INTERNATIONAL ATOMIC ENERGY AGENCY
UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION
INTERNATIONAL CENTRE FOR THEORETICAL PHYSICS
I.C.T.P., P.O. BOX 586, 34100 TRIESTE, ITALY, CABLE CENTRATOM TRIESTE

SMR.761/10

Workshop on Commutative Algebra
and its Relation to
Combinatorics and Computer Algebra

(16 - 27 May 1994)

Gröbner Bases

from
Commutative Algebra with a view toward
Algebraic Geometry

D. Eisenbud
Brandeis University
Waltham, MA 02254
U.S.A.

These are preliminary lecture notes, intended only for distribution to participants

From Commutative Algebra with A View Toward Algebraic Geometry by David Eisenbud. (Springer-Verlag, Oct. 1994).

Chapter 15: Gröbner Bases

> Man kann dieses Verfahren dazu benützen, den Restkalssenring eines nulldimensionalen Polynomideals wirklich zu berechnen...
>
> (One can use this process to actually compute a zero-dimensional residue class ring of a polynomial ring...)
>
> W. Gröbner [1939]

We will work throughout this chapter with a polynomial ring $S = k[x_1, \ldots ,x_r]$ over a field k. The elements of k will be called scalars. All S-modules mentioned will be assumed finitely generated.

A great deal of modern commutative algebra and algebraic geometry is formulated in an essentially nonconstructive fashion. To take a simple example, Hilbert's basis theorem assures us that there exists a finite basis of the syzygies for any finite set of elements of S, but at first glance it would seem that one must investigate syzygies of all degrees to find one. Nevertheless, one can find generators for such a syzygy module algorithmically (Hilbert's original proof was algorithmic!), and one can effectively perform a very large proportion of the other central operations as well. In fact practical algorithms are known and implemented in various computer algebra packages. In this chapter we will take up a notion that is central to many such algorithms, the notion of a Gröbner basis. Gröbner bases have had interesting theoretical applications as well as computational ones, and there are currently many open problems in the theory.

In brief, a **Gröbner basis** for an ideal I in S is a set of generators for I with an additional property; **Buchberger's Algorithm** yields a simple and effective method for computing Gröbner bases and syzygies. Through the use of Gröbner bases, many questions about ideals in polynomial rings can be reduced to questions about monomial ideals, which are far easier. The kinds of problems that can be attacked with Gröbner bases can be very roughly divided into two groups:

- **Constructive Module Theory**

In this heading we group all the operations carried out on modules over a fixed ring. A few samples:

- **Division with remainder and ideal membership** : Given generators for an ideal I ⊂ S, determine a vector space basis for S/I, and given a polynomial f, compute its image in S/I in terms of this basis. If f ∈ I (that is, if the image is 0) compute an expression for f as a linear combination of the generators of I.
- **Compute syzygies** ; that is, compute the kernel of a map φ: G → F of free S-modules. Equivalently, solve a system of linear equations over S.
- **Compute the intersection of two ideals.**
- **Compute the annihilator of a module.**
- **For ideals I, J ⊂ S, compute the saturation $(I : J^{\infty})$.**
- **Compute the module of homomorphisms between two given modules; more generally, compute Ext and Tor.**
- **Compute the Hilbert Function and Polynomial of a graded module.**

- Elimination Theory

In this heading we group the operations that involve two different rings. The most basic operation in this class is

- **Elimination** : **Compute the intersection J of an ideal I**

$\subset k[x_1, \ldots ,x_r]$ with a subring $R' = k[x_1, \ldots ,x_s]$.

The geometric meaning of elimination is projection: Given an algebraic variety $X \subset \mathbf{A}^r$ defined by the vanishing of the polynomials in I, the projection of X to $\mathbf{A}^s$ is a set whose closure (in the Zariski topology) is defined by J. One of the main uses of elimination is in actually finding solutions for a system of polynomial equations -- that is, finding points of a variety: The idea is to reduce the problem to a problem in fewer variables, and eventually to a problem in one variable, where other techniques (factorization of polynomials) can be used. We will take up the solution of equations by elimination in a later chapter. In this chapter we will explain how to use it to solve problems such as:

- **Compute the equations satisfied by given elements of an affine ring;** geometrically, compute the closure of the image of an affine or projective variety under a morphism.

In particular:

- **Find a presentation of the blowup algebra and associated graded ring of a ring R = S/I, with respect to an ideal $\mathfrak{m}$.**

- **Given a variety $V \subset \mathbf{A}^r$, find equations for its closure in $\mathbf{P}^r$.**

This long chapter is somewhat inhomogeneous. The main results, on which the computational uses of Gröbner Bases are based, are proved in the first part, ending with the treatment of syzygies and the special property of the reverse lexicographic order. In a phrase of Sturmfels', these are the Gröbner Basics. Subsequent sections on flat families and generic initial ideals present more advanced topics. Some of the ways of applying Gröbner Basis techniques in constructive module theory are then described. At the end I have collected some historical remarks. The novice might want to read just the "Basics"and browse a little among the applications to get a flavor of what is possible. For those wishing to go deeper into the use of computers in commutative algebra and algebraic geometry, I have provided some "computer algebra projects, with suggestions for implementation, in addition to more traditional exercises.

Another part of constructive commutative algebra that certainly deserves mention, but that we will not treat here, concerns methods for factoring polynomials. This field is dominated by ideas of E. Berlekamp; a beautiful exposition may be found in the book of D. Knuth [1969, Vol. II, Sect. 4.6].

Monomials and terms

Since the main idea in the use of Gröbner bases is to reduce all questions to questions about monomials, we begin with these.

We write monomials in S using multi-indices: If $a = (a_1, \ldots ,a_r)$ then x^a will denote the monomial

$$x_1^{a_1} \cdot \ldots \cdot x_r^{a_r}.$$

An ideal generated by such monomials will be called a **monomial ideal.** More generally, let F be a finitely generated free module with basis $\{e_i\}$. **A monomial in F** is an element of the form

$$m = x^a e_i$$

for some i; we will say that such an m **involves the basis element e_i.** A **monomial submodule of F** is a submodule generated by elements of this form. Any monomial submodule M of F may be written as

$$M = \oplus I_j e_j \quad \subset \quad \oplus S e_j = F$$

with I_j the monomial ideal generated by those monomials m such that $me_j \in M$.

A **term** in F is a monomial multiplied by a scalar. Since the monomials form a vector space basis for F, every element $f \in F$ is uniquely expressible as a finite sum of nonzero terms involving distinct monomials, which we call the terms of f; the monomials in these terms will be called the monomials of f. Since we have assumed that k is a field, the distinction between terms and monomials will not play much of a role in our theory.

These definitions all depend on the chosen basis $\{e_i\}$ of F. Whenever possible, we will suppress the actual basis $\{e_i\}$ from our notation, and speak simply of F as a **free module with basis** .

If m, n are monomials of S and $u,v \in k$, and $v \neq 0$, then we say that the term ume_i is **divisible** by the term vne_j if $i = j$ and m is divisible by n in S; the **quotient** is then $um/vn \in S$.

A number of operations are far simpler for monomials than for arbitrary polynomials. For example, the **greatest common divisor and least common multiple** of two monomials in S are obtained componentwise: If $b = (b_1, \ldots ,b_r)$ then

$$\mathbf{GCD}(x^a, x^b) = x_1^{\min(a_1,b_1)} x_2^{\min(a_2,b_2)} \ldots x_r^{\min(a_r,b_r)},$$

$$\mathbf{LCM}(x^a, x^b) = x_1^{\max(a_1,b_1)} x_2^{\max(a_2,b_2)} \ldots x_r^{\max(a_r,b_r)}.$$

We extend these operations to terms in any free module with basis F: If $m, n \in F$ are terms involving the same basis element e_i of F, then the GCD of m and n will be taken to be the largest monomial in F by which both m and n can be divided. It is easy to write down the intersection or quotient of monomial submodules in terms of these operations; see Exercise 15.3 and Exercise 15.7.

If $M \subset F$ is a submodule generated by monomials $m_1, \ldots ,m_t$, it is trivial to decide whether a monomial m belongs to M: It does iff it is divisible by at least one of the m_i. More generally, the "membership problem" is easy to solve for a monomial submodule: An arbitrary element $f \in F$ belongs to M iff each of its monomials belongs to M.

Given any set of monomial generators for M, we may remove any that are divisible by others in the set and still have a set of generators for M. In this way we get the unique minimal set of monomials generating M: The set of monomials in M that are minimal elements in the partial order by divisibility on the monomials of F. We will refer to the monomials in this set as **minimal generators of M.**

Hilbert function and polynomial

These simple ideas already suffice to compute the Hilbert function and polynomial of a monomial submodule $M \subset F$, or equivalently of the quotient $P = F/M$, quite efficiently. Because the submodule M is a direct sum of modules of the form $I_j\, e_j$, where the e_j are basis elements of F, we get $P \cong \oplus\, S/I_j$. Since the Hilbert function is additive, it suffices to treat the case $P = S/I$, where I is a monomial ideal.

We make an induction using the following idea: Choosing one of the minimal generators n of I, we write $I = (I',n)$, where I' is a monomial ideal generated by fewer monomials than I, and let d be the degree of n. There is an exact sequence of graded modules and degree 0 maps

$$S(-d) \xrightarrow{\varphi} S/I' \rightarrow S/I \rightarrow 0,$$

where S(-d) is the free module with generator in degree d and φ is the map that sends the generator of S(-d) to the class of n in S/I'. Now the kernel of φ is easy to compute: It is the monomial ideal

$$J := (I' : n) = \{m \in S \mid mn \in I'\},$$

shifted in degree to be a submodule of S(-d). By Fxercise 15.3,

$$J = (m_1/\mathrm{GCD}(m_1,n), \ldots , m_t/\mathrm{GCD}(m_t,n)),$$

so like I', the ideal J has fewer minimal generators than I, and we can suppose by induction that we know the Hilbert function and polynomial of S/I' and S/J.

From the short exact sequence of graded modules

$$0 \to (S/J)(-d) \to S/I' \to S/I \to 0,$$

we get for each integer ν a short exact sequence of vector spaces

$$0 \to (S/J)_{\nu-d} \to (S/I')_\nu \to (S/I)_\nu \to 0.$$

Thus, on the level of Hilbert functions,

$$H_{S/I}(\nu) = H_{S/I'}(\nu) - H_{S/J}(\nu-d),$$

solving our problem.

By choosing n sensibly, we can make the process much faster: If n contains the largest power of some variable x_1 of any of the minimal generators of I, then the minimal generators of the resulting ideal J will not involve x_1 at all, and thus will involve strictly fewer of the variables than do the minimal generators of I.

This process leads to an expression for the Hilbert function or polynomial as an alternating sum. A variant of the method, which leads directly to an expression for the Hilbert function as a sum of binomial coefficients (all terms positive) is presented in Exercise 15.4. The worst case behavior of these methods (with the best known choices for the monomial n) is exponential in the number of variables, and Bayer and Stillman, in [1992] (from which the method above is taken), show that finding the Hilbert function of a monomial ideal is an NP-hard problem in

a suitable sense. Nevertheless, in many cases of interest, the method works quite quickly.

Syzygies of monomial submodules

Syzygies of monomial submodules are also quite simple. The following result not only gives generators for the syzygies of a monomial submodule, but gives precise information on the coefficients necessary to express arbitrary syzygies in terms of the generators.

In the following, we let F be a free module with basis, and let M be a submodule of F generated by monomials $m_1, \ldots, m_t$. Let

$$\varphi\colon \oplus_{j=1}^{t} S\varepsilon_j \to F; \qquad \varphi(\varepsilon_j) = m_j$$

be a homomorphism from a free module whose image is M. For each pair of indices i,j such that m_i and m_j involve the same basis element of F, we define

$$m_{ij} = m_i/\mathrm{GCD}(m_i, m_j),$$

and we define σ_{ij} to be the element of ker φ given by

$$\sigma_{ij} = m_{ji}\, \varepsilon_i - m_{ij}\, \varepsilon_j.$$

Lemma 15.1: With notation as above, ker φ is generated by the σ_{ij}.

Proof: We first observe that as a vector space over k, ker φ is the direct sum, over all monomials $n \in F$, of the vector spaces

$$(\ker \varphi)_n = \{ \Sigma a_\nu n_\nu \varepsilon_\nu \in \ker \varphi \mid m_\nu \text{ divides } n,\ n_\nu = n/m_\nu, \text{ and } a_\nu \in k \}.$$

Indeed, suppose that

$$\sigma = \Sigma p_i \varepsilon_i \in S^t, \qquad p_i \in S$$

is a syzygy, so that $\Sigma p_i m_i = 0$. For any monomial n of F that occurs in one of the $p_j m_j$, and for each i let $p_{i,n}$ be the term of p_i (if any) such that $p_{i,n} m_i$ is a scalar times n. We must have $\Sigma p_{i,n} m_i = 0$, so $\Sigma p_{i,n} \varepsilon_i \in (\ker \varphi)_n$. The representation is clearly unique.

We now do induction on the number of nonzero terms of σ. If $\sigma \neq 0$ then because σ is a syzygy, at least two of the $a_v n_v$ must be nonzero, say the i^{th} and the j^{th}, with $i < j$. It follows that n is divisible both by m_i and m_j, and thus n_i is divisible by

$$\mathrm{LCM}(m_i, m_j)/m_i = m_j/\mathrm{GCD}(m_i, m_j) = m_{ji}.$$

Consequently we may subtract a scalar times $(n_i/m_{ji})\sigma_{ij}$ from σ to get a relation with fewer terms. //

The proof actually gives a stronger result, which we will use in the proof of Theorem 15 8:

Lemma 15 1 bis: With notation as in Lemma 15 1, every element of ker φ is uniquely expressible as a sum of elements $\tau = \Sigma a_v n_v \varepsilon_v \in \ker \varphi$ such that all the $n_v m_v$ are equal to the same monomial $n \in F$. For such an element we may write

$$\tau = \Sigma\, n_{ij}\, \sigma_{ij}\ ,$$

where the sum is over all $i<j$ such that $\mathrm{LCM}(m_i, m_j)$ divides n and where n_{ij} is a scalar times the monomial $n/\mathrm{LCM}(m_i, m_j) = n_i/m_{ji}$.

Proof: The first paragraph of the proof of Lemma 15 1 above proves the first statement. For the second, look again at the last paragraph of the proof of Lemma 15 1. The element σ_{ij} used there meets the conditions of Lemma 15 1 bis, and we never introduce any new term in τ in the course of the induction.//

The syzygies σ_{ij} in Lemma 15 1 are sometimes called **divided Koszul relations** because of their similarity to the relations in the Koszul complex that we shall study in Chapter 17. We have shown that they generate all the syzygies on monomial ideals, but they do not in general form a minimal set of generators (see Exercise 15 6).
In Exercise 17.11 we will see that a very similar construction gives a whole (nonminimal) free resolution of a monomial submodule, which is a kind of "divided Koszul complex".

Monomial orders

If $J \subset S$ is a monomial ideal, then the set B of all monomials not in J forms a vector space basis for S/J that makes computation in S/J quite convenient. If I is an arbitrary ideal of S, we would like to obtain a similarly simple picture of S/I. Since the monomials of S form a vector space basis, their images span S/I, and a maximal linearly independent subset B will be a basis. These exist by Zorn's Lemma, so any S/I has such a **monomial basis** .

If we can choose B to be the complement of the set of monomials in a monomial ideal J, as in the case where I is itself a monomial ideal, we get an extra advantage. Because a monomial ideal can be specified by giving finitely many monomial generators, it is easy to determine whether a given monomial is in B: We must simply test for divisibility by one of the generators of J. We will show in Theorem 15 3 that there is a monomial basis B for any S/I obtained in this way. We begin with some remarks to motivate the construction:

First, if J is a monomial ideal and B is the set of monomials not in J, then it is not hard to see that the elements of B remain linearly independent modulo an ideal I iff

*) J contains at least one monomial from every polynomial in I.

For the set B to be a basis of S/I, the ideal J must (at least!) be minimal with property *).

As a first example, let $I = (m_1+m_2)$ be a principal ideal generated by the sum of two monomials m_i. A monomial ideal contains at least one monomial from each polynomial in I iff it contains one of the monomial ideals (m_i). However, if m_1 divides m_2 and we take $J = (m_1)$, then B will not be a basis, since J is not minimal: m_1 itself is superfluous. Taking $J = (m_2)$ in these circumstances DOES make B a basis, however; we will

prove a much more general statement in a moment, but the reader may wish to pause to think through this special case.

To find a monomial ideal J that contains at least one monomial from each polynomial of I it seems natural to look for a method of choosing one monomial from each polynomial of S. Given such a method, we can apply it to choose a monomial from each polynomial in I, and use the chosen monomials to generate J. To make J minimal , some interesting additional conditions must be met.

Suppose for example that m_1, m_2, m_3 are distinct monomials of the same degree d and that

$$I = (m_1 + m_2, m_2 + m_3) + (\text{all monomials of degree} > d).$$

Suppose that we have chosen m_1 from $m_1 + m_2$ and m_2 from $m_2 + m_3$ to put into J. The ideal I also contains

$$(m_1 + m_2) - (m_2 + m_3) = m_1 - m_3.$$

We must at this point choose m_1 (rather than m_3) to put into J; for if we put m_3 into J, then J would not be minimal. Thus if we write "$m_1 > m_2$" for the relation "m_1 is chosen over m_2", then > must satisfy the axiom for an order relation, $m_1 > m_2 > m_3 \Rightarrow m_1 > m_3$. A more careful analysis shows that the same thing is true even when the m_i have different degrees.

Thus we must totally order the monomials of S, and put into J the greatest monomial in each polynomial of I. Because we wish to take J to be an ideal, there are two further requirements that the order > must satisfy with respect to multiplication:

First, as shown in the first example above, > must refine the partial order defined by divisibility: That is if m_2 is divisible by m_1, we must take $m_2 > m_1$.

Second, > must be preserved by multiplication: Suppose that $I = (m_1 + m_2)$ and that we have chosen $m_1 > m_2$ so that $m_1 \in J$ and m_1 does not divide m_2. Then $nm_1 + nm_2 \in I$, but already, since J is an ideal, $nm_1 \in J$, so choosing $nm_2 > nm_1$, would lead (under many circumstances) to nonmimimal sets J. Thus we must have $nm_1 > nm_2$.

The following definition encapsulates these conditions:

Definition : Let F be a free S-module with basis. A **monomial order** on F is a total order > on the monomials of F such that if m_1, m_2, are monomials of F and $n \neq 1$ is a monomial of S then

$$m_1 > m_2 \quad \text{implies} \quad nm_1 > nm_2 > m_2.$$

Bearing in mind that we are supposing F to be finitely generated, the second inequality has an extremely useful consequence:

Lemma 15 2: Let F be a free S-module with basis. Any monomial order on F is **Artinian** (every subset has a least element).

Proof: If X is a set of monomials of F, then since S is Noetherian the submodule of F generated by X is already generated by a finite subset $Y \subset X$. The least element of Y will be the least element in X because every element of X is a multiple, by a monomial in S, of an element of Y. //

We will extend this notation to terms: If um and vn are terms with $0 \neq u,v \in k$, and m, n monomials with $m > n$ (respectively $m \geq n$) then we say $um > vn$ (respectively $um \geq vn$). Note that this is NOT a partial order on terms, since even if $u \neq v$ we have $um \geq vm$ and $vm \geq um$. It is nonetheless convenient.

If > is a monomial order, then for any $f \in F$ we define the **initial term of f,** written $\mathbf{in}_>(\mathbf{f})$ to be the greatest term of f with respect to the order >, and if M is a submodule of F we define $\mathrm{in}_>(M)$ to be the monomial

submodule generated by the elements $\mathrm{in}_>(f)$ for all $f \in M$. When there is no danger of confusion we will simply write **in** in place of $\mathbf{in}_>$.

Note that if $p \in S$ and $f \in F$ and we write n for the (unique) term of p such that n in(f) is greatest, then

$$\mathrm{in}(pf) = n\ \mathrm{in}(f).$$

For if m is a term of f other than in(f) and n' is a term of p other than n we will have

$$n\ \mathrm{in}(f) > n'\ \mathrm{in}(f) \qquad \text{(by hypothesis)}$$

$$> n'\ m \qquad \text{(because > is a monomial order).}$$

Monomial orders do all that we might have hoped:

Theorem 15 3 (Macaulay) : Let F be a free S-module with basis, and let M be an arbitrary submodule. For any monomial order > on F, the set B of all monomials not in $\mathrm{in}_>(M)$ forms a basis for F/M.

Proof: To show that B is linearly independent, note that if there were a dependence relation

$$p = \Sigma\, u_i\, m_i \in M \quad m_i \in B,\ \ 0 \neq u_i \in k$$

then $\mathrm{in}(p) \in \mathrm{in}(M)$. Since in(p) is one of the m_i, which are supposed to be in B, this is a contradiction.

Now suppose that B does not span F/M. Among the set of elements of F that are not in the span of M and B, we may take f to be one with minimal initial term. If in(f) were in B, we could subtract it, getting a polynomial with a still smaller initial term. Thus we may suppose that $\mathrm{in}(f) \in \mathrm{in}(M)$. Subtracting an element of M with the same initial term as f we arrive again at a contradiction. //

Monomial orders abound. Here are some significant examples with F = S. We write $a = (a_1, .. ,a_r)$ and $b = (b_1, ... ,b_r)$ for multi-indices, and set

$$m = x^a, \quad n = x^b.$$

By renaming the variables, we may always achieve $x_1 > x_2 > ... > x_r$, and we will only describe orders with this property.

Lexicographic order : $m >_{lex} n$ iff $a_i > b_i$ for the **first** index i with $a_i \neq b_i$.

Homogeneous Lexicographic order : $m >_{hlex} n$ iff degree m > degree n or degree m = degree n and $a_i > b_i$ for the **first** index i with $a_i \neq b_i$.

If we are given a sequence of partial orders $>_1, >_2, ...$ then we may define the partial order that is their **lexicographic product** to be the order in which m > n if $m >_i n$ for the first i such that m and n are comparable with respect to the order $>_i$. We sometimes say that the lexicographic product order is the order $>_1$ **refined by** the order $>_2$, refined by .... . The homogeneous lexicographic order above is the lexicographic product of the partial order by degree (m > n if degree m > degree n) refined by the partial orders by the degree in x_1, the degree in x_2, ...

