APPLICATIONS OF GRÖBNER BASES

SARAH BENNETT

Abstract. This paper will provide a brief introduction to Gröbner bases and some of their applications: identifying and proving geometric theorems, solving coloring problems, and computing minimal polynomials.

Contents

1. Background

We will work with ideals of polynomial rings with coefficients in a field F of characteristic 0. As we will see, Gröbner bases are a particularly useful generating set with many interesting and unexpected applications. The construction in this section follows the construction in [CLO] chapter 2 and [DF] section 9.6

Definition 1.1. The ideal of leading terms of a polynomial ideal I, denoted $LT(I)$, is the ideal generated by the leading terms of the polynomials of I. To avoid confusion, the notation $lt(f)$ will be used to refer to the leading term of an individual polynomial, while $LT(I)$ will refer to the leading term ideal of I.

Of course, the leading term of a polynomial will depend on the order in which the terms of the polynomial are written. Thus, before any calculation can be made, one must specify a well-ordering on the monomials of the ideal and list the polynomials according to that order. For the purposes of this paper, we will use the lexicographic order $x_1 > x_2 > \ldots > x_n$, called the lex order, unless otherwise specified.

Example 1.2. In the lex order $x > y$, the following inequalities hold:

(1) $x > y$
(2) $x > y^2$
(3) $x^2 > x$
(4) $x^2 > xy^2$

Definition 1.3. A Gröbner basis for an ideal I in $F[x_1, \ldots, x_n]$ is a generating set $G = \{g_1, \ldots, g_m\}$ such that $\{lt(g_i) : 1 \leq i \leq n\}$ generates $LT(I)$.

Theorem 1.4. *(Hilbert Basis Theorem) If R is a Noetherian ring, then the polynomial ring $R[x_1, \ldots, x_n]$ is also Noetherian. [CLO ch2.5]*

A Gröbner basis for an ideal I is unique among the other generating sets because Gröbner bases have the following property:

Date: August 22, 2008.

Theorem 1.5. *Fix a monomial ordering on $R = F[x_1, \ldots, x_n]$ and let $G = \{g_1, \ldots, g_m\}$ be a Gröbner basis for a non-zero ideal I in R. Then*

1. *If f is in R, there is a unique f_1 in I and r in R so that $f = f_1 + r$ where no monomial in r is divisible by any leading term $lt(g_i)$*
2. *f_1 and r can be computed by polynomial division by the elements of the Gröbner basis, and the order in which these polynomials are used does not impact the f_1 and r.*
3. *The remainder r is a unique representative of the coset of f in $F[x_1, \ldots, x_n]/I$. In particular, f is an element of I if and only if $r = 0$.*

Proof. By general polynomial division, $f = \sum_{i=1}^{m}(q_i g_i) + r$, and $\sum_{i=1}^{m}(q_i g_i)$ is in I, so let $f_1 = \sum_{i=1}^{m}(q_i g_i)$. To show uniqueness, suppose $f = f_1 + r = f_1' + r'$. Then $r - r' = f_1' - f_1$ which is an element of I, so $lt(r - r')$ is in $LT(I)$, and thus $lt(r - r)$ is a sum of multiples of the leading terms of $\{g_1, \ldots, g_m\}$. However, by definition of remainder, r and r' and thus $r - r'$ are sums of monomial terms none of which is divisible by any $lt(g_i)$, so $r - r' = 0$. But then $r = r'$ and $f_1 = f_1' = f - r$, so the decomposition is unique. This uniqueness proves that the order in which the division occurs does not affect the final result, completing the proofs of 1 and 2.

Further, since r is unique, it provides a unique representative of the coset of f in $F[x_1, \ldots, x_n]/I$. If $r = 0$, then $f = f_1$ and f_1 is an element of I, so f is an element of I. If f is in I, then $f = f_1 + 0$ for $f = f_1$ and uniqueness of r implies that $r = 0$. □

It remains to show that Gröbner bases exist. In fact, Gröbner bases exist for all ideals of polynomial rings with coefficients in a field. To show this, we first need a lemma:

Lemma 1.6. *If I is a non-zero ideal in $F[x_1, \ldots, x_n]$ and I is generated by a set of polynomials S, then I is generated by a finite subset of S.*

