GROEBNER BASES

BRIAN OSSERMAN

Most of the included material on Groebner bases is adapted from Dummit and Foote.

1. Motivation: the variety-ideal correspondence

The study of ideals in polynomial rings over fields is absolutely central to algebraic geometry. We think of an affine variety (usually called affine algebraic set without an irreducibility hypothesis) in \( n \) dimensions as defined to be the common zero set of a collection of polynomials \( f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n) \) with coefficients in some field \( k \). We see that if a point \((c_1, \ldots, c_n)\) is a zero of each of the \( f_i \), then it is a zero of any polynomials in the ideal \( I \subseteq k[x_1, \ldots, x_n] \) generated by the \( x_i \). We further see that if \( f \in k[x_1, \ldots, x_n] \) has \( f^d \in I \) for some \( d \geq 1 \), then \( f^d(c_1, \ldots, c_n) = 0 \), so \( f(c_1, \ldots, c_n) = 0 \). This motivates the following definitions:

Definition 1.1. Given an ideal \( I \subseteq k[x_1, \ldots, x_n] \), we define \( V(I) \subseteq k^n \) to be the set of points \((c_1, \ldots, c_n)\) with \( f(c_1, \ldots, c_n) = 0 \) for all \( f \in I \).

Given a subset \( S \subseteq k^n \), we define \( I(S) \subseteq k[x_1, \ldots, x_n] \) to be the set of functions \( f \) such that \( f(c_1, \ldots, c_n) = 0 \) for all \((c_1, \ldots, c_n) \in S\).

Finally, if \( I \subseteq R \) is an ideal in a commutative ring, we set \( \text{rad}(I) := \{ f \in R : \exists d \geq 1, f^d \in I \} \), and say \( I \) is radical if \( \text{rad}(I) = I \).

From the preceding discussion, it is clear that \( I(S) \) is always an ideal, and indeed always a radical ideal. Less obvious but not difficult to see is that \( \text{rad}(I) \) is also an ideal. When \( k \) is algebraically closed, it works well to think of a variety as the zero set \( V(I) \) itself. Indeed, we have Hilbert’s Nullstellensatz (zero set lemma):

Theorem 1.2. Suppose \( k \) is algebraically closed. Then affine varieties \( V \subseteq k^n \) are in bijection with radical ideals \( I \subseteq k[x_1, \ldots, x_n] \), via the maps \( V \mapsto I(V) \) and \( I \mapsto V(I) \).

When \( k \) is not algebraically closed, it makes more sense to think of varieties in terms of the solutions not only in \( k^n \), but also in \( L^n \) for all extensions \( L/k \). After all, when we talk about the solutions of a polynomial like \( y^2 = x^3 - x \), we want to be able to think about the solutions not only over \( \mathbb{Q} \), but also over \( \mathbb{R} \) or \( \mathbb{C} \). The content of the Nullstellensatz is that it is enough to know the solutions over the algebraic closure, since we can recover the ideals of defining polynomials in that case, and the defining polynomials determine the zero sets over all field extensions. This point of view is further reinforced by the idea that we do not want to view \( x^2 + y^2 = -1 \) and \( y^2 = x^3 + 2 \) as defining the same varieties \( \mathbb{Q} \), even though neither of them has points over \( \mathbb{Q} \).

The solution to this is simple, and underlies the modern approach to algebraic geometry: to formalize varieties, work with the ideals, rather than the points in \( k^n \). Of course, it is still important to work with the geometry implicit in looking
at zero sets, and the ultimate goal is still to understand the zero sets better, but
the ideals are elevated to a central role. Ultimately, in order to avoid dependence
on imbeddings, one forgets the original polynomial ring, and thinks of an abstract
affine variety as determined by the quotient ring \( k[x_1, \ldots, x_n]/I \), where \( I \) is radical.