If r = 1 then the requirement that $nm_2 > m_2$ for a monomial n not equal to 1 shows that there is a unique monomial order on S: The order by degree. Similarly, if r = 2, then there is only one monomial order on S that refines the order by degree and satisfies our convention $x_1 > x_2$. To see this, suppose $m = x_1^{a_1}x_2^{a_2}$ and $n = x_1^{b_1}x_2^{b_2}$ have the same degree $a_1+a_2 = b_1+b_2$. If $a_1 > b_1$, so $\varepsilon := a_1-b_1 > 0$ then writing $p = x_1^{b_1}x_2^{a_2}$ for the greatest common divisor we have

$$m = x_1^{\varepsilon}p,$$

$$n = x_2^{\varepsilon}p.$$

But $x_1 > x_2$ implies $x_1^{\varepsilon} > x_2^{\varepsilon}$ (in fact induction gives $x_1^{\varepsilon} > x_1^{\varepsilon-1}x_2 > x_2^{\varepsilon}$), so m > n.

There are in general many other orders. By far the most important is:

Reverse Lexicographic order: $m >_{rlex} n$ iff degree m > degree n or degree m = degree n and $a_i < b_i$ for the **last** index i with $a_i \neq b_i$.

Note the direction of the inequality $a_i < b_i$! The name "reverse lexicographic" comes from the fact that on the monomials of a given degree, this is the reverse of the order obtained by reversing the order of the variables and using homogeneous lexicographic order. Reverse lexicographic order was introduced by Macaulay in [1927]. The difference between the homogeneous lexicographic and reverse lexicographic orders is subtle, but the use of reverse lexicographic order in place of homogeneous lexicographic order in the algorithms described below sometimes improves the efficiency of computation enormously (Bayer-Stillman [1987a and b]). See the section on generic coordinates, below, for a hint of a possible reason.

The first case in which $>_{hlex}$ and $>_{rlex}$ could differ is for quadratic monomials in 3 variables. Here indeed we have

$$x_1x_3 >_{hlex} x_2^2$$

while

$$x_1x_3 <_{rlex} x_2^2.$$

Roughly, we can describe the difference by saying that if m and n have the same degree, then $m >_{hlex} n$ iff m involves **more** from the **beginning** of the list of variables while $m >_{rlex} n$ iff m involves **less** from the **end** of the list of variables. Most of the uses made of these orders depend on the following easily verified properties (which actually characterize them -- see Exercise 15 10). These properties make it clear that the subtlety above is the difference between a subring and an ideal.

Characteristic properties of lex, hlex, and rlex 15 4:

a) If $\mathrm{in}_{lex}(f) \in k[x_s, \ldots, x_r]$ for some s, then $f \in k[x_s, \ldots, x_r]$.

b) $>_{hlex}$ refines the order by total degree; and if f is homogeneous with $\mathrm{in}_{hlex}(f) \in k[x_s, \ldots, x_r]$ for some s, then $f \in k[x_s, \ldots, x_r]$.

c) $>_{rlex}$ refines the order by total degree; and if f is homogeneous with $\mathrm{in}_{rlex}(f) \in (x_s, \ldots, x_r)$ for some s, then $f \in (x_s, \ldots, x_r)$.

Weight orders: We define a **weight function** λ for S to be a linear function $\mathbb{R}^r \to \mathbb{R}$; λ will be called **integral** if it comes from a linear map $\mathbb{Z}^r \to \mathbb{Z}$. Any weight function λ defines a partial order $>_\lambda$, called the **weight order associated to λ**, by the rule $m = x^a >_\lambda n = x^b$ iff $\lambda(a) > \lambda(b)$. We say that λ is **compatible** with a given monomial order $>$ if $m >_\lambda n$ implies $m > n$. Similar things could be done for a free module, but we shall not use this. There are always compatible weight orders: In fact it can be shown (Robbiano [1986]; see Exercise 15 11 Exercise 15 12 and Exercise 15 13) that every monomial order is the lexicographic product of r weight orders, the first of which is necessarily compatible with the given order. For example, defining π_i: $\mathbb{R}^r \to \mathbb{R}$ to be the projection onto the i^{th} coordinate, the lexicographic order is the lexicographic product of the weight orders corresponding to the π_i, while reverse lexicographic order is the lexicographic product of the weight orders corresponding to the total degree function $\sigma = \Sigma\pi_i$ and the functions $-\pi_r, -\pi_{r-1}, \ldots, -\pi_1$ (the last of which may of course be omitted). In fact any monomial order $>$ can be approximated by a single weight order $>_\lambda$ in the sense that $>_\lambda$ can be made to agree with $>$ on any given finite set of pairs of monomials: See Exercise 15 12.

In Proposition 15 16 we will have occasion to use a small extension of the notion of initial term: Given a weight order λ on the polynomial ring S, we define $\mathrm{in}_\lambda(f)$ to be the sum of all those terms of f that are maximal for $>_\lambda$.

One way of getting monomial orders on a free module F with given basis $\{e_i\}$ is to choose a monomial order $>$ on S, choose an order $>$ among the e_i, and use a lexicographic product of the partial orders on the monomials of F induced by $>$ and $>$. In particular, **a reverse lexicographic order on F** is the result of refining the reverse lexicographic order on the monomials of S by an order of the basis e_i in this way.

Now let F be a free S-module with basis and let M be a submodule of F. It turns out to be extremely useful to know the modules $\mathrm{in}_>(M)$ with respect to various orders $>$. "Knowing" such a module means of course having a system of generators for it. It turns out to be practical to ask for a little more information: A system of generators for $\mathrm{in}_>(M)$, and for each one an element of M whose initial form it is. The following central definition encapsulates a convenient description of this information:

Definition: A **Gröbner basis** with respect to an order $>$ on a free module with basis F is a set of elements $g_1, \ldots, g_t \in F$ such that if M is the submodule of F generated by $g_1, \ldots, g_t$ then $\mathrm{in}_>(g_1), \ldots, \mathrm{in}_>(g_t)$ generate $\mathrm{in}_>(M)$; we then say that $g_1, \ldots, g_t$ is a **Gröbner basis for M.**

Examples : **The case of no variables:** Let S be a field and let F be a vector space of dimension s, with basis $\{e_i\}$; we may identify elements of F with columns vectors of length s. The only monomials of F are the e_i; let $>$ be the monomial order in which $e_1 > e_2 > \ldots$.

With this ordering, a set of elements $g_1, \ldots, g_t \in F$ is simply an s×t matrix G over S. We claim that G is a Gröbner basis iff it contains a maximal linearly independent set in "echelon form"; that is if some maximal independent subset of the column vectors g_i have their first nonzero entries in distinct rows, as in Figure 15.1.

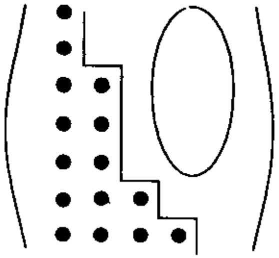


Figure 15.1

The case of one variable: Next consider the case $S = k[x]$, a polynomial ring over k in one variable, and take $F = S$. The only monomial order is the order by degree. A submodule $M \subset F$ is then just an ideal. The monomial ideal in(M) is generated by x^d where d is the smallest degree of any polynomial in M; thus a Gröbner basis of M consists of any set of generators of M containing an element of minimal degree. Note that Lemma 15 5 provides a proof that an ideal is generated by any element of minimal degree.

There is a Gröbner basis for any submodule M of F, with respect to any monomial order: If $g_1, \dots, g_t$ are generators for M that are not a Gröbner basis, then to get a Gröbner basis we simply adjoin elements $g_{t+1}, \dots g_{t'}$ of M until the initial terms $in(g_1), \dots, in(g_{t'})$ generate in(M); this is possible by the Hilbert Basis Theorem.

The following Lemma shows that any set of elements of M whose initial terms generate in(M) actually generate M; thus to check that a set of elements is a Gröbner basis for M, it is enough to check that their initial terms generate in(M):

Lemma 15 5: If $N \subset M \subset F$ are submodules and $in(N) = in(M)$ with respect to a monomial order, then $N = M$.

Proof: If not, then there would be an element $f \in M$ whose initial term is smallest among initial terms of elements not in N. Since $in(f) \in in(M) = in(N)$, we may write $in(f) = in(g)$ with $g \in N$. But then $f - g \in M - N$, and has smaller initial term than f -- a contradiction. //

Once we can compute Gröbner bases, Lemma 15 5 suffices to solve the "submodule membership" problem: Given a submodule M of a free module with basis F and an element $f \in F$, decide whether $f \in M$. To do this, choose a monomial order on F and find in(M) and in(M+Sf). By Lemma 15 5, the element f is in M iff $in(M) = in(M+Sf)$, and this is easy to test because in(M) and in(M+Sf) are monomial submodules. (In practice one would probably use the Division Algorithm presented in the next section instead of this method).

A Gröbner basis $g_1, \dots, g_t$ such that $in(g_i)$ does not divide $in(g_j)$ for any $i \neq j$ (that is, such that the $in(g_i)$ are a minimal set of generators for the monomial submodule they generate) is called a **minimal** Gröbner basis. We can make a Gröbner basis for M into a minimal Gröbner basis just by leaving out some elements. More interesting perhaps, a Gröbner basis $g_1, \dots, g_t$ such that $in(g_i)$ does not divide any term of g_j for $i \neq j$ is called **reduced** . If we assume in addition that $in(g_i)$ is a monomial (that is, the coefficient from k is 1) then we get something uniquely defined in terms of the submodule, the basis of F, the choice of variables in S, and the choice of order -- see Exercise 15 14.

The Division Algorithm

One of the most elementary and useful operations with polynomials in one variable is "division with remainder"; given polynomials f and g this algorithm constructs an expression of the form

$$f = f_1 g + f'$$

with degree $f_1 g$ = degree f and degree f' < degree g (or possibly $f'=0$). Given such an expression, f' is called the remainder on division. If we order the monomials of S by degree (that is: $x_1^s < x_1^t$ iff $s < t$; this is the unique monomial order on S, as the reader may easily verify) then we can restate the conditions on f_1 and f' above by saying that f' has no monomials in the initial ideal of (g), and $in(f) \geq in(f_1 g)$ (actually the monomials in question are equal). We will now extend this process to the general case. A side effect will be an algorithm for computing a Gröbner basis.

Proposition - Definition 15 6: Let F be a free S-module with basis and monomial order >. If $f, g_1, \dots, g_t \in F$ then there is an expression

$$f = \Sigma f_i g_i + f' \qquad \text{with } f' \in F,\ f_i \in S,$$

where none of the monomials of f' is in $(in(g_1), \dots, in(g_t))$ and

$$in(f) \geq in(f_i g_i)$$

for every i. Any such f' is called a **remainder** of f with respect to $g_1, \dots, g_t$, and an expression $f = \Sigma f_i g_i + f'$ satisfying the condition of the Proposition is called a **standard expression** for f in terms of the g_i.

The proof consists of an algorithm for finding a standard expression of the desired sort:

Division Algorithm 15 7: Let F be a free S-module with basis and a fixed monomial order. If $f, g_1, \dots, g_t \in F$ then we may produce a standard expression

$$f = \Sigma m_u g_{s_u} + f'$$

for f with respect to $g_1, \dots, g_t$ by defining the indices s_u and the terms m_u inductively: Having chosen $s_1, \dots, s_p$ and $m_1, \dots, m_p$, if

$$f'_p := f - \Sigma_{u=1}^{p} m_u g_{s_u} \neq 0$$

and m is the maximal term of f'_p that is divisible by some $in(g_i)$, then we choose

$$s_{p+1} = i$$

$$m_{p+1} = m/in(g_i).$$

This process terminates when either $f'_p = 0$ or no $in(g_i)$ divides a monomial of f'_p; the remainder f' is then the last f'_p produced. //

Lemma 15 2 guarantees that the algorithm terminates after finitely many steps because the maximal term of f'_p divisible by some g_i decreases at each step.

The division algorithm is most important in the case when the g_i form a Gröbner basis for a submodule M of F; then from the conditions of a standard expression, we see that the remainder f' gives the expression for f mod M in terms of the basis of F/M guaranteed us by Theorem 15 3. In fact, since Gröbner bases always exist, the Division algorithm gives us another, more constructive version of the second half of the proof of Theorem 15 3.

Note that standard expressions are far from unique: The division algorithm as we have stated it is indeterminate, in that the remainder depends on some choices made in carrying out the process. This is occasionally useful to make the computations in the Algorithms given below more efficient. In fact the division algorithm still terminates if at each stage we simply choose *some* monomial of f'_p divisible by some $in(g_i)$, instead of the greatest such. This gives a still more indeterminate version of the division algorithm, which works just as well for the purposes of this chapter. See Exercise 15 16.

It is sometimes useful to have a **determinate Division Algorithm** ; we can do this by specifying (for example) that at each step we take m to be the greatest monomial of f'_p that is divisible by some $in(g_i)$, and s_{p+1} the smallest i for which this division is possible. Such determinate division gives a unique standard expression satisfying certain auxiliary conditions. See Exercise 15 17.

It is easy to check that the division algorithm works just as well for weight orders and other monomial partial orders, so long as the initial forms of all the polynomials considered are monomials (the initial form is by definition the sum of *all* the maximal terms).

Gröbner bases

The division algorithm leads to a computation of Gröbner bases and syzygies on them, the two major topics of this chapter. We will make use of the following notation:

Let F be a free module over S with basis and monomial order >. Let $g_1, \dots, g_t$ be nonzero elements of F. Let $\oplus S\varepsilon_i$ be a free module with basis $\{\varepsilon_i\}$ corresponding to the elements $\{g_i\}$ of F, and let

$$\varphi: \oplus S\varepsilon_i \to F \quad ; \varepsilon_i \mapsto g_i$$

be the corresponding map.

For each pair of indices i,j such that $in(g_i)$ and $in(g_j)$ involve the same basis element of F, we define

$$m_{ij} = in(g_i) / GCD(in(g_i), in(g_j)) \in S$$

and we set

$$\sigma_{ij} = m_{ji}\, \varepsilon_i - m_{ij}\, \varepsilon_j,$$

so that the σ_{ij} generate the syzygies on the elements $in(g_i)$ by Lemma 15 1. For each such pair i,j, we choose a standard expression

$$m_{ji}\, g_i - m_{ij}\, g_j = \Sigma f_u^{(ij)} g_u + h_{ij}$$

for $m_{ji}\, g_i - m_{ij}\, g_j$ with respect to $g_1, \dots, g_t$. Note that $in(f_u^{(ij)} g_u) < in(m_{ji}\, g_i)$. For convenience we set $h_{ij} = 0$ if $in(g_i)$ and $in(g_j)$ involve distinct basis elements of F.

With this notation we have:

Theorem 15 8 (Buchberger's Criterion): The elements $g_1, \dots, g_t$ form a Gröbner basis iff $h_{ij} = 0$ for all ij.

Proof: Let $M = (g_1, \dots, g_t) \in F$. From the expression for h_{ij} we see that $h_{ij} \in M$, and thus $in(h_{ij}) \in in(M)$. If $g_1, \dots, g_t$ is a Gröbner basis, then, as remarked just after the proof of the division algorithm, the definition of a standard expression shows that $h_{ij} = 0$.

Conversely, suppose that all $h_{ij} = 0$, so that $\varphi(\sigma_{ij}) = \Sigma f_u^{(ij)} g_u$ with $in(f_u^{(ij)} g_u) < in(m_{ji} g_i)$. If $g_1, \dots, g_t$ is not a Gröbner basis then we may choose an expression

$$f = \Sigma_u f_u g_u \text{ with } in(f) \notin (in(g_1), \dots, in(g_t)).$$

Let m be the maximum among the terms $in(f_u g_u)$. We may suppose that the expression for f has been chosen so that m is as small as possible. Now let $\Sigma' f_v g_v$ be the sum of all those $f_v g_v$ for which $in(f_v g_v)$ is m times a scalar. We may write $in(f_v g_v) = n_v \, in(g_v)$ for some term n_v of f_v. If the sum of the corresponding initial terms $\Sigma' n_v \, in(g_v)$ is nonzero, then it is the initial term of f; as it is a multiple of m, it is a multiple of $in(g_v)$, contradicting the choice of f. Thus

$$\Sigma' n_v \, in(g_v) = 0,$$

so that $\Sigma' n_v \varepsilon_v$ is a syzygy among the $in(g_v)$.

By Lemma 15 1 bis, we may write $\Sigma' n_v \varepsilon_v = \Sigma_{i<j} a_{ij}\sigma_{ij}$ where a_{ij} is a scalar times $m/(in(g_i)$. If we apply φ and substitute $\Sigma f_u^{(ij)} g_u$ for $\varphi(\sigma_{ij})$, we find a relation of the form

$$\Sigma' n_v g_v = \Sigma h_s g_s$$

with all $in(h_s g_s) < m$. Subtracting the expression $\Sigma' n_v \; g_v - \Sigma h_s g_s$ from the expression for f and cancelling the terms of $\Sigma' n_v \, in(g_v)$, we get a new expression for f of the same form but where the maximum of the $in(f_u g_u)$ is smaller, contradicting our construction. //

One can slightly sharpen the criterion in a way that is occasionally useful in practice: It is enough for h_{ij} to be zero for any subset of pairs i,j such that the corresponding σ_{ij} generate all the syzygies on the elements $in(g_i)$, and if $F = S$ we may further omit any pair i,j such that $GCD(in(g_i), in(g_j)) = 1$; see Exercise 15 19 and Exercise 15 20.

From Theorem 15 8 we get an effective method for computing Gröbner bases and syzygies

Buchberger's Algorithm 15 9: In the situation of Theorem 15 8, suppose that M is a submodule of F, and let $g_1, \dots, g_t \in M$ be a set of generators of M. Compute the remainders h_{ij}. If all the $h_{ij} = 0$, then the g_i form a Gröbner basis for M. If some $h_{ij} \neq 0$, then replace $g_1, \dots, g_t$ with $g_1, \dots, g_t, h_{ij}$ and repeat the process. As the submodule generated by the initial forms of $g_1, \dots, g_t, h_{ij}$ is strictly larger than that generated by the initial forms of $g_1, \dots, g_t$, this process must terminate after finitely many steps.

The process involved in Buchberger's Algorithm is even more useful than first appears: Theorem 15 10 below shows that the equations $h_{ij} = 0$ that result if the g_i are a Gröbner basis give all the syzygies on M (this is Schreyer's Algorithm for computing syzygies).

A worked example is given at the end of the following subsection.

There is a fairly sharp "worst case" upper bound b for the degree of the elements of the Gröbner basis for a homogeneous ideal $(g_1, \dots, g_t) \subset S$ (the inhomogeneous case can be reduced to this) with respect to the lexicographic order. The bound, which is due to H. M. Möller and F. Mora [1984] is in terms of:

r = the number of variables,
d = the maximum degree of the polynomials g_i,

s = the degree of the Hilbert polynomial (this will be studied extensively below as the dimension; it ranges from 0 to ≤ r-1).

The bound is

$$b = ((r+1)(d+1)+1)^{2^{(s+1)}(r+1)},$$

and thus is potentially doubly exponential in the number of variables.

For example, for the homogeneous ideal of a curve of degree δ in $\mathbb{P}^3$, it is known that we can take $r = 4$, $s = 2$, $d = \delta-1$, and we get

$$b \sim (4\delta+1)^{32}.$$

This estimate is so large as to suggest that Buchberger's Algorithm and Gröbner bases would be useless in practice. Fortunately this is not at all the case: In actual use the algorithm terminates quite quickly on very many problems of interest. There is a partial understanding of why this is so, and various other bounds are known in some special cases; see for example Gruson-Lazarsfeld-Peskine[1983], F. Winkler [1984], and Bayer-Stillman [1987a].

Syzygies

We retain the notation introduced in the previous section.

There is a bonus from Buchberger's algorithm: An effective method for computing syzygies. The process in Algorithm 15 9 gives a linear combination of the g_u that is equal to h_{ij}. Thus if $h_{ij} = 0$ we get a linear relation among the g_u -- that is, a syzygy. It turns out that these syzygies generate the entire module of syzygies on the g_i.

We retain the notation developed for Theorem 15 8. In addition, for $i < j$ such that $\mathrm{in}(g_i)$ and $\mathrm{in}(g_j)$ involve the same basis element of F, we set

$$\tau_{ij} = m_{ji}\, \varepsilon_i - m_{ij}\, \varepsilon_j - \Sigma_u\, f_u^{(ij)}\, \varepsilon_u.$$

Theorem 15 10 (Schreyer): With notation as above, suppose that $g_1, \dots, g_t$ is a Gröbner basis. Let > be the monomial order on $\oplus_{j=1}^{t} S\varepsilon_j$ defined by taking $m\varepsilon_u > n\varepsilon_v$ iff

$$\mathrm{in}(mg_u) > \mathrm{in}(ng_v) \text{ with respect to the given order on F}$$

or

$$\mathrm{in}(mg_u) = \mathrm{in}(ng_v) \text{ (up to a scalar) but } u < v.$$

The τ_{ij} generate the syzygies on the g_i. In fact, the τ_{ij} are a Gröbner basis for the syzygies with respect to the order >, and $\mathrm{in}(\tau_{ij}) = m_{ji}\, \varepsilon_i$.

Proof: We show first that the initial term of τ_{ij} is $m_{ji}\varepsilon_i$. We have

$$m_{ji}\, \mathrm{in}(g_i) = m_{ij}\, \mathrm{in}(g_j),$$

and these terms are by hypothesis greater than any that appear in the $f_u^{(ij)} g_u$. Thus $\mathrm{in}(\tau_{ij})$ is either $m_{ji}\varepsilon_i$ or $-m_{ij}\, \varepsilon_j$ by the first part of the definition of >, and since i < j we have $m_{ji}\varepsilon_i > m_{ij}\,\varepsilon_j$.

Now we show that the τ_{ij} form a Gröbner basis. Let $\tau = \Sigma f_v\,\varepsilon_v$ be any syzygy. We must show that $in(\tau)$ is divisible by one of the $in(\tau_{ij})$; that is, $in(\tau)$ is a multiple of some $m_{ji}\varepsilon_i$ with i < j.

For each index v, set $n_v\varepsilon_v = in(f_v\varepsilon_v)$. Since these terms cannot cancel with each other, we have $in(\Sigma f_v\,\varepsilon_v) = n_i\,\varepsilon_i$ for some i. Let $\sigma = \Sigma' n_v\,\varepsilon_v$ be the sum over all indices v for which $n_v\,in(g_v) = n_i\,in(g_i)$ up to a scalar; all indices v in this sum must be ≥ i because we have assumed that $n_i\varepsilon_i$ is the initial term of τ.

