Chapter 6

Free Resolutions

In Chapter 5, we saw that to work with an R-module M, we needed not just the generators $f_1, \ldots, f_t$ of M, but the relations they satisfy. Yet the set of relations $\operatorname{Syz}(f_1, \ldots, f_t)$ is an R-module in a natural way and, hence, to understand it, we need not just its generators $g_1, \ldots, g_s$, but the set of relations $\operatorname{Syz}(g_1, \ldots, g_s)$ on these generators, the so-called second syzygies. The second syzygies are again an R-module and to understand it, we again need a set of generators *and* relations, the third syzygies, and so on. We obtain a sequence, called a resolution, of generators and relations of successive syzygy modules of M. In this chapter, we will study resolutions and the information they encode about M. Throughout this chapter, R will denote the polynomial ring $k[x_1, \ldots, x_n]$ or one of its localizations.

§1 Presentations and Resolutions of Modules

Apart from the possible presence of nonzero elements in the module of syzygies on a minimal set of generators, one of the important things that distinguishes the theory of modules from the theory of vector spaces over a field is that many properties of modules are frequently stated in terms of homomorphisms and exact sequences. Although this is primarily cultural, it is very common and very convenient. In this first section, we introduce this language.

To begin with, we recall the definition of exact.

(1.1) Definition. Consider a sequence of R-modules and homomorphisms

$$\cdots \longrightarrow M_{i+1} \xrightarrow{\varphi_{i+1}} M_i \xrightarrow{\varphi_i} M_{i-1} \longrightarrow \cdots$$

a. We say the sequence is *exact at* M_i if $\operatorname{im}(\varphi_{i+1}) = \ker(\varphi_i)$.
b. The entire sequence is said to be *exact* if it is exact at each M_i which is not at the beginning or the end of the sequence.

Many important properties of homomorphisms can be expressed by saying that a certain sequence is exact. For example, we can phrase what it means for an R-module homomorphism $\varphi : M \to N$ to be onto, injective, or an isomorphism:

- $\varphi : M \to N$ is onto (or surjective) if and only if the sequence
$$M \xrightarrow{\varphi} N \to 0$$
is exact, where $N \to 0$ is the homomorphism sending every element of N to 0. To prove this, recall that onto means $\mathrm{im}(\varphi) = N$. Then the sequence is exact at N if and only if $\mathrm{im}(\varphi) = \ker(N \to 0) = N$, as claimed.
- $\varphi : M \to N$ is one-to-one (or injective) if and only if the sequence
$$0 \to M \xrightarrow{\varphi} N$$
is exact, where $0 \to M$ is the homomorphism sending 0 to the additive identity of M. This is equally easy to prove.
- $\varphi : M \to N$ is an isomorphism if and only if the sequence
$$0 \to M \xrightarrow{\varphi} N \to 0$$
is exact. This follows from the above since φ is an isomorphism if and only if it is one-to-one and onto.

Exact sequences are ubiquitous. Given any R-module homomorphism or any pair of modules, one a submodule of the other, we get an associated exact sequence as follows.

(1.2) Proposition.

a. *For any R-module homomorphism $\varphi : M \to N$, we have an exact sequence*
$$0 \to \ker(\varphi) \to M \xrightarrow{\varphi} N \to \mathrm{coker}(\varphi) \to 0,$$
where $\ker(\varphi) \to M$ is the inclusion mapping and $N \to \mathrm{coker}(\varphi) = N/\mathrm{im}(\varphi)$ is the natural homomorphism onto the quotient module, as in Exercise 12 from §1 of Chapter 5.

b. *If $Q \subset P$ is a submodule of an R-module P, then we have an exact sequence*
$$0 \to Q \to P \xrightarrow{\nu} P/Q \to 0,$$
where $Q \to P$ is the inclusion mapping, and ν is the natural homomorphism onto the quotient module.

Proof. Exactness of the sequence in part a at $\ker(\varphi)$ follows from the above bullets, and exactness at M is the definition of the kernel of a homomorphism. Similarly, exactness at N comes from the definition of the

cokernel of a homomorphism (see Exercise 28 of Chapter 5, §1), and exactness at coker(φ) follows from the above bullets. In the exercises, you will show that part b follows from part a. □

Choosing elements of an R-module M is also conveniently described in terms of homomorphisms.

(1.3) Proposition. *Let M be an R-module.*

a. *Choosing an element of M is equivalent to choosing a homomorphism $R \to M$.*
b. *Choosing t elements of M is equivalent to choosing a homomorphism $R^t \to M$.*
c. *Choosing a set of t generators of M is equivalent to choosing a homomorphism $R^t \to M$ which is onto (i.e., an exact sequence $R^t \to M \to 0$).*
d. *If M is free, choosing a basis with t elements is equivalent to choosing an isomorphism $R^t \to M$.*

Proof. To see part a, note that the identity 1 is the distinguished element of a ring R. Choosing an element f of a module M is the same as choosing the R-module homomorphism $\varphi : R \to M$ which satisfies $\varphi(1) = f$. This is true since $\varphi(1)$ determines the values of φ on all $g \in R$:

$$\varphi(g) = \varphi(g \cdot 1) = g \cdot \varphi(1) = gf.$$

Thus, choosing t elements in M can be thought of as choosing t R-module homomorphisms from R to M or, equivalently, as choosing an R-module homomorphism from R^t to M. This proves part b. More explicitly, if we think of R^t as the space of column vectors and denote the standard basis in R^t by $e_1, e_2, \ldots, e_t$, then choosing t elements $f_1, \ldots, f_t$ of M corresponds to choosing the R-module homomorphism $\varphi : R^t \to M$ defined by setting $\varphi(e_i) = f_i$, for all $i = 1, \ldots, t$. The image of φ is the submodule $\langle f_1, \ldots, f_t \rangle \subset M$. Hence, choosing a set of t generators for M corresponds to choosing an R-module homomorphism $R^t \to M$ which is onto. By our previous discussion, this is the same as choosing an exact sequence

$$R^t \to M \to 0.$$

This establishes part c, and part d follows immediately. □

In the exercises, we will see that we can also phrase what it means to be projective in terms of homomorphisms and exact sequences. Even more useful for our purposes, will be the interpretation of presentation matrices in terms of this language. The following terminology will be useful.

(1.4) Definition. Let M be an R-module. A *presentation* for M is a set of generators $f_1, \ldots, f_t$, together with a set of generators for the syzygy module Syz $(f_1, \ldots, f_t)$ of relations among $f_1, \ldots, f_t$.

One obtains a presentation matrix for a module M by arranging the generators of $\operatorname{Syz}(f_1, \ldots, f_t)$ as columns—being given a presentation matrix is essentially equivalent to being given a presentation of M. To reinterpret Definition (1.4) in terms of exact sequences, note that the generators $f_1, \ldots, f_t$ give a surjective homomorphism $\varphi : R^t \to M$ by part c of Proposition (1.3), which means an exact sequence

$$R^t \xrightarrow{\varphi} M \to 0.$$

The map φ sends $(g_1, \ldots, g_t) \in R^t$ to $\sum_{i=1}^t g_i f_i \in M$. It follows that a syzygy on $f_1, \ldots, f_t$ is an element of the kernel of φ, i.e.,

$$\operatorname{Syz}(f_1, \ldots, f_t) = \ker(\varphi : R^t \to M).$$

By part c of Proposition (1.3), choosing a set of generators for the syzygy module corresponds to choosing a homomorphism ψ of R^s onto $\ker(\varphi) = \operatorname{Syz}(f_1, \ldots, f_t)$. But ψ being onto is equivalent to $\operatorname{im}(\psi) = \ker(\varphi)$, which is just the condition for exactness at R^t in the sequence

$$R^s \xrightarrow{\psi} R^t \xrightarrow{\varphi} M \to 0. \tag{1.5}$$

This proves that a presentation of M is equivalent to an exact sequence of the form (1.5). Also note that the matrix of ψ with respect to the standard bases of R^s and R^t is a presentation matrix for M.

We next observe that *every* finitely generated R-module has a presentation.

(1.6) Proposition. *Let M be a finitely generated R-module.*

a. *M has a presentation of the form given by (1.5).*

b. *M is a homomorphic image of a free R-module. In fact, if $f_1, \ldots, f_t$ is a set of generators of M, then $M \cong R^t/S$ where S is the submodule of R^t given by $S = \operatorname{Syz}(f_1, \ldots, f_t)$. Alternatively, if we let the matrix A represent ψ in (1.5), then $AR^s = \operatorname{im}(\psi)$ and $M \cong R^t/AR^s$.*

PROOF. Let $f_1, \ldots, f_t$ be a finite generating set of M. Part a follows from the fact noted in Chapter 5, §2 that every submodule of R^t, in particular $\operatorname{Syz}(f_1, \ldots, f_t) \subset R^t$, is finitely generated. Hence we can choose a finite generating set for the syzygy module, which gives the exact sequence (1.5) as above.

Part b follows from part a and Proposition 1.10 of Chapter 5, §1. □

Here is a simple example. Let $I = \langle x^2 - x, xy, y^2 - y \rangle$ in $R = k[x, y]$. In geometric terms, I is the ideal of the variety $V = \{(0,0), (1,0), (0,1)\}$ in k^2. We claim that I has a presentation given by the following exact sequence:

$$R^2 \xrightarrow{\psi} R^3 \xrightarrow{\varphi} I \to 0, \tag{1.7}$$

where φ is the homomorphism defined by the 1×3 matrix

$$A = \begin{pmatrix} x^2 - x & xy & y^2 - y \end{pmatrix}$$

and ψ is defined by the 3×2 matrix

$$B = \begin{pmatrix} y & 0 \\ -x+1 & y-1 \\ 0 & -x \end{pmatrix}.$$

The following exercise gives one proof that (1.7) is a presentation of I.

Exercise 1. Let S denote $\operatorname{Syz}(x^2 - x, xy, y^2 - y)$.

a. Verify that the matrix product AB equals the 1×2 zero matrix, and explain why this shows that $\operatorname{im}(\psi)$ (the module generated by the columns of the matrix B) is contained in S.
b. To show that S is generated by the columns of B, we can use Schreyer's Theorem—Theorem (3.3) from Chapter 5 of this book. Check that the generators for I form a *lex* Gröbner basis for I.
c. Compute the syzygies $\mathbf{s}_{12}$, $\mathbf{s}_{13}$, $\mathbf{s}_{23}$ obtained from the S-polynomials on the generators of I. By Schreyer's Theorem, they generate S.
d. Explain how we could obtain a different presentation

$$R^3 \xrightarrow{\psi'} R^3 \xrightarrow{\varphi} I \to 0$$

of I using this computation, and find an explicit 3×3 matrix representation of the homomorphism ψ'.
e. How do the columns of B relate to the generators $\mathbf{s}_{12}$, $\mathbf{s}_{13}$, $\mathbf{s}_{23}$ of S? Why does B have only two columns? Hint: Show that $\mathbf{s}_{13} \in \langle \mathbf{s}_{12}, \mathbf{s}_{23} \rangle$ in R^3.

We have seen that specifying any module requires knowing both generators and the relations between the generators. However, in presenting a module M, we insisted only on having a set of generators for the module of syzygies. Shouldn't we have demanded a set of relations on the generators of the syzygy module? These are the so-called *second syzygies*.

For example, in the presentation from part d of Exercise 1, there is a relation between the generators $\mathbf{s}_{ij}$ of $\operatorname{Syz}(x^2 - x, xy, y^2 - y)$, namely

$$(y-1)\mathbf{s}_{12} - \mathbf{s}_{13} + x\mathbf{s}_{23} = 0, \tag{1.8}$$

so $(y-1, -1, x)^T \in R^3$ would be a second syzygy.

Likewise, we would like to know not just a generating set for the second syzygies, but the relations among those generators (the third syzygies), and so on. As you might imagine, the connection between a module, its first syzygies, its second syzygies, and so forth can also be phrased in terms of an exact sequence of modules and homomorphisms. The idea is simple—we just iterate the construction of the exact sequence giving a presentation. For instance, starting from the sequence (1.6) corresponding to a presentation

for M, if we want to know the second syzygies as well, we need another step in the sequence:

$$R^r \xrightarrow{\lambda} R^s \xrightarrow{\psi} R^t \xrightarrow{\varphi} M \ \rightarrow \ 0,$$

where now the image of $\lambda : R^r \rightarrow R^s$ is equal to the kernel of ψ (the second syzygy module). Continuing in the same way to the third and higher syzygies, we produce longer and longer exact sequences. We wind up with a free resolution of M. The precise definition is as follows.

(1.9) Definition. Let M be an R-module. A *free resolution* of M is an exact sequence of the form

$$\cdots \rightarrow F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \rightarrow 0,$$

where for all i, $F_i \cong R^{r_i}$ is a free R-module. If there is an ℓ such that $F_{\ell+1} = F_{\ell+2} = \cdots = 0$, but $F_\ell \neq 0$, then we say the resolution is *finite*, of *length* ℓ. In a finite resolution of length ℓ, we will usually write the resolution as

$$0 \rightarrow F_\ell \rightarrow F_{\ell-1} \rightarrow \cdots \rightarrow F_1 \rightarrow F_0 \rightarrow M \rightarrow 0.$$

For an example, consider the presentation (1.7) for

$$I = \langle x^2 - x, xy, y^2 - y \rangle$$

in $R = k[x, y]$. If

$$a_1 \begin{pmatrix} y \\ -x+1 \\ 0 \end{pmatrix} + a_2 \begin{pmatrix} 0 \\ y-1 \\ -x \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

$a_i \in R$, is any syzygy on the columns of B with $a_i \in R$, then looking at the first components, we see that $ya_1 = 0$, so $a_1 = 0$. Similarly from the third components $a_2 = 0$. Hence the kernel of ψ in (1.7) is the zero submodule. An equivalent way to say this is that the columns of B are a basis for $\mathrm{Syz}(x^2 - x, xy, y^2 - y)$, so the first syzygy module is a free module. As a result, (1.7) extends to an exact sequence:

$$0 \rightarrow R^2 \xrightarrow{\psi} R^3 \xrightarrow{\varphi} I \rightarrow 0. \tag{1.10}$$

According to Definition (1.9), this is a free resolution of length 1 for I.

Exercise 2. Show that I also has a free resolution of length 2 obtained by extending the presentation given in part d of Exercise 1 above:

$$0 \rightarrow R \xrightarrow{\lambda} R^3 \xrightarrow{\psi} R^3 \xrightarrow{\varphi} I \rightarrow 0, \tag{1.11}$$

where the homomorphism λ comes from the syzygy given in (1.8).

Generalizing the observation about the matrix B above, we have the following characterization of finite resolutions.

(1.12) Proposition. *In a finite free resolution*

$$0 \to F_\ell \stackrel{\varphi_\ell}{\to} F_{\ell-1} \stackrel{\varphi_{\ell-1}}{\longrightarrow} F_{\ell-2} \to \cdots \to F_0 \stackrel{\varphi_0}{\to} M \to 0,$$

$\ker(\varphi_{\ell-1})$ *is a free module. Conversely, if* M *has a free resolution in which* $\ker(\varphi_{\ell-1})$ *is a free module for some* ℓ*, then* M *has a finite free resolution of length* ℓ*.*

PROOF. If we have a finite resolution of length ℓ, then φ_ℓ is one-to-one by exactness at F_ℓ, so its image is isomorphic to F_ℓ, a free module. Also, exactness at $F_{\ell-1}$ implies $\ker(\varphi_{\ell-1}) = \operatorname{im}(\varphi_\ell)$, so $\ker(\varphi_{\ell-1})$ is a free module. Conversely, if $\ker(\varphi_{\ell-1})$ is a free module, then the partial resolution

$$F_{\ell-1} \stackrel{\varphi_{\ell-1}}{\longrightarrow} F_{\ell-2} \to \cdots \to F_0 \stackrel{\varphi_0}{\to} M \to 0$$

can be completed to a finite resolution of length ℓ

$$0 \to F_\ell \to F_{\ell-1} \stackrel{\varphi_{\ell-1}}{\longrightarrow} F_{\ell-2} \to \cdots \to F_0 \stackrel{\varphi_0}{\to} M \to 0,$$

by taking F_ℓ to be the free module $\ker(\varphi_{\ell-1})$ and letting the arrow $F_\ell \to F_{\ell-1}$ be the inclusion mapping. □

Both (1.11) and the more economical resolution (1.10) came from the computation of the syzygies $\mathbf{s}_{ij}$ on the Gröbner basis for I. By Schreyer's Theorem again, the same process can be applied to produce a free resolution of any submodule M of a free module over R. If $\mathcal{G} = \{g_1, \ldots, g_s\}$ is a Gröbner basis for M with respect to any monomial order, then the $\mathbf{s}_{ij}$ are a Gröbner basis for the first syzygy module (with respect to the $>_\mathcal{G}$ order from Theorem (3.3) of Chapter 5). Since this is true, we can iterate the process and produce Gröbner bases for the modules of second, third, and all higher syzygies. In other words, Schreyer's Theorem forms the basis for an *algorithm* for computing any finite number of terms in a free resolution. This algorithm is implemented in `Singular`, in CoCoA, in the CALI package for REDUCE, and in the `resolution` command of *Macaulay 2*.

For example, consider the homogeneous ideal

$$M = \langle yz - xw, y^3 - x^2z, xz^2 - y^2w, z^3 - yw^2 \rangle$$

in $k[x, y, z, w]$. This is the ideal of a rational quartic curve in $\mathbb{P}^3$. Here is a *Macaulay 2* session calculating and displaying a free resolution for M:

```
i1 : R = QQ[x,y,z,w]

o1 = R

o1 : PolynomialRing
```

```
i2 : M = ideal(z^3-y*w^2,y*z-x*w,y^3-x^2*z,x*z^2-y^2*w)

             3     2             3   2     2   2
o2 = ideal (z  - y*w , y*z - x*w, y  - x z, x*z  - y w)

o2 : Ideal of R

i3 : MR = resolution M

      1     4     4     1
o3 = R  <-- R  <-- R  <-- R

     0     1     2     3

o3 : ChainComplex

i4 : MR.dd

                   1
o4 = -1 : 0 <----- R  : 0
              0

              1                                          4
         0 : R  <------------------------------------- R  : 1
                 {0} | yz-xw y3-x2z xz2-y2w z3-yw2 |

              4                                4
         1 : R  <--------------------------- R  : 2
                 {2} | -y2 -xz -yw -z2 |
                 {3} | z   w   0   0   |
                 {3} | x   y   -z  -w  |
                 {3} | 0   0   x   y   |

              4                 1
         2 : R  <-------------- R  : 3
                 {4} | w  |
                 {4} | -z |
                 {4} | -y |
                 {4} | x  |

o4 : ChainComplexMap
```

The output shows the matrices in a finite free resolution of the form

$$0 \to R \to R^4 \to R^4 \to M \to 0, \tag{1.13}$$

from the "front" of the resolution "back." In particular, the first matrix (1×4) gives the generators of M, the columns of the second matrix give generators for the first syzygies, and the third matrix (4×1) gives a generator for the second syzygy module, which is free.

Exercise 3.

a. Verify by hand that at each step in the sequence (1.13), the image of the mapping "coming in" is contained in the kernel of the mapping "going out."

b. Verify that the generators of M form a Gröbner basis of M for the *grevlex* order with $x > y > z > w$, and compute the first syzygy module using Schreyer's theorem. Why is the first syzygy module generated by just 4 elements (the columns of the 4×4 matrix), and not $6 = \binom{4}{2}$ elements $\mathbf{s}_{ij}$ as one might expect?

