $m = 2$ , we need two polynomials where one is a multiple of the other and their degrees sum to 3. Thus, we need a linear polynomial and a quadratic, and since we want neither of them to be multiples of  $X$ , we get:

$$\{x + 1, (x + 1)^2 = x^2 + 1\}$$

as our only option.

Finally when  $m = 3$ , we need all our polynomials to be linear, and since they're all multiples of each other, we get

$$\{x + 1, x + 1, x + 1\}$$

as our only option.

Thus, there are 6 conjugacy classes, corresponding to each set of invariant factors.

What are the representatives of the conjugacy classes?

In the beginning of lecture today, we learned how to put our matrices in rational canonical form, based on the invariant factors. Doing this gives us the following table of representatives:

invariant factors	representative
$\{x + 1, x + 1, x + 1\}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
$\{x + 1, x^2 + 1\}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$
$\{x^3 + 1\}$	$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$
$\{x^3 + x^2 + 1\}$	$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$
$\{x^3 + x + 1\}$	$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$
$\{x^3 + x^2 + x + 1\}$	$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$

**Example 20.6.** Determine the number of conjugacy classes for  $g \in \text{GL}_3(K)$  with  $g^5 = 1$ , for various fields  $K$ .

Here, we are looking for monic polynomials  $a_1 \mid \cdots \mid a_m \in K[X]$  where  $\deg a_1 > 0$ ,  $\deg a_1 + \cdots + \deg a_m = 3$ , and  $g$  is a root of  $X^5 - 1$ , so  $m_g = a_m \mid x^5 - 1$ .

(a) when  $K = \mathbb{C}$ :

In this case, note that we can factor  $x^5 - 1$  as

$$(x - 1)(x - \zeta)(x - \zeta^2)(x - \zeta^3)(x - \zeta^4), \quad \zeta = e^{2i\pi/5}.$$

Then, we again proceed via casework on the size of  $m$ .

When  $m = 1$ :

We know that  $\deg a_1 = 3$ , so  $a_1$  must be a product of three distinct factors

$$(x - \zeta^{k_1})(x - \zeta^{k_2})(x - \zeta^{k_3}).$$

Since the order of these factors doesn't matter, there are

$$\binom{5}{3} = 10 \text{ choices}$$

for the invariant factors.

When  $m = 2$ :

We know that  $\deg a_1 = 1$  and  $\deg a_2 = 2$ , so our invariant factors are of the form

$$\left\{ (x - \zeta^{k_1}), (x - \zeta^{k_1})(x - \zeta^{k_2}) \right\}.$$

There are 5 choices for the first factor and then 4 choices for the second factor, for a total of

$$20 \text{ choices}$$

for the invariant factors in this case.

When  $m = 3$ :

We know that  $a_1 = a_2 = a_3$  and all of these are linear factors of  $x^5 - 1$ , so there are

$$5 \text{ choices}$$

for the invariant factors in this case.

This gives us a total of 35 such conjugacy classes.

(b) when  $K = \mathbb{R}$ :

When  $m = 1$ :

We know that  $\deg a_1 = 3$ , so this must be a product of three distinct factors of  $x^5 - 1$ . But for this product to have real coefficients, the product must be of the form  $(x - 1)(x - \zeta^{k_1})(x - \zeta^{5-k_1})$ , since  $\zeta^{k_1}$  and  $\zeta^{5-k_1}$  are complex conjugates. We can see that then we have

$$2 \text{ choices}$$

for the  $k_1, 5 - k_1$  pair, and therefore there are only two possible sets of invariant factors in this case.

When  $m = 2$ :

We know that  $\deg a_1 = 1$  and  $\deg a_2 = 2$ . But then for  $a_1$  to have real coefficients, we must have  $a_1 = x - 1$ , and then there is no other linear factor of  $x^5 - 1$  that we can multiply by  $x - 1$  to get a polynomial with real coefficients, so there are no options with  $m = 2$ .

When  $m = 3$ :

We can see that  $x - 1$  is our only factor with real coefficients, so  $\{x - 1, x - 1, x - 1\}$  is our only option in this case.

This gives us a total of  $\boxed{3}$  such conjugacy classes.

(c) when  $K = \mathbb{F}_2$ :

In this field, we can factor  $x^5 - 1$  as  $(x - 1)(x^4 + x^3 + x^2 + x + 1)$ . We claim that the latter term is irreducible: we can see that it has no linear factors because neither 0 nor 1 are roots, so if it were to have a factorization, it would be into two quadratics. But the only irreducible quadratic in this field is  $x^2 + x + 1$ , and  $(x^2 + x + 1)^2 = x^4 + x^2 + 1$ , which is not the factor we have above. Thus, this is irreducible.

But then, we know that we cannot use our  $x^4 + x^3 + x^2 + x + 1$  factor, because it is too large, so all our invariant factors have to be  $x + 1$ , and therefore our only conjugacy class is the one corresponding to

$$\{x + 1, x + 1, x + 1\}.$$

(d) when  $K = \mathbb{F}_5$ :

In this field, we can see that  $x^5 - 1 = (x - 1)^5$ .

Then, when  $m = 3$ , we get the invariant factor  $\{(x - 1)^3\}$ , when  $m = 2$  we get the invariant factors  $\{x - 1, (x - 1)^2\}$  and when  $m = 1$  we get the invariant factors  $\{x - 1, x - 1, x - 1\}$ , for a total of  $\boxed{3}$  conjugacy classes.



## LECTURE 21: PROOF OF THE STRUCTURE THEOREM

We begin by returning to our vector space  $V$  over a field  $K$ , where we can make  $V$  into a  $K[X]$ -module by having  $X$  act by some endomorphism  $T \in \text{End}_K(V)$ . The structure theorem for modules over a PID tells us that we then have some monic polynomials  $a_1 \mid \cdots \mid a_m$  where  $\deg a_i > 0$ , such that

$$V \cong \bigoplus_{i=1}^m K[x]/(a_i),$$

and then we can use the obvious basis to write  $V$  as a matrix in rational canonical form.

If  $K$  is algebraically closed, there is another way we can express this matrix. We can see that since  $K[X]$  is a UFD, we can express each  $a_i$ , up to associate factors, as

$$p_1^{m_1} p_2^{m_2} \cdots p_{k_i}^{m_{k_i}}$$

where each  $p_j$  is irreducible. But since  $K$  is algebraically closed, we know that all of the irreducible factors are linear, so we can write each  $p_j$  as  $X - \lambda_j$ . Thus, we can write

$$V \cong \bigoplus_{j=1}^{\ell} K[X]/(X - \lambda_j)^{m_j},$$

for some  $\lambda_j \in K$ . (Note that these  $\lambda_j$ 's can repeat, since  $a_i$  and  $a_{i+1}$  will have common factors.)

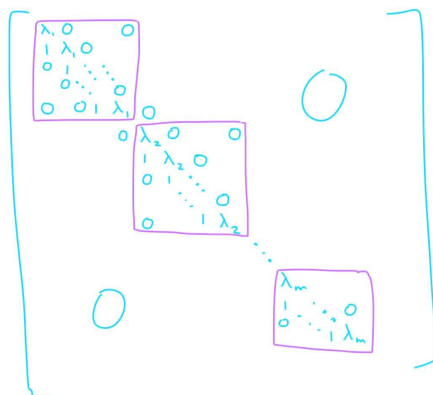
But then, we can write the “multiplication by  $X$ ” matrix over  $K[X]/(X - \lambda_j)^{m_j}$  with respect to the basis  $\{1, X - \lambda_j, \dots, (X - \lambda_j)^{m_j-1}\}$ .

We can see that 1 gets mapped to  $X$ , which equals  $1(X - \lambda_j) + \lambda_j(1)$ , and similarly, for any  $k < m_j - 1$ ,  $(X - \lambda_j)^k$  gets mapped to  $1(X - \lambda_j)^{k+1} + \lambda_j(X - \lambda_j)^k$ . However,  $(X - \lambda_j)^{m_j-1}$  gets mapped to  $X(X - \lambda_j)^{m_j-1} = \lambda_j(X - \lambda_j)^{m_j-1}$  when taken mod  $(X - \lambda_j)^{m_j}$ . Thus, we get the matrix

$$\begin{pmatrix} \lambda_j & 0 & \cdots & \\ 1 & \lambda_j & 0 & \cdots \\ 0 & \ddots & \ddots & \\ \vdots & & 1 & \lambda_j \end{pmatrix}$$

with  $\lambda_j$  along the diagonal, 1's below the diagonal, and zeroes everywhere else.

Then, combining across the dot product, we get the final matrix



with  $\lambda_j$ 's on the diagonal, 1's below the diagonal (besides at the end of a block, and zeroes everywhere else. Note that blocks may be of different sizes, because the  $(x - \lambda_j)$ s may appear with different multiplicities, and there can be multiple  $\lambda_j$ 's which are equal.

This is known as **Jordan normal form**. It is easier to work with than the rational canonical form (as in, it is more clear to see what to do if we try to take large powers of this matrix) but it only exists when  $K$  is algebraically closed.

This concludes our discussion of applications of the structure theorem for finitely generated modules over a PID; we now turn to a proof of the theorem.

As a reminder, we had:

**Theorem 19.1.** Suppose  $R$  is a PID and  $N \subset R^{\oplus n}$  is a submodule. Then,  $N$  must be free, and we can find a basis  $\{e_1, \dots, e_n\}$  of  $R^{\oplus n}$  and elements

$$a_1 \mid a_2 \mid \dots \mid a_m \neq 0 \in R$$

such that  $\{a_i e_i\}$  is a basis of  $N$ .

Moreover, these  $a_i$ 's are unique up to associates.

We will prove this now.

*Proof.* The case where  $N = (0)$  is clear, so we assume  $N$  is nonzero.

Our intuition is that, in the basis we are trying to construct, every basis element of  $N$  is a multiple of  $a_1$ , so for any linear map  $R^{\oplus n} \rightarrow R$ , we expect the image of  $N$  to be a subset of  $(a_1) \triangleleft R$ , so maybe we can define  $a_1$  by looking at such maps ...

Let us consider the set

$$\mathcal{X} = \left\{ \phi N \triangleleft R \mid \phi : R^{\oplus n} \rightarrow R \text{ is } R\text{-linear} \right\}.$$

This is nonempty, because we know for example that  $\pi_i$ , which maps each element of  $R^{\oplus n}$  to its  $e_i$ -coordinate, is such an  $R$ -linear map. Then, since this is a nonempty set of ideals of  $R$ , which is a PID and therefore noetherian, we know there is a maximal element, which we will call

$$(a_1) = \phi_1 N,$$

noting that we know this ideal is principal because this is a PID.

Now, we can see that if  $\phi_1(N) = (a_1)$ , we can find some  $y \in N$  such that  $\phi_1(y) = a_1$ . We claim that for any other  $\psi N \in \mathcal{X}$ ,  $\psi(y)$  is still a multiple of  $a_1$ .

To prove this, we can consider the ideal  $(\phi_1(y), \psi(y)) = (a_1, \psi(y)) \supseteq (a_1)$ . Since  $R$  is a PID, this ideal is just  $(d)$  for some  $d \in R$ . This means there exists  $\alpha, \beta \in R$  such that

$$d = \alpha \phi_1(y) + \beta \psi(y) = (\alpha \phi_1 + \beta \psi)(y).$$

But since  $y \in N$ , this means that

$$(\alpha \phi_1 + \beta \psi)(N) \supseteq (d) \supseteq (a_1),$$

and since the ideal on the LHS is also an element of  $\mathcal{X}$ , we get that  $(\alpha \phi_1 + \beta \psi)(N) = (a_1)$  so as to not contradict the maximality of  $\phi_1(N) \in \mathcal{X}$ . But then  $d = (a_1, \psi(y)) = (a_1)$ , so  $\psi(y) \in (a_1)$ , as we desired.

Specifically, this means that for each projection map  $\pi_i$ , which projects an element of  $R^{\oplus n}$  onto its  $e_i$ -coordinate, we get that  $\pi_i(y) \in (a_i)$ . This means that as a whole,  $y$  is a multiple of  $a_1$ , so we can write

$$y = a_1 y_1,$$

and we can see that by  $R$ -linearity of  $\phi_1$ ,  $\phi_1(y_1) = 1$ .

But this means that for any  $m \in R^{\oplus n}$ , we can write

$$m = \phi(m)y_1 + (m - \phi(m)y_1),$$

and we can see that  $\phi(m - \phi(m)y_1) = \phi(m) - \phi(m)\phi(y_1) = 0$ , so

$$R^{\oplus n} = Ry_1 \oplus \ker \phi_1$$

and therefore

$$N = Ra_1 y_1 \oplus N \cap \ker \phi_1.$$

From here, we would want to continue this process by inductively pulling out  $Ry_2$  from  $\ker \phi_1$  and a corresponding  $Ra_2 y_2$  from  $N \cap \ker \phi_1$ , and so on. But in our proof above, we used the fact that  $R^{\oplus n}$  is free over  $R$ . So we first need to show that  $\ker \phi_1$  and  $N \cap \ker \phi_1$  are free  $R$ -modules.

**Claim.** Any submodule  $M$  of  $R^{\oplus n}$  is free.

We will prove this via induction on the dimension of  $M_{(0)}$ . For a base case, we can see that when  $\dim M_{(0)} = 0$ , this means that  $M = (0)$  and therefore  $M$  is free. For the inductive case, assume  $\dim M_{(0)} = k > 0$ . Then, we can use the above process to write  $M = Ra'_1 y'_1 \oplus (M \cap \ker \phi'_1)$ , for some  $a'_1 \in R, y'_1 \in R^{\oplus n}, \phi'_1 : R^{\oplus n} \rightarrow R$ . But then  $M \cap \ker \phi'_1$  is a different submodule of  $R^{\oplus n}$ , and we can see that since

$$M_{(0)} = QR + (M \cap \ker \phi'_1)_{(0)},$$

$(M \cap \ker \phi'_1)_{(0)}$  must have dimension  $k - 1$ , so we can apply the inductive hypothesis to see that  $M$  is the direct sum of two free modules and is therefore free as well. Thus, via induction, we get that any submodule of  $R^{\oplus n}$  is free.

Thus, by our claim,  $\ker \phi_1$  is a submodule of  $R^{\oplus n}$  and therefore is free, so we can repeat our extraction step above (with  $\ker \phi_1$  substituted for  $R^{\oplus n}$  and  $N \cap \ker \phi$  substituted for  $N$ ) to get some  $\phi_2, a_2, y_2$  such that

$$\begin{aligned} \ker \phi_1 &= Ry_2 \oplus \ker \phi_2 \\ N \cap \ker \phi_1 &= Ra_2 y_2 \oplus N \cap \ker \phi_1 \cap \ker \phi_2. \end{aligned}$$

Continuing inductively, and plugging back into our original equations, we get that

$$\begin{aligned} R^{\oplus n} &= Ry_1 \oplus Ry_2 \oplus \cdots \oplus Ry_n \oplus \ker \phi_n \\ N &= Ra_1 y_1 \oplus Ra_2 y_2 \oplus \cdots \oplus Ra_n y_n \oplus N \cap \ker \phi_1 \cap \cdots \cap \ker \phi_n. \end{aligned}$$

But we know that the degree of  $R^{\oplus n}$  is  $n$ , so  $\ker \phi_n$  must be  $(0)$ , and then we get our desired bases.

The last step is to make sure that each  $a_i$  divides  $a_{i+1}$ . We will just show that  $a_1 \mid a_2$ ; to show the rest, one can proceed inductively.

We can see that there is an  $R$ -linear map  $\psi : R^{\oplus n} \rightarrow R$  such that

$$\psi(y_1) = \psi(y_2) = 1$$

but for all other basis elements  $y_i$ ,

$$\psi(y_i) = 0.$$

Thus,  $\psi$  maps an element of  $R^{\oplus n}$  to the sum of its  $y_1$  coefficient and its  $y_2$  coefficient.

But this implies that

$$\psi(N) = (a_1, a_2) \in \mathcal{X}.$$

But since  $(a_1)$  is maximal in  $\mathcal{X}$ ,  $(a_1, a_2) = (a_1)$ , so  $a_1 \mid a_2$ , as we desired.  $\square$

Recall the corollary:

**Corollary 19.2** (structure theorem for finitely generated modules over a PID). If  $R$  is a PID and  $M$  is a finitely generated  $R$ -module, then there exists

$$a_1 \mid a_2 \mid \cdots \mid a_m \neq 0 \in R,$$

where none of the  $a_i$ 's are units, such that

$$M \cong R^{\oplus d} \oplus \bigoplus_{i=1}^m (R/(a_i)).$$

Moreover,  $d, m$ , and the  $a_i$ 's are uniquely determined by  $M$ .

We proved this based on the above theorem last time, so I will not restate the proof.

However, we have not yet shown uniqueness of the invariant factors. We will do that now.

**Theorem 21.1.** In the above corollary,  $d, m$  and the ideals  $(a_i)$  are uniquely determined by  $M$ .

To prove this, we first have the following lemma:

**Lemma 21.2.** If  $c_1 \mid \cdots \mid c_t$  are elements of  $R$  such that  $c_1 \notin R^\times$ , then  $t$  is the minimal number of generators for the module

$$M = R/(c_1) \oplus R/(c_2) \oplus \cdots \oplus R/(c_t).$$

*Proof.* We know there exists some maximal ideal  $\mathfrak{m} \supset (c_1)$ . Then

$$M/\mathfrak{m}M \cong \underbrace{R/\mathfrak{m} \oplus R/\mathfrak{m} \oplus \cdots \oplus R/\mathfrak{m}}_{t \text{ times}}.$$

If  $M$  can be generated by  $s < t$  elements, then  $M/\mathfrak{m}M$  can be as well, but  $M/\mathfrak{m}M$  is a dimension- $t$  vector space over  $R/\mathfrak{m}$ , so this is a contradiction.

Thus,  $t$  is the minimal number of generators for this module.  $\square$

Based on this, we have a proposition which proves the theorem:

**Proposition 21.3.** If

$$R^{\oplus d} \oplus \bigoplus_{i=1}^m R/(a_i) \cong R^{\oplus e} \oplus \bigoplus_{i=1}^n R/(b_i),$$

where  $a_1 \mid \cdots \mid a_m \neq 0$  and  $b_1 \mid \cdots \mid b_n \neq 0$ , and  $a_1, b_1 \notin R^\times$ , then  $d = e$ ,  $m = n$ , and for each  $i$ ,  $(a_i) = (b_i)$ .

*Proof.* First, we will localize at  $(0)$  to get that

$$QR^{\oplus d} \cong QR^{\oplus e},$$

which implies  $d = e$ .

From this point, we will assume  $d = e = 0$ . We can do this because it is the same as working within the submodule  $M^{\text{tor}}$ ; this is just easier notationally.