Proof. By the Hilbert Basis Theorem, I is generated by a finite set of polynomials $\{f_1, \ldots, f_k\}$ (not necessarily in S). Since I is generated by S, we know that if f_i is in I, $f_i = \sum_{j=1}^{l} \alpha_j q_j$ where α_j is an element of F and q_j is an element of S. Then the set $\cup_{i=1}^{k}\{q_j\}$ is a finite generating set for I. □

Theorem 1.7. *Fix a monomial ordering on $R = F[x_1, \ldots, x_n]$ and let I be a non-zero ideal in R. Then*

1. *If $g_1, \ldots, g_m$ are elements of I such that $LT(I) = \langle lt(g_1), \ldots, lt(g_m)\rangle$, then $\{g_1, \ldots, g_m\}$ is a Gröbner basis for I.*
2. *I has a Gröbner basis.*

Proof. Let $g_1, \ldots, g_m$ be in I such that $LT(I) = \langle lt(g_1), \ldots, lt(g_m)\rangle$. Let f be an element of I. Then by general polynomial division, $f = \sum_{i=1}^{m}(q_i g_i) + r$. Now, r is an element of I since f is an element of I, but then $lt(r)$ is in $LT(I)$ and is divisible by one of the leading terms of $\{g_i\}$. This contradicts the definition of remainder unless $r = 0$, so $f = \sum_{i=1}^{m}(q_i g_i)$ and $\{g_1, \ldots, g_m\}$ generate I and is a Gröbner basis for I.

Next, note that $LT(I)$ is a monomial ideal generated by a set of monomials - specifically the leading terms of the polynomials in I. Then, by the previous lemma, there

is a finite subset $\{g_1, \ldots, g_m\}$ generating I, and by (1) this is a Gröbner basis for I. □

Gröbner bases are only of use if we can compute them, however. While for most ideals, computation of the Gröbner basis by hand is too long to be practical, there are algorithms that make it possible to compute the Gröbner basis by computer.

Definition 1.8. The S-polynomial of two polynomials f_1, f_2 is given by

$$S(f_1, f_2) = \frac{M}{LT(f_1)} f_1 - \frac{M}{LT(f_2)} f_2$$

where M is the least common multiple of $LT(f_1)$ and $LT(f_2)$.

Theorem 1.9. *(Buchberger's Criterion) Fix a monomial ordering on $R = F[x_1, \ldots, x_n]$. If $I = (g_1, \ldots, g_m)$ is a non-zero ideal in R, then $G = \{g_1, \ldots, g_m\}$ is a Gröbner basis for I if and only if $S(g_i, g_j) \equiv 0$ mod G for $1 \leq i < j \leq m$. [CLO ch2.7]*

This will not necessarily give a unique Gröbner basis. Changing the order in which the terms of G are listed can change the resulting set, and there is no provision for removing redundant terms. To find a unique generating set, called a *reduced Gröbner basis*, we eliminate g_i from G if there is a $j < i$ such that $LT(g_j)$ divides $LT(g_i)$.

Example 1.10. To find the reduced Gröbner basis for the ideal

$$I = (x^2 - y, xy - y, x - y^2) \subset F[x, y],$$

we let $x > y$ in the lexicographic order and denote:

$$f_1 = x^2 - y$$
$$f_2 = xy - y$$
$$f_3 = x - y^2$$

Let $G = \{f_1, f_2, f_3\}$. Then

$$\begin{aligned} S(f_1, f_2) &= y f_1 - x f_2 \\ &= xy - y^2 \\ &\equiv -y^2 + y \end{aligned}$$

$$\begin{aligned} S(f_1, f_3) &= f_1 - x f_3 \\ &\equiv y^2 - y \end{aligned}$$

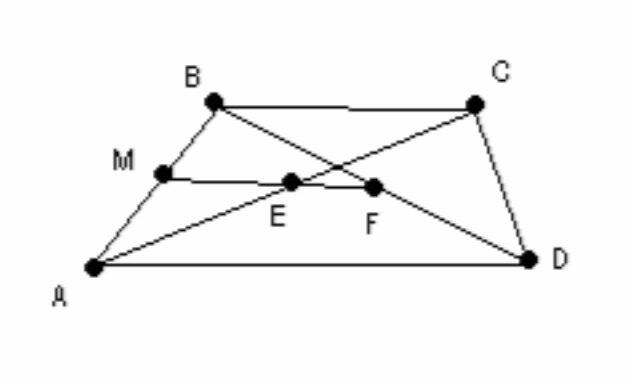
$$\begin{aligned} S(f_2, f_3) &= f_2 - y f_3 \\ &\equiv y^3 - y \end{aligned}$$