The programs `Singular` and CALI can be used to compute resolutions of ideals whose generators are not homogeneous (and, more generally, modules which are not graded), as well as resolutions of modules over local rings. Here, for example, is a `Singular` session computing a resolution of the ideal

$$I = \langle z^3 - y, yz - x, y^3 - x^2z, xz^2 - y^2 \rangle \tag{1.14}$$

in $k[x, y, z]$ (note that I is obtained by dehomogenizing the generators of M above).

```
> ring r=0, (x,y,z), dp;
> ideal I=(z3-y,yz-x,y3-x2z,xz2-y2);
> res(I,0);
[1]:
   _[1]=z3-y
   _[2]=yz-x
   _[3]=y3-x2z
   _[4]=xz2-y2
[2]:
   _[1]=x*gen(1)-y*gen(2)-z*gen(4)
   _[2]=z2*gen(2)-y*gen(1)+1*gen(4)
   _[3]=xz*gen(2)-y*gen(4)-1*gen(3)
[3]:
   _[1]=0
```

The first line of the input specifies that the characteristic of the field is 0, the ring variables are x, y, z, and the monomial order is graded reverse lex. The argument "0" in the `res` command says that the resolution should have as many steps as variables (the reason for this choice will become clear in the next section). Here, again, the output is a set of columns that generate (`gen(1), gen(2), gen(3), gen(4)` refer to the standard basis columns e_1, e_2, e_3, e_4 of $k[x, y, z]^4$).

See the exercises below for some additional examples. Of course, this raises the question whether *finite* resolutions always exist. Are we in a situation of potential infinite regress or does this process always stop eventually, as in the examples above? See Exercise 11 below for an example where the answer is no, but where R is not a polynomial ring. We shall return to this question in the next section.

Additional Exercises for §1

Exercise 4.
a. Prove the second bullet, which asserts that $\varphi : M \to N$ is one-to-one if and only if $0 \to M \to N$ is exact.
b. Explain how part b of Proposition (1.2) follows from part a.

Exercise 5. Let M_1, M_2 be R-submodules of an R-module N. Let $M_1 \oplus M_2$ be the direct sum as in Exercise 4 of Chapter 5, §1, and let $M_1 + M_2 \subset N$ be the sum as in Exercise 14 of Chapter 5, §1.
a. Let $\varepsilon : M_1 \cap M_2 \to M_1 \oplus M_2$ be the mapping defined by $\varepsilon(m) = (m, m)$. Show that ε is an R-module homomorphism.
b. Show that $\delta : M_1 \oplus M_2 \to M_1 + M_2$ defined by $\delta(m_1, m_2) = m_1 - m_2$ is an R-module homomorphism.
c. Show that

$$0 \to M_1 \cap M_2 \xrightarrow{\varepsilon} M_1 \oplus M_2 \xrightarrow{\delta} M_1 + M_2 \to 0$$

is an exact sequence.

Exercise 6. Let M_1 and M_2 be submodules of an R-module N.
a. Show that the mappings $\psi_i : M_i \to M_1 + M_2$ $(i = 1, 2)$ defined by $\psi_1(m_1) = m_1 + 0 \in M_1 + M_2$ and $\psi_2(m_2) = 0 + m_2 \in M_1 + M_2$ are one-to-one module homomorphisms. Hence M_1 and M_2 are submodules of $M_1 + M_2$.
b. Consider the homomorphism $\varphi : M_2 \to (M_1 + M_2)/M_1$ obtained by composing the inclusion $M_2 \to M_1 + M_2$ and the natural homomorphism $M_1 + M_2 \to (M_1 + M_2)/M_1$. Identify the kernel of φ, and deduce that there is an isomorphism of R-modules $(M_1 + M_2)/M_1 \cong M_2/(M_1 \cap M_2)$.

Exercise 7.
a. Let

$$0 \to M_n \xrightarrow{\varphi_n} M_{n-1} \xrightarrow{\varphi_{n-1}} M_{n-2} \xrightarrow{\varphi_{n-2}} \cdots \xrightarrow{\varphi_1} M_0 \to 0$$

be a "long" exact sequence of R-modules and homomorphisms. Show that there are "short" exact sequences

$$0 \to \ker(\varphi_i) \to M_i \to \ker(\varphi_{i-1}) \to 0$$

for each $i = 1, \ldots, n$, where the arrow $M_i \to \ker(\varphi_{i-1})$ is given by the homomorphism φ_i.

b. Conversely, given

$$0 \to \ker(\varphi_i) \to M_i \xrightarrow{\varphi_i} N_i \to 0$$

where $N_i = \ker(\varphi_{i-1}) \subset M_{i-1}$, show that these short exact sequences can be spliced together into a long exact sequence

$$0 \to \ker(\varphi_{n-1}) \to M_{n-1} \xrightarrow{\varphi_{n-1}} M_{n-2} \xrightarrow{\varphi_{n-2}} \cdots \xrightarrow{\varphi_2} M_1 \xrightarrow{\varphi_1} \operatorname{im}(\varphi_1) \to 0.$$

c. Explain how a resolution of a module is obtained by splicing together presentations of successive syzygy modules.

Exercise 8. Let V_i, $i = 0, \ldots, n$ be finite dimensional vector spaces over a field k, and let

$$0 \to V_n \xrightarrow{\varphi_n} V_{n-1} \xrightarrow{\varphi_{n-1}} V_{n-2} \xrightarrow{\varphi_{n-2}} \cdots \xrightarrow{\varphi_1} V_0 \to 0$$

be an exact sequence of k-linear mappings. Show that the alternating sum of the dimensions of the V_i satisfies:

$$\sum_{\ell=0}^{n} (-1)^\ell \dim_k(V_\ell) = 0.$$

Hint: Use Exercise 7 and the *dimension theorem* for a linear mapping $\varphi : V \to W$:

$$\dim_k(V) = \dim_k(\ker(\varphi)) + \dim_k(\operatorname{im}(\varphi)).$$

Exercise 9. Let

$$0 \to F_\ell \to \cdots \to F_2 \to F_1 \to F_0 \to M \to 0$$

be a finite free resolution of a submodule $M \subset R^n$. Show how to obtain a finite free resolution of the quotient module R^n/M from the resolution for M. Hint: There is an exact sequence $0 \to M \to R^n \to R^n/M \to 0$ by Proposition (1.2). Use the idea of Exercise 7 part b to splice together the two sequences.

Exercise 10. For each of the following modules, find a free resolution either by hand or by using a computer algebra system.

a. $M = \langle xy, xz, yz \rangle \subset k[x, y, z]$.

b. $M = \langle xy - uv, xz - uv, yz - uv \rangle \subset k[x, y, z, u, v]$.

c. $M = \langle xy - xv, xz - yv, yz - xu \rangle \subset k[x, y, z, u, v]$.

d. M the module generated by the columns of the matrix

$$M = \begin{pmatrix} a^2 + b^2 & a^3 - 2bcd & a - b \\ c^2 - d^2 & b^3 + acd & c + d \end{pmatrix}$$

in $k[a, b, c, d]^2$.

e. $M = \langle x^2, y^2, z^2, xy, xz, yz\rangle \subset k[x, y, z]$.
f. $M = \langle x^3, y^3, x^2y, xy^2\rangle \subset k[x, y, z]$.

Exercise 11. If we work over other rings R besides polynomial rings, then it is not difficult to find modules with no finite free resolutions. For example, consider $R = k[x]/\langle x^2\rangle$, and $M = \langle x\rangle \subset R$.
a. What is the kernel of the mapping $\varphi : R \to M$ given by multiplication by x?
b. Show that

$$\cdots \xrightarrow{x} R \xrightarrow{x} R \xrightarrow{x} M \to 0$$

is an infinite free resolution of M over R, where x denotes multiplication by x.
c. Show that *every* free resolution of M over R is infinite. Hint: One way is to show that any free resolution of M must "contain" the resolution from part b in a suitable sense.

Exercise 12. We say that an exact sequence of R-modules

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

splits if there is a homomorphism $\varphi : P \to N$ such that $g \circ \varphi = \mathrm{id}$.
a. Show that the condition that the sequence above splits is equivalent to the condition that $N \cong M \oplus P$ such that f becomes the inclusion $a \mapsto (a, 0)$ and g becomes the projection $(a, b) \mapsto b$.
b. Show that the condition that the sequence splits is equivalent to the existence of a homomorphism $\psi : N \to M$ such that $\psi \circ f = \mathrm{id}$. Hint: use part a.
c. Show that P is a projective module (that is, a direct summand of a free module—see Definition (4.12) of Chapter 5) if and only if every exact sequence of the form above splits.
d. Show that P is projective if and only if given every homomorphism $f : P \to M_1$ and any surjective homomorphism $g : M_2 \to M_1$, there exists a homomorphism $h : P \to M_2$ such that $f = g \circ h$.

§2 Hilbert's Syzygy Theorem

In §1, we raised the question of whether every R-module has a finite free resolution, and we saw in Exercise 11 that the answer is no if R is the finite-dimensional algebra $R = k[x]/\langle x^2\rangle$. However, when $R = k[x_1, \ldots, x_n]$ the situation is much better, and we will consider only polynomial rings in this section. The main fact we will establish is the following famous result of Hilbert.

(2.1) Theorem (Hilbert Syzygy Theorem). *Let $R = k[x_1, \dots, x_n]$. Then every finitely generated R-module has a finite free resolution of length at most n.*

A comment is in order. As we saw in the examples in §1, it is not true that all finite free resolutions of a given module have the same length. The Syzygy Theorem only asserts the existence of *some* free resolution of length $\leq n$ for every finitely-generated module over the polynomial ring in n variables. Also, remember from Definition (1.9) that length $\leq n$ implies that an R-module M has a free resolution of the form

$$0 \to F_\ell \to \cdots \to F_1 \to F_0 \to M, \quad \ell \leq n.$$

This has $\ell + 1 \leq n + 1$ free modules, so that the Syzygy Theorem asserts the existence of a free resolution with at most $n + 1$ free modules in it.

The proof we will present is due to Schreyer. It is based on the following observation about resolutions produced by the Gröbner basis method described in §1, using Schreyer's Theorem—Theorem (3.3) of Chapter 5.

(2.2) Lemma. *Let $\mathcal{G}$ be a Gröbner basis for a submodule $M \subset R^t$ with respect to an arbitrary monomial order, and arrange the elements of $\mathcal{G}$ to form an ordered s-tuple $G = (g_1, \dots, g_s)$ so that whenever $\operatorname{LT}(g_i)$ and $\operatorname{LT}(g_j)$ contain the same standard basis vector e_k and $i < j$, then $\operatorname{LM}(g_i)/e_k >_{lex} \operatorname{LM}(g_j)/e_k$, where $>_{lex}$ is the lex order on R with $x_1 > \cdots > x_n$. If the variables $x_1, \dots, x_m$ do not appear in the leading terms of $\mathcal{G}$, then $x_1, \dots, x_{m+1}$ do not appear in the leading terms of the $\mathbf{s}_{ij} \in \operatorname{Syz}(G)$ with respect to the order $>_{\mathcal{G}}$ used in Theorem (3.3) of Chapter 5.*

Proof of the lemma. By the first step in the proof of Theorem (3.3) of Chapter 5,

$$\operatorname{LT}_{>_{\mathcal{G}}}(\mathbf{s}_{ij}) = (m_{ij}/\operatorname{LT}(g_i))E_i, \tag{2.3}$$

where $m_{ij} = \operatorname{LCM}(\operatorname{LT}(g_i), \operatorname{LT}(g_j))$, and E_i is the standard basis vector in R^s. As always, it suffices to consider only the $\mathbf{s}_{ij}$ such that $\operatorname{LT}(g_i)$ and $\operatorname{LT}(g_j)$ contain the same standard basis vector e_k in R^t, and such that $i < j$. By the hypothesis on the ordering of the components of G, $\operatorname{LM}(g_i)/e_k >_{lex} \operatorname{LM}(g_j)/e_k$. Since $x_1, \dots, x_m$ do not appear in the leading terms, this implies that we can write

$$\begin{aligned} \operatorname{LM}(g_i)/e_k &= x_{m+1}^a n_i \\ \operatorname{LM}(g_j)/e_k &= x_{m+1}^b n_j, \end{aligned}$$

where $a \geq b$, and n_i, n_j are monomials in R containing only $x_{m+2}, \dots, x_n$. But then $\operatorname{lcm}(\operatorname{LT}(g_i), \operatorname{LT}(g_j))$ contains x_{m+1}^a, and by (2.3), $\operatorname{LT}_{>_{\mathcal{G}}}(\mathbf{s}_{ij})$ does not contain $x_1, \dots, x_m, x_{m+1}$. □

We are now ready for the proof of Theorem (2.1).

PROOF OF THE THEOREM. Since we assume M is finitely generated as an R-module, by (1.5) of this chapter, there is a presentation for M of the form

$$F_1 \stackrel{\varphi_1}{\to} F_0 \to M \to 0 \tag{2.4}$$

corresponding to a choice of a generating set $(f_1, \ldots, f_{r_0})$ for M, and a Gröbner basis $\mathcal{G}_0 = \{g_1, \ldots, g_{r_1}\}$ for $\operatorname{Syz}(f_1, \ldots, f_{r_0}) = \operatorname{im}(\varphi_1) \subset F_0 = R^{r_0}$ with respect to any monomial order on F_0. Order the elements of $\mathcal{G}_0$ as described in Lemma (2.2) to obtain a vector G_0, and apply Schreyer's Theorem to compute a Gröbner basis $\mathcal{G}_1$ for the module $\operatorname{Syz}(G_0) \subset F_1 = R^{r_1}$ (with respect to the $>_{\mathcal{G}_0}$ order). We may assume that $\mathcal{G}_1$ is reduced. By the lemma, at least x_1 will be missing from the leading terms of $\mathcal{G}_1$. Moreover if the Gröbner basis contains r_2 elements, we obtain an exact sequence

$$F_2 \stackrel{\varphi_2}{\to} F_1 \stackrel{\varphi_1}{\to} F_0 \to M \to 0$$

with $F_2 = R^{r_2}$, and $\operatorname{im}(\varphi_2) = \operatorname{Syz}(G_1)$. Now iterate the process to obtain $\varphi_i : F_i \to F_{i-1}$, where $\operatorname{im}(\varphi_i) = \operatorname{Syz}(G_{i-1})$ and $\mathcal{G}_i \subset R^{r_i}$ is a Gröbner basis for $\operatorname{Syz}(G_{i-1})$, where each time we order the Gröbner basis $\mathcal{G}_{i-1}$ to form the vector G_{i-1} so that the hypothesis of Lemma (2.2) is satisfied.

Since the number of variables present in the leading terms of the Gröbner basis elements decreases by at least one at each step, by an easy induction argument, after some number $\ell \leq n$ of steps, the leading terms of the reduced Gröbner basis $\mathcal{G}_\ell$ do not contain any of the variables $x_1, \ldots, x_n$. At this point, we will have extended (2.4) to an exact sequence

$$F_\ell \stackrel{\varphi_\ell}{\to} F_{\ell-1} \to \cdots \to F_1 \stackrel{\varphi_1}{\to} F_0 \to M \to 0, \tag{2.5}$$

and the leading terms in $\mathcal{G}_\ell$ will be non-zero constants times standard basis vectors from F_ℓ. In Exercise 8 below, you will show that this implies $\operatorname{Syz}(G_{\ell-1})$ is a free module, and $\mathcal{G}_\ell$ is a module basis as well as a Gröbner basis. Hence by Proposition (1.12) we can extend (2.5) to another exact sequence by adding a zero at the left, and as a result we have produced a free resolution of length $\ell \leq n$ for M. □

Here are some additional examples illustrating the Syzygy Theorem. In the examples we saw in the text in §1, we always found resolutions of length strictly less than the number of variables in R. But in some cases, the shortest possible resolutions are of length exactly n.

Exercise 1. Consider the ideal $I = \langle x^2 - x, xy, y^2 - y \rangle \subset k[x, y]$ from (1.7) of this chapter, and let $M = k[x, y]/I$, which is also a module over $R = k[x, y]$. Using Exercise 9 from §1, show that M has a free resolution of length 2, of the form

$$0 \to R^2 \to R^3 \to R \to M \to 0.$$

In this case, it is also possible using localization (see Chapter 4) to show that M has no free resolution of length ≤ 1. See Exercise 9 below for a sketch.

On the other hand, we might ask whether having an especially *short* finite free resolution indicates something special about an ideal or a module. For example, if M has a resolution $0 \to R^r \to M \to 0$ of length 0, then M is isomorphic to R^r as an R-module. Hence M is free, and this is certainly a special property! From Chapter 5, §1, we know this happens for ideals only when $M = \langle f \rangle$ is principal. Similarly, we can ask what can be said about free resolutions of length 1. The next examples indicate a special feature of resolutions of length 1 for a certain class of ideals.

Exercise 2. Let $I \subset k[x, y, z, w]$ denote the ideal of the twisted cubic in $\mathbb{P}^3$, with the following generators:

$$I = \langle g_1, g_2, g_3 \rangle = \langle xz - y^2, xw - yz, yw - z^2 \rangle.$$

a. Show that the given generators form a *grevlex* Gröbner basis for I.
b. Apply Schreyer's Theorem to find a Gröbner basis for the module of first syzygies on the given generators for I.
c. Show that $\mathbf{s}_{12}$ and $\mathbf{s}_{23}$ form a basis for $\mathrm{Syz}(xz - y^2, xw - yz, yw - z^2)$.
d. Use the above calculations to produce a finite free resolution of I, of the form

$$0 \to R^2 \xrightarrow{A} R^3 \to I \to 0.$$

e. Show that the determinants of the 2×2 minors of A are just the g_i (up to signs).

Exercise 3. (For this exercise, you will probably want to use a computer algebra system.) In k^2 consider the points

$$p_1 = (0, 0),\ p_2 = (1, 0),\ p_3 = (0, 1)$$
$$p_4 = (2, 1),\ p_5 = (1, 2),\ p_6 = (3, 3),$$

and let $I_i = \mathbf{I}(\{p_i\})$ for each i, so for instance $I_3 = \langle x, y - 1 \rangle$.
a. Find a *grevlex* Gröbner basis for

$$J = \mathbf{I}(\{p_1, \ldots, p_6\}) = I_1 \cap \cdots \cap I_6.$$

b. Compute a free resolution of J of the form

$$0 \to R^3 \xrightarrow{A} R^4 \to J \to 0,$$

where each entry of A is of total degree at most 1 in x and y.
c. Show that the determinants of the 3×3 minors of A are the generators of J (up to signs).

The examples in Exercises 2 and 3 are instances of the following general result, which is a part of the Hilbert-Burch Theorem.

(2.6) Proposition. *Suppose that an ideal I in $R = k[x_1, \ldots, x_n]$ has a free resolution of the form*

$$0 \to R^{m-1} \xrightarrow{A} R^m \xrightarrow{B} I \to 0$$

for some m. Then there exists a nonzero element $g \in R$ such that $B = (\,g\tilde{f}_1 \quad \ldots \quad g\tilde{f}_m\,)$, where $\tilde{f}_i$ is the determinant of the $(m-1) \times (m-1)$ submatrix of A obtained by deleting row i. If k is algebraically closed and $\mathbf{V}(I)$ has dimension $n-2$, then we may take $g = 1$.

PROOF. The proof is outlined in Exercise 11 below. □

The full Hilbert-Burch Theorem also gives a sufficient condition for the existence of a resolution of the form given in the proposition. For example, such a resolution exists when the quotient ring R/I is *Cohen-Macaulay* of codimension 2. This condition is satisfied, for instance, if $I \subset k[x, y, z]$ is the ideal of a finite subset of $\mathbb{P}^2$ (including the case where one or more of the points has multiplicity > 1 as defined in Chapter 4). We will not give the precise definition of the Cohen-Macaulay condition here. Instead we refer the interested reader to [Eis], where this and many of the other known results concerning the shapes of free resolutions for certain classes of ideals in polynomial and local rings are discussed. In particular, the length of the shortest finite free resolution of an R-module M is an important invariant called the *projective dimension* of M.