By our lemma,  $m$  is the minimum number of elements needed to generate  $M$ , so  $n \geq m$ . But we can also apply our lemma to  $\bigoplus_{i=1}^n R/(b_i)$  to get that  $m \geq n$ , so we conclude that  $m = n$ .

Then, for any  $a \in R$ , we say that  $M[a]$  is the submodule of  $M$  defined by

$$M[a] = \{m \in M : am = 0\}.$$

We can see that for any  $i$ ,  $R/(a_i)[a]$  is the set of equivalence classes of elements  $r \in R$  such that  $ra$  is a multiple of  $a_i$ . This is  $(r_{a_i,a})/(a_i)$ , where  $r_{a_i,a} \gcd(a_i, a) = a_i$ . Note that  $(r_{a_i,a}) = R$  whenever  $a$  is a multiple of  $a_i$ .

Thus, we have that, for any  $a \in R$ ,

$$M/M[a] \cong \bigoplus_{i=1}^n R/(r_{b_i,a}) \cong \bigoplus_{i=1}^n R/(r_{a_i,a}).$$

Then, taking  $a = a_i$ , we get that the first  $i$  terms zero out,  $M/M[a_i]$  must have  $n - i$  generators. But this means that exactly the first  $i$  terms of the direct sum on the LHS must zero out, so we get that  $a_i \mid b_i \mid \cdots \mid b_n$ , and applying the lemma to  $M/M[b_i]$  similarly gives us  $b_i \mid a_i \mid \cdots \mid a_n$ , so  $(a_i) = (b_i)$ , as we desired.  $\square$

## LECTURE 22: ADDITIVE CATEGORIES, ABELIAN CATEGORIES, AND SHEAVES

Recall that  $X$  is an **initial object** for a category  $\mathcal{C}$  if for every  $Y \in \text{ob}(\mathcal{C})$ , there exists a unique morphism  $X \rightarrow Y$ .

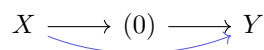
Similarly,  $X$  is a **final object** for a category  $\mathcal{C}$  if for every  $Y \in \text{ob}(\mathcal{C})$ , there exists a unique morphism  $Y \rightarrow X$ .

Using this, we have the following definitions:

**Definition 22.1.** We say that a category  $\mathcal{C}$  is a **pointed category** if  $\mathcal{C}$  has an initial object and a final object, and the two are isomorphic.

We call this the **null object** of the category, and denote it  $(0)$ .

Note that if  $\mathcal{C}$  is pointed, then for any  $X, Y \in \text{ob}(\mathcal{C})$ , there exists a unique morphism  $X \rightarrow Y$  such that the diagram

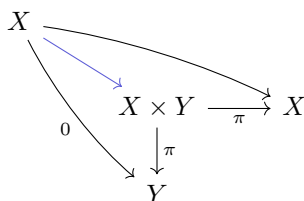
$$X \longrightarrow (0) \longrightarrow Y$$


commutes. This is called the **zero morphism**.

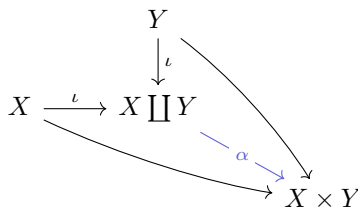
**Proposition 22.2.** If our category is pointed, and finite products and coproducts exist, then there is a natural morphism from the coproduct to the product.

*Proof.* We will show that for any  $X, Y \in \text{ob}(\mathcal{C})$ , there exists a natural morphism  $X \amalg Y \rightarrow X \times Y$ .

We can first see that the universal property of the product gives us a natural morphism  $X \rightarrow X \times Y$ , via the commutative diagram:

$$\begin{array}{ccc} X & & \\ \downarrow & \searrow & \\ X \times Y & \xrightarrow{\pi} & X \\ \downarrow \pi & & \\ Y & & \end{array}$$


and we can similarly get a natural morphism  $Y \rightarrow X \times Y$ . But then the universal property of the coproduct gives us a natural morphism  $\alpha : X \amalg Y \rightarrow X \times Y$ , via the diagram

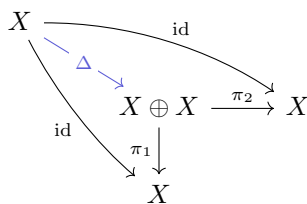
$$\begin{array}{ccc} & Y & \\ & \downarrow \iota & \\ X & \xrightarrow{\iota} & X \amalg Y \\ & \searrow & \downarrow \alpha \\ & & X \times Y \end{array}$$


□

Now, we will assume that  $\alpha$  is an isomorphism.

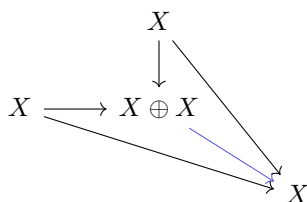
In this case, we denote the finite product/coproduct as  $X \oplus Y$ .

**Definition 22.3.** For any  $X \in \text{ob}(\mathcal{C})$ , the **diagonal embedding**  $\Delta$  is the unique morphism  $X \rightarrow X \oplus X$  that makes the diagram



commute; its existence follows from the universal property of the product.

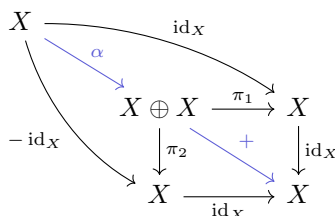
**Definition 22.4.** For any  $X \in \text{ob}(\mathcal{C})$ , the **addition map** is the unique morphism that makes the diagram



commute.

**Definition 22.5.** We say that  $\mathcal{C}$  is an **additive category** if:

- $\mathcal{C}$  has a null object  
(this gives us a zero morphism between any two objects)
- $\mathcal{C}$  has finite products and coproducts  
(this, combined with the zero morphism, gives us a morphism from the coproduct to the product)
- any finite coproduct is isomorphic to the corresponding finite product  
(this lets us define the addition map)
- there exists an  $-\text{id}_X \in \text{Hom}_{\mathcal{C}}(X, X)$  such that the induced map

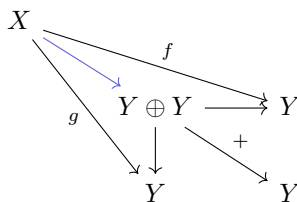


$\alpha \circ +$  equals the zero morphism.

**Proposition 22.6.** When  $\mathcal{C}$  is an additive category, then for any  $X, Y \in \mathcal{C}$ , we can give  $\text{Hom}_{\mathcal{C}}(X, Y)$  an abelian group structure.

To make  $\text{Hom}_{\mathcal{C}}(X, Y)$  into an abelian group, we define  $f + g$  to be the induced map  $X \rightarrow Y \oplus Y \rightarrow Y$  defined

by



We leave it as an exercise to show that additive inverses follow from the last part of the definition.

**Proposition 22.7.** In an additive category  $\mathcal{C}$  where  $\text{Hom}_{\mathcal{C}}(X, Y)$  has this abelian group structure, the composition map

$$\circ : \text{Hom}_{\mathcal{C}}(X, Y) \times \text{Hom}_{\mathcal{C}}(Y, Z) \longrightarrow \text{Hom}_{\mathcal{C}}(X, Z)$$

is **bilinear**, in the sense that for any  $f \in \text{Hom}_{\mathcal{C}}(X, Y)$  the map

$$\begin{aligned} \text{Hom}_{\mathcal{C}}(Y, Z) &\longrightarrow \text{Hom}_{\mathcal{C}}(X, Z) \\ g &\mapsto f \circ g \end{aligned}$$

is a group homomorphism, and for any  $g \in \text{Hom}_{\mathcal{C}}(Y, Z)$  the map

$$\begin{aligned} \text{Hom}_{\mathcal{C}}(X, Y) &\longrightarrow \text{Hom}_{\mathcal{C}}(X, Z) \\ f &\mapsto f \circ g \end{aligned}$$

is also a group homomorphism.

**Definition 22.8.** We say that a functor between additive groups is **additive** if it preserves finite products and coproducts, and initial and final objects.

Thus, if  $\mathcal{C}$  is an additive group, and  $F$  is additive, the map

$$F : \text{Hom}_{\mathcal{C}}(X, Y) \longrightarrow \text{Hom}_{\mathcal{D}}(FX, FY)$$

is also a group homomorphism.

**Definition 22.9.** We say that a category  $\mathcal{C}$  is **pre-additive** if we give each  $\text{Hom}_{\mathcal{C}}(X, Y)$  the structure of an abelian group, such that for any  $X, Y, Z \in \text{ob}(\mathcal{C})$ , the composition map

$$\circ : \text{Hom}_{\mathcal{C}}(X, Y) \times \text{Hom}_{\mathcal{C}}(Y, Z) \longrightarrow \text{Hom}_{\mathcal{C}}(X, Z)$$

is bilinear.

**Definition 22.10.** A functor  $F$  between pre-additive categories  $\mathcal{C}$  and  $\mathcal{D}$  is called **additive** if

$$F : \text{Hom}_{\mathcal{C}}(X, Y) \longrightarrow \text{Hom}_{\mathcal{D}}(FX, FY)$$

is a group homomorphism.

We just showed that all additive categories have this group structure, so we can think of additive categories as a special type of pre-additive category. In fact, we have that:

**Proposition 22.11.** A category  $\mathcal{C}$  is additive if and only if it is pre-additive and has finite products and coproducts.



*Proof.* In our discussion of additive categories above, we already showed that if  $\mathcal{C}$  is additive, it has finite products and coproducts, and it is pre-additive.

For the other direction, we need to show that if  $\mathcal{C}$  has finite products and coproducts and is pre-additive, then it has a null object, and the finite products are isomorphic to the finite coproducts.

Because  $\mathcal{C}$  has finite coproducts, it has an initial object  $X_i$  (as the empty coproduct), and because it has finite products, it has a terminal object  $X_f$  (as the empty product). By definition of the initial object, there is a unique morphism  $X_i \rightarrow X_f$ , and moreover, since  $\text{Hom}_{\mathcal{C}}(X_f, X_i)$  is an abelian group, it must have a 0. To show that  $X_i \cong X_f$ , we must show that these morphisms are inverses. We have the maps

$$X_i \longrightarrow X_f \xrightarrow{0} X_i$$

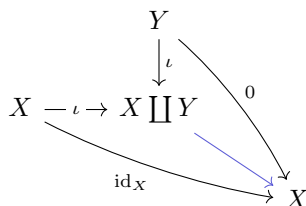
but we know that  $\text{id}$  is the unique morphism  $X_i \rightarrow X_i$ , so this composition must be the identity. Similarly, we have the composition

$$X_f \xrightarrow{0} X_i \longrightarrow X_f$$

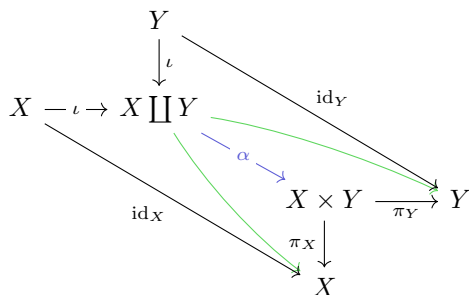
but we know that  $\text{id}$  is the unique morphism  $X_f \rightarrow X_f$  (since by definition of the final object, these morphisms are unique), so this composition must also be the identity.

Thus, the initial and final objects are isomorphic, so this category has a null object.

Then, we need to show that for any  $X, Y \in \text{ob}(\mathcal{C})$ ,  $X \amalg Y \cong X \times Y$ . We will do this via a series of commutative diagrams. First, we can see that by definition of the coproduct, there exist unique maps  $X \amalg Y \rightarrow X$  such that the diagram



commutes, and we can find a similar map  $X \amalg Y \rightarrow Y$ . But then, by the universal property of the product, there exists a unique  $\alpha : X \amalg Y \rightarrow X \times Y$  such that the diagram



commutes, where the green maps are the induced morphisms we just found.

Then, we claim that  $\alpha$  has inverse  $\iota_X \circ \pi_X + \iota_Y \circ \pi_Y$ . We can see that

$$(\iota_X \circ \pi_X + \iota_Y \circ \pi_Y) \circ \alpha \circ \iota_X = \iota_X \circ (\pi_X \circ \alpha \circ \iota_X) + \iota_Y \circ (\pi_Y \circ \alpha \circ \iota_X) = \iota_X + 0 = \iota_X.$$

Similarly, we can see that this composition, composed with  $\iota_Y$ , gives us  $\iota_Y$ , and then applying the universal property of the coproduct, we can see that this must be the identity map  $\text{id}_{X \amalg Y}$ .

We can apply similar logic to see that  $\alpha \circ (\iota_X \circ \pi_x + \iota_Y \circ \pi_Y)$  must be the identity map  $\text{id}_{X \times Y}$ , and therefore these two maps are inverses and  $\alpha$  really is an isomorphism.  $\square$

We leave it as an exercise to check that, if we start with a preadditive category which has finite products and coproducts, the additive structure we get from the addition map coincides with the additive structure we get from the preadditive category.

Recall that a **monomorphism** is a morphism  $f : X \rightarrow Y$ , such that, for any other  $g : Z \rightarrow X$ ,  $h : Z \rightarrow X$ ,  $f \circ g = f \circ h$  only if  $g = h$ . We can think of this as a generalization of injectivity.

A **epimorphism** is a morphism  $f : X \rightarrow Y$ , such that, for any other  $g : Y \rightarrow Z$ ,  $h : Y \rightarrow Z$ ,  $g \circ f = h \circ f$  only if  $g = h$ . We can think of this as a generalization of surjectivity.

Using this, we have the following definition:

**Definition 22.12.** We say that an additive category  $\mathcal{C}$  is **abelian** if for any  $f \in \text{Hom}_{\mathcal{C}}(X, Y)$ , the diagram

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ & \xrightarrow{0} & \end{array}$$

has a limit  $\ker f \rightarrow X$  (called a **kernel**) and a colimit  $Y \rightarrow \text{coker } f$  (called a **cokernel**), and, moreover, any monomorphism is the kernel of some  $X \rightarrow Y$ , and any epimorphism is the cokernel of some  $X \rightarrow Y$ .

We leave it as an exercise to check that any kernel is a monomorphism and any cokernel is an epimorphism.

**Example 22.13.**  $\mathbf{R}\text{-Mod}$  is an example of an abelian category.

Another example is: if  $\Gamma$  is an abelian group, then  $\Gamma\text{-Mod}$ , which is the set of abelian groups  $M$  with some defined action of  $\gamma$  on  $M$ , is an abelian category.

We will now move on to talking about *sheaves*.

**Example 22.14.** Let  $X$  be a topological space. Then, we can define the category  $\underline{\text{Open}}(X)$  to be the category of all open subsets of  $X$ , where the only morphisms are inclusion morphisms between objects and their supersets.

**Definition 22.15.** We say that a **pre-sheaf** on  $X$  is the contravariant functor  $F : \underline{\text{Open}}(X) \rightarrow \underline{\text{Ab}}$ . This means that for all open sets  $U, V \subset X$  we associate abelian groups  $F(U)$  and  $F(V)$ , and if  $V \subset U$  then we have a morphism  $F(U) \rightarrow F(V)$ , called the **restriction morphism**.

Notation-wise, we say that the restriction morphism maps  $m \in F(U)$  to  $m|_V$ .

Moreover, for  $F$  to be a pre-sheaf, we require the restriction morphisms to have the property that for any  $W \subset V \subset U$ , the diagram

$$\begin{array}{ccccc} F(U) & \xrightarrow{m \mapsto m|_V} & F(V) & \xrightarrow{m \mapsto m|_W} & F(W) \\ & \searrow & \xrightarrow{m \mapsto m|_W} & \nearrow & \\ & & & & \end{array}$$

commutes.

*Note that there is a bit of notational ambiguity here, because our notation for the restriction morphism only indicates the codomain, and not the domain, of the restriction. This means there are times in the rest of this lecture where we use the same notation to indicate two different morphisms; please be careful about this*

when trying to read the lecture notes!

**Definition 22.16.** A morphism between pre-sheaves is a natural transformation  $\phi : F \rightarrow G$ , which means that it collection of maps  $\phi_U : F(U) \rightarrow G(U)$  such that for all  $V \subset U$ , the diagram

$$\begin{array}{ccc} F(U) & \xrightarrow{\phi_U} & G(U) \\ \downarrow m \mapsto m|_V & & \downarrow m \mapsto m|_V \\ F(V) & \xrightarrow{\phi_V} & G(V) \end{array}$$

commutes, or

$$\phi(m)|_V = \phi(m|_V).$$

**Definition 22.17.** Now that we have morphisms between pre-sheaves, we can define  $\text{Pre-Sh}(X)$  as the category of all pre-sheaves on  $X$ .

**Definition 22.18.** We say that a pre-sheaf  $F$  is a **sheaf** if for all open sets  $U \subset X$  and for all open covers  $\{U_i\}_{i \in I}$  of  $U$ ,  $F(U)$  is the limit of

$$\prod_i F(U_i) \begin{array}{c} \xrightarrow{(s_i)_{i \mapsto (s_i|_{U_i \cap U_j})_{(i,j)}}} \\ \xrightarrow{(s_i)_{i \mapsto (s_i|_{U_i \cap U_j})_{(j,i)}}} \end{array} \prod_{i,j} F(U_i \cap U_j)$$

Intuitively, we want the behavior of  $F(U)$  to match the behavior of  $F$  on the open cover, at the places where the open cover agrees with itself.

More formally, this implies that:

- If  $s \in F(U)$  such that  $s|_{U_i} = 0$  for all  $i$ , then  $s = 0$ .
- If we have some  $(s_i) \in \prod_i F(U_i)$  such that, for all  $i, j$ ,  $s_i|_{U_i \cap U_j} = s_j|_{U_i \cap U_j}$  (so the two arrows in the diagram agree), then there is a unique  $s \in F(U)$  such that for all  $i$ ,  $s|_{U_i} = s_i$ .

**Proposition 22.19.** We say that  $\text{Sh}(X)$  is the category of all sheaves on  $X$ ; this is a full subcategory of  $\text{Pre-Sh}(X)$

**Example 22.20.** One sheaf on  $X$  is the functor  $\mathcal{C}$ , where

$$\mathcal{C}(U) = \{f : U \rightarrow \mathbb{C} \text{ continuous}\}.$$

Then, the restriction morphism is what we might expect: if  $V \subseteq U$  and  $f : U \rightarrow \mathbb{C}$ , then  $f|_V$  is just the restricted function  $V \rightarrow \mathbb{C}$ .

Moreover, we can see that if  $U_i, U_j \subset U$ , then for any  $f \in \mathcal{C}(U)$ ,

$$f|_{U_i|_{U_i \cap U_j}} = f|_{U_j|_{U_i \cap U_j}}.$$

## LECTURE 23: EXACT SEQUENCES IN ABELIAN CATEGORIES

We begin by finishing our lecture on sheaves.