where all the equivalences are modulo the set G. Note that $-y^2 + y \equiv y^2 - y$ mod G, since $S(-y^2 + y, y^2 - y) = 0$. Further, we can reduce the generating set because $lt(f_3)$ divides $lt(f_1)$, and $lt(f_2)$ and $lt(y^2 - y)$ divide $lt(y^3 - y)$. Now, we revise the set G, adding the remainders we obtained from the S-polynomial and removing the reducible terms. This gives $G' = \{f_3, y^2 - y\}$. G' is then the reduced Gröbner basis generating I.

2. Geometric Theorem Proving and Discovery

One surprising application of Gröbner bases is their ability to prove and discover geometric theorems. If the conclusion polynomials all belong to the ideal generated by the hypothesis polynomials, then they are true, as are all geometric statements corresponding to polynomials in the ideal. This application is presented in [W].

Example 2.1. We will use Gröbner bases to show that if E is the midpoint of $\overline{AC}$, F is the midpoint of $\overline{BD}$, and M is the intersection of $\overline{AB}$ and $\overline{EF}$ in the figure below, then M is the midpoint of $\overline{AB}$. We will use Gröbner bases to show that if



E is the midpoint of $\overline{AC}$, F is the midpoint of $\overline{BD}$, and M is the intersection of $\overline{AB}$ and $\overline{EF}$ in the figure above, then M is the midpoint of $\overline{AB}$.
First, assign coordinates to the points $A - M$ as follows:

$$\begin{aligned} A &= (x_1, 0) \\ B &= (x_3, x_4) \\ C &= (x_5, x_4) \\ D &= (x_2, 0) \\ E &= (x_6, x_7) \\ F &= (x_8, x_9) \\ M &= (x_{10}, x_{11}). \end{aligned}$$

Note that the choice of coordinates means that our figure is a quadrilateral with two parallel sides. The polynomials in $\mathbb{Q}[x_1, \ldots, x_n, y]$ corresponding to the figure are:

$$\begin{aligned} h_1 &= 2x_6 - x_5 - x_1 = 0 \\ h_2 &= 2x_7 - x_4 = 0 \\ h_3 &= 2x_8 - x_3 - x_2 = 0 \\ h_4 &= 2x_9 - x_4 = 0 \\ h_5 &= (x_8 - x_6)x_{11} - (x_9 - x_7)x_{10} + x_6x_9 - x_7x_8 = 0 \\ h_6 &= (x_3 - x_1)x_1 1 - x_4(x_{10} - x_1) = 0 \\ h_7 &= x_4z - 1 = 0. \end{aligned}$$

The first two polynomials correspond to the statement E is the midpoint of $\overline{AC}$; the first for the x coordinate and the other for the y coordinate. The second two correspond to the analogous statement for F, the third pair to to definition of M as the intersection of $\overline{AB}$ and $\overline{EF}$, and the final polynomial, with the introduction of a new variable z, to the statement $x_4 \neq 0$ - namely, our quadrilateral is not a straight line.
The conclusion of the theorem is also represented by two polynomials,with the first again representing the x-coordinate and the second the y-coordinate:

$$c_1 = 2x_{10} - x_3 - x_1 = 0 c_2 \qquad\qquad = 2x_{11} - x_4 = 0.$$

When we compute the reduced Gröbner basis for the ideal generated by the polynomials $h_1, \ldots, h_7$ we obtain

$$G = \{h_1, \ldots, h_4, (x_5 - x_3 - x_2 + x_1)(2x_{10} - x_3 - x_1),$$
$$h_6, 2(x_5 - x_2)x_{11} - x_4(2x_{10} + x_5 - x_3 - x_2 - x_1), h_7\}.$$

We can use the ability of Gröbner bases to determine ideal membership to decide whether or not the polynomial equivalents of our conclusion are in the ideal. Since the two conclusion polynomials do not reduce to 0 mod G and the theorem can be verified by elementary geometry, we know that we are missing a condition. To discover the missing condition, we turn to another form of reducing a set of polynomials:

Definition 2.2. Consider the set S of polynomials of leading variable x_i in $F[x_1, \ldots, x_n]$ and choose the polynomial b_i of minimal degree in x_i. Then the q-basic set of S is $\{b_i : 1 \leq i \leq n\}$.