Thus σ is a syzygy on the $in(g_v)$ with $v \geq i$. By Lemma 15 1, all such syzygies are generated by the σ_{uv} for $u,v \geq i$, and the ones in which ε_i appears are the σ_{ij} for j > i. It follows that the coefficient n_i is in the ideal generated by the m_{ji} for j > i, and we are done. //

As with Buchberger's Criterion, we can sharpen this result slightly in a useful way: To find a set of τ_{ij}, which generate all the syzygies on the g_i, it is enough to take a set of pairs i,j such that the σ_{ij} generate the syzygies of the elements $in(g_i)$. See Exercise 15 18.

If we wish to use Theorem 15 10 to compute syzygies on a fixed set of elements $g_1, \ldots, g_t$, we first use Buchberger's Algorithm to obtain a Gröbner basis for $(g_1, \ldots, g_t)$ and the syzygies on the Gröbner basis elements. To get the syzygies on the g_i, we need only substitute into these the expressions for the Gröbner basis elements in terms of the g_i.

This process usually will not give us a minimal set of syzygies: To replace it with a minimal set (say in the case where everything is homogeneous, so the minimal resolutions are well defined; see Chapter 21) we must do some further work, finding at least the degree 0 syzygies among the nonminimal syzygies, and using them to eliminate superfluous relations. Nevertheless, this process is by far the most efficient method known for computing syzygies.

An example will help to clarify all this:

Example: The simplest nontrivial Gröbner basis computation : Take $g_1 = x^2$, $g_2 = xy+y^2$. We will find a Gröbner basis with respect to the lexicographic order, taking x > y. We have $in(g_1) = x^2$, $in(g_2) = xy$. The GCD is x. We apply the Division algorithm to

$$(in(g_2)/x)\ g_1 - (in(g_1)/x)\ g_2 = -xy^2.$$

In the first step we add yg_2, getting y^3. Since this is not divisible by either initial form, it is the remainder; as it is not 0, we take it as

$$g_3 = y^3,$$

and we have the syzygy

$$\tau_{1,2} :\ y\ \varepsilon_1 - x\ \varepsilon_2 + y\ \varepsilon_2\ - \varepsilon_3\ .$$

Since g_1 and g_3 are monomials, we get from them a syzygy

$$\tau_{1,3} : y^3\varepsilon_1 - x^2\ \varepsilon_3\ .$$

The only other pair to check is g_2 and g_3: Applying the division algorithm to

$$(in(g_3)/y)\ g_2 - (in(g_2)/y)\ g_3 = y^4,$$

we subtract y g_3 and find a remainder of 0. Thus we get the syzygy

$$\tau_{2,3} : y^2\ \varepsilon_2 - x\ \varepsilon_3 - y\ \varepsilon_3 = y^2\ \varepsilon_2 - (x + y)\ \varepsilon_3\ .$$

From Buchberger's Criterion we see now that

$$x^2,\ xy+y^2,\ y^3$$

is a Gröbner basis, and from Theorem 15 10 we know that $\tau_{1,2}$, $\tau_{2,3}$ and $\tau_{1,3}$ generate the syzygies on them. If we wish to derive from this a set of generators for the syzygies on the original generators g_1, g_2, we must substitute the expression for g_3 in terms of g_1 and g_2 given by the syzygy $\tau_{1,2}$ into the other syzygies. We get

$$\tau_{1,2} : \ 0$$

$$\tau_{1,3}: \ y^3\varepsilon_1 - x^2(y\ \varepsilon_1 - x\ \varepsilon_2 + y\ \varepsilon_2) = (y^3-x^2y)\ \varepsilon_1 + (x^3-x^2y)\ \varepsilon_2$$

$$\tau_{2,3} : y^2\ \varepsilon_2 - (x + y)\ \varepsilon_3 = y^2\ \varepsilon_2 - (x + y)\ (y\ \varepsilon_1 - x\ \varepsilon_2 + y\ \varepsilon_2)$$

$$= x^2\varepsilon_2 - (xy+y^2)\ \varepsilon_1.$$

We see that $\tau_{1,3} = (x-y)\tau_{1,2}$, so in fact the syzygies are generated by $\tau_{2,3}$. (In this simple case it is easy to see directly that $\tau_{2,3}$ generates the syzygies on g_1, g_2: Just use unique factorization and the fact that g_1 and g_2 are relatively prime.)

One Corollary of Theorem 15 10 is a sharpened form of the Hilbert Syzygy Theorem, which says that every finitely generated S-module has a free resolution of length $\le r$. We will give a more abstract proof in Chapter 19.

Corollary 15 11: With notation as in Theorem 15 10 suppose that the g_i are arranged so that whenever $\mathrm{in}(g_i)$, $\mathrm{in}(g_j)$ involve the same basis vector e of F, say $\mathrm{in}(g_i) = n_i e$ and $\mathrm{in}(g_j) = n_j e$ with $n_i, n_j \in S$ we have

$$i < j \quad \Rightarrow \quad n_i > n_j \text{ in the lexicographic order.}$$

If the variables $x_1, \dots ,x_s$ are missing from the initial terms of the g_i, then the variables $x_1, \dots ,x_{s+1}$ are missing from the $\mathrm{in}(\tau_{ij})$, and $F/(g_1, \dots ,g_t)$ has a free resolution of length $\le r - s$.

In particular, every finitely generated S-module has a free resolution of length $\le$ r.

Remark: The last statement is true for all S-modules: The Hilbert Syzygy Theorem with Auslander's Lemma (Lemma A3.18) shows that every S-module has a projective resolution of length $\le$ r, and in fact Quillen has showed that every projective S-module is free. (See for example Lam [1978] for an exposition.)

Proof: By Theorem 15 10 we have $\mathrm{in}(\tau_{ij}) = m_{ji}\ \varepsilon_i$, and $m_{ji} = m_j/\mathrm{GCD}(m_i,m_j)$. Since $m_i = \mathrm{in}(g_i)$ is $\ge m_j = \mathrm{in}(g_j)$ in the lexicographic order, x_{s+1} appears to at least as high a power in m_i as in m_j, and thus does not appear at all in m_{ji}. This proves the first statement.

We next show that $F/(g_1, \dots ,g_t)$ has a free resolution of length $\le r - s$ by induction on r-s. Suppose first that r-s = 0, so that none of the variables x_i appear in the terms $\mathrm{in}(g_i)$; we must show that $F/(g_1, \dots ,g_t)$ is free.

Since the initial terms of the g_i must be scalars times basis elements of F, we see that $\mathrm{in}(g_1, \dots ,g_t)$ is the free submodule of F generated by the e_i that appear among the $\mathrm{in}(g_i)$. Let F' be the free submodule spanned by the other e_j, and consider the composite map

$$F' \subset F \rightarrow F/(g_1, \dots ,g_t).$$

By Theorem 15 3, $F/(g_1, \dots ,g_t)$ has a basis consisting of precisely the monomials coming from F', so the map is an isomorphism and $F/(g_1, \dots ,g_t) \cong F'$ is free as required.

Now suppose r-s > 0. By the first statement, $x_1, \dots ,x_{s+1}$ are missing from the initial terms of the τ_{ij}. We may order the τ_{ij} so as to satisfy the same hypothesis as that on the g_i. It follows from the induction that $F_1/(\{\tau_{ij}\})$ has a free resolution of length $\le r - s - 1$, and putting this together with the map $F_1 \rightarrow F$, we get the desired free resolution of

$F/(g_1, \dots , g_t)$.//

A property of reverse lexicographic order

The reverse lexicographic order on a S satisfies a key property not shared by other orders that makes the connection between an ideal and its initial ideal particularly tight. As Bayer and Stillman show in [1987a], it also has practical consequences that make the reverse lexicographic order preferable for computation in some circumstances.

Since we wish to be able to work with modules, we need the following definition:

Definition: Let F be a graded free S-module with basis $\{e_1, \dots ,e_n\}$. A monomial order > on F is called a **reverse lexicographic order** if it refines the order by total degree and satisfies the following property: If $f \in F$ is a homogeneous element and $in(f) \in (x_s,\dots,x_r)F$ for some $1 \le s \le r$, then $f \in (x_s,\dots,x_r)F$.

Equivalently, as the reader may check, a reverse lexicographic order is defined by choosing an order on the e_i, say $e_1 > \dots > e_n$, and setting $me_i > ne_j$ iff either degree $me_i >$ degree ne_j or the degrees are the same and $m >_{revlex} n$ or $m = n$ and $i < j$.

The defining property of reverse lexicographic orders translates into good behavior upon factoring out the last variable. The following easy result is the key:

Proposition 15 12: Suppose that F is a free S-module with basis $\{e_1, \dots ,e_n\}$ and reverse lexicographic order, and suppose that $g_1, \dots ,g_t$ is a homogeneous Gröbner basis of a graded submodule M.

a) $in(M+x_rF) = in(M) +x_rF$. Thus $g_1, \dots ,g_t, x_re_1, \dots ,x_re_n$ is a Gröbner basis of $M+x_rF$.

b) $(in(M) :_F x_r) = in(M :_F x_r)$. Further, if we set $\tilde{g}_i = g_i/(GCD(x_r, g_i)$, then $\tilde{g}_1, \dots ,\tilde{g}_t$ is a Gröbner basis for $(M :_F x_r)$.

The Proposition remains true, by virtually the same proof, if x_r is replaced by x_r^d. See Exercise 15 41 for an application.

Proof: a) We must show that $in(M + x_rF) = in(M) + x_rF$. The inclusion $\supseteq$ is clear. To prove the opposite inclusion, choose $f \in M + x_rF$ homogeneous; we must show that $in(f) \in in(M) + x_rF$. Write $f = g + h$, with $g \in M$ homogeneous and $h \in x_rF$. If in(f) is not a scalar multiple of in(g), then $in(f) = in(h) \in x_rF$, and it follows that every term of g is ≤ this monomial in x_rF. From the definition of a reverse lexicographic order, we see that every term of g, and thus g itself, is in x_rF. Thus $f \in x_rF$, and so also $in(f) \in x_rF$, as required.

b) If x_r divides in(g) for some homogeneous $g \in F$ then since we are using reverse lexicographic order, x_r divides g. The first statement of b) follows at once.

By the same reasoning, $(in(g_i):_F x_r)$ is generated by $in(\tilde{g}_i)$ for every i, whence

$$(in(M) :_F x_r) = (in(\tilde{g}_1), \dots ,in(\tilde{g}_t)).$$

since clearly $\tilde{g}_1, \dots ,\tilde{g}_t \in (M :_F x_r)$, this shows that the $in(\tilde{g}_i)$ form a Gröbner basis.//

Using these properties, we get a criterion for x_r to be a nonzerodivisor on an S-module, or more generally for the last variables in reverse order to be a regular sequence. (Recall from Chapter 10 that $x_r, \dots , x_s$ form a regular sequence on an S-module N if, first, $(x_r, \dots , x_s)N \neq N$, and second, x_r is a nonzerodivisor on N, x_{r-1} is a nonzerodivisor on N/x_rN, and so on.)

Theorem 15 13 (Bayer-Stillman [1987]): Let F be a free module with basis and a reverse lexicographic monomial order. Suppose $M \subset F$ is a homogeneous submodule. The elements $x_r, \dots, x_s$ form a regular sequence on F/M iff $x_r, \dots, x_s$ form a regular sequence on $F/\mathrm{in}(M)$.

These results may be used to show that certain homological properties of F/M may be deduced from $F/\mathrm{in}(M)$; see Corollary 19.11 and Corollary 20.21.

We note that if M is a graded submodule of F then any permutation of a regular sequence on F/M is again a regular sequence on F/M. Thus we could make the same statement with the variables in the natural order $x_s, \dots, x_r$. But this "permutability of regular sequences" is somewhat subtle: It is not true without either local or graded hypotheses. We shall return to this issue in Chapter 17.

Before proving the Theorem we need an elementary criterion:

Proposition 15 14: Let F be a free module with basis $\{e_1, \dots, e_n\}$. If $N \subset F$ is a monomial submodule minimally generated by $n_1, \dots, n_t$, then a sequence of monomials $m_1, \dots, m_u \in S$ is a regular sequence modulo N iff each m_i is relatively prime to each n_i and to each m_j for $j \neq i$.

Proof: Suppose first that each m_j is relatively prime to each n_i and to each m_i for $j \neq i$. Since al the m_i and n_i are monomials, any polynomial annihilating m_v modulo $N + (m_1, \dots, m_{v-1})F$ is a sum of monomials from the sets $(Sn_i : m_v) = Sn_i$ and $(m_iF: m_v) = m_iF$. This shows that $m_1, \dots, m_u$ is a regular sequence on F/N.

Conversely, suppose that $m_1, \dots, m_u$ is a regular sequence on F/N. We will do induction on u. First we show that m_1 is relatively prime to each n_i. If $\mathrm{GCD}(m_1, n_i) = n$, then $m_1 n_i/n \in N$, and since m_1 is a nonzerodivisor on F/N, we see that $n_i/n \in N$. Since n_i is part of a minimal set of generators of N, we must have $n_i/n = n_i$, so $n = 1$.

Since in addition no m_1e_i is in N, it is immediate that

$n_1, \dots, n_t, m_1e_1, \dots, m_1e_n$ is a minimal set of generators for $N + m_1F$. Now $m_2, \dots, m_u$ satisfy the hypothesis of the Proposition with respect to the submodule $N + m_1F$, so by induction these m_i are relatively prime to each other and to each n_i and to each m_1e_i. From the last condition we deduce that they are relatively prime to m_1, and we are done.//

The next result is a generalization of one implication of Theorem 15 13. We will say that a monomial order > on a free S-module F with basis $\{e_i\}$ is **compatible** with a monomial order > on S itself if for $h \in S$ and $f \in F$ we have $\mathrm{in}(hf) = \mathrm{in}(h)\,\mathrm{in}(f)$. Equivalently, a compatible monomial order on F is one that compares monomials me_i and $m'e_i$ involving the same basis vector by using the given ordering on m and m'. Most monomial orders used in practice have this property.

Proposition 15 15: Let F be a free S-module with basis and monomial order compatible with a given monomial order on S. If $M \subset F$ is any submodule and $h_1, \dots, h_u \in S$ are such that $\mathrm{in}(h_1), \dots, \mathrm{in}(h_u)$ is a regular sequence on $F/\mathrm{in}(M)$, then $h_1, \dots, h_u$ is a regular sequence on F/M.

Proof: Note that the condition of Proposition 15 14 is symmetric, so that any permutation of $\mathrm{in}(h_1), \dots, \mathrm{in}(h_u)$ is a regular sequence on $F/\mathrm{in}(M)$, and, in particular, each of the $\mathrm{in}(h_i)$ is a nonzerodivisor modulo $\mathrm{in}(M)$. Further, the condition of the Proposition implies the corresponding condition with $N = 0$, so the $\mathrm{in}(h_i)$ form a regular sequence on F.

We proceed by induction on u; using the symmetry of Proposition 15 14 we may assume that every proper subset of the h_i forms a regular sequence. Suppose that $f = \Sigma_{i=1}^{u} h_if_i \in M$. We will show that, for some v,

$$\mathrm{in}(f_v) \in \mathrm{in}(M) + (\mathrm{in}(h_1), \dots, \mathrm{in}(h_{v-1}))F.$$

We may then subtract an element of $M + (h_1, \dots, h_{v-1})F$ from f_v and lower $\mathrm{in}(f_v)$. Proceeding in this way, we arrive at a situation where some $f_v = 0$. By our induction, the h_i other than h_v form a regular sequence, and we conclude that $f_u \in M + (h_1, \dots ,h_{v-1})F$, showing that $h_1, \dots ,h_u$ is a regular sequence on F/M as required.

Let n be the maximal monomial that appears among the $\mathrm{in}(h_i)\mathrm{in}(f_i)$, and let v be one of the i for which it appears. If

$$\Sigma_{i \text{ such that } \mathrm{in}(f_i)\mathrm{in}(h_i)=n}\, \mathrm{in}(h_i)\ \mathrm{in}(f_i) = 0,$$

then we must have $\mathrm{in}(f_v) \in (\mathrm{in}(h_1), \dots ,\mathrm{in}(h_{v-1}))F$ because the $\mathrm{in}(h_i)$ form a regular sequence on F, and we are done. If, on the contrary, the sum is not 0, then it is in(f), and thus an element of in(M). Since each of the $\mathrm{in}(h_i)$ is a nonzerodivisor modulo in(M), it follows that $\mathrm{in}(f_v) \in \mathrm{in}(M)$, and again we are done.//

Proof of Theorem 15 13: If $x_r, \dots ,x_s$ is a regular sequence on $F/\mathrm{in}(M)$ then $x_r, \dots ,x_s$ is a regular sequence on F/M by Proposition 15 15.

It remains to prove the converse. In the case s = r, Proposition 15 12 b` shows that x_r is a nonzerodivisor on $F/\mathrm{in}(M)$, as required. Factoring out x_rF and using Proposition 15 12 a) we are done by induction.//

Gröbner bases and flat families

All the applications of the idea of Gröbner bases work by comparing an arbitrary ideal with its "initial" ideal, which is a monomial ideal (and more generally, by comparing a submodule of a free module with an associated initial submodule). Why should these two be similar enough to make the comparison profitable? The situation is quite similar to that of the associated graded ring treated in Chapter 5. As in the case of the Rees algebra construction defined in Chapter 6, an "explanation" is provided by the existence of certain flat families, which we will now describe. For simplicity we give the constructions below for ideals, rather than for arbitrary submodules of a free module with basis; the (easy) extension to the case of modules is left to the interested reader.

The flat family that we will describe is defined in terms of an integral weight function $\lambda: \mathbb{Z}^r \to \mathbb{Z}$. For convenience of notation, we think of λ as a function on monomials, and if $m = x^a$, we write $\lambda(m) \in \mathbb{Z}$ in place of $\lambda(a)$. Let $>_\lambda$ be the weight order defined by λ on the monomials of S. Although it is only a partial order, much of our formalism for monomial orders can be imitated for $>_\lambda$. For example, given $g \in S$ we write $\mathrm{in}_\lambda(g)$ for the sum of all the terms of g that are maximal with respect to $>_\lambda$, and if I is an ideal we write $\mathrm{in}_\lambda(I)$ for the ideal generated by $\mathrm{in}_\lambda(g)$ for all $g \in I$.

Before describing the flat family, we will show that integral weight orders are potent enough to capture the transition from a given ideal to its initial ideal with respect to an arbitrary monomial order. Suppose that > is a monomial order on S, and $I \subset S$ is an ideal. Given any finite set of pairs of monomials $\mathcal{S} = \{(m_i > n_i)\}$, Exercise 15 12 shows that there is an integral weight order $>_\lambda$ such that $m_i >_\lambda n_i$ for all i. Thus we may apply the following Proposition.

Proposition 15 16: Let > be a monomial order on S, and suppose that $g_1, \dots ,g_t$ is a Gröbner basis for an ideal I with respect to >. There is a finite set $\mathcal{S} = \{(m_1 > n_1), \dots ,(m_s > n_s)\}$ of pairs of monomials such that if $>_\lambda$ is a weight order on S with $(m_1 >_\lambda n_1), \dots ,(m_s >_\lambda n_s)$, then $g_1, \dots ,g_t$ is a Gröbner basis for I with respect to $>_\lambda$ and $\mathrm{in}_\lambda (I) = \mathrm{in}_>(I)$.

Proof: For each i = 1, ... ,t we put into $\mathcal{S}$ all the pairs of monomials of the form $(\mathrm{in}(g_i) > n)$, where n is a monomial of g_i. Next, we use use the Buchberger criterion, Theorem 15 8, to verify that the g_i are a Gröbner basis with respect to >; the verification depends on computing the initial terms of finitely many polynomials, and involves finitely many uses of the division algorithm. For each polynomial g whose initial term we must compute, we put the pairs $(\mathrm{in}_>(g), n)$ into $\mathcal{S}$ for every monomial n of g. Similarly, each use of the division algorithm involves finitely many comparisons of pairs of monomials. We expand the list of monomials by including the pairs of monomials involved.

Now the Division algorithm and the proof of Buchberger's Criterion work for weight orders and other monomial partial orders satisfying the multiplicative properties in the definition of monomial orders just as well as for total orders, so long as all the initial terms involved are monomials. Thus a second use of the Buchberger algorithm shows that the g_i form a Gröbner basis with respect to $>_\lambda$. In particular, the in(g_i) generate in$_\lambda$(I). Since in$_>$(g_i) = in$_\lambda$(g_i), we are done. //

We may describe the flat family of algebras informally as follows: Let λ be an integral weight function. For any $0 \neq t \in k$, there is an automorphism of S carrying x_i to $t^{-\lambda(x_i)}x_i$, and we write I_t for the image of I under this automorphism. Clearly all the rings S/I_t for $t \neq 0$ are isomorphic. But as t approaches 0, the initial terms of polynomials in I_t -- those whose values under λ are largest -- come to dominate the polynomials, and the limit, the fiber over $t = 0$, will be S/in$_\lambda$(I).

To make precise mathematics out of this description, let S[t] be a polynomial ring in one variable over S. For any $g \in S$, we define $\tilde{g} \in S[t]$ as follows. Write $g = \Sigma u_i m_i$ where the m_i are monomials and $0 \neq u_i \in k$. Let $b = \max \lambda(m_i)$, and set

$$\tilde{g} = t^b g(t^{-\lambda(x_1)}x_1, \dots , t^{-\lambda(x_r)}x_r).$$

Because of the way b was defined, we see that $\tilde{g}$ is in$_\lambda$(g) plus t times a polynomial in t and $x_1, \dots , x_r$. For any ideal $I \subset S$, let $\tilde{I}$ be the ideal of S[t] generated by $\{\tilde{g} \mid g \in I\}$. It follows that $S[t]/((t) + \tilde{I}) \cong S/\mathrm{in}_\lambda(I)$. The next result extends this and gives a more sophisticated interpretation:

Theorem 15 17: For any ideal $I \subset S$, the k[t]-algebra $S[t]/\tilde{I}$ is free -- and thus flat -- as a k[t]-module. Furthermore,

$$S[t]/\tilde{I} \ \otimes_{k[t]} k[t,t^{-1}] \ \cong S/I\ [t,t^{-1}],$$

while

$$S[t]/\tilde{I} \ \otimes_{k[t]} k[t]/(t) \ \cong S/\mathrm{in}_\lambda(I).$$

Thus $S[t]/\tilde{I}$ is a flat family over k[t] of quotients of S whose fiber over 0 is S/in$_\lambda$(I) and whose fiber over any (t-u), for $0 \neq u \in k$, is S/I.

(To give the flat family constructively, in the spirit of this chapter, we should specify a finite set of generators for the ideal $\tilde{I}$. Results of this sort may be found in Exercise 15 25.)