2. Monomial orders

Whether or not one’s interests are ultimately computational, it is difficult to work
in a field without being to at least work out examples occasionally, and this can
be surprisingly difficult in algebraic geometry. Basic questions about dealing with
polynomial rings and their ideals can be remarkably subtle to answer. One of the
most basic: given an ideal \( I \) generated by polynomials \( f_1, \ldots, f_m \in k[x_1, \ldots, x_n] \),
and another \( f \in k[x_1, \ldots, x_n] \), is \( f \) in \( I \)? Equivalently, does \( f \) map to 0 in \( R/I \)?
If, for instance, the \( f_i \) are all monomials, this question is easy to answer, but in
general, it’s not so obvious what to do. One could also ask how to test when two
ideals are equal, how to compute the dimension of a variety, and how to describe
the image of a map of varieties (implicitization). Groebner bases provide the basic
tool to answer all these questions.

The fundamental idea underlying Groebner bases is simply to reduce to the case
of ideals generated by monomials. The first step necessary is to have a notion of
“highest order term” in a polynomial. To this end, we define:

**Definition 2.1.** The **multidegree** of a monomial \( cx_1^{e_1} \cdots x_n^{e_n} \in k[x_1, \ldots, x_n] \) is
the integer tuple \((e_1, \ldots, e_n) \in \mathbb{Z}^n_{\geq 0}\). A **monomial order** on \( k[x_1, \ldots, x_n] \) is a well
ordering on \( \mathbb{Z}^n_{\geq 0} \) which is invariant under addition.

Given a monomial order, we compare the size of monomials by applying our
order to the multidegrees of the monomials; thus, monomials that differ by a scalar
multiple are considered to have the same size. Multiplication of monomials cor-
responds to addition of multidegrees, so a monomial order preserves size when we
multiply by a fixed monomial.

We have the following lemma:

**Lemma 2.2.** An order on \( \mathbb{Z}^n_{\geq 0} \) is a monomial order if and only if it is invariant
under addition and has the property that \((c_1, \ldots, c_n) \geq (0, \ldots, 0)\) for all \( c_i \).

The proof of the lemma is not difficult, if we assume the following:

**Lemma 2.3.** ("Dickson’s" lemma) Suppose \( S \subseteq \mathbb{Z}^n_{\geq 0} \) has the property that for all
\( c \in S \) and \( d \in \mathbb{Z}^n_{\geq 0} \), we have \( c + d \in S \). Then \( S \) can be written as a finite union of
sets of the form \( c + \mathbb{Z}^n_{\geq 0} \).

This can be proved directly, or is easily seen to be equivalent to Hilbert’s basis
theorem for monomial ideals in polynomial rings. Arguably, the proof of Hilbert’s
basis theorem is no harder than proving the lemma directly.

The most basic example of a monomial order is the following:

**Example 2.4.** The **lexicographic order** is determined by \((c_1, \ldots, c_n) > (d_1, \ldots, d_n)\)
if for the smallest \( i \) with \( c_i \neq d_i \), we have \( c_i > d_i \). Its name comes from the ordering
of words in a dictionary.

Note that if we reorder our variables, we get a different lexicographic order.
Oddly enough, the choice of monomial order can have a substantial impact on
computational complexity, and the lexicographic order tends to yield more complex calculations. However, it is important for certain applications. In any case, with a given monomial order, we immediately have a notion of leading terms of polynomials:

**Definition 2.5.** Suppose we have a monomial ordering on \( k[x_1, \ldots, x_n] \), and \( f \in k[x_1, \ldots, x_n] \). The leading term \( \text{LT}(f) \) of \( f \) (with respect to the chosen ordering) is the largest monomial occurring in \( f \). The multidegree of \( f \) is the multidegree of the leading term of \( f \). Given an ideal \( I \subseteq k[x_1, \ldots, x_n] \), the ideal of leading terms \( \text{LT}(I) \) is the ideal generated by the set of \( \text{LT}(f) \) for all \( f \in I \).