If  $X$  is a topological space,  $F$  is a pre-sheaf on  $X$ , and  $U \subset X$  is an open set, then:

**Definition 23.1.** We say that  $F(U)$  is a **section** of  $F$  at  $U$ .

**Definition 23.2.** We say that

$$F_x = \varinjlim_{U \ni x \in U} F(U)$$

is the **stalk** of  $F$  at  $x$ .

We also have the following remark, which we will not prove in class:

**Proposition 23.3.** If  $F, G$  are sheaves on  $X$ , then:

The following statements are equivalent:

- $\phi : F \rightarrow G \in \text{mor}(\text{Sh}(X))$  is a monomorphism
- $\phi_U : F(U) \rightarrow G(U)$  is injective for all open sets  $U \subset X$
- $\phi_x : F_x \rightarrow G_x$  is injective for all  $x \in X$

Similarly,  $\phi : F \rightarrow G \in \text{mor}(\text{Sh}(X))$  is an epimorphism if and only if  $\phi_x : F_x \rightarrow G_x$  is surjective for all  $x \in X$ .

However, epimorphisms don't play as nicely with sections;  $\phi : F \rightarrow G$  being an epimorphism doesn't necessarily imply that  $\phi_U : F(U) \rightarrow G(U)$  is surjective.

Now, we will return to talking about general abelian categories.

Last time, we mentioned that in an abelian category, for any morphism  $X \rightarrow Y$ , we can extend this to

$$\ker f \longrightarrow X \longrightarrow Y \longrightarrow \text{coker } f,$$

where the first part is a monomorphism and the second part is an epimorphism.

**Definition 23.4.** An abelian category also has the concept of an **image**, where

$$\text{im } f = \text{coker}(\ker f \longrightarrow X) = \ker(Y \longrightarrow \text{coker } f).$$

**Definition 23.5.** Then, we say that something of the form:

$$\cdots \longrightarrow X_0 \xrightarrow{f_0} X_1 \xrightarrow{f_1} X_2 \xrightarrow{f_2} X_3 \xrightarrow{f_3} X_4 \longrightarrow \cdots$$

is a **complex** if for all  $i$ ,  $f_{i+1} \circ f_i = 0$ , and it is **exact** if  $\text{im } f_i = \ker f_{i+1}$  for all  $i$ .

**Definition 23.6.** If a sequence of the form

$$0 \longrightarrow X \longrightarrow Y \longrightarrow Z \longrightarrow 0$$

is exact, then it is called **short exact**.

**Definition 23.7.** If a sequence of the form

$$0 \longrightarrow X \longrightarrow Y \longrightarrow Z$$

is exact, then it is called **left exact**.

**Proposition 23.8.** A sequence is left exact if and only if  $X = \ker(Y \rightarrow Z)$ .

**Definition 23.9.** If a sequence of the form

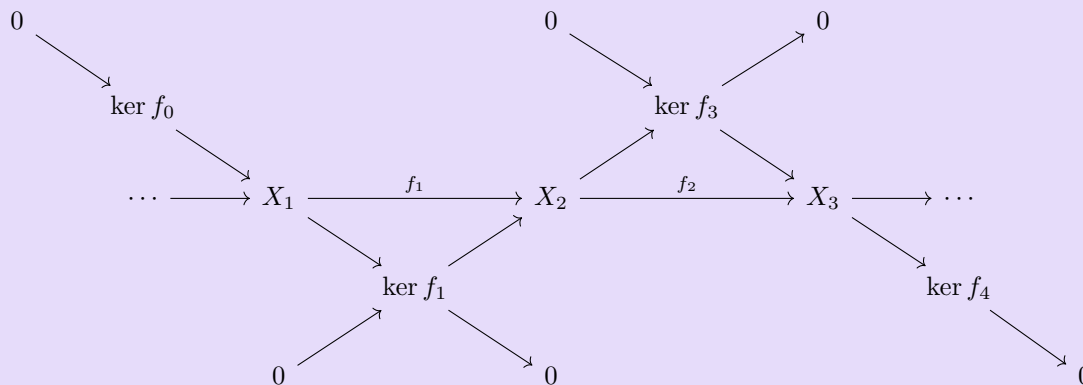
$$X \longrightarrow Y \longrightarrow Z \longrightarrow 0$$

is exact, then it is called **right exact**.

**Proposition 23.10.** A sequence is right exact if and only if  $Z = \text{coker}(X \rightarrow Y)$ .

**Proposition 23.11.** A sequence is short exact if and only if it is left exact and right exact.

**Proposition 23.12.** We can split a long exact sequence into a bunch of short exact sequences, as follows:



and for every collection of short exact sequences

$$0 \longrightarrow \text{coker } f_{i-2} \longrightarrow X_i \longrightarrow \ker f_{i+1} \longrightarrow 0,$$

we can combine them into a long exact sequence.

*Proof.* For the first part, we leave it as an exercise to check that  $\ker f_i = \text{im } f_{i-1} = \text{coker } f_{i-2}$  for all  $i$ . We leave the second part as an exercise. □

Between abelian categories, the only useful kind of functor is an additive functor. As a reminder, additive functors preserve  $(0)$  and they preserve direct sums  $\oplus$ , but not in general kernels and cokernels.

We can give an example of this:

**Example 23.13.** Consider the functor  $\underline{\text{Ab}} \rightarrow \underline{\text{Ab}}$  defined by  $G \mapsto G \otimes_{\mathbb{Z}} \mathbb{Z}/(2)$ .

The image of the short exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \longrightarrow \mathbb{Z}/(2) \longrightarrow 0$$

is the right exact sequence

$$\mathbb{Z}/(2) \xrightarrow{0} \mathbb{Z}/(2) \longrightarrow \mathbb{Z}/(2) \longrightarrow 0$$

but the first map is no longer injective, so this functor does not preserve kernels.

Similarly, the image of the short exact sequence under the functor  $G \mapsto \text{Hom}_{\mathbb{Z}}(\mathbb{Z}/(2), G)$  is the left exact sequence

$$0 \longrightarrow (0) \longrightarrow (0) \longrightarrow \mathbb{Z}/(2)$$

but the second map is no longer surjective, so this functor does not preserve cokernels.

In a sense, homological algebra is entirely about understanding how additive functors interact with kernels and cokernels.

We have special words for the functors that do preserve these:

**Definition 23.14.** An additive (covariant) functor  $F$  is **left exact** if it preserves kernels.

Note that this is equivalent to  $F$  preserving left-exact sequences.

**Definition 23.15.** An additive (covariant) functor  $F$  is **right exact** if it preserves cokernels.

Note that this is equivalent to  $F$  preserving right-exact sequences.

**Definition 23.16.** An additive (covariant) functor  $F$  is **exact** if it preserves kernels and cokernels.

Note that this is equivalent to  $F$  preserving short exact sequences, which is equivalent to  $F$  preserving exact sequences.

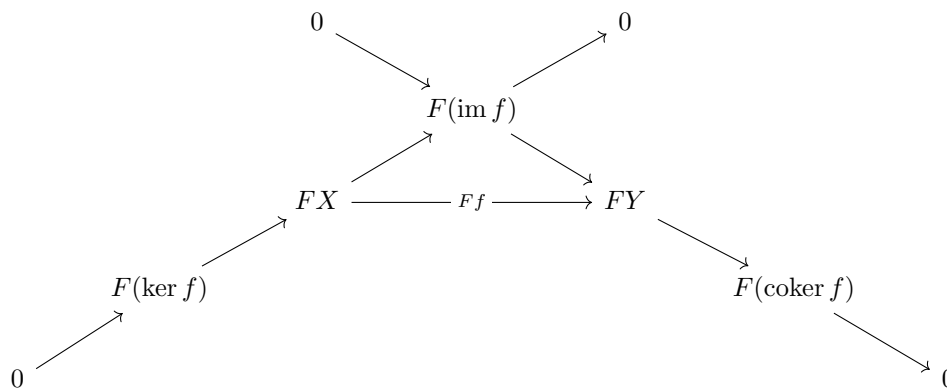
It should be clear that if  $F$  preserves kernels and cokernels, then it preserves images, so it preserves exact sequences (and therefore short exact sequences). However, it is harder than one might think to show that if  $F$  preserves short exact sequences, then it preserves kernels and cokernels:

**Lemma 23.17.** If an additive (covariant) functor  $F$  preserves short exact sequences, then it preserves kernels and cokernels.

*Proof.* We have the sequences

$$\begin{array}{ccccc}
 & & 0 & & 0 \\
 & & \searrow & & \swarrow \\
 & & & \text{im } f & \\
 & & \swarrow & & \searrow \\
 & & X & \xrightarrow{f} & Y \\
 & \swarrow & & & \searrow \\
 & \text{ker } f & & & \text{coker } f \\
 & \swarrow & & & \searrow \\
 0 & & & & 0
 \end{array}$$

Applying  $F$ , we have the sequences

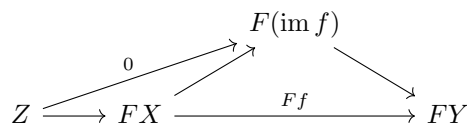


which are still short exact.

We want to show that  $F(\ker f) = \ker Ff$ . We can see that  $F(\ker f) = \ker(FX \rightarrow F(\text{im } f))$  from exactness of this sequence. What we want to show is that for any other  $Z$  such that

$$\begin{array}{ccccc}
 Z & \longrightarrow & FX & \xrightarrow{Ff} & FY \\
 & \searrow & & \searrow & \\
 & & & & 0
 \end{array}$$

commutes,  $Z$  factors uniquely through  $F(\ker f)$ . But if we add in the  $F(\text{im } f)$  part of the sequence, and note that  $F(\text{im } f) \rightarrow FY$  is a monomorphism, the diagram



must commute, and then using the fact that  $F(\ker f) = \ker(FX \rightarrow F(\text{im } f))$ , we get that these maps must factor uniquely through  $F(\ker f)$ , so

$$F(\ker f) = \ker(Ff)$$

as we desired.

The proof that  $F(\text{coker } f) = \text{coker}(Ff)$  is similar, so we leave it as an exercise. □

We have similar definitions for contravariant functors:

**Definition 23.18.** A contravariant additive functor  $F : \mathcal{C} \rightarrow \mathcal{D}$  is:

- **left exact** if  $F^{\text{op}} : \mathcal{C}^{\text{op}} \rightarrow \mathcal{D}$  is left exact.
- **right exact** if  $F^{\text{op}} : \mathcal{C}^{\text{op}} \rightarrow \mathcal{D}$  is right exact.
- **exact** if  $F^{\text{op}} : \mathcal{C}^{\text{op}} \rightarrow \mathcal{D}$  is exact.

Thus, for example,  $F$  is left exact if and only if for all right exact sequences  $X \rightarrow Y \rightarrow Z \rightarrow 0$  in  $\mathcal{C}$ , the image

$$0 \longrightarrow FZ \longrightarrow FY \longrightarrow FX$$

is left exact. So  $F$  is named after the sequences in the *target*.

**Proposition 23.19.** Similarly to before,  $F$  is left exact if and only if it takes cokernels to kernels, and  $F$  is right exact if and only if it takes kernels to cokernels.

Let's look at some examples of such functors.

**Example 23.20.** In the category  $R\text{-Mod}$ :

- the functor  $M \mapsto D^{-1}M$  is *exact* (we showed this in a homework problem)
- the functor  $M \mapsto M \otimes N$ , for a fixed  $N$ , is *right exact* (but not necessarily left exact)
- the functor  $M \mapsto \text{Hom}_R(N, M)$  is *left exact* (but not necessarily right exact)
- the functor  $M \mapsto \text{Hom}_R(M, N)$  is *left exact* (but not necessarily right exact)

The functor  $\text{Sh}(X) \rightarrow \text{Ab}$  defined by  $F \mapsto F(X)$  is *left exact* but not in general right exact (because of Proposition 23.3).

The functor  $\Gamma\text{-Mod} \rightarrow \text{Ab}$  defined by  $M \mapsto M^\Gamma$ , where

$$M^\Gamma = \{m \in M \mid \gamma m = m \text{ for all } \gamma \in \Gamma\},$$

is *left exact* but not in general right exact.

But in some special cases, *any* additive functor will preserve exactness!

**Lemma 23.21.** If

$$0 \longrightarrow M \longrightarrow N \longrightarrow F_R(X) \longrightarrow 0$$

is a short exact sequence of  $R$ -modules and  $F : R\text{-Mod} \rightarrow \mathcal{D}$  is additive, then

$$0 \longrightarrow FM \longrightarrow FN \longrightarrow F(F_R(X)) \longrightarrow 0$$

is again exact.

*Proof.* We have the short exact sequence

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} F_R(X) \longrightarrow 0$$

But we can construct a “section”  $s : F_R(X) \rightarrow N$ , which is a one-sided inverse to  $g$ , so that  $g \circ s = \text{id}_{F_R(X)}$  but  $s \circ g$  is not necessarily the identity.

Specifically, for any basis element  $e_x$ , we define  $s(e_x)$  to be any preimage of  $e_x$ , and we know this uniquely defines an  $R$ -linear map  $F_R(X) \rightarrow N$ .

Then, we have that  $N \cong M \oplus F_R(X)$  via the maps

$$\begin{aligned} f(m) + s(p) &\longleftarrow (m, p) \\ n &\longmapsto (f^{-1}(n - s(g(n))), g(n)), \end{aligned}$$

and we leave it as an exercise to see that these are inverses.

Then, we know we have the standard exact sequence

$$0 \longrightarrow FM \longrightarrow FM \oplus F(F_R(X)) \longrightarrow F(F_R(X)) \longrightarrow 0$$

via the projection and inclusion maps. But since  $F$  preserves direct sums, this induces the exact sequence

$$0 \longrightarrow FM \longrightarrow FN \longrightarrow F(F_R(X)) \longrightarrow 0,$$

as we desired. □



The important part in this proof was not really that  $F_R(X)$  was free, but that we were able to create this section  $s$ . Thus, we can generalize our above strategy to any abelian category:

**Definition 23.22.** We say that  $P \in \text{ob}(\mathcal{C})$  is **projective** if for any

$$\begin{array}{ccc} & & P \\ & & \downarrow \\ X & \twoheadrightarrow & Y \end{array}$$

there exists a morphism  $P \rightarrow X$  that makes the diagram

$$\begin{array}{ccc} & & P \\ & \swarrow & \downarrow \\ X & \twoheadrightarrow & Y \end{array}$$

commute.

**Example 23.23.** In the category  $\mathcal{C} = \mathbf{R}\text{-Mod}$ , any free module is projective.

**Definition 23.24.** We say that  $I \in \text{ob}(\mathcal{C})$  is **injective** if for any

$$\begin{array}{ccc} I & & \\ \uparrow & & \\ X & \hookrightarrow & Y \end{array}$$

there exists a morphism  $Y \rightarrow I$  that makes the diagram

$$\begin{array}{ccc} I & & \\ \uparrow & \swarrow & \\ X & \hookrightarrow & Y \end{array}$$

commute.

**Lemma 23.25.** If  $0 \rightarrow X \rightarrow Y \rightarrow Z \rightarrow 0$  is exact in  $\mathcal{C}$  and  $F : \mathcal{C} \rightarrow \mathcal{D}$  is additive, then if  $X$  is injective or  $Z$  is projective, the image

$$0 \rightarrow DX \rightarrow DY \rightarrow DZ \rightarrow 0$$

is exact in  $\mathcal{D}$ .

**Definition 23.26.** We say that  $\mathcal{C}$  has **enough projectives** if for any  $X \in \text{ob}(\mathcal{C})$ , there exists an epimorphism  $P \rightarrow X$ , where  $P$  is projective.

We say that  $\mathcal{C}$  has **enough injectives** if for any  $X \in \text{ob}(\mathcal{C})$ , there exists a monomorphism  $X \rightarrow I$ , where  $I$  is injective.

**Proposition 23.27.** If  $\mathcal{C}$  has enough projectives, then for any  $X$ , we can construct the exact sequence

$$\dots \rightarrow P^{-2} \rightarrow P^{-1} \rightarrow P^0 \rightarrow X \rightarrow 0,$$

where each  $P^i$  is projective. We call this the **projective resolution of  $X$** .

If  $\mathcal{C}$  has enough injectives, then for any  $X$ , we can construct the exact sequence

$$0 \longrightarrow X \longrightarrow I^0 \longrightarrow I^1 \longrightarrow I^2 \longrightarrow \dots,$$

where each  $I^i$  is injective. We call this the **injective resolution of  $X$** .

The main idea of homological algebra is that we can replace  $X$  with these resolutions to get nicer properties.

## LECTURE 24: PROJECTIVES AND INJECTIVES

First, as a note, there was an error in the initial definition of an additive category - we need to additionally assume that in every  $\text{Hom}_{\mathcal{C}}(X, X)$  there exists a  $-\text{id}_X$  function such that  $-\text{id}_X + \text{id}_X = 0$ , in order to be able to show that the homomorphisms actually form an abelian group. (This is now fixed in the notes for the additive categories lecture.)

Last lecture, we left off defining projectives, injectives, and what it means to have enough projectives or enough injectives.

**Example 24.1.**  $R\text{-Mod}$  and  $\Gamma\text{-Mod}$  have enough projectives and enough injectives.

$\text{Sh}(X)$  has enough injectives, but it doesn't usually have enough projectives.

**Definition 24.2.** We say that an  $R$ -module  $P$  is **finitely presented** if there exists some finite  $a, b$  such that we have the right exact sequence

$$R^{\oplus b} \longrightarrow R^{\oplus a} \longrightarrow P \longrightarrow 0.$$

Note that this is a stronger condition than just being finitely generated.

**Example 24.3.** When  $P$  is finitely generated over a noetherian ring, it is finitely presented.

**Lemma 24.4.** Suppose that  $P$  is an  $R$ -module. Then, the following are equivalent:

1.  $P$  is projective
2. There exists a set  $\Omega$  and an  $R$ -module  $Q$  such that  $P \oplus Q \cong F_R(\Omega)$  (so it is a summand of a free module).

Moreover, if  $P$  is finitely presented, these are also equivalent to:

3.  $P_{\mathfrak{p}}$  is free over  $R_{\mathfrak{p}}$  for all  $\mathfrak{p} \triangleleft R$  prime.
4.  $P_{\mathfrak{m}}$  is free over  $R_{\mathfrak{m}}$  for all  $\mathfrak{m} \triangleleft R$  maximal.

*Proof.* We will first show  $1 \implies 2$ :

Recall that since  $P$  is projective, there is a morphism  $s : P \rightarrow F_R(P)$  that makes the diagram

$$\begin{array}{ccc} & & P \\ & \swarrow s & \downarrow \\ F_R(P) & \longrightarrow & P \end{array}$$

commute, so  $\pi \circ s = \text{id}_P$ .