Example 2.3. Consider the set

$$S = \{x_1^2 + 2x_2, x_1x_2 + x_2^3, x_2^2 + x_2x_3^2, x_2^2 + x_3\}$$

under the lex order $x_1 > x_2 > x_3$. Then

$$b_1 = x_1x_2 + x_2^3$$
$$b_2 = x_1^2 + 2x^2$$
$$b_3 = x_2^2 + x_3$$

so the q-basic set of S is $B = \{b_1, b_2, b_3\}$.

We can compute the q-basic set of the Gröbner basis and use this as a second test. When we do so, we obtain the q-basic set

$$B = \{h_1, \ldots, h_4, (x_5 - x_3 - x_2 + x_1)(2x_{10} - x_3 - x_1), h_6\}.$$

In fact, both c_1 and c_2 are equivalent to 0 mod B, implying that they are true under additional conditions. The additional conditions are obtained from the leading coefficients of the polynomials in the q-basic set - provided that those are non-zero, the theorem is true.

Example 2.4. In the example of a q-basic set, the leading coefficient of b_1 is x_2, the leading coefficient of b_2 is 2, and the leading coefficient of b_3 is 1. Note that these are not necessarily the leading coefficients under the same polynomials in the order $x_1 > x_2 > x_3$, but rather the leading coefficients of the monomial they represent in the q-basic set.

The leading coefficients of $h_1, \ldots, h_4$ are all 2, but the leading coefficient of $(x_5 - x_3 - x_2 + x_1)(2x_{10} - x_3 - x_1)$ is $x_5 - x_3 - x_2 + x_1$ with respect to x_{10} and the leading coefficient of h_6 is $x_3 - x_1$ with respect to x_{11}. The new condition is thus that

$$2(x_5 - x_3 - x_2 + x_1)(x_3 - x_1) \neq 0$$

Since 2 is always non-zero, that imposes no new conditions on our figure. The condition $x_3 - x_1 \neq 0$ removes the case of a trapezoid with one pair of right angles, even though the theorem is still true under that condition. The last factor, however, can be rewritten as $(x_5 - x_3) - (x_2 - x_1)$, which is the polynomial interpretation of the geometric statement that $\overline{AB}$ is parallel to $\overline{CD}$. In this case, the figure is a parallelogram and it can be easily verified that E and F are, in fact, the same point. However, then the line $\overline{EF}$ is no longer uniquely determined and M could be any point on $\overline{AB}$.

3. Coloring of Graphs

Gröbner bases can be used to determine whether or not a system of equations has a solution, and thus are a simple way to solve the system of equations associated with graph colorings. The ideas and example in this section follow those in [AL] section 2.8 and [DF] exercise 45 in section 9.6.

Definition 3.1. We say a graph is n-colorable if we can assign one of n colors to each vertex so that no two vertices that are connected by an edge have the same color.

Consider a graph with k vertices. We assign a variable x_i to each vertex and an element α_i to each color. Then consider a field F containing the set $\{\alpha_i : 1 \leq i \leq n\}$. Define the function $f(x) = \prod_{i=1}^{n}(x - \alpha_i)$. Then a given $x_j = \alpha_j$ if $f(x_j) = 0$, so each vertex is colored. To distinguish between different colorings, note that if $\alpha_i \neq \alpha_j$ then $f(x_i) = f(x_j)$, where $x_i$and x_j are vertices colored by α_i and α_j, respectively. We want a function $g(x_i, x_j)$ such that $g(x_i, x_j) = 0$ when x_i, x_j represent vertices connected by an edge in the graph. The easy choice for g is then $g(x_i, x_j) = \frac{f(x_i) - f(x_j)}{x_i - x_j}$. It then suffices to solve the system of equations

$$f(x_i) = 0 \quad g(x_i, x_j) = 0 \qquad \text{for all } i, j \text{ such that } (i, j) \text{ is an edge in the graph.}$$