Note that the set of leading terms themselves don’t form an ideal because they are monomials, so to define \( \text{LT}(I) \) we are required to take the ideal they generate. However, \( \text{LT}(I) \) is (by definition) a monomial ideal, so it is easier to compute with than \( I \). If \( f_1, \ldots, f_m \) is a set of generators for \( I \), it is not necessarily the case that \( \text{LT}(f_1), \ldots, \text{LT}(f_m) \) generate \( \text{LT}(I) \). Indeed, this observation leads directly to the definition of a Groebner basis.

### 3. Groebner bases

We assume throughout this section that we have fixed a monomial order on \( k[x_1, \ldots, x_n] \). Given such an order, we can make the following definition:

**Definition 3.1.** Suppose we are given an ideal \( I \subseteq k[x_1, \ldots, x_n] \). A Groebner basis for \( I \) is a set \( g_1, \ldots, g_d \in I \) such that \( \text{LT}(g_1), \ldots, \text{LT}(g_d) \) generate \( \text{LT}(I) \).

The term “Groebner basis” is really two lies for the price of one: it was not invented by Groebner but by his student Buchberger, and it is not a basis since it incorporates no minimality or “linear independence” condition. But “Buchberger generating set” just doesn’t have the same ring to it. However, we will see shortly that a Groebner basis for \( I \) does at least have the property that it generates \( I \).

Note that it follows from Dickson’s lemma that every ideal \( I \) has a Groebner basis, since \( \text{LT}(I) \) is a monomial ideal and therefore finitely generated.

Having defined Groebner bases, we are faced with two obvious questions: can we write them down explicitly, and are they useful? We now proceed to answer both questions in the affirmative, beginning by developing some of the basic properties of Groebner bases. The key idea involves a generalization of the division algorithm for polynomials in one variable to polynomials in more than one variable. If we have \( f, g \in k[x] \) single variable polynomials, we can describe the process of dividing \( f \) by \( g \) as follows: if the leading term of \( g \) divides the leading term of \( f \), there is a unique monomial multiple of \( g \) making the leading terms agree, and we subtract it off. Repeating the process, we end up with the remainder \( r \), whose leading term is not divisible by the leading term of \( g \), and the quotient \( q \), obtained by collecting all the monomials we used to subtract off multiples of \( g \).

We note that the remainder when \( f \) is divided by \( g \) is 0 if and only if \( f \) is in the ideal generated by \( g \). We would like to generalize this to multiple polynomials in multiple variables.

**Definition 3.2.** Suppose we have an ordered tuple of non-zero polynomials \( (g_1, \ldots, g_d) \in k[x_1, \ldots, x_n]^d \), and an additional polynomial \( f \in k[x_1, \ldots, x_n] \). The division algorithm for dividing \( f \) by \( (g_1, \ldots, g_d) \) is an algorithm for writing \( f = q_1g_1 + \cdots + q_dg_d + r \), where \( r \) has the property that none of its monomials are divisible by the leading term of any of the \( g_i \). The division algorithm is:
\begin{proof}
It is clear that (2) implies (1). In the division algorithm with all \(g_i\) monomials we will always subtract off one monomial at a time from \(f\), so it also clear that (3) implies (2). Finally, if \(f \in I\), we have \(f = q_1g_1 + \cdots + q_dg_d\) for some \(q_i\), and if we isolate the monomials of a fixed multidegree, we find each monomial of \(f\) can be written as \(q_i'g_1 + \cdots + q_d'g_d\) for monomials \(q_i'\) with each \(q_i'g_i\) having the same multidegree as the chosen monomial of \(f\). At least one \(q_i'\) must be non-zero, so we find at least one \(g_i\) divides the given monomial of \(f\). Thus we conclude that (1) implies (3).
\end{proof}

\begin{proposition}
Given an ideal \(I \subseteq k[x_1, \ldots, x_n]\) and a Groebner basis \(g_1, \ldots, g_d\) for \(I\), we have that the \(g_i\) generate \(I\).