This implies that  $F_R(P) \cong \ker \pi \oplus P$ , via the isomorphisms

$$\begin{aligned} a + s(b) &\longleftarrow (a, b) \\ c &\longmapsto (c - s(\pi(c)), \pi(c)) \end{aligned}$$

We leave it as an exercise to check that these are really inverses.

Now we will show that 2  $\implies$  1:

We have  $P \oplus Q \cong F_R(\Omega)$ , and we want to show that for any  $X, Y$  such that we have the diagram

$$\begin{array}{ccc} & & P \\ & & \downarrow \\ X & \longrightarrow & Y \end{array}$$

there exists some  $s : P \rightarrow X$  that makes the diagram commute. But we know there exists some  $\alpha$  that makes the diagram

$$\begin{array}{ccc} & & F_R(\Omega) \\ & & \downarrow \pi \\ & & P \\ & & \downarrow \\ X & \longrightarrow & Y \end{array}$$

$\alpha$  (arrow from  $F_R(\Omega)$  to  $X$ )

commute, since all free modules are projective, and then we can just take  $s = \alpha \circ \iota$ , where  $\iota$  is the inclusion map  $P \rightarrow P \oplus Q$ .

Now, we will show that if  $P$  is finitely presented, then 1 and 2 imply 3:

Let  $\Omega$  be a finite set that generates  $P$ . We know that there is a projection map  $F_R(\Omega) \rightarrow P$ , and then using the same argument as 1  $\implies$  2, we are able to say  $P \oplus Q = F_R(\Omega)$ , for some finite  $\Omega$ .

Then, localizing at  $\wp$ , we get that

$$F_{R_\wp}(\Omega) \cong P_\wp \oplus Q_\wp$$

as  $R_\wp$ -modules.

Then, taking everything mod  $\wp$ , we get that

$$F_{R_\wp/\wp}(\Omega) \cong P_\wp/\wp P_\wp \oplus Q_\wp/\wp Q_\wp.$$

But  $R_\wp/\wp$  is a field, so this is now an equivalence in terms of vector spaces. That means we can find a basis  $\{\bar{e}_1, \dots, \bar{e}_a\}$  of  $P_\wp/\wp P_\wp$  and a basis  $\{\bar{e}_{a+1}, \dots, \bar{e}_n\}$  of  $Q_\wp/\wp Q_\wp$ .

Then, Nakayama's lemma tells us that if we take  $\{e_1, \dots, e_a\}$  such that  $e_i/\wp P_\wp = \bar{e}_i$  for each  $i$ , this forms a generating set for  $P_\wp$  as an  $R_\wp$ -module. So we have the surjection

$$R_\wp^{\oplus a} \twoheadrightarrow P_\wp$$

and we similarly get the surjection

$$R_\wp^{\oplus n-a} \twoheadrightarrow Q_\wp.$$

Combining these, we get that

$$R_\wp^{\oplus b} \twoheadrightarrow P_\wp \oplus Q_\wp = F_{R_\wp}(\Omega).$$

We can represent this surjection with some  $n \times n$  matrix  $A$ . But we can see that  $A \pmod{\wp}$  is an isomorphism, so  $\det A \notin \wp$ , and since  $\wp$  is the unique maximal ideal of  $R_\wp$ ,  $\det A$  must be a unit in  $R_\wp$ .

Thus,  $A$  is invertible, which means this surjection is invertible; specifically, this implies that

$$R_\wp^{\oplus a} \twoheadrightarrow P_\wp$$

is also injective and therefore must also be an isomorphism, as we desired.

Then,  $3 \implies 4$  is clear, so we will skip this and show that  $4 \implies 1$ .

We want to show that for any  $M, N$  such that we have the diagram

$$\begin{array}{ccc} & P & \\ & \downarrow & \\ M & \twoheadrightarrow & N \end{array}$$

we can find a map  $P \rightarrow M$  that makes the diagram commute.

This is equivalent to showing that  $\text{Hom}_R(P, M) \rightarrow \text{Hom}_R(P, N)$  is surjective; we have the right exact sequence

$$\text{Hom}_R(P, M) \longrightarrow \text{Hom}_R(P, N) \longrightarrow Q \longrightarrow 0$$

and we want to show that  $Q = 0$ .

To do so, we can localize at a maximal ideal  $\mathfrak{m}$  to get the right exact sequence

$$\text{Hom}_R(P, M)_{\mathfrak{m}} \longrightarrow \text{Hom}_R(P, N)_{\mathfrak{m}} \longrightarrow Q_{\mathfrak{m}} \longrightarrow 0.$$

**Claim.** The above sequence is equal to the right exact sequence

$$\text{Hom}_{R_{\mathfrak{m}}}(P_{\mathfrak{m}}, M_{\mathfrak{m}}) \longrightarrow \text{Hom}_{R_{\mathfrak{m}}}(P_{\mathfrak{m}}, N_{\mathfrak{m}}) \longrightarrow Q_{\mathfrak{m}} \longrightarrow 0.$$

We will assume this claim is true for now; then we can see that since  $P_{\mathfrak{m}}$  is free,  $\text{Hom}_{R_{\mathfrak{m}}}(P_{\mathfrak{m}}, M_{\mathfrak{m}})$  must surject onto  $\text{Hom}_{R_{\mathfrak{m}}}(P_{\mathfrak{m}}, N_{\mathfrak{m}})$ , so  $Q_{\mathfrak{m}}$  is 0, which means  $Q = 0$ , as we desired.  $\square$

To prove the claim in the middle, we have the following sub-lemma:

**Lemma 24.5.** If  $M, N$  are  $R$ -modules with  $M$  finitely presented and  $D \subset R$  multiplicative, then

$$D^{-1} \text{Hom}_R(M, N) \cong \text{Hom}_{D^{-1}R}(D^{-1}M, D^{-1}N).$$

*Proof.* We don't have time to fully prove this, but the idea is that:

We first prove the case where  $M$  is a finite free module, so we can write  $M \cong R^{\oplus a}$ ,

and then we use the right exact sequence  $R^{\oplus b} \rightarrow R^{\oplus a} \rightarrow M \rightarrow 0$ , and note that this induces a left exact sequence

$$0 \longrightarrow \text{Hom}(M, N) \longrightarrow \text{Hom}(R^{\oplus a}, N) \longrightarrow \text{Hom}(R^{\oplus b}, N).$$

If we apply the  $D^{-1}$  before the homomorphism operator, then we get the sequence

$$\text{Hom}_{D^{-1}R}(D^{-1}M, D^{-1}N) \longrightarrow \text{Hom}_{D^{-1}R}(D^{-1}R^{\oplus a}, D^{-1}N) \longrightarrow \text{Hom}_{D^{-1}R}(D^{-1}R^{\oplus b}, D^{-1}N),$$

while if we apply the  $D^{-1}$  after the homomorphism operator, we get

$$D^{-1} \text{Hom}_R(M, N) \longrightarrow D^{-1} \text{Hom}_R(R^{\oplus a}, N) \longrightarrow D^{-1} \text{Hom}_R(R^{\oplus b}, N).$$

It is possible to show that this implies the isomorphism we want.  $\square$

Now, we will move on to proving a few facts about injectives.

**Definition 24.6.** We say that a  $\mathbb{Z}$ -module  $M$  is **divisible** if for all  $m \in M$  and all  $a \in \mathbb{Z}_{\neq 0}$ , there exists some  $m' \in M$  such that  $am' = m$ .

**Example 24.7.**  $\mathbb{Q}$  and  $\mathbb{Q}/\mathbb{Z}$  are examples of divisible  $\mathbb{Z}$ -modules.

**Lemma 24.8.** A  $\mathbb{Z}$ -module  $I$  is injective if and only if it is divisible.

*Proof.* If  $I$  is injective, then for any such  $m, a$ , we can consider the maps

$$\begin{array}{ccc} & I & \\ & \uparrow & \\ 1 \mapsto m & & \\ \mathbb{Z} & \xrightarrow{n \mapsto an} & \mathbb{Z} \end{array}$$

and we know there exists a map

$$\begin{array}{ccc} & I & \\ & \uparrow & \swarrow 1 \mapsto m' \\ 1 \mapsto m & & \\ \mathbb{Z} & \xrightarrow{n \mapsto an} & \mathbb{Z} \end{array}$$

that makes the diagram commute. But we can see that moving from  $\mathbb{Z}$  to  $I$  in one direction will give us  $1 \mapsto m$  and moving from  $\mathbb{Z}$  to  $I$  in the other direction will give us  $1 \mapsto am'$ . Thus, we must have

$$am' = m,$$

as we desired.

If  $I$  is divisible, then we want to show that for any  $X, Y$  such that we have this diagram:

$$\begin{array}{ccc} & I & \\ & \uparrow & \\ \alpha & & \\ X & \longrightarrow & Y \end{array}$$

there is a map  $Y \rightarrow I$  such that the diagram commutes.

We will do so by essentially granularly extending the map  $\alpha$ .

Consider the set

$$\mathcal{X} = \{(Z, \beta) \mid X \subseteq Z \subseteq Y \text{ submodules, } \beta : Z \rightarrow I, \beta|_X = \alpha\}.$$

That is, we consider the set of all morphisms  $\beta : Z \rightarrow I$  that extend  $\alpha$ . We can apply a partial ordering to this set, by saying

$$(Z, \beta) \geq (Z', \beta') \text{ if } Z \supseteq Z' \text{ and } \beta|_{Z'} = \beta'.$$

We can see that this is a nonempty set, because  $(X, \alpha)$  is an element of the set, and we can see that for any chain  $C \subset \mathcal{X}$ , we have an upper bound  $(W, \gamma)$  defined by

$$W = \bigcup_{(Z, \beta) \in C} Z \subset Y,$$

and since for any  $w \in W$ ,  $w \in Z$  for some  $(Z, \beta) \in C$ , we can define  $\gamma(w) = \beta(w)$ .

Thus, every chain has an upper bound, so we can apply Zorn's lemma to get a maximum  $(Z, \beta)$  of this set.

If  $Z = Y$  then we have won.

We will assume  $Z \neq Y$  and arrive at a contradiction. Specifically, choose some  $y \in Y - Z$ , and then consider the ideal

$$J = \{n \mid ny \in Z\} \triangleleft \mathbb{Z}.$$

Since  $\mathbb{Z}$  is a PID, we can write  $J = (a)$ , and then we know there exists some  $m = \beta(ay)$ , and some  $m' \in I$  such that  $am' = m$ . Then, we can consider the morphism

$$\beta' : \langle Z, y \rangle \longrightarrow I$$

defined by

$$z + ny \mapsto \beta(z) + nm'.$$

We leave it as an exercise to check that this is a well-defined morphism. Then, we see that  $(\langle Z, y \rangle, \beta') \in \mathcal{X}$ , contradicting the maximality of  $(Z, \beta)$ .

Thus,  $Z = Y$ , and we have the extension we wanted.  $\square$

**Corollary 24.9.** If  $I$  is an injective  $\mathbb{Z}$ -module and  $M \subset I$  is a submodule then  $I/M$  is injective.

This is because divisibility of  $I$  is preserved under quotients.

**Corollary 24.10.**  $\mathbb{Z}$ -mod has enough injectives.

*Proof.* For every  $\mathbb{Z}$ -module  $M$ , we can construct the exact sequence

$$0 \longrightarrow K \longrightarrow F_{\mathbb{Z}}(M) \longrightarrow M \longrightarrow 0,$$

which means  $M \cong F_{\mathbb{Z}}(M)/K$ . But  $F_{\mathbb{Z}}(M)/K \subset F_{\mathbb{Q}}(M)/K$ , which is divisible and therefore injective. Thus,  $M$  is contained in an injective, as we wanted.  $\square$

**Lemma 24.11.**

1. If  $I$  is an injective  $\mathbb{Z}$ -module then  $\text{Hom}_{\mathbb{Z}}(R, I)$  (which is an  $R$ -module when  $R$  acts via  $(af)(b) = f(ab)$ ) is an injective  $R$ -module.
2. Then, for any  $R$ ,  $R\text{-Mod}$  has enough injectives.

We will not prove this formally, but the idea is that  $\text{Hom}_{\mathbb{Z}}(R, I)$  is right adjoint to the forgetful functor, and right adjoints preserve injectives. Then, for the second part, we know there exists some injective  $I$  such that  $M \hookrightarrow I$  as  $\mathbb{Z}$ -modules, and then  $M \hookrightarrow \text{Hom}_{\mathbb{Z}}(R, I)$  as  $R$ -modules.

**LECTURE 25: MAPS BETWEEN COMPLEXES**

**Definition 25.1.** If we have the complexes

$$\dots \longrightarrow C^{i-1} \longrightarrow C^i \longrightarrow C^{i+1} \longrightarrow \dots$$

and

$$\dots \longrightarrow D^{i-1} \longrightarrow D^i \longrightarrow D^{i+1} \longrightarrow \dots$$

then we say that a **chain map** or **map of complexes**  $f^\bullet : I^\bullet \rightarrow J^\bullet$  is a collection of maps

$$\begin{array}{ccccccc} \dots & \longrightarrow & C^{i-1} & \longrightarrow & C^i & \longrightarrow & C^{i+1} & \longrightarrow & \dots \\ & & \downarrow f^{i-1} & & \downarrow f^i & & \downarrow f^{i+1} & & \\ \dots & \longrightarrow & D^{i-1} & \longrightarrow & D^i & \longrightarrow & D^{i+1} & \longrightarrow & \dots \end{array}$$

**Definition 25.2.** If  $f^\bullet, g^\bullet : C^\bullet \rightarrow D^\bullet$  are maps of complexes, we say that they are **homotopic** if there exist maps  $k^i : C^{i+1} \rightarrow D^i$  with

$$f^i - g^i = \partial_D^{i-1} \circ k^{i-1} + k^i \circ \partial_C^i.$$

This gives us the commutative diagram

$$\begin{array}{ccccccc} \dots & \longrightarrow & C^{i-1} & \xrightarrow{\partial_C^{i-1}} & C^i & \xrightarrow{\partial_C^i} & C^{i+1} & \longrightarrow & \dots \\ & & \downarrow f^{i-1} - g^{i-1} & \swarrow k^{i-1} & \downarrow f^i - g^i & \swarrow k^i & \downarrow f^{i+1} - g^{i+1} & & \\ \dots & \longrightarrow & D^{i-1} & \xrightarrow{\partial_D^{i-1}} & D^i & \xrightarrow{\partial_D^i} & D^{i+1} & \longrightarrow & \dots \end{array}$$

If two maps of complexes are homotopic, we denote this  $f^\bullet \cong g^\bullet$ .

**Lemma 25.3.** Suppose  $\mathcal{C}$  is an abelian category with enough injectives. If  $f : X \rightarrow Y$  is a morphism in  $\mathcal{C}$  and  $X$  and  $Y$  have the injective resolutions

$$\begin{array}{ccccccc} 0 & \longrightarrow & X & \longrightarrow & I^0 & \longrightarrow & I^1 & \longrightarrow & \dots \\ & & & & & & & & \\ 0 & \longrightarrow & Y & \longrightarrow & J^0 & \longrightarrow & J^1 & \longrightarrow & \dots \end{array}$$

then there exists a chain map  $f^\bullet : I^\bullet \rightarrow J^\bullet$ , and  $f^\bullet$  is unique up to homotopy.

*Proof.* We can prove the existence of  $f^\bullet$  inductively. First, we can see that we have the maps

$$\begin{array}{ccccccc} 0 & \longrightarrow & X & \longrightarrow & I^0 & \longrightarrow & \dots \\ & & \downarrow f & & & & \\ 0 & \longrightarrow & Y & \longrightarrow & J^0 & \longrightarrow & \dots \end{array}$$



and since  $J^0$  is injective, this induces a map  $f^0 : I^0 \rightarrow J^0$ , so that we get this diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & X & \longrightarrow & I^0 & \longrightarrow & \dots \\ & & \downarrow f & & \downarrow f^0 & & \\ 0 & \longrightarrow & Y & \longrightarrow & J^0 & \longrightarrow & \dots \end{array}$$

Then, we will show that if we have the maps  $f^{i-1}$  and  $f^i$ , we can construct  $f^{i+1}$ . We have maps of the form

$$\begin{array}{ccccccc} & & & & \text{coker } \partial_I^{i-1} & & \\ & & & & \swarrow & & \searrow \\ \dots & \longrightarrow & I^{i-1} & \xrightarrow{\partial_I^{i-1}} & I^i & & I^{i+1} \longrightarrow \dots \\ & & \downarrow f^{i-1} & & \downarrow f^i & & \\ \dots & \longrightarrow & J^{i-1} & \longrightarrow & J^i & \longrightarrow & J^{i+1} \longrightarrow \dots \end{array}$$

Since this diagram commutes, we can see that  $I^{i-1} \rightarrow I^i \rightarrow J^i \rightarrow J^{i+1}$  is the same as  $I^{i-1} \rightarrow J^{i-1} \rightarrow J^i \rightarrow J^{i+1}$ . But since this complex is exact, we know that  $J^{i-1} \rightarrow J^i \rightarrow J^{i+1}$  is just the zero map, so  $I^{i-1} \rightarrow I^i \rightarrow J^i$  is also the zero map, and the universal property of the quotient gives us an induced map  $\text{coker } \partial_I^{i-1} \rightarrow J^{i+1}$ . Then, since  $J^{i+1}$  is injective, we get our desired  $f^{i+1}$ , so we have the map

$$\begin{array}{ccccccc} & & & & \text{coker } \partial_I^{i-1} & & \\ & & & & \swarrow & & \searrow \\ \dots & \longrightarrow & I^{i-1} & \xrightarrow{\partial_I^{i-1}} & I^i & & I^{i+1} \longrightarrow \dots \\ & & \downarrow f^{i-1} & & \downarrow f^i & & \downarrow f^{i+1} \\ \dots & \longrightarrow & J^{i-1} & \longrightarrow & J^i & \longrightarrow & J^{i+1} \longrightarrow \dots \end{array}$$

and thus, inductively, we get the map of complexes  $f^\bullet$ .