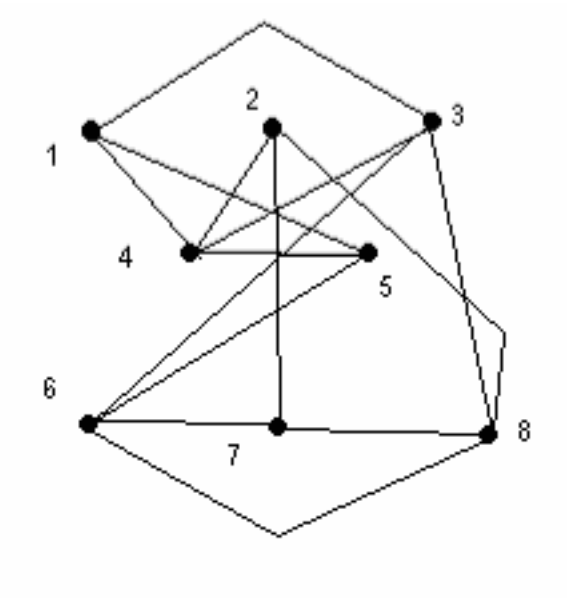
.

A solution to this system of equations corresponds to a coloring of the graph. We can use Gröbner bases to solve the system by calculating the Gröbner basis for the ideal generated by the equations. If, however, this ideal is not proper, then the following variant of the Nullstellansatz says that there is no solution. This means that if the Gröbner basis consists solely of the element (1), then there is no n-coloring of the graph.

Theorem 3.2. *(Hilbert's Nullstellensatz - Variant) An ideal I over a polynomial ring is proper if and only if there is a common zero in the zero set of the polynomials in I. [DF ch15.3]*

We can use this process to determine whether or not a graph has an n-coloring and to calculate any such coloring in the following manner:

Example 3.3. The graph on the following page is 3-colorable and has precisely two three colorings.



Since 3 is prime, we assign the values 0, 1, and 2 in an algebraic closure of $\mathbb{Z}/3\mathbb{Z}$ to the three colors. Without loss of generality, let $x_1 = 0$. Our ideal is generated by the polynomials $f(x) = x^3 - x$ and $g(x_i, x_j) = x_i^2 + x_i x_j + x_j^2 - 1$, evaluating g for only values of x_i, x_j such that the edge (i, j) is in the graph. Under the lex order $x_1 > \ldots > x_8$, we find a Gröbner basis

$$G = \{x_1, x_2, x_3 + x_8, x_4 + 2x_8, x_5 + x_8, x_6, x_7 + x_8, x_8^2 + 2\}.$$

Since 1 is not an element of G, we know that there is at least one 3-coloring of the graph. It is readily apparent that $x_1 = x_2 = x_6 = 0$. Since $1^2 + 2 = 3 \equiv 0 \pmod 3$ and $2^2 + 2 = 6 \equiv 0 \pmod 3$, x_8 could be either 1 or 2. Assume that $x_8 = 1$. Then $x_3 = x_5 = x_7 = 2$ and $x_4 = 1$. If $x_8 = 2$, then $x_3 = x_5 = x_7 = 1$ and $x_4 = 2$. Either map provides a valid 3-coloring of the graph.

4. Minimal Polynomials

For a slightly more algebraic application, Gröbner bases can be used to calculate the minimal polynomial of an algebraic element over a field extension. The ideas in this section follow [AL] section 2.4 and 2.6.

Lemma 4.1. *Let $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ be elements of a commutative ring R. Then $a_1 a_2 \cdots a_n - b_1 b_2 \cdots b_n$ is an element of the ideal $I = \langle a_1 - b_1, \ldots, a_n - b_n \rangle$*

Proof. The proof is by induction on n. Define $I_n = \langle a_1 - b_1, \ldots, a_n - b_n \rangle$. It is clearly true for $n = 1$. For $n = k$, note that $a_1 a_2 \cdots a_k - b_1 b_2 \cdots b_k = a_1(a_2 \cdots a_k - b_2 \cdots b_k) + (a_1 - b_1)(b_2 \cdots b_k)$ By the inductive hypothesis, $a_2 \cdots a_k - b_2 \cdots b_k$ is an element of I_{k-1}, so $a_1(a_2 \cdots a_k - b_2 \cdots b_k) + (a_1 - b_1)(b_2 \cdots b_k)$ is in I_k. □