Moreover, given any \(f \in k[x_1, \ldots, x_n]\), there exists a unique \(r\) such that \(f = q_1g_1 + \cdots + q_dg_d + r\), with no monomial in \(r\) divisible by any \(\text{LT}(g_i)\). In particular, \([f : (g_1, \ldots, g_d)]\) is independent of the order of the \(g_i\), and equal to 0 if and only if \(f \in I\).

Together with the earlier observed existence of Groebner bases, this proposition implies that every polynomial ideal is finitely generated. Thus, assuming a direct proof of Dickson’s lemma, we have given a proof of Hilbert’s basis theorem in the case of polynomial rings over fields. Of course, we emphasize that Hilbert’s theorem is more general, and the general proof is also simpler.
More importantly, this proposition says that if we have a Groebner basis for \( I \), we can use it to test algorithmically whether any given \( f \) lies in \( I \).

**Proof.** First note that by Lemma 3.3 applied to the LT\((g_i)\) as generators of LT\((I)\), if \( r \in I \) is any non-zero element, then LT\((g_i)|\)LT\((r)\) for some \( i \). It follows immediately that if \( f \in I \), we have \([f : (g_1, \ldots, g_d)] = 0\), so the \( g_i \) generate \( I \). Moreover, if we have

\[
f = q_1g_1 + \cdots + q_dg_d + r = q'_1g_1 + \cdots + q'_dg_d + r',
\]

then \( r - r' \in I \) and has no monomials divisible by any LT\((g_i)\), so we conclude \( r = r' \), giving the desired uniqueness assertion.

Finally, since \([f : (g_1, \ldots, g_d)]\) satisfies the conditions for \( r \), which are independent of order, we conclude the last statement as well. \( \square \)

4. Buchberger’s algorithm

We now move on to the question of how to tell whether a given generating set is a Groebner basis, and how to construct Groebner bases. We continue with our blanket assumption that we have chosen a monomial order on \( k[x_1, \ldots, x_n] \). We begin with a preliminary definition:

**Definition 4.1.** Given any non-zero \( f, g \in k[x_1, \ldots, x_n] \), denote by \( S(f, g) \) the polynomial \( \frac{L(f)}{\text{LT}(f)} - \frac{L(g)}{\text{LT}(g)} \), where \( L \) is the monic least common multiple of \( \text{LT}(f) \) and \( \text{LT}(g) \).

A basic lemma justifying the definition is:

**Lemma 4.2.** Suppose \( f_1, \ldots, f_m \in k[x_1, \ldots, x_n] \) have the same multidegree, and we have some linear combination

\[
c_1f_1 + \cdots + c_nf_m
\]

with the \( c_i \) in \( k \), having strictly smaller multidegree. Then we have \( b_1, \ldots, b_{m-1} \in k \) such that

\[
c_1f_1 + \cdots + c_nf_m = b_1S(f_1, f_2) + \cdots + b_{m-1}S(f_{m-1}, f_m).
\]

We leave the proof of the lemma as an exercise for the reader.

The main result classifying Groebner bases is the following:

**Theorem 4.3.** Given an ideal \( I \subseteq k[x_1, \ldots, x_n] \) and \( g_1, \ldots, g_d \) generating \( I \), the following are equivalent:

1. \( g_1, \ldots, g_d \) is a Groebner basis for \( I \);
2. \([S(g_i, g_j) : (g_1, \ldots, g_d)] = 0\) for all \( i \neq j \);
3. given any \( f \in k[x_1, \ldots, x_n] \), the remainder \([f : (g_1, \ldots, g_d)]\) is independent of the order of the \( g_i \), and equal to 0 if and only if \( f \in I \);
4. given any \( f \in k[x_1, \ldots, x_n] \), there exists a unique \( r \) such that for some \( q_i \) we have \( f = q_1g_1 + \cdots + q_dg_d + r \), with no monomial in \( r \) divisible by any \( \text{LT}(g_i) \).

(2) is known as Buchberger’s criterion.