Now, we need to show that  $f^\bullet$  is unique up to homotopy. Specifically, if we have two such chain maps  $f^\bullet, g^\bullet$ , we will show via induction that they are homotopic. Subtracting these two gives us the complex starting with

$$\begin{array}{ccccccc} 0 & \longrightarrow & X & \longrightarrow & I^0 & \longrightarrow & \dots \\ & & \downarrow 0 & & \downarrow f^0 - g^0 & & \\ 0 & \longrightarrow & Y & \longrightarrow & J^0 & \longrightarrow & \dots \end{array}$$

But then, we we did before, we note that  $X \rightarrow I^0 \rightarrow J^0 = X \rightarrow Y \rightarrow J^0 = 0$ , so the universal property of the quotient gives us an induced map  $I^0/X \rightarrow J^0$ , and then since  $J^0$  is injective, this gives us an induced map  $k^0 : I^1 \rightarrow J^0$  that makes the diagram commute:

$$\begin{array}{ccccccc} 0 & \longrightarrow & X & \longrightarrow & I^0 & \xrightarrow{\partial_I^0} & I^1 \longrightarrow \dots \\ & & \downarrow 0 & & \downarrow f^0 - g^0 & & \downarrow k^0 \\ 0 & \longrightarrow & Y & \longrightarrow & J^0 & \longrightarrow & \dots \end{array}$$

and  $f^0 - g^0 = k^0 \circ \partial_I^0$ , as we desired.

For the inductive step, if we already have

$$\begin{array}{ccccccc} \dots & \longrightarrow & I^{i-1} & \xrightarrow{\partial_I^{i-1}} & I^i & \longrightarrow & I^{i+1} \longrightarrow \dots \\ & & \downarrow f^{i-1} - g^{i-1} & & \downarrow f^i - g^i & & \\ \dots & \longrightarrow & J^{i-1} & \xrightarrow{\partial_J^{i-1}} & J^i & \longrightarrow & J^{i+1} \longrightarrow \dots \end{array}$$

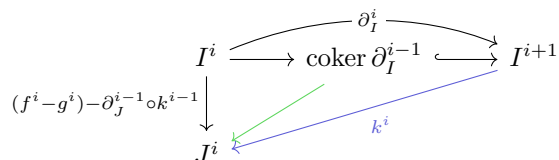
then we can consider the map  $f^i - g^i - \partial_J^{i-1} \circ k^{i-1} : I^i \rightarrow J^i$ . Following the commutative diagram above, we can see that  $(f^i - g^i) \circ \partial_I^{i-1} = \partial_J^{i-1} \circ (f^{i-1} - g^{i-1})$ . Thus,

$$(f^i - g^i - \partial_J^{i-1} \circ k^{i-1}) \circ \partial_I^{i-1} = \partial_J^{i-1} \circ (f^{i-1} - g^{i-1} - k^{i-1} \circ \partial_I^{i-1}).$$

But our inductive assumption says that  $f^{i-1} - g^{i-1} = k^{i-1} \circ \partial_I^{i-1} + \partial_J^{i-2} \circ k^{i-2}$ . So

$$(f^i - g^i - \partial_J^{i-1} \circ k^{i-1}) \circ \partial_I^{i-1} = \partial_J^{i-1} \circ \partial_J^{i-2} \circ k^{i-2} = 0$$

by exactness of this sequence. Now, as before, we can apply the universal property of the quotient and then use injectivity to get the induced maps



and thus  $f^i - g^i - \partial_J^{i-1} \circ k^{i-1} = k^{i-1} \circ \partial_I^i$ , as we desired.

Thus, by induction,  $f^\bullet$  and  $g^\bullet$  are homotopic. □

**Corollary 25.4.** If we have two distinct injective resolutions  $0 \rightarrow X \rightarrow I^\bullet$  and  $0 \rightarrow X \rightarrow J^\bullet$ , then there exists  $f^\bullet : I^\bullet \rightarrow J^\bullet$  extending  $\text{id}_X$  which is unique up to homotopy, and there exists  $g^\bullet : J^\bullet \rightarrow I^\bullet$  extending  $\text{id}_X$  which is unique up to homotopy.

Note that this implies  $g^\bullet \circ f^\bullet$  is a chain map  $I^\bullet \rightarrow I^\bullet$  extending  $\text{id}_X$ , and  $g^\bullet \circ f^\bullet \cong \text{id}_{I^\bullet}$ . Similarly,  $f^\bullet \circ g^\bullet \cong \text{id}_{J^\bullet}$ .

**Definition 25.5.** We say that two injective resolutions  $I^\bullet$  and  $J^\bullet$  are **homotopic** if there exists  $f^\bullet : I^\bullet \rightarrow J^\bullet$  and  $g^\bullet : J^\bullet \rightarrow I^\bullet$  such that  $f^\bullet \circ g^\bullet \cong \text{id}_{J^\bullet}$  and  $g^\bullet \circ f^\bullet \cong \text{id}_{I^\bullet}$ .

**Definition 25.6.** Suppose  $C^\bullet$  is a chain complex. We say that the  $i^{\text{th}}$  **cohomology** of  $C^\bullet$  is

$$H^i(C^\bullet) = \ker \partial_C^i / \text{im } \partial_C^{i-1}.$$

**Example 25.7.** Consider an injective resolution

$$0 \rightarrow X \rightarrow I^0 \rightarrow I^1 \rightarrow \dots$$

Then,  $H^0(I^\bullet) = X$ , and for all  $i \geq 1$ ,  $H^i(I^\bullet) = 0$ , since  $I$  is exact.

**Remark 25.8.** If  $f^\bullet : C^\bullet \rightarrow D^\bullet$  is a map of complexes, then we get the induced maps

$$H^i(f^\bullet) : H^i(C^\bullet) \rightarrow H^i(D^\bullet).$$

This is because we know the diagram

$$\begin{array}{ccccccc} \dots & \longrightarrow & C^{i-1} & \xrightarrow{\partial_C^{i-1}} & C^i & \xrightarrow{\partial_C^i} & C^{i+1} & \longrightarrow & \dots \\ & & \downarrow f^{i-1} & & \downarrow f^i & & \downarrow f^{i+1} & & \\ \dots & \longrightarrow & D^{i-1} & \xrightarrow{\partial_D^{i-1}} & D^i & \xrightarrow{\partial_D^i} & D^{i+1} & \longrightarrow & \dots \end{array}$$

commutes, so  $f^i$  maps  $\text{im } \partial_C^{i-1}$  to  $\text{im } \partial_D^{i-1}$  and it maps  $\ker \partial_C^i$  to  $\ker \partial_D^i$ . Thus, we can construct an induced map  $H^i(C^\bullet) \rightarrow H^i(D^\bullet)$ , as we desired.

**Lemma 25.9.** If  $f^\bullet, g^\bullet : C^\bullet \rightarrow D^\bullet$  are homotopic, then for each  $i$ ,

$$H^i(f^\bullet) = H^i(g^\bullet).$$

We will just show this for chain complexes in  $\mathbf{R}\text{-Mod}$ . Consider any  $x \in \ker \partial_C^i$ . We want to show that  $H^i(f)(x) - H^i(g)(x) = 0 \in H^i(D^\bullet)$ , or  $f^i(x) - g^i(x) \in \text{im } \partial_D^{i-1}$ . But we can see that since  $f^\bullet$  and  $g^\bullet$  are homotopic,

$$\begin{aligned} f^i(x) - g^i(x) &= \partial_D^{i-1} \circ k^{i-1}(x) + k^i \circ \partial_C^i(x) \\ &= \partial_D^{i-1}(k^{i-1}(x)) + 0, \end{aligned}$$

which is clearly in  $\text{im } \partial_D^{i-1}$ , as we wanted.

Thus, cohomology is invariant under homotopy.

**Example 25.10.** Say we have abelian categories  $\mathcal{C}, \mathcal{D}$ , where  $\mathcal{C}$  has enough injectives, and we have the left-exact additive functor  $F : \mathcal{C} \rightarrow \mathcal{D}$ .

Then, for any  $X \in \text{ob}(\mathcal{C})$ , we have an injective resolution  $0 \rightarrow X \rightarrow I^\bullet$ , and  $FI^\bullet$  is a complex in  $\mathcal{D}$  (though not necessarily exact).

We say that the  $i^{\text{th}}$  **right derived functor** of  $F$  is

$$R^i F(X) = H^i(FI^\bullet).$$

We must check that:

- (a)  $R^i F(X)$  is well-defined on objects  $X$ .

If we had two different injective resolutions of  $X$ , then they would be homotopic, so we'd have the maps

$$\begin{array}{ccccc} 0 & \longrightarrow & X & \longrightarrow & I^\bullet \\ & & \text{id}_X \downarrow & & g^\bullet \uparrow \downarrow f^\bullet \\ 0 & \longrightarrow & X & \longrightarrow & J^\bullet \end{array}$$

such that  $f^\bullet \circ g^\bullet \cong \text{id}_{J^\bullet}$  and  $g^\bullet \circ f^\bullet \cong \text{id}_{I^\bullet}$ .

Remember that if  $FI^\bullet$  and  $FJ^\bullet$  were homotopic, then  $H^i(FI^\bullet) = H^i(FJ^\bullet)$ . So what's left is to prove that  $F$  preserves homotopies. That is, we want to show that we have the diagram

$$\begin{array}{ccc} & FI^\bullet & \\ Fg^\bullet \uparrow & & \downarrow Ff^\bullet \\ & FJ^\bullet & \end{array}$$

such that  $Ff^\bullet \circ Fg^\bullet \cong \text{id}_{FJ^\bullet}$  and  $Fg^\bullet \circ Ff^\bullet \cong \text{id}_{FI^\bullet}$ .

Indeed, we can see that if

$$f^i - g^i = \partial_J^{i-1} \circ k^{i-1} + k^i \circ \partial_I^i$$

then since  $F$  is additive,

$$F(f^i) - F(g^i) = F(\partial_J^{i-1}) \circ F(k^{i-1}) + F(k^i) \circ F(\partial_I^i)$$

and therefore  $Ff^\bullet \cong Fg^\bullet$ , as we desired.

Thus,  $R^i F(X)$  is well-defined.

(b)  $R^i F$  is well-defined on morphisms  $f : X \rightarrow Y$ .

If  $I^\bullet$  is our injective resolution of  $X$  and  $J^\bullet$  is our injective resolution of  $Y$ , but we have two chain maps  $f^\bullet, g^\bullet : I^\bullet \rightarrow J^\bullet$  extending  $f$ :

$$\begin{array}{ccccccc} 0 & \longrightarrow & X & \longrightarrow & I^\bullet & & \\ & & f \downarrow & & f^\bullet \downarrow & \left( \downarrow \right) & g^\bullet \\ 0 & \longrightarrow & Y & \longrightarrow & J^\bullet & & \end{array}$$

then as we showed above, since  $f^\bullet \cong g^\bullet$ ,  $Ff^\bullet \cong Fg^\bullet$ , so  $H^i(Ff^\bullet) = H^i(Fg^\bullet)$ , and  $R^i F(f)$  is well-defined.

(c)  $R^i F : \mathcal{C} \rightarrow \mathcal{D}$  is additive.

This is easy to check.

(d)  $R^0 F = F$ .

We can consider the start of the injective resolution

$$0 \longrightarrow X \longrightarrow I^0 \longrightarrow I^1.$$

This is a left-exact sequence, and since  $F$  is left-exact, the image is also a left-exact sequence

$$0 \longrightarrow FX \longrightarrow FI^0 \longrightarrow FI^1,$$

and therefore  $H^0(FI^\bullet) = FX$ .

(e) If  $I$  is injective and  $i > 0$  then  $R^i F(I) = 0$ .

**Example 25.11.** If  $X$  is a topological space, then

$$\begin{array}{ccc} \Gamma : \underline{\text{Sh}}(X) & \longrightarrow & \underline{\text{Ab}} \\ F & \mapsto & F(X) \end{array}$$

is the **global section functor**. Since  $\Gamma$  is left-exact and  $\underline{\text{Sh}}(X)$  has enough injectives, this has the right derived functors

$$R^i \Gamma : \underline{\text{Sh}}(X) \longrightarrow \underline{\text{Ab}}.$$

**Theorem 25.12.** Suppose  $X$  is a second countable topological space where every point has an open neighborhood homeomorphic to an open set in  $\mathbb{R}^n$  (so it is a manifold). Then, for all  $i$ ,

$$R^i \Gamma(\underline{\mathbb{Z}}_X) \cong H_{\text{ring}}^i(X, \mathbb{Z}),$$

where  $\underline{\mathbb{Z}}_X$  is the constant sheaf mapping each  $U \subseteq X$  to  $\mathbb{Z}$ .

LECTURE 26: SEQUENCES OF COMPLEXES

**Proposition 26.1.** Suppose  $\mathcal{C}$  has enough injectives and

$$0 \rightarrow X \rightarrow Y \rightarrow Z \rightarrow 0$$

is short exact. Then, there exist injective resolutions  $0 \rightarrow X \rightarrow I^\bullet$ ,  $0 \rightarrow Y \rightarrow K^\bullet$ , and  $0 \rightarrow Z \rightarrow J^\bullet$  such that there is a commutative diagram

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & X & \longrightarrow & Y & \longrightarrow & Z \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & I^0 & \longrightarrow & K^0 & \longrightarrow & J^0 \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & I^1 & \longrightarrow & K^1 & \longrightarrow & J^1 \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & \vdots & & \vdots & & \vdots \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & I^i & \longrightarrow & K^i & \longrightarrow & J^i \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & \vdots & & \vdots & & \vdots
 \end{array}$$

with exact rows.

More specifically, for any injective resolutions  $0 \rightarrow X \rightarrow I^\bullet$ ,  $0 \rightarrow Z \rightarrow J^\bullet$ , there exists an injective resolution  $0 \rightarrow Y \rightarrow K^\bullet$  that makes the statement true.

*Proof.* Let's say we have injective resolutions  $0 \rightarrow X \rightarrow I^\bullet$ ,  $0 \rightarrow Z \rightarrow J^\bullet$ . We claim that the  $K^\bullet$  that makes this diagram commute is  $K^i = I^i \oplus J^i$ .

We can see that each  $K^i$  is injective because it is the direct sum of two injectives.

Then, we first need to find a map  $J \rightarrow I^0 \oplus J^0$  that makes the diagram

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & X & \xrightarrow{f} & Y & \xrightarrow{g} & Z \longrightarrow 0 \\
 & & \downarrow \partial_I^0 & & \downarrow & & \downarrow \partial_J^0 \\
 0 & \longrightarrow & I^0 & \longrightarrow & I^0 \oplus J^0 & \longrightarrow & J^0 \longrightarrow 0
 \end{array}$$

commute.

*I missed the part of lecture where we construct this part of the map, so I'll fill this in later, but if you have notes for this, please let me know!*

Afterwards, we need to inductively find a map  $I^i \oplus J^i \rightarrow I^{i+1} \oplus J^{i+1}$  such that the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & I^i & \longrightarrow & I^i \oplus J^i & \longrightarrow & J^i \longrightarrow 0 \\ & & \downarrow \partial_I^{i+1} & & \downarrow & & \downarrow \partial_J^{i+1} \\ 0 & \longrightarrow & I^{i+1} & \longrightarrow & I^{i+1} \oplus J^{i+1} & \longrightarrow & J^{i+1} \longrightarrow 0 \end{array}$$

commutes. But we can see that for the square on the right to commute, we need this map to be something of the form

$$(x, y) \mapsto (\partial_J^{i+1} y)$$

and then for the square on the left to commute, we need this map to be something of the form

$$(x, y) \mapsto (\partial_I^{i+1} x + h^{i+1} y, \partial_J^{i+1} y),$$

where  $h^{i+1}$  is some map  $J^i \rightarrow I^{i+1}$ .

So we have found maps between each of these exact sequences that preserve commutativity, but we still have freedom over what our  $h^i$ 's are. This is good, because we still need to ensure that

$$0 \longrightarrow Y \longrightarrow I^0 \oplus J^0 \longrightarrow I^1 \oplus J^1 \longrightarrow \dots$$

is actually an injective resolution.

Since we already said each term in this sequence is an injective, it is sufficient to pick our  $h^i$ 's such that this becomes an exact sequence.

We can first see that, in order for this to be a complex, we need to pick our  $h^i$ 's such that the composition of any two maps is zero. We will leave the case of the  $Y \rightarrow I^0 \oplus J^0 \rightarrow I^1 \oplus J^1$  map as an exercise, and focus on the maps beyond that.

We can see that the composition of any two maps is then

$$(x, y) \mapsto (\partial_I^i x + h^i y, \partial_J^i y) \mapsto (\partial_I^{i+1} h^i y + h^{i+1} \partial_J^i y, 0).$$

Thus, for this to be a complex, we will pick our  $h^i$ 's such that

$$\partial_I^{i+1} h^i y + h^{i+1} \partial_J^i y = 0.$$

But this also makes this an exact sequence! We can see that if  $(x, y) \in I^i \oplus J^i$  maps to  $0 \in I^{i+1} \oplus J^{i+1}$ , then

$$\partial_J^{i+1} y = 0,$$

and since  $J^\bullet$  is an injective resolution, this implies there exists  $y' \in J^{i-1}$  such that  $\partial_J^i y' = y$ . Similarly, we know

$$\partial_I^i x + h^i y = 0,$$

or

$$\partial_I^i x + h^i \partial_J^{i-1} y' = 0,$$

but then by the definition of  $h^i$  we just chose,  $h^i \partial_J^{i-1} y' = -\partial_I^i h^{i-1} y'$ , so

$$\partial_I^i (x - h^{i-1} y') = 0,$$

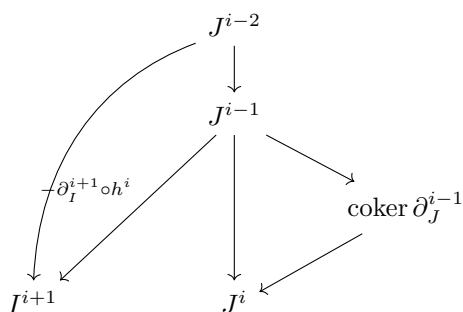
and then by exactness of  $I^\bullet$ , we get that there exists some  $x'$  such that

$$(x, y) = (\partial_I^{i-1} x' + h^{i-1} y', \partial_J^{i-1} y'),$$

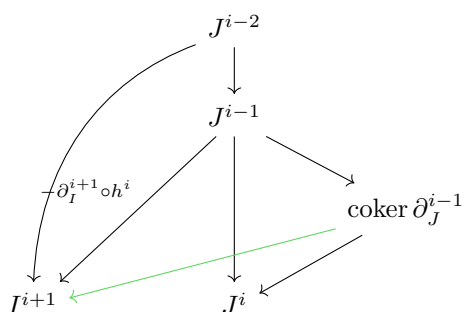
as we desired.

But does there actually exist an  $h^i$  that satisfies this definition?