Additional Exercises for §2

Exercise 4. Let I be the ideal in $k[x, y]$ generated by the *grevlex* Gröbner basis

$$\{g_1, g_2, g_3\} = \{x^2 + 3/2xy + 1/2y^2 - 3/2x - 3/2y, xy^2 - x, y^3 - y\}$$

This ideal was considered in Chapter 2, §2 (with $k = \mathbb{C}$), and we saw there that $\mathbf{V}(I)$ is a finite set containing 5 points in k^2, each with multiplicity 1.

a. Applying Schreyer's Theorem, show that $\mathrm{Syz}(g_1, g_2, g_3)$ is generated by the columns of the matrix

$$A = \begin{pmatrix} y^2 - 1 & 0 \\ -x - 3y/2 + 3/2 & y \\ -y/2 + 3/2 & -x \end{pmatrix}$$

b. Show that the columns of A form a module basis for $\mathrm{Syz}(g_1, g_2, g_3)$, and deduce that I has a finite free resolution of length 1:

$$0 \to R^2 \xrightarrow{A} R^3 \to I \to 0.$$

c. Show that the determinants of the 2×2 minors of A are just the g_i (up to signs).

Exercise 5. Verify that the resolution from (1.8) of §1 has the form given in Proposition (2.6). (In this case too, the module being resolved is the ideal of a finite set of points in k^2, each appearing with multiplicity 1.)

Exercise 6. Let

$$I = \langle z^3 - y, yz - x, y^3 - x^2z, xz^2 - y^2 \rangle$$

be the ideal in $k[x, y, z]$ considered in §1 see (1.16).

a. Show that the generators of I are a Gröbner basis with respect to the *grevlex* order.

b. The `sres` command in `Singular` produces a resolution using Schreyer's algorithm. The `Singular` session is as follows.

```
> ring r=0, (x,y,z), (dp, C);
> ideal I=(z3-y,yz-x,y3-x2z,xz2-y2);
> sres(I,0);
[1]:
  _[1]=yz-x
  _[2]=z3-y
  _[3]=xz2-y2
  _[4]=y3-x2z
[2]:
  _[1]=-z2*gen(1)+y*gen(2)-1*gen(3)
  _[2]=-xz*gen(1)+y*gen(3)+1*gen(4)
  _[3]=-x*gen(2)+y*gen(1)+z*gen(3)
  _[4]=-y2*gen(1)+x*gen(3)+z*gen(4)
[3]:
  _[1]=x*gen(1)+y*gen(3)-z*gen(2)+1*gen(4)
```

Show that the displayed generators are Gröbner bases with respect to the orderings prescribed by Schreyer's Theorem from Chapter 5, §3.

c. Explain why using Schreyer's Theorem produces a longer resolution in this case than that displayed in §1.

Exercise 7. Find a free resolution of length 1 of the form given in Proposition (2.6) for the ideal

$$I = \langle x^4 - x^3y, x^3y - x^2y^2, x^2y^2 - xy^3, xy^3 - y^4 \rangle$$

in $R = k[x, y]$. Identify the matrix A and the element $g \in R$ in this case in Proposition (2.6). Why is $g \neq 1$?

Exercise 8. Let $\mathcal{G}$ be a monic reduced Gröbner basis for a submodule $M \subset R^t$, with respect to some monomial order. Assume that the leading

terms of all the elements of $\mathcal{G}$ are constant multiples of standard basis vectors in R^t.

a. If e_i is the leading term of some element of $\mathcal{G}$, show that it is the leading term of exactly one element of $\mathcal{G}$.
b. Show that $\mathrm{Syz}(\mathcal{G}) = \{0\} \subset R^s$.
c. Deduce that M is a free module.

Exercise 9. In this exercise, we will sketch one way to show that every free resolution of the quotient R/I for

$$I = \langle x^2 - x, xy, y^2 - y \rangle \subset R = k[x, y]$$

has length ≥ 2. In other words, the resolution $0 \to R^2 \to R^3 \to R \to R/I \to 0$ from Exercise 1 is as short as possible. We will need to use some ideas from Chapter 4 of this book.

a. Let M be an R-module, and let P be a maximal ideal in R. Generalizing the construction of the local ring R_P, define the *localization* of M at P, written M_P, to be the set of "fractions" m/f, where $m \in M$, $f \notin P$, subject to the relation that $m/f = m'/f'$ whenever there is some $g \in R$, $g \notin P$ such that $g(f'm - fm') = 0$ in M. Show that M_P has the structure of a module over the local ring R_P. If M is a free R-module, show that M_P is a free R_P-module.
b. Given a homomorphism $\varphi : M \to N$ of R-modules, show that there is an induced homomorphism of the localized modules $\varphi_P : M_P \to N_P$ defined by $\varphi_P(m/f) = \varphi(m)/f$ for all $m/f \in M_P$. Hint: First show that this rule gives a well-defined mapping from M_P to N_P.
c. Let

$$M_1 \stackrel{\varphi_1}{\to} M_2 \stackrel{\varphi_2}{\to} M_3$$

be an exact sequence of R-modules. Show that the localized sequence

$$(M_1)_P \stackrel{(\varphi_1)_P}{\longrightarrow} (M_2)_P \stackrel{(\varphi_2)_P}{\longrightarrow} (M_3)_P$$

is also exact.
d. We want to show that the shortest free resolution of $M = R/I$ for $I = \langle x^2 - x, xy, y^2 - y \rangle$ has length 2. Aiming for a contradiction, suppose that there is some resolution of length 1: $0 \to F_1 \to F_0 \to M \to 0$. Explain why we may assume $F_0 = R$.
e. By part c, after localizing at $P = \langle x, y \rangle \supset I$, we obtain a resolution $0 \to (F_1)_P \to R_P \to M_P \to 0$. Show that M_P is isomorphic to $R_P/\langle x, y \rangle R_P \cong k$ as an R_P-module.
f. But then the image of $(F_1)_P \to R_P$ must be $\langle x, y \rangle$. Show that we obtain a contradiction because this is not a free R_P-module.

Exercise 10. In $R = k[x_1, \ldots, x_n]$, consider the ideals

$$I_m = \langle x_1, x_2, \ldots, x_m \rangle$$

generated by subsets of the variables, for $1 \leq m \leq n$.

a. Find explicit resolutions for the ideals $I_2, \dots, I_5$ in $k[x_1, \dots, x_5]$.
b. Show in general that I_m has a free resolution of length $m-1$ of the form

$$0 \to R^{\binom{m}{m}} \to \cdots \to R^{\binom{m}{3}} \to R^{\binom{m}{2}} \to R^m \to I \to 0,$$

where if we index the basis B_k of $R^{\binom{m}{k}}$ by k-element subsets of $\{1, \dots, m\}$:

$$B_k = \{e_{i_1 \dots i_k} : 1 \le i_1 < i_2 < \cdots < i_k \le m\},$$

then the mapping $\varphi_k : R^{\binom{m}{k}} \to R^{\binom{m}{k-1}}$ in the resolution is defined by

$$\varphi_k(e_{i_1 \dots i_k}) = \sum_{j=1}^{k} (-1)^{j+1} x_{i_j} e_{i_1 \dots i_{j-1} i_{j+1} \dots i_k},$$

where in the term with index j, i_j is omitted to yield a $(k-1)$-element subset. These resolutions are examples of *Koszul complexes*. See [Eis] for more information about this topic.

Exercise 11. In this exercise, we will sketch a proof of Proposition (2.6). The basic idea is to consider the linear mapping from K^{m-1} to K^m defined by the matrix A in a resolution

$$0 \to R^{m-1} \xrightarrow{A} R^m \xrightarrow{B} I \to 0,$$

where $K = k(x_1, \dots, x_n)$ is the field of rational functions (the field of fractions of R) and to use some linear algebra over K.

a. Let V be the space of solutions of the the homogeneous system of linear equations $XA = 0$ where $X \in K^m$ is written as a row vector. Show that the dimension over K of V is 1. Hint: The columns $A_1, \dots, A_{m-1}$ of A are linearly independent over R, hence over K.
b. Let $B = \begin{pmatrix} f_1 & \dots & f_m \end{pmatrix}$ and note that exactness implies that $BA = 0$. Let $\tilde{f}_i = (-1)^{i+1} \det(A_i)$, where A_i is the $(m-1) \times (m-1)$ submatrix of A obtained by deleting row i. Show that $X = (\tilde{f}_1, \dots, \tilde{f}_m)$ is also an element of the space V of solutions of $XA = 0$. Hint: append any one of the columns of A to A to form an $m \times m$ matrix $\widetilde{A}$, and expand $\det(\widetilde{A})$ by minors along the new column.
c. Deduce that there is some $r \in K$ such that $r\tilde{f}_i = f_i$ for all $i = 1, \dots, m$.
d. Write $r = g/h$ where $g, h \in R$ and the fraction is in lowest terms, and consider the equations $g\tilde{f}_i = hf_i$. We want to show that h must be a nonzero constant, arguing by contradiction. If not, then let p be any irreducible factor of h. Show that $A_1, \dots, A_{m-1}$ are linearly dependent modulo $\langle p \rangle$, or in other words that there exist $r_1, \dots, r_{m-1}$ not all in $\langle p \rangle$ such that $r_1 A_1 + \cdots + r_{m-1} A_{m-1} = pB$ for some $B \in R^m$.
e. Continuing from part d, show that $B \in \operatorname{Syz}(f_1, \dots, f_m)$ also, so that $B = s_1 A_1 + \cdots + s_{m-1} A_{m-1}$ for some $s_i \in R$.

f. Continuing from part e, show that $(r_1 - ps_1, \ldots, r_{m-1} - ps_{m-1})^T$ would be a syzygy on the columns of A. Since those columns are linearly independent over R, $r_i - ps_i = 0$ for all i. Deduce a contradiction to the way we chose the r_i.
g. Finally, in the case that $\mathbf{V}(I)$ has dimension $n-2$, show that g must be a nonzero constant also. Hence by multiplying each f_i by a nonzero constant, we could take $g = 1$ in Proposition (2.6).

§3 Graded Resolutions

In algebraic geometry, free resolutions are often used to study the homogeneous ideals $I = \mathbf{I}(V)$ of projective varieties $V \subset \mathbb{P}^n$ and other modules over $k[x_0, \ldots, x_n]$. The key fact we will use is that these resolutions have an extra structure coming from the *grading* on the ring $R = k[x_0, \ldots, x_n]$, that is the direct sum decomposition

$$R = \bigoplus_{s \geq 0} R_s \tag{3.1}$$

into the additive subgroups (or k-vector subspaces) $R_s = k[x_0, \ldots, x_n]_s$, consisting of the homogeneous polynomials of total degree s, together with 0. To begin this section we will introduce some convenient notation and terminology for describing such resolutions.

(3.2) Definition. A *graded module* over R is a module M with a family of subgroups $\{M_t : t \in \mathbb{Z}\}$ of the additive group of M. The elements of M_t are called the *homogeneous elements* of degree t in the grading, and the M_t must satisfy the following properties.
a. As additive groups,

$$M = \bigoplus_{t \in \mathbb{Z}} M_t.$$

b. The decomposition of M in part a is compatible with the multiplication by elements of R in the sense that $R_s M_t \subset M_{s+t}$ for all $s \geq 0$ and all $t \in \mathbb{Z}$.

It is easy to see from the definition that each M_t is a module over the subring $R_0 = k \subset R$, hence a k-vector subspace of M. If M is finitely-generated, the M_t are finite dimensional over k.

Homogeneous ideals $I \subset R$ are the most basic examples of graded modules. Recall that an ideal is homogeneous if whenever $f \in I$, the homogeneous components of f are all in I as well (see for instance, [CLO], Chapter 8, §3, Definition 1). Some of the other important properties of these ideals are summarized in the following statement.

- (Homogeneous Ideals) Let $I \subset k[x_0, \ldots, x_n]$ be an ideal. Then the following are equivalent:
  a. I is a homogeneous ideal.
  b. $I = \langle f_1, \ldots, f_s \rangle$ where f_i are homogeneous polynomials.
  c. A reduced Gröbner basis for I (with respect to any monomial order) consists of homogeneous polynomials.

(See for instance [CLO], Theorem 2 of Chapter 8, §3.)

To show that a homogeneous ideal I has a graded module structure, set $I_t = I \cap R_t$. For $t \geq 0$, this is the set of all homogeneous elements of total degree t in I (together with 0), and $I_t = \{0\}$ for $t < 0$. By the definition of a homogeneous ideal, we have $I = \oplus_{t \in \mathbb{Z}} I_t$, and $R_s I_t \subset I_{s+t}$ is a direct consequence of the definition of an ideal and the properties of polynomial multiplication.

The free modules R^m are also graded modules over R provided we take $(R^m)_t = (R_t)^m$. We will call this the *standard* graded module structure on R^m. Other examples of graded modules are given by submodules of the free modules R^m with generating sets possessing suitable homogeneity properties, and we have statements analogous to those above for homogeneous ideals.

(3.3) Proposition. *Let $M \subset R^m$ be submodule. Then the following are equivalent.*

a. *The standard grading on R^m induces a graded module structure on M, given by taking $M_t = (R_t)^m \cap M$—the set of elements in M where each component is a homogeneous polynomial of degree t (or 0).*
b. *$M = \langle f_1, \ldots, f_r \rangle$ in R^m where each f_i is a vector of homogeneous polynomials of the same degree d_i.*
c. *A reduced Gröbner basis (for any monomial order on R^m) consists of vectors of homogeneous polynomials where all the components of each vector have the same degree.*

PROOF. The proof is left to the reader as Exercise 8 below. □

Submodules, direct sums, and quotient modules extend to graded modules in the following ways. If M is a graded module and N is a submodule of M, then we say N is a *graded submodule* if the additive subgroups $N_t = M_t \cap N$ for $t \in \mathbb{Z}$ define a graded module structure on N. For example, Proposition (3.3) says that the submodules $M = \langle f_1, \ldots, f_r \rangle$ in R^m where each f_i is a vector of homogeneous polynomials of the same degree d_i are graded submodules of R^m.

Exercise 1.

a. Given a collection of graded modules $M_1, \ldots, M_m$, we can produce the direct sum $N = M_1 \oplus \cdots \oplus M_m$ as usual. In N, let

$$N_t = (M_1)_t \oplus \cdots \oplus (M_m)_t.$$

Show that the N_t define the structure of a graded module on N.

b. If $N \subset M$ is a graded submodule of a graded module M, show that the quotient module M/N also has a graded module structure, defined by the collection of additive subgroups

$$(M/N)_t = M_t/N_t = M_t/(M_t \cap N).$$

Given any graded R-module M, we can also produce modules that are isomorphic to M as abstract R-modules, but with different gradings, by the following trick of shifting the indexing of the family of submodules.

(3.4) Proposition. *Let M be a graded R-module, and let d be an integer. Let $M(d)$ be the direct sum*

$$M(d) = \bigoplus_{t \in \mathbb{Z}} M(d)_t,$$

where $M(d)_t = M_{d+t}$. Then $M(d)$ is also a graded R-module.

PROOF. The proof is left to the reader as Exercise 9. □

For instance, the modules $(R^m)(d) = R(d)^m$ are called shifted or *twisted* graded free modules over R. The standard basis vectors e_i still form a module basis for $R(d)^m$, but they are now homogeneous elements of degree $-d$ in the grading, since $R(d)_{-d} = R_0$. More generally, part a of Exercise 1 shows that we can consider graded free modules of the form

$$R(d_1) \oplus \cdots \oplus R(d_m)$$

for any integers $d_1, \ldots, d_m$, where the basis vector e_i is homogeneous of degree $-d_i$ for each i.

Exercise 2. This exercise will generalize Proposition (3.3). Suppose that we have integers $d_1, \ldots, d_m$ and elements $f_1, \ldots, f_s \in R^m$ such that

$$f_i = (f_{i1}, \ldots, f_{im})^T$$

where the f_{ij} are homogeneous and $\deg f_{i1} - d_1 = \cdots = \deg f_{im} - d_m$ for each i. Then prove that $M = \langle f_1, \ldots, f_s \rangle$ is a graded submodule of $F = R(d_1) \oplus \cdots \oplus R(d_m)$. Also show that every graded submodule of F has a set of generators of this form.

As the examples given later in the section will show, the twisted free modules we deal with are typically of the form

$$R(-d_1) \oplus \cdots \oplus R(-d_m).$$

Here, the standard basis elements $e_1, \ldots, e_m$ have respective degrees $d_1, \ldots, d_m$.

Next we consider how homomorphisms interact with gradings on modules.

(3.5) Definition. Let M, N be graded modules over R. A homomorphism $\varphi : M \to N$ is said to a *graded homomorphism of degree* d if $\varphi(M_t) \subset N_{t+d}$ for all $t \in \mathbb{Z}$.

For instance, suppose that M is a graded R-module generated by homogeneous elements $f_1, \ldots, f_m$ of degrees $d_1, \ldots, d_m$. Then we get a graded homomorphism

$$\varphi : R(-d_1) \oplus \cdots \oplus R(-d_m) \longrightarrow M$$

which sends the standard basis element e_i to $f_i \in M$. Note that φ is onto. Also, since e_i has degree d_i, it follows that φ has degree zero.

Exercise 3. Suppose that M is a finitely generated R-module. As usual, M_t denotes the set of homogeneous elements of M of degree t.

a. Prove that M_t is a finite dimensional vector space over the field k and that $M_t = \{0\}$ for $t \ll 0$. Hint: Use the surjective map φ constructed above.
b. Let $\psi : M \to M$ be a graded homomorphism of degree zero. Prove that ψ is an isomorphism if and only if $\psi : M_t \to M_t$ is onto for every t. Conclude that ψ is an isomorphism if and only if it is onto.

Another example of a graded homomorphism is given by an $m \times p$ matrix A all of whose entries are homogeneous polynomials of degree d in the ring R. Then A defines a graded homomorphism φ of degree d by matrix multiplication

$$\begin{aligned} \varphi : R^p &\to R^m \\ f &\mapsto Af. \end{aligned}$$

If desired, we can also consider A as defining a graded homomorphism of degree zero from the shifted module $R(-d)^p$ to R^m. Similarly, if the entries of the jth column are all homogeneous polynomials of degree d_j, but the degree varies with the column, then A defines a graded homomorphism of degree zero

$$R(-d_1) \oplus \cdots \oplus R(-d_p) \to R^m.$$

Still more generally, a graded homomorphism of degree zero

$$R(-d_1) \oplus \cdots \oplus R(-d_p) \to R(-c_1) \oplus \cdots \oplus R(-c_m)$$

is defined by an $m \times p$ matrix A where the ij entry $a_{ij} \in R$ is homogeneous of degree $d_j - c_i$ for all i, j. We will call a matrix A satisfying this condition

for some collection d_j of column degrees and some collection c_i of row degrees a *graded matrix* over R.