Proof: From the fact that $\tilde{g}$ is in$_\lambda$(g) plus t times a polynomial in t and $x_1, \dots , x_r$, it is clear that

$$S[t]/\tilde{I} \ \otimes_{k[t]} k[t]/(t) \ = S[t]/(\tilde{I} + (t)) = S/\mathrm{in}_\lambda(I).$$

Let φ be the automorphism of $S \otimes_{k[t]} k[t,t^{-1}] = S[t,t^{-1}]$ defined by $\varphi(x_i) = t^{\lambda(x_i)}x_i$. This automorphism takes the ideal $\tilde{I}S[t,t^{-1}]$ to the ideal $IS[t,t^{-1}]$; it follows that φ induces an isomorphism $S[t]/\tilde{I} \ \otimes_{k[t]} k[t,t^{-1}] \ \cong S/I\ [t,t^{-1}]$.

It thus remains to prove the first statement of the Theorem. Let > be a monomial order refining $>_\lambda$ and let B be the set of monomials not in in$_>$(I). B is a basis of S/I by Theorem 15 3. We claim that B is also a k[t]-basis for $S[t]/\tilde{I}$.

First, to prove linear independence, it is enough to show that the elements of B are linearly independent over $k[t,t^{-1}]$, as elements of $S[t,t^{-1}]$. From Theorem 15 3 we deduce that the elements of B form a $k[t,t^{-1}]$-basis of $S[t,t^{-1}]/IS[t,t^{-1}]$. Thus $\varphi^{-1}(B)$ is a basis for $S[t,t^{-1}]/\tilde{I}S[t,t^{-1}]$. But the automorphism φ^{-1} carries any monomial m into $t^{-\lambda(m)}m$, that is, a unit of $S[t,t^{-1}]$ times m. Thus B itself is a $k[t,t^{-1}]$-basis of $S[t,t^{-1}]/\tilde{I}S[t,t^{-1}]$. In particular its elements are linearly independent in $S[t]/\tilde{I}$.

Finally, we must show that B generates $S[t]/\tilde{I}$ as a k[t]-module.

Regarding B as a subset of S[t], we must show that the k[t]-span of B contains, modulo elements of $\tilde{I}$, every monomial m in the x_i. Because the order > is Artinian, we may inductively assume that this has been verified for every monomial $n < m$. The monomial m is either in B or else $m = \mathrm{in}_>(g)$ for some $g \in I$. In the latter case $m - \tilde{g}$ is a k[t]-linear combination of monomials that are $< m$, and we are done by induction. //

The technique embodied in the preceding result can be used to give a flat family connecting any given finite set of ideals to their initial ideals. (If one is willing to exchange the simple "base" k[t] of the family used above for something more complicated -- generally not Noetherian -- one can give a deformation that works for all ideals at once; see Exercise 15 26.)

Here are some examples in pictures. We treat the case of 3 points in the projective plane (Figures 15.3 and 15.4) and the case of a smooth conic in the projective plane (Figures 15.5 and 15.6; first with the lexicographic and then the reverse lexicographic orders. We thus work in the polynomial ring in 3 variables, k[x,y,z], with $x > y > z$. The coordinate triangle of lines $x = 0$, $y = 0$, and $z = 0$ is distinguished by the choice of coordinates, shown in Figure 15.2.

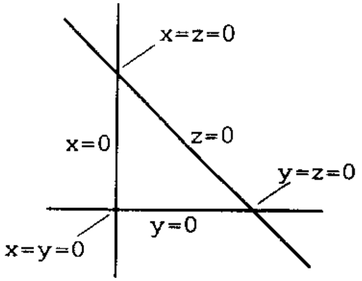


Figure 15.2

To simulate the lexicographic order we use two weight orders. First we deform according to the family corresponding to weights (1, 0, 0). This may be interpreted either as "attract to x=0" or as "repel from y=z=0. Next we deform according to the family corresponding to weights (0,1,0). This may be interpreted either as "attract to y=0" or as "repel from x=z=0".

Similarly, to simulate the reverse lexicographic order we use first the deformation corresponding to the weight vector (1,1,0), or equivalently (0,0,-1). Its effect is to attract to the point x=y=0 and repel from the line z=0. Next we use the weight vector (1,0,1) or equivalently (0,-1,0): The effect is to attract to x=z=0 and repel from y=0.

When looking at the Figures, bear in mind that in each deformation each corner of the coordinate triangle is fixed under the deformations, and each of the three lines of the triangle is sent into itself.

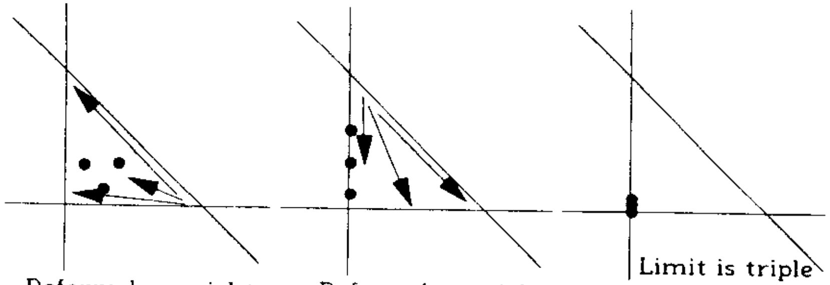
Here is the case of a set Γ of 3 general points in the plane. If we take these to be the points (1,1,1), (1/3,1/2,1), and (1/2,1/3,1), then the ideal of Γ is

$$\begin{aligned} I(\Gamma) = \quad (\quad & x^2 + xy - (11/6)xz - yz + (5/6)z^2, \\ & xy + y^2 - xz - (11/6)yz + (5/6)z^2, \\ & y^2 - (2/7)xz - (47/42)yz + (17/42)z^2 \quad). \end{aligned}$$

With a little computation one sees that in lexicographic order the initial ideal is $(x^2, xy, xz, y^3) = (x(x,y,z), y^3)$. This last ideal is not saturated; its saturation is (x,y^3). Thus the limiting position for this deformation is the 2nd order neighborhood of the point x=y=0 in the line x=0. It is perhaps easier to see that in reverse lexicographic order the initial ideal is (x^2, xy, y^2), so the limiting position is the first order neighborhood of the point x=y=0 in the plane. From these computations we see that the two deformations have nonisomorphic limits.

Lexicographic deformation of 3 points

Start with general points
(1,1,1), (1/2,1/3,1), (1/3,1/2,1).



Deform by weight vector 1, 0, 0

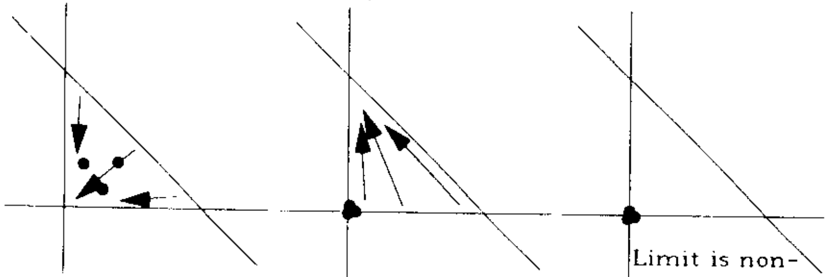
Deform by weight vector 0, 1, 0

Limit is triple point aligned on x=0.

Figure 15.3

Reverse lexicographic deformation of 3 points

Start with genera. points
(1,1,1), (1/2,1/3,1), (1/3,1/2,1).



Deform by weight vector 1, 1, 0

Deform by weight vector 1, 0, 1

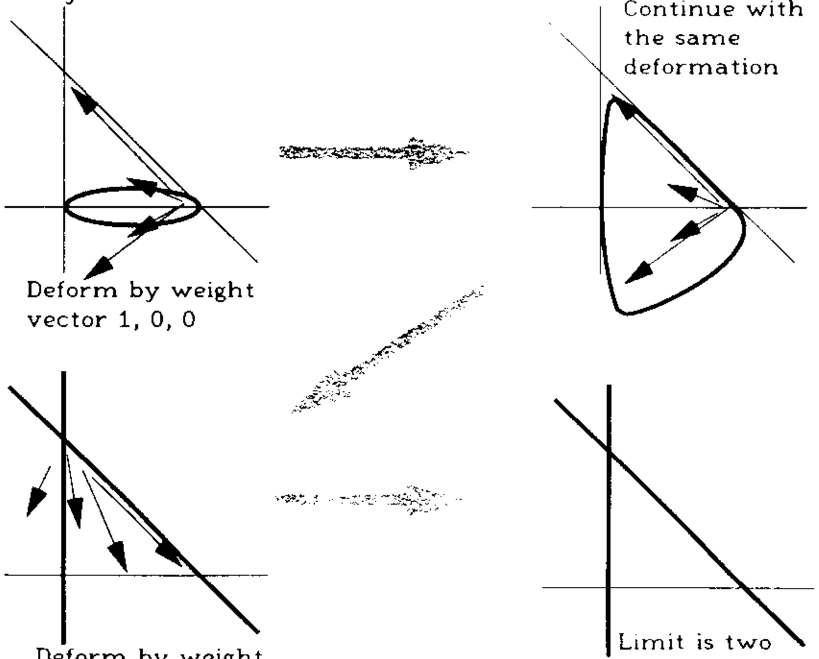
Limit is non-colinear triple point

Figure 15.4

Next we try the same deformations on the conic with equation $xz - y^2 = 0$. We draw this as an ellipse tangent to the lines x=0 and z=0 along the line y=0. In lexicographic order the initial term is xz, corresponding to a limiting position that is the union of the lines x=0 and z=0. In reverse lexicographic order, on the other hand, the initial term of the equation is y^2, corresponding to the double line with reduced line y=0. We have added a picture of the stage in which the first deformation is merely approaching its limit.

Lexicographic deformation of conic

Start with the conic
$xz-y^2 = 0$.



Continue with the same deformation

Deform by weight vector 1, 0, 0

Deform by weight vector 0, 1, 0

Limit is two lines, x=0 and z=0.

Figure 15.5

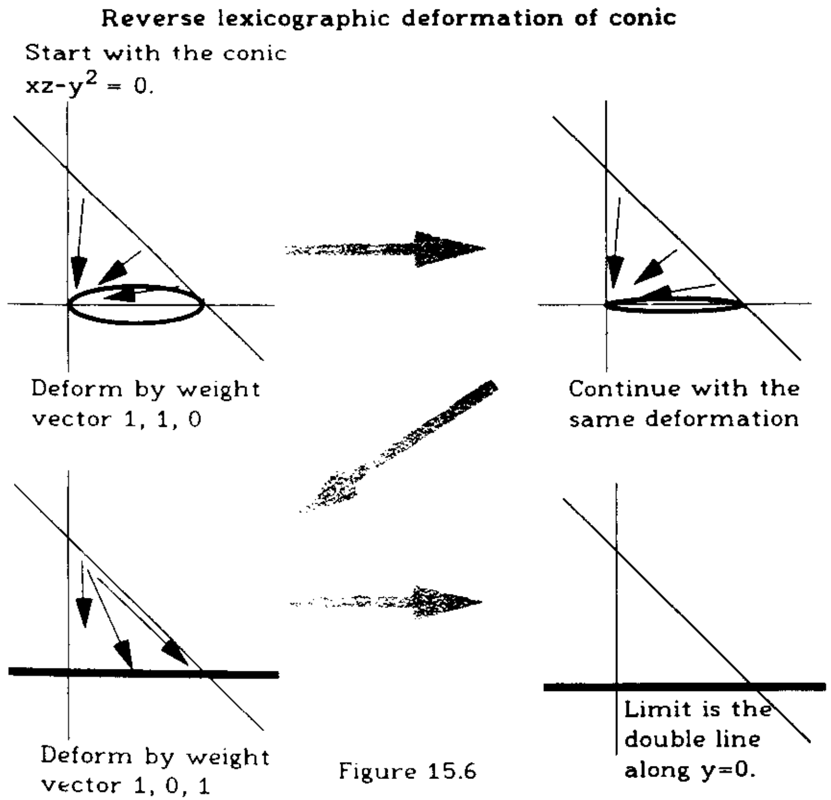

Reverse lexicographic deformation of conic
Start with the conic
xz-y^2 = 0.
Deform by weight vector 1, 1, 0
Continue with the same deformation
Deform by weight vector 1, 0, 1
Limit is the double line along y=0.

Figure 15.6

There is more to be seen in Figures 15.5 and 15.6. For example, as a conic undergoes the degeneration corresponding to one of the two orders, the dual conic (the set of its tangent lines) undergoes the other. This phenomenon is "visible" in the pictures; can the reader spot it?

Generic Initial Ideals

So far we have always considered Gröbner bases with respect to some fixed set of variables in a polynomial ring, and fixed set of generators of a free module. The results of Gröbner basis computations depend heavily

on the choice of variables and basis made. By allowing a generic change of basis and coordinates, we may eliminate this dependence, and we get a **generic initial ideal** that depends only on a choice of monomial order. Some of the properties of generic initial ideals were exploited by Hartshorne in his 1963 thesis to prove the connectedness of Hilbert schemes [1966]. We will prove stronger properties below; these sections should give the reader a good preparation for the algebraic part of Hartshorne's paper. Generic initial ideals were als considered by Grauert [1972] in the case of power series rings. He seems to have been the first to observe that the generic initial ideal is a combinatorial invariant that contains quite a lot of information. Generic initial ideals have also been exploited to bound the invariants of projective varieties (see Cook [****] and Braun-Fløystad [****]).

To get a sense of the information contained in the generic initial ideal, suppose $I \subset S$ is an ideal and we take reverse lexicographic order on S. In generic coordinates we can read off from in(I) the depth of S/I (= the largest t such that $x_{r-t+1}, \dots, x_r \notin$ in(I)) and the regularity of I (= the regularity of in(I); in characteristic 0 this is just the maximal degree of a minimal generator of in(I)), as well as things like the Hilbert function of S/I that we could read off from in(I) in any coordinate system. See Bayer-Stillman [1987b] for more information.

In this section we will explain the basic facts about generic initial ideals. The first treatment, in characteristic 0, is that of Galligo [1974]. The theory was done in arbitrary characteristic by Bayer-Stillman [1987a]. The combinatorial analysis and the properties of Borel-fixed ideals in characteristic p were worked out by Pardue [****], who has given a treatment covering many other group actions. We shall follow his treatment here, adapted to our special case. Although everything we do can be extended to the case of submodules of a graded free module with basis, we will stick for simplicity to the case of ideals.

Throughout this section we will work with a fixed monomial order > on $S = k[x_1, \dots, x_r]$ that refines the partial order by degree and that satisfies $x_1 > \dots > x_r$. We assume that the ground field k is infinite. All ideals considered will be homogeneous.

It is convenient to speak of taking initial ideals with respect to a given coordinate system and order, so instead of making a generic transformation of coordinates, we will transform an ideal by a generic linear transformation and take its initial ideal in the given coordinates.

We begin by establishing some notation for the groups of transformations that we will use. The general linear group $\mathcal{G} := GL(r,k)$ of invertible $r\times r$ matrices over k acts as a group of algebra automorphisms on S as follows: If $g \in \mathcal{G}$ then g acts on $\mathbf{A}^r$ as a linear transformation, and acts on the x_i, regarded as a basis for the space of linear functionals on $\mathbf{A}^r$, as $(g^{tr})^{-1}$, the inverse of the transpose of g. Explicitly, if $m = \Pi_i x_i^{a_i}$ and $(g^{tr})^{-1} = (h_{uv})$, then $gm = \Pi_i(\Sigma_v h_{ui}x_i)^{a_i}$.

Because we have distinguished an ordering of the variables, certain subgroups of $\mathcal{G}$ play an important role. Let $\mathcal{B}$ be the **Borel subgroup** of $\mathcal{G}$ consisting of upper triangular invertible matrices, and let $\mathcal{B}'$ be the group of invertible lower triangular matrices. Let $\mathcal{U} \subset \mathcal{B}$ be the **Unipotent subgroup** consisting of upper triangular matrices with ones on the diagonal. $\mathcal{U}$ is generated by the **elementary upper triangular matrices** γ^c_{ij} for $i < j$ and $c \in k$, where $\gamma^c_{ij}\, x_j = cx_i+x_j$ and $\gamma^c_{ij}\, x_u = x_u$ for $u \neq j$. Similarly, $\mathcal{B}'$ is generated by the diagonal matrices and the **elementary lower triangular matrices** $\gamma'_{ij}{}^c$ for $1 \leq i < j \leq r$ whose action is given by $\gamma'_{ij}{}^c\, x_i = x_i + cx_j$ and $\gamma'_{ij}{}^c\, x_u = x_u$ for $u \neq i$.

If $V \subset S_d$ is a t-dimensional space of forms of degree d, then we may represent V as a one-dimensional subspace $L = \wedge^t V \subset \wedge^t S_d$: If V has basis $f_1, \dots ,f_t$ then the subspace L is spanned by $f := f_1\wedge\dots\wedge f_t$. The reader unfamiliar with multilinear algebra will find more information in Appendix 2. We define a **monomial** of $\wedge^t S_d$ to be an element of the form $n = n_1\wedge\dots\wedge n_t$, where the n_i are degree d monomials of S. If the n_i are not distinct, then $n = 0$; in the contrary case the line kn determines and is determined by the finite set $\{n_1, \dots ,n_t\}$. We define a **term** in $\wedge^t S_d$ to be a product $a\cdot n$, where $a \in k$ and n is a monomial. We will say that $a\cdot n = a\cdot n_1\wedge\dots\wedge n_t$ is a **normal expression** if the n_i are ordered so that $n_1 > \dots > n_t$.

We order the monomials of $\wedge^t S_d$ by ordering their normal expressions lexicographically. That is, if $n = n_1\wedge\dots\wedge n_t$ and $n' = n'_1\wedge\dots\wedge n'_t$ are normal expressions, then $n > n'$ iff $n_i > n'_i$ for the smallest i such that $n_i \neq n'_i$. As usual, we extend the order to terms, and define the initial term of an element $f \in \wedge^t S_d$ to be the greatest term with respect to the given order.

Write m_i for $\mathrm{in}(f_i)$. We may replace the f_i by some linear combinations of themselves (without changing V) to ensure that the m_i are distinct and that $m_1 > \dots > m_t$. With this choice, $m_1\wedge \dots \wedge m_t$ is the normal expression for the initial term of f.

Existence of the generic initial ideal

Theorem 15.18: Let $I \subset S$ be a homogeneous ideal. There is a Zariski open set $U = \mathcal{B}'U \subset \mathcal{G}$, meeting $\mathcal{U}$ nontrivially, and a monomial ideal $J \subset S$ such that for all $g \in U$ we have $\mathrm{in}(gI) = J$. For each $d \geq 0$, if the degree d part J_d of J has dimension t, then $\wedge^t J_d$ is spanned by the greatest monomial of $\wedge^t S_d$ that appears in any $\wedge^t(gI_d)$ with $g \in \mathcal{G}$.

Definition: With I, J as in the Theorem, J is called the **generic initial ideal** of I, written $J = \mathrm{Gin}(I)$.

The significance of the assertion $U = \mathcal{B}'U$, is that all the action takes place in the coset space $\mathcal{B}' \setminus \mathcal{G}$. This is a much-studied object, which may be identified with the space of complete flags of linear subspaces of $\mathbf{A}^r$.

Proof: First consider the degree d part I_d of I. Let $f_1, \dots ,f_t$ be a basis for I_d. If $h = (h_{ij})$ is a matrix of indeterminates, then $h(f_1\wedge\dots\wedge f_t) = h(f_1)\wedge\dots\wedge h(f_t)$ is a linear combination of monomials of $\wedge^t S_d$ with coefficients that are polynomials in the h_{ij}. Suppose that $m = m_1\wedge\dots\wedge m_t$ is the earliest monomial that appears with a nonzero coefficient, and let $p_d(h_{11}, \dots ,h_{rr})$ be that coefficient. Let U_d be the set of $g = (g_{ij}) \in \mathcal{G}$ such that $p_d(g_{11}, \dots ,g_{rr}) \neq 0$. The degree d part of the initial ideal of gI will be $(m_1, \dots ,m_t)$ iff $g \in U_d$. Write J_d for the subspace of S_d spanned by $m_1, \dots ,m_t$.

We next show that $J := \oplus J_d$ is an ideal. It suffices to show for each d that $S_1 J_d \subset J_{d+1}$. Since U_d and U_{d+1} are open and dense, there is an element $g \in U_d \cap U_{d+1}$. We have $\mathrm{in}(gI)_d = J_d$ and $\mathrm{in}(gI)_{d+1} = J_{d+1}$, and the assertion follows.

The ideal J satisfies the last statement of the Theorem by definition, and we will show that $U = \cap_{d=1}^{\infty} U_d$ is Zariski open and dense in $\mathcal{G}$. Since each U_d is Zariski open and dense, it suffices to show that U is equal to a finite intersection of U_d's. Supposing that J is generated by forms of degree $\leq e$, we will show that in fact $U = \cap_{d=1}^{e} U_d$.

Suppose that $g \in \cap_{d=1}^{e} U_d$. We know that $\mathrm{in}(gI_d) = J_d$ for all $d \leq e$. Thus $\mathrm{in}(gI) \supset J$. Since $\dim_k J_d = \dim_k I_d = \dim_k (gI)_d$ for every d, we see that $\mathrm{in}(gI) = J$ as required.

We next show that $U = \mathcal{B}'U$. In fact, a little more is true:

Lemma 15 19: If $I_d \subset S_d$ is a subspace of dimension t and $b \in \mathcal{B}'$, then $\mathrm{in}(\wedge^t I_d) = \mathrm{in}(\wedge^t b I_d)$.

Proof: Since $\mathcal{B}'$ is generated by diagonal matrices and elementary lower triangular matrices, it suffices to check the assertion when b is of one of these types. Choose a basis $f_1, \dots, f_t$ for I_d and let $m_i = \mathrm{in}\, f_i$. Changing basis if necessary we may assume that $m_1 > \dots > m_t$. The diagonal matrices simply alter the coefficients of the terms of $f = f_1 \wedge \dots \wedge f_t$ by nonzero scalars, so the assertion is true if b is diagonal.

