Undergraduate Commutative Algebra
Homological Algebra at Notre Dame

Adam Boocher

May 2019

Contents

0 Introduction and Outline

What is commutative algebra? The most general answer is probably something along the lines of "the study of polynomials." As such, this statement is too vague for us to know exactly what to expect.

- Will we be solving polynomials equations like $x^n + y^n = z^n$ over the integers? (Things like this are the subject of number theory.)
- Or perhaps using Newton's method to solve polynomial equations on the real line? (This problem and its generalizations make for the beautiful theory of real algebraic geometry. Andrew Sommese says "Everyone should write a polynomial solver at least once." See [6])
- Or what about studying the cubic formula, or the quartic formula?

All of the above problems are dedicated to *solving* polynomial equations over some specific number system (be it $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$) and which number system we choose will greatly affect what the answers are. Generally the solution set to a system of polynomial equations is called an algebraic variety, and typically we work with polynomials that are defined over a field (usually denoted k, for the german *Körper*.) Polynomials in one variable have a finite number of solutions, but in two or more variables there are often infinitely many solutions that form a geometric object (think: the solutions to $y = x^2$ in $\mathbb{R}^2$). In commutative algebra we can study these polynomials themselves, namely the *ideal* generated by them. Like other objects that come up in algebra (including vector spaces, subspaces, groups, subrings, fields, etc) an ideal is an subset of a larger thing that is "closed" under some operations. I like to think about this as some sort of mystical property.

A Trip to that Mystical Land of Closure: If you have an ideal I, then you know that I is closed under addition, so for instance if you know that $x \in I$ and also $y - x \in I$ then you know that $y \in I$ as well. I think of this like a pond full of fish. If you know certain fish are in the pond, then truly you know about lots of other fish that **must** be there.

Why the digression on ponds and fish? My goal with these notes is two-fold. On the one hand I want you to learn about the beautiful properties of ideals in polynomial rings, but also I want to present the material in such a way that it is friendly, accessible and puts things in context with other ideas. Indeed, our approach to prove our theorems isn't the quickest (nor the easiest). In some cases we will give the idea of a proof rather than all the technical details. Along the way we will adopt tools from **homological algebra** and see them in action.

0.1 Where are we going

We begin with a quick game with some dots on the board and will see some rather surprising patterns. These patterns are no coincidence (and it will take us a week to get to the bottom of this.) In the first lecture we'll explore ideals in $\mathbb{R}[x_1, \ldots, x_n]$ that arise in many different ways and then prove the Hilbert Basis Theorem, which says that ideals always have a finite number of generators. We'll use Macaulay2 for examples and solve problems about how many generators an ideal can have.

In the second and third lectures we'll focus on the question: "Does an ideal have a basis?" We'll quickly see that the answer is basically always **no**. Undeterred, we'll look at other objects that behave like ideals (things like quotient rings and R^r) and see when those objects have bases (again hardly ever). We'll introduce the Hilbert Function and prove that it is eventually a polynomial function. To do this, we'll start using the abstract language of **exact sequences** and some hocus pocus (homology, diagram chases, and some strange examples). In the exercises we'll continue to explore our calculations of ideals, Hilbert functions, kernels, etc. In the final lecture we'll sketch a proof of the Hilbert Syzygy Theorem. We'll do this by defining what a free resolution is.

Adam Boocher May 2019

1 From Counting Dots to Hilbert Series

In this lecture we will begin with a combinatorial game that presents an interesting counting problem. We will relate this problem to a question about monomial ideals and define something called the Hilbert Function. We will compute the Hilbert Function of the polynomial ring, and for some simple quotients. We will end with a question (later to be answered by the Hilbert Basis Theorem) that will be one of our main motivations throughout the week.

Mysterious Warmup: Consider the following limit:

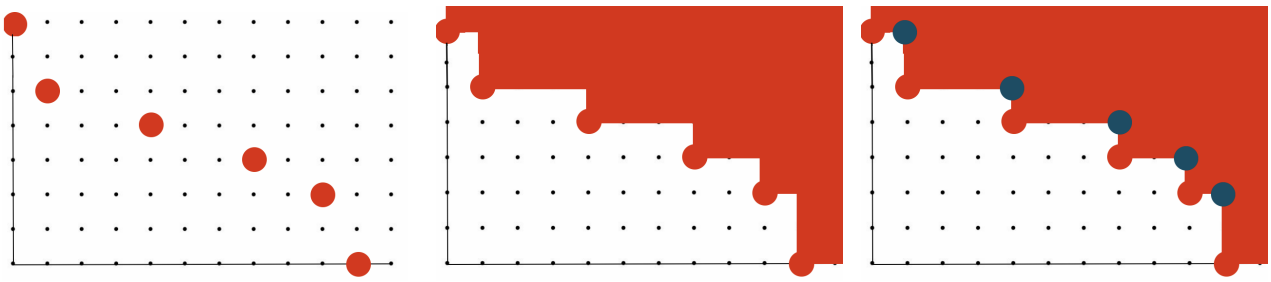
$$\lim_{t\to 1} \frac{1 - t^6 - t^7 - t^8 - 2t^{10} - t^{11} + t^8 + t^9 + t^{11} + 2t^{12}}{(1-t)^2} = 42.$$

(we could compute this say by L'Hopital's rule if we wanted). Let's keep this in mind as we continue.

1.1 A combinatorial game

We begin with a combinatorial game. Suppose we start with the first quadrant in the plane, and mark of a point on each of the coordinate axes. Then go ahead and add as many dots as you'd like at lattice points in the first quadrant. For example, below we have added the points

$$(0,7), (1,5), (4,4), (7,3), (9,2), (10,0).$$



Now we'll draw lines up and to the right, erasing all the dots out there. We will be left with a finite number of dots. How many do we have? In this case we have 42 dots. Pause now to imagine what the situation might look like if instead, the points we added were something like:

$$(5347, 0), (0, 167), (23, 67), (67, 233), (233, 2), (17, 170), \cdots$$

Surely we could find a way to count the number of dots remaining. But it wouldn't be immediate. Below we will show one approach that solves this problem and by the end of the week we will explain why it works.

Notice that the shaded region (the dots we removed) has the shape of a staircase. The given points are in red (think of these as the lower steps) and we've added in blue dots (the upper steps). Now we can record the total weight of each step, (we just mean the sum of the coordinates), so our weights are

$$7, 6, 8, 10, 11, 10, \quad 8, 9, 11, 12, 12.$$

Now let's return to that limit we had earlier. Notice that the exponents that appear are precisely the degrees of our steps:

$$\frac{1 - t^6 - t^7 - t^8 - 2t^{10} - t^{11} + t^8 + t^9 + t^{11} + 2t^{12}}{(1-t)^2}$$

In fact if we factor the numerator and cancel we obtain:

$$1 + 2t + 3t^2 + 4t^3 + 5t^4 + 6t^5 + 6t^6 + 5t^7 + 4t^8 + 4t^9 + 2t^{10}.$$

Notice something quite surprising in this: The coefficients of successive powers of t are precisely the number of dots on the ith diagonal in our picture!

$$\#\text{ of dots under staircase encoded as coefficients} = \frac{1 - \sum_{\text{lower steps}} t^{\text{deg. step}} + \sum_{\text{upper steps}} t^{\text{deg. step}}}{(1-t)^2} \tag{1.1}$$

1.2 What are all those dots?

All those dots are actually the building blocks of the polynomial ring $\mathbb{R}[x, y]$ - our first object of study. Indeed, every polynomial in $\mathbb{R}[x, y]$ is built out of **monomials** - terms $x^i y^j$ where $i, j \geqslant 0$. We can think of the exponents as vectors (i, j) and thus think of them as points in the first quadrant of the plane. You'll notice that there are infinitely many dots in the first quadrant, just as there are infinitely many monomials in $\mathbb{R}[x, y]$. However if we count them **by degree** then we will get a finite number in each time.

Notation: Throughout these notes we will use the letter R to denote the polynomial ring $\mathbb{R}[x_1, \ldots, x_n]$ where there are some number of variables. Sometimes these variables will be x, y, z and other times $x_1, \ldots, x_n$.

Definition 1.1. The Hilbert Function of $R = \mathbb{R}[x, y]$, denoted $HF_R(d)$ is defined by

$$HF_R(d) = \text{the number of degree } d \text{ monomials in } R.$$

We sometimes think of the Hilbert function as a sequence $\{HF_R(0), HF_R(1), \ldots\}$. Because we will later generalize this definition, let's point out an equivalent form:

$$HF_R(d) = \text{the dimension of the vector space of homogeneous degree } d \text{ polynomials in } R.$$

We say that a polynomial $f(x, y)$ is **homogenous of degree** d if each nonzero monomial of $f(x, y)$ has degree d. (Note that the zero polynomial has degree d for every d - don't fret about this much)

Example 1.2. The polynomial $f = x^4 + xyz^2 - 45x^2w^2$ is homogeneous of degree 4. The polynomial $x^2 + y$ is not homogeneous.

If we count the number of dots in the first quadrant we see that the sequence we obtain is

$$\{1, 2, 3, 4, 5, \ldots\}.$$

Hence the Hilbert Function of $\mathbb{R}[x, y]$ is equal to this sequence of numbers.

Proposition 1.3. *There are exactly $d + 1$ monomials of degree d in $\mathbb{R}[x, y]$. Hence*

$$HF_{\mathbb{R}[x,y]}(d) = d + 1, \text{ for } d \geqslant 0.$$

Proof. We can actually count them all - the correspond to the $d + 1$ dots on the dth diagonal in the first quadrant. $x^d, x^{d-1}y, \ldots, y^d$. Yep - there's $d + 1$. □

Now naturally we can extend this to a polynomial ring in any number of variables. For instance if we counted degree d monomials in $\mathbb{R}[x]$ we'd get just 1 of each degree, so $HF_{\mathbb{R}[x]}(d) = 1$ for all d. More generally if $R = \mathbb{R}[x_1, \ldots, x_n]$ then we define $HF_R(d)$ to be the dimension of the vector space of polynomials of degree d. In the exercises you will show that $HF_R(d) = \binom{n+d-1}{d}$.

Talking about sequences of numbers is great, but it's a bit inconvenient because we have to say things like "the Hilbert function of **this** ring in **this** degree is **blank**." Instead, why not encode everything all at once:

Definition 1.4. Let $a_0, a_1, \ldots,$ be a sequence of numbers. We define the **generating function** for this sequence to be the power series

$$a_0 + a_1 t + a_2 t^2 + a_3 t^3 + \cdots .$$

The power series coming from the Hilbert Function is called the **Hilbert Series**:

$$HF_R(0) + HF_R(1)t + HF_R(2)t^2 +$$

Notice that a generating series is nothing or less than a sequence - to go from one to the other is just a matter of copying down coefficients. However, generating sequences are slightly more useful because can can do algebra with them.

Example 1.5. If $R = \mathbb{R}[x]$ then the Hilbert sequence for R is

$$\{HF_R(d)\} = \{1, 1, 1, 1, \ldots, \}$$

so the Hilbert Series is

$$1 + t + t^2 + t^3 + \cdots = \frac{1}{1-t}.$$

If you're skeptical of this (maybe you should be!) then just multiply both sides by $1 - t$ and check that you get equal quantities on both sides.

Example 1.6. If $R = \mathbb{R}[x, y]$ then the Hilbert sequence for R is

$$\{HF_R(d)\} = \{1, 2, 3, 4, \ldots, \}$$

so the Hilbert Series is

$$1 + 2t + 3t^2 + 4t^3 + \cdots = \text{the derivative of } (1 + t + t^2 + \cdots)$$

$$= \left(\frac{1}{1-t}\right)' = \frac{1}{(1-t)^2}.$$

As you'll see in the exercises, the Hilbert series of $\mathbb{R}[x, y, z]$ will be

$$HS(\mathbb{R}[x, y, z]) = 1 + 3t + 6t^2 + \cdots = \frac{1}{2}(\text{the derivative of} \frac{1}{(1-t)^2}) = \frac{1}{(1-t)^3}.$$

This pattern continues as you will prove:

$$HS(\mathbb{R}[x_1, \ldots, x_n]) = \frac{1}{(1-t)^n}.$$

1.3 What are all those shaded dots? Ideals

Now let's move to the shaded region in our picture. What properties does it have? Let's examine the point $(3, 2)$ which corresponds to the monomial x^3y^2. We've decided to shade everything to the right and above this point. Moving to the right is multiplying by x and moving up is multiplying by y. These are the basic properties of an **ideal**. Remember R will always mean $\mathbb{R}[x_1, \ldots, x_n]$.