The reason for discussing graded matrices in detail is that these matrices appear in free resolutions of graded modules over R. For example, consider the resolution of the homogeneous ideal

$$M = \langle z^3 - yw^2, yz - xw, y^3 - x^2z, xz^2 - y^2w \rangle$$

in $R = k[x, y, z, w]$ from (1.13) of this chapter, computed using *Macaulay 2*. The ideal itself is the image of a graded homomorphism of degree zero

$$R(-3) \oplus R(-2) \oplus R(-3)^2 \to R,$$

where the shifts are just the negatives of the degrees of the generators, ordered as above. The next matrix in the resolution:

$$A = \begin{pmatrix} -y^2 & -xz & -yw & -z^2 \\ z & w & 0 & 0 \\ x & y & -z & -w \\ 0 & 0 & x & y \end{pmatrix}$$

(whose columns generate the module of syzygies on the generators of M) defines a graded homomorphism of degree zero

$$R(-4)^4 \xrightarrow{A} R(-2) \oplus R(-3)^3.$$

In other words, $d_j = 4$ for all j, and $c_2 = c_3 = c_4 = 3, c_1 = 2$ in the notation as above, so all entries on rows 2, 3, 4 of A are homogeneous of degree $4 - 3 = 1$, while those on row 1 have degree $4 - 2 = 2$. The whole resolution can be written in the form

$$0 \to R(-5) \to R(-4)^4 \to R(-2) \oplus R(-3)^3 \to M \to 0, \tag{3.6}$$

where all the arrows are graded homomorphisms of degree zero.

Here is the precise definition of a graded resolution.

(3.7) Definition. If M is a graded R-module, then a *graded resolution* of M is a resolution of the form

$$\cdots \to F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \to 0,$$

where each F_ℓ is a twisted free graded module $R(-d_1) \oplus \cdots \oplus R(-d_p)$ and each homomorphism φ_ℓ is a graded homomorphism of degree zero (so that the φ_ℓ are given by graded matrices as defined above).

The resolution given in (3.6) is clearly a graded resolution. What's nice is that *every* finitely generated graded R-module has a graded resolution of finite length.

(3.8) Theorem (Graded Hilbert Syzygy Theorem). *Let $R = k[x_1, \dots, x_n]$. Then every finitely generated graded R-module has a finite graded resolution of length at most n.*

PROOF. This follows from the proof of Theorem (2.1) (the Syzygy Theorem in the ungraded case) with minimal changes. The reason is that by Proposition (3.3) and the generalization given in Exercise 2, if we apply Schreyer's theorem to find generators for the module of syzygies on a homogeneous ordered Gröbner basis $(g_1, \dots, g_s)$ for a graded submodule of $R(-d_1) \oplus \cdots \oplus R(-d_p)$, then the syzygies $\mathbf{s}_{ij}$ are also homogeneous and "live" in another graded submodule of the same form. We leave the details of the proof as Exercise 5 below. □

The `resolution` command in *Macaulay 2* will compute a finite graded resolution using the method outlined in the proof of Theorem (3.8). However, the resolutions produced by *Macaulay 2* are of a very special sort.

(3.9) Definition. Suppose that

$$\cdots \to F_\ell \xrightarrow{\varphi_\ell} F_{\ell-1} \to \cdots \to F_0 \to M \to 0$$

is a graded resolution of M. Then the resolution is *minimal* if for every $\ell \geq 1$, the nonzero entries of the graded matrix of φ_ℓ have positive degree.

For an example, the reader should note that the resolution (3.6) is a minimal resolution. But not all resolutions are minimal, as shown by the following example.

Exercise 4. Show that the resolution from (1.11) can be homogenized to give a graded resolution, and explain why it is not minimal. Also show that the resolution from (1.10) is minimal after we homogenize.

In *Macaulay 2*, `resolution` computes a minimal resolution.

We will soon see that minimal resolutions have many nice properties. But first, let's explain why they are called "minimal". We say that a set of generators of a module is *minimal* if no proper subset generates the module. Now suppose that we have a graded resolution

$$\cdots \to F_\ell \xrightarrow{\varphi_\ell} F_{\ell-1} \to \cdots \to F_0 \to M \to 0.$$

Each φ_ℓ gives a surjective map $F_\ell \to \operatorname{im}(\varphi_\ell)$, so that φ_ℓ takes the standard basis of F_ℓ to a generating set of $\operatorname{im}(\varphi_\ell)$. Then we can characterize minimality as follows.

(3.10) Proposition. *The above resolution is minimal if and only if for each $\ell \geq 0$, φ_ℓ takes the standard basis of F_ℓ to a minimal generating set of* $\mathrm{im}(\varphi_\ell)$.

PROOF. We will prove one direction and leave the other as an exercise. Suppose that for some $\ell \geq 1$ the graded matrix A_ℓ of φ_ℓ has entries of positive degree. We will show that $\varphi_{\ell-1}$ takes the standard basis of $F_{\ell-1}$ to a minimal generating set of $\mathrm{im}(\varphi_{\ell-1})$. Let $e_1, \ldots, e_m$ be the standard basis vectors of $F_{\ell-1}$. If $\varphi_{\ell-1}(e_1), \ldots, \varphi_{\ell-1}(e_m)$ is not a minimal generating set, then some $\varphi_{\ell-1}(e_i)$ can be expressed in terms of the others. Reordering the basis if necessary, we can assume that

$$\varphi_{\ell-1}(e_1) = \sum_{i=2}^{m} a_i \varphi_{\ell-1}(e_i), \quad a_i \in R.$$

Then $\varphi_{\ell-1}(e_1 - a_2 e_2 - \cdots - a_m e_m) = 0$, so $(1, -a_2, \ldots, -a_m) \in \ker(\varphi_{\ell-1})$. By exactness, $(1, -a_2, \ldots, -a_m) \in \mathrm{im}(\varphi_\ell)$. Since A_ℓ is the matrix of φ_ℓ, the columns of A_ℓ generate $\mathrm{im}(\varphi_\ell)$. We are assuming that the nonzero components of these columns have positive degree. Since the first entry of $(1, -a_2, \ldots, -a_m)$ is a nonzero constant, it follows that this vector cannot be an R-linear combination of the columns of A_ℓ. This contradiction proves that the $\varphi_{\ell-1}(e_i)$ give a minimal generating set of $\mathrm{im}(\varphi_{\ell-1})$. □

The above proposition shows that minimal resolutions are very intuitive. For example, suppose that we have built a graded resolution of an R-module M out to stage $\ell - 1$:

$$F_{\ell-1} \stackrel{\varphi_{\ell-1}}{\to} F_{\ell-2} \to \cdots \to F_0 \to M \to 0.$$

We extend one more step by picking a generating set of $\ker(\varphi_{\ell-1})$ and defining $\varphi_\ell : F_\ell \to \ker(\varphi_{\ell-1}) \subset F_{\ell-1}$ by mapping the standard basis of F_ℓ to the chosen generating set. To be efficient, we should pick a minimal generating set, and if we do this at every step of the construction, then Proposition (3.10) guarantees that we get a minimal resolution.

Exercise 5. Give a careful proof of Theorem (3.8) (the Graded Syzygy Theorem), and then modify the proof to show that every finitely generated graded module over $k[x_1, \ldots, x_n]$ has a *minimal* resolution of length $\leq n$. Hint: Use Proposition (3.10).

We next discuss to what extent a minimal resolution is unique. The first step is to define what it means for two resolutions to be the same.

(3.11) Definition. Two graded resolutions $\cdots \to F_0 \stackrel{\varphi_0}{\to} M \to 0$ and $\cdots \to G_0 \stackrel{\psi_0}{\to} M \to 0$ are *isomorphic* if there are graded isomorphisms $\alpha_\ell : F_\ell \to G_\ell$ of degree zero such that $\psi_0 \circ \alpha_0 = \varphi_0$ and, for every $\ell \geq 1$,

the diagram

$$\begin{array}{ccc} F_\ell & \xrightarrow{\varphi_\ell} & F_{\ell-1} \\ \alpha_\ell \downarrow & & \downarrow \alpha_{\ell-1} \\ G_\ell & \xrightarrow{\psi_\ell} & G_{\ell-1} \end{array} \tag{3.12}$$

commutes, meaning $\alpha_{\ell-1} \circ \varphi_\ell = \psi_\ell \circ \alpha_\ell$.

We will now show that a finitely generated graded module M has a unique minimal resolution up to isomorphism.

(3.13) Theorem. *Any two minimal resolutions of M are isomorphic.*

PROOF. We begin by defining $\alpha_0 : F_0 \to G_0$. If $e_1, \dots, e_m$ is the standard basis of F_0, then we get $\varphi_0(e_i) \in M$, and since $G_0 \to M$ is onto, we can find $g_i \in G_0$ such that $\psi_0(g_i) = \varphi_0(e_i)$. Then setting $\alpha_0(e_i) = g_i$ defines a graded homomorphism $\alpha_0 : F_0 \to G_0$ of degree zero, and it follows easily that $\psi_0 \circ \alpha_0 = \varphi_0$.

A similar argument gives $\beta_0 : G_0 \to F_0$, also a graded homomorphism of degree zero, such that $\varphi_0 \circ \beta_0 = \psi_0$. Thus $\beta_0 \circ \alpha_0 : F_0 \to F_0$, and if $1_{F_0} : F_0 \to F_0$ denotes the identity map, then

$$\varphi_0 \circ (1_{F_0} - \beta_0 \circ \alpha_0) = \varphi_0 - (\varphi_0 \circ \beta_0) \circ \alpha_0 = \varphi_0 - \psi_0 \circ \alpha_0 = 0. \tag{3.14}$$

We claim that (3.14) and minimality imply that $\beta_0 \circ \alpha_0$ is an isomorphism.

To see why, first recall from the proof of Proposition (3.10) that the columns of the matrix representing φ_1 generate $\operatorname{im}(\varphi_1)$. By minimality, the nonzero entries in these columns have positive degree. If we let $\langle x_1, \dots, x_n \rangle F_0$ denote the submodule of F_0 generated by $x_i e_j$ for all i, j, it follows that $\operatorname{im}(\varphi_1) \subset \langle x_1, \dots, x_n \rangle F_0$.

However, (3.14) implies that $\operatorname{im}(1_{F_0} - \beta_0 \circ \alpha_0) \subset \ker(\varphi_0) = \operatorname{im}(\varphi_1)$. By the previous paragraph, we see that $v - \beta_0 \circ \alpha_0(v) \in \langle x_1, \dots, x_n \rangle F_0$ for all $v \in F_0$. In Exercise 11 at the end of the section, you will show that this implies that $\beta_0 \circ \alpha_0$ is an isomorphism. In particular, α_0 is one-to-one.

By a similar argument using the minimality of the graded resolution $\cdots \to G_0 \to M \to 0$, $\alpha_0 \circ \beta_0$ is also an isomorphism, which implies that α_0 is onto. Hence α_0 is an isomorphism as claimed. Then Exercise 12 at the end of the section will show that α_0 induces an isomorphism $\bar{\alpha}_0 : \ker(\varphi_0) \to \ker(\psi_0)$.

Now we can define α_1. Since $\varphi_1 : F_1 \to \operatorname{im}(\varphi_1) = \ker(\varphi_0)$ is onto, we get a minimal resolution

$$\cdots \to F_1 \xrightarrow{\varphi_1} \ker(\varphi_0) \to 0,$$

of $\ker(\varphi_0)$ (see Exercise 7 of §1), and similarly

$$\cdots \to G_1 \xrightarrow{\psi_1} \ker(\psi_0) \to 0$$

is a minimal resolution of $\ker(\psi_0)$. Then, using the isomorphism $\bar{\alpha}_0 : \ker(\varphi_0) \to \ker(\psi_0)$ just constructed, the above argument easily adapts to give a graded isomorphism $\alpha_1 : F_1 \to G_1$ of degree zero such that $\bar{\alpha}_0 \circ \varphi_1 = \psi_1 \circ \alpha_1$. Since $\bar{\alpha}_0$ is the restriction of α_0 to $\operatorname{im}(\varphi_1)$, it follows easily that (3.12) commutes (with $\ell = 1$).

If we apply Exercise 12 again, we see that α_1 induces an isomorphism $\bar{\alpha}_1 : \ker(\varphi_1) \to \ker(\psi_1)$. Repeating the above process, we can now define α_2 with the required properties, and continuing for all ℓ, the theorem now follows easily. □

Since we know by Exercise 5 that a finitely generated R-module M has a finite minimal resolution, it follows from Theorem (3.13) that *all* minimal resolutions of M are finite. This fact plays a crucial role in the following refinement of the Graded Syzygy Theorem.

(3.15) Theorem. *If*

$$\cdots \to F_\ell \xrightarrow{\varphi_\ell} F_{\ell-1} \to \cdots \to F_0 \to M \to 0,$$

is any graded resolution of M over $k[x_1, \ldots, x_n]$, then the kernel $\ker(\varphi_{n-1})$ is free, and

$$0 \to \ker(\varphi_{n-1}) \to F_{n-1} \to \cdots \to F_0 \to M \to 0$$

is a graded resolution of M.

Proof. We begin by showing how to simplify a given graded resolution $\cdots \to F_0 \to M \to 0$. Suppose that for some $\ell \geq 1$, $\varphi_\ell : F_\ell \to F_{\ell-1}$ is not minimal, i.e., the matrix A_ℓ of φ_ℓ has a nonzero entry of degree zero. If we order the standard bases $\{e_1, \ldots, e_m\}$ of F_ℓ and $\{u_1, \ldots, u_t\}$ of $F_{\ell-1}$ appropriately, we can assume that

$$\varphi_\ell(e_1) = c_1u_1 + c_2u_2 + \cdots + c_tu_t \tag{3.16}$$

where c_1 is a nonzero constant (note that $(c_1, \ldots, c_t)^T$ is the first column of A_ℓ). Then let $G_\ell \subset F_\ell$ and $G_{\ell-1} \subset F_{\ell-1}$ be the submodules generated by $\{e_2, \ldots, e_m\}$ and $\{u_2, \ldots, u_t\}$ respectively, and define the maps

$$F_{\ell+1} \xrightarrow{\psi_{\ell+1}} G_\ell \xrightarrow{\psi_\ell} G_{\ell-1} \xrightarrow{\psi_{\ell-1}} F_{\ell-2}$$

as follows:

- $\psi_{\ell+1}$ is the projection $F_\ell \to G_\ell$ (which sends $a_1e_1 + a_2e_2 + \cdots + a_me_m$ to $a_2e_2 + \cdots + a_me_m$) composed with $\varphi_{\ell+1}$.
- If the first row of A_ℓ is $(c_1, d_2, \ldots, d_m)$, then ψ_ℓ is defined by $\psi_\ell(e_i) = \varphi_\ell(e_i - \frac{d_i}{c_1}e_1)$ for $i = 2, \ldots, m$. Since $\varphi_\ell(e_i) = d_iu_1 + \cdots$ for $i \geq 2$, it follows easily from (3.16) that $\psi_\ell(e_i) \in G_{\ell-1}$.
- $\psi_{\ell-1}$ is the restriction of $\varphi_{\ell-1}$ to the submodule $G_{\ell-1} \subset F_{\ell-1}$.

We claim that

$$\cdots \to F_{\ell+2} \overset{\varphi_{\ell+1}}{\to} F_{\ell+1} \overset{\psi_{\ell+1}}{\to} G_\ell \overset{\psi_\ell}{\to} G_{\ell-1} \overset{\psi_{\ell-1}}{\to} F_{\ell-2} \overset{\varphi_{\ell-2}}{\to} F_{\ell-3} \to \cdots$$

is still a resolution of M. To prove this, we need to check exactness at $F_{\ell+1}$, G_ℓ, $G_{\ell-1}$ and $F_{\ell-2}$. (If we set $M = F_{-1}$ and $F_k = 0$ for $k < -1$, then the above sequence makes sense for all $\ell \geq 1$.)

We begin with $F_{\ell-2}$. Here, note that applying $\varphi_{\ell-1}$ to (3.16) gives

$$0 = c_1\varphi_{\ell-1}(u_1) + c_2\varphi_{\ell-1}(u_2) + \cdots + c_2\varphi_{\ell-1}(u_m).$$

Since c_1 is a nonzero constant, $\varphi_{\ell-1}(u_1)$ is an R-linear combination of $\varphi_{\ell-1}(u_i)$ for $i = 2, \ldots, m$, and then $\operatorname{im}(\varphi_{\ell-1}) = \operatorname{im}(\psi_{\ell-1})$ follows from the definition of $\psi_{\ell-1}$. The desired exactness $\operatorname{im}(\psi_{\ell-1}) = \ker(\varphi_{\ell-2})$ is now an easy consequence of the exactness of the original resolution.

Next consider $G_{\ell-1}$. First note that for $i \geq 2$, $\psi_{\ell-1} \circ \psi_\ell(e_i) = \psi_{\ell-1} \circ \varphi_\ell(e_i - \frac{d_i}{c_1} e_1) = 0$ since $\psi_{\ell-1}$ is just the restriction of $\varphi_{\ell-1}$. This shows that $\operatorname{im}(\psi_\ell) \subset \ker(\psi_{\ell-1})$. To prove the opposite inclusion, suppose that $\psi_{\ell-1}(v) = 0$ for some $v \in G_{\ell-1}$. Since $\psi_{\ell-1}$ is the restriction of $\varphi_{\ell-1}$, exactness of the original resolution implies that $v = \varphi_\ell(a_1e_1 + \cdots + a_me_m)$. However, since u_1 does not appear in $v \in G_{\ell-1}$ and $\varphi_\ell(e_i) = d_iu_1 + \cdots$, one easily obtains

$$a_1c_1 + a_2d_2 + \cdots + a_md_m = 0 \tag{3.17}$$

by looking at the coefficients of u_1. Then

$$\begin{aligned}\psi_\ell(a_2e_2 + \cdots + a_me_m) &= a_2\psi_\ell(e_2) + \cdots + a_m\psi_\ell(e_m)\\ &= a_2\varphi_\ell(e_2 - \tfrac{d_2}{c_1} e_1) + \cdots + a_m\varphi_\ell(e_m - \tfrac{d_m}{c_1} e_1)\\ &= \varphi_\ell(a_1e_1 + \cdots + a_me_m) = v,\end{aligned}$$

where the last equality follows by (3.17). This completes the proof of exactness at $G_{\ell-1}$.

The remaining proofs of exactness are straightforward and will be covered in Exercise 13 at the end of the section.

Since the theorem we're trying to prove is concerned with $\ker(\varphi_{n-1})$, we need to understand how the kernels of the various maps change under the above simplification process. If $e_1 \in F_\ell$ has degree d, then we claim that:

$$\begin{aligned}\ker(\varphi_{\ell-1}) &\cong R(-d) \oplus \ker(\psi_{\ell-1})\\ \ker(\varphi_\ell) &\cong \ker(\psi_\ell)\\ \ker(\varphi_{\ell+1}) &= \ker(\psi_{\ell+1})\end{aligned} \tag{3.18}$$

We will prove the first and leave the others for the reader (see Exercise 13). Since $\psi_{\ell-1}$ is the restriction of $\varphi_{\ell-1}$, we certainly have $\ker(\psi_{\ell-1}) \subset \ker(\varphi_{\ell-1})$. Also, $\varphi_\ell(e_1) \in \ker(\varphi_{\ell-1})$ gives the submodule $R\varphi_\ell(e_1) \subset \ker(\varphi_{\ell-1})$, and the map sending $\varphi_\ell(e_1) \mapsto 1$ induces an isomorphism $R\varphi_\ell(e_1) \cong R(-d)$. To prove that we have a direct sum, note that (3.16)

implies $R\varphi_\ell(e_1) \cap G_{\ell-1} = \{0\}$ since $G_{\ell-1}$ is generated by $u_2, \dots, u_m$ and c_1 is a nonzero constant. From this, we conclude $R\varphi_\ell(e_1) \cap \ker(\psi_{\ell-1}) = \{0\}$, which implies

$$R\varphi_\ell(e_1) + \ker(\psi_{\ell-1}) = R\varphi_\ell(e_1) \oplus \ker(\psi_{\ell-1}).$$

To show that this equals all of $\ker(\varphi_{\ell-1})$, let $w \in \ker(\varphi_{\ell-1})$ be arbitrary. If $w = a_1u_1 + \cdots + a_tu_t$, then set $\widetilde{w} = w - \frac{a_1}{c_1}\varphi_\ell(e_1)$. By (3.16), we have $\widetilde{w} \in G_{\ell-1}$, and then $\widetilde{w} \in \ker(\psi_{\ell-1})$ follows easily. Thus $w = \frac{a_1}{c_1}\varphi_\ell(e_1) + \widetilde{w} \in R\varphi_\ell(e_1) \oplus \ker(\psi_{\ell-1})$, which gives the desired direct sum decomposition.