Next suppose that $b = \gamma'_{ij}{}^{c}$ is an elementary lower triangular matrix. For any monomial $n = x_i^{w} m \in S_d$, where m is not divisible by x_i, bn is n plus a linear combination of monomials of the form $n' = x_i^{w-s} x_j^{s} m$ with $0 < s \leq w$. Since $x_i > x_j$, we see that each $n' < n$. Thus $\mathrm{in}(bf_i) = m_i$ for $1 \leq i \leq t$, so $\mathrm{in}(bf) = m_1 \wedge \dots \wedge m_t = \mathrm{in}(f)$.//

To complete the proof of 15 18 we check that U meets the unipotent subgroup $\mathfrak{U}$ nontrivially. Since the U_d are Zariski open and $\mathfrak{U}$ is irreducible (it is an affine space), the intersection $U_d \cap \mathfrak{U}$ is Zariski open and dense in $\mathfrak{U}$ if it is nonempty. Since U is a finite intersection of U_d, it thus suffices to show that each U_d meets $\mathfrak{U}$ nontrivially. The set $\mathcal{B}'\mathfrak{U}$ is a dense open subset of $\mathcal{G}$; see Exercise 15 24 and its hint for a proof. Thus the dense set U contains an element of the form bu with $b \in \mathcal{B}'$ and $u \in \mathfrak{U}$. Since $U = \mathcal{B}'U$, it follows that $u = b^{-1}bu \in U$ as required. //

The generic initial ideal is Borel-fixed

The next result shows that generic initial ideals are quite special among monomial ideals. The description will be made explicit in Theorem 15 23.

Theorem 15 20 (Galligo, Bayer-Stillman): If $I \subset S$ is a homogeneous ideal then Gin(I) is Borel-fixed in the sense that for all $g \in \mathcal{B}$, $g(\mathrm{Gin}(I)) = \mathrm{Gin}(I)$.

Proof: Replacing I by gI for generic g, we may assume by Theorem 15 18 that $\mathrm{in}(I) = \mathrm{Gin}(I)$. Fix $i < j$, and let $\gamma_{ij}{}^{1} = 1+\gamma$ be an elementary upper triangular matrix, where γ is a strictly upper triangular matrix with a single nonzero entry. Along with diagonal matrices, such matrices generate the Borel group $\mathcal{B}$. Since the diagonal matrices stabilize any monomial ideal, it suffices to show that for each degree d we have $(1+\gamma)(\mathrm{in}(I_d)) = \mathrm{in}(I_d)$.

We may choose a basis $f_1, \dots, f_t$ for I_d with $\mathrm{in}(f_1) > \dots > \mathrm{in}(f_t)$. Let $f = f_1 \wedge \dots \wedge f_t$ be the corresponding generator of the one dimensional subspace $\wedge^t I_d \subset \wedge^t S_d$. We have $\mathrm{in}(f) = \mathrm{in}(f_1) \wedge \dots \wedge \mathrm{in}(f_t)$.

Write $\gamma\,\mathrm{in}(f) = a_0 m$, where a_0 is a nonzero scalar and m is a monomial of $\wedge^t S_d$. If $(1+\gamma)(\mathrm{in}(I_d)) \neq \mathrm{in}(I_d)$ then, since γ is strictly upper triangular, $m > \mathrm{in}(f)$. We shall show that for nearly all diagonal matrices δ the monomial m appears with nonzero coefficient in $(1+\gamma)\delta f$. This will contradict the last statement of Theorem 15 18, proving that $(1+\gamma)(\mathrm{in}(I_d)) = \mathrm{in}(I_d)$ after all.

For each term $n = a n_1 \wedge \dots \wedge n_t \in \wedge^t S_d$ we define the **weight of n to** be the monomial $w(x_1, \dots, x_r) = \prod_s n_i \in S$. Let $f_w \in \wedge^t S_d$ be the sum of all the terms of f having weight w, so that we have $f = \Sigma_w f_w$. Note that if w_0 is the weight of in(f), then $f_{w_0} = \mathrm{in}(f)$ is nonzero. If δ is a diagonal matrix and $\delta(x_i) = \delta_i x_i$ with $\delta_i \in k^*$, then

$$\delta f = \Sigma_w\ w(\delta_1,\dots,\delta_r)f_w.$$

Thus

$$\begin{aligned}(1+\gamma)\delta f &= \Sigma_w\ (1+\gamma)(w(\delta_1,\dots,\delta_r)f_w) \\ &= \Sigma_w\ w(\delta_1,\dots,\delta_r)\ (1+\gamma)f_w \\ &= w_0(\delta_1,\dots,\delta_r)\ \gamma\mathrm{in}(f) + w_0(\delta_1,\dots,\delta_r)\ \mathrm{in}(f) \\ &\qquad + \Sigma_{w\neq w_0}\ w(\delta_1,\dots,\delta_r)\ (1+\gamma)f_w.\end{aligned}$$

Since f_w is a sum of terms of weight w, the terms of γf_w have weight γw. Thus if we break the final sum above into terms of given weights, the term of weight γw_0 has the form

$$*)\qquad w_0(\delta_1,\dots,\delta_r)\ \gamma\mathrm{in}(f) + \Sigma_{w\neq w_0}\ w(\delta_1,\dots,\delta_r)\ \gamma f_w,$$

the sum extending over all those $w \neq w_0$ such that the weight of γf_w is γw_0. The coefficient of m in $(1+\gamma)\delta f$ is the same as the coefficient of m in *), and may be written as

$$**)\qquad a_0 w_0(\delta_1,\dots,\delta_r) \quad \Sigma_{w\neq w_0} a_w w(\delta_1,\dots,\delta_r).$$

where again the sum is over a certain collection of $w \neq w_0$. We may regard **) as a polynomial in $\delta_1,\dots,\delta_n$. Since the monomials in the δ_i that appear are distinct, and at least the term $a_0 w_0(\delta_1,\dots,\delta_r)$ is nonzero, we see that the polynomial is nonzero. It follows that for sufficiently general values of $\delta_1,\dots,\delta_n$, the value of the polynomial is nonzero, and this is what we had to prove.//

The nature of Borel-fixed ideals

We next investigate the nature of Borel-fixed ideals. If the characteristic of k is p, then it is useful to introduce a partial order $<_p$ on the natural numbers as follows: We say that $a <_p b$ if the binomial coefficient $\binom{b}{a} \not\equiv 0$ (mod p). Of course $<_0$ is the usual total order. For p >

0 it was described by Gauss:

Proposition 15 21 (Gauss): Suppose p is a prime number. We have $a <_p b$ iff each digit in the base p expansion of a is ≤ the corresponding digit in the base p expansion of b.

The proof is immediate from a more refined result of Lucas:

Lemma 15 22 (Lucas): If $a = \Sigma\, a_i p^i$ and $b = \Sigma b_i p^i$ with $0 \le a_i, b_i < p$, then $\binom{b}{a} \equiv \Pi_i \binom{b_i}{a_i}$ (mod p).

Proof: Compare the coefficients of t^a in the expressions

$$(t+1)^b = (t+1)^{\Sigma b_i p^i} = \Pi(t+1)^{b_i p^i}$$

$$\equiv \Pi(t^{p^i}+1)^{b_i} \quad (\mathrm{mod}\ p).\ //$$

We now give the combinatorial characterization of Borel-fixed ideals.

Theorem 15 23: Let $J \subset S = k[x_1, \dots, x_r]$ be an ideal, and let char k = p ≥ 0.

a) J is fixed by the group of diagonal matrices iff J is generated by monomials.

b) J is fixed by the group $\mathcal{B}$ of upper-triangular matrices (that is, J is **Borel-fixed**) iff J is generated by monomials and the following condition is satisfied for all i < j and all monomial generators m of J:

If m is divisible by $x_j{}^t$ but by no higher power of x_j,
then $(x_i/x_j)^s m \in J$ for all i < j and $s <_p t$.

Proof: a) Clearly any monomial ideal is fixed by the group of diagonal matrices. To prove the converse, let $f \in J$; it is enough to show that some monomial of f is in J. Choose a weight vector λ such that $\mathrm{in}_\lambda(f)$ is a monomial; that is, only one monomial of f has maximal weight with respect to λ. We will show that $\mathrm{in}_\lambda(f) \in J$.

Let w be the weight of the term $in_\lambda(f)$. If we act on f with a diagonal matrix g_c having diagonal terms $(c^{-\lambda_1}, \dots, c^{-\lambda_r})$, we replace each variable x_i by $c^{-\lambda_i} x_i$, so $in_\lambda(f)$ is multiplied by c^{-w}, and the other terms of f are multiplied by strictly less negative powers of c. Thus we may write $c^w g_c f = in_\lambda(f) + c\, F(c,x)$ for some polynomial $F(c,x)$. Consider the morphism $\varphi\colon \mathbf{A}^1_k \to S$ defined by $\varphi(c) = c^w g_c f = in_\lambda(f) + cF(c,x)$. Since For $c \neq 0$ the matrix g_c is invertible. Since J is fixed under the group of diagonal matrices, $\varphi(c) \in J$ for $c \neq 0$. Since J is a Zariski closed subset, in fact a linear subspace, this implies that $\varphi(c) \in J$ for all c. (The fact that S is infinite dimensional is not a problem: if J is the common zero locus of a set of linear functions $\alpha_i\colon S \to k$, then composing the α_i with φ we get polynomial functions from $\mathbf{A}^1_k$ to k that vanish simultaneously on precisely those c for which $\varphi(c) \in J$. Since these polynomials vanish for all nonzero c, they vanish for all c.)

b) If J is Borel-fixed then, by a), J is generated by monomials. If $m \in J$ is a monomial generator, we consider the action on m of an elementary upper triangular matrix $\gamma = \gamma_{ij}{}^c$, with $0 \neq c \in k$. We may write $m = x_j{}^t m'$, where m' is not divisible by x_j, and we get

$$\gamma m = (cx_i+x_j)^t m' = \Sigma_{s<_p t} \left(\begin{smallmatrix} t \\ s \end{smallmatrix}\right) c^s (x_i/x_j)^s m.$$

Since J is fixed under $\gamma = \gamma_{ij}{}^c$, we see that each $(x_i/x_j)^s m$ with $s <_p t$ is a monomial belonging to some polynomial in J. Being a monomial ideal, J contains all the monomials that appear in polynomials from J, and J thus contains the monomial $(x_i/x_j)^s m$ as required.

Conversely, suppose J is a monomial ideal satisfying the condition in b). The formula above shows that for every monomial generator of J the polynomial γm is a sum of monomials in J. Since J is generated by monomials, $\gamma J = J$. Since the group of upper triangular matrices is generated by diagonal matrices and matrices $\gamma_{ij}{}^c$, we are done. //

A few examples will clarify the Theorem. For simplicity we take only examples with all generators in a single degree. First in characteristic 0: In 2 variables the Borel fixed ideals are precisely the ideals generated by "initial segments of the monomials" in each degree, such as $(x_1{}^3, x_1{}^2x_2, x_1x_2{}^2)$. But already in 3 variables there are more possibilities. For example the ideals

$$(x_1{}^3, x_1{}^2x_2, x_1x_2{}^2)$$

and

$$(x_1{}^3, x_1{}^2x_2, x_1{}^2x_3)$$

are both Borel-fixed in any characteristic. In characteristic $p > 0$ any ideal of the form $(x_1{}^{p^e}, \dots, x_u{}^{p^e})$ is Borel-fixed. Products, intersections, sums, and quotients of Borel-fixed ideals are Borel-fixed, so it is easy to make further examples.

To exploit the results on generic initial ideals we use the following fundamental property of Borel-fixed ideals:

Proposition 15 24 (Bayer-Stillman): Suppose that $I \subset S = k[x_1, \dots, x_r]$ is a Borel-fixed ideal. For any $j = 1, \dots, r$ we have

$$(I : x_j{}^\infty) = (I : (x_1, \dots, x_j)^\infty).$$

If char $k = 0$, then in addition

$$(I : x_j{}^s) = (I : (x_1, \dots, x_j)^s)$$

for every $s \geq 0$.

Proof: Suppose that for some integer s and some monomial m we have $x_j{}^s m \in I$. For the first statement it suffices to show that if $1 \leq i < j$ then for some $s' \geq s$ we have $x_i{}^{s'} m \in I$. For if s is sufficiently large, then

$$(I : x_j{}^\infty) = (I : x_j{}^s)$$

$$\subset (I : (x_1{}^{s'}, \dots, x_j{}^{s'}) \subset (I : (x_1, \dots, x_j)^{js'}) \subset (I : (x_1, \dots, x_j)^\infty);$$

and the reverse inclusion is obvious.

Increasing s if necessary we may assume that x_j does not divide m. If char k = p > 0 and we choose e so that $s' = p^e \geq s$, then $x_j^{s'}m \in I$, and it follows from the condition of Theorem 15 23 that $x_i^{s'}m \in I$ as required.

Suppose now that char k = 0. If $x_j^s m \in I$ then by the characterization of Theorem 15 23, any monomial $n = x_1^{s_1} \ldots x_j^{s_j}$ with $\Sigma_u s_u = s$ satisfies $nm \in I$, so $(I : x_j^s) \subset (I : (x_1, \ldots ,x_j)^s)$. Again, the reverse inclusion is obvious.//

Corollary 15 25: If I is a Borel-fixed ideal in S, and P is an associated prime of I, then $P = (x_1, \ldots , x_j)$ for some j. If $Q = (x_1,\ldots,x_t)$ is a maximal associated prime, then $x_{t+1},\ldots,x_r$ (in any order) is a maximal S/I-regular sequence in $(x_1, \ldots , x_r)$.

Proof: Since I is a monomial ideal, every associated prime of I is generated by a set of variables. Suppose that j is the largest index such that $x_j \in P$; we must show that $x_i \in P$ for $i < j$. Since P is an associated prime we may write $P = (I : f)$ for some polynomial f. Since $x_j f \in I$ it follows from Proposition 15 24 that $x_i^s f \in I$ for some s. Thus $x_i^s \in P$, so $x_i \in P$ as required.

If $Q = (x_1,\ldots,x_t)$ is a maximal associated prime, then the variables $x_{t+1},\ldots,x_r$ cannot appear in the minimal generators of I. Thus $x_{t+1},\ldots,x_r$ (in any order) is a regular sequence modulo I. Since Q is associated to I there is a monomial $m \notin I$ such that $Qm \subset I$. Since the generators of I do not involve $x_{t+1},\ldots,x_r$, we may factor these variable out of m, and assume that $m \notin I + (x_{t+1},\ldots,x_r)$. It follow that $Q+(x_{t+1},\ldots,x_r) = (x_1, \ldots , x_r)$ is associated to $I + (x_{t+1},\ldots,x_r)$, so $x_{t+1},\ldots,x_r$ is a maximal S/I-regular sequence in $(x_1, \ldots , x_r)$. //

For an analysis of these ideas and a different proof of Corollary 15 25 see Exercise 15 22 and Exercise 15 23.

Applications

We now apply these methods to the problems mentioned at the beginning of this section.

1) Ideal membership : Given generators for an ideal $I \subset S$, determine a vector space basis for S/I, and given a polynomial f, compute its image in S/I in terms of this basis. If $f \in I$ (that is, if the image is 0) compute an expression for f as a linear combination of the generators of I.

This problem is solved by Theorem 15 3 and the division algorithm: Choose a monomial order on S, and from the original generators $f_1, \dots, f_s$ of I, compute a Gröbner basis $g_1, \dots, g_t$ for I. The set of monomials not in $\text{in}(I)$, that is, not divisible by any one of the $\text{in}(g_i)$, is a basis for S/I. The remainder of any $f \in S$ on division by $g_1, \dots, g_t$ has no monomials in $\text{in}(I)$ and is thus the unique expression for the image of f in terms of this basis.

If $f \in I$, then the division process exhibits f as a linear combination of the generators g_i. Since the algorithm that produces the g_i exhibits them as linear combinations of the original f_j, we are done.

For a generalization and a more formal treatment of the second part, see application 8), below.

2) Hilbert Function and Polynomial: Following Hilbert, we could deduce the Hilbert function or polynomial of a graded module from a graded free resolution for the module, computed with the algorithms above. However, this is extremely inefficient, and better schemes are based on the following fundamental result of Macaulay (1927). This theorem was the reason for Macaulay's introduction of monomial orders, and is thus historically at the very root of the material in this chapter.

Theorem 15 26 : Let P be a finitely generated graded S-module, given by generators and relations as $P = F/M$, where F is a free module with a homogeneous basis and M is a submodule generated by homogeneous elements. The Hilbert function of P is the same as the Hilbert function of $F/\text{in}(M)$.

Proof: Let B be the set of monomials not in $\text{in}(M)$. Write F_d for the set of elements of degree d of F, and similarly for M, P, and B. Because P is graded, we have $P = \oplus_d P_d$, where $P_d = F_d/M_d$.

By Theorem 15 3, B maps to a (vector space) basis for P, so B_d maps to a basis for P_d. Thus $\dim_k P_d$ is the number of elements of B_d. Since the argument applies as well to $P' = F/\text{in}(M)$, we are done. //

Theorem 15 26 shows that to compute the Hilbert function of an arbitrary module, it is enough to compute the Hilbert function of the quotient of a free module by a monomial submodule, and this we have already done in the section on monomials, above.

Macaulay's original application of Theorem 15 26 was to give a characterization of all possible Hilbert functions of ideals: By virtue of the Theorem, it is enough to characterize the Hilbert functions of monomial ideals, and this leads to a complex but manageable combinatorial problem.

3) Associated Graded ring

Let $R = S/I$, and set $\mathfrak{m} = (x_1, \dots, x_r)$. The associated graded ring $\text{gr}_{\mathfrak{m}} R$ of R with respect to $\mathfrak{m}$ is significant geometrically, algebraically, and computationally: The geometric and algebraic significance has been explained in Chapter 4; its main computational significance comes from the fact that its Hilbert function is the same as that of R, and is easier to compute, for instance by the method above. To understand $\text{gr}_{\mathfrak{m}} R$ we must find a presentation of the form $\text{gr}_{\mathfrak{m}} R = S/I'$, where I' is the homogeneous ideal consisting of the sum f_{bottom} of the monomials of lowest degree from each polynomial f in I. Our goal is thus to produce finitely many elements g_i of I such that I' is generated by the forms $g_{i,\mathrm{bottom}}$. Interestingly, in order to do this we need only compute Gröbner bases of homogeneous ideals! A similar idea will suffice to compute the associated graded module of any S-module with respect to $\mathfrak{m}$; see Exercise 15 36. Of course we could also ask for the associated graded ring of R (or any S-module) with respect to an arbitrary ideal I. This can be done by using elimination theory; see Exercise 15 38.

Choose any set of generators $f_1, \dots, f_s$ of I, and for each i let F_i be the **homogenization** of f_i with respect to a new variable x_0, that is,

$$F_i(x_0, x_1, \dots, x_r) = x_0^{\deg f_i}\, f_i(x_1/x_0, \dots, x_r/x_0).$$

Proposition 15 28: With notation as above, let $(G_1, \dots, G_t)$ be a Gröbner basis of the ideal $(F_1, \dots, F_s)$ with respect to any monomial order on $S[x_0]$ that refines the partial order by degree in x_0. If we set $G_i(1, x_1, \dots, x_r) = g_i(x_1, \dots, x_r) \in S$, then $I' = (g_{1\ \mathrm{bottom}}, \dots, g_{t\ \mathrm{bottom}})$.

Proof: Suppose $g \in I$; we must show that g_{bottom} is a linear combination of the $g_{i\ \mathrm{bottom}}$. Write $g = \Sigma\, p_i f_i$. If G, P_i, and F_i are the homogenizations of g, p_i, and f_i respectively then for some integers a,b we have

$$x_0^a\, G = \Sigma\, P_i F_i \in (F_1, \dots, F_s)$$

$$x_0^a\, G = x_0^b g_{\mathrm{bottom}} + (\text{terms of lower degree in } x_0).$$

Because the G_i form a Gröbner basis for $(F_1, \dots, F_s)$, there is a standard expression

$$x_0^a\, G = \Sigma\, Q_i G_i\,, \quad \mathrm{in}(Q_i G_i) \le \mathrm{in}(x_0^a\, G).$$

In particular, the degree in x_0 of $Q_i G_i$ is $\le$ b for each i.

It follows that $x_0^b g_{\mathrm{bottom}}$ is the sum of the products of the terms of highest degree in x_0 in Q_i and G_i. Setting $x_0 = 1$, we see that g_{bottom} itself is the sum of the products of the terms of lowest degree in $Q_i(1, x_1, \dots, x_r)$ and $G_i(1, x_1, \dots, x_r)$; that is, it is a linear combination of the $g_{i\ \mathrm{bottom}}$, as claimed. //

4) Elimination

Given an ideal $I \subset S[y_1, \dots, y_s]$, we wish to compute $J = I \cap S$. The name elimination comes from thinking of the generators of I as a system of equations in x_i and y_j from which one wants to eliminate the variables y_j.

Elimination was a popular topic in the nineteenth century, partly because of its relation to the problem of solving equations. We have already discussed a part of Elimination Theory in Chapter 14.

To do elimination using Gröbner bases, one uses an order on T = $k[x_1, \dots, x_r, y_1, \dots, y_s]$ satisfying:

If $f \in T$ and $\mathrm{in}(f) \in S$, then $f \in S$.

An order with this property is called an **elimination order (with respect to $y_1, \dots, y_s$).**

Examples: 1) The simplest way to make an elimination order is to take the partial order by total degree in $y_1, \dots, y_s$, refined by any monomial order; in practice it is often most efficient to take reverse lexicographic order as the second order.

2) Lexicographic order is an elimination order with respect to every initial subset of the variables.

To find $J = S \cap I$ we need only compute a Gröbner basis with respect to an order satisfying E:

Proposition 15 29: Let > be a monomial order on $T = S[y_1, \dots, y_s] =$

$k[x_1, \dots, x_r, y_1, \dots, y_s]$, and suppose that $>$ has property E with respect to the variables $y_1, \dots, y_s$. If $I \subset T$ is an ideal, then with respect to the monomial order on S gotten by restricting the given one from T, we have

$$\mathrm{in}(I \cap S) = \mathrm{in}(I) \cap S.$$

Further, if $g_1, \dots, g_t$ is a Gröbner basis for I, and $g_1, \dots, g_u$ are those g_i that do not involve the variables y_i, then $g_1, \dots, g_u$ is a Gröbner basis in S for $I \cap S$.

Proof: Let $J = I \cap S$ Clearly $\mathrm{in}(J) \subset \mathrm{in}(I) \cap S$. We will show that the $\mathrm{in}(g_i)$ for $i \le u$ generate $\mathrm{in}(I) \cap S$. By Lemma 15 5, this will prove both statements.

Suppose $m \in \mathrm{in}(I) \cap S$. Since $g_1, \dots, g_t$ form a Gröbner basis, m is a multiple of $\mathrm{in}(g_i)$ for some $i \le t$. Because $m \in S$, we must have $\mathrm{in}(g_i) \in S$, so $g_i \in S$ by property E, whence $i \le u$ as required. //

There is an analogue of Proposition 15 29 for submodules of a free module; if $M \subset F := \oplus Te_i$, then it gives us a way to construct $M \cap \oplus Se_i$. See Exercise 15 37.