Definition 1.7. We say that a subset $I \subset R = \mathbb{C}[x_1, \ldots, x_n]$ is an **ideal** if

1. $0 \in I$
2. if $f, g \in I$ then $f + g \in I$
3. if $f \in I$ and $r \in R$ then $rf \in I$.

Example 1.8. The set of all multiplies of x^3 is an ideal. Indeed, 0 is a multiple of x^3. If we add two multiples of x^3 then we get another multiple of x^3. And if we multiply a multiple of x^3 by an arbitrary polynomial then we get another multiple of x^3. This is called the **ideal generated by** x^3 and is denoted by (x^3). Ideals generated by single polynomials are called **principal ideals.**

In our example with the staircase above, our ideal is **generated** by the lower steps and we write

$$I = (x^4, x^3y^2, xy^4, y^5).$$

This means that I contains things like

$$x^4 + y^5$$

$$(3x + 1700)x^4$$

$$(x + y + 100)(xy^4) + x^{100}$$

So our shaded region corresponds to the monomials in our ideal I.

Our staircase diagram above gives a graphic depiction of the **monomial ideal** $I = (x^4, x^3y, xy^5, y^7)$. It is called a monomial ideal because its generators are monomials. If we think what polynomials are in this ideal I then every element in the ideal must be of the form:

$$f = ax^4 + bx^3y + cxy^5 + dy^7.$$

where a, b, c, d are **polynomials**. In other words, every term of f must be a multiple of one of our generators (bottom steps). In other words, this means that every term of f is in the shaded region of our diagram. This is what we mean when we say that the shaded region of the diagram represents the ideal I. In this case I was given to us and had 4 generators.

Often ideals are presented to us by giving a set of **generators**. For instance

$$I = \langle f_1, \ldots, f_r \rangle$$

means "I is the smallest ideal that contains $f_1, \ldots, f_r$." What does this mean? Well since I is an ideal, it must be closed under addition and multiplication by elements in the ring R. So this means that I certainly contains all polynomials of the form:

$$a_1 f_1 + \cdots + a_r f_r$$

where $a_1, \ldots, a_r \in R$ are arbitrary polynomials. In fact, the set of all such **linear combinations** forms an ideal. (Exercise: check that the three properties in the definition are satisfied).

Remark 1.9. Note that if our ideal is not a monomial ideal, then such a depiction isn't readily available. We'll do lots of examples with monomial ideals, but it's important to remember that not every ideal is monomial. Indeed, one of the most famous ideals is the ideal of the Twisted Cubic curve defined as

$$I = (xz - y^2, xw - yz, yw - z^2).$$

In this case elements of the ideal I are those polynomials that are linear combinations of these three polynomials. What might a picture of this ideal look like?

Definition 1.10. We say that an ideal is homogeneous if there is a generating set that consists of homogeneous polynomials. If I is homogeneous then we define the Hilbert Function of I to be:

$$HF_I(d) = \text{the dimension of the vector space of homogeneous degree } d \text{ polynomials in } I.$$

Example 1.11. If $R = \mathbb{R}[x, y]$ and $I = (x^3)$ then there are no polynomials of degrees 0,1, or 2 in I. And then in degrees $3, 4, 5$ we have the monomials

$$x^3$$
$$x^4, x^3y$$
$$x^5, x^4y, x^3y^2.$$

Thus the Hilbert Series is

$$0 + 0t + 0t^2 + t^3 + 2t^4 + 3t^5 + \cdots = t^3(1 + t + 2t + \cdots) = t^3\frac{1}{(1-t)^2} = \frac{t^3}{(1-t)^2}.$$

Example 1.12. What about the ideal $I = (x^3, y^3)$? (Drawing the picture will help here.) The Hilbert Series is

$$0 + 0t + 0t^2 + 2t^3 + 4t^4 + 6t^5 + 7t^6 + 8t^7 + \cdots$$

notice that from t^5 onward we have all the possible dots. So if you want, you can think about it this way.

$$HR_I = HR_{\mathbb{R}[x,y]} - (1 + 2t + 3t^2 + 2t^3 + t^4)$$

$$= \frac{1}{(1-t)^2} - (1 + 2t + 3t^2 + 2t^3 + t^4) = \frac{1 - 2t^3 + t^6}{(1-t)^2}.$$

Notice that we see our lower (red) and upper (blue) steps appearing in this formula.

Example 1.13. In our example from the picture $I = (x^{10}, x^9y^2, x^7y^3, x^4y^4, xy^5, y^7)$ and we can use Macaulay2 to calculate the HilbertSeries of I:

```
i1 : R=QQ[x,y]; I = ideal(x^10, x^9*x^2,x^7*y^3,x^4*y^4,x*y^5,y^7); hilbertSeries(module I, Reduce=>true)

o2 : Ideal of R

        6    7    9     10    11    13
       T  + T  - T  + 2T   - T   - T
o3 = -------------------------------
                          2
                  (1 - T)

o3 : Expression of class Divide
```

Notice in both of these examples the Hilbert series was equal to some polynomial divided by $(1-t)^2$.

1.4 What are all those unshaded dots? Quotient Rings

Definition 1.14. If $I \subset R$ is an ideal then the quotient ring R/I is defined to be the ring whose elements are elements of the form $\overline{f}$ for $f \in R$ where $\overline{f} = \overline{g}$ if $f - g \in I$. Arithmetic in the ring behaves as you'd expect and is probably best done by example.

Example 1.15. Continuing with the example above, let

$$I = (x^{10}, x^9y^2, x^7y^3, x^4y^4, xy^5, y^7).$$

Then R/I is a ring just like R except now some polynomials are equal that weren't before. For instance $\overline{x^{10}} = \overline{0}$ since $x^{10} - 0 \in I$. Indeed, if $f \in I$ then it follows that $\overline{f} = \overline{0}$. So all of those parts of our shaded region are going to be zero in R/I. What's left then - the unshaded part. It is true (Exercise!) that for a monomial ideal I, R/I is spanned (as a k-vector space) by those monomials not in I. Macaulay2 can give us a list of these monomials which we can count:

```
i1 :  R = QQ[x,y]; I = ideal"x10,x9y2,x7y3,x4y4,xy5,y6"; apply(15, i-> # flatten entries basis(i,R/I))

o2 : Ideal of R

o3 = {1, 2, 3, 4, 5, 6, 5, 5, 4, 4, 2, 0, 0, 0, 0}

o3 : List
```

If you think about our staircase diagram, it's clear that every dot is either above the staircase or it isn't.

Proposition 1.16. *If I is a homogeneous ideal in a polynomial ring $R = \mathbb{R}[x_1, \ldots, x_n]$ then*

$$HS(R/I) + HS(I) = HS(R) = \frac{1}{(1-t)^n}.$$

Proof. If I is monomial then the result is clear since bases for the degree d piece of I can be chosen to be "dots on the dth diagonal that are in I" and a basis for the degree d piece of R/I can be chosen to be "all the remaining dots on that diagonal."

If I is not monomial, then one can proceed in two different ways. One way leads to the beautiful subject of Gröbner bases in which we can reduce questions about arbitrary ideals to ones about monomial ideals. Instead, we'll chose a more "homological" approach that proceeds with a linear algebra trick. Our goal is simply to show that we can find bases of I_d and $(R/I)_d$ such that their union is a basis of R_d. This is not so bad:

1. Take a basis of I_d (every vector space has a basis) $f_1, \ldots, f_r$
2. Extend this basis to a basis of R_d by adding elements $g_1, \ldots, g_s$
3. Show that $g_1, \ldots, g_s$ is a basis for $(R/I)_d$.

We leave this final step as an exercise for the reader who wants to practice their linear algebra skills. (Highly recommended, though probably skippable on the first pass). □

The above proposition shows us that if we are concerned with Hilbert Series, then whether we compute the Hilbert Series of I or R/I we can obtain the other. This is not a one-off situation. Indeed, it is actually an instance of an **exact sequence**, which will be the topic of the next sections in this course.

1.5 Where are we going?

The main theorem we will aim for this week is the following:

Theorem 1.17. *Let I be* **any** *ideal in $R = \mathbb{R}[x_1, \ldots, x_n]$. Then the Hilbert Series of R/I is given by*

$$HS(R/I) = \frac{p(t)}{(1-t)^n}$$

for some polynomial $p(t)$ with integer coefficients. Furthermore, if $p(t)$ is put into **lowest terms** *then*

$$HS(R/I) = \frac{h(t)}{(1-t)^d}$$

where d is the dimension of the **algebraic variety defined by** *I.*

In other words, the number of "dots under the staircase" is always given by a nice rational function. In the exercises we'll explore more of the ramifications of this.

Summary:

- We are dealing with polynomial rings called $R = \mathbb{R}[x_1, \ldots, x_n]$.
- There are infinitely many polynomials, but if we look in a given degree, then degree d polynomials in R form a finite-dimensional vector space R_d.
- We also studied **ideals** which are sets that are closed under addition and scalar multiplication. We've mostly studied monomial ideals and will keep studying these in the coming days.
- We learned about **quotient rings** R/I which are what happens when we "kill" (or set equal to zero) all the elements in an ideal I.
- Whether we're looking at I or R or R/I we can **count** the number of independent polynomials of a given degree d. This function is called the Hilbert Function. If we encode the Hilbert function as coefficients in a power series we get something called the Hilbert Series.
- We saw that

$$HF_R = HF_{R/I} + HF_I,$$

$$HS(R) = HS(R/I) + HS(I),$$

$$HS(R) = \frac{1}{(1-t)^n}.$$

- We stated our Main Theorem that the Hilbert Series of any homogeneous ideal I in R (or a quotient R/I) is a rational function with denominator $(1-t)^n$. More generally this is also true for the Hilbert series of any graded R-module.)

1.6 Exercises for Day 1

Exercise 1. Let $R = \mathbb{R}[x, y, z]$ and $I = (x^2, y^2, z^3)$.

a. Write down all the nonzero monomials in R/I in each degree d.

b. Similarly, write down the monomials **in** I in each degree (for small d, say) (it might help to keep R/I and I in two columns of a table.

c. Why does it make sense that

$$HF(R/I) + HF(I) = HF(R)$$

and thus

$$HS(R/I) + HS(I) = \frac{1}{(1-t)^3}.$$

(A sketch of a proof of this is in the notes)

d. Use this to find an expression for $HS(I)$. (No real need to get a common denominator).

e. Are you convinced that $HS(I)$ and $HS(R/I)$ are each of the form $\frac{p(t)}{(1-t)^3}$?

Exercise 2.

a. Prove that in any polynomial ring $\mathbb{R}[x_1, \ldots, x_n]$ the set of homogeneous polynomials of degree d forms a vector space. Show that its dimension is $\binom{n+d-1}{d}$. You may have seen this in a discrete math class in terms of "bars and stars" if that rings any bells. In any case you might also want to try counting these things yourself in 3 variables to get used to the sequence $1, 3, 6, 10, 15, \ldots$.

b. Prove that the Hilbert Series of $\mathbb{R}[x_1, \ldots, x_n]$ is equal to $\dfrac{1}{(1-t)^n}$. Try proving it in two different ways:

- Take derivatives of your formula for $HS(\mathbb{R}[x_1, \ldots, x_n]$ and show by induction that this can help compute the Hilbert series for the polynomial ring of one bigger dimension.
- Can you relate the number of polynomials of degree d in n variables to the number of polynomials of degree $\leqslant d$ in $n-1$ variables? (Hint: the answer should be a resounding yes!) Then can you somehow make sense of the equation

$$\frac{1}{1-t} \cdot \frac{1}{(1-t)^n} = \frac{1}{(1-t)^{n+1}}$$

Exercise 3.

a. Consider the sequence $\{1, 2, 4, 8, \ldots, 2^n, \ldots\}$. What is the generating function for this sequence?

b. Consider the Fibonacci sequence: $1, 1, 2, 3, 5, 8, \ldots$ where each term is the sum of the previous terms. Let

$$F = 1 + t + 2t^2 + 3t^3 + 5t^4 + \ldots.$$

Calculate the series $F - tF - t^2F$. (Your answer should be very simple). Now solve for F. You've just found a closed-form expression for the generating function of the Fibonacci numbers.