Hence, we have proved that whenever we have a φ_ℓ with a nonzero matrix entry of degree zero, we create a resolution with smaller matrices whose kernels satisfy (3.18). It follows that if the theorem holds for the smaller resolution, then it automatically holds for the original resolution.

Now the theorem is easy to prove. By repeatedly applying the above process whenever we find a nonzero matrix entry of degree zero in some ψ_ℓ, we can reduce to a minimal resolution. But minimal resolutions are isomorphic by Theorem (3.13), and hence, by Exercise 5, the minimal resolution we get has length $\le n$. Then Proposition (1.12) shows that $\ker(\varphi_{n-1})$ is free for the minimal resolution, which, as observed above, implies that $\ker(\varphi_{n-1})$ is free for the original resolution as well.

The final assertion of the theorem, that

$$0 \to \ker(\varphi_{n-1}) \to F_{n-1} \to \cdots \to F_0 \to M \to 0$$

is a free resolution, now follows immediately from Proposition (1.12). □

The simplification process used in the proof of Theorem (3.15) can be used to show that, in a suitable sense, every graded resolution of M is the direct sum of a minimal resolution and a trivial resolution. This gives a structure theorem which describes *all* graded resolutions of a given finitely generated module over $k[x_1, \dots, x_n]$. Details can be found in Theorem 20.2 of [Eis].

Exercise 6. Show that the simplification process from the proof of Theorem (3.15) transforms the homogenization of (1.11) into the homogenization of (1.10) (see Exercise 4).

There is also a version of the theorem just proved which applies to partial resolutions.

(3.19) Corollary. *If*

$$F_{n-1} \stackrel{\varphi_{n-1}}{\to} F_{n-2} \to \cdots \to F_0 \to M \to 0$$

is a partial graded resolution over $k[x_1, \dots, x_n]$*, then* $\ker(\varphi_{n-1})$ *is free, and*

$$0 \to \ker(\varphi_{n-1}) \to F_{n-1} \to \cdots \to F_0 \to M \to 0$$

is a graded resolution of M*.*

PROOF. Since any partial resolution can be extended to a resolution, this follows immediately from Theorem (3.15). □

One way to think about Corollary (3.19) is that over $k[x_1, \ldots, x_n]$, the process of taking repeated syzygies leads to a free syzygy module after at most $n-1$ steps. This is essentially how Hilbert stated the Syzygy Theorem in his classic paper [Hil], and sometimes Theorem (3.15) or Corollary (3.19) are called the Syzygy Theorem. Modern treatments, however, focus on the *existence* of a resolution of length $\leq n$, since Hilbert's version follows from existence (our Theorem (3.8)) together with the properties of minimal resolutions.

As an application of these results, let's study the syzygies of a homogeneous ideal in two variables.

(3.20) Proposition. *Suppose that $f_1, \ldots, f_s \in k[x, y]$ are homogeneous polynomials. Then the syzygy module* $\operatorname{Syz}(f_1, \ldots, f_s)$ *is a twisted free module over $k[x, y]$.*

PROOF. Let $I = \langle f_1, \ldots, f_s \rangle \subset k[x, y]$. Then we get an exact sequence

$$0 \to I \to R \to R/I \to 0$$

by Proposition (1.2). Also, the definition of the syzygy module gives an exact sequence

$$0 \to \operatorname{Syz}(f_1, \ldots, f_s) \to R(-d_1) \oplus \cdots \oplus R(-d_s) \to I \to 0$$

where $d_i = \deg f_i$. Splicing these two sequences together as in Exercise 7 of §1, we get the exact sequence

$$0 \to \operatorname{Syz}(f_1, \ldots, f_s) \to R(-d_1) \oplus \cdots \oplus R(-d_s) \xrightarrow{\varphi_1} R \to R/I \to 0.$$

Since $n = 2$, Corollary (3.19) implies that $\ker(\varphi_1) = \operatorname{Syz}(f_1, \ldots, f_s)$ is free, and the proposition is proved. □

In §4, we will use the Hilbert polynomial to describe the degrees of the generators of $\operatorname{Syz}(f_1, \ldots, f_s)$ in the special case when all of the f_i have the same degree.

ADDITIONAL EXERCISES FOR §3

Exercise 7. Assume that $f_1, \ldots, f_s \in k[x, y]$ are homogeneous and not all zero. We know that $\operatorname{Syz}(f_1, \ldots, f_s)$ is free by Proposition (3.20), so that if we ignore gradings, $\operatorname{Syz}(f_1, \ldots, f_s) \cong R^m$ for some m. This gives an exact sequence

$$0 \to R^m \to R^s \to I \to 0.$$

Prove that $m = s - 1$ and conclude that we are in the situation of the Hilbert-Burch Theorem from §2. Hint: As in Exercise 11 of §2, let $K = k(x_1, \ldots, x_n)$ be the field of rational functions coming from $R = k[x_1, \ldots, x_n]$. Explain why the above sequence gives a sequence

$$0 \to K^m \to K^s \to K \to 0$$

and show that this new sequence is also exact. The result will then follow from the dimension theorem of linear algebra (see Exercise 8 of §1). The ideas used in Exercise 11 of §2 may be useful.

Exercise 8. Prove Proposition (3.3). Hint: Show a $\Rightarrow$ c $\Rightarrow$ b $\Rightarrow$ a.

Exercise 9. Prove Proposition (3.4).

Exercise 10. Complete the proof of Proposition (3.10).

Exercise 11. Suppose that M is a module over $k[x_1, \ldots, x_n]$ generated by $f_1, \ldots, f_m$. As in the proof of Theorem (3.13), let $\langle x_1, \ldots, x_n \rangle M$ be the submodule generated by $x_i f_j$ for all i, j. Also assume that $\psi : M \to M$ is a graded homomorphism of degree zero such that $v - \psi(v) \in \langle x_1, \ldots, x_n \rangle M$ for all $v \in M$. Then prove that ψ is an isomorphism. Hint: By part b of Exercise 3, it suffices to show that $\psi : M_t \to M_t$ is onto. Prove this by induction on t, using part a of Exercise 3 to start the induction.

Exercise 12. Suppose that we have a diagram of R-modules and homomorphisms

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \alpha \downarrow & & \downarrow \beta \\ C & \xrightarrow{\psi} & D \end{array}$$

which commutes in the sense of Definition (3.11). If in addition φ, ψ are onto and α, β are isomorphisms, then prove that α restricted to $\ker(\varphi)$ induces an isomorphism $\bar{\alpha} : \ker(\varphi) \to \ker(\psi)$.

Exercise 13. This exercise is concerned with the proof of Theorem (3.15). We will use the same notation as in that proof, including the sequence of mappings

$$\cdots \to F_{\ell+1} \stackrel{\psi_{\ell+1}}{\to} G_\ell \stackrel{\psi_\ell}{\to} G_{\ell-1} \stackrel{\psi_{\ell-1}}{\to} F_{\ell-2} \to \cdots.$$

a. Prove that $\varphi_\ell(\sum_{i=1}^m a_i e_i) = 0$ if and only if $\psi_\ell(\sum_{i=2}^m a_i e_i) = 0$ and $a_1 c_1 + \sum_{i=2}^m a_i d_i = 0$.
b. Use part a to prove that the above sequence is exact at G_ℓ.
c. Prove that the above sequence is exact at $F_{\ell+1}$. Hint: Do you see why it suffices to show that $\ker(\varphi_{\ell+1}) = \ker(\psi_{\ell+1})$?

d. Prove the second line of (3.18), i.e., that $\ker(\varphi_\ell) \cong \ker(\psi_\ell)$. Hint: Use part a.
e. Prove the third line of (3.18), i.e., that $\ker(\varphi_{\ell+1}) = \ker(\psi_{\ell+1})$. Hint: You did this in part c!

Exercise 14. In the proof of Theorem (3.15), we constructed a certain homomorphism $\psi : G_\ell \to G_{\ell-1}$. Suppose that A_ℓ is the matrix of $\varphi_\ell : F_\ell \to F_{\ell-1}$ with respect to the bases $e_1, \dots, e_m$ of F_ℓ and $u_1, \dots, u_t$ of $F_{\ell-1}$. Write A_ℓ in the form

$$A_\ell = \begin{pmatrix} A_{00} & A_{01} \\ A_{10} & A_{11} \end{pmatrix}$$

where $A_{00} = c_1$ and $A_{01} = (c_2, \dots, c_t)$ as in (3.16), and $A_{10} = (d_2, \dots, d_m)^T$, where the d_i are from the definition of ψ_ℓ. If we let B_ℓ be the matrix of ψ_ℓ with respect to the bases $e_2, \dots, e_m$ of G_ℓ and $u_2, \dots, u_t$ of $G_{\ell-1}$, then prove that

$$B_\ell = A_{00} - A_{01}A_{00}^{-1}A_{10}.$$

What's remarkable is that this formula is identical to equation (6.5) in Chapter 3. As happens often in mathematics, the same idea can appear in very different contexts.

Exercise 15. In $k[x_0, \dots, x_n]$, $n \geq 2$, consider the homogeneous ideal I_n defined by the determinants of the $\binom{n}{2}$ 2×2 submatrices of the $2 \times n$ matrix

$$M = \begin{pmatrix} x_0 & x_1 & \cdots & x_{n-1} \\ x_1 & x_2 & \cdots & x_n \end{pmatrix}.$$

For instance, $I_2 = \langle x_0x_2 - x_1^2 \rangle$ is the ideal of a conic section in $\mathbb{P}^2$. We have already seen I_3 in different notation (where?).

a. Show that I_n is the ideal of the *rational normal curve* of degree n in $\mathbb{P}^n$—the image of the mapping given in homogeneous coordinates by

$$\begin{aligned} \varphi : \mathbb{P}^1 &\to \mathbb{P}^n \\ (s, t) &\mapsto (s^n, s^{n-1}t, \dots, st^{n-1}, t^n). \end{aligned}$$

b. Do explicit calculations to find the graded resolutions of the ideals I_4, I_5.
c. Show that the first syzygy module of the generators for I_n is generated by the three-term syzygies obtained by appending a copy of the first (resp. second) row of M to M, to make a $3 \times n$ matrix M' (resp. M''), then expanding the determinants of all 3×3 submatrices of M' (resp. M'') along the new row.
d. Conjecture the general form of a graded resolution of I_n. (Proving this conjecture requires advanced techniques like the *Eagon-Northcott complex*. This and other interesting topics are discussed in Appendix A2.6 of [Eis].)

§4 Hilbert Polynomials and Geometric Applications

In this section, we will study Hilbert functions and Hilbert polynomials. These are computed using the graded resolutions introduced in §3 and contain some interesting geometric information. We will then give applications to the ideal of three points in $\mathbb{P}^2$, parametric equations in the plane, and invariants of finite group actions.

Hilbert Functions and Hilbert Polynomials

We begin by defining the Hilbert function of a graded module. Because we will be dealing with projective space $\mathbb{P}^n$, it is convenient to work over the polynomial ring $R = k[x_0, \ldots, x_n]$ in $n+1$ variables.

If M is a finitely generated graded R-module, recall from Exercise 3 of §3 that for each t, the degree t homogeneous part M_t is a finite dimensional vector space over k. This leads naturally to the definition of the Hilbert function.

(4.1) Definition. If M is a finitely generated graded module over $R = k[x_0, \ldots, x_n]$, then the *Hilbert function* $H_M(t)$ is defined by

$$H_M(t) = \dim_k M_t,$$

where as usual, $\dim_k$ means dimension as a vector space over k.

The most basic example of a graded module is $R = k[x_0, \ldots, x_n]$ itself. Since R_t is the vector space of homogeneous polynomials of degree t in $n+1$ variables, Exercise 19 of Chapter 3, §4 implies that for $t \geq 0$, we have

$$H_R(t) = \dim_k R_t = \binom{t+n}{n},$$

If we adopt the convention that $\binom{a}{b} = 0$ if $a < b$, then the above formula holds for *all* t. Similarly, the reader should check that the Hilbert function of the twisted module $R(d)$ is given by

$$H_{R(d)}(t) = \binom{t+d+n}{n}, \quad t \in \mathbb{Z}. \tag{4.2}$$

An important observation is that for $t \geq 0$ and n fixed, the binomial coefficient $\binom{t+n}{n}$ is a polynomial of degree n in t. This is because

$$\binom{t+n}{n} = \frac{(t+n)!}{t!n!} = \frac{(t+n)(t+n-1)\cdots(t+1)}{n!}. \tag{4.3}$$

It follows that $H_R(t)$ is given by a polynomial for t sufficiently large ($t \geq 0$ in this case). This will be important below when we define the Hilbert polynomial.

Here are some exercises which give some simple properties of Hilbert functions.

Exercise 1. If M is a finitely generated graded R-module and $M(d)$ is the twist defined in Proposition (3.4), then show that

$$H_{M(d)}(t) = H_M(t+d)$$

for all t. Note how this generalizes (4.2).

Exercise 2. Suppose that M, N and P are finitely generated graded R-modules.

a. The direct sum $M \oplus N$ was discussed in Exercise 1 of §3. Prove that $H_{M\oplus N} = H_M + H_N$.
b. More generally, if we have an exact sequence

$$0 \to M \xrightarrow{\alpha} P \xrightarrow{\beta} N \to 0$$

where α and β are graded homomorphisms of degree zero, then show that $H_P = H_M + H_N$.
c. Explain how part b generalizes part a. Hint: What exact sequence do we get from $M \oplus N$?

It follows from these exercises that we can compute the Hilbert function of any twisted free module. However, for more complicated modules, computing the Hilbert function can be rather nontrivial. There are several ways to study this problem. For example, if $I \subset R = k[x_0, \ldots, x_n]$ is a homogeneous ideal, then the quotient ring R/I is a graded R-module, and in Chapter 9, §3 of [CLO], it is shown than if $\langle \text{LT}(I) \rangle$ is the ideal of initial terms for a monomial order on R, then the Hilbert functions $H_{R/I}$ and $H_{R/\langle \text{LT}(I)\rangle}$ are equal. Using the techniques of Chapter 9, §2 of [CLO], it is relatively easy to compute the Hilbert function of a monomial ideal. Thus, once we compute a Gröbner basis of I, we can find the Hilbert function of R/I. (Note: The Hilbert function $H_{R/I}$ is denoted HF_I in [CLO].)

A second way to compute Hilbert functions is by means of graded resolutions. Here is the basic result.

(4.4) Theorem. *Let $R = k[x_0, \ldots, x_n]$ and let M be a graded R-module. Then, for any graded resolution of M*

$$0 \to F_k \to F_{k-1} \to \cdots \to F_0 \to M \to 0,$$

we have

$$H_M(t) = \dim_k M_t = \sum_{j=0}^{k} (-1)^j \dim_k (F_j)_t = \sum_{j=0}^{k} (-1)^j H_{F_j}(t).$$

PROOF. In a graded resolution, all the homomorphisms are homogeneous of degree zero, hence for each t, restricting all the homomorphisms to the degree t homogeneous parts of the graded modules, we also have an exact sequence of finite dimensional k-vector spaces

$$0 \to (F_k)_t \to (F_{k-1})_t \to \cdots \to (F_0)_t \to M_t \to 0.$$

The alternating sum of the dimensions in such an exact sequence is 0, by Exercise 8 of §1. Hence

$$\dim_k M_t = \sum_{j=0}^{k} (-1)^j \dim_k (F_j)_t,$$

and the theorem follows by the definition of Hilbert function. □

Since we know the Hilbert function of any twisted free module (by (4.2) and Exercise 2), it follows that the Hilbert function of a graded module M can be calculated easily from a graded resolution. For example, let's compute the Hilbert function of the homogeneous ideal I of the twisted cubic in $\mathbb{P}^3$, namely

$$I = \langle xz - y^2, xw - yz, yw - z^2 \rangle \subset R = k[x, y, z, w]. \tag{4.5}$$

In Exercise 2 of §2 of this chapter, we found that I has a graded resolution of the form

$$0 \to R(-3)^2 \to R(-2)^3 \to I \to 0.$$

As in the proof of Theorem (4.4), this resolution implies

$$\dim_k I_t = \dim_k R(-2)_t^3 - \dim_k R(-3)_t^2$$

for all t. Applying Exercise 2 and (4.2), this can be rewritten as

$$\begin{aligned} H_I(t) &= 3\binom{t-2+3}{3} - 2\binom{t-3+3}{3} \\ &= 3\binom{t+1}{3} - 2\binom{t}{3}. \end{aligned}$$

Using the exact sequence $0 \to I \to R \to R/I \to 0$, Exercise 2 implies that

$$H_{R/I}(t) = H_R(t) - H_I(t) = \binom{t+3}{3} - 3\binom{t+1}{3} + 2\binom{t}{3}$$

for all t. For $t = 0, 1, 2$, one (or both) of the binomial coefficients from H_I is zero. However, computing $H_{R/I}(t)$ separately for $t \leq 2$ and doing some

algebra, one can show that

$$H_{R/I}(t) = 3t + 1 \tag{4.6}$$

for all $t \geq 0$.

In this example, the Hilbert function is a polynomial once t is sufficiently large ($t \geq 0$ in this case). This is a special case of the following general result.

(4.7) Proposition. *If M is a finitely generated R-module, then there is a unique polynomial HP_M such that*

$$H_M(t) = HP_M(t)$$

for all t sufficiently large.

PROOF. The key point is that for a twisted free module of the form

$$F = R(-d_1) \oplus \cdots \oplus R(-d_m),$$

Exercise 2 and (4.2) imply that

$$H_F(t) = \sum_{i=1}^{m} \binom{t - d_i + n}{n}.$$

Furthermore, (4.3) shows that this is a polynomial in t provided $t \geq \max(d_1, \ldots, d_m)$.

Now suppose that M is a finitely generated R-module. We can find a finite graded resolution

$$0 \to F_\ell \to \cdots \to F_0 \to M \to 0,$$

and Theorem (4.4) tells us that

$$H_M(t) = \sum_{j=0}^{\ell} (-1)^j H_{F_j}(t).$$

The above computation implies that $H_{F_j}(t)$ is a polynomial in t for t sufficiently large, so that the same is true for $H_M(t)$. □

The polynomial HP_M given in Proposition (4.7) is called the *Hilbert polynomial* of M. For example, if I is the ideal given by (4.5), then (4.6) implies that

$$HP_{R/I}(t) = 3t + 1 \tag{4.8}$$

in this case.

The Hilbert polynomial contains some interesting geometric information. For example, a homogeneous ideal $I \subset k[x_0, \ldots, x_n]$ determines the projective variety $V = \mathbf{V}(I) \subset \mathbb{P}^n$, and the Hilbert polynomial tells us the following facts about V:

- The degree of the Hilbert polynomial $HP_{R/I}$ is the *dimension* of the variety V. For example, in Chapter 9 of [CLO], this is the *definition* of the dimension of a projective variety.
- If the Hilbert polynomial $HP_{R/I}$ has degree $d = \dim V$, then one can show that its leading term is $(D/d!)\,t^d$ for some positive integer D. The integer D is defined to be the *degree* of the variety V. One can also prove that D equals the number of points where V meets a generic $(n-d)$-dimensional linear subspace of $\mathbb{P}^n$.