**Proof.** We have already seen (1) \( \Rightarrow \) (4) \( \Rightarrow \) (3) in Proposition 3.4. Moreover, it is also clear that (3) implies (2) since \( S(g_i, g_j) \in I \).

Finally, we are left with the hard part: checking that (2) implies (1). Suppose we have \( f \in I \); we want to see that LT\((f)\) is in the ideal generated by the LT\((g_i)\).
We can write \( f = q_1g_1 + \cdots + q dg_d \), and of all such representations of \( f \), we assume we have chosen the one minimizing the maximum multidegree of the \( q ig_i \). Denote this maximal multidegree by \( d \in \mathbb{Z}_{\geq 0}^n \), and let \( i_1, \ldots, i_m \) be the indices for which the multidegree of \( q ig_i \) is \( d \). Then we can write

\[
f = q_1g_1 + \cdots + q dg_d = \sum_{j=1}^{m} \text{LT}(q_{i_j})g_{i_j} + \sum_{j=1}^{m} (q_{i_j} - \text{LT}(q_{i_j}))g_{i_j} + \sum_{j \notin \{i_1, \ldots, i_m\}} q_jg_j.
\]

We claim that the multidegree of \( f \) must be equal to \( d \). Clearly, it cannot be greater, so suppose it is strictly smaller. Then \( f \) and the last two sums must have multidegree strictly less than \( d \), so it follows that \( \sum_{j=1}^{m} \text{LT}(q_{i_j})g_{i_j} \) also has multidegree strictly less than \( d \). By Lemma 4.2, we conclude that \( \sum_{j=1}^{m} \text{LT}(q_{i_j})g_{i_j} = \sum_{j=1}^{m-1} b_jS(\text{LT}(q_{i_j})g_{i_j}, \text{LT}(q_{i_{j+1}})g_{i_{j+1}}) \) for some constants \( b_j \). Now, it is clear that each \( S(\text{LT}(q_{i_j})g_{i_j}, \text{LT}(q_{i_{j+1}})g_{i_{j+1}}) \) has multidegree strictly less than \( d \), and one easily sees that it must be a monomial times \( S(g_{i_j}, g_{i_{j+1}}) \). On the other hand, the hypothesis that \( [S(g_{i_j}, g_{i_{j+1}}) : (g_1, \ldots, g_d)] = 0 \) implies that we can write \( S(g_{i_j}, g_{i_{j+1}}) = \sum q'_{i_j}g_{i_j} \), where each \( q'_{i_j}g_{i_j} \) has multidegree less than or equal to the multidegree of \( S(g_{i_j}, g_{i_{j+1}}) \). We conclude that each \( S(\text{LT}(q_{i_j})g_{i_j}, \text{LT}(q_{i_{j+1}})g_{i_{j+1}}) \) can be written as a combination of the \( g_i \) with each term having multidegree strictly less than \( d \), which means we can rewrite our expression for \( f \) as a combination of the \( g_i \) having multidegree strictly less than \( d \), contradicting our assumed minimality. We have thus proved our claim that \( f \) must have multidegree \( d \).

But then it is clear by taking the terms of multidegree \( d \) that we have

\[
\text{LT}(f) = \sum_{j=1}^{m} \text{LT}(q_{i_j}) \text{LT}(g_{i_j}),
\]

and \( \text{LT}(f) \) is in the ideal generated the \( \text{LT}(g_i) \), as desired.  

As a corollary of the theorem, we also have an algorithm for starting with any generating set for \( I \) and producing a Groebner basis:

**Corollary 4.4. (Buchberger’s algorithm)** Given a set of generators \( f_1, \ldots, f_d \) for an ideal \( I \), we can produce a Groebner basis for \( I \) using the following algorithm:

1. Start with \( g_1, \ldots, g_d = f_1, \ldots, f_d \).
2. (For each \( 1 \leq j < \ell \leq d' \), compute \( r_{j,\ell} := [S(g_j, g_\ell) : (g_1, \ldots, g_{d'})] \). If \( r_{j,\ell} \neq 0 \), add \( S(g_j, g_\ell) \) to the \( g_\ell \), increment \( d' \), and start over at the beginning of (1). Otherwise, continue to the next pair \( j < \ell \).)
3. (If \( r_{j,\ell} = 0 \) for all \( j < \ell \), stop.)