Notice in these examples, these generating functions were **not** of the form

$$\frac{\text{polynomial with integer coefficients}}{(1-t)^n}.$$

This means that these sequences do not arise as the Hilbert function of any module over a polynomial ring.

Exercise 4. Compute the Hilbert Function or Series for the following rings

a. $\mathbb{R}[x, y]/(x^2, y^2)$

b. $\mathbb{R}[x, y]/(x^2, xy, y^3)$

c. (Draw the staircase diagrams for the above examples. If you'd like, can you find other examples of different ideals that have the same Hilbert function?)

d. $\mathbb{R}[x, y, z]/(xy, xz, yz)$

Exercise 5.

a. Show that if I is a principal ideal generated in degree e then the Hilbert Series of I is equal to $\dfrac{t^e}{(1-t)^n}$.

b. Let f be a polynomial of degree d in $R = k[x_1, \ldots, x_n]$. Compute $HS(R/(f))$. Your answer should only depend on the degree of f.

Exercise 6. Compute the Hilbert series of $\mathbb{R}[x, y, z]/(x^2, y^3, z^4)$. Can you compute the Hilbert series of

$$\mathbb{R}[x_1, \ldots, x_n]/(x_1^2, x_2^3, \ldots, x_n^{n+1})?$$

Try using Macaulay2 to test some examples. Note that the commands might help:

```
apply(10, i $->$ hilbertFunction(i,R/I))

apply(10, $i ->$ hilbertFunction(i,module(I)))

hilbertSeries(I,Reduced$=>$true)
```

2 How Many Generators Does An Ideal Have - and Why Do We Care?

2.1 A strategy for computing the Hilbert series

Let's restate our **goal** from last time: If I is an ideal in $R = \mathbb{R}[x_1, \ldots, x_n]$ then the Hilbert series of R/I is a rational function $p(t)/(1-t)^n$ where $p(t)$ is a polynomial with integer coefficients.

We also saw that $HS(R/I) = HS(R) - HS(I)$. Our reason for that was simply that if we take bases for R/I and I then their union will be a basis for R. Today we will take a slightly more abstract view - our first step towards something called **homological algebra.**

Definition 2.1. We say that a sequence of maps

$$\cdots \to M \xrightarrow{\alpha} N \xrightarrow{\beta} P \to \cdots$$

exact at N if $\operatorname{im}\alpha = \ker\beta$. A sequence is **exact** if it is exact at every spot.

Example 2.2.

- Consider the maps:

$$0 \longrightarrow \mathbb{R}^2 \xrightarrow{\quad\alpha\quad} \mathbb{R}^3 \xrightarrow{\quad\beta\quad} \mathbb{R}^2$$

  where

$$\alpha\left(\begin{bmatrix} a \\ b \end{bmatrix}\right) = \begin{bmatrix} 0 \\ 0 \\ a \end{bmatrix}, \quad \beta\left(\begin{bmatrix} x \\ y \\ z \end{bmatrix}\right) = \begin{bmatrix} x \\ y \end{bmatrix}.$$

  The map β is the projection onto the xy plane in $\mathbb{R}^3$. Notice that the image of α is the z-axis, which is also the kernel of β. This means that the sequence is **exact** at $\mathbb{R}^3$.

  But what about on the left. Is the kernel of α equal to the image of that first (zero) map? No, the kernel of α includes vectors like $\begin{bmatrix} 0 \\ \star \end{bmatrix}$ which are nonzero for many choices of $\star$. Thus the sequence is not exact at the $\mathbb{R}^2$ (on the left).

- If $\mathbb{R}^m \xrightarrow{\alpha} \mathbb{R}^n \to 0$ is exact, then it means that $\operatorname{im}\alpha = \mathbb{R}^n$, i.e. that α is surjective.
- If $0 \to \mathbb{R}^m \xrightarrow{\alpha} \mathbb{R}^n$ is exact, then it means that $\ker\alpha = 0$, i.e. that α is injective.
- The following is an exact sequence:*

$$\mathbb{R}^1 \xrightarrow{t\mapsto(\cos t, \sin t)} \mathbb{R}^2 \xrightarrow{(x,y)\mapsto x^2+y^2-1} \mathbb{R}^1.$$

- The following is an exact sequence.

$$0 \to I \to S \to R/I \to 0.$$

  Exact sequences with 0s on both ends and three terms in the middle are called **short exact sequences**.

Short exact sequences are of great importance in algebra. Suffice it to say, they come up a lot! But for now, let us just consider the following fact.

*technically this example doesn't fit into our framework since the maps aren't linear, but we include it because it captures the notion of kernel and image well.

Proposition 2.3. *Suppose that we have a short exact sequence of things (actually called modules)*

$$0 \to M \to N \to P \to 0$$

such that these maps **preserve degrees of elements**. *Then*

$$HS(P) = HS(N) - HS(M).$$

In particular, since $0 \to I \to S \to R/I \to 0$ *is exact* **and preserves degrees**, *we have that* $HS(R/I) = HS(R) - HS(I)$.

We will define what a module is in the section chapter of these notes, but for now you should think of this proposition as a generalization of our discovery from Chapter 1 - that $HS(R/I) = HS(R) - HS(I)$.

This now motivates a strategy for us:

- If we want to calculate the Hilbert series of R/I, we can use a short exact sequence to reduce this to computing the Hilbert series of R (which we know) and I.
- How can we continue this process?

One way to continue this process is to introduce a new object R^r called the free module of rank r.

Definition 2.4. Let $R = \mathbb{R}[x_1, \ldots, x_n]$ be a polynomial ring in n variables. Then R^r will denote the **free module** of rank r. This consists of all ordered r-tuples of elements of R, that is

$$R^r = \left\{ \begin{bmatrix} f_1 \\ \vdots \\ f_r \end{bmatrix}, \quad f_i \in R \right\}.$$

We will talk about the elements of R^r as vectors and by e_i we will denote the vectors whose only nonzero entry is 1 in the ith position. E.g. $e_2 = (0, 1, 0, 0, \ldots, 0)$.

Example 2.5. If $R = \mathbb{R}[x, y]$ then R^2 contains things like (x, y), $(-y, x)$, $(0, 0)$, $(1, 0)$, $(x^3, -x + y^{100})$. Note that there is no restriction as to what can appear in the first position and what can appear in the second.

Definition 2.6. We define the "degree d piece" of R^r to be those vectors $(f_1, \ldots, f_r)$ all of whose entries are of degree d. As before, we may define the Hilbert Function and Hilbert Series for R^r as

$$HF_{R^r}(d) = \text{the dimension of the vector space spanned by the degree } d \text{ pieces of } R^r.$$

Example 2.7. Let's look at $R = \mathbb{R}[x, y]$ and try to compute the Hilbert function of R^3. Remember that the Hilbert Function of R is just $\{1, 2, 3, 4, 5, 6, 7, 8\}$. For R^3 we'll just list the (independent) elements of each degree:

degree 0: $(1, 0, 0), (0, 1, 0), (0, 0, 1)$
degree 1: $(x, 0, 0), (0, x, 0), (0, 0, x), (y, 0, 0), (0, y, 0), (0, 0, y)$
degree 2: $(x^2, 0, 0), (0, x^2, 0), (0, 0, x^2), (xy, 0, 0), (0, xy, 0), (0, 0, xy), (y^2, 0, 0), (0, y^2, 0), (0, 0, y^2)$.

You see a pattern emerge. That the Hilbert function of R^3 is just three times the Hilbert function of R.

Proposition 2.8. *Let* $R = \mathbb{R}[x_1, \ldots, x_n]$. *The Hilbert Series of* R^r *is just equal to* r *times the Hilbert Series of* R.

$$HS(R^r) = \frac{r}{(1-t)^n}.$$

Proof. The proof is left to the reader. But actually the reader is just encouraged to do some examples to understand what is true. □

Example 2.9. Consider the ideal $I = (x^2, y^2)$. Now let's see if we can calculate the Hilbert series of I. We first consider the map $\beta : R^2 \to I$ given by $\beta(\begin{bmatrix} a_1 \\ a_2 \end{bmatrix}) = a_1x^2 + a_2y^2$. This map is surjective, (but it does not preserve degree!) Nonetheless we can compute the kernel of β and see that it is $K = \{(ay^2, -ax^2) \in R^2 : a \in R\}$. This seems like success!

Proposition 2.10. *If I is an ideal generated by c elements $(f_1, \ldots, f_c)$ then the map*

$$\beta : R^c \to I, \quad \beta(r_1, \ldots, r_c) = r_1f_1 + \cdots + r_cf_c$$

is surjective. If its kernel is K, then the following is a short exact sequence

$$0 \to K \to R^c \to I \to 0.$$

- We have reduced the computation of the Hilbert Series of R/I to computing that of I.
- If we can find some surjective map $\beta : R^r \to I$, then this will give rise to a short exact sequence

  $$0 \to K \to R^r \to I \to 0.$$

  where K is the kernel of β.
- Then by the magic of short exact sequences, this should reduce our computation to computing $HS(K)$.

There are two issues in the above. First - how do we know there is a surjective map from R^r to I. This is tantamount to saying that I has a finite number of generators. Secondly, we need to deal with the fact that these maps don't preserve degree (this might seem more major, but it's actually just a small technical problem that we'll address on the final day).

2.2 How many generators does an ideal have?

It's important to realize that every nonzero ideal in $\mathbb{R}[x_1, \ldots, x_n]$ has infinitely many elements. Indeed, it's even infinite dimensional as a vector space. (We need all those dots in the picture!) However, all of the ideals that we have seen so far were **finitely generated** meaning that there was a finite set of polynomials such that any polynomial in the ideal could be written as a combination **with polynomial coefficients** of those polynomials.

Example 2.11. Let I be the set of all polynomials with constant term 0. We can check that this set forms an ideal. (It's closed under addition and scalar multiplication). Can we find a set of generators for this ideal? It turns out that

$$I = (x_1, x_2, \ldots, x_n).$$

Indeed, any polynomial with a zero constant term can be written as a combination of $x_1, \ldots, x_n$ and conversely any combination of the form

$$g_1x_1 + \cdots + g_nx_n$$

will have a constant term of zero. It's because these coefficients are allowed to be polynomials (and not just constants) that give us this freedom.

In the previous example we saw the first time that we defined an ideal in a way other than "giving finitely many generators." Instead we gave a holistic description (the constant term is zero). In general there are lots of ways to define an ideal and depending on the definition it's not at all clear whether that ideal is finitely generated. This leads us to our first major question:

Question 2.12. If I is an ideal in $\mathbb{R}[x_1, \ldots, x_n]$ then is I finitely generated?

Example 2.13. Consider the ideal I in $\mathbb{R}[x]$ defined by:

$$I = (x^2 - 1, x^3 - 1, x^5 - 1, \ldots, x^p - 1, \ldots, \quad \text{where } p \text{ is prime})$$

At first glance it's not clear whether or not I can be generated by a finite number of polynomials. For instance, is I generated by the first 1000 polynomials of the form $x^p - 1$? If so, then is it obvious how to write $x^{7927} - 1$ (that's the 1001st prime) as a combination of the previous polynomials? As it turns out, the ideal I is in fact generated by a single element of I!

$$I = (x - 1).$$

Why is this true? Well first notice that every generator of I is a multiple of $(x - 1)$, so it's true that $I \subset (x - 1)$. Now for the other inclusion we just need to show that $x - 1 \in I$. But notice that

$$(x^3 - 1) - x(x^2 - 1) = x - 1$$

and the left hand side is evidently in I.

Example 2.14. Let's move on to ideals with 2 variables, for instance our staircase diagrams. In this case it is possible to have arbitrarily many generators. Indeed, the ideal

$$I = (x^n, x^{n-1}y, x^{n-2}y^2, \ldots, xy^{n-1}, y^n)$$

requires all $n + 1$ of those generators. (Exercise: What does the staircase picture of this ideal look like?) So if we wanted to, we could write down an ideal in two variables that requires a million generators.