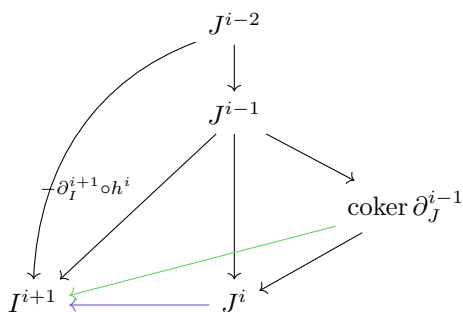
It turns out there does; we can construct it inductively using the same sort construction we used repeatedly last lecture:



induces a map



which induces a map



as we desired. □

Ok, now let's say we have an exact sequence

$$0 \rightarrow X \rightarrow Y \rightarrow Z \rightarrow 0,$$

and then we apply our injective resolution to get the diagram

$$\begin{array}{ccccccc} & & 0 & & 0 & & 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & X & \longrightarrow & Y & \longrightarrow & Z \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & I^\bullet & \longrightarrow & K^\bullet & \longrightarrow & J^\bullet \longrightarrow 0 \end{array}$$

Then, if we have an additive functor  $F$ , we can apply it to this diagram to get

$$0 \rightarrow FI^\bullet \rightarrow FK^\bullet \rightarrow FJ^\bullet \rightarrow 0.$$

Here, the columns are still complexes, but they no longer have to be exact. However, the rows are exact, because additive functors preserve short exact sequences when the first term is an injective.

**Lemma 26.2.** Suppose  $C^\bullet, D^\bullet, E^\bullet$  are complexes that fit the commutative diagram

$$0 \longrightarrow C^\bullet \longrightarrow D^\bullet \longrightarrow E^\bullet \longrightarrow 0,$$

with exact rows.

Then, there is a long exact sequence

$$\cdots \longrightarrow H^i(C^\bullet) \longrightarrow H^i(D^\bullet) \longrightarrow H^i(E^\bullet) \longrightarrow H^{i+1}(C^\bullet) \longrightarrow H^{i+1}(D^\bullet) \longrightarrow \cdots .$$

It should be somewhat clear that  $H^i(C^\bullet) \rightarrow H^i(D^\bullet) \rightarrow H^i(E^\bullet)$  is exact; the unusual part is the  $H^i(E^\bullet) \rightarrow H^{i+1}(C^\bullet)$  map, which we call a **boundary map**.

**Corollary 26.3.** If  $F : \mathcal{C} \rightarrow \mathcal{D}$  is left exact and  $\mathcal{C}$  has enough injectives, and if  $0 \rightarrow X \rightarrow Y \rightarrow Z \rightarrow 0$  is exact in  $\mathcal{C}$ , then

$$0 \longrightarrow R^0FX \longrightarrow R^0FY \longrightarrow R^0FZ \longrightarrow R^1FX \longrightarrow R^1FY \longrightarrow \cdots$$

is long exact.

*Proof of lemma.* We will first show exactness at  $H^i(D)$ . We have the diagram

$$\begin{array}{ccccccc} & & \vdots & & \vdots & & \vdots \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & C^{i-1} & \longrightarrow & D^{i-1} & \longrightarrow & E^{i-1} \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & C^i & \longrightarrow & D^i & \longrightarrow & E^i \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & C^{i+1} & \longrightarrow & D^{i+1} & \longrightarrow & E^{i+1} \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ & & \vdots & & \vdots & & \vdots \end{array}$$

Then, for any  $d + \text{im } \partial_D^{i-1} \in H^i(D^\bullet)$  such that  $g^i(d) = \partial_E^{i-1}(e)$ , we want  $d + \text{im } \partial_D^{i-1}$  to equal  $f^i(c)$  for some  $c \in \ker \partial_C^i$ .

Indeed, we can see that since our rows are exact, there must be some  $d' \in D^{i-1}$  such that

$$\partial_E^{i-1}(e) = \partial_E^{i-1}(g^{i-1}(d')) = g^i(\partial_D^{i-1}(d')).$$

But this means that  $g^i(d - \partial_D^{i-1}d') = 0$ , so by exactness of the rows, there must exist some  $c \in C^i$  such that

$$d - \partial_D^{i-1}d' = f^i(c).$$

Now, we want to show that  $c \in \ker \partial_C^i$ . Indeed, we can see that

$$f^{i+1}(\partial_C^i(c)) = \partial_D^i(f^i(c)) = \partial_D^i(d) - \partial_D^i(\partial_D^{i-1}(d')) = 0,$$

since  $d \in \ker \partial_D^i$ . But since  $f^{i+1}$  is injective,  $f^{i+1}(\partial_C^i(c)) = 0$  implies that  $\partial_C^i(c) = 0$ , so this sequence is exact at  $H^i(D^\bullet)$ , as we desired.

Showing exactness at  $H^i(C^\bullet)$  and  $H^i(E^\bullet)$  is harder, because we need to define the boundary maps. We will do this at the start of next lecture.  $\square$



## LECTURE 27: SEQUENCES OF COMPLEXES, II

We begin by continuing our proof from last lecture.

*Proof, cont'd.* Last time, we showed that our induced sequence was exact at  $H^i(D^\bullet)$ . We will now define our boundary map  $H^i(E^\bullet) \rightarrow H^{i+1}(C^\bullet)$  so that we can show exactness at  $H^i(E^\bullet)$  and  $H^i(C^\bullet)$ .

We will focus on this part of the commutative diagram:

$$\begin{array}{ccccccc}
 & & & D^{i-1} & \xrightarrow{g^{i-1}} & E^{i-1} & \\
 & & & \downarrow \partial_D^{i-1} & & \downarrow \partial_E^{i-1} & \\
 0 & \longrightarrow & C^i & \xrightarrow{f^i} & D^i & \xrightarrow{g^i} & E^i \longrightarrow 0 \\
 & & \downarrow \partial_C^i & & \downarrow \partial_D^i & & \downarrow \partial_E^i \\
 0 & \longrightarrow & C^{i+1} & \xrightarrow{f^{i+1}} & D^{i+1} & \xrightarrow{g^{i+1}} & E^{i+1} \longrightarrow 0 \\
 & & \downarrow \partial_C^{i+1} & & \downarrow \partial_D^{i+1} & & \\
 0 & \longrightarrow & C^{i+2} & \xrightarrow{f^{i+2}} & D^{i+2} & & 
 \end{array}$$

where we note that the rows are exact but the columns are (not necessarily exact) complexes.

Consider an arbitrary element in  $H^i(E^\bullet)$ . That is, consider some  $e + \text{im } \partial_E^{i-1}$ , where  $e \in \ker \partial_E^i$ . Then, since  $g^i$  is surjective, there exists some  $d \in D^i$  such that  $g^i d = e$ . Moreover, we can see that since this is a commutative, diagram,

$$g^{i+1} \partial_D^i d = \partial_E^i g^i d = \partial_E^i e = 0.$$

So  $\partial_D^i d \in \ker g^{i+1} = \text{im } f^{i+1}$ , so there exists some  $c \in C^{i+1}$  such that  $f^{i+1} c = \partial_D^i d$ . We want  $c$  to be an element of  $\ker \partial_C^{i+1}$ . Indeed, we can see that

$$f^{i+2} \partial_C^{i+1} c = \partial_D^{i+1} f^{i+1} c = \partial_D^{i+1} \partial_D^i d = 0,$$

and since  $f^{i+2}$  is injective, this implies  $\partial_C^{i+1} c = 0$ , as we desired.

Thus, our boundary map is the function  $e + \text{im } \partial_E^{i-1} \mapsto c + \text{im } \partial_C^i$ .

We need to first check that this is well defined.

Consider some

$$e' + \text{im } \partial_E^{i-1} = e + \text{im } \partial_E^{i-1}.$$

This implies that  $e' - e \in \text{im } \partial_E^{i-1}$ , so there exists some  $e'' \in E^{i-1}$  such that  $e' - e = \partial_E^{i-1} e''$ .

Then, by surjectivity of  $g^i$  and  $g^{i-1}$ , we know there exist  $d, d', d''$  such that:

$$\begin{aligned}
 g^i d &= e \\
 g^i d' &= e' \\
 g^{i-1} d'' &= e''.
 \end{aligned}$$

As before, we note that  $\partial_D^i d, \partial_D^i d' \in \ker g^{i+1} = \text{im } f^{i+1}$ , so there exists  $c, c' \in C^{i+1}$  such that  $f^{i+1}c = d$ ,  $f^{i+1}c' = d'$ . We can show, moreover, that  $c, c' \in \ker \partial_C^{i+1}$ .

Then,  $c + \text{im } \partial_C^i$  is the image of  $e + \text{im } \partial_E^{i-1}$  and  $c' + \text{im } \partial_C^i$  is the image of  $e' + \text{im } \partial_E^{i-1}$ . Thus, we want to show that these are equal; that is,  $c' - c \in \text{im } \partial_C^i$ .

But we can see that, indeed,

$$e' - e = \partial_E^{i-1} g^{i-1} d'' = g^i \partial_D^{i-1} d''.$$

This implies that

$$g^i(d' - d - \partial_D^{i-1} d'') = e' - e - (e' - e) = 0,$$

so this is in  $\ker g^i = \text{im } f^i$ , and there exists some  $c''$  such that  $f^i c'' = d' - d - \partial_D^{i-1} d''$ . This implies that

$$f^{i+1} \partial_C^i c'' = \partial_D^i f^i c'' = \partial_D^i d' - \partial_D^i d - \partial_D^i \partial_D^{i-1} d'' = f^{i+1} c' - f^{i+1} c.$$

But since  $f^{i+1}$  is injective, this implies that

$$c' - c = \partial_C^i c'',$$

so  $c' - c \in \text{im } \partial_C^i$ , and this boundary map is well-defined, as we desired.

Now that we have a well-defined boundary map, we can show that this map is exact at  $H^i(E^\bullet)$ .

First, we will show that

$$H^i(D^\bullet) \longrightarrow H^i(E^\bullet) \longrightarrow H^{i+1}(C^\bullet)$$

is the zero map. We can see that, for any  $d \in \ker \partial_D^i$ , we map  $d + \text{im } \partial_E^{i-1}$  to  $g^i(d) + \text{im } \partial_E^{i-1}$ . Then, the boundary map takes  $g^i(d) + \text{im } \partial_E^{i-1}$ , maps this back to  $d$ , and then maps this to some  $c + \text{im } \partial_C^i \in H^i(C^\bullet)$  such that  $f^{i+1}c = \partial_D^i d$ . But since  $d \in \ker \partial_D^i$ , this implies  $f^{i+1}c = 0$ , and since  $f^{i+1}$  is injective, this implies  $c = 0$ , as we desired.

Then, we will show that this is exact. Consider any  $e + \text{im } \partial_E^{i-1}$  which maps to  $0 \in H^{i+1}(C^\bullet)$ . We want this to be the image of an element of  $H^i(D^\bullet)$ . By our definition of the boundary map, this means there exists some  $d \in D^i$  such that  $g^i d = e$ , and then some  $c \in \text{im } \partial_C^i$  such that  $f^{i+1}c = \partial_D^i d$ . But this means that there exists  $c' \in C^i$  such that  $\partial_C^i c' = c$ , and then we can see that

$$\partial_D^i(d - f^i c') = \partial_D^i d - f^{i+1} c = 0,$$

so  $d - f^i c' \in \ker \partial_D^i$ , and this is an element of  $H^i(D^\bullet)$  whose image under  $g^i$  is  $e + \text{im } \partial_E^{i-1}$ .

Showing that this sequence is also exact at  $H^i(C^\bullet)$  is a very similar process, so we will leave this as an exercise.  $\square$

(Note that the everything we are proving about sequences of complexes also holds in general abelian categories, but we are just proving them for  $R$ -modules because it is a lot easier notationally to describe morphisms of  $R$ -modules.)

**Lemma 27.1.** Suppose we have a commutative diagram of complexes:

$$\begin{array}{ccccccc} 0 & \longrightarrow & C^\bullet & \longrightarrow & D^\bullet & \longrightarrow & E^\bullet & \longrightarrow & 0 \\ & & f^\bullet \downarrow & & g^\bullet \downarrow & & h^\bullet \downarrow & & \\ 0 & \longrightarrow & C'^\bullet & \longrightarrow & D'^\bullet & \longrightarrow & E'^\bullet & \longrightarrow & 0 \end{array}$$

where the rows are exact. Then, we get a commutative diagram

$$\begin{array}{ccccccc} \cdots & \longrightarrow & H^i(C^\bullet) & \longrightarrow & H^i(D^\bullet) & \longrightarrow & H^i(E^\bullet) & \longrightarrow & H^{i+1}(C^\bullet) & \longrightarrow & \cdots \\ & & H^i(f^\bullet) \downarrow & & H^i(g^\bullet) \downarrow & & H^i(h^\bullet) \downarrow & & H^{i+1}(f^\bullet) \downarrow & & \\ \cdots & \longrightarrow & H^i(C'^\bullet) & \longrightarrow & H^i(D'^\bullet) & \longrightarrow & H^i(E'^\bullet) & \longrightarrow & H^{i+1}(C'^\bullet) & \longrightarrow & \cdots \end{array}$$

where the rows are still exact.

The proof of this lemma is very similar to the previous lemma; we will skip it in the interest of time. The fact that the square

$$\begin{array}{ccccc} H^i(C^\bullet) & \longrightarrow & H^i(D^\bullet) & \longrightarrow & H^i(E^\bullet) \\ H^i(f^\bullet) \downarrow & & H^i(g^\bullet) \downarrow & & H^i(h^\bullet) \downarrow \\ H^i(C'^\bullet) & \longrightarrow & H^i(D'^\bullet) & \longrightarrow & H^i(E'^\bullet) \end{array}$$

commutes should just follow from definitions, so the difficult part is just showing commutativity with the boundary maps.

**Lemma 27.2.** Suppose we have abelian categories  $\mathcal{C}, \mathcal{D}$ , and a left exact additive functor  $F : \mathcal{C} \rightarrow \mathcal{D}$ . Suppose moreover that  $\mathcal{C}$  has enough injectives. Then, if

$$\begin{array}{ccccccc} 0 & \longrightarrow & X & \longrightarrow & Y & \longrightarrow & Z & \longrightarrow & 0 \\ & & f \downarrow & & g \downarrow & & h \downarrow & & \\ 0 & \longrightarrow & X' & \longrightarrow & Y' & \longrightarrow & Z' & \longrightarrow & 0 \end{array}$$

is a commutative diagram in  $\mathcal{C}$  with exact rows, then

$$\begin{array}{ccccccc} 0 & \longrightarrow & R^0FX & \longrightarrow & R^0FY & \longrightarrow & R^0FZ & \longrightarrow & R^1FX & \longrightarrow & \cdots \\ & & R^0Ff \downarrow & & R^0Fg \downarrow & & R^0Fh \downarrow & & R^1Ff \downarrow & & \\ 0 & \longrightarrow & R^0FX' & \longrightarrow & R^0FY' & \longrightarrow & R^0FZ' & \longrightarrow & R^1FX' & \longrightarrow & \cdots \end{array}$$

also commutes.

*Proof sketch.* Recall that  $R^iFX$  is the  $i^{\text{th}}$  right derived functor of  $F$ , and it equals  $H^i(FI^\bullet)$ , where  $I^\bullet$  is an injective resolution of  $X$ .

Recall that [Proposition 26.1](#) gives us a commutative diagram of injective resolutions

$$\begin{array}{ccccccc} 0 & \longrightarrow & X & \longrightarrow & Y & \longrightarrow & Z & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & I^\bullet & \longrightarrow & I^\bullet \oplus J^\bullet & \longrightarrow & J^\bullet & \longrightarrow & 0 \end{array}$$

with exact rows. Then,

$$0 \longrightarrow FI^\bullet \longrightarrow FI^\bullet \oplus FJ^\bullet \longrightarrow FJ^\bullet \longrightarrow 0$$

is still an exact sequence, since additive functors preserve exact sequences that start with injectives. We similarly construct

$$0 \longrightarrow I'^\bullet \longrightarrow I'^\bullet \oplus J'^\bullet \longrightarrow J'^\bullet \longrightarrow 0$$

and the induced exact sequence

$$0 \longrightarrow FI'^\bullet \longrightarrow FI'^\bullet \oplus FJ'^\bullet \longrightarrow FJ'^\bullet \longrightarrow 0.$$

Then, the map  $f : X \rightarrow X'$  induces a map  $f^\bullet : I^\bullet \rightarrow I'^\bullet$ , and the map  $h : Z \rightarrow Z'$  induces a map  $h^\bullet : J^\bullet \rightarrow J'^\bullet$ . Thus, we have the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I^\bullet & \longrightarrow & I^\bullet \oplus J^\bullet & \longrightarrow & J^\bullet & \longrightarrow & 0 \\ & & f^\bullet \downarrow & & & & h^\bullet \downarrow & & \\ 0 & \longrightarrow & I'^\bullet & \longrightarrow & I'^\bullet \oplus J'^\bullet & \longrightarrow & J'^\bullet & \longrightarrow & 0 \end{array}$$

What remains is to define a map  $I^\bullet \oplus J^\bullet \rightarrow I'^\bullet \oplus J'^\bullet$  which makes the diagram commute; from there, we can apply the previous lemma to get our desired result.  $\square$

A lot of our work so far has been in terms of turning these short exact sequences of complexes into long exact sequences of objects: we will generalize this now.

**Definition 27.3.** If  $\mathcal{C}$  and  $\mathcal{D}$  are abelian categories, then a  $\delta$ -functor (**delta-functor**)  $\mathcal{C} \rightarrow \mathcal{D}$  is a sequence of functors  $S^0, S^1, \dots : \mathcal{C} \rightarrow \mathcal{D}$  such that:

1. For each short exact sequence

$$0 \longrightarrow X \longrightarrow Y \longrightarrow Z \longrightarrow 0$$

in  $\mathcal{C}$ , there exist morphisms  $\delta^i : S^i Z \rightarrow S^{i+1} X$  such that

$$0 \longrightarrow S^0 X \longrightarrow S^0 Y \longrightarrow S^0 Z \xrightarrow{\delta^0} S^1 X \longrightarrow \dots$$

is long exact.

2. For any commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X & \longrightarrow & Y & \longrightarrow & Z & \longrightarrow & 0 \\ & & f \downarrow & & g \downarrow & & h \downarrow & & \\ 0 & \longrightarrow & X' & \longrightarrow & Y' & \longrightarrow & Z' & \longrightarrow & 0 \end{array}$$

with exact rows, the diagram

$$\begin{array}{ccc} S^i Z & \xrightarrow{\delta^i} & S^{i+1} X \\ S^i h \downarrow & & S^{i+1} f \downarrow \\ S^i Z' & \xrightarrow{\delta^i} & S^{i+1} X \end{array}$$

commutes.

(This property is known as **functoriality**.)