**Proof.** Since we start with a set of generators for \( I \), by Buchberger’s criterion we see that if the algorithm terminates, we have obtained a Groebner basis. But we note that if \( r_{j,\ell} \neq 0 \), then \( \text{LT}(r_{j,\ell}) \) is not in the ideals generated by the \( \text{LT}(g_i) \). Indeed, no monomial in \( r_{j,\ell} \) is divisible by any \( \text{LT}(g_i) \) by definition, so the assertion follows from Lemma 3.3 applied to the ideal generated by the \( \text{LT}(g_i) \). We thus see that each time we add an element to the \( g_\ell \), we strictly increase the ideal generated by the \( \text{LT}(g_\ell) \). But we cannot have an infinite strictly ascending chain of ideals (their union would be an ideal, which is necessarily finitely generated), so we see that the algorithm must terminate, as desired.  

\[\square\]
5. First applications

We summarize what we have found: given an ideal \( I \subseteq k[x_1, \ldots, x_n] \) generated by some \( f_1, \ldots, f_m \), if we choose any monomial order on \( k[x_1, \ldots, x_n] \), we can use Buchberger’s algorithm to produce a Groebner basis \( g_1, \ldots, g_d \) for \( I \). We can then use the division algorithm with the \( g_i \) to test membership in \( I \): any \( f \) lies in \( I \) if and only if \([ f : (g_1, \ldots, g_d)] = 0 \). In particular, we see we can test algorithmically whether \( I = k[x_1, \ldots, x_n] \), or equivalently, whether \( 1 \in I \). We conclude

**Corollary 5.1.** If \( k \) is algebraically closed, and we have polynomials \( f_1, \ldots, f_m \in k[x_1, \ldots, x_n] \), we have an algorithm to test whether the \( f_i \) have a common solution.

**Proof.** Indeed, by Hilbert’s Nullstellensatz, the \( f_i \) have a common solution if and only if the ideal they generate is all of \( k[x_1, \ldots, x_n] \), which we have just seen we can use Groebner bases to test algorithmically. \( \square \)

We also see:

**Corollary 5.2.** If \( I, I' \subseteq k[x_1, \ldots, x_n] \) are ideals generated by \( f_1, \ldots, f_m \) and \( f'_1, \ldots, f'_m \), we have an algorithm to test whether \( I = I' \).

**Proof.** Indeed, we can test \( I \subseteq I' \) by using Groebner bases to test whether each \( f_i \) is in \( I' \), and we can test \( I' \subseteq I \) similarly. \( \square \)

Geometrically, this almost corresponds to testing whether two sets of equations define the same variety, but not quite – varieties correspond to radical ideals, so for the geometric version we want to test whether \( I \) and \( I' \) have the same radical. This may be accomplished with the help of the following theoretical proposition:

**Proposition 5.3.** Given \( I \subseteq k[x_1, \ldots, x_n] \), and any \( f \in k[x_1, \ldots, x_n] \), then \( f \in \text{rad}(I) \) if and only if the ideal generated by \( I \) together with \( 1 - tf \) in \( k[x_1, \ldots, x_n, t] \) is equal to all of \( k[x_1, \ldots, x_n, t] \).

For the proof of this proposition, see Dummit and Foote, Proposition 34 of Chapter 15.

**Corollary 5.4.** If \( I, I' \subseteq k[x_1, \ldots, x_n] \) are ideals generated by \( f_1, \ldots, f_m \) and \( f'_1, \ldots, f'_m \), we have an algorithm to test whether \( \text{rad}(I) = \text{rad}(I') \).