Example 2.15. Consider the following ideal

$$I = (x^{2p+1} - x^{p-2}y^{p+3} + y^{2p+1}, \text{ where } p \text{ is prime and } p > 500).$$

This ideal is again defined by infinitely many polynomials and it is wildly unclear how many generators this ideal needs - perhaps it needs all infinitely many of these. I'm actually not sure how many generators this ideal needs - can you figure it out? I've checked that if you only go up to $p < 6000$ then the ideal of all those polynomials is in fact generated by just four polynomials (see below for the Macaulay2 readout):

```
i1 : R = QQ[x,y];

i2 : I = ideal (select(6000, p-> isPrime p  and p > 500)/(p-> x^(2*p+1) - x^(p-2)*y^(p+3) + y^(2*p+1)));

o2 : Ideal of R

i3 : mingens I

o3 = | x1007-x501y506+y1007 x513y506-x507y512-x12y1007+y1019 x30y1013-x18y1025-x12y1031+y1043
x511y536-x509y538+x22y1025-x20y1027+x16y1031-x14y1033-x10y1037+x8y1039-2x4y1043+x2y1045+y1047 |

             1       4
o3 : Matrix R  <--- R
```

In general now imagine an ideal in n variables, defined in some way - perhaps as the kernel of a ring map, or perhaps with an ostensibly infinite generating set. With that in mind, hopefully the following theorem comes as a reasonable surprise:

Theorem 2.16 (Hilbert's Basis Theorem)**.** *In a polynomial ring* $\mathbb{R}[x_1, \ldots, x_n]$ **every** *ideal is finitely generated.*

There are many proofs of the Hilbert Basis theorem. For those interested in computation, I recommend reading the book "Ideals, Varieties and Algorithms" by Cox, Little and O'Shea [3] There the authors develop the theory of Gröbner bases. After this is done, they are able to reduce the proof of the Hilbert Basis Theorem from the general case to the case that I is generated by (potentially infinitely many) monomials. Then it's a combinatorial argument to prove that such an ideal must be finitely generated. Even this isn't trivial though. Before we begin the proof, we mention that rings where every ideal is finitely generated are called **Noetherian** rings after Emmy Noether.

Proof. Notice that e.g. $\mathbb{R}$ and $\mathbb{R}[x]$ are both Noetherian as worked out in the examples above, so if we can prove

$$R \text{ Noetherian } \implies R[y] \text{ Noetherian}$$

then by induction we will have that $\mathbb{R}[x_1, \ldots, x_n]$ is Noetherian.

So suppose that R is a Noetherian ring and suppose that I is an ideal in $R[y]$ that is not finitely generated. We will hope for a contradiction. As before, suppose that there is a sequence of elements $f_1, f_2, \ldots$ such that $f_i \in I \backslash (f_1, \ldots, f_{i-1})$ Further, suppose that in this process when we are finding f_i, we choose f_i to be of $\boxed{\textit{smallest}}$ possible degree in y. So for instance, to find f_8 we look for polynomials in I that are not in $(f_1, \ldots, f_7)$ (there must be some since I is not finitely generated) - take one of lowest degree. Then we have that

$$\deg f_1 \leqslant \deg f_2 \cdots$$

Now we want to somehow use our hypothesis that R is Noetherian. Well remember that each polynomial f_i is just some polynomial in y with coefficients in R. So it's something like

$$f_i = (\text{leading coefficient}) y^m + \ldots + a_0.$$

Let a_i be that leading coefficient of f_i. Note that $a_i \in R$. Then we can form a chain of ideals in R. Let J denote the ideal generated by all the a_i.

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

Now since R is Noetherian, J is finitely generated. So that means that $J = (a_1, \ldots, a_{N-1})$ for some N. (Think about why this is true).

This means that a_N is in the ideal generated by the previous a_i, say

$$a_N = \sum_{j=1}^{N-1} r_j a_j, \quad r_j \in R.$$

Now let's try to cook up a polynomial in y. Let's try

$$g = \sum_{j=1}^{N-1} r_j x^{\deg f_N - \deg f_i} f_i.$$

What is going on? Well the leading coefficient of this polynomial is going to have degree $\deg f_N$, and the leading coefficient will be a_N. (Think about why this is true - the leading coefficient of f_i is a_i.) Note that $g \in (f_1, \ldots, f_{N-1})$ and by construction we chose f_N to not be in $(f_1 \ldots, f_{N-1})$. So this means that $f_N - g$ is not in $(f_1, \ldots, f_{N-1})$, but since the leading terms of f_N and g are the same, it means that $f_N - g$ has lower degree. But this is a contradiction since we chose f_N to be the $\boxed{\textit{smallest}}$ possible degree with this property. $\square$

2.3 Summary

In this section we have

- Defined exact sequences and discussed how they help us compute Hilbert Series
- We have seen that every ideal in $\mathbb{R}[x_1, \ldots, x_n]$ is finitely generated.
- This finite generation allows us to construct short exact sequences

$$0 \to K \to R^c \to I \to 0$$

  and thus reduce our Hilbert function computation to computing that of K.

Still TODO are the following:

- We've been a bit handwavey about what happens when the degrees aren't preserved in these exact sequences. We'll see this isn't a big deal, but is something to examine.
- What next? What if K is even more complicated that I? (it probably is) Can we repeat this process? (yes) will it ever end? (we'll see!)

2.4 Exercises for Day 2

Exercise 1. If your group would like to talk through the proof of the Hilbert Basis Theorem, please check out the proof in the notes. Also you can work through the proof that $(x^p - 1,\ p \text{ is prime}) = (x - 1)$.

Exercise 2.

a. Consider the following maps of "$\mathbb{Z}$ modulo 4" where each map is "multiply by 2"

$$\cdots \xrightarrow{(2)} \mathbb{Z}/4\mathbb{Z} \xrightarrow{(2)} \mathbb{Z}/4\mathbb{Z} \xrightarrow{(2)} \mathbb{Z}/4\mathbb{Z} \xrightarrow{(2)} \cdots$$

Show that this is exact everywhere.

b. Let V and W be vector spaces. Find appropriate definitions of α and β so that

$$0 \longrightarrow V \xrightarrow{\alpha} V \oplus W \xrightarrow{\beta} W \longrightarrow 0$$

is exact. Recall that $V \oplus W$ consists of all vectors $\begin{bmatrix} v \\ w \end{bmatrix}$ such that $v \in V$ and $w \in W$.

Exercise 3. In this exercise you'll see why if $0 \longrightarrow M \xrightarrow{\alpha} N \xrightarrow{\beta} P \longrightarrow 0$ is a short exact sequence that preserves degree then $HS(P) = HS(N) - HS(M)$.

a Let M_d, N_d, P_d denote (respectively) the vector space of degree d elements of M, N and P. Since α and β preserve degrees means that for any d, we have an exact sequence

$$0 \longrightarrow M_d \xrightarrow{\alpha} N_d \xrightarrow{\beta} P_d \longrightarrow 0$$

of **vector spaces**.

b Conclude that you may reduce to the claim: If

$$0 \longrightarrow U \xrightarrow{\alpha} V \xrightarrow{\beta} W \longrightarrow 0$$

is an exact sequence of vector spaces then $\dim W = \dim V - \dim U$.

c What does the rank nullity theorem say about the map α? About the map β?

d Use your answers from above to prove that $\dim W = \dim V - \dim U$. Your proof should use every part of the short exact sequence.

e As an application of Exercise 2 b) use this to prove that $HS(R^2) = 2HS(R)$.

(Optional - probably best to come back to this later) Can you generalize this result: Show that if

$$0 \to V_n \to V_{n-1} \to V_{n-2} \to \cdots \to V_0 \to 0$$

is an exact sequence of vector spaces then

$$\dim V_0 = \dim V_1 - \dim V_2 + \dim V_3 \pm \cdots + (-1)^{n+1} \dim V_n.$$

Exercise 4. If you know that for all e, the HF of A in degree d is equal to the HF of B in degree $d + e$ for all e then which of the following is true

$$HS(A) = t^e HS(B), \quad \textit{or} \quad t^e HS(A) = HS(B)?$$

Exercise 5. Let I be an ideal such that

$$HS(R/I) = (1 - 3t^2 + 2t^3)/(1-t)^3.$$

Find an explicit formula for the coefficient of t^N for N large. Hint: First factor and then use the fact that $1/(1-t) = \sum t^j$.

Exercise 6. Suppose that $f : T \to R$ is a **ring homomorphism**, that is, it's a map that preserves the ring properties:

$$f(ab) = f(a)f(b), \quad f(a+b) = f(a) + f(b).$$

Show that the kernel of f is an ideal in T.

Exercise 7.

1. Can you find two different staircase diagrams that have the same Hilbert function (i.e. dots under the staircase)? If so, write down their Hilbert series using the formula from the notes:

$$HS(R/I) = \frac{1 - \sum_{\text{lower steps}} t^{\text{deg. step}} + \sum_{\text{upper steps}} t^{\text{deg. step}}}{(1-t)^2} \tag{2.1}$$

   What do you notice? (You should see that some dots will cancel in the numerator. These are sometimes called **ghost terms**)

2. By hand, compute the Hilbert series for the quotient of $\mathbb{R}[x,y]$ by the following three ideals:

$$I = (x^2, y^2), J = (x^2, xy, y^3), L = (x^2 + xy, y^2).$$

   For the third one, the ideal is not a monomial ideal so be careful. You can check your answers with Macaulay2. Note that the command `hilbertSeries I` computes the Hilbert series of R/I. If you want the Hilbert series of I itself you can type `hilbertSeries module I`. You can also try the commands

```
hilbertSeries(I, Reduced=> true)
```

   to put things in lowest terms.

Exercise 8. Do you want to try something called a "diagram chase"? If you feel like the answer to this question might be yes, then this could be the exercise for you! It's something called the Five Lemma, and it uses the words **commutative diagram** which means e.g. in the following diagram that no matter how you get from A_1 to B_2, you'll end up in the same place. I.e. that if $x \in A_1$ then $t_2(f_1(x)) = g_1(t_1(x))$. With that in mind, here goes!

Suppose the following is a commutative diagram with exact rows - that means the rows are exact sequences, (each):

$$\begin{array}{ccccccccc}
A_1 & \xrightarrow{f_1} & A_2 & \xrightarrow{f_2} & A_3 & \xrightarrow{f_3} & A_4 & \xrightarrow{f_4} & A_5 \\
\downarrow{\scriptstyle t_1} & & \downarrow{\scriptstyle t_2} & & \downarrow{\scriptstyle t_3} & & \downarrow{\scriptstyle t_4} & & \downarrow{\scriptstyle t_5} \\
B_1 & \xrightarrow{g_1} & B_2 & \xrightarrow{g_2} & B_3 & \xrightarrow{g_3} & B_4 & \xrightarrow{g_4} & B_5
\end{array}$$

Then prove:

a. If t_2 and t_4 are surjective and t_5 is injective, then t_3 is surjective.

b. If t_2 and t_4 are injective and t_1 is surjective, then t_3 is injective.

c. Conclude that if t_1, t_2, t_4, t_5 are isomorphisms then t_3 is an isomorphism.

You can assume that all of the A_i and B_i are vector spaces and that all the maps are **linear transformations**. (All that's really important though is that e.g. $f_1(x+y) = f_1(x) + f_1(y)$.)

3 Modules

We begin with comparing how linear algebra works over a field (the study of vector spaces) and over a polynomial ring (the study of **modules**).

3.1 What is a module?

We begin by comparing some of the properties of vector spaces as compared with those of modules.

Linear Algebra over $\mathbb{R}$	**Linear Algebra over $\mathbb{R}[x_1, \ldots, x_n]$**
1) We study **vector spaces** V. $$v, w \in V, \quad c \in \mathbb{R} \text{ a scalar.}$$	1) We study **modules** M. $$m, n \in M, \quad f \in R \text{ a polynomial (scalar)}$$
V is closed under addition and scalar multiplication: $$v + w \in V, \quad cv \in V.$$	M is closed under addition and scalar multiplication: $$m + n \in M, \quad fm \in M.$$
(and there are a bunch of axioms)	(and there are a bunch of axioms)
2) The maps we care about between vector spaces are **linear maps** $T : V \to W$ $$T(v + w) = T(v) + T(w), \quad T(cv) = cT(v).$$	2) The maps between modules are **linear maps** $T : M \to N$ $$T(m + n) = T(m) + T(n), \quad T(fm) = fT(m).$$
3) Vector spaces have subspaces: $U \subset V$ is a subspace if U is closed under addition and scalar multiplication.	3) Modules have sub-modules: $P \subset M$ is a submodule if P is closed under addition and multiplication by polynomial (scalars).
4) A basis for V is a set $\{v_1, \ldots, v_n\}$ that spans V that is linearly independent. (i.e. the only solution to $$c_1 v_1 + \cdots + c_n v_n = 0$$ is when all the c_i are zero.)	4) A basis for M is a set $\{m_1, \ldots, m_n\}$ that spans M that is linearly independent. (i.e. the only solution to $$c_1 m_1 + \cdots + c_n m_n = 0.$$ is when all the c_i are zero.)
5) Every vector space has a basis.	5) It is madly false that every module has a basis!