**Definition 27.4.** We say that a  $\delta$  functor is a **universal  $\delta$ -functor** if for any other delta functor  $\{T\}$  and natural transformation  $\phi^0 : S^0 \rightarrow T^0$ , there exist unique natural transformations  $\phi^i : S^i \rightarrow T^i$  for all  $i$ , such that for any short exact sequence

$$0 \longrightarrow X \longrightarrow Y \longrightarrow Z \longrightarrow 0$$

in  $\mathcal{C}$ , the diagram

$$\begin{array}{ccc} S^i Z & \xrightarrow{\delta_S^i} & S^{i+1} X \\ \phi_Z^i \downarrow & & \downarrow \phi_X^i \\ T^i Z & \xrightarrow{\delta_T^i} & T^{i+1} X \end{array}$$

commutes.

## LECTURE 28: RIGHT DERIVED FUNCTORS

We left off last lecture defining universal  $\delta$ -functors. We have the following lemma:

**Lemma 28.1.** For any left-exact additive functor  $F$ ,  $\{R^i F\}$  is a universal  $\delta$ -functor.

*Proof.* We have some other  $\delta$ -functor  $\{S_i\}$  and a natural transformation  $\phi^0 : R^0 F = F \rightarrow S^0$ .

We want to inductively create each  $\phi^i$ , prove that it is a natural transformation, and show that it is compatible with boundary maps.

Recall that a natural transformation is a morphism  $\phi_X^i : R^i F X \rightarrow S^i X$ , for each  $X \in \text{ob}(\mathcal{C})$ . Let's consider an arbitrary such  $X$ . We know that there exists an exact sequence

$$0 \longrightarrow X \longrightarrow I \longrightarrow Q \longrightarrow 0,$$

where  $I$  is injective, and  $Q$  is the cokernel of the map  $X \rightarrow I$ .

Then, by our inductive hypothesis, we have natural transformations  $\phi_I^{i-1}$  and  $\phi_Q^{i-1}$  which make the diagram

$$\begin{array}{ccc} R^{i-1}FI & \longrightarrow & R^{i-1}FQ \\ \phi_I^{i-1} \downarrow & & \phi_Q^{i-1} \downarrow \\ S^{i-1}I & \longrightarrow & S^{i-1}Q \end{array}$$

commute.

Then, we define  $\phi_X^i$  to be the induced map that makes the diagram

$$\begin{array}{ccccc} R^{i-1}FI & \longrightarrow & R^{i-1}FQ & \longrightarrow & R^{i-1}FX \\ \phi_I^{i-1} \downarrow & & \phi_Q^{i-1} \downarrow & & \phi_X^i \downarrow \\ S^{i-1}I & \longrightarrow & S^{i-1}Q & \longrightarrow & S^i X \end{array}$$

commute; since  $R^{i-1}FQ \rightarrow R^{i-1}FX$  is surjective, the existence of  $\phi_X^i$  follows from the universal property of the quotient.

Now, we need to show that this  $\phi_X^i$  is independent of our choice of  $I$ , is a natural transformation, and it is compatible with the general boundary map.

Let's say we have some morphism  $f : X \rightarrow Y$ ; this induces the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & X & \longrightarrow & I & \longrightarrow & Q \longrightarrow 0 \\ & & f \downarrow & & g \downarrow & & h \downarrow \\ 0 & \longrightarrow & Y & \longrightarrow & J & \longrightarrow & Q' \longrightarrow 0 \end{array}$$

where  $I$  and  $J$  are injectives. Here, we know there exists an induced  $g$  since  $I$  is injective, and then there exists an induced  $h$  by universal property of the quotient.

Then, to show the naturality of  $\phi^i$ , we can start with the diagram

$$\begin{array}{ccc}
 R^{i-1}FQ & \xrightarrow{R^{i-1}Fh} & R^{i-1}FQ' \\
 \downarrow \phi_Q^{i-1} & & \downarrow \phi_{Q'}^{i-1} \\
 S^{i-1}Q & \xrightarrow{S^{i-1}h} & S^{i-1}Q'
 \end{array}$$

Then, we note that since these are both  $\delta$ -functors, we can add in the  $\delta$  maps induced from the short exact sequence to get

$$\begin{array}{ccc}
 R^iFX & \xrightarrow{R^iFf} & R^iFY \\
 \swarrow & & \searrow \\
 R^{i-1}FQ & \xrightarrow{R^{i-1}Fh} & R^{i-1}FQ' \\
 \downarrow \phi_Q^{i-1} & & \downarrow \phi_{Q'}^{i-1} \\
 S^{i-1}Q & \xrightarrow{S^{i-1}h} & S^{i-1}Q' \\
 \swarrow & & \searrow \\
 S^iX & \xrightarrow{S^if} & S^iY
 \end{array}$$

Then, by the way we defined the  $\phi_X^i$ 's, we know they commute with the  $\delta$  maps, so we get the diagram

$$\begin{array}{ccc}
 R^iFX & \xrightarrow{R^iFf} & R^iFY \\
 \swarrow & & \searrow \\
 R^{i-1}FQ & \xrightarrow{R^{i-1}Fh} & R^{i-1}FQ' \\
 \downarrow \phi_Q^{i-1} & & \downarrow \phi_{Q'}^{i-1} \\
 S^{i-1}Q & \xrightarrow{S^{i-1}h} & S^{i-1}Q' \\
 \swarrow & & \searrow \\
 S^iX & \xrightarrow{S^if} & S^iY
 \end{array}$$

$\phi_{X,I}^i$  (left vertical arrow)       $\phi_{Y,J}^i$  (right vertical arrow)

where the outer square show that  $\phi^i$  is a natural transformation. Moreover, we can see that by taking  $Y = X$  and  $f = \text{id}_X$ , we have shown that  $\phi_X^i$  is independent of our choice of  $I$ .

Finally, we need to show that  $\phi^i$  commutes with boundary maps. As before, we can extend any short exact sequence to

$$\begin{array}{ccccccc}
 0 & \longrightarrow & X & \longrightarrow & Y & \longrightarrow & Z & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 0 & \longrightarrow & X & \longrightarrow & I & \longrightarrow & Q & \longrightarrow & 0
 \end{array}$$

where the  $X \rightarrow X$  map is just the identity, the  $Y \rightarrow I$  map is induced by the fact that  $I$  is an injective, and the  $Z \rightarrow Q$  map is induced by the universal property of the quotient.

Again, we will start with the commutative diagram

$$\begin{array}{ccc}
 R^{i-1}FQ & \longrightarrow & R^iFX \\
 \phi_Q^{i-1} \downarrow & & \downarrow \phi_X^i \\
 S^{i-1}Q & \longrightarrow & S^iX
 \end{array}$$

and then extend it into

$$\begin{array}{ccccc}
 R^{i-1}FZ & \xrightarrow{\hspace{10em}} & R^iFX & & \\
 \downarrow \phi_Z^{i-1} & \searrow & \swarrow \text{id} & & \downarrow \phi_X^i \\
 & R^{i-1}FQ & \longrightarrow & R^iFX & \\
 & \downarrow \phi_Q^{i-1} & & \downarrow \phi_X^i & \\
 & S^{i-1}Q & \longrightarrow & S^iX & \\
 S^{i-1}Z & \xrightarrow{\hspace{10em}} & S^iX & & \\
 & \nearrow & \swarrow \text{id} & & \\
 & & & & 
 \end{array}$$

where the green arrows follow from naturality of the  $\phi^i$ 's, and the purple arrows follow from the fact that these are  $\delta$ -functors. We leave the details of the diagram chasing as an exercise.

Thus, we have inductively shown that  $\phi^i$  has all our desired properties, so  $R^iF$  is a universal  $\delta$ -functor.  $\square$

**Definition 28.2.** We say that  $X \in \text{ob}(\mathcal{C})$  is **acyclic** if  $R^iFX = 0$  for all  $i > 0$ .

**Example 28.3.** All injectives are acyclic.

*(I'm missing a lemma about acyclics here because I'm not entirely sure what the statement of the lemma is, and I don't want to include incorrect information)*

**Definition 28.4.** Recall that in any abelian category  $\mathcal{C}$ , the functor

$$\text{Hom}_{\mathcal{C}}(X, -) : \mathcal{C} \longrightarrow \underline{\text{Ab}}$$

is a covariant left-exact functor.

If  $\mathcal{C}$  has enough injectives, we say that  $\overline{\text{Ext}}_{\mathcal{C}}^i(X, -)$  is the  $\delta$ -functor

$$\overline{\text{Ext}}_{\mathcal{C}}^i(X, -) = R^i \text{Hom}_{\mathcal{C}}(X, -) : \mathcal{C} \longrightarrow \underline{\text{Ab}}.$$

Similarly, in any abelian category  $\mathcal{C}$ , the functor

$$\text{Hom}_{\mathcal{C}}(-, Y) : \mathcal{C} \longrightarrow \underline{\text{Ab}}$$

is a contravariant left exact functor, and if  $\mathcal{C}$  has enough projectives, we define  $\text{Ext}_{\mathcal{C}}^i(-, Y)$  to be

$$\text{Ext}_{\mathcal{C}}^i(-, Y) = R^i \text{Hom}_{\mathcal{C}}(-, Y) : \mathcal{C} \longrightarrow \underline{\text{Ab}}.$$



Thus, we can apply  $\overline{\text{Ext}}$  to a short exact sequence

$$0 \longrightarrow Y_1 \longrightarrow Y_2 \longrightarrow Y_3 \longrightarrow 0$$

to get a long exact sequence

$$0 \longrightarrow \text{Hom}(X, Y_1) \longrightarrow \text{Hom}(X, Y_2) \longrightarrow \text{Hom}(X, Y_3) \longrightarrow \overline{\text{Ext}}^1(X, Y_1) \longrightarrow \overline{\text{Ext}}^1(X, Y_2) \longrightarrow \dots$$

and we can apply  $\text{Ext}$  to a short exact sequence

$$0 \longrightarrow X_1 \longrightarrow X_2 \longrightarrow X_3 \longrightarrow 0$$

to get a long exact sequence

$$0 \longrightarrow \text{Hom}(X_3, Y) \longrightarrow \text{Hom}(X_2, Y) \longrightarrow \text{Hom}(X_1, Y) \longrightarrow \text{Ext}^1(X_3, Y) \longrightarrow \dots$$

**Theorem 28.5.** If  $\mathcal{C}$  has enough injectives and enough projectives, then

$$\text{Ext}_{\mathcal{C}}^i(X, Y) \cong \overline{\text{Ext}}_{\mathcal{C}}^i(X, Y).$$

**Lemma 28.6.** The following are equivalent:

1.  $X$  is a projective
2. for all  $Y$ ,  $\text{Ext}^i(X, Y) = 0$  for all  $i > 0$
3. for all  $Y$ ,  $\text{Ext}^1(X, Y) = 0$

*Proof.* We will first show that  $1 \implies 2$ .

Recall that  $\text{Ext}^i(-, Y) = R^i \text{Hom}(-, Y)$ . Moreover, we can see that since  $X$  is projective,

$$\dots \longrightarrow 0 \longrightarrow 0 \longrightarrow X \longrightarrow X \longrightarrow 0$$

is a projective resolution of  $X$ . But then, applying our homomorphism functor gives us

$$\text{Hom}(X, Y) \longrightarrow \text{Hom}(0, Y) \longrightarrow \text{Hom}(0, Y) \longrightarrow \dots,$$

and then we can see that  $\text{Ext}^i(X, Y)$  is  $H^i$  of this complex, which is 0 for all  $i > 0$ .

It is obvious that  $2 \implies 3$ .

Finally, we will show that  $3 \implies 1$ .

We have some  $X$  such that (3) holds. Then, consider the exact sequence

$$0 \longrightarrow K \longrightarrow P \longrightarrow X \longrightarrow 0,$$

where  $P$  is a projective. This induces the long exact sequence

$$0 \longrightarrow \text{Hom}(X, K) \longrightarrow \text{Hom}(P, K) \longrightarrow \text{Hom}(K, K) \longrightarrow \text{Ext}^1(X, K) \longrightarrow \dots$$

However, note that  $\text{Ext}^1(X, K) = 0$ , so  $\text{Hom}(P, K)$  surjects onto  $\text{Hom}(K, K)$ . Specifically, we can find some  $f \in \text{Hom}(P, K)$  which maps onto  $\text{id}_K \in \text{Hom}(K, K)$ , so our short exact sequence splits as

$$0 \longrightarrow K \xrightarrow{f} P \longrightarrow X \longrightarrow 0$$

and then  $P \cong K \oplus \ker f$ , which implies  $\ker f \cong X$ , and since  $X$  is a direct summand of a projective, it must also be a projective.  $\square$

## LECTURE 29: EXT FUNCTORS

Last time, we defined the functors  $\overline{\text{Ext}}$  and  $\text{Ext}$ , and we had a lemma about projectives and  $\text{Ext}$ . We will now prove a similar lemma about injectives and  $\text{Ext}$ .

**Lemma 29.1.** The following are equivalent:

1.  $Y$  is injective
2. for all  $X$ ,  $\text{Ext}^i(X, Y) = 0$  for all  $i > 0$
3. for all  $X$ ,  $\text{Ext}^1(X, Y) = 0$

*Proof.* We will first prove that 1  $\implies$  2.

First, note that for any  $X$ , we can construct a short exact sequence

$$0 \longrightarrow K \longrightarrow P \longrightarrow X \longrightarrow 0,$$

where  $P$  is projective. Then, the induced long exact sequence is

$$0 \longrightarrow \text{Hom}(X, Y) \longrightarrow \text{Hom}(P, Y) \longrightarrow \text{Hom}(K, Y) \longrightarrow \text{Ext}^1(X, Y) \longrightarrow \cdots$$

However, since  $Y$  is an injective, and  $K \rightarrow P$  is injective, we know any morphism  $K \rightarrow Y$  must factor through  $P$ , and therefore  $\text{Hom}(P, Y) \rightarrow \text{Hom}(K, Y)$  is surjective. This implies that the rest of this long exact sequence must be zeroes, and in particular,  $\text{Ext}^i(X, Y) = 0$  for all  $i$ .

It is clear that 2  $\implies$  3.

We will now show that 3  $\implies$  1.

Consider any injective map  $A \rightarrow B$ . This implies that there is a short exact sequence

$$0 \longrightarrow A \longrightarrow B \longrightarrow Q \longrightarrow 0,$$

which induces a long exact sequence that starts with

$$0 \longrightarrow \text{Hom}(Q, Y) \longrightarrow \text{Hom}(B, Y) \longrightarrow \text{Hom}(A, Y) \longrightarrow \text{Ext}^1(Q, Y) = 0$$

which implies that  $\text{Hom}(B, Y) \rightarrow \text{Hom}(A, Y)$  is surjective, so any map  $A \rightarrow Y$  factors through  $B$ , and therefore  $Y$  is injective.  $\square$

**Lemma 29.2.** We defined  $\text{Ext}^i(X, Y)$  as a functor of  $X$ , but it is also a  $\delta$  functor when considered as a function of  $Y$ .

*Proof.* To prove this, we need to show that for any map  $f : Y_1 \rightarrow Y_2$ , there exists a corresponding natural transformation  $\text{Ext}^i(-, Y_1) \rightarrow \text{Ext}^i(-, Y_2)$ .

We start with  $i = 0$ ; in this case we want a map  $\text{Hom}(-, Y_1) \rightarrow \text{Hom}(-, Y_2)$ . In this case, we can just take the natural transformation  $\phi_X : g \mapsto f \circ g$ . As we have shown before, this is a natural transformation between homomorphism functors.

But then, since  $\text{Ext}^i(-, Y_1)$  is a universal  $\delta$ -functor and  $\text{Ext}^i(-, Y_2)$  is a  $\delta$ -functor, we know that this induces a unique collection of natural transformations

$$\phi^i : \text{Ext}^i(-, Y_1) \longrightarrow \text{Ext}^i(-, Y_2)$$

which is compatible with the boundary maps.

Thus, we have found our induced morphisms, so we have shown  $\text{Ext}^i(X, -)$  fulfills the second part of [Definition 27.3](#).

We leave it as an exercise to finish the proof that  $\text{Ext}^i(X, -)$  is a  $\delta$ -functor.  $\square$

**Lemma 29.3.** For any category  $\mathcal{C}$  which has enough injectives, and for any  $X \in \mathcal{C}$ , there exists a natural isomorphism

$$\overline{\text{Ext}}^i(X, -) \xrightarrow{\sim} \text{Ext}^i(X, -).$$

*Proof.* We can see that when  $i = 0$ , we need a map  $\text{Hom}(X, -) \rightarrow \text{Hom}(X, -)$ , and we can just use the identity map here.

Then, since  $\overline{\text{Ext}}^i(X, -)$  is a universal  $\delta$ -functor and  $\text{Ext}^i(X, -)$  is a  $\delta$ -functor, the definition of a universal  $\delta$ -functor tells us we can uniquely extend the natural transformation above into a collection of natural transformations

$$\overline{\text{Ext}}^i(X, -) \longrightarrow \text{Ext}^i(X, -)$$

which commutes with the boundary maps.

Then, we need to show that this is an isomorphism for each  $i$ . We can show this inductively; note that since  $\mathcal{C}$  has enough injectives, for any  $Y \in \text{ob}(\mathcal{C})$  we can produce the short exact sequence

$$0 \longrightarrow Y \longrightarrow I \longrightarrow Q \longrightarrow 0,$$

where  $I$  is an injective.

Then, we induce the long exact sequence

$$\begin{array}{ccccccc} \cdots & \longrightarrow & \overline{\text{Ext}}^{i-1}(X, Q) & \longrightarrow & \overline{\text{Ext}}^i(X, Y) & \longrightarrow & \overline{\text{Ext}}^i(X, I) \longrightarrow \cdots \\ & & \downarrow & & \downarrow & & \downarrow \\ \cdots & \longrightarrow & \text{Ext}^{i-1}(X, Q) & \longrightarrow & \text{Ext}^i(X, Y) & \longrightarrow & \text{Ext}^i(X, I) \longrightarrow \cdots \end{array}$$

By our inductive assumption, the green map on the left is an isomorphism, and since  $I$  is injective,  $\overline{\text{Ext}}^i(X, I) = \text{Ext}^i(X, I) = 0$ , so the green map on the right is an isomorphism of 0 modules, and via diagram chasing, this implies the purple map must be an isomorphism, as we desired.  $\square$

Let's look at some examples of  $\text{Ext}$ .

**Example 29.4.** We will work in the category  $\mathbb{Z}$ -mod.

1. Since  $\mathbb{Z}$  is projective,  $\text{Ext}^0(\mathbb{Z}, A) = A$  and  $\text{Ext}^i(\mathbb{Z}, A) = 0$  for all  $i > 0$ .
2. What is  $\text{Ext}^i(\mathbb{Z}/n\mathbb{Z}, A)$ ?