For example, the Hilbert polynomial $HP_{R/I}(t) = 3t+1$ from (4.8) shows that the twisted cubic has dimension 1 and degree 3. In the exercises at the end of the section, you will compute additional examples of Hilbert functions and Hilbert polynomials.

The Ideal of Three Points

Given a homogeneous ideal $I \subset k[x_0, \dots, x_n]$, we get the projective variety $V = \mathbf{V}(I)$. We've seen that a graded resolution enables us to compute the Hilbert polynomial, which in turn determines geometric invariants of V such as the dimension and degree. However, the actual terms appearing in a graded resolution of the ideal I encode additional geometric information about the variety V. We will illustrate this by considering the form of the resolution of the ideal of a collection of points in $\mathbb{P}^2$. For example, consider varieties consisting of three distinct points, namely $V = \{p_1, p_2, p_3\} \subset \mathbb{P}^2$. There are two cases here, depending on whether the p_i are collinear or not.

We begin with a specific example.

Exercise 3. Suppose that $V = \{p_1, p_2, p_3\} = \{(0,0,1), (1,0,1), (0,1,1)\}$.
a. Show that $I = \mathbf{I}(V)$ is the ideal $\langle x^2 - xz, xy, y^2 - yz\rangle \subset R = k[x,y,z]$.
b. Show that we have a graded resolution

$$0 \to R(-3)^2 \to R(-2)^3 \to I \to 0$$

and explain how this relates to (1.10).
c. Compute that the Hilbert function of R/I is

$$\begin{aligned} H_{R/I}(t) &= \binom{t+2}{2} - 3\binom{t}{2} + 2\binom{t-1}{2} \\ &= \begin{cases} 1 & \text{if } t = 0, \\ 3 & \text{if } t \geq 1. \end{cases} \end{aligned}$$

The Hilbert polynomial in Exercise 3 is the constant polynomial 3, so the dimension is 0 and the degree is 3, as expected. There is also some nice intuition lying behind the graded resolution

$$0 \to R(-3)^2 \to R(-2)^3 \to I \to 0 \tag{4.9}$$

found in part b of the exercise. First, note that $I_0 = \{0\}$ since 0 is the only constant vanishing on the points, and $I_1 = \{0\}$ since the points of $V = \{(0,0,1),(1,0,1),(0,1,1)\}$ are noncollinear. On the other hand, there are quadratics which vanish on V. One way to see this is to let ℓ_{ij} be the equation of the line vanishing on points p_i and p_j. Then $f_1 = \ell_{12}\ell_{13}$, $f_2 = \ell_{12}\ell_{23}$, $f_3 = \ell_{13}\ell_{23}$ are three quadratics vanishing precisely on V. Hence it makes sense that I is generated by three quadratics, which is what the $R(-2)^3$ in (4.9) says. Also, notice that f_1, f_2, f_3 have obvious syzygies of degree 1, for example, $\ell_{23}f_1 - \ell_{13}f_2 = 0$. It is less obvious that two of these syzygies are free generators of the syzygy module, but this is what the $R(-3)^2$ in (4.9) means.

From a more sophisticated point of view, the resolution (4.9) is fairly obvious. This is because of the converse of the Hilbert-Burch Theorem discussed at the end of §2, which applies here since $V \subset \mathbb{P}^2$ is a finite set of points and hence is Cohen-Macaulay of dimension $2 - 2 = 0$.

The example presented in Exercise 3 is more general than one might suspect. This is because for three noncollinear points p_1, p_2, p_3, there is a linear change of coordinates on $\mathbb{P}^2$ taking p_1, p_2, p_3 to $(0,0,1),(1,0,1),(0,1,1)$. Using this, we see that if I is the ideal of *any* set of three noncollinear points, then I has a free resolution of the form (4.9), so that the Hilbert function of I is given by part c of Exercise 3.

The next two exercises will study what happens when the three points *are* collinear.

Exercise 4. Suppose that $V = \{(0,1,0),(0,0,1),(0,\lambda,1)\}$, where $\lambda \neq 0$. These points lie on the line $x = 0$, so that V is a collinear triple of points.
a. Show that $I = \mathbf{I}(V)$ has a graded resolution of the form

$$0 \to R(-4) \to R(-3) \oplus R(-1) \to I \to 0.$$

Hint: Show that $I = \langle x, yz(y - \lambda z)\rangle$.
b. Show that the Hilbert function of R/I is

$$H_{R/I}(t) = \begin{cases} 1 & \text{if } t = 0, \\ 2 & \text{if } t = 1, \\ 3 & \text{if } t \geq 2. \end{cases}$$

Exercise 5. Suppose now that $V = \{p_1, p_2, p_3\}$ is *any* triple of collinear points in $\mathbb{P}^2$. Show that $I = \mathbf{I}(V)$ has a graded resolution of the form

$$0 \to R(-4) \to R(-3) \oplus R(-1) \to I \to 0, \tag{4.10}$$

and conclude that the Hilbert function of R/I is as in part b of Exercise 4. Hint: Use a linear change of coordinates in $\mathbb{P}^2$.

The intuition behind (4.10) is that in the collinear case, V is the intersection of a line and a cubic, and the only syzygy between these is the obvious

one. In geometric terms, we say that V is a *complete intersection* in this case since its dimension ($= 0$) is the dimension of the ambient space ($= 2$) minus the number of defining equations ($= 2$). Note that a noncollinear triple isn't a complete intersection since there are three defining equations.

This sequence of exercises shows that for triples of points in $\mathbb{P}^2$, their corresponding ideals I all give the same Hilbert polynomial $HP_{R/I} = 3$. But depending on whether the points are collinear or not, we get different resolutions (4.10) and (4.9) and different Hilbert functions, as in part c of Exercise 3 and part b of Exercise 4. This is quite typical of what happens.

Here is a similar but more challenging example.

Exercise 6. Now consider varieties $V = \{p_1, p_2, p_3, p_4\}$ in $\mathbb{P}^2$, and write $I = \mathbf{I}(V) \subset R = k[x, y, z]$ as above.

a. First assume the points of V are in general position in the sense that no three are collinear. Show that I_2 is 2-dimensional over k, and that I is generated by any two linearly independent elements of I_2. Deduce that a graded resolution of I has the form

$$0 \to R(-4) \to R(-2)^2 \to I \to 0,$$

and use this to compute $H_{R/I}(t)$ for all t. Do you see how the $R(-2)^2$ is consistent with Bézout's Theorem?

b. Now assume that three of the points of V lie on a line $L \subset \mathbb{P}^2$ but the fourth does not. Show that every element of I_2 is reducible, containing as a factor a linear polynomial vanishing on L. Show that I_2 does not generate I in this case, and deduce that a graded resolution of I has the form

$$0 \to R(-3) \oplus R(-4) \to R(-2)^2 \oplus R(-3) \to I \to 0.$$

Use this to compute $H_{R/I}(t)$ for all t.

c. Finally, consider the case where all four of the points are collinear. Show that in this case, the graded resolution has the form

$$0 \to R(-5) \to R(-1) \oplus R(-4) \to I \to 0,$$

and compute the Hilbert function of R/I for all t.

d. In which cases is V a complete intersection?

Understanding the geometric significance of the shape of the graded resolution of $I = \mathbf{I}(V)$ in more involved examples is an area of active research in contemporary algebraic geometry. A conjecture of Mark Green concerning the graded resolutions of the ideals of canonical curves has stimulated many of the developments here. See [Schre2] and [EH] for some earlier work on Green's conjecture. Recent articles of Montserrat Teixidor ([Tei]) and Claire Voisin ([Voi]) have proved Green's conjecture for a large class of curves. [EH] contains articles on other topics concerning resolutions. Sec-

tion 15.12 of [Eis] has some interesting projects dealing with resolutions, and some of the exercises in Section 15.11 are also relevant.

Parametric Plane Curves

Here, we will begin with a curve in k^2 parametrized by rational functions

$$x = \frac{a(t)}{c(t)}, \ y = \frac{b(t)}{c(t)}, \tag{4.11}$$

where $a, b, c \in k[t]$ are polynomials such that $c \neq 0$ and $\mathrm{GCD}(a, b, c) = 1$. We also set $n = \max(\deg a, \deg b, \deg c)$. Parametrizations of this form play an important role in computer-aided geometric design, and a question of particular interest is the *implicitization problem*, which asks how the equation $f(x, y) = 0$ of the underlying curve is obtained from the parametrization (4.11). An introduction to implicitization can be found in Chapter 3 of [CLO].

A basic object in this theory is the ideal

$$I = \langle c(t)x - a(t), c(t)y - b(t) \rangle \subset k[x, y, t]. \tag{4.12}$$

This ideal has the following interpretation. Let $W \subset k$ be the roots of $c(t)$, i.e., the solutions of $c(t) = 0$. Then we can regard (4.11) as the function $F : k - W \to k^2$ defined by

$$F(t) = \left(\frac{a(t)}{c(t)}, \frac{b(t)}{c(t)} \right).$$

In Exercise 14 at the end of the section, you will show that the graph of F, regarded as a subset of k^3, is precisely the variety $\mathbf{V}(I)$. From here, one can prove that the intersection $I_1 = I \cap k[x, y]$ is an ideal in $k[x, y]$ such that $\mathbf{V}(I_1) \subset k^2$ is the smallest variety containing the image of the parametrization (4.11) (see Exercise 14). In the terminology of Chapter 2, $I_1 = I \cap k[x, y]$ is an elimination ideal, which we can compute using a Gröbner basis with respect to a suitable monomial order.

It follows that the ideal I contains a lot of information about the curve parametrized by (4.11). Recently, it was discovered (see [SSQK] and [SC]) that I provides other parametrizations of the curve, different from (4.11). To see how this works, let $I(1)$ denote the subset of I consisting of all elements of I of total degee at most 1 in x and y. Thus

$$I(1) = \{f \in I : f = A(t)x + B(t)y + C(t)\}. \tag{4.13}$$

An element in $A(t)x + B(t)y + C(t) \in I(1)$ is called a *moving line* since for t fixed, the equation $A(t)x + B(t)y + C(t) = 0$ describes a line in the plane, and as t moves, so does the line.

Exercise 7. Given a moving line $A(t)x + B(t)y + C(t) \in I(1)$, suppose that $t \in k$ satisfies $c(t) \neq 0$. Then show that the point given by (4.11) lies on the line $A(t)x + B(t)y + C(t) = 0$. Hint: Use $I(1) \subset I$.

Now suppose that we have moving lines $f, g \in I(1)$. Then, for a fixed t, we get a pair of lines, which typically intersect in a point. By Exercise 7, each of these lines contains $(a(t)/c(t), b(t)/c(t))$, so this must be the point of intersection. Hence, as we vary t, the intersection of the moving lines will trace out our curve.

Notice that our original parametrization (4.11) is given by moving lines, since we have the vertical line $x = a(t)/c(t)$ and the horizontal line $y = b(t)/c(t)$. However, by allowing more general moving lines, one can get polynomials of smaller degree in t. The following exercise gives an example of how this can happen.

Exercise 8. Consider the parametrization

$$x = \frac{2t^2 + 4t + 5}{t^2 + 2t + 3}, \qquad y = \frac{3t^2 + t + 4}{t^2 + 2t + 3}.$$

a. Prove that $p = (5t + 5)x - y - (10t + 7)$ and $q = (5t - 5)x - (t + 2)y + (-7t + 11)$ are moving lines, i.e., $p, q \in I$, where I is as in (4.12).
b. Prove that p and q generate I, i.e., $I = \langle p, q \rangle$.

In Exercise 8, the original parametrization had maximum degree 2 in t, while the moving lines p and q have maximum degree 1. This is typical of what happens, for we will show below that in general, if n is the maximum degree of a, b, c, then there are moving lines $p, q \in I$ such that p has maximum degree $\mu \leq \lfloor n/2 \rfloor$ in t and q has maximum degree $n - \mu$. Furthermore, p and q are actually a basis of the ideal I. In the terminology of [CSC], this is the *moving line basis* or *μ-basis* of the ideal.

Our goal here is to prove this result—the existence of a μ-basis—and to explain what this has to do with graded resolutions and Hilbert functions. We begin by studying the subset $I(1) \subset I$ defined in (4.13). It is closed under addition, and more importantly, $I(1)$ is closed under multiplication by elements of $k[t]$ (be sure you understand why). Hence $I(1)$ has a natural structure as a $k[t]$-module. In fact, $I(1)$ is a syzygy module, which we will now show.

(4.14) Lemma. *Let $a, b, c \in k[t]$ satisfy $c \neq 0$ and $\mathrm{GCD}(a, b, c) = 1$, and set $I = \langle cx - a, cy - b \rangle$. Then, for $A, B, C \in k[t]$,*

$$A(t)x + B(t)y + C(t) \in I \iff A(t)a(t) + B(t)b(t) + C(t)c(t) = 0.$$

Thus the map $A(t)x + B(t)y + C(t) \mapsto (A, B, C)$ defines an isomorphism of $k[t]$-modules $I(1) \cong \mathrm{Syz}\,(a, b, c)$.

PROOF. To prove $\Rightarrow$, consider the ring homomorphism $k[x,y,t] \to k(t)$ which sends x, y, t to $\frac{a(t)}{c(t)}, \frac{b(t)}{c(t)}, t$. Since the generators of I map to zero, so does $A(t)x + B(t)y + C(t) \in I$. Thus $A(t)\frac{a(t)}{c(t)} + B(t)\frac{b(t)}{c(t)} + C(t) = 0$ in $k(t)$, and multiplying by $c(t)$ gives the desired equation.

For the other implication, let $S = k[t]$ and consider the sequence

$$S^3 \xrightarrow{\alpha} S^3 \xrightarrow{\beta} S \tag{4.15}$$

where $\alpha(h_1,h_2,h_3) = (ch_1 + bh_3, ch_2 - ah_3, -ah_1 - bh_2)$ and $\beta(A,B,C) = Aa + Bb + Cc$. One easily checks that $\beta \circ \alpha = 0$, so that $\operatorname{im}(\alpha) \subset \ker(\beta)$. It is less obvious that (4.15) is exact at the middle term, i.e., $\operatorname{im}(\alpha) = \ker(\beta)$. This will be proved in Exercise 15 below. The sequence (4.15) is the *Koszul complex* determined by a, b, c (see Exercise 10 of §2 for another example of a Koszul complex). A Koszul complex is not always exact, but Exercise 15 will show that (4.15) is exact in our case because $\operatorname{GCD}(a,b,c) = 1$.

Now suppose that $Aa + Bb + Cc = 0$. We need to show that $Ax + By + C \in I$. This is now easy, since our assumption on A, B, C implies $(A,B,C) \in \ker(\beta)$. By the exactness of (4.15), $(A,B,C) \in \operatorname{im}(\alpha)$, which means we can find $h_1, h_2, h_3 \in k[t]$ such that

$$A = ch_1 + bh_3,\ B = ch_2 - ah_3,\ C = -ah_1 - bh_2.$$

Hence

$$\begin{aligned} Ax + By + C &= (ch_1 + bh_3)x + (ch_2 - ah_3)y - ah_1 - bh_2 \\ &= (h_1 + yh_3)(cx - a) + (h_2 - xh_3)(cy - b) \in I, \end{aligned}$$

as desired. The final assertion of the lemma now follows immediately. □

(4.16) Definition. Given a parametrization (4.11), we get the ideal $I = \langle cx - a, cy - b\rangle$ and the syzygy module $I(1)$ from (4.13). Then we define μ to the minimal degree in t of a nonzero element in $I(1)$.

The following theorem shows the existence of a μ-basis of the ideal I.

(4.17) Theorem. *Given (4.11) where $c \neq 0$ and $\operatorname{GCD}(a,b,c) = 1$, set $n = \max(\deg a, \deg b, \deg c)$ and $I = \langle cx - a, cy - b\rangle$ as usual. If μ is as in Definition (4.16), then*

$$\mu \leq \lfloor n/2 \rfloor,$$

and we can find $p, q \in I$ such that p has degree μ in t, q has degree $n - \mu$ in t, and $I = \langle p, q\rangle$.

PROOF. We will study the syzygy module $\operatorname{Syz}(a,b,c)$ using the methods of §3. For this purpose, we need to homogenize a, b, c. Let t, u be homogeneous variables and consider the ring $R = k[t,u]$. Then $\tilde{a}(t,u)$ will denote the

degree n homogenization of $a(t)$, i.e.,

$$\tilde{a}(t,u) = u^n\, a(\tfrac{t}{u}) \in R$$

In this way, we get degree n homogeneous polynomials $\tilde{a}, \tilde{b}, \tilde{c} \in R$, and the reader should check that $\mathrm{GCD}(a,b,c) = 1$ and $n = \max(\deg a, \deg b, \deg c)$ imply that $\tilde{a}, \tilde{b}, \tilde{c}$ have no common zeros in $\mathbb{P}^1$. In other words, the only solution of $\tilde{a} = \tilde{b} = \tilde{c} = 0$ is $t = u = 0$.

Now let $J = \langle \tilde{a}, \tilde{b}, \tilde{c} \rangle \subset R = k[t,u]$. We first compute the Hilbert polynomial HP_J of J. The key point is that since $\tilde{a} = \tilde{b} = \tilde{c} = 0$ have only one solution, no matter what the field is, the Finiteness Theorem from §2 of Chapter 2 implies that the quotient ring $R/J = k[t,u]/J$ is a finite dimensional vector space over k. But J is a homogeneous ideal, which means that R/J is a graded ring. In order for S/J to have finite dimension, we must have $\dim_k (R/J)_s = 0$ for all s sufficiently large (we use s instead of t since t is now one of our variables). It follows that $HP_{R/J}$ is the zero polynomial. Then the exact sequence

$$0 \to J \to R \to R/J \to 0$$

and Exercise 2 imply that

$$HP_J(s) = HP_R(s) = \binom{s+1}{1} = s+1 \tag{4.18}$$

since $R = k[t,u]$. For future reference, note also that by (4.2),

$$HP_{R(-d)}(s) = \binom{s-d+1}{1} = s-d+1.$$

Now consider the exact sequence

$$0 \to \mathrm{Syz}\,(\tilde{a}, \tilde{b}, \tilde{c}) \to R(-n)^3 \xrightarrow{\alpha} J \to 0,$$

where $\alpha(A,B,C) = A\tilde{a} + B\tilde{b} + C\tilde{c}$. By Proposition (3.20), the syzygy module $\mathrm{Syz}\,(\tilde{a}, \tilde{b}, \tilde{c})$ is free, which means that we get a graded resolution

$$0 \to R(-d_1) \oplus \cdots \oplus R(-d_m) \xrightarrow{\beta} R(-n)^3 \xrightarrow{\alpha} J \to 0 \tag{4.19}$$

for some $d_1, \ldots, d_m$. By Exercise 2, the Hilbert polynomial of the middle term is the sum of the other two Hilbert polynomials. Since we know HP_J from (4.18), we obtain

$$\begin{aligned} 3(s-n+1) &= (s-d_1+1) + \cdots + (s-d_m+1) + (s+1) \\ &= (m+1)s + m + 1 - d_1 - \cdots - d_m. \end{aligned}$$

It follows that $m = 2$ and $3n = d_1 + d_2$. Thus (4.19) becomes

$$0 \to R(-d_1) \oplus R(-d_2) \xrightarrow{\beta} R(-n)^3 \xrightarrow{\alpha} J \to 0. \tag{4.20}$$

The matrix L representing β is a 3×2 matrix

$$L = \begin{pmatrix} p_1 & q_1 \\ p_2 & q_2 \\ p_3 & q_3 \end{pmatrix}, \tag{4.21}$$

and since β has degree zero, the first column of L consists of homogeneous polynomials of degree $\mu_1 = d_1 - n$ and the second column has degree $\mu_2 = d_2 - n$. Then $\mu_1 + \mu_2 = n$ follows from $3n = d_1 + d_2$.