Definition 3.1. (First Definition) Let R be a polynomial ring. Then an R-module M is a mathematical object defined so that we can add elements of M and multiply elements of M by polynomials in R (and some basic rules apply).

Example 3.2. Let R be a polynomial ring and let I be an ideal. Then the following are all R-modules:

- R;
- I;
- R/I;
- Free modules R^r

There are modules other than these, but for now these modules will be good for our purposes.

Example 3.3. What does it mean to be a sub-module of R? A set $M \subset R$ is a submodule if for $f, g \in M$ and $r \in R$, $f + g \in M$ and $rf \in M$. This means that

- Submodules of R are ideals.

Example 3.4. The module R is generated by one element 1. But submodules (i.e. ideals) can require many many generators.

3.2 Do Modules have a basis?

Example 3.5. Does the ideal $I = (x, y)$ have a basis? The answer is no. First, it's clear that there can be no basis of size 1. (No single polynomial in I can span all of I). Now suppose there is a basis of size $\geqslant 2$. Then the basis will contain two polynomials, call them f and g. But then these are not linearly independent. Indeed $g(f) + (-f)g = 0$.

Ideals with more than two generators do not have a basis (as R-modules)! We can always write down linear dependence relations on polynomials f, g:

$$(g)f + (-f)g = 0$$

.

Definition 3.6. The module R^r is called **free module of rank** r. This module has a basis (verify this) $e_1, \ldots, e_r$ where $e_1 = [1, 0, \ldots, 0], \ldots, e_r = [0, \ldots, 0, 1]$.

Proposition 3.7. *If a module M has a finite basis of cardinality r then $M \cong R^r$.*

3.3 Maps between Modules

Now that we have modules, we will want to find **maps between modules**. Let's imagine we have a map between modules $\phi : M \to N$. We could imagine lots of such functions that randomly jumble the elements of M and N together. But rarely do we study such functions.

- In real analysis we endeavor to study things like continuous functions. Why is this? Well the real numbers have a beautiful property of being complete - points can get arbitrarily close to one another. In a sense, continuity preserves this closeness. If x and y are sufficiently close to each other and f is continuous, then we can guarantee, say that $f(x)$ and $f(y)$ are within 0.0001 of each other. Continuous preserves something we care about. And whoa, it turns out that continuous functions are great functions to study.

- In linear algebra we study maps that are linear - things like $T(u + v) = Tu + Tv$, $T(cv) = cTv$. Why is this? Well it's because in a vector space we might not have continuity, but we definitely have a way to add vectors and we have a way to multiply by scalars. It's reasonable to want our transformations to preserve this. So if $u + v = w$ then it's reasonable to want that $Tu + Tu = Tw$. This is precisely what linear maps do. And if you set about studying linear maps you'll wind up typing a linear algebra textbook and discover all sorts of beautiful things!

- In a module M we can add elements and multiply by scalars (polynomials) so we will require that a **map** $\phi : M \to N$ **of modules** be **linear** in the sense that if $m_1, m_2, \in M$ and $f \in R$ then

$$\phi(m + n) = \phi(m) + \phi(n)$$

$$\phi(fm) = f\phi(m).$$

3.4 Noetherian Modules

Remember, throughout these notes $R = \mathbb{R}[x_1, \ldots, x_n]$.

Definition 3.8. We say that an R-module M is Noetherian if every sub-module of M is finitely generated.

Proposition 3.9. *Since every ideal is finitely generated, R is a Noetherian R-module.*

Proposition 3.10. *If $0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$ is a short exact sequence of R-modules then M is Noetherian if and only if M' and M'' are both Noetherian.*

Proof. Suppose that M is Noetherian. Then suppose that M' has a submodule $N \subset M'$ that if not finitely generated. Then consider the image $\alpha(N) \subset M$. This has to be finitely generated since M is Noetherian. This means that some set $\alpha(n_1), \ldots, \alpha(n_g)$ must generate $\alpha(N)$. Now you can check that $(n_1, \ldots, n_g)$ must generate N. Indeed, if $n \in N$ then $\alpha(n)$ is a combination of the $\alpha(n_i)$. Thus

$$\alpha(n) = \sum c_i \alpha(n_i) = \sum \alpha(c_i n_i)$$

By the fact that α is injective, we must have that n is a linear combination of the n_i, so that they generate all of N.

The rest of the proof is left as an exercise. □

Corollary 3.11.

1. *If $\phi : M \to N$ is a map of R-modules and M is Noetherian then $\ker \phi$ is Noetherian.*
2. *Free modules R^r are Noetherian.*
3. *Any R-module that is finitely generated is Noetherian.*

Proof. a) follows immediately from the previous proposition and the fact that

$$0 \to \ker \phi \to M \to \operatorname{im} \phi \to 0$$

is a short exact sequence.

For b) we proceed by induction. For instance, to see that R^2 is Noetherian, consider the exact sequence

$$0 \to R^1 \to R^2 \to R^1 \to 0$$

where the first maps sends $(f) \mapsto (f, 0)$ and the second sends $(f, g) \mapsto (g)$. The reader can verify that this is a short exact sequence. Since both the module on the left and right are Noetherian, so must the module in the middle. We to continue the induction we just note that there is an exact sequence

$$0 \to R^r \to R^{r+1} \to R \to 0$$

so if we know that R^r is Noetherian, then the lemma guarantees that R^{r+1} is Noetherian.

(c) This is a great exercise. □

3.5 Exercises for Day 3

Exercise 1. Let $M = (f)$ be a principal ideal. Prove that M has a basis, and thus that M is isomorphic to R. Can you find an explicit isomorphism $\phi : R \to (f)$?

Exercise 2. Recall that if $R = \mathbb{R}[x_1, \ldots, x_n]$ then by R_d we mean the **vector space of homogeneous polynomials of degree d.**

In this exercise we're going to put a funky (but very useful) different grading on R. We will denote this funky grading by $R(e)$.

- As a module, $R(e)$ is just the same as R. It's the degrees of the elements which are different.
- The degree d piece of $R(e)$ is equal to R_{d+e}. That is

$$R(e)_d = R_{d+e}.$$

If $R = \mathbb{R}[x, y]$

a. Write down a basis for the following:

$$R(3)_1, \quad R(-3)_4, \quad R(-2)_2, \quad R(-2)_1$$

b. In $R(-4)$ what is the degree of the polynomial x^3?

c. In $R(-d)$ what is the degree of the polynomial 1?

d. Does the map $\phi : R \to R$ defined by $\phi(f) = x^2 f$ preserve degree? (No)

e. Does the map $\phi : R(-2) \to R$ defined by $\phi(f) = x^2 \cdot f$ preserve degree? (Yes!) Indeed, check this: what is the degree of x^2y^2 in $R(-2)$? What is the degree of $\phi(x^2y^2)$ in R?

f. In the module $R(-2) \oplus R(-3)$ convince yourself that the vector $\begin{bmatrix} x^2 \\ y \end{bmatrix}$ has degree 4.

g. Prove that the map $\phi : R(-2) \oplus R(-3) \to R$ defined by $\phi(\begin{bmatrix} a \\ b \end{bmatrix}) = ax^2 + by^3$ preserves degree. If you want, just check that $\begin{bmatrix} x^2 \\ y \end{bmatrix}$ (which has degree 4 by the previous part of this exericse) gets maped to something of degree 4 in R.

h. Prove that the Hilbert series of $R(-d)$ is $\cdot \frac{t^d}{(1-t)^2}$. (or more generally $\frac{t^d}{(1-t)^n}$.)

Exercise 3. Let $I = (x^2, xy^2)$. Consider the map $\phi : R^2 \to R$ defined by

$$\phi(\begin{bmatrix} a \\ b \end{bmatrix}) = ax^2 + bxy^2.$$

1. Convince yourself (or prove) that the image of ϕ is equal to I.
2. Calculate the kernel of ϕ. There should be one element that generates the kernel. All other elements in the kernel will be multiples of it.
3. Go to www.macaulay2.com and type

```
R=QQ[x,y]; I = ideal(x^2, x*y^2); C= res I; C.dd
```

Macaulay2 should display some output. The first line gives the **generators of** I. Next comes the generator of the kernel (as a column) vector. This should match very closely what you got.

Exercise 4. Let $I = (x, y, z)$ in $\mathbb{R}[x, y, z]$. Consider the map $\phi : R^3 \to R$ defined by

$$\phi(\begin{bmatrix} a \\ b \\ c \end{bmatrix}) = ax + by + cz.$$

1. Convince yourself (or prove) that the image of ϕ is equal to I.
2. Calculate the kernel K of ϕ. This will be more challenging that the previous example. Hint: Aim to find three different elements in the kernel: one with a zero in the first row, one with a zero in the second, and one with a zero in the third row. You might not be able to completely prove that you've computed the whole kernel, but your goal should be to find three independent elements $\begin{bmatrix} a \\ b \\ c \end{bmatrix}$ in the kernel.
3. Now if your three kernel elements are v_1, v_2, v_3 (thought of as vectors) then consider the map $\psi : R^3 \to R^3$ defined by the 3×3 matrix $\psi = [v_1\ v_2\ v_3]$. Convince yourself that the image of ψ is K. Can you compute the kernel of ψ?
4. Go to www.macaulay2.com and type

```
R=QQ[x,y,z]; I = ideal(x,y,z); C= res I; C.dd
```

Macaulay2 should display some output. The first line gives the **generators of** I. Next will come the three elements of the kernel that you found, these are presented as the columns of the matrix ψ. Finally, you get the kernel of ψ as a column matrix.

Exercise 5. Consider the short exact sequence,

$$0 \to M \to M \oplus N \to N \to 0$$

where the first map just sends m to $\begin{bmatrix} m \\ 0 \end{bmatrix}$ and the the second map sends $\begin{bmatrix} m \\ n \end{bmatrix}$ to n. These maps will preserve degrees (since we're not changing anything). Conclude that the Hilbert Function / Hilbert Series of $M \oplus N$ is equal to that of M plus that of N:

$$HS(M \oplus N) = HS(M) + HS(N).$$

1. Use this to calculate the Hilbert Series of $R(-d) \oplus R(-e)$.
2. What is the Hilbert Series of $R(-3)^4 \oplus R(-4)^2 \oplus R(-5)^7$?

Exercise 6. If you want to get some practice with the Noetherian property, complete the proof of Proposition 3.10 and Corollary 3.11 c.

4 Putting it all together: The Hilbert Syzygy Theorem

We are now ready for our triumphant conclusion - a discussion of the Hilbert Syzygy Theorem! Let's recall what we've done up to this point:

- $R = \mathbb{R}[x_1, \ldots, x_n]$ and I is an ideal.
- $0 \to I \to R \to R/I \to 0$ is an exact sequence.
- I is finitely generated (Hilbert Basis Theorem) say by b_1 elements.
- So there's an exact sequence $0 \to K_1 \to R^{b_1} \to I \to 0$
- Since R^{b_1} is Noetherian, we know that K_1 is finitely generated, say by b_2 elements. This means that we can find an exact sequence $0 \to K_2 \to R^{b_2} \to K_1 \to 0$.
- We can continue this process.