**Proof.** We observe that \( \text{rad}(I) = \text{rad}(I') \) if and only if \( I \subseteq \text{rad}(I') \) and \( I' \subseteq \text{rad}(I) \), since if \( I \subseteq \text{rad}(I') \), we must have \( \text{rad}(I) \subseteq \text{rad}(I') \), because \( \text{rad}(I) \) is the smallest radical ideal containing \( I \). We then argue as before: using the proposition and Groebner bases, we can test whether each \( f_i \) is in \( \text{rad}(I') \), and vice versa. \( \square \)

6. A brief survey of elimination theory and applications

When attempting to solve several equations in several variables, it is natural to try to manipulate the equations to eliminate variables, ultimately finding a solution by solving for one variable at a time. This is the basis for Gaussian elimination in solving linear equations, and may also be applied to solving polynomial equations, albeit with more limited success. This is the subject of elimination theory. It occasionally works to provide closed solutions of polynomial equations, but also turns out to be an important theoretical tool, giving us algorithms to perform various computations of interest.
One of the distinguishing factors of algorithms based on elimination theory is that unlike anything we have done previously, we are forced to use a particular monomial order – namely, the lexicographic order. Therefore, whenever we mention Groebner bases in this section, it should be understood that we work with the lexicographic order (although we will sometimes make explicit the order of the variables). The basic definition of elimination theory is:

**Definition 6.1.** Suppose \( I \subseteq k[x_1, \ldots, x_n] \) is an ideal. For \( 0 \leq i \leq n \), we define the \( i \)th elimination ideal of \( I \) to be the ideal of \( k[x_{i+1}, \ldots, x_n] \) given by \( I \cap k[x_{i+1}, \ldots, x_n] \).

The \((n-1)\)st elimination ideal is then precisely the set of polynomials involving only \( x_n \) which can be obtained by manipulating a set of generators for \( I \). If one solves the polynomial generating the \((n-1)\)st ideal, one can plug values of \( x_n \) into the polynomials generating the \((n-2)\)nd elimination ideal, and attempt to solve for \( x_{n-1} \), and so forth. The point, of course, is that Groebner bases can be used to compute elimination ideals:

**Proposition 6.2.** Given a Groebner basis \( g_1, \ldots, g_d \) for \( I \), the \( i \)th elimination ideal has \( \{g_1, \ldots, g_d\} \cap k[x_{i+1}, \ldots, x_n] \) as a Groebner basis.

This is Proposition 29 of Chapter 9 of Dummit and Foote.

If a system of polynomial equations has a finite (non-empty) solution set, and if the single-variable polynomials one runs into at each stage are amenable to explicit solution (for instance, if they have degree at most 4, or if we get lucky), this process will work. Otherwise, however, we will quickly get stuck, as elimination ideals will be 0, or we will have polynomials we can’t solve in closed form.

Forgoing examples of using elimination theory to compute solutions, we move on to theoretical applications. The first is a simple one:

**Proposition 6.3.** If \( I, I' \subseteq k[x_1, \ldots, x_n] \) are a pair of ideals, we can compute \( I \cap I' \) as the first elimination ideal of \( tI + (1 - t)I' \subseteq k[t, x_1, \ldots, x_n] \), under the variable order \( t > x_1 > \ldots x_d \).

See Dummit and Foote, Proposition 30 of Chapter 9 for the proof. Geometrically, this proposition can be interpreted to calculate the polynomial defining a union of two varieties, although the fact that radicals aren’t involved makes it somewhat finer.