We may assume that $\mu_1 \le \mu_2$. Since the first column (p_1, p_2, p_3) of (4.21) satisfies $p_1\tilde{a} + p_2\tilde{b} + p_3\tilde{c} = 0$, setting $u = 1$ gives

$$p_1(t,1)a(t) + p_2(t,1)b(t) + p_3(t,1)c(t) = 0.$$

Thus $p = p_1(t,1)x + p_2(t,1)y + p_3(t,1) \in I(1)$ by Lemma (4.14). Similarly, the second column of (4.21) gives $q = q_1(t,1)x + q_2(t,1)y + q_3(t,1) \in I(1)$. We will show that p and q satisfy the conditions of the theorem.

First observe that the columns of L generate $\operatorname{Syz}(\tilde{a}, \tilde{b}, \tilde{c})$ by exactness. In Exercise 16, you will show this implies that p and q generate $I(1)$. Since $cx - a$ and $cy - b$ are in $I(1)$, we obtain $I = \langle cx - a, cy - b\rangle \subset \langle p, q\rangle$. The other inclusion is immediate from $p, q \in I(1) \subset I$, and $I = \langle p, q\rangle$ follows.

The next step is to prove $\mu_1 = \mu$. We begin by showing that p has degree μ_1 in t. This follows because $p_1(t,u), p_2(t,u), p_3(t,u)$ are homogeneous of degree μ_1. If the degree of all three were to drop when we set $u = 1$, then each p_i would be divisible by u. However, since p_1, p_2, p_3 give a syzygy on $\tilde{a}, \tilde{b}, \tilde{c}$, so would $p_1/u, p_2/u, p_3/u$. Hence we would have a syzygy of degree $< \mu_1$. But the columns of L generate the syzygy module, so this is impossible since $\mu_1 \le \mu_2$. Hence p has degree μ_1 in t, and then $\mu \le \mu_1$ follows from the definition of μ. However, if $\mu < \mu_1$, then we would have $Ax + By + C \in I(1)$ of degree $< \mu_1$. This gives a syzygy of a, b, c, and homogenizing, we would get a syzygy of degree $< \mu_1$ among $\tilde{a}, \tilde{b}, \tilde{c}$. As we saw earlier in the paragraph, this is impossible.

We conclude that p has degree μ in t, and then $\mu_1 + \mu_2 = n$ implies that q has degree $\mu_2 = n - \mu$ in t. Finally, $\mu \le \lfloor n/2 \rfloor$ follows from $\mu = \mu_1 \le \mu_2$, and the proof of the theorem is complete. □

As already mentioned, the basis p, q constructed in Theorem (4.17) is called a *μ-basis* of I. One property of the μ-basis is that it can be used to find the implicit equation of the parametrization (4.11). Here is an example of how this works.

Exercise 9. The parametrization studied in Exercise 8 gives the ideal

$$I = \left\langle (t^2 + 2t + 3)x - (2t^2 + 4t + 5), (t^2 + 2t + 3)y - (3t^2 + t + 4)\right\rangle.$$

a. Use Gröbner basis methods to find the intersection $I \cap k[x, y]$. This gives the implicit equation of the curve.
b. Show that the resultant of the generators of I with respect to t gives the implicit equation.

c. Verify that the polynomials $p = (5t + 5)x - y - (10t + 7)$ and $q = (5t - 5)x - (t + 2)y + (-7t + 11)$ are a μ-basis for I. Thus $\mu = 1$, which is the biggest possible value of μ (since $n = 2$).
d. Show that the resultant of p and q also gives the implicit equation.

Parts b and d of Exercise 9 express the implicit equation as a resultant. However, if we use the Sylvester determinant, then part b uses a 4×4 determinant, while part d uses a 2×2 determinant. So the μ-basis gives a smaller expression for the resultant. In general, one can show (see [CSC]) that for the μ-basis, the resultant can be expressed as an $(n - \mu) \times (n - \mu)$ determinant. Unfortunately, it can also happen that this method gives a power of the actual implicit equation (see Section 4 of [CSC]).

Earlier in this section, we considered the ideal of three points in $\mathbb{P}^2$. We found that although all such ideals have the same Hilbert polynomial, we can distinguish the collinear and noncollinear cases using the Hilbert function. The situation is similar when dealing with μ-bases. Here, we have the ideal $J = \langle \tilde{a}, \tilde{b}, \tilde{c} \rangle \subset R = k[t, u]$ from the proof of Theorem (4.17). In the following exercise you will compute the Hilbert function of R/J.

Exercise 10. Let $J = \langle \tilde{a}, \tilde{b}, \tilde{c} \rangle$ be as in the proof of Theorem (4.17). In the course of the proof, we showed that the Hilbert polynomial of R/J is the zero polynomial. But what about the Hilbert function?
a. Prove that the Hilbert function $H_{R/J}$ is given by

$$H_{R/J}(s) = \begin{cases} s + 1 & \text{if } 0 \le s \le n - 1 \\ 3n - 2s - 2 & \text{if } n \le s \le n + \mu - 1 \\ 2n - s - \mu - 1 & \text{if } n + \mu \le s \le 2n - \mu - 1 \\ 0 & \text{if } 2n - \mu \le s. \end{cases}$$

b. Show that the largest value of s such that $H_{R/J}(s) \neq 0$ is $s = 2n - \mu - 2$, and conclude that knowing μ is equivalent to knowing the Hilbert function of the quotient ring R/J.
c. Compute the dimension of R/J as a vector space over k.

In the case of the ideal of three points, note that the noncollinear case is generic. This is true in the naive sense that one expects three randomly chosen points to be noncollinear, and this can be made more precise using the notion of generic given in Definition (5.6) of Chapter 3. Similarly, for μ-bases, there is a generic case. One can show (see [CSC]) that among parametrizations (4.11) with $n = \max(\deg a, \deg b, \deg c)$, the "generic" parametrization has $\mu = \lfloor n/2 \rfloor$, the biggest possible value. More generally, one can compute the dimension of the set of all parametrizations with a given μ. This dimension decreases as μ decreases, so that the smaller the μ, the more special the parametrization.

We should also mention that the Hilbert-Burch Theorem discussed in §2 has the following nice application to μ-bases.

(4.22) Proposition. *The μ-basis coming from the columns of (4.21) can be chosen such that*

$$\tilde{a} = p_2q_3 - p_3q_2,\ \tilde{b} = -(p_1q_3 - p_3q_1),\ \tilde{c} = p_1q_2 - p_1q_2.$$

Dehomogenizing, this means that a, b, c can be computed from the coefficients of the μ-basis

$$\begin{aligned} p &= p_1(t,1)x + p_2(t,1)y + p_3(t,1) \\ q &= q_1(t,1)x + q_2(t,1)y + q_3(t,1). \end{aligned} \tag{4.23}$$

Proof. To see why this is true, first note that the exact sequence (4.20) has the form required by Proposition (2.6) of §2. Then the proposition implies that if $\tilde{f}_1, \tilde{f}_2, \tilde{f}_3$ are the 2×2 minors of (4.21) (this is the notation of Proposition (2.6)), then there is a polynomial $g \in k[t,u]$ such that $\tilde{a} = g\tilde{f}_1, \tilde{b} = g\tilde{f}_2, \tilde{c} = g\tilde{f}_3$. However, since $\tilde{a}, \tilde{b}, \tilde{c}$ have no common roots, g must be a nonzero constant. If we replace p_i with gp_i, we get a μ-basis with the desired properties. □

Exercise 11. Verify that the μ-basis studied in Exercises 8 and 9 satisfies Proposition (4.22) after changing p by a suitable constant.

It is also possible to generalize Theorem (4.17) by considering curves in m-dimensional space k^m given parametrically by

$$x_1 = \frac{a_1(t)}{c(t)},\ \ldots\ , x_m = \frac{a_m(t)}{c(t)}, \tag{4.24}$$

where $c \neq 0$ and $\mathrm{GCD}(a_1, \ldots, a_m) = 1$. In this situation, the syzygy module $\mathrm{Syz}\,(a_1, \ldots, a_m, c)$ and its homogenization play an important role, and the analog of the μ-basis (4.13) consists of m polynomials

$$p_j = p_{1j}(t,1)x_1 + \cdots + p_{mj}(t,1)x_m + p_{m+1j}(t,1),\ 1 \leq j \leq m, \tag{4.25}$$

which form a basis for the ideal $I = \langle cx_1 - a_1, \ldots, cx_m - a_m \rangle$. If we fix t in (4.25), then the equation $p_j = 0$ is a hyperplane in k^m, so that as t varies, we get a *moving hyperplane*. One can prove that the common intersection of the m hyperplanes $p_j = 0$ sweeps out the given curve and that if p_j has degree μ_j in t, then $\mu_1 + \cdots + \mu_m = n$. Thus we have an m-dimensional version of Theorem (4.17). See Exercise 17 for the proof.

We can use the Hilbert-Burch Theorem to generalize Proposition (4.22) to the more general situation of (4.24). The result is that up to sign, the polynomials $a_1, \ldots, a_m, c$ are the $m \times m$ minors of the matrix $(p_{ij}(t,1))$ coming from (4.25). Note that since p_j has degree μ_j in t, the $m \times m$ minors $(p_{ij}(t,1))$ have degree at most $\mu_1 + \cdots + \mu_m = n$ in t. So the degrees work out nicely. The details will be covered in Exercise 17 below.

The proof given of Theorem (4.17) makes nice use of the results of §3, especially Proposition (3.20), and the generalization (4.24) to curves in k^m shows just how powerful these methods are. The heart of what we did

in Theorem (4.17) was to understand the structure of the syzygy module $\operatorname{Syz}(\tilde{a}, \tilde{b}, \tilde{c})$ as a free module, and for the m-dimensional case, one needs to understand $\operatorname{Syz}(\tilde{a}_1, \dots, \tilde{a}_m, \tilde{c})$ for $\tilde{a}_1, \dots, \tilde{a}_m, \tilde{c} \in k[t, u]$. Actually, in the special case of Theorem (4.17), one can give a proof using elementary methods which don't require the Hilbert Syzygy Theorem. One such proof can be found in [CSC], and another was given by Franz Meyer, all the way back in 1887 [Mey].

Meyer's article is interesting, for it starts with a problem completely different from plane curves, but just as happened to us, he ended up with a syzygy problem. He also considered the more general syzygy module $\operatorname{Syz}(\tilde{a}_1, \dots, \tilde{a}_m, \tilde{c})$, and he conjectured that this was a free module with generators of degrees $\mu_1, \dots, \mu_m$ satisfying $\mu_1 + \cdots + \mu_m = n$. But in spite of many examples in support of this conjecture, his attempts at a proof "ran into difficulties which I have at this time not been able to overcome" [Mey, p. 73]. However, three years later, Hilbert proved everything in his groundbreaking paper [Hil] on syzygies. For us, it is interesting to note that after proving his Syzygy Theorem, Hilbert's first application is to prove Meyer's conjecture. He does this by computing a Hilbert polynomial (which he calls the *characteristic function*) in a manner remarkably similar to what we did in Theorem (4.17)—see [Hil, p. 516]. Hilbert then concludes with the Hilbert-Burch Theorem in the special case of $k[t, u]$.

One can also consider surfaces in k^3 parametrized by rational functions

$$x = \frac{a(s,t)}{d(s,t)}, \quad y = \frac{b(s,t)}{d(s,t)}, \quad z = \frac{c(s,t)}{d(s,t)},$$

where $a, b, c, d \in k[s, t]$ are polynomials such that $d \neq 0$ and

$$\operatorname{GCD}(a, b, c, d) = 1.$$

As above, the goal is to find the implicit equation of the surface. Surface implicitization is an important problem in geometric modeling.

This case is more complicated because of the possible presence of *base points*, which are points (s, t) at which a, b, c, d all vanish simultaneously. As in the curve case, it is best to work homogeneously, though the commutative algebra is also more complicated—for example, the syzygy module is rarely free. However, there are still many situations where the implicit equation can be computed using syzygies. See [Cox2] and [Cox3] for introductions to this area of research and references to the literature.

Rings of Invariants

The final topic we will explore is the invariant theory of finite groups. In contrast to the previous discussions, our presentation will not be self-contained. Instead, we will assume that the reader is familiar with the

material presented in Chapter 7 of [CLO]. Our goal is to explain how graded resolutions can be used when working with polynomials invariant under a finite matrix group.

For simplicity, we will work over the polynomial ring $S = \mathbb{C}[x_1, \ldots, x_m]$. Suppose that $G \subset \mathrm{GL}(m, \mathbb{C})$ is a finite group. If we regard $g \in G$ as giving a change of coordinates on $\mathbb{C}^m$, then substituting this coordinate change into $f \in S = \mathbb{C}[x_1, \ldots, x_m]$ gives another polynomial $g \cdot f \in S$. Then define

$$S^G = \{f \in \mathbb{C}[x_1, \ldots, x_m] : g \cdot f = f \text{ for all } \ g \in G\}.$$

Intuitively, S^G consists of all polynomials $f \in S$ which are unchanged (i.e., invariant) under all of the coordinate changes coming from elements $g \in G$. The set S^G has the following structure:

- (Graded Subring) The set of invariants $S^G \subset S$ is a subring of S, meaning that S is closed under addition and multiplication by elements of S^G. Also, if $f \in S^G$, then every homogeneous component of f also lies in S^G.

(See Propositions 9 and 10 of Chapter 7, §2 of [CLO].) We say that S^G is a *graded subring* of S. Hence the degree t homogeneous part S^G_t consists of all invariants which are homogeneous polynomials of degree t. Note that S^G is *not* an ideal of S.

In this situation, we define the *Molien series* of S^G to be the formal power series

$$F_G(u) = \sum_{t=0}^{\infty} \dim_{\mathbb{C}}(S^G_t)\, u^t. \tag{4.26}$$

Molien series are important objects in the invariant theory of finite groups. We will see that they have a nice relation to Hilbert functions and graded resolutions.

A basic result proved in Chapter 7, §3 of [CLO] is:

- (Finite Generation of Invariants) For a finite group $G \subset \mathrm{GL}(m, \mathbb{C})$, there are $f_1, \ldots, f_s \in S^G$ such that every $f \in S^G$ is a polynomial in $f_1, \ldots, f_s$. Furthermore, we can assume that $f_1, \ldots, f_s$ are homogeneous.

This enables us to regard S^G as a module over a polynomial ring as follows. Let $f_1, \ldots, f_s$ be homogeneous generators of the ring of invariants S^G, and set $d_i = \deg f_i$. Then introduce variables $y_1, \ldots, y_s$ and consider the ring $R = \mathbb{C}[y_1, \ldots, y_s]$. The ring R is useful because the map sending y_i to f_i defines a ring homomorphism

$$\varphi : R = \mathbb{C}[y_1, \ldots, y_s] \longrightarrow S^G$$

which is onto since every invariant is a polynomial in $f_1, \ldots, f_s$. An important observation is that φ becomes a graded homomorphism of degree zero

provided we regard the variable y_i as having degree $d_i = \deg f_i$. Previously, the variables in a polynomial ring always had degree 1, but here we will see that having $\deg y_i = d_i$ is useful.

The kernel $I = \ker \varphi \subset R$ consists of all polynomial relations among the f_i. Since φ is onto, we get an isomorphism $R/I \cong S^G$. Regarding S^G as an R-module via $y_i \cdot f = f_i f$ for $f \in S^G$, $R/I \cong S^G$ is an isomorphism of R-modules. Elements of I are called *syzygies* among the invariants $f_1, \dots, f_s$. (Historically, syzygies were first defined in invariant theory, and only later was this term used in module theory, where the meaning is slightly different).

For going any further, let's pause for an example. Consider the group $G = \{e, g, g^2, g^3\} \subset \mathrm{GL}(2, \mathbb{C})$, where

$$g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{4.27}$$

The group G acts on $f \in S = \mathbb{C}[x_1, x_2]$ via $g \cdot f(x_1, x_2) = f(-x_2, x_1)$. Then, as shown in Example 4 of Chapter 7, §3 of [CLO], the ring of invariants S^G is generated by the three polynomials

$$f_1 = x_1^2 + x_2^2, \quad f_2 = x_1^2 x_2^2, \quad f_3 = x_1^3 x_2 - x_1 x_2^3. \tag{4.28}$$

This gives $\varphi : R = \mathbb{C}[y_1, y_2, y_3] \to S^G$ where $\varphi(y_i) = f_i$. Note that y_1 has degree 2 and y_2, y_3 both have degree 4. One can also show that the kernel of φ is $I = \langle y_3^2 - y_1^2 y_2 + 4y_2^2 \rangle$. This means that all syzygies are generated by the single relation $f_3^2 - f_1^2 f_2 + 4f_2^2 = 0$ among the invariants (4.28).

Returning to our general discussion, the R-module structure on S^G shows that the Molien series (4.26) is built from the Hilbert function of the R-module S^G. This is immediate because

$$\dim_{\mathbb{C}}(S_t^G) = H_{S^G}(t).$$

In Exercises 24 and 25, we will see more generally that any finitely generated R-module has a *Hilbert series*

$$\sum_{t=-\infty}^{\infty} H_M(t)\, u^t.$$

The basic idea is that one can compute any Hilbert series using a graded resolution of M. In the case when all of the variables have degree 1, this is explained in Exercise 24.

However, we are in a situation where the variables have degree $\deg y_i = d_i$ (sometimes called the *weight* of y_i). Formula (4.2) no longer applies, so instead we use the key fact (to be proved in Exercise 25) that the Hilbert series of the weighted polynomial ring $R = \mathbb{C}[y_1, \dots, y_s]$ is

$$\sum_{t=0}^{\infty} H_R(t)\, u^t = \sum_{t=0}^{\infty} \dim_{\mathbb{C}}(R_t)\, u^t = \frac{1}{(1-u^{d_1}) \cdots (1-u^{d_s})}. \tag{4.29}$$

Furthermore, if we define the twisted free module $R(-d)$ in the usual way, then one easily obtains

$$\sum_{t=0}^{\infty} H_{R(-d)}(t)\, u^t = \frac{u^d}{(1-u^{d_1})\cdots(1-u^{d_s})} \tag{4.30}$$

(see Exercise 25 for the details).

Let us see how this works in the example begun earlier.

Exercise 12. Consider the group $G \subset \mathrm{GL}(2,\mathbb{C})$ given in (4.27) with invariants (4.28) and syzygy $f_3^2 + f_1^2 f_2 + 4f_2^2 = 0$.

a. Show that a minimal free resolution of S^G as a graded R-module is given by

$$0 \longrightarrow R(-8) \xrightarrow{\psi} R \xrightarrow{\varphi} R^G \longrightarrow 0$$

where ψ is the map represented by the 1×1 matrix $(y_3^2 + y_1^2 y_2 + 4y_2^2)$.

b. Use part a together with (4.29) and (4.30) to show that the Molien series of G is given by

$$\begin{aligned} F_G(u) &= \frac{1-u^8}{(1-u^2)(1-u^4)^2} = \frac{1+u^4}{(1-u^2)(1-u^4)} \\ &= 1 + u^2 + 3u^4 + 3u^6 + 5u^8 + 5u^{10} + \cdots \end{aligned}$$

c. The coefficient 1 of u^2 tells us that we have a unique (up to constant) invariant of degree 2, namely f_1. Furthermore, the coefficient 3 of u^4 tells us that besides the obvious degree 4 invariant f_1^2, we must have two others, namely f_2 and f_3. Give similar explanations for the coefficients of u^6 and u^8 and in particular explain how the coefficient of u^8 proves that we must have a nontrivial syzygy of degree 8.