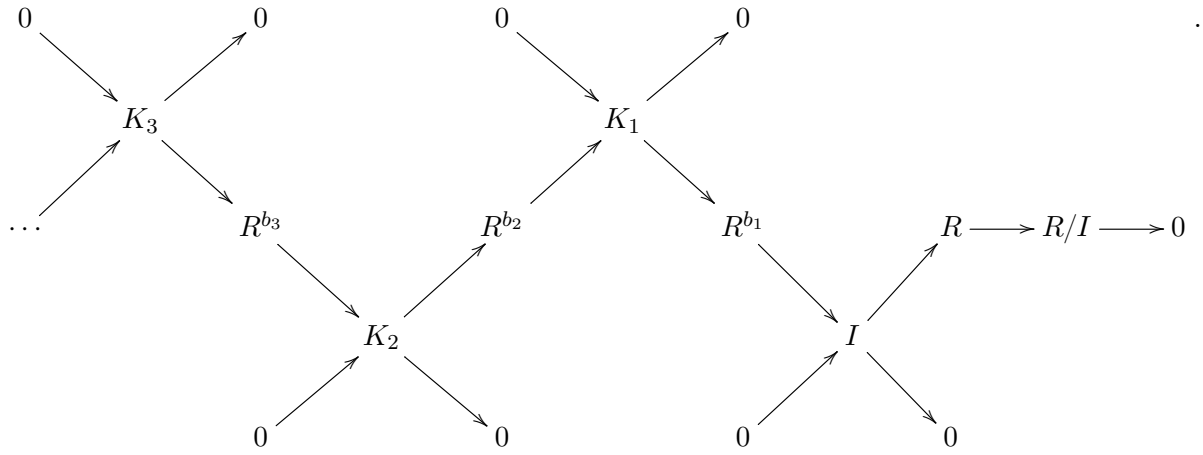
We put all this information into the following schematic:

Definition 4.1 (/Proposition)**.** If M is a finitely generated module over R then there process above will yield an **exact** sequence of maps:

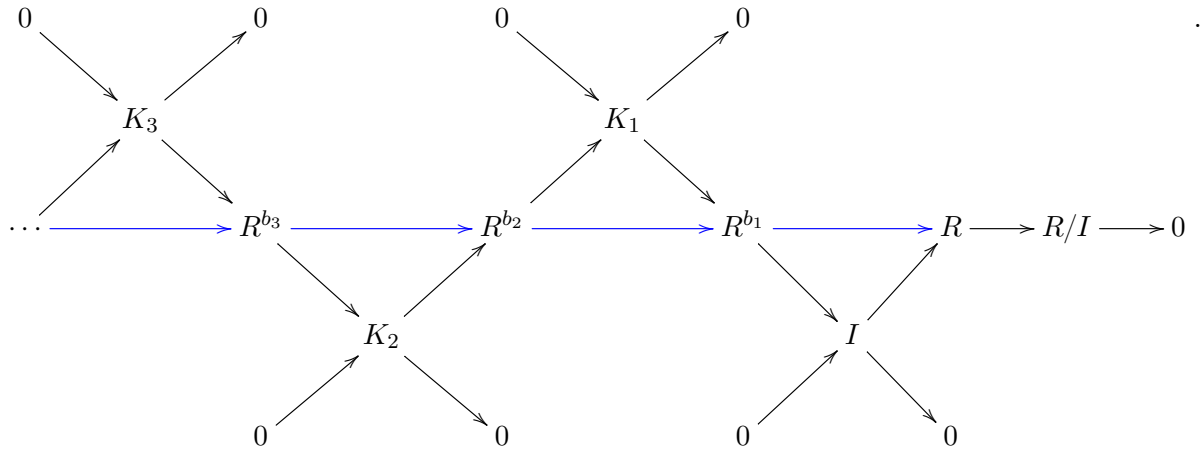
$$\cdots \longrightarrow R^{b_i} \longrightarrow R^{b_{i-1}} \longrightarrow \cdots \longrightarrow R^{b_1} \longrightarrow R \longrightarrow R/I \to 0.$$

This sequence of maps is called a **free resolution** of R/I.

Proof. If we put everything together in the algorithm we described above we'll get a smorgasbord of maps like this:



Notice that there is a well-defined map from R^{b_i} to $R^{b_{i-1}}$ obtained just by composing the diagonal maps. We will use those maps to define the new (blue) maps in the diagram below



Finally we remove the noise and are left with a sequence of maps.

$$\cdots \longrightarrow R^{b_3} \longrightarrow R^{b_2} \longrightarrow R^{b_1} \longrightarrow R \longrightarrow R/I \longrightarrow 0$$

Checking that this sequence is exact is an exercise. □

The numbers b_i that arise in this construction are called the **betti** numbers of R/I. There are many tantalizing questions about the betti numbers of R/I. By convention $b_0 = 1$.

Conjecture 1 (Buchsbaum-Eisenbud-Horrocks Rank Conjecture (1977) [2])**.** Suppose that $I \subset \mathbb{R}[x_1, \ldots, x_n]$ is an ideal and that I contains a power of each variable. Then $b_i \geqslant \binom{n}{i}$ for all i.

4.1 Examples

Let's do some examples on Macaulay2 and see if we see any patterns. We actually begin with the ideal that started it all - that staircase from Section 1:

$$I = (x^{10}, x^9y^2, x^7y^3, x^4y^4, xy^5, y^7).$$

The following code will return the resolution of R/I.

```
R = QQ[x,y];  I = ideal(x^10, x^9*y,x^7*y^3,x^4*y^4,x*y^5,y^7); res I

       1      6      5
o14 = R  <-- R  <-- R  <-- 0

      0      1      2      3
```

This means that $b_1(R/I) = 6$ and $b_2(R/I) = 5$. Let's try another example.

$$I = (x^2, y^3, z^4)$$

```
i1 : R = QQ[x,y,z];  I = ideal(x^2, y^3, z^4); C = res I

o16 : Ideal of R

       1      3      3      1
o17 = R  <-- R  <-- R  <-- R  <-- 0

      0      1      2      3      4
```

This means that $b_1 = 3, b_2 = 3, b_3 = 1$. In fact we can peek at the maps: by

```
i1 : C.dd

           1                    3
o25 = 0 : R  <----------------- R  : 1
               | x2 y3 z4 |

           3                           3
      1 : R  <----------------------- R  : 2
               {2} | -y3 -z4 0   |
               {3} | x2  0   -z4 |
               {4} | 0   x2  y3  |

           3                   1
      2 : R  <--------------- R  : 3
               {5} | z4  |
               {6} | -y3 |
               {7} | x2  |

           1
      3 : R  <----- 0 : 4
               0
```

Those numbers on the left are telling us the degrees of the maps. More on this in the next section.

Even ideals with as few as three generators can have a long resolution. For instance

$$I = (x^3, y^3, x^2z + xyw + y^2v)$$

has only three generators, but its resolution has length five:

```
R = QQ[x,y,z,w,v];  I = ideal (x^3, y^3,x^2*z + x*y*w+y^2*v); C = res I

       1      3      8      10      5      1
o34 = R  <-- R  <-- R  <-- R   <-- R  <-- R  <-- 0

      0      1      2      3       4      5      6
```

In fact, for each N there are examples of ideals I with three generators whose resolution has length N. However, if we look at all of our examples so far, they've all had a really nice property:

$$\text{the length of the resolution} \leqslant \text{the number of variables in } R.$$

This is the content of Hilbert's Syzygy Theorem:

Theorem 4.2 (The Hilbert Syzygy Theorem)**.** *Let I be an ideal in $R = \mathbb{R}[x_1, \ldots, x_n]$. Then there is an exact sequence of free modules:*

$$0 \to R^{b_n} \to \cdots \to R^{b_1} \to R \to R/I.$$

Note that the most important part of the above statement is the 0 at the left hand side. We will use this to achieve our goal of computing the Hilbert series of R/I.

Remark 4.3. We should remark on the proof of the Hilbert syzygy theorem. Hilbert proved this theorem essentially by developing the notion of a Gröbner Basis, and coming up with a computational. This is outlined in [1] and also in [4]. There are many technical details, but the main insight is that if we choose our generators and maps in the right way, then at each stage of the resolution fewer variables will appear, and then at some point we must run out of variables - and hence our resolution must terminate. We illustrate this on the next few pages with some examples.

Consider the ideal $I = (x^2, y^3, z^4, w^5)$. The free resolution is below.

```
           1                        4
o161 = 0 : R  <------------------- R  : 1
                 | x2 y3 z4 w5 |

           4                                      6
      1 : R  <---------------------------------- R  : 2
                {2} | -y3 -z4 0   -w5 0   0   |
                {3} | x2  0   -z4 0   -w5 0   |
                {4} | 0   x2  y3  0   0   -w5 |
                {5} | 0   0   0   x2  y3  z4  |

           6                                4
      2 : R  <--------------------------- R  : 3
                {5} | z4  w5  0   0   |
                {6} | -y3 0   w5  0   |
                {7} | x2  0   0   w5  |
                {7} | 0   -y3 -z4 0   |
                {8} | 0   x2  0   -z4 |
                {9} | 0   0   x2  y3  |

           4                    1
      3 : R  <---------------- R  : 4
                {9}  | -w5 |
                {10} | z4  |
                {11} | -y3 |
                {12} | x2  |

           1
      4 : R  <----- 0 : 5
                0
```

Look at the bottom of each column.

- In the first matrix all 4 variables appear in the bottom of a column
- In the second matrix at most 3 variables appear in the bottom of a column
- In the third matrix at most 2 variables appear in the bottom of a column
- In the fourth matrix at most 1 variable appears in the bottom of a column

In general, if $R = \mathbb{R}[x_1, \ldots, x_n]$ Hilbert showed that if you label things carefully, as you go back a step in the resolution, the number of variables that can appear "in the bottom of a column" goes down by 1. Since there are only n variables, the resolution must stop after n steps!

Check out the following examples with Macaulay2 to see that this pattern persists. Notice that we have to use $\mathbb{Z}[x_i]$ to get Macaulay2 to sort things appropriately. The condition we want to confirm is that

- In the first matrix - anything goes
- In subsequent matrices look at the polynomials that occur as bottom-most entries.
- In the second matrix - there is a variable, say x_n, such that for each of those bottom-most entries, there is a term that doesn't contain x_n.
- In the third matrix - there are two variables, say x_n, x_{n-1}, such that for each of those bottom-most entries, they have a term that doesn't contain x_n or x_{n-1}.
- $\cdots$
- In the nth matrix - there are $n-1$ variables, say $x_n, x_{n-1}, \ldots, x_2$ such that for each of those bottom-most entries, they have a term that doesn't contain those variables.
- In the $(n+1)$st matrix - there are no terms - since we have no variables left!

```
R = ZZ[x,y,z,w];  I = ideal(x^2, y^3, z^4,w^5); C = res I;

R = ZZ[x,y];  I = ideal schreyerOrder gens ideal(x^10, x^9*y^2,x^7*y^3,x^4*y^4,x*y^5, y^7);
C = res image gens I; netList {gens I, C.dd_1}

R = ZZ[x,y,z,w];  I = ideal(x^2, x*y,y^2, z^2,  z*w, w^2); C = res image gens I;
netList ({gens I}|apply(3, i-> C.dd_(i+1)))

R = ZZ[x,y,z,w,v];  I = ideal (x^3, y^3,x^2*z + x*y*w+y^2*v); C = res image gens I;
netList ({gens I}|apply(4, i-> C.dd_(i+1)))

R = ZZ[x,y,z]; I = ideal"x4,x2y,y3,z4"; C = res image gens I;
netList ({gens I}|apply(2, i-> C.dd_(i+1)))
```

We now close by showing how the Hilbert Syzygy Theorem allows us to compute the Hilbert Series of R/I (and why it is of the form $p(t)/(1-t)^n$. We first fix the grading so that the maps in our free resolution preserve degree. Remember that to use Proposition 2.3 and its generalization it was essential that the maps preserve degree.

4.2 Fixing the Grading

As introduced in the Exercises yesterday, we consider the following:

Definition 4.4. If M is a graded module then we define the module $M(-d)$ to be the module that is exactly the same as M except that we've adjusted the grading so that

$$M(-d)_e = M_{e-d}.$$

Example 4.5. Consider the map $R \to R$ that is multiplication by x^3. This map does not preserve degree. For instance it induces a map $R_4 \to R_7$. However, consider that same map but as

$$\cdot x^3 : R(-3) \to R.$$

Now this map preserves degree. Indeed, $R(-3)_d \to R_d$. (Convince yourself of this, for instance, but checking that $R(-3)_{10} \to R_{10}$).

Example 4.6. Consider the exact sequence

$$0 \longrightarrow R(-4) \xrightarrow{\begin{bmatrix} -y^2 \\ x \end{bmatrix}} \begin{matrix} R(-2) \\ \oplus \\ R(-3) \end{matrix} \xrightarrow{\begin{bmatrix} xy & y^3 \end{bmatrix}} R \longrightarrow 0$$

Let's follow some vectors through this sequence and check that these maps preserve degrees. Let's start with something on the left in degree 10. Remember that $R(-4)_{10} = R_6$ so we'll take something like x^6. Then we apply this map and it goes to

$$\begin{bmatrix} -x^6y \\ x^7 \end{bmatrix} \in \begin{matrix} R(-2) \\ \oplus \\ R(-3) \end{matrix}$$

And indeed, this is again an element of degree 10.