One of the most frequent applications of elimination is solving the following problem:

Find the equations satisfied by given elements of an affine ring. (Geometrically: find the closure of the image of a variety under an arbitrary map.)

Let $R = k[y_1, \dots, y_s]/K$ for some ideal K, and let $f_1, \dots, f_r$ be elements of R. Define a map

$$\varphi: S = k[x_1, \dots, x_r] \to R; \quad x_i \mapsto f_i.$$

We wish to find ker φ. Geometrically, this is the ideal defining the Zariski

closure of the image of algebraic set corresponding to K under the map corresponding to $f_1, \dots, f_r$.

To this end, set $Q = k[y_1, \dots, y_s]$, and consider the ring $T = k[x_1, \dots, x_r, y_1, \dots, y_s]$. For each i, let $F_i \in Q$ be a polynomial that maps to $f_i \in R$. Regarding the F_i as elements of T, let $I \subset T$ be the ideal

$$I = KT + (F_1 - x_1, \dots, F_r - x_r).$$

Proposition 15 30: $\ker \varphi = I \cap S$.

Proof: Consider the map φ: $T \to Q$ sending $x_i \mapsto F_i$. The ideal $J := (F_1 - x_1, \dots, F_r - x_r)$ is obviously contained in ker φ. We claim that $J = \ker \varphi$. Indeed, it is clear that $J \subset \ker \varphi$, and the reverse inclusion follows because each x_i is equal to a polynomial in the y_j modulo J.

It follows that the kernel of the composite map $T \to Q \to R$ is I, so the kernel of the composite $S \hookrightarrow T \to Q \to R$ is $S \cap I$, as claimed. //

If K and the f_i are homogeneous, then ker φ will be a homogeneous ideal too if we take the variables x_i to have the same degrees as the f_i. If, for example, all the f_i were of the same degree. then we could afterwards change gradings to give the x_i all degree 1, and the ideal ker φ would remain homogeneous. In this case we are computing the equations for the projective variety that is the image of V(K) under the map corresponding to φ -- in this case the image is already closed, by the "Main Theorem of Elimination Theory", Theorem 14.1.

5) Projective closure and ideal at infinity

Given an algebraic set $V \subset \mathbb{A}^r$, we wish to compute the ideal I' of the closure $\overline{V}$ of V in $\mathbb{P}^s \times \mathbb{A}^{r-s}$ and the ideal I_∞ of the intersection of $\overline{V}$ with the "**hyperplane at infinity** " $\mathbb{P}^{s-1} \times \mathbb{A}^{r-s} \subset \mathbb{P}^s \times \mathbb{A}^{r-s}$.

To describe them, it is convenient to introduc the term **s-degree** to denote the degree of a polynomial with respect to the first s variables of the polynomial ring S. The **s-homogenization** of a polynomial $g(x_1, \dots, x_r)$ of s-degree d, with respect to a new variable x_0, is then defined as

$$g'(x_0, x_1, \dots, x_r) := x_0{}^d g(x_1/x_0, \dots, x_s/x_0, x_{s+1}, \dots, x_r).$$

Less formally, p' is the sum of the terms of p, each multiplied by a power of x_0 to bring it up to s-degree d.

If $f \in S[x_0] = k[x_0, x_1, \dots, x_r]$ is a form homogeneous with respect to $x_0, \dots, x_s$, and $W \subset \mathbb{P}^s \times \mathbb{A}^{r-s}$ is the corresponding hypersurface, then $W \cap (\mathbb{A}^s \times \mathbb{A}^{r-s}) = W \cap \mathbb{A}^r$ is defined by the equation $f(1, x_1, \dots, x_r) = 0$. It follows easily that I' is the set of elements in the preimage of I under the map

$$\varphi\colon\ S[x_0] \to S\ ;\quad x_0 \mapsto 1$$

that are homogeneous in the variables $x_0, \dots, x_s$. Equivalently, I' is the ideal generated by the s-homogenizations g' of all the elements $g \in I$. From this second description and the fact that the hyperplane at infinity has equation $x_0 = 0$, we see that we may write $I_\infty = \{g_\infty \mid g \in I\}$, where g_∞ denotes the sum of all those terms of g with maximal s-degree.

The problem is that these description of I' and I_∞ involve infinitely many polynomials. (It is easy to show that if $\{h_i\} \subset I$ is any set of elements such that the set $(\{h_i\}_\infty)$ generates I_∞, then I' is generated by the set of s-homogenizations of the h_i, but this still does not solve the problem.) The following result shows how to compute both I' and I_∞ in finite terms, using Gröbner bases:

Proposition 15.31: With notation as above, suppose that > is a monomial order on S refining the order by degree in $x_1, \dots, x_s$. If $g_1, \dots, g_t$ is a Gröbner basis of I with respect to >, then

a) $\mathrm{in}(I_\infty) = \mathrm{in}(I)$ and $\{(g_1)_\infty, \dots, (g_t)_\infty\}$ is a Gröbner basis for I_∞.

b) $\mathrm{in}(I') = \mathrm{in}(I)$ and $\{g'_1, \dots, g'_t\}$ is a Gröbner basis of I'.

Proof: a) We have $\mathrm{in}(g_\infty) = \mathrm{in}(g)$ for any $g \in S$ by our choice of order. It follows that $\mathrm{in}(I_\infty) = \mathrm{in}(I')$ and this ideal is generated by the $\mathrm{in}(g'_i) = \mathrm{in}(g_i)$.

b) Again, we have $\mathrm{in}(g') = \mathrm{in}(g)$ for any $g \in S$ by our choice of order. As in part a) it follows that $\mathrm{in}(I') = \mathrm{in}(I)$ and this ideal is generated by the $\mathrm{in}(g'_i) = \mathrm{in}(g_i)$.//

6) Saturation

If M is a submodule of a free S-module F and J is an ideal of S, we define

$$(M : J) = \{\, f \in F \mid fJ \subset M \,\} \subset F$$

$$(\, M : J^\infty\,) = \cup_{d=1}^{\infty}\ (M : J^d) \subset F.$$

The submodule $(\, M : J^\infty\,)$ is called the **saturation of M with respect to J**. Saturations arise in the theory of primary decomposition and in local cohomology theory, both of which will be treated in later chapters. They can also be used for finding projective closures -- see Exercise 15.40.

In the section on applications of syzygies, we will see that we can compute $(M : J^d\,)$. We could compute these one at a time, increasing d until we obtained $(I : J^d) = (I : J^{d+1})$ (which must happen eventually because S is Noetherian). For this value of d we have $(I : J^\infty) = (I : J^d)$, and this is a rather practical method in many cases. However, part a) of Exercise 15.41, with $d = \infty$, shows that if J is the ideal generated by a single variable, then the problem can be solved using a single Gröbner basis computation with respect to a suitable order. The general case can easily be reduced to the special case, using the other ideas in Exercise 15 41.

7) Lifting homomorphisms

The following generalization of the ideal membership problem is central to many constructions involving maps of modules and homological algebra. The application to the kernels of maps of modules below is an example.

Let F, G, and H be free S-modules with basis, and suppose we are given maps

$$\begin{tikzcd} & G \arrow[d, "\gamma"'] \\ H \arrow[r, "\varphi"] & F \end{tikzcd}$$

such that im $\gamma \subset$ im φ. We would like to construct a "lift" $\psi: G \to H$ such that $\varphi\psi = \gamma$.

To this end, we choose a monomial order on F. Write $g_1, \ldots, g_s$ for the images under φ of the basis vectors of H. Using Buchberger's algorithm, we may find a Gröbner basis $h_1, \ldots, h_t$ for im φ. Let

$$\varphi': \; H' = \oplus Se_i \to F; \qquad e_i \mapsto h_i$$

be the corresponding map. Buchberger's algorithm produces at the same time an expression for each h_i in terms of the g_j; that is, a "change of basis map" $\alpha: H' \to H$ such that $\varphi' = \varphi\alpha$. For each basis vector $\varepsilon_i \in G$, we use the division algorithm to find an expression $\gamma(\varepsilon_i) = \Sigma\, p_i h_i$. We may define a map

$$\psi': G \to H' ; \qquad \varepsilon_i \mapsto \Sigma\, p_i e_i,$$

so that $\varphi'\psi' = \gamma$ (see Figure 15.7). It follows that $\psi = \alpha\psi'$ is the desired lifting.

$$\begin{tikzcd} & G \arrow[dl, "\psi'"'] \arrow[dd, "\gamma"] \arrow[ddl, bend right=70, "\psi"'] \\ H' \arrow[d, "\alpha"'] \arrow[dr, "\varphi'"] & \\ H \arrow[r, "\varphi"] & F \end{tikzcd}$$

Figure 15.7

8) Syzygies and constructive module theory

A module may be determined in many ways by giving its properties. By contrast, we will say that we have **constructed** a module P only if we can give generators and relations for it -- that is, if we can write it as F/M where F is a free module and M is a submodule generated by explicitly given elements of F, or equivalently as the cokernel of a map $\varphi: G \to F$ of free modules with image M. Since we can compute ker φ, we may also regard the submodule M as having been constructed. If we have constructed a module P = F/M, and have specified a submodule $P' \subset P$ by giving a set of generators for it as the images of given elements of F then it is clear that we can construct the quotient P/P'; we simply adjoin the new elements of F to the list of relations for P. It is not quite so obvious that we can find the relations for the submodule P', but this will follow from the pullback construction below (Exercise 15 45). In the remainder of this section we will make a few of the central operations on modules constructive in this sense. The list here could be prolonged very greatly.

a) Pullbacks, intersections, annihilators

If $\varphi: G \to F$ and $\psi: H \to F$ are maps of free modules, it is often useful to find the "pullback" of φ and ψ, by which we mean the submodule of $G \oplus H$ consisting of elements (g,h) such that $\varphi(g) = \psi(h)$. We construct this pullback as the kernel of $(\varphi, -\psi): G \oplus H \to F$. Since we are able to compute syzygies, we can find a free module PB mapping onto the kernel -- that is, we can find a set of generators for the pullback. We will often need the projection to one of the factors; we will write $\pi_G : PB \to G$ and π_H: $PB \to H$ for the compositions of $PB \to G\oplus H$ with the projections. We get a commutative diagram

$$\begin{tikzcd}
PB \arrow[r, "\pi_G"] \arrow[d, "\pi_H"'] & G \arrow[d, "\varphi"] \\
H \arrow[r, "\psi"'] & F
\end{tikzcd}$$

This gives us a way to compute the intersection of two submodules of F, the images of φ and ψ say: The intersection is simply the image of $\varphi\, \pi_G = \psi\, \pi_H$. See Exercise 15 42 for another construction of intersections, and Exercise 15 45, Exercise 15 46 for further uses of pullbacks.

b) The kernel of a map between arbitrary modules

Given S-modules P and Q by means of free presentations

$$G_P \xrightarrow{\kappa_P} F_P \to P \to 0$$

$$G_Q \xrightarrow{\kappa_Q} F_Q \to Q \to 0,$$

and given a homomorphism $P \to Q$ presented as a map φ: $F_P \to F_Q$ taking the image of G_P into the image of G_Q, we may construct the kernel of the map induced by φ as follows:

Proposition 15 32: With notation as above, let F_K be a free module mapping onto the pullback of κ_Q, φ, and let ψ: $F_K \to F_P$ be the composite

$$F_K \to G_Q\oplus F_P \to F_P.$$

Let κ_K': $G \to F_K$ be a map onto the kernel of ψ. Let φ_1: $G_P \to G_Q$ be a map lifting the map $\varphi\kappa_P$ along κ_Q and let κ_K'': $G_P \to F_K$ be a lifting of the map $(-\varphi_1, \kappa_P)$: $G_P \to G_Q\oplus F_P$, which maps into the kernel of $(-\kappa_Q, \varphi)$. Then

$$\pi_K = (\kappa_K', \kappa_K'') : G_P \oplus G \to F_K \to K \to 0$$

is a free presentation of the kernel of $P \to Q$, and the injection $K \subset P$ is defined by the map ψ_K.

We leave the proof to the reader (Exercise 15 41).

c) Hom, Ext, Tor, and all that

Much can be computed by putting together what we have already done. We give only some hints, and leave the working out of these constructions to the reader with sufficient background.

If P and Q are S-modules given by free presentations as in a) above, then

$$\mathrm{Hom}_S(P,Q) = \ker\,(\mathrm{Hom}\,(F_P,Q) \to \mathrm{Hom}(G_P, Q)\,),$$

while $\mathrm{Hom}(F_P,Q)$ is a module with free presentation

$$\mathrm{Hom}(F_P, G_Q) \to \mathrm{Hom}(F_P, F_Q) \to \mathrm{Hom}(F_P,Q) \to 0,$$

and similarly for $\mathrm{Hom}(G_P,Q)$.

Once we can compute free resolutions, Hom, and kernels, Ext is easy; and the same is true for Tor if we can compute tensor products. But tensor products are elementary (that is, one doesn't need to solve equations) because, for example, the tensor product of P and Q is presented as

$$F_P \otimes G_Q \oplus F_Q \otimes G_P \to F_P \otimes F_Q \to P \otimes Q \to 0,$$

by the right exactness of tensor products.

Multiplicities (in the sense of Samuel or Serre) can be computed from computations of Tor; those in the sense of Vogel can also be found, using the computation of saturations.

The cohomology of coherent sheaves can be handled from this using either duality theory or directly, since the usual expression for the cohomology as the limit of certain Ext groups actually converges, in each degree, in a predictable, finite number of steps. More generally, local cohomology can be approximated. The interested reader may find details of these and other constructions in Vasconcelos [****].

What's left?

Many further things can be done with Gröbner bases well enough to have been implemented on computers, for example in the program **Macaulay** . In this category fall for example

- Finding syzygies over factor rings

- Computing the radical of an ideal.

Other algorithms are known, but not implemented for various reasons. A few examples from many:

- Primary Decomposition (the first algorithm was by Grete Hermann, a student of Emmy Noether [1926]; for recent work see Seidenberg [1984], Gianni-Trager-Zacharias [1988], and Eisenbud-Huneke-Vasconcelos [1992].

- Normalization of a ring (this was studied by Seidenberg [1974]; for recent work see Vasconcelos [1992])

- Flattening stratifications

There are also plenty of problems where no algorithms are known as of this writing. Again a few examples:

- Decide whether a module can be written as a direct sum of submodules nontrivially; if so, decompose it. For example, decide whether a projective module is free.

- Decide whether two varieties are in the same component of the Hilbert scheme.

- Compute the versal deformation of a factor ri ig S/I in the case that this is finite dimensional.

- Decide the growth rate of the (infinite) free resolution of a module over a factor ring of S.

- Given generators for an ideal, decide whether a smaller number of generators can generate an ideal with the same radical; in particular, decide whether an algebraic variety is a "set theoretic complete intersection" -- that is, set theoretically the intersection of c hypersurfaces, where c is the codimension. The leading open case is perhaps the ideal of the rational quartic curve in $\mathbb{P}^3$

$$(x_2^3 - x_1x_3^2,\ x_1x_2 - x_0x_3,\ x_1^3 - x_0^2x_2,\ x_0x_2^2 - x_1^2x_3) \subset k[x_0, \dots, x_3],$$

which is the kernel of the map

$$\begin{aligned} &k[x_0, \dots, x_3] \to k[s,t] \\ &x_0 \mapsto s^4 \\ &x_1 \mapsto s^3t \\ &x_2 \mapsto st^3 \\ &x_3 \mapsto t^4. \end{aligned}$$

It is known that if the characteristic of k is positive hen this ideal has the same radical as an ideal generated by 2 elements (the elements depend on the characteristic). It is not known whether this is true in characteristic 0. See Jaffe [1989] for recent results and an exposition.

History

The earliest use of what amounts to the existence of Gröbner bases may be that of P. Gordan [1900, pp 141-156]. Gordan uses Gröbner bases ("le systeme irreducible N" on page 152 is one) and the finite generation of monomial ideals to deduce Hilbert's Basis Theorem, just as in Exercise 15 15, below.

A major step towards the theory presented in this chapter was taken by F. S. Macaulay, who introduced total orderings of the set of monomials of a ring in [1927] and used them to characterize the possible Hilbert functions of graded ideals by comparing them with monomial ideals.

W. Gröbner published applications of Macaulay's idea of ordering monomials and explicitly finding a basis for a zero-dimensional factor ring as early as [1939], though his use of them apparently goes back even earlier, perhaps to 1932. In a paper on elimination theory [1950] he writes, "Ich habe diese Methode seit etwa 17 Jahren in den verschiedensten, auch komplizierten Fällen verwendet und erprobt and glaube auf Grund meiner Erfahrungen sagen zu können, dass sie tatsächlich in allen Fällen ein brauchbares und wertvolles Werkzeug zur Lösung von diesen und ähnlichen idealtheoretischen Aufgaben darstellt." ("I have used and tested these methods for about 17 years in the most varied and sometimes complicated cases, and I believe that I can say on the basis of my experience that they represent in all cases a useful and worthwhile tool for the solution of these and similar ideal-theoretic problems.") In 1964 he posed to his student B. Buchberger the problem of computing such bases as a thesis problem. As was also his practice in some other cases, he apparently did not mention to Buchberger that he already had a solution of the problem! It was not until 1984 that Buchberger learned the early part of the story (see Buchberger [1987] for this and related history).

As Gröbner must have hoped, Buchberger's solution to his thesis problem contained ideas going beyond what Gröbner had himself known. The thesis [1965; University of Innsbruck] contained Buchberger's Criterion and Algorithm (our 15 8 and 15 9) in implicit form. The essential added ingredient was the notion of critical pairs. Buchberger made his ideas more explicit and usable in his papers [1970] and [1976].

There were several independent streams of activity that produced closely related methods and algorithms. H. Hironaka used a division algorithm closely related to the one we have presented in his landmark paper on resolution of singularities [1964]. He introduced "standard bases", which are analogous to what we have called Gröbner bases, following a now more common usage. It is worth noting that Hironaka's work was done for power series (with questions of convergence treated) -- in some ways a deeper form of the division algorithm than the one treated here; he thought of it as generalizing the classical Weierstrass preparation and division theorems for convergent power series in one variable.

H. Grauert independently introduced "standard bases" and a division algorithm in power series rings in his [1972], applying them to the construction of versal deformation spaces. Grauert also studied in this paper the effect of a general change of coordinates.

G. Bergman studied a more general version of Gröbner bases, aimed at associative (noncommutative) algebras and still more general algebraic systems in his paper [1978 especially sect. 10.3]. Bergman's ideas specialize to Buchberger's Algorithm in the commutative case. He remarked that the ideas had already been used -- and called "obvious" -- by P. M. Cohn [1966] and others. Other sources for the noncommutative theory include Priddy [1970] and Knuth-Bendix [1967].

D. A. Spear [1977] and F.-O. Schreyer [1980] seem to be the first to have written down a method for the computation of syzygies by means of the division algorithm. (Spear's work, written as a report on a package he was developing for Macsyma, contains no mathematical details.) The

formulation of Theorem 15 10 and the proof of the Hilbert Syzygy Theorem that we have given are Schreyer's.

Exercises

In Exercises 1-6 below the letters m, n m_i, n_i denote monomials.

Exercise 15 1 *: Solve the "elimination problem" in the monomial case: If $I = (m_1, \dots, m_t) \in S$ and $s < r$, find $I \cap k[x_1, \dots, x_s]$.

The next two (easy) exercises are used in the computation of Hilbert functions and polynomials:

Exercise 15 2 *: Show that any monomial submodule of a free module $\oplus Se_i$ is a direct sum of modules of the form I_ie_i with I_i a monomial ideal of S.

Exercise 15 3 *: Let $I = (m_1, \dots, m_t)$ be a monomial ideal, and let n be a monomial of S. Prove that the ideal

$$(I : n) = \{f \in S \mid fn \in I\}$$

is generated by the monomials $m_i/\mathrm{GCD}(m_i,n)$.

Exercise 15 4 : Show that if I is a monomial ideal, then the Hilbert function or polynomial of S/I can be computed as a sum of binomial coefficients by using the following "divide and conquer" strategy:

a) First, if I is generated by some number s of the r variables of S, then

$$H_{S/I}(\nu) = H_{k[x_1, \dots, x_{r-s}]}(\nu) = \binom{r-s-1+\nu}{r-s-1}.$$

Note that we can think of the binomial coefficient "combinatorially" -- so that it is 0 for all sufficiently small ν -- in which case it is the Hilbert function, or as a polynomial in ν of degree r-s-1, in which case it is the Hilbert polynomial.

b) If I is not generated by such a subset of variables, let $n \in S$ be any monomial properly dividing one of the minimal generators of I, and let d be the degree of n. Write $J := (I : n)$. Show that there is an exact sequence of graded modules and degree 0 maps

$$0 \to S/J(-d) \xrightarrow{\varphi} S/I \to S/(I,n) \to 0$$

and thus

$$H_{S/I}(\nu) = H_{S/J}(\nu-d) + H_{S/(I,n)}(\nu).$$

It is an open problem to determine the most efficient choice for n, but an obvious idea would be to take it to be "half" the "largest" monomial among the generators of I.

Exercise 15 5 : Let $I = (x_1x_3, x_1x_4, x_2x_4)$. Compute the Hilbert function and the Hilbert polynomial of I.

Exercise 15 6 : For each of the following ideals, compute a minimal set of divided Koszul relations that generates the syzygies:

a) $(x_1^{34}x_2^7, x_1^{23}x_2^{19})$ b) (x_1, x_2, x_3) c) (x_1x_2, x_1x_3, x_2x_3) .

Exercise 15 7 *: Let $I_1 = (m_1, \dots, m_s)$ and $I_2 = (n_1, \dots, n_t)$ be monomial ideals of S. Show that $I_1 \cap I_2$ is generated by the elements $\mathrm{LCM}(m_i,n_j)$. When is this equal to the ideal I_1I_2?

Exercise 15 8 : a) If F is a free module with basis, $M \subset F$ is any monomial submodule, and > is any monomial order on F, then $\mathrm{in}_>(M) = M$.

b) For any submodule M show that $\mathrm{in}_>(M)$ is spanned as a vector space by the elements $\{\mathrm{in}_>(f) \mid f \in M\}$; that is, we do not need to impose the condition that $\mathrm{in}_>(M)$ is a submodule.

Exercise 15 9 : If $I \subset S$ is a homogeneous ideal, show that $\mathrm{in}_>(I)$ is generated by the monomials $\{\mathrm{in}_>(f) \mid f \in I$ is a homogeneous polynomial$\}$.