Lemma 4.2. *Let I be an ideal of $k[x_1, \ldots, x_n]$, J an ideal of $k[y_1, y_m]$, ϕ a homomorphism $\phi : k[y_1, \ldots, y_m]/J \to k[x_1, \ldots, x_n]/I$ such that $\phi : y_i + J \mapsto f_i + I$ with f_i in $k[x_1, \ldots x_n]$. Let $K = \langle I, y_1 - f_1, \ldots, y_m - f_m \rangle$. Then $ker(\phi) = K \cap k[y_1, \ldots, y_m]$.*

Proof. Define

$$f'(y_1,\dots,y_m)=\sum_{i=1}^{m}(y_i-f_i(x_1,\dots,x_n))h_i(y_1,\dots,y_m,x_1,\dots,x_n) + w(y_1,\dots,y_m,x_1,\dots,x_n)$$

where

$$w(y_1,\dots,y_m,x_1,\dots,x_n)=\sum_j u_j(y_1,\dots,y_m,x_1,\dots,x_n)v_j(x_1,\dots,x_n)$$

with v_j in I and h_i and u_j in $k[y_1,\dots,y_m,x_1,\dots,x_n]$. Since the v_j are in I, we can write

$$w(f_1,\dots,f_m,x_1,\dots,x_n)=\sum j(u_j(f_1,\dots,f_m,x_1,\dots,x_n)v_j(x_1,\dots,x_n))\in I.$$

Then

$$\begin{aligned}\phi(f'+J)&=f'(f_1,\dots,f_m)+I\\&=w(f_1,\dots,f_m,x_1,x_n)+I\\&=0\end{aligned}$$

so $f'+J\in ker\phi$.
To prove the opposite inclusion, let f' be an element of $k[y_1,\dots,y_m]$ such that $\phi(f'+J)=0$. Then $f'(f_1,\dots,f_m)$ is in I. Define $f'(y_1,\dots,y_m)=\sum_j c_j y_1^{(}j_1)\cdots y_m^{(}j_m)$, with finitely many non-zero c_j and $j=(j_1,\dots,j_m)$ with each j_t in the natural. Then by adding and subtracting $f'(f_1,\dots,f_m)$ from $f'(y_1,\dots,y_m)$, we obtain

$$f'(y_1,\dots,y_m)=\sum_j c_j(y_1^{(}j_1)\cdots y_m^{(}j_m)-f_1^{(}j_1)\cdots f_m^{(}j_m))$$

which is in K by the previous lemma. □

Theorem 4.3. *Let $k\subset K$ be a field extension and let α be algebraic over k with minimal polynomial p. Let $f(x)=a_0+a_1x^1+\ldots+a_nx^n$ and $g(x)=b_0+b_1x^1+\ldots+b_mx^m$ and define β in $k(\alpha)$ so that*

$$\beta=\frac{f(\alpha)}{g(\alpha)}.$$

Let $J=\langle p,gy-f\rangle$ be an ideal in $k[x,y]$. Then the minimal polynomial of β over k is the monic polynomial generating the ideal $J\cap k[y]$.

Proof. First, note that the monic polynomial generating $J\cap k[y]$ is uniquely determined, since $k[y]$ is a PID.
Since $k[x]/\langle p\rangle$ is a field and $g(\alpha)$ is non-zero, there is some ℓ such that $g\ell-1\equiv 0 \pmod{<}p>$. Let $h=f\ell$ and note that $h(\alpha)=\beta$. Let ϕ is the composition of homomorphisms such that

$$\begin{aligned}\phi: k[y]\to k[x]/\langle p\rangle &\to^{\cong} k(\alpha)\\ y&\mapsto\ h+<p>\mapsto\beta.\end{aligned}$$

Since q is in kerϕ if and only if $q(\beta)=0$, it suffices to find the generator of kerϕ, since this will by definition divide all other elements in ker*phi*. By the previous lemma, $ker\phi=\langle p,y-h\rangle\cap k[y]$. We need to show

$$\langle p,y-h\rangle=\langle p,gy-f\rangle.$$

First, $y - h = y - fl$ by definition and

$$y - fl \equiv l(gy - f) \pmod{\langle p \rangle}.$$

Then $y - h$ is an element of $\langle p, gy - f \rangle$. Conversely,

$$gy - f \equiv g(y - fl) = g(y - h),$$

so $gy - f$ is an element of $\langle p, y - h \rangle$. □

Not all elements β can be expressed in terms of a single α, however. The following theorem is a quick analog of the previous one, but generalized to the case of multiple variables.

Notation 4.4. Let $K = k(\alpha_1, \ldots, \alpha_