Alternatively, let's start with a random element of degree 20 in $R(-2) \oplus R(-3)$. Say, something like (y^{18}, x^{17}), say. Then the next map will send this to

$$xy^{19} + x^{17}y^3 \in R.$$

Sure enough this went to something of degree 20.

Proposition 4.7. *Let M be an R-module with r generators of degrees $d_1, \ldots, d_r$. Then the following surjective map preserves degree:*

$$R(-d_1) \oplus \cdots \oplus R(-d_r) \to M.$$

We might choose to write this as

$$\bigoplus_j R(-j) \to M$$

where it is understood that the j's represent the degrees we need to generate M.

Inductively (and by the Hilbert Syzygy Theorem) this means that if I is any ideal then there exists an exact sequence that **preserves degree***:*

$$0 \longrightarrow \bigoplus_j R(-j)^{b_{nj}} \longrightarrow \cdots \longrightarrow \bigoplus_j R(-j)^{b_{2j}} \longrightarrow \bigoplus_j R(-j)^{b_{1j}} \longrightarrow R \longrightarrow R/I \longrightarrow 0.$$

Proposition 4.8. *The Hilbert Series of $R(-j)$ is $\frac{t^j}{(1-t)^n}$.*

Proof. The Hilbert Series of $R(-j)$ will be

$$HS(R(-j)) = \sum \dim R(-j)_d t^d = \sum \dim R_{d-j} t^d = t^j \sum \dim R_{d-j} t^{d-j} = t^j HS(R) = \frac{t^j}{(1-t)^n}.$$

□

Finally, we are ready to prove our main theorem:

Theorem 4.9. *If $R = \mathbb{R}[x_1, \ldots, x_n]$ and I is an ideal, then there is a polynomial $p(t)$ with integer coefficients such that*

$$HS(R/I) = \frac{p(t)}{(1-t)^n}.$$

Proof. By the previous proposition, we can find a resolution of R/I that preserves degree:

$$0 \longrightarrow \bigoplus_j R(-j)^{b_{nj}} \longrightarrow \cdots \longrightarrow \bigoplus_j R(-j)^{b_{2j}} \longrightarrow \bigoplus_j R(-j)^{b_{1j}} \longrightarrow R \longrightarrow R/I \longrightarrow 0.$$

Let's simplify that for a second, and just write:

$$0 \longrightarrow F_n \longrightarrow F_{n-1} \longrightarrow \cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow R/I \longrightarrow 0.$$

The Hilbert series of R/I can be expressed as an alternating sum of the Hilbert Series of the F_i by Exercise 2.3.

$$HS(R/I) = \sum (-1)^i HS(F_i).$$

Now each F_i is a sum of things of the form $R(-j)$, which has Hilbert series $t^j/(1-t)^n$. Hence $HS(R/I)$ is of the form $p(t)/(1-t)^n$.

Explicitly,

$$HS(R/I) = \sum_{i,j} \frac{(-1)^i b_{ij} t^j}{(1-t)^n}.$$

□

Example 4.10. Let $I = (x, y, z) \subset \mathbb{R}[x, y, z]$. Suppose we want to compute the Hilbert Series of R/I. Well our first step is going to be to start with

$$0 \to I \to R \to R/I \to 0 \qquad \text{record: } \boxed{HS(R/I) = HS(R) - HS(I)}.$$

all these maps preserve degree. Now we want to look at the module on the left (that is, I) and find a minimal generating set. The set (x, y, z) does the trick, so let's now consider

$$0 \longrightarrow K_1 \longrightarrow R^2 \xrightarrow[\text{deg } 2]{\phi=[x,y,z]} I \to 0.$$

$$0 \longrightarrow K_1 \longrightarrow R(-1)^3 \xrightarrow[\text{preserves deg}]{\phi=[x,y,z]} I \to 0\ .$$

We will use the second option because if ϕ preserves degree then we will be able to compute our Hilbert Series and record: $\boxed{HS(I) = HS(R(-1)^3) - HS(K_1).}$

Now what can we say about K_1? Well it is the kernel of the map $[x, y, z]$. So what vectors $\overline{v} \in R(-2)^3$ will satisfy

$$[x, y, z] \cdot \begin{bmatrix} f_1 \\ f_2 \\ f_2 \end{bmatrix}.$$

We can quickly see that the following vectors are in K

$$v_1 = \begin{bmatrix} y \\ -x \\ 0 \end{bmatrix}, \quad v_2 = \begin{bmatrix} z \\ 0 \\ -x \end{bmatrix}, \quad v_3 = \begin{bmatrix} 0 \\ z \\ -y \end{bmatrix}$$

With a little work, you can show that these elements **generated** all of the elements in the kernel of ϕ. Finally, in what degree do these vectors live in? (They live in K_2 - think about why.) Hence we can find a surjective map $R(-2)^3 \to K \to 0$. which gives rise to a short exact sequence

$$0 \longrightarrow K_2 \longrightarrow R(-2)^3 \xrightarrow[\text{preserves deg}]{\phi_2 = \begin{bmatrix} y & z & 0 \\ -x & 0 & z \\ 0 & x & -y \end{bmatrix}} K \to 0 \,.$$

Finally we can calculate the kernel of ϕ_2 and see that it is generated by

$$w = \begin{bmatrix} x \\ y \\ z \end{bmatrix}.$$

Which is an element of degree 3.

$$0 \longrightarrow K_3 \longrightarrow R(-3)^1 \xrightarrow[\text{preserves deg}]{\phi_3 = \begin{bmatrix} x \\ y \\ z \end{bmatrix}} K_2 \to 0 \,.$$

And now finally we have that K_3 is zero. If we compose all of the maps then we get

$$0 \longrightarrow R(-3)^1 \xrightarrow[\text{preserves deg}]{\phi_3 = \begin{bmatrix} x \\ y \\ z \end{bmatrix}} R(-2)^3 \xrightarrow[\text{preserves deg}]{\phi_2 = \begin{bmatrix} y & z & 0 \\ -x & 0 & z \\ 0 & x & -y \end{bmatrix}} R(-1)^3 \xrightarrow[\text{preserves deg}]{\phi = [x,y,z]} R \longrightarrow R/I \longrightarrow 0 \,.$$

Example 4.11. Let's go back to our original staircase example:

$$I = (x^{10}, x^9y^2, x^7y^3, x^4y^4, xy^5, y^7).$$

We can use Macaulay 2 to get a resolution of R/I:

```
 R = QQ[x,y];  I = ideal(x^10, x^9*y^2,x^7*y^3,x^4*y^4,x*y^5, y^7);  C = res I;
netList apply(3, i-> tally degrees C_i); -- this will return the degrees of the generators

       +----------------+
o362 = |Tally{{0} => 1} |
       +----------------+
       |Tally{{6} => 1 }|
```

```
|      {7} => 1  |
|      {8} => 1  |
|      {10} => 2 |
|      {11} => 1 |
+----------------+
|Tally{{8} => 1 }|
|      {9} => 1  |
|      {11} => 1 |
|      {12} => 2 |
+----------------+
```

This means that the minimal free resolution of R/I is

$$0 \longrightarrow \begin{matrix} R(-8) \\ \oplus \\ R(-9) \\ \oplus \\ R(-11) \\ \oplus \\ R(-12)^2 \end{matrix} \longrightarrow \begin{matrix} R(-6) \\ \oplus \\ R(-7) \\ \oplus \\ R(-8) \\ \oplus \\ R(-10)^2 \\ \oplus \\ R(-11) \end{matrix} \longrightarrow R \longrightarrow R/I \longrightarrow 0.$$

So this means that the Hilbert Series of R/I is

$$HS(R/I) = \frac{1 - t^6 - t^7 - t^8 - 2t^{10} - t^{11} + t^8 + t^9 + t^{11} + 2t^{12}}{(1-t)^2}$$

4.3 The last section

Where to go from here:

- As we said above, the computational proof of the Hilbert Syzygy Theorem we have hinted at can be made rigorous e.g. by looking at [1, 4].
- If that proof still leaves something to be desired, and you'd like to go deeper as to how homological tools might help offer a "nicer" proof. Then you might want to continue learning more homological algebra, perhaps from the text *Computational Algebraic Geometry* [5] by Hal Schenck. The following quote from Hal Schenck maybe sums it up best:

> I asked the professor what good Tor was; the answer that Tor is the derived functor of tensor product did not grip me. When I complained to my advisor, he said "Ah, but you can give a two line proof of the Hilbert syzygy theorem using Tor - go figure it out".

4.4 Exercises for Day 4

Exercise 1. By hand, calculate a free resolution of R/I that preserves degree in the case that $R = \mathbb{R}[x, y]$ and $I = (x^2, xy^2)$. (Hint: you may have computed the kernel yesterday). Write your resolution using $R(-j)$ notation and use it to calculate $HS(R/I)$. Does your answer match the procedure:

$$HS(R/I) = \frac{1 - \sum_{\text{lower steps}} t^{\text{deg. step}} + \sum_{\text{upper steps}} t^{\text{deg. step}}}{(1-t)^2} \tag{4.1}$$

Exercise 2. Repeat Exercise 1 with a different ideal, perhaps something like $I = (x^3, x^2y, xy^2, y^3)$.

- The staircase has 4 lower steps (your four generators)
- The staircase has 3 upper steps (which will correspond to your four generators of the kernel) in

$$0 \to K \to R^4 \to I.$$

- Write down these kernel elements, and your resolution and verify that the degrees are what they should be.

Exercise 3. Suppose that the Hilbert Series of R/I is equal to

$$\frac{f(t)}{(1-t)^d}$$

where this fraction is written in lowest terms. Then the **dimension** of the corresponding (affine) geometric object defined by I will have dimension d. Check this using Macaulay2 on the following examples: (use

```
hilbertSeries(I, Reduce=>true)
```

1. $I = (y - x) \subset \mathbb{R}[x, y]$ is a line in $\mathbb{R}^2$.
2. $I = (x + y, z + y) \subset \mathbb{R}[x, y]$ is a line in $\mathbb{R}^3$.
3. $I = (x, y, z)$ is a point in $\mathbb{R}^3$.
4. Let X be the subset of $\mathbb{R}^6$ corresponding to all 2×3 matrices whose rank is $\leqslant 1$.

$$X = \left\{ A = \begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix}, \ \operatorname{rank} A \leqslant 1 \right\}$$

   Discuss with your group what you think the **dimension** of this object should be - how many degrees of freedom do you think it has? Now note that A is defined by the vanishing of the 2×2 minors of A:

$$I = (ae - bd, af - cd, bf - ce).$$

   Using Macaulay2 compute the Hilbert series of I and determine the dimension of X. Does it match?

5. What do you think about the set of 3×3 matrices of rank $\leqslant 1$? This can be viewed as a subset of $\mathbb{R}^9$. What do you think its dimension is? Check with Macaulay2. The command `dim I` will return the dimension of the geometric object associated to I. Check that this agrees with the degree of the denominator in `hilbertSeries(I, Reduced=>true)`. Try something like this:

```
R = QQ[x_1..x_9];
A = genericMatrix(R,3,3)
I = minors(2,A)
hilbertSeries(I, Reduce=>true)
dim I
```

Exercise 4. Now prove that if the Hilbert Series is $\frac{f(t)}{(1-t)^d}$ then if you expand out the series then the coefficient of t^N for N large will be a **polynomial** of degree $d-1$. Hint: your solution should use the fact that this fraction is in lowest terms. It being in lowest terms is equivalent to requiring that $f(1) \neq 0$. What is the leading coefficient?

Exercise 5. (Open Problem) A $n \times n$ magic square with magic number d is an $n \times n$ matrix with nonnegative entries whose rows and columns all sum to d. For instance,

$$\begin{pmatrix} 2 & 7 & 6 \\ 9 & 5 & 1 \\ 4 & 3 & 8 \end{pmatrix}$$

is a 3×3 magic square with magic number 15. Let $M(n,d)$ denote the number of $n \times n$ magic squares with magic number d. Richard Stanley proved that if you fix n then $M(n,d)$ is a polynomial in d of degree $(n-1)^2$.