Exercise 15 10 : Show that the following properties characterize the orders $>_{\mathrm{lex}}$, $>_{\mathrm{hlex}}$, and $>_{\mathrm{rlex}}$ among monomial orders on S:

a) If $\mathrm{in}_{\mathrm{lex}}(f) \in k[x_s, \dots , x_r]$ for some s, then $f \in k[x_s, \dots , x_r]$.

b) $>_{\mathrm{hlex}}$ refines the order by total degree; and if f is homogeneous with $\mathrm{in}_{\mathrm{hlex}}(f) \in k[x_s, \dots , x_r]$ for some s, then $f \in k[x_s, \dots , x_r]$.

c) $>_{\mathrm{rlex}}$ refines the order by total degree; and if f is homogeneous with $\mathrm{in}_{\mathrm{rlex}}(f) \in (x_s, \dots , x_r)$ for some s, then $f \in (x_s, \dots , x_r)$. More generally, suppose F is a free module with basis over S having a reverse lexicographic monomial order, and $f \in F$. If $\mathrm{in}_{\mathrm{rlex}}(f) \in (x_s, \dots , x_r)F$ for some s, then $f \in (x_s, \dots , x_r)F$.

Exercise 15 11 : Given a monomial order < on S, define the **positive cone** $P_< \subset \mathbb{Z}^r$ of > to be the set of differences a-b such that a, b are vectors of nonnegative integers and (in multi-index notation for monomials) $x^a > x^b$. Show that P is a convex cone in the sense that

$$u, v \in P_< \Rightarrow pu+qv \in P_< \text{ whenever } 0 \le p, q \in \mathbb{Q} \text{ and } pu+qv \in \mathbb{Z}^r$$

and is even strictly convex in the sense that

$$u \in P_< \Rightarrow -u \notin P_<.$$

Exercise 15 12 *: Let > be a monomial order on S, and suppose that m_i, n_i are monomials such that $m_i > n_i$ for $i = 1, \dots ,t$. Show that there is an integral weight order defined by some $\lambda\colon \mathbb{Z}^r \to \mathbb{Z}$ such that λ is compatible with > and $m_i >_\lambda n_i$ for $i = 1, \dots ,t$. (I learned this from Bayer [1982]).

Exercise 15 13 *: Show that every monomial order on S is a lexicographic product of at most r weight orders (L. Robbiano, [1986]).

Exercise 15 14 : Let F be a free module with basis, and fix a monomial order on F. Suppose that $g_1, \dots ,g_t \in M \subset F$.

a) Prove that if in(M) is generated by $\mathrm{in}(g_1), \dots ,\mathrm{in}(g_s)$, then $g_1, \dots ,g_s$ is also a Gröbner basis for M. If $\mathrm{in}(g_1), \dots ,\mathrm{in}(g_s)$ is a minimal set of generators for in(M), then $g_1, \dots ,g_s$ is called a **minimal Gröbner basis** of M.

b) Show that there exists a Gröbner basis $h_1, \dots ,h_s$ for M with the properties

i) $\mathrm{in}(h_i)$ is a monomial (that is, the coefficient from k is 1)

ii) $\mathrm{in}(h_i)$ does not divide any term of h_j for $i \neq j$.

Show that for such a Gröbner basis, the elements $\mathrm{in}(h_i)$ are the minimal generators of in(M). Show that if $g_1, \dots ,g_s$ also has properties i and ii, then $g_i = h_i$ for every i. The Gröbner basis $h_1, \dots ,h_s$ is called **the reduced Gröbner basis of M.**

Exercise 15 15 (Gordan's Proof of the Hilbert Basis Theorem): Gordan, initially shocked by Hilbert's proof of the finite generation of certain rings of invariants by means of the Basis Theorem, recovered quickly and gave his own, simplified proof in [1900]. This proof represents an early (the earliest??) use of the idea of an "initial" ideal of monomials associated to an ideal in a polynomial ring. Here is a proof of the Hilbert Basis Theorem in the spirit of Gordan. (Gordan needed only a special case, and thus proved only a special case, though his argument works generally. It can even be extended to give a proof of the form of the Basis Theorem saying that if R is a Noetherian ring then R[x] is too.)

a) Give a combinatorial proof that any set of monomials of $S = k[x_1, \dots , x_r]$ has only finitely many minimal elements in the partial order by divisibility. (This part is sometimes called "Dickson's Lemma"). In particular, every monomial ideal is finitely generated.

b) By a), any ideal in S has a finite Gröbner basis (with respect to any given monomial order). Deduce that S is Noetherian.

Exercise 15 16 *: Show that the division algorithm still terminates if at each stage we simply choose some monomial of f'_t divisible by some $in(g_i)$, instead of the greatest such. This gives a still more indeterminate version of the division algorithm, which works just as well for the purposes of this chapter as the one given in the text.

Exercise 15 17 : (Characterization of determinate division): Suppose that $f = \Sigma\, m_u\, g_{s_u} + f'$ is the standard expression for f with respect to $g_1, \dots, g_t$ produced by the determinate division algorithm. If we take h_v to be the sum of all the monomials m_u such that $s_u = v$, we may rewrite this expression as

$$f = \Sigma\, h_v\, g_v + f'.$$

Show that this is the unique such expression for which the monomials of h_v lie in the set of monomials n of S such that

$$n\, in(g_v) \notin (\, in(g_1), \dots ,in(g_{v-1})\,)$$

and the monomials of f' do not lie in ($in(g_1), \dots ,in(g_t)$).

Exercise 15 18 *: Pro e that with notation as in Theorem 15 10, ker φ is generated by any set of τ_{ij} such that the corresponding σ_{ij} generate the syzygies on the elements $in(g_i)$.

The following two results of Buchberger sometimes help to speed up the process of computing a Gröbner basis:

Exercise 15 19 : Imitate the proof of Theorem 15 8 to show that in applying Buchberger's Criterion it is enough to check any subset of pairs i,j such that the corresponding σ_{ij} generate all the syzygies on the elements $in(g_i)$.

Exercise 15 20 *: With notation as in Algorithm 15 9, suppose F = S. Show that if $in(g_i)$ and $in(g_j)$ are relatively prime, then the division algorithm can be carried out so that the remainder on division of $m_{ji}g_i - m_{ij}g_j$ by g_i and g_j is 0, and thus the remainder on division of $m_{ji}g_i - m_{ij}g_j$ by $(g_1, \dots ,g_t)$ may be taken to be 0. Thus such syzygies of the $in(g_i)$ may be ignored in computing a Gröbner basis. (This is a case where it is good to have an indeterminate division algorithm!)

Exercise 15 21 *: Some plausible-sounding variations on Proposition 15 15 are FALSE. For simplicity we take the case F = S. Let $I \subset S$ be an ideal, and choose a monomial order on S. Find an example of a sequence of elements $h_1, \dots ,h_u \in S$ such that $h_1, \dots ,h_u$ is a regular sequence on $S/in(I)$, and $in(h_1), \dots ,in(h_u)$ is a regular sequence on S/I, but $h_1, \dots ,h_u$ is not a regular sequence on S/I.

Exercise 15 22 : If I is an ideal of a Noetherian ring S, and $x, y \in S$, then the following are equivalent: 1) $(I: y^\infty) = (I : (x,y)^\infty)$

2) Every associated prime of I that contains y also contains x.

Exercise 15 23 : Prove that the closures of an orbit of $\mathcal{B}$ on k^r is, for some i, the subspace spanned by the last i basis elements. Use this to give another proof of Corollary 15 25.

Exercise 15 24 ((Bruhat)) *: If g is an r×r matrix, then the **principal minor** of order s ≤ r is the determinant of the "upper left" s×s **submatrix** of g; that is, if $g = (g_{ij})_{1\le i,j\le r}$ then the principal minor of order s is $\det((g_{ij})_{1\le i,j\le s})$. If $\mathcal{U}$ is the set of upper triangular r×r matrices with ones on the diagonal and $\mathcal{B}'$ is the set of invertible lower triangular matrices, show that $\mathcal{B}'\mathcal{U}$ is the set of invertible matrices whose principal minors are all nonzero. In particular, $\mathcal{B}'\mathcal{U}$ is a Zariski open and dense subset of $\mathcal{G}$. (In fact $\mathcal{B}'\mathcal{U}$ is the "big cell" in the Bruhat decomposition of $\mathcal{G}$; see Humphreys [1975] or Fulton-Harris [1991] for the some more of the story.)

Exercise 15 25 With notation as in Theorem 15 17 show that if $g_1, \dots, g_t \in I$ are chosen so that $\mathrm{in}_>(g_1), \dots, \mathrm{in}_>(g_t)$ generate $\mathrm{in}_>(I)$, or even so that $\mathrm{in}_\lambda(g_1), \dots, \mathrm{in}_\lambda(g_t)$ generate $\mathrm{in}_\lambda(I)$, then $\tilde{g}_1, \dots, \tilde{g}_t$ generate $\tilde{I}$.

Exercise 15 26 : Let > be a monomial order on S, and T be the subring of the quotient field of S generated by all the fractions m/n, with m and n monomial of S such that $m \geq n$ (we consider $m > 1$ for any nontrivial monomial, so T contains the polynomial ring S).

a)* Show that $\{m/n \mid m, n \in S$ are monomials and $m > n\}$ generates a proper ideal J of T, and that the quotient T/J is k. Show that

$$S \subset T \subset S[y_1^{-1}, \dots, x_r^{-1}] = T[x_1^{-1}, \dots, x_r^{-1}].$$

Show that T need not be Noetherian.

We will consider $\tilde{S} := T \otimes_k S$ as a flat family of algebras over T (it is flat because S is flat -- indeed, free -- as a k-module). For convenience of notation, we think of T as coming from a polynomial ring in a different set of variables, $y_1, \dots, y_r$. With this notation, the fractions

$$x^\alpha y^\beta / y^\gamma \quad \text{with} \quad y^\beta > y^\gamma$$

form a k-basis for $\tilde{S}$.

For any polynomial $g(x_1, \dots, x_r) \in S$, with inital monomial x^α, let $\tilde{g} \in \tilde{S}$ be defined as

$$\tilde{g} = y^\alpha\, g(x_1/y_1, \dots, x_r/y_r),$$

which is in $\tilde{S}$ precisely because all the monomials of g are $\leq x^\alpha$. For any ideal I of S, let $\tilde{I} \subset \tilde{S}$ be the ideal generated by all $\tilde{g}$ with $g \in I$.

b) Show that $T[y_1^{-1}, \dots, y_r^{-1}] \otimes_T \tilde{S}/\tilde{I} \cong T[y_1^{-1}, \dots, y_r^{-1}] \otimes_T S/I$

while $T/J \otimes_T \tilde{S}/\tilde{I} \cong S/\mathrm{in}_>(I)$.

c) Show that $\tilde{S}/\tilde{I}$ is flat over T by showing that it is free on the monomials in $x_1, \dots, x_r$ not in $\mathrm{in}_>(I)$.

Exercise 15 27 * (The simplest nontrivial syzygy computation): Take $g_1 = x^2$, $g_2 = y^2$, $g_3 = xy+yz \in k[x,y,z]$. Find a Gröbner basis and syzygies using the reverse lexicographic order, and $x > y > z$.

Exercise 15 28 * (Five points in $\mathbb{P}^3$): Find a minimal free resolution of the ideal

$$I = (x_0^2 - x_2x_3,\ x_0x_1 - x_3^2,\ x_0x_2 - x_1^2,\ x_1x_3 - x_2^2,\ x_0x_3 - x_1x_2)$$

in the polynomial ring $S = k[x_0, \dots, x_3]$ (this is the ideal of 5 points in $\mathbb{P}^3$).

Exercise 15 29 *: Let $M = (x^2, txy+y^3) \subset k[t,x,y]$. Compute a Gröbner basis with respect to reverse lexicographic order using $t > x > y$.

Exercise 15 30 : Using the result of Exercise 15 29, find a presentation for the associated graded ring of $k[x,y]/(x^2, xy+y^3)$ with respect to the ideal (x,y).

Exercise 15 31 : Let $I = (x_1x_3 - x_2^2, x_1x_4 - x_2x_3, x_2x_4 - x_3^2)$ be the ideal of 2×2 minors of the matrix

$$\begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_4 \end{pmatrix},$$

and let I' be the ideal of minors of the matrix

$$\begin{pmatrix} x_2 & x_1 & x_3 \\ x_1 & x_3 & x_4 \end{pmatrix}$$

obtained by interchanging x_1 and x_2. Find Gröbner bases for I and I' with respect to the reverse lexicographic order on the monomials.

Exercise 15 32 : Let I be the ideal of Exercise 15 31. Is $x_2^4 \in I$?

Exercise 15 33 : Let R be the ring $k[x_{11},x_{12},x_{21},x_{22}]$ and let

$$X = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}$$

be the generic 2×2 matrix over R. Let I be the ideal generated by the 4 entries of the matrix X^2, so that $I = (x_{11}^2+x_{12}x_{21}, \dots)$. If the polynomials of I vanish when we substitute the entries a_{ij} of some 2×2 matrix A over k, then evidently $A^2 = 0$ -- that is, A is nilpotent. It follows from the Nullstellensatz that if $g(x_{11}, \dots ,x_{22})$ is any polynomial vanishing on 2×2 nilpotent matrices, then some power of g lies in I. The trace and determinant, $x_{11}+x_{22}$ and $x_{11}x_{22}-x_{12}x_{21}$ are such polynomials. Compute a Gröbner basis of I and use it and the division algorithm to decide which powers of the trace and determinant lie in I.

It is known that if X is a generic n×n matrix then the coefficients of the characteristic polynomial of X (in the 2×2 case the trace and determinant) generate the prime ideal corresponding to the variety of nilpotent n×n matrices, and one can ask in general what is the smallest integer d such that T^d belongs to the ideal of entries of X^n, where T is the trace $x_{11}+\dots+x_{nn}$. Considering diagonal matrices it is easy to show that $d \geq n^2-n+1$. In fact, B. Mourrain has shown me a proof that $d = n^2-n+1$ using a "Sagbi base" for the ring of invariants under the conjugation action of GL(n,k), the ring generated by the coefficients of the characteristic polynomial. See Robbiano-Sweedler [1990] for the definitions.

Exercise 15 34 (The general submodule membership problem) : Let P be any S-module, given by "generators and relations", that is, as

$$P = F/M,$$

where F is a free module with basis and $M = (f_1, \dots ,f_t)$ is a submodule of F. Let $Q \subset P$ be a submodule, given as the image of a submodule N of F. Generalize the idea given for solving problem 1) to decide, for any element $p \in P$, whether or not $p \in Q$.

Exercise 15 35 : Compute the Hilbert function and polynomial of the determinantal ideal I from Exercise 15 31.

Exercise 15 36 *: Let P be any finitely generated S-module, and write $P = F/M$ with F a free S-module. Let $\mathfrak{m} = (x_1, \dots ,x_r)$. Use a technique analogous to that of Proposition 15 28 to construct a homogeneous submodule $M' \subset F$ (with F regarded as a graded module having all its generators in degree 0) such that $\mathrm{gr}_{\mathfrak{m}} M = F/M'$.

Exercise 15 37 : Let $T = S[y_1, \dots , y_s]$ and let F be a free T-module with basis e_i. Let > be a monomial order on F satisfying E with respect to the variables y_i. If $g_1, \dots ,g_t$ is a Gröbner basis in F, and $g_1, \dots ,g_s$ are those of the g_i that do not involve the variables y_i, show that $g_1, \dots ,g_s$ is a Gröbner basis in $F' = \oplus Se_i$ for $J = S \cap (g_1, \dots ,g_t)$ with respect to the monomial order on S gotten by restricting the given one from T.

Exercise 15 38 : Show how to use elimination, via Proposition 15 30, to find presentations of the blowup algebra and associated graded ring of a ring S/I with respect to a given ideal $\mathfrak{m}$.

Exercise 15 39 (Inhomogeneous Gröbner bases from homogeneous ones): Some computer algebra systems handle Gröbner bases only in the homogeneous case. The following shows that this is enough to compute Gröbner bases of arbitrary ideals.

Given a monomial order > on S, extend it to $S[x_0]$ as follows: If m and n are monomials of S, define $mx_0^d > nx_0^e$ if $m > n$ or $m = n$ and $d < e$. Suppose that I is a (not necessarily homogeneous) ideal of S, and I' is any ideal of $S[x_0]$ that goes to I under the "specialization" map $S[x_0] \to S$

sending $x_0 \mapsto 1$ and $x_i \mapsto x_i$ for $i > 0$. Show that in(I') goes to in(I) under the specialization, and that any Gröbner basis of I' goes to a Gröbner basis of I under the specialization.

Exercise 15 40 (Projective closure by saturation): Let $I \subset S$ be an ideal, and let I' be the ideal of s-homogeneous elements (in the sense of the section on projective closures) in the preimage of I under the map

$$S[x_0] \rightarrow S\ ; \quad x_0 \mapsto 1.$$

If I'' is the ideal obtained by s-homogenizing the elements of some set of generators for I, then

$$I' = (I'' : x_0^\infty).$$

Exercise 15 41 ((M : J) and (M : J $^\infty$) in general): Suppose that F is a finitely generated free S-module and $M \subset F$ is a submodule. Let $J \subset S$ be any ideal. We wish to compute (M : J) and (M : J^∞).

a) (Solution of the problem in case J is generated by a variable). Suppose that $J = (x_r)$. Proposition 15 12 b) allows one to compute (M: J) in this case. Show that Proposition 15 12 remains true if x_r is replaced by $x_r{}^d$ for any $d \leq \infty$; the case $d = \infty$ gives a computation of (M : J^∞). This idea comes from Bayer [1982].

b) (Reduction to the case where J is a principal ideal) Let S' = S[y], where y is a new indeterminate, and regard S as a subring of S'. Let $M' = S'\otimes_S M \subset S'\otimes_S F$. Suppose $J = (f_1, \dots ,f_t)$, and let $f = f_1+yf_2+\dots+y^{t-1}f_t$. Show that (M' : f) = S'(M : J), and thus (M : J) = (M' : f)∩S, and deduce similar formulas for (M : J^∞). (One could also do this by introducing t new variables y_i, and using $f = \Sigma y_i f_i$. This is often less efficient computationally.)

c) (Reduction to the case where J is generated by a variable) Suppose that J = (f) is a principal ideal. Let $M' = S'\otimes_S M+(y-f)F \subset S'\otimes_S F$. (Note that if M is a graded module and f is homogeneous of degree d, we should take y to have degree d to get a graded module M'.) Show that (M' : y) = S'(y-f) + S'(M : f), and that (M : f) = (M' : y) ∩ S. Deduce corresponding formulas for (M : f^∞).

d) (Reduction to the homogeneous case) Independent of the reductions above, the computation of (M : J) and (M : J^∞) can be reduced to the homogeneou case as follows: Suppose $M \subset F$ is an arbitrary submodule, let x_0 be a new indeterminate, and let $\tilde{M} \subset S[x_0]\otimes_S F$ be an $S[x_0]$-module obtained by homogenizing with respect to x_0 any set of generators for M -- that is, by regarding the generators of M as vectors of polynomials, and homogenizing each component of that vector to some common degree. Let $\tilde{J}$ be the ideal of $S[x_0]$ obtained by homogenizing any set of generators of J. ($\tilde{M}$ and $\tilde{J}$ depend on lots of choices.) Show that generators for (M : J) may be obtained from any set of generators for ($\tilde{M}$: $\tilde{J}$) by setting x_0 to 1, and similary for (M : J^∞).

Exercise 15 42 (Another way to compute intersections): If $I = (f_1, \dots f_s)$ and $J = (g_1, \dots ,g_t)$ are ideals of S, show that the kernel of the map $S^{s+t+1} \rightarrow S^2$ with matrix

$$\begin{pmatrix} 1 & f_1 & \cdots & f_s & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 & g_1 & \cdots & g_t \end{pmatrix}$$

consists of vectors whose first coordinates generate the ideal I∩J. Generalize this to a construction for the intersection of two submodules of an arbitrary free module.

Exercise 15 43 (Yet Another way to compute intersections): If I and J are ideals of S, define an ideal K of S[t] as K = (tI + (1-t)J). Show that I∩J = K∩S, reducing the problem of intersection to a problem of elimination.

The following sequence of exercises provide applications for the pullback construction described in the text.

Exercise 15 44 (Kernels): Prove Proposition 15 32, constructing kernels.

Exercise 15 45 (Images): Let $\varphi: G \to F$ be a map of free modules, $P =$ coker φ. Given a map of free modules $H \to F$, use the pullback to find a presentation of the module that is the image of H in P.

Exercise 15 46 : Let

$$\begin{tikzcd} G \arrow[r, "\varphi"] & F \arrow[r] & P \arrow[r] & 0 \end{tikzcd}$$

be a free presentation of a module P, and M be the image of φ, so that $P = F/M$.

a) **The annihilator of an element of P** . Given an element $\tilde{e}$ of P, choose $e \in F$ mapping to $\tilde{e}$. Define a map $S \to F$ by sending 1 to e. Show that the annihilator of $\tilde{e}$ is the image of the map π_S in the pullback diagram

$$\begin{tikzcd} PB \arrow[r, "\pi_S"] \arrow[d] & S \arrow[d] \\ G \arrow[r] & F. \end{tikzcd}$$

b) **Annihilators i ı general.** To compute the annihilator of P itself one can compute the annihilator of each of a set of generators, and take the intersection; however, there is a convenient way of doing this all at once: Choosing a basis $\{e_i\}$ of F let $\psi: S \to \mathrm{Hom}(F,F)$ be the map sending 1 to the identity map. Write $\mathrm{Hom}(F, \varphi)$ for the map $\mathrm{Hom}(F,G) \to \mathrm{Hom}(F,F)$ induced by φ. Show that the annihilator of P is the image of the map π_S in the pullback diagram

$$\begin{tikzcd} PB \arrow[r, "\pi_S"] \arrow[d] & S \arrow[d, "\psi"] \\ \mathrm{Hom}(F,G) \arrow[r, "\mathrm{Hom}(F,\varphi)"'] & \mathrm{Hom}(F,F) \end{tikzcd}$$.

c) **Quotient by an element.** If $g \in S$, show that the submodule $(M : g) \subset F$ is the image of π_F in the pullback diagram

$$\begin{tikzcd} PB \arrow[r, "\pi_F"] \arrow[d] & F \arrow[d, "\psi"] \\ G \arrow[r, "\varphi"'] & F \end{tikzcd},$$

where $\psi: F \to F$ is multiplication by g.

d) **Quotients in general.** If $J \subset S$ is an ideal with t generators $g_1, \dots, g_t$, we could compute $(M : J)$ from the formula $(M : J) = \cap\, (M : g_i)$, but we can do it all at once as follows: Define a map $\alpha: S \to S^t$ sending $1 \in S$ to the column vector with i^{th} entry g_i. Let $F \otimes \alpha: F = F\otimes S \to F\otimes S^t$ be the tensor product of the identity map and α, and let $\varphi\otimes S^t$ be the tensor product of φ with the identity map of S^t. Show that the submodule $(M : J)$ is image of π_F in the pullback diagram

$$\begin{tikzcd} PB \arrow[r, "\pi_F"] \arrow[d] & F \arrow[d, "F \otimes \alpha"] \\ G\otimes S^t \arrow[r, "\varphi\otimes S^t"'] & F\otimes S^t \end{tikzcd}$$.