In general, one can show that if the invariant ring of a finite group G is generated by homogeneous invariants $f_1, \ldots, f_s$ of degree $d_1, \ldots, d_s$, then the Molien series of G has the form

$$F_G(u) = \frac{P(u)}{(1-u^{d_1})\cdots(1-u^{d_s})}$$

for some polynomial $P(u)$. See Exercise 25 for the proof. As explained in [Sta2], $P(u)$ has the following intuitive meaning. If there are no nontrivial syzygies between the f_i, then the Molien series would have been

$$\frac{1}{(1-u^{d_1})\cdots(1-u^{d_s})}.$$

Had R^G been generated by homogeneous elements $f_1, \ldots, f_s$ of degrees $d_1, \ldots, d_s$, with homogeneous syzygies $S_1, \ldots, S_w$ of degrees $\beta_1, \ldots, \beta_w$ and no second syzygies, then the Molien series would be corrected to

$$\frac{1-\sum_j u^{\beta_j}}{\prod_i (1-u^{d_i})}.$$

In general, by the Syzygy Theorem, we get

$$F_G(u) = (1 - \underbrace{\textstyle\sum_j u^{\beta_j} + \sum_k u^{\gamma_k} - \cdots}_{\text{at most } s \text{ sums}})/\textstyle\prod_i (1-u^{d_i}).$$

One important result not mentioned so far is *Molien's Theorem*, which states that the Molien series (4.26) of a finite group $G \subset \mathrm{GL}(m,\mathbb{C})$ is given by the formula

$$F_G(u) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I - ug)}$$

where $|G|$ is the number of elements in G and $I \in \mathrm{GL}(m,\mathbb{C})$ is the identity matrix. This theorem is why (4.26) is called a Molien series. The importance of Molien's theorem is that it allows one to compute the Molien series in advance. As shown by part c of Exercise 12, the Molien series can predict the existence of certain invariants and syzygies, which is useful from a computational point of view (see Section 2.2 of [Stu1]). A proof of Molien's Theorem will be given in Exercise 28.

A second crucial aspect we've omitted is that the ring of invariants S^G is Cohen-Macaulay. This has some far-reaching consequences for the invariant theory. For example, being Cohen-Macaulay predicts that there are algebraically independent invariants $\theta_1, \ldots, \theta_r$ such that the invariant ring S^G is a *free* module over the polynomial ring $\mathbb{C}[\theta_1, \ldots, \theta_r]$. For example, in the invariant ring $S^G = \mathbb{C}[f_1, f_2, f_3]$ considered in Exercise 12, one can show that as a module over $\mathbb{C}[f_1, f_2]$,

$$S^G = \mathbb{C}[f_1, f_2] \oplus f_3\mathbb{C}[f_1, f_2].$$

(Do you see how the syzygy $f_3^2 - f_1 f_2^2 + 4f_2^2 = 0$ enables us to get rid of terms involving f_3^2, f_3^3, etc?) This has some strong implications for the Molien series, as explained in [Sta2] or [Stu1].

Hence, to really understand the invariant theory of finite groups, one needs to combine the free resolutions discussed here with a variety of other tools, some of which are more sophisticated (such as Cohen-Macaulay rings). Fortunately, some excellent expositions are available in the literature, and we especially recommend [Sta2] and [Stu1]. Additional references are mentioned at the end of Chapter 7, §3 of [CLO].

This brings us to the end of our discussion of resolutions. The examples presented in this section—ideals of three points, μ-bases, and Molien series—are merely the beginning of a wonderful collection of topics related to the geometry of free resolutions. When combined with the elegance of the algebra involved, it becomes clear why the study of free resolutions is one of the richer areas of contemporary algebraic geometry.

To learn more about free resolutions, we suggest the references [Eis], [Schre2] and [EH] mentioned earlier in the section. The reader may also wish to consult [BH, Chapter 4] for a careful study of Hilbert functions.

Additional Exercises for §4

Exercise 13. The Hilbert polynomial has the property that $H_M(t) = HP_M(t)$ for all t sufficiently large. In this exercise, you will derive an explicit bound on how large t has to be in terms of a graded resolution of M.

a. Equation (4.3) shows that the binomial coefficient $\binom{t+n}{n}$ is given by a polynomial of degree n in t. Show that this identity holds for all $t \geq -n$ and also explain why it fails to hold when $t = -n-1$.

b. For a twisted free module $M = R(-d_1) \oplus \cdots \oplus R(-d_m)$, show that $H_M(t) = HP_M(t)$ holds for $t \geq \max_i(d_i - n)$.

c. Now suppose we have a graded resolution $\cdots \to F_0 \to M$ where $F_j = \oplus_i R(-d_{ij})$. Then show that $H_M(t) = HP_M(t)$ holds for all $t \geq \max_{ij}(d_{ij} - n)$.

d. For the ideal $I \subset k[x, y, z, w]$ from (4.5), we found the graded resolution

$$0 \to R(-3)^2 \to R(-2)^3 \to R \to R/I \to 0.$$

Use this and part c to show that $H_{R/I}(t) = HP_{R/I}(t)$ for all $t \geq 0$. How does this relate to (4.6)?

Exercise 14. Given a parametrization as in (4.11), we get the ideal $I = \langle c(t)x - a(t), c(t)y - b(t)\rangle \subset k[x, y, t]$. We will assume $\mathrm{GCD}(a, b, c) = 1$.

a. Show that $\mathbf{V}(I) \subset k^3$ is the graph of the function $F : k - W \to k^2$ defined by $F(t) = (a(t)/c(t), b(t)/c(t))$, where $W = \{t \in k : c(t) = 0\}$.

b. If $I_1 = I \cap k[x, y]$, prove that $\mathbf{V}(I_1) \subset k^2$ is the smallest variety containing the parametrization (4.11). Hint: This follows by adapting the proof of Theorem 1 of Chapter 3, §3 of [CLO].

Exercise 15. This exercise concerns the Koszul complex used in the proof of Proposition (4.14).

a. Assuming $\mathrm{GCD}(a, b, c) = 1$ in $S = k[t]$, prove that the sequence (4.15) is exact at its middle term. Hint: Our hypothesis implies that there are polynomials $p, q, r \in k[t]$ such that $pa + qb + rc = 1$. Then if $(A, B, C) \in \ker(\beta)$, note that

$$\begin{aligned} A &= paA + qbA + rcA \\ &= p(-bB - cC) + qbA + rcA \\ &= c(-pC + rA) + b(-pB + qA). \end{aligned}$$

b. Using Exercise 10 of §2 as a model, show how to extend (4.15) to the full Koszul complex

$$0 \to S \to S^3 \xrightarrow{\alpha} S^3 \xrightarrow{\beta} S \to 0$$

of a, b, c. Also, when $\text{GCD}(a, b, c) = 1$, prove that the entire sequence is exact.

c. More generally, show that $a_1, \ldots, a_m \in k[t]$ give a Koszul complex and prove that it is exact when $\text{GCD}(a_1, \ldots, a_m) = 1$. (This is a challenging exercise.)

Exercise 16. In the proof of Theorem (4.17), we noted that the columns of the matrix (4.20) generate the syzygy module $\text{Syz}\,(\tilde{a}, \tilde{b}, \tilde{c})$. If we define p, q using (4.23), then prove that p, q generate $I(1)$.

Exercise 17. In this exercise, you will study the m-dimensional version of Theorem (4.17). Thus we assume that we have a parametrization (4.24) of a curve in k^m such that $c \neq 0$ and $\text{GCD}(a_1, \ldots, a_m) = 1$. Also let

$$I = \langle cx_1 - a_1, \ldots, cx_m - a_m \rangle \subset k[x_1, \ldots, x_m, t]$$

and define

$$I(1) = \{f \in I : f = A_1(t)x_1 + \cdots + A_m(t)x_m + C(t)\}.$$

a. Prove the analog of Lemma (4.14), i.e., show that there is a natural isomorphism $I(1) \cong \text{Syz}\,(a_1, \ldots, a_m, c)$. Hint: You will use part c of Exercise 15.

b. If $n = \max(\deg a_1, \ldots, \deg a_m, c)$ and $\tilde{a}_i, \tilde{c} \in R = k[t, u]$ are the degree n homogenizations of a_i, c, then explain why there is an injective map

$$\beta : R(-d_1) \oplus \cdots \oplus R(-d_s) \to R(-n)^{m+1}$$

whose image is $\text{Syz}\,(\tilde{a}_1, \ldots, \tilde{a}_m, \tilde{c})$.

c. Use Hilbert polynomials to show that $s = m$ and that $d_1 + \cdots + d_m = (m + 1)n$.

d. If L is the matrix representing β, show that the jth column of L consists of homogeneous polynomials of degree $\mu_j = d_j - n$. Also explain why $\mu_1 + \cdots + \mu_s = n$.

e. Finally, by dehomogenizing the entries of the jth column of L, show that we get the polynomial p_j as in (4.25), and prove that $I = \langle p_1, \ldots, p_m \rangle$.

f. Use the Hilbert-Burch Theorem to show that if p_1 is modified by a suitable constant, then up to a constant, $a_1, \ldots, a_m, c$ are the $m \times m$ minors of the matrix $(p_{ij}(t, 1))$ coming from (4.25).

Exercise 18. Compute the Hilbert function and Hilbert polynomial of the ideal of the rational quartic curve in $\mathbb{P}^3$ whose graded resolution is given in (3.6). What does the Hilbert polynomial tell you about the dimension and the degree?

Exercise 19. In $k[x_0, \dots, x_n]$, $n \geq 2$, consider the homogeneous ideal I_n defined by the determinants of the $\binom{n}{2}$ 2×2 submatrices of the $2 \times n$ matrix

$$M = \begin{pmatrix} x_0 & x_1 & \cdots & x_{n-1} \\ x_1 & x_2 & \cdots & x_n \end{pmatrix}.$$

(We studied this ideal in Exercise 15 of §3.) Compute the Hilbert functions and Hilbert polynomials of I_4 and I_5. Also determine the degrees of the curves $\mathbf{V}(I_4)$ and $\mathbf{V}(I_5)$ and verify that they have dimension 1. Hint: In part b of Exercise 15 of §3, you computed graded resolutions of these two ideals.

Exercise 20. In this exercise, we will show how the construction of the rational normal curves from the previous exercise and Exercise 15 of §3 relates to the moving lines considered in this section.

a. Show that for each $(t, u) \in \mathbb{P}^1$, the intersection of the lines $\mathbf{V}(tx_0 + ux_1)$ and $\mathbf{V}(tx_1 + ux_2)$ lies on the conic section $\mathbf{V}(x_0x_2 - x_1^2)$ in $\mathbb{P}^2$. Express the equation of the conic as a 2×2 determinant.

b. Generalizing part a, show that for all $n \geq 2$, if we construct n *moving hyperplanes* $H_i(t, u) = \mathbf{V}(tx_{i-1} + ux_i)$ for $i = 1, \dots, n$, then for each (t, u) in $\mathbb{P}^1$, the intersection $H_1(t, u) \cap \cdots \cap H_n(t, u)$ is a point on the standard rational normal curve in $\mathbb{P}^n$ given as in Exercise 15 of §3, and show how the determinantal equations follow from this observation.

Exercise 21. In $k[x_0, \dots, x_n]$, $n \geq 3$, consider the homogeneous ideal J_n defined by the determinants of the $\binom{n-1}{2}$ 2×2 submatrices of the $2 \times (n-1)$ matrix

$$N = \begin{pmatrix} x_0 & x_2 & \cdots & x_{n-1} \\ x_1 & x_3 & \cdots & x_n \end{pmatrix}.$$

The varieties $\mathbf{V}(J_n)$ are surfaces called *rational normal scrolls* in $\mathbb{P}^n$. For instance, $J_3 = \langle x_0x_3 - x_1x_2 \rangle$ is the ideal of a smooth quadric surface in $\mathbb{P}^3$.

a. Find a graded resolution of J_4 and compute its Hilbert function and Hilbert polynomial. Check that the dimension is 2 and compute the degree of the surface.

b. Do the same for J_5.

Exercise 22. The (degree 2) *Veronese surface* $V \subset \mathbb{P}^5$ is the image of the mapping given in homogeneous coordinates by

$$\begin{aligned} \varphi : \mathbb{P}^2 &\to \mathbb{P}^5 \\ (x_0, x_1, x_2) &\mapsto (x_0^2, x_1^2, x_2^2, x_0x_1, x_0x_2, x_1x_2). \end{aligned}$$

a. Compute the homogeneous ideal $I = \mathbf{I}(V) \subset k[x_0, \dots, x_5]$.

b. Find a graded resolution of I and compute its Hilbert function and Hilbert polynomial. Also check that the dimension is equal to 2 and the degree is equal to 4.

Exercise 23. Let $p_1 = (0,0,1), p_2 = (1,0,1), p_3 = (0,1,1), p_4 = (1,1,1)$ in $\mathbb{P}^2$, and let $I = \mathbf{I}(\{p_1, p_2, p_3, p_4\})$ be the homogeneous ideal of the variety $\{p_1, p_2, p_3, p_4\}$ in $R = k[x_0, x_1, x_2]$.

a. Show that I_3 (the degree 3 graded piece of I) has dimension exactly 6.

b. Let $f_0, \ldots, f_5$ be any vector space basis for I_3, and consider the rational mapping $\varphi : \mathbb{P}^2 - - \to \mathbb{P}^5$ given in homogeneous coordinates by

$$\varphi(x_0, x_1, x_2) = (y_0, \ldots, y_5) = (f_0(x_0, x_1, x_2), \ldots, f_5(x_0, x_1, x_2)).$$

Find the homogeneous ideal J of the image variety of φ.

c. Show that J has a graded resolution as an $S = k[y_0, \ldots, y_5]$-module of the form

$$0 \to S(-5) \to S(-3)^5 \xrightarrow{A} S(-2)^5 \to J \to 0.$$

d. Use the resolution above to compute the Hilbert function of J.

The variety $V = \mathbf{V}(J) = \varphi(\mathbb{P}^2)$ is called a *quintic del Pezzo surface*, and the resolution given in part d has some other interesting properties. For instance, if the ideal basis for J is ordered in the right way and signs are adjusted appropriately, then A is skew-symmetric, and the determinants of the 4×4 submatrices obtained by deleting row i and column i ($i = 1, \ldots, 5$) are the squares of the generators of J. This is a reflection of a remarkable structure on the resolutions of *Gorenstein codimension 3* ideals proved by Buchsbaum and Eisenbud. See [BE].

Exercise 24. One convenient way to "package" the Hilbert function H_M for a graded module M is to consider its *generating function*, the formal power series

$$H(M, u) = \sum_{t=-\infty}^{\infty} H_M(t) u^t.$$

We will call $H(M, u)$ the *Hilbert series* for M.

a. Show that for $M = R = k[x_0, \ldots, x_n]$, we have

$$\begin{aligned} H(R, u) &= \sum_{t=0}^{\infty} \binom{n+t}{n} u^t \\ &= 1/(1-u)^{n+1}, \end{aligned}$$

where the second equality comes from the formal geometric series identity $1/(1-u) = \sum_{t=0}^{\infty} u^t$ and induction on n.

b. Show that if $R = k[x_0, \ldots, x_n]$ and

$$M = R(-d_1) \oplus \cdots \oplus R(-d_m)$$

is one of the twisted graded free modules over R, then

$$H(M,u) = (u^{d_1} + \cdots + u^{d_m})/(1-u)^{n+1}.$$

c. Let I be the ideal of the twisted cubic in $\mathbb{P}^3$ studied in Exercise 2 of §2, and let $R = k[x,y,z,w]$. Find the Hilbert series $H(R/I,u)$.
d. Using part b and Theorem (4.4) deduce that the Hilbert series of any graded $k[x_0,\ldots,x_n]$-module M can be written in the form

$$H(M,u) = P(u)/(1-u)^{n+1}$$

where P is a polynomial in u with coefficients in $\mathbb{Z}$.

Exercise 25. Consider the polynomial ring $R = k[y_1,\ldots,y_s]$, where y_i has weight or degree $\deg y_i = d_i > 0$. Then a monomial $y^{a_1}\cdots y_s^{a_s}$ has (weighted) degree $t = d_1a_1 + \cdots + d_sa_s$. This gives a grading on R such that R_t is the set of k-linear combinations of monomials of degree t.
a. Prove that the Hilbert series of R is given by

$$\sum_{t=0}^{\infty} \dim_k(R_t)\, u^t = \frac{1}{(1-u^{d_1})\cdots(1-u^{d_s})}.$$

Hint: $1/(1-u^{d_i}) = \sum_{a_i=0}^{\infty} u^{d_i a_i}$. When these series are multiplied together for $i = 1,\ldots,s$, do you see how each monomial of weighted degree t contributes to the coefficient of u^t?
b. Explain how part a relates to part a of Exercise 24.
c. If $R(-d)$ is defined by $R(-d)_t = R_{t-d}$, then prove (4.30).
d. Generalize parts b, c and d of Exercise 24 to $R = k[y_1,\ldots,y_s]$.

Exercise 26. Suppose that $a,b,c \in k[t]$ have maximum degree 6. As usual, we will assume $c \neq 0$ and $\mathrm{GCD}(a,b,c) = 1$.
a. If $a = t^6 + t^3 + t^2$, $b = t^6 - t^4 - t^2$ and $c = t^6 + t^5 + t^4 - t - 1$, show that $\mu = 2$ and find a μ-basis.
b. Find an example where $\mu = 3$ and compute a μ-basis for your example. Hint: This is the generic case.

Exercise 27. Compute the Molien series for the following finite matrix groups in $\mathrm{GL}(2,\mathbb{C})$. In each case, the ring of invariants $\mathbb{C}[x_1,x_2]^G$ can be computed by the methods of Chapter 7, §3 of [CLO].
a. The Klein four-group generated by $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.
b. The two-element group generated by $g = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.
c. The four-element group generated by $g = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$.

Exercise 28. Let $G \subset \mathrm{GL}(m,\mathbb{C})$ be a finite group and let $S = \mathbb{C}[x_1,\ldots,x_m]$. The goal of this exercise is to prove Molien's Theorem, which

asserts that

$$\sum_{t=0}^{\infty} \dim_{\mathbb{C}}(S_t^G)u^t = \frac{1}{|G|}\sum_{g\in G}\frac{1}{\det(I-ug)}.$$

a. By Chapter 7, §3 of [CLO], the Reynolds operator $R_G(f)(\mathbf{x}) = \frac{1}{|G|}\sum_{g\in G} f(g\cdot\mathbf{x})$ defines a projection operator $R_G : S_t \to S_t^G$. Use this to prove that

$$\dim_{\mathbb{C}}(S_t^G) = \frac{1}{|G|}\sum_{g\in G}\operatorname{trace}(g_t),$$

where $g_t : S_t \to S_t$ is defined by $f(\mathbf{x}) \mapsto f(g\cdot\mathbf{x})$. Hint: First explain why the trace of a projection operator is the dimension of its image.

b. Fix $g \in G$ and a basis $y_1, \ldots, y_m$ of $S_1 \cong \mathbb{C}^m$ such that g_1 is upper triangular on S_1 with eigenvalues $\lambda_1, \ldots, \lambda_m$. Prove that y^α for $|\alpha| = t$ give a basis of S_t such that g_t is upper triangular on S_t with eigenvalues λ^α. Conclude that $\operatorname{trace}(g_t) = \sum_{|\alpha|=t}\lambda^\alpha$.

c. Explain why

$$\sum_{\alpha}\lambda^\alpha u^{|\alpha|} = \prod_{i=1}^{m}\frac{1}{1-\lambda_i u} = \frac{1}{\det(I-ug)}$$

and use this to complete the proof of Molien's Theorem.