1. If $n = 1$ then explain why $M(1,d) = 1$ for all d. (This is polynomial of degree 0^2.)
2. By hand you should be able to guess a formula for $M(2,d)$. (It should be a polynomial of degree 1^2.)
3. $M(3,d) = \frac{1}{8}(d^4 + 6d^3 + 15d^2 + 18d + 8)$.
4. Now for general n: let $R = \mathbb{R}[x_1, \ldots, x_{n!}]$ (yes, $n!$). Then there is an ideal I in R such that

   $$M(n,d) = HF_{R/I}(d).$$

   That is, this magic-square-counting-function is just the Hilbert function of some ring R/I. As such you know by our work this week that the generating function for $M(n,d)$ is rational

   $$\sum M(n,d)t^d = \frac{h(t)}{(1-t)^{(n-1)^2+1}}$$

   if you'd like to explore, check out the Macaulay2 code I wrote that will generate the ideal I for you. I think in general it is not known what sorts of numbers show in in the Hilbert function. Or what this polynomial $p(t)$ is!
5. See `http://www-math.mit.edu/~rstan/transparencies/durer` and `http://www2.math.uu.se/~qimh/Magic.pdf` for more information.

```
--- Magic Squares Code
 magicSquareIdeal = (n)->(
    A = (permutations entries id_(ZZ^n))/matrix;
    M = first A;
    R = ZZ/101[x_(0,0)..x_(n-1,n-1)];
    Phi=apply(A, M-> (
p = 1;
     for i from 0 to n-1 do (
    for j from 0 to n-1 do (
        if M_(i,j) != 0 then p =p*(x_(i,j));
    );
);
    p));
S = ZZ/101[y_1..y_(n!)];
I = ker map(R,S, Phi)
)

I = magicSquareIdeal 4
apply(10, i-> hilbertFunction(i, I))
hilbertSeries(J, Reduce=>true)
```

Exercise 6. Draw the projective plane $\mathbb{RP}^2$ by drawing a circle and identify opposite sides antipodally. Sonja's notes have a great picture. By introducing points on the circle and interior, draw a **triangulation** of $\mathbb{RP}^2$. This means that you will split the surface into triangles such that the triangles all have three distinct vertices and that those vertices determine (at most) one triangle. (Hint: Label your vertices a, b, c, d, e, f).

- Now that you have your triangles, write down the set of squarefree degree three monomials that do *not* correspond to any triangle. Let I be the ideal that these generate. This is called the Stanley-Reisner Ideal of this triangulation.
- Input this ideal into Macaulay2 using the commands:

  `R = QQ[a,b,c,d,e,f]`

  `I = ideal"abc,def,???"`

  `codim I, betti res I`
- Work out the Hilbert Series of R/I using `HilbertSeries(I, Reduce=>true)`. You'll find that

$$HS(R/I) = \frac{1 + 3T + 6T^2}{(1-T)^3}$$

  The numerator is called the **h-polynomial**, for "Hilbert". Note that

$$1 + 3T + 6T^2 = 6(T-1)^2 + 15(T-1) + 10.$$

  The coefficients on the right $(6, 15, 10)$ are called the **f-vector**, for "face." Notice that your picture has 6 vertices, 15 edges and 10 triangles.

Note: When inputting an ideal you can either type `x^2*y^3+3*x*y` with the carats and stars. Or else you can input `ideal"x2y3+3xy"`.

5 Miscellaneous Exercises

Exercise 7. We say that an ideal I is prime if when $fg \in I$, either $f \in I$ or $g \in I$. Prove that the following ideals are prime in $\mathbb{C}[x, y, z]$

1. (x)
2. $(x, y - 2)$
3. $(x^2 - yz)$

Exercise 8. If I is an ideal in R then the **quotient ring** R/I is the ring which is best thought of as follows: The elements are all of the form $\overline{r}$ for $r \in R$ and the ring operations are exactly what you think they are:

$$\overline{r} + \overline{s} = \overline{r + s}$$

$$\overline{r} \cdot \overline{s} = \overline{rs}.$$

Finally (and this is the tricky part) we define $\overline{r} = \overline{s}$ if $r - s \in I$. In other words, $\overline{r}$ and $\overline{s}$ can be equal even if $r \neq s$.

Suppose that $I = (x^2 + 1)$ in $\mathbb{R}[x]$.

1. Prove that $\overline{x^2} = \overline{-1}$
2. Prove that $\overline{x^3 + 3x} = \overline{2x}$
3. Prove that $\overline{x^4} = \overline{1}$
4. Show that for every polynomial $f \in \mathbb{R}[x]$ there are $a, b \in \mathbb{R}$ such that

$$\overline{f} = \overline{ax + b}.$$

Exercise 9. Let $I = (x^2, y^3, z^4) \subset \mathbb{C}[x, y, z]$. Show that R/I is a finite dimensional vector space over $\mathbb{C}$. What is the dimension of this space? Write down a basis.

Exercise 10. A commutative ring R is called an integral domain if the following implication is true:

$$f, g \in R, \quad fg = 0 \implies f = 0 \; or \; g = 0.$$

1. Prove that $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain.
2. Prove that $\mathbb{Z}/7\mathbb{Z}$ is an integral domain.
3. Prove that $I \subset R$ is a prime ideal if and only if R/I is an integral domain.
4. Prove that $I = (x - 1, y - 2, z - 3)$ is a prime ideal in $R = \mathbb{C}[x, y, z]$ by explaining why R/I is isomorphic to $\mathbb{C}$.

The last part of the last exercise is a prototypical example of the following idea that comes up all the time in algebra.

Find a map. Make it surjective. Compute the kernel. Quotient out and you get an isomorphism! Indeed, if

$$\phi : R \to R$$

is a surjective **homomorphism of rings** then

$$R/\ker \phi \cong R.$$

This is so important it's called the **First Isomorphism Theorem**.

Exercise 11.

1. Prove the first isomorphism theorem.
2. Explain how the first isomorphism theorem implies the following: if

   $$\phi : R \to S$$

   is any **homomorphism of rings** then

   $$R/\ker\phi \cong \mathrm{im}\phi.$$

3. Let $\alpha_1, \ldots, \alpha_n \in k$ be arbitrary scalars. Prove that

   $$\mathbb{R}[x_1, \ldots, x_n]/(x_1 - \alpha_1, \ldots, x_n - \alpha_n) \cong k$$

   as follows:

   - First define a map $\phi : \mathbb{R}[x_1, \ldots, x_n] \to k$ by defining $\phi(f) = f(\alpha_1, \ldots, \alpha_n)$. That is, ϕ is the evaluation map.
   - Check that $\ker\phi = (x_1 - \alpha_1, \ldots, x_n - \alpha_n)$. (This may require a careful division argument...)
   - Now apply the first homomorphism theorem.

Exercise 12. (From Artin's Algebra) Describe the kernel of the following maps

- $\mathbb{R}[x, y] \to \mathbb{R}$ defined by $f(x, y) \to f(0, 0)$
- $\mathbb{R}[x] \to \mathbb{C}$ defined by $f(x) \to f(2 + i)$
- $\mathbb{Z}[x] \to \mathbb{R}$ defined by $f(x) \to f(1 + \sqrt{2})$
- $\mathbb{C}[x, y] \to \mathbb{C}[t]$ defined by $x \to t, y \to t^2$,
- $\mathbb{C}[x, y] \to \mathbb{C}[t]$ defined by $x \to t, y \to t^2, z \to t^3$.,

Exercise 13. Let I and J be ideals in a ring R. Show that $I \cup J$ is not necessarily an ideal. However, if we define

$$I + J = \{r \in R \ : \ r = i + j, \text{for } i \in I \text{ and } j \in J\}$$

then show that $I + J$ is an ideal of R.

Similarly, the product of two ideals I and J is defined to be the ideal generated by all products fg for $f \in I$ and $g \in J$.

Exercise 14. Let I and J be two ideals in a ring R such that $I + J = R$. Prove that $IJ = I \cap J$

Exercise 15. Work out some of the following "staircases" using the techniques above to verify that the number of dots under the staircase is given by Equation 4.1.

1. Take the points $(2,0),(1,1),(0,2)$
2. Take the points $(3,0),(2,1),(1,2),(0,3)$
3. Take the points $(n,0),(n-1,1),\ldots,(1,n-1),(0,n)$
4. Take the points $(2,0),(0,2)$
5. Take the points $(3,0),(0,3)$
6. Take the points $(n,0),(0,n)$
7. Take the points $(4,0),(2,2),(0,4)$.

Exercise 16. Determine whether the following sequence is exact:

$$0 \longrightarrow V \xrightarrow{\phi} V \longrightarrow 0.$$

where V is $\mathbb{R}^3$ and ϕ is the matrix

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

Exercise 17. Check that $R/(x_1,\ldots,x_n)$ is isomorphic to k (in other words the only thing left are the constant polynomials). Use this to conclude that

$$HS(R/(x_1,\ldots,x_n)) = 1 + 0t + 0t^2 + \cdots . = 1.$$

Finally conclude that

$$HS((x_1,\ldots,x_n)) = \frac{1}{(1-t)^2} - 1.$$

Exercise 18. Prove in fact that every ideal in $\mathbb{R}[x]$ has exactly one generator, namely the gcd of all the polynomials in the ideal. We call $\mathbb{R}[x]$ a **principal ideal domain** since every ideal in $\mathbb{R}[x]$ is principal. **Warning Warning Warning:** this is very much false if there is more than one variable.

Exercise 19. Dickson's Lemma says that any ideal in $\mathbb{R}[x_1,\ldots,x_n]$ generated by **monomials** must be generated by finitely many of those monomials. Try proving this for $n = 1, 2, 3.$ (or in general if you like.) You should notice that $n = 3$ is considerably harder than $n = 2$.

Exercise 20.

- Every module M has a zero element defined by the property that $0 + m = m$ for all $m \in M$. Use this to prove that if ϕ is a linear map of modules then $\phi(0) = 0$.
- Suppose that N is any module and $\phi : R \to M$ is a linear map of modules. Then show that ϕ is determined by where it sends 1. That is, if you know that $\phi(1) = m$ then find a formula for $\phi(f)$ for any polynomial $f \in R$.
- Let $I = (x, y)$ be the ideal generated by x and y and $R = \mathbb{R}[x, y]$. Show that there is no module map $\phi : I \to R^2$ that satisfies $\phi(x) = (x, 0)$ and $\phi(y) = (0, y)$.

Exercise 21. Prove that if $\phi : R^r \to M$ then $\ker \phi$ is finitely generated.

Exercise 22. Suppose that the following sequence of maps is **commutative** meaning that now matter how you move through the arrows, the result will be the same, e.g. $\gamma(f(x)) = g(\alpha(x))$ for each $x \in A$.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & M & \xrightarrow{\gamma} & N & \xrightarrow{\delta} & P & \longrightarrow & 0. \end{array}$$

If the two rows are exact sequences prove that there is an exact sequence

$$0 \longrightarrow \ker f \xrightarrow{\overline{\alpha}} \ker g \xrightarrow{\overline{\beta}} \ker h \xrightarrow{\phi} M/\operatorname{im}(f) \xrightarrow{\overline{\gamma}} N/\operatorname{im}(g) \xrightarrow{\overline{\delta}} P/\operatorname{im}(h) \longrightarrow 0$$

Warning: This exercise is what is called a "diagram chase". It has a bazillion parts, and the reader is encouraged to perhaps begin by trying to figure out how the map ϕ might be defined. Indeed, if you take $x \in \ker h$ how on earth could you map it to something in $M/\operatorname{im}(f)$.

Exercise 23. Suppose that M is a finitely generated R-module. Show that M is Noetherian. That is, show that any submodule is finitely generated. Hint: try to use 3.9.

Exercise 24. Let $I = (xy, yz, xz)$. Compute $HS(M)$ with $M = R/I$ and $M = I$.

References

[1] Christine Berkesch and Frank-Olaf Schreyer. Syzygies, finite length modules, and random curves. *Commutative algebra and noncommutative algebraic geometry*, 1:25–52, 2015.

[2] David A Buchsbaum and David Eisenbud. Algebra structures for finite free resolutions, and some structure theorems for ideals of codimension 3. *American Journal of Mathematics*, 99(3):447–485, 1977.

[3] David Cox, John Little, and Donal OShea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Springer Science & Business Media, 2013.

[4] David Eisenbud. *Commutative Algebra: with a view toward algebraic geometry*, volume 150. Springer Science & Business Media, 2013.

[5] Henry Schenck and Hal Schenck. *Computational algebraic geometry*, volume 58. Cambridge University Press, 2003.

[6] Andrew J. Sommese and Charles W. Wampler, II. *The numerical solution of systems of polynomials*. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2005. Arising in engineering and science.