We now move on to a more substantive application, to implicitization. The idea here is that we have a map of varieties, and we want to know what polynomials cut out the image of the map. More precisely, we have:

**Proposition 6.4.** Suppose \( k \) is algebraically closed, and we have varieties \( V \subseteq k^n \) and \( V' \subseteq k^{n'} \), and a map \( f : V \rightarrow V' \) given by \( n' \) polynomials \( f_1, \ldots, f_{n'} \in k[x_1, \ldots, x_n] \). Suppose \( I(V) \) is generated by \( g_1, \ldots, g_d \), and \( I(V') \) is generated by \( g_1', \ldots, g_{d'}' \). Thus \( f \) induces a map

\[
   f^* : k[x_1', \ldots, x_{n'}']/\langle g_1', \ldots, g_{d'}' \rangle \rightarrow k[x_1, \ldots, x_n]/\langle g_1, \ldots, g_d \rangle.
\]

Then we have

\[
   I(f(V)) = (\ker f^*, I(V')).
\]

Note that the condition for the \( f_i \) to induce a well-defined map is that \( g_i'(f_1, \ldots, f_{n'}) \in I(V) \) for each \( i \). For a proof of the proposition, see Proposition 16 of Chapter 15 of Dummit and Foote.
This proposition implies formally that \( f(V) \) is “Zariski dense” in \( V(\ker f^\# , I(V')) \), but this is a rather weak statement. For instance, in cases like \( k = \mathbb{C} \) where we have a classical topology to consider, it does not imply that \( f(V) \) is dense in \( V((\ker f^\#, I(V')) \) in the complex topology. However, much more is true: Chevalley’s theorem states that \( f(V) \) can be written as a finite sequence of complements and unions of nested subvarieties, and in particular \( f(V) \) is in fact dense in \( V((\ker f^\#, I(V')) \) in the complex topology when \( k = \mathbb{C} \).

In any case, the proposition motivates a desire to compute kernels of maps of (quotients of) polynomial rings, and again we can apply elimination theory:

**Proposition 6.5.** Suppose we have a ring map

\[
 f^\#: k[x'_1, \ldots , x'_n]/(g'_1, \ldots , g'_d) \to k[x_1, \ldots , x_n]/(g_1, \ldots , g_d)
\]

given by \( n' \) polynomials \( f_1, \ldots , f_{n'} \in k[x_1, \ldots , x_n] \). Then \( (\ker f^\#, (g'_1, \ldots , g'_d)) \) is the \( n \)th elimination ideal of the ideal generated by \( x'_1 - f_1, \ldots , x'_n - f_{n'} \) in the ring \( k[x_1, \ldots , x_n, x'_1, \ldots , x'_n] \), where the variables are ordered \( x_1 < \cdots < x_n < x'_1 < \cdots < x'_n \).

See Proposition 8 of Chapter 15 of Dummit and Foote.

We conclude by describing how elimination theory may be used to compute the dimension of a variety. We first recall the relevant definitions from algebraic geometry:

**Definition 6.6.** A variety is **irreducible** if it cannot be written as the union of two smaller varieties, neither contained in the other. The **dimension** of a variety \( V \) is one less than the length of the longest chain of irreducible varieties contained in \( V \).

Thus, a point has dimension 0, a curve in the plane has dimension 1, and so forth. Typically, adding an equation reduces the dimension of the corresponding variety by 1, but this is not always the case, and indeed some varieties require more equations to define than you would expect. Every variety can be written as a finite union of irreducible varieties, which correspond to prime ideals. Since different irreducible components of a variety can have different dimension, we typically focus our attention on computing the dimension of an irreducible variety. This can be computed by elimination theory as follows:

**Proposition 6.7.** Suppose \( V \) is an irreducible variety corresponding to the prime ideal \( P \), and let \( P_i \) be the \( i \)th elimination ideal of \( P \). Then the dimension of \( V \) is equal to the number of \( i \) such that \( P_{i-1} \subseteq k[x_1, \ldots , x_n] \) is equal to the ideal generated by \( P_i \) inside \( k[x_1, \ldots , x_n] \).

The geometry here is that we project \( V \) repeatedly, and at each stage, either the dimension stays the same (if the fibers of projection are generically 0-dimensional), or drops by 1 (if the fibers are each equal to the entire affine line). The content of the proposition is then that the fibers are the entire affine line precisely when \( P_{i-1} \) is the ideal generated by \( P_i \); see Exercise 29 of §15.4 of Dummit and Foote.