Appendix: Some computer algebra projects

Several current computer algebra systems allow the computation of Gröbner bases. Unfortunately, as of this writing the general purpose systems such as Macsyma, Maple, Mathematica, and Axiom do not have the flexibility in their algorithms or simply do not run fast enough to make experimentation of the sort suggested below very attractive. At least two systems that were designed primarily for Gröbner basis computation are generally available (and for free!): **CoCoA** (Computations in Commutative Algebra) by Alessandro Giovini and Gianfranco Niesi, of the Department of Mathematics, University of Genova, Italy, and **Macaulay** , by Dave Bayer and Michael Stillman (Department of Mathematics, Columbia University and Cornell University, respectively. **Macaulay** is available free from the authors for many machines including the Macintosh, IBM-PC, Sun, Vax, and others. It can be obtained from a public account on a machine at Harvard University. For experts the following instructions should suffice: ftp to 128.103.28.10, or math.harvard.edu, login ftp, password any, cd Macaulay. The C language source code files are in tar format in M3.tar, along with "make" files for various machines; the manual is in the document Macman.ps.) CoCoA is relatively easy to use and is well suited for experimentation with Gröbner bases; but it lacks many of the facilities that the more mature system **Macaulay** has developed for handling problems from commutative algebra and algebraic geometry. On the other hand, certain design decisions taken to make **Macaulay** efficient may look odd to the beginner: **Macaulay** only computes Gröbner bases of homogeneous ideals, and works exclusively over finite fields $\mathbf{Z}/p$, for various p. In any case, I have mainly had experience with **Macaulay** and the discussion below is slanted toward its use.

Macaulay is partially "responsible" for quite a number of published theorems, in the sense that people have been able to look at examples that have lead them to guess at results, or to reassure themselves of the truth of results, which they otherwise would not have proved. I have

tried to reproduce the spirit -- and in some cases the topics -- of some of these investigations at a suitable level below. I am certain that there are still new phenomena to be discovered in each of these realms; perhaps the student will hit on something genuinely original. With each project I have listed the names of some **Macaulay** commands and scripts that I would find useful if I were doing the project. (The reader can tell the difference because scripts are written beginning with the character <, while commands do not have this prefix. If the user types

```
    <scriptname
or
    commandname
```

then **Macaulay** should provide a help message on the script or command referred to, from which the action and the correct syntax can be inferred. Of course given the rate of developmen of computer algebra, these suggestions are not likely to be valid for terribly long. For all the projects I would use the scripts <ring and <ideal, which make defining objects somewhat more convenient.

Here are the projects:

Project 1) Zero-dimensional Gorenstein ideals. Compute some ideals of the form $I = ((x_1^s, \ldots ,x_r^s) : p)$, where p is a homogeneous polynomial. It's easy to do the case r = 1 and the case p a monomial, r = anything, by hand. Try the case r = 2 with more complicated p on the machine. (In **Macaulay** , use the "quotient" command.) How many generators does I require? Next try r = 3, various p. Here there is a greater range in the possible numbers of generators. Is there any restriction? Make a conjecture! How about with r = 4? One way to get polynomials p to try is to take random ones (made with <random_mat, for example). The answers you get in this case should depend only on r,s and deg p. What's the pattern here? Of course there will be more possibilities visible if you choose very special polynomials p.

It is also interesting to use res to resolve these ideals I. Their resolutions have a certain unusual property, visible (in **Macaulay**) through the command "betti". Can you spot it? What are the possible sequences of betti numbers in the cases r = 2, 3, 4? Any conjectures?

There is also something funny about the Hilbert function. (In **Macaulay** , use hilb and <hilb-fcn.)

For your information, the ideals I that can be obtained as above are exactly what are usually called "0-dimensional, homogeneous Gorenstein ideals". See Chapter 21.

Reference: This is actually the first project that involved me personally with computer algebra. David Buchsbaum and I were interested in Gorenstein ideals in about 1971-2. Ray Zibman, then an undergraduate at Brandeis, programmed the PDP 10 computer in Lisp to find the ideals I (this can be done without Gröbner bases, since in this problem all the rings involved are finite dimensional over k). We also made a number of hand computations of the syzygies of these ideals and found a regularity in the case r = 3 that may not be so apparent without a good deal of study of the matrices in the resolution. You can find the results inspired by our computations in the paper Buchsbaum-Eisenbud [1977] .//

Project 2) Factoring out a general element from an s-syzygy

One way for an S-module P = coker π_p: $G_p \to F_p$ to be an s^{th} syzygy -- that is, for it to be the kernel at the s^{th} step of a free resolution -- is the following: Let

$\mathcal{H}$: $\quad 0 \to H_t \to \dots \to H_1 \to F_p^* \to G_p^*$

be the free resolution of the cokernel Q of the dual of the map π_p, and dualize $\mathcal{H}$ to get a complex

$\mathcal{H}^*$: $\quad G_p \to F_p \to H_1^* \to \dots \to H_t^* \to 0 \to \dots$

The homology of $\mathcal{H}^*$ (kernel of one map modulo the image of the one before) at the module H_i^* is called $Ext^{i-1}(N,S)$. If these modules are 0 for i = 1, ... ,s, then M is a s^{th} syzygy -- let us say that M is a "standard s^{th} syzygy" in this case. Is every s^{th} syzygy a standard s^{th} syzygy? If so, this gives a test for whether a module is an s^{th} syzygy; otherwise, we have defined a new notion. Try some examples to get a feel for what might be true.

Next take a (standard) s^{th} syzygy and kill a random element. For what t is the result a (standard) t^{th} syzygy? What if you start with a free module? Perhaps the simplest case is when P = S^t/Sf, where S is the column vector with entries $f_1, \dots, f_t$. Can you tell whether P is an s^{th} syzygy from some property of the ideal generated by the f_i?

The situation is relatively simple if, as above, we work over S. Completely new phenomena -- which no one understands as of this writing -- arise if we replace the polynomial ring S by a factor ring, say $S/(g_1,\dots,g_u)$. Even the case u = 1 is challenging -- see project 3 below -- but the general case seems still more baffling.

Reference : The phenomena that the reader is most likely to discover here were first noticed and exploited by W. Bruns [1976]. See for example Evans-Griffith [1985] for a general treatment of related matters.

Project 3) Resolutions over hypersurfaces : Find some modules over $k[x,y]/(y^2)$. (For example, take any k[x,y]-module M and factor out y^2 times it. (Take note of whether or not y^2 was a nonzerodivisor on M; you could test for this with the script <nzd.) Resolve over k[x,y], and over $k[x,y]/(y^2)$. (Use fetch; explicit length of res, as in res I, Ires, n; betti. Keep n ≤ 15 or so.) Can you make a conjecture about the resolutions? Can you prove it? How about replacing y^2 by an arbitrary polynomial p(x,y)? How about in n variables?

Reference : Eisenbud [1980].

One source of examples that will probably always be interesting is the family of "rational curves" of degree d in $\mathbb{P}^r$. From an algebraic point of view rational curves are subrings

$$R = k[f_0(s,t), f_1(s,t), \dots , f_r(s,t)] \subset k[s,t]$$

of a polynomial ring in 2 variables generated by r+1 independent polynomials of degree d. (Use <subring and, for the special case where all the f_i are monomials, <monomial_curve to construct these conveniently). The **defining ideal** of the curve is by definition the kernel I of the map

$$k[x_0, \dots ,x_r] \to k[s,t]; \ \ x_i \mapsto f_i.$$

The next three projects explore various aspects of these examples.

Project 4) Rational curves of degree r+1 in $\mathbb{P}^r$. Consider the case of the subring R generated by 4 polynomials $f_0(s,t), \dots , f_3(s,t)$ of degree 4 in k[s,t]. For various choices, compute the defining ideal I in $k[x_0, \dots ,x_3]$ and its free resolution. How do the betti numbers depend on the polynomials chosen? How many types are there? (Try the monomial examples first, then something just a little more general. Note that the result depends only on the vector space spanned by the f_i, not on the f_i themselves.) What about the situation of r forms of degree r? Note that we are excluding just one form; that is, the space of r forms of degree r is the kernel of a linear form on the space of all forms of degree r. (In **Macaulay** , use the command diff.) One way to write down such a linear form is as a differential operator of order r with constant coefficients -- that is, essentially, as a single polynomial of degree r. This point of view may make the results more intelligible by giving natural invariants of such codimension 1 subspaces -- for example, you might distinguish a single polynomial g of degree d by the smallest number t such g is expressible as the sum of t d^{th} powers of linear forms, or is in the closure of the set of polynomials that are expressible this way. (If you like this point of view, you might want to look up "Catalecticants" in the old book on invariant theory by Grace and Young [1903].)

Project 5) Regularity of rational curves : If M is a graded S-module then we define the regularity of M (in the sense of Castelnuovo) from the minimal free resolution of M

$$\dots \to F_s \to \dots \to F_0 \to M \to 0$$

to be the least integer ρ such that for each s, all the free generators of F_s lie in degree $\leq s + \rho$. (See Chapter 20). In **Macaulay** , the command res always computes minimal free resolutions after the first step; use nres to make the first step minimal too. Thus, in **Macaulay** , the regularity is the number of rows in the diagram produced by the command betti.) The regularity of M is an important measure of how hard it will be to compute a free resolution of M.

What is the possible regularity of S/I if I is the defining ideal of a rational curve? Try monomial curves (where all the f_i are monomials) first. What range of values can you get? Another interesting invariant to study in these cases is the last betti number of the curve. One way (of many) to produce interesting families of monomial curves is to fix a pattern of exponents -- that is, an increasing sequence of numbers $b_1, \dots b_r$ -- and try something like

$$1, t^{a+b_1}, t^{a+b_2}, \dots ,t^{a+b_r}$$

for varying a.

Reference: Gruson-Lazarsfeld-Peskine [1983].

(**Helpful Macaulay** scripts: <regularity, <res, <random_mat, <monomial_curve)

Project 6) Some monomial curve singularities: Let

$$f_i = s^{d_i}t^{e_i} \text{ with } d_i + e_i = d,\ 0 \le e_0 \le \dots \le e_r \le d$$

and consider the corresponding rational curve. Show that factoring out $s^{d_r}t^{e_0}$ from each of the f_i will not change the defining ideal of the curve, so we may assume $e_0 = 0$, $e_r = d$.

Dehomogenize the defining ideal $I \subset k[x_0, \dots, x_r]$ of the curve by setting $x_0 = 1$ (this will be the defining ideal of the subring $k[t^{e_1}, \dots, t^{e_r}] \subset k[t]$). Compute the associated graded ring of the curve with respect to the maximal ideal. (In **Macaulay** use the script <l_tangentcone.)

What are the possible lengths of the minimal free resolution of this graded ring? Can you find any families of examples where the length is r-1? Can you find any where the betti numbers (ranks of the free modules in the resolution) are symmetric around the middle? Try patterns of exponents, as described in Project 5.

Project 7) Some interesting prime ideals. For each $0 \le u \le r$, consider the prime ideal $I_{u,r}$ that is the kernel of the ring homomorphism

$$k[x_0, \dots, x_r] \to [s, t, z_0, \dots, z_u]; \qquad x_i \mapsto F_i$$

where the elements F_i are obtained as homogenizations with respect to s

$$F_i = s^n\varphi_i(t/s, z_0/s, \dots, z_u/s)$$

of the entries φ_i of the product shown in Figure 15.8,

$$(z_0, z_1, \dots, z_u)\begin{bmatrix} 1 & t & t^2 & t^3 & \dots & & t^r \\ 0 & 1 & 2t & 3t^2 & \dots & & rt^{r-1} \\ 0 & 0 & 2 & 6x & \dots & & \\ & & \cdots & \cdots & \cdots & \cdots & \\ 0 & \dots & 0 & u! & \dots & & r!/(r-u)!t^{r-u} \end{bmatrix} = (\varphi_0, \varphi_1, \dots, \varphi_r)$$

Figure 15.8

where the rows of the large matrix are obtained by successively differentiating the entries of the first row with respect to t. Thus for example for u = 0 the F_i are $z_0s^r, z_0s^{r-1}t, \dots, z_0t^r$, while for u = 1 we get

$$z_0s^r,\quad z_0s^{r-1}t + z_1s^r\ ,\quad z_0s^{r-2}t^2 + 2z_1s^{r-1}t\ , \dots .$$

What degree elements do you think it takes to generate $I_{u,r}$ if r is rather larger than u? For u = 1 the resolution of $I_{u,r}$ has a particularly interesting property; can you find it? Can you see any interesting properties of the resolution for other values of s: In general, how long do you think the resolution will be? (You will probably have to guess at these answers from rather small values of r, u -- say $r \le 9$ or 10, u = 0, 1, 2 and perhaps a little more.) Suppose you take the ideal generated by just the quadratic forms in $I_{u,r}$ (respectively, forms of degree $\le$ d for some d.) Do you get anything interesting?

(Use the commands power, diff, concat, to form the big matrix; mult to form the row of φ_i; homog (applied to the transposed vector to homogenize it. Use <subring to compute $I_{u,r}$. Note that one must then use std or nres to get a minimal set of generators for the ideal.)

These ideals arise in geometry as follows: The vector

$$1, t, t^2, \dots t^r$$

that is the first row of the matrix above may be thought of as parametrizing a curve C in $\mathbb{P}^r$ whose closure is called the **rational normal curve.** Thus $I_{0,r}$ is the ideal of the rational normal curve in $\mathbb{P}^r$.

The second row of the matrix is obtained by differentiating the first row with respect to x; thus a linear combination

z_0(first row) + z_1(second row)

represents a point on a tangent line to this curve, and $I_{1,r}$ is the ideal of the **tangent developable surface to the rational normal curve** (that is, the surface consisting of the union of the tangent lines to the curve). Similarly, for arbitrary u, the linear combination of the u+1 rows represents a point on an **osculating u-plane** to the curve. Thus is the ideal of the union of the osculating u planes. These ideals have been much studied for u = 0 (easy) and for u=1 (the "generic Green's conjecture" is a guess at the form of the free resolution of $I_{1,r}$ (see Eisenbud [1992] for an exposition). I think there are not even conjectures for u > 1; perhaps the reader will make some interesting ones!

Hints for selected exercises

Exercise 15 1 : It is generated by monomials.

Exercise 15 2 : If the submodule is generated by monomials $\{g_i\}$, let M_i = I_ie_i be the submodule generated by all the g_j that are of the form me_i.

Exercise 15 3 : The given elements are certainly in (I : n). On the other hand if f $\in$ (I : n) then fn $\in$ I, so the terms of fn are multiples of some m_i. It follows from unique factorization that the terms of f are multiples of some $m_i/\mathrm{GCD}(m_i,n)$.

Exercise 15 7 : $I_1 \cap I_2 = I_1I_2$ iff a minimal generating set $\{m_i\}$ for I_1 and a minimal generating set $\{n_j\}$ for I_2 do not have any variables in common. The "if" part is easy. To prove "only if", suppose on the contrary $I_1 \cap I_2 = I_1I_2$ but $m_i = pm'_i$ and $n_j = pn'_j$ have GCD $p \neq 1$, and that m'_i is chosen with minimal degree. Since $I_1 \cap I_2 \supset pm'_in'_j$, we see that $pm'_in'_j$ is a multiple of some m_un_v. Deduce a contradiction from the assumed minimality of degrees.

Exercise 15 12 : From Exercise 15 11 it follows that 0 is not in the convex hull of the finitely many elements $m_i-n_i \in P_<$. Equivalently, there is a rational hyperplane H through the origin in $\mathbb{Q}^r$ such that a translate of H separates 0 from the m_i-n_i. Writing H as the set of zeros of a linear functional λ, we see that λ is either strictly positive or strictly negative on all the $m_i - n_i$. In the second case we replace λ by $-\lambda$. Since we may multiply λ by a positive integer without changing H, we may assume that λ is integral.

Exercise 15 13 : Find a rational linear functional w whose hyperplane of zeros does not meet the interior of the positive cone $P_<$. If w is non-negative on $P_<$, use w for the first weight vector; otherwise use -w. Do induction on the dimension of the span of $P_<$, considering the intersection of $P_<$ with the hyperplane of zeros of w.

Exercise 15 16 : The sequence $\mathrm{in}(f'_t)$ is non-increasing, and thus must eventually stabilize; let m_1 be its eventual value. Similarly, the sequence $\mathrm{in}(f'_t - m_1)$ must eventually stabilize; let m_2 be its eventual value, and so on. Show that if the process did not terminate, then $m_1, m_2, \dots$ would be an infinite strictly descending sequence.

Exercise 15 18 : If not all the syzygies were linear combinations of the given syzygies we could choose one, say $\Sigma\, p_u\varepsilon_u$, with the property that the largest monomial m among the $\mathrm{in}(p_u g_u)$ is minimal. Let $\Sigma'\, p_v\, g_v$ be the sum of all those terms $p_v g_v$ for which $\mathrm{in}(p_v g_v)$ is m up to a scalar. Writing

$$\mathrm{in}(p_v g_v) = n_v\ \mathrm{in}(g_v),$$

for some term n_v of p_v we have $\Sigma'\, n_v\ \mathrm{in}(g_v) = 0$, so there is a linear combination of the given syzygies that has the form $\Sigma'\, n_v\, \varepsilon_v - \Sigma\, f_u\varepsilon_u$ for some f_u with $\mathrm{in}(f_u g_u) < m$. Subtract this from the syzygy $\Sigma\, p_u\varepsilon_u$ to get a contradiction.

Exercise 15 20 : In this case we have $m_{ij} = \mathrm{in}(g_j)/e_i$ and $m_{ji} = \mathrm{in}(g_j)/e_j$. We have

$$\begin{aligned} -m_{ji}g_i + m_{ij}g_j &= (g_j g_i - g_i g_j) - (\mathrm{in}(g_j)g_i - \mathrm{in}(g_i)g_j) \\ &= (g_j - \mathrm{in}(g_j))g_i - (g_i - \mathrm{in}(g_i))g_j \\ &= p_j\, g_i - p_i\, g_j \end{aligned}$$

with $\mathrm{in}(p_j) < \mathrm{in}(g_j)$ and $\mathrm{in}(p_i) < \mathrm{in}(g_i)$. We claim that the initial term of such an expression is necessarily $\mathrm{in}(p_j)\ \mathrm{in}(g_i)$ or $\mathrm{in}(p_i)\ \mathrm{in}(g_j)$. Indeed, the only other possibility is that these terms cancel. But since $\mathrm{in}(g_i)$ and $\mathrm{in}(g_j)$ are relatively prime, cancellation is only possible if $\mathrm{in}(g_i)$ divides $\mathrm{in}(p_i)$, this is impossible because of the inequality. Now subtract the appropriate multiple of g_i or g_j, and repeat the argument....

Exercise 15 21 : You need go no further than u = 1 and the case of 2 variables.

Exercise 15 25 : Modify the last paragraph of the given proof to use only the elements g_i from I.

Exercise 15 24 : First, if $b' \in \mathcal{B}'$ and $u \in \mathfrak{U}$, observe that the upper left s×s submatrix of b'u is the product of the upper left s×s submatrix of b' and the upper left s×s submatrix of U. In particular, it is the product of invertible matrices, so the principal minors of b'u are all nonzero.

Conversely, suppose that the principal minors of a matrix g are all nonzero. It suffices to show that there is a lower triangular matrix b such that u = bg is in $\mathfrak{U}$; then $g = b^{-1}u$ shows that $g \in \mathcal{B}'\mathfrak{U}$. But multiplying g on the left by a lower triangular matrix may be expressed as a sequence of elementary transformations, in each of which one either multiplies a row of g by a nonzero scalar or adds a row of g to a later row. Since the 1×1 principal minor of g, which is the upper left entry g_{11}, is nonzero we may multiply the first row by ${g_{11}}^{-1}$ and then subtract a multiple of the first row from each succeeding row to make g into a matrix whose first column has entries 1,0, ... ,0. The effect of this is to multiply the principal minors by ${g_{11}}^{-1} \neq 0$. In particular, the principal minor of order 2, which is now equal to g_{22}, is nonzero. Multiplying the second row by ${g_{22}}^{-1}$ and then adding a multiple of it to each succeeding row, we may assume that the second column of g has entries g_{12}, 1, 0, ... ,0. Continuing in this way, we eventually reduce to an element $g \in \mathfrak{U}$ as claimed.

Since each of the principal minors is a polynomial function of the entries of g, the locus where they are all nonzero is open; as $\mathcal{G}$ is itself an open subset of an affine space, any open subset is dense.

Exercise 15 26 a): Take r = 2 and > the lexicographic order. Let K be the ideal generated by all $x_1/x_2{}^s$ for $s \geq 0$. Show that $x_2K = K$. Since T is a domain, Corollary 4.7 shows that K cannot be finitely generated.

Exercise 15 27 : To get a Gröbner basis adjoin $g_4 = yz^2$. The syzygies on the original 3 generators are generated by the columns of

$$\begin{pmatrix} y^2 & 0 & (x+z)y \\ -x^2 & x+z & 0 \\ 0 & -y & -x^2 \end{pmatrix} .$$

Exercise 15 28 : The resolution will be symmetric, with ranks of free modules 1,5,5,1, and the first and last matrices should be transposes of one another up to change of basis; if you make the change of basis necessary to make the first and last matrices actually be transposes of one another, the middle matrix will be skew symmetric. This phenomena will be "explained" in Chapter 21.

Exercise 15 29 : x^2, $txy+y^3$, xy^3, y^5

Exercise 15 36 : Begin by homogenizing the elements of a presentation matrix for M with respect to a new variable x_0 and multiplying each element by whatever power of x_0 is necessary to bring them all to the same degree, to get a homogeneous submodule $M'' \subset F$ whose cokernel is a graded $S[x_0]$-module. Then argue as in the Proposition.