We have the exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$$

and by looking at the induced long exact sequence, and using the fact that  $\text{Ext}^i(\mathbb{Z}, A) = 0$  for all

$i > 0$ , we get that

$$\text{Ext}^0(\mathbb{Z}/n\mathbb{Z}, A) = \text{Hom}(\mathbb{Z}/n\mathbb{Z}, A)$$

$$\text{Ext}^1(\mathbb{Z}/n\mathbb{Z}, A) = A/nA$$

$$\text{Ext}^i(\mathbb{Z}/n\mathbb{Z}, A) = 0 \text{ when } i > 1.$$

**Exercise 29.5.** As a challenge, compute  $\text{Ext}^i(\mathbb{Q}, \mathbb{Z})$  for all  $i$ .

We now switch to talking about the Tor functor.

**Definition 29.6.** Consider the map

$$\begin{aligned} M \otimes - : \mathbf{R}\text{-Mod} &\longrightarrow \mathbf{R}\text{-Mod} \\ N &\longmapsto M \otimes N. \end{aligned}$$

This is a covariant and right-exact functor.

Since  $\mathbf{R}\text{-Mod}$  has enough projectives, we can define the **Tor functor** to be the  $\delta$ -functors:

$$\begin{aligned} \text{Tor}_i^R(M, -) : \mathbf{R}\text{-Mod} &\longrightarrow \mathbf{R}\text{-Mod} \\ N &\longmapsto L_i(M \otimes_R N), \end{aligned}$$

where  $L_i$  is the left-derived functor.

This is a universal  $\delta$ -functor.

This means that given any short-exact sequence

$$0 \longrightarrow N_1 \longrightarrow N_2 \longrightarrow N_3 \longrightarrow 0$$

we induce the long-exact sequence

$$\cdots \longrightarrow \text{Tor}_1^R(M, N_2) \longrightarrow \text{Tor}_1^R(M, N_3) \longrightarrow M \otimes N_1 \longrightarrow M \otimes N_2 \longrightarrow M \otimes N_3 \longrightarrow 0.$$

**Definition 29.7.** We say that  $M$  is a **flat module** if  $M \otimes_R -$  is an exact functor.

## LECTURE 30: TOR FUNCTORS

At the end of last lecture, we defined the Tor  $\delta$ -functor. (Note that I have added in this definition at the end of last lecture, but I didn't have it there before.)

We have a very similar lemma to what we proved for Ext:

**Lemma 30.1.** The following are equivalent:

1.  $N$  is a flat module.
2. For all  $M$ ,  $\text{Tor}_i(N, M) = 0$  for all  $i > 0$ .
3. For all  $M$ ,  $\text{Tor}_1(N, M) = 0$ .

Based on the above lemma, we can also prove the following:

**Lemma 30.2.**

1.  $M_1 \oplus M_2$  is flat if and only if  $M_1$  and  $M_2$  are flat.
2. All free modules are flat.
3. All projective modules are flat.

**Lemma 30.3.** If

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

is exact, then

$$\cdots \longrightarrow \text{Tor}_1(M_2, N) \longrightarrow \text{Tor}_1(M_3, N) \longrightarrow M_1 \otimes N \longrightarrow M_2 \otimes N \longrightarrow M_3 \otimes N \longrightarrow 0$$

is long exact.

*Proof.* Consider the projective resolution  $P^\bullet \rightarrow N \rightarrow 0$ . Then, we know that the induced sequence

$$0 \longrightarrow M_1 \otimes P^\bullet \longrightarrow M_2 \otimes P^\bullet \longrightarrow M_3 \otimes P^\bullet \longrightarrow 0$$

has exact rows. This implies a long-exact sequence in the cohomology, which implies there is a long exact sequence of our left-derived functors, which are exactly the Tor functors.  $\square$

Now, we can consider the Tor functor on the first coordinate, and we get similar results.

**Lemma 30.4.** The following are equivalent:

1.  $N$  is a flat module.
2. For all  $M$ ,  $\text{Tor}_i(M, N) = 0$  for all  $i > 0$ .
3. For all  $M$ ,  $\text{Tor}_1(M, N) = 0$ .

*Proof.* We will first show that 1  $\implies$  2.

We proceed via induction on  $i$ . First, given an  $M$ , we know there exists an exact sequence

$$0 \longrightarrow K \longrightarrow P \longrightarrow M \longrightarrow 0,$$

where  $P$  is a projective, and  $K$  is the kernel of  $P \rightarrow M$ . At a base case, when  $i = 1$ , we are looking at the exact sequence

$$\cdots \longrightarrow \mathrm{Tor}_1(P, N) \longrightarrow \mathrm{Tor}_1(M, N) \longrightarrow K \otimes N \longrightarrow P \otimes N \longrightarrow \cdots$$

But  $\mathrm{Tor}_1(P, N) = 0$  since  $P$  is projective and therefore flat. This means  $\mathrm{Tor}_1(M, N) \rightarrow K \otimes N$  must be injective. But since  $N$  is flat, we know that  $- \otimes N$  preserves exact sequences, so  $K \otimes N \rightarrow P \otimes N$  is an injective map. For this sequence to be exact, we then need  $\mathrm{Tor}_1(M, N) = 0$ . For the inductive case, we are looking at the exact sequence

$$\cdots \longrightarrow \mathrm{Tor}_i(P, N) \longrightarrow \mathrm{Tor}_i(M, N) \longrightarrow \mathrm{Tor}_{i-1}(K, N) \longrightarrow \cdots$$

and we can see that because  $P$  is projective,  $\mathrm{Tor}_i(P, N) = 0$  and by the inductive hypothesis  $\mathrm{Tor}_{i-1}(K, N) = 0$ , so for this sequence to be exact, we need  $\mathrm{Tor}_i(M, N)$  to be 0 as well.

It is clear that  $2 \implies 3$ .

To show that  $3 \implies 1$ , we will look at an arbitrary exact sequence

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0.$$

Then, we know that the induced long exact sequence is

$$\cdots \longrightarrow \mathrm{Tor}_1(M_3, N) \longrightarrow M_1 \otimes N \longrightarrow M_2 \otimes N \longrightarrow M_3 \otimes N \longrightarrow 0.$$

But  $\mathrm{Tor}_1(M_3, N) = 0$ , so

$$0 \longrightarrow M_1 \otimes N \longrightarrow M_2 \otimes N \longrightarrow M_3 \otimes N \longrightarrow 0$$

is short exact, as we desired! □

As we might expect,  $\mathrm{Tor}$  is a  $\delta$ -functor in the first variable as well:

**Proposition 30.5.**

1.  $M \mapsto \mathrm{Tor}_i(M, N)$  is a  $\delta$ -functor.
2. For all  $M, N$ ,  $\mathrm{Tor}_i(M, N) \cong \mathrm{Tor}_i(N, M)$ .

The proofs of these were covered in class but I am very tired and these are very similar to the corresponding proofs for  $\mathrm{Ext}$ , so I am leaving these as an exercise.

**Remark 30.6.** The functor  $\mathrm{Tor}_i(-, M)$  is the left-derived functor of  $- \otimes_R M$ .

Let's try to understand flatness better. The following lemma essentially tells us that flatness is a local property:

**Lemma 30.7.** The following are equivalent:

1.  $M$  is flat over  $R$
2.  $M_\varphi$  is flat over  $R_\varphi$ , for any prime ideal  $\varphi \triangleleft R$ .
3.  $M_{\mathfrak{m}}$  is flat over  $R_{\mathfrak{m}}$ , for any maximal ideal  $\mathfrak{m} \triangleleft R$ .

*Proof.* First, we will show that  $1 \implies 2$ :

For any short exact sequence

$$0 \longrightarrow N_1 \longrightarrow N_2 \longrightarrow N_3 \longrightarrow 0,$$

where each  $N_i$  is an  $R_\varphi$ -module, we note that since  $M$  is flat,

$$0 \longrightarrow M \otimes_R N_1 \longrightarrow M \otimes_R N_2 \longrightarrow M \otimes_R N_3 \longrightarrow 0$$

is short exact. But then we can see that for each  $N_i$ ,

$$M \otimes_R N_i \cong M \otimes_R (R_\varphi \otimes_{R_\varphi} N_i) \cong (M \otimes_R R_\varphi) \otimes_{R_\varphi} N_i \cong M_\varphi \otimes_{R_\varphi} N_i,$$

so this gives us an exact sequence over  $R_\varphi$ , and  $M_\varphi$  is flat over  $R_\varphi$ , as we desired.

It is clear that 2  $\implies$  3.

We now show that 3  $\implies$  1.

Consider any short exact sequence

$$0 \longrightarrow N_1 \longrightarrow N_2 \longrightarrow N_3 \longrightarrow 0$$

of  $R$ -modules. Then, we know that since  $M_{\mathfrak{m}}$  is flat,

$$0 \longrightarrow M_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} N_{1\mathfrak{m}} \longrightarrow M_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} N_{2\mathfrak{m}} \longrightarrow M_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} N_{3\mathfrak{m}} \longrightarrow 0$$

is short exact. Moreover, since  $M \otimes_R -$  is always a right-exact functor, we know that there is an induced exact sequence

$$0 \longrightarrow K \longrightarrow M \otimes_R N_1 \longrightarrow M \otimes_R N_2 \longrightarrow M \otimes_R N_3 \longrightarrow 0,$$

for some kernel  $K$ . But localizing this at  $\mathfrak{m}$  should preserve exactness, so  $K_{\mathfrak{m}} = 0$  for all  $\mathfrak{m}$  (to match the above short exact sequence). But this means that  $K = 0$ , and we get our desired short exact sequence, and  $M$  is flat over  $R$ .  $\square$

**Definition 30.8.** A **local ring** is one with a unique maximal ideal.

**Lemma 30.9.** If  $R$  is a Noetherian local ring and  $M$  is a finitely-generated  $R$ -module, then  $M$  is free over  $R$  if and only if it is flat over  $R$ .

**Definition 30.10.** Showing that free implies flat is easy.

For the other direction, consider the unique maximal ideal  $\mathfrak{m}$ . We know that  $M/\mathfrak{m}M$  is finitely generated over  $R/\mathfrak{m}$ , which is a field, and therefore it must have a basis over this field. Thus, we can write

$$M/\mathfrak{m}M \cong (R/\mathfrak{m})^{\oplus d},$$

where  $d$  is the degree of  $M/\mathfrak{m}M$ .

Then, Nakayama's lemma tells us that  $R^{\oplus d} \rightarrow M$  is a surjection, so we have the exact sequence

$$0 \longrightarrow K \longrightarrow R^{\oplus d} \longrightarrow M \longrightarrow 0.$$

Then, we can consider the functor  $R/\mathfrak{m} \otimes_R -$ . We can apply the induced Tor functor to this short exact sequence to get the long exact sequence

$$\cdots \longrightarrow \mathrm{Tor}_1^R(R/\mathfrak{m}, M) \longrightarrow K/\mathfrak{m} \longrightarrow (R/\mathfrak{m})^{\oplus d} \longrightarrow M/\mathfrak{m}M \longrightarrow 0.$$

But since  $M$  is flat,  $\mathrm{Tor}_1^R(R/\mathfrak{m}, M) = 0$ , so  $K/\mathfrak{m} = \ker((R/\mathfrak{m})^{\oplus d} \rightarrow M/\mathfrak{m}M)$ . But we know that this

is an isomorphism, so the kernel is 0, and  $K/\mathfrak{m} = 0$ . Since  $K$  is finitely generated over  $R$  (since  $R$  is Noetherian), Nakayama's lemma tells us this implies  $K = 0$ , and therefore  $M \cong R^{\oplus d}$ .

Now, let's look at some examples of torsion functors.

**Example 30.11.** What is  $\mathrm{Tor}_i^{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Z}/(m))$ ?

Well, we can consider the short exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\times m} \mathbb{Z} \longrightarrow \mathbb{Z}/(m) \longrightarrow 0$$

We can see that tensoring this with  $\mathbb{Z}/(n)$  gives us the short exact sequence

$$0 \longrightarrow \mathbb{Z}/(n) \xrightarrow{\times m} \mathbb{Z}/(n) \longrightarrow \mathbb{Z}/(m, n) \longrightarrow 0$$

and if we look at the left derived functors of this, we get that

$$\mathrm{Tor}_i^{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Z}/(m)) = \begin{cases} \mathbb{Z}/(m, n) & \text{if } i = 0, 1 \\ (0) & \text{otherwise.} \end{cases}$$

For example, consider the short exact sequence

$$0 \longrightarrow \mathbb{Z}/2 \xrightarrow{\times 2} \mathbb{Z}/4 \longrightarrow \mathbb{Z}/2 \longrightarrow 0$$

Tensoring this with  $\mathbb{Z}/2$  gives us the induced torsion sequence

$$0 \longrightarrow \mathrm{Tor}_1(\mathbb{Z}/2, \mathbb{Z}/2) \longrightarrow \mathrm{Tor}_1(\mathbb{Z}/2, \mathbb{Z}/4) \longrightarrow \mathrm{Tor}_1(\mathbb{Z}/2, \mathbb{Z}/2) \longrightarrow \mathbb{Z}/2 \longrightarrow \mathbb{Z}/2 \longrightarrow \mathbb{Z}/2 \longrightarrow 0,$$

which is just the long exact sequence

$$0 \longrightarrow \mathbb{Z}/2 \xrightarrow{\sim} \mathbb{Z}/2 \xrightarrow{0} \mathbb{Z}/2 \xrightarrow{\sim} \mathbb{Z}/2 \xrightarrow{\times 2} \mathbb{Z}/2 \xrightarrow{\sim} \mathbb{Z}/2 \longrightarrow 0$$



## APPENDIX A: TENSOR PRODUCTS REVIEW

I'm collecting some information about tensor products here, because I keep getting lost looking for the relevant information in the actual notes.

First, we have a tensor product of rings:

**Definition A.1.** If  $R, S, T$  are rings, and  $\phi : R \rightarrow S$  and  $\psi : S \rightarrow T$  are ring morphisms, then the **tensor product**  $S \otimes_R T$  is defined as

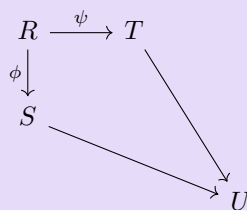
$$R[X_s, Y_t]_{s \in S, t \in T} / I,$$

where  $I$  is the ideal

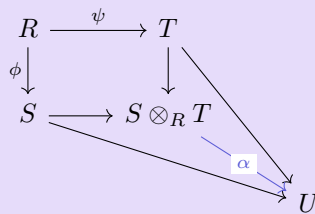
$$I = \left( \begin{array}{cc} X_{s_1+s_2} - X_{s_1} - X_{s_2}, & Y_{t_1+t_2} - Y_{t_1} - Y_{t_2}, \\ X_{s_1 s_2} - X_{s_1} X_{s_2}, & Y_{t_1 t_2} - Y_{t_1} Y_{t_2}, \\ X_{\phi(r)} - r, & Y_{\psi(r)} - r \end{array} \right)_{s_1, s_2 \in S, t_1, t_2 \in T, r \in R}.$$

The tensor product of rings has the following universal property:

**Lemma A.2.** For any ring morphisms  $S \rightarrow U$  and  $T \rightarrow U$  such that the diagram



commutes, there exists a unique ring morphism  $\alpha : S \otimes_R T \rightarrow U$  such that the diagram



commutes.

We have a few useful lemmas about tensor products of rings, starting with [Lemma 7.12](#).

Then, we have the tensor product of a ring and a module:

**Definition A.3.** If  $R$  and  $S$  are rings,  $M$  is an  $R$ -module, and  $\phi : R \rightarrow S$  is a ring morphism, then the **tensor product**  $S \otimes_R M$  is defined as

$$F_S(M) / N,$$

where  $N$  is the submodule

$$N = \langle e_n + e_m - e_{m+n}, e_{rm} - \phi(r)e_m \rangle_{r \in R, m, n \in M}.$$

This has the universal property:

**Lemma A.4.** For any  $S$ -module  $P$  and  $R$ -linear map  $f : M \rightarrow P$  (where  $R$  acts on  $P$  by  $r \cdot p = \phi(r)p$ ), there is a unique  $S$ -linear map  $\tilde{f} : S \otimes_R M \rightarrow P$  such that the diagram

$$\begin{array}{ccc} M & \xrightarrow{f} & P \\ \downarrow & \nearrow \tilde{f} & \\ S \otimes_R M & & \end{array}$$

commutes and  $\tilde{f}(s \otimes m) = sf(m)$ .

We have a few useful lemmas about tensor products of a ring and a module, starting with [Lemma 16.2](#).

Note that the above two tensor products are equivalent, in the sense that:

**Lemma A.5.** If  $R, S, T$  are rings and we have ring morphisms  $\phi : R \rightarrow S$ ,  $\psi : R \rightarrow T$ , then we have the ring tensor product  $S \otimes_R T$ .

But we can also consider  $T$  as an  $R$ -module, via the action  $r \cdot t = \psi(r)t$ , and then get the ring-module tensor product  $S \otimes_R T$ .

These two are isomorphic as  $S$ -modules.

Finally, we have the tensor product of multiple modules:

**Definition A.6.** If  $M_1, \dots, M_a$  are  $R$ -modules, then the **tensor product over  $R$**   $M_1 \otimes \dots \otimes M_a$  is defined as

$$F_R(M_1 \times \dots \times M_a)/N,$$

where we are taking the free module generated by the set-theoretic product  $M_1 \times \dots \times M_a$ , and then quotienting out by the submodule

$$N = \langle e_{(m_1, \dots, m_i + rm'_i, \dots, m_a)} - e_{(m_1, \dots, m_a)} - re_{(m_1, \dots, m'_i, \dots, m_a)} \rangle_{m_j \in M_j, m'_i \in M_i, r \in R}.$$

This has the following universal property:

**Lemma A.7.** For any  $R$ -module  $P$  and multilinear map  $\psi : M_1 \times \dots \times M_a \rightarrow P$ , there exists a unique  $R$ -linear map  $\tilde{\psi} : M_1 \otimes \dots \otimes M_a \rightarrow P$  such that the diagram

$$\begin{array}{ccc} M_1 \times \dots \times M_a & \xrightarrow{\psi} & P \\ \downarrow & \nearrow \tilde{\psi} & \\ M_1 \otimes \dots \otimes M_a & & \end{array}$$

commutes.

We have a few useful lemmas about the tensor products of modules, starting with [Proposition 18.2](#).

This is also equivalent to the previous tensor products, in the sense that:

**Lemma A.8.** If  $R$  and  $S$  are rings, with a ring morphism  $\phi : R \rightarrow S$ , and we have an  $R$ -module  $M$ , then we have the ring-module tensor product  $S \otimes_R M$ , which turns  $M$  into an  $S$ -module.

But we can also consider  $S$  as an  $R$ -module, with the action  $r \cdot s = \phi(r)s$ , and then  $S \otimes_R M$  is the

$R$ -module induced by the set product  $S \times M$ .

These two tensor products are isomorphic as  $R$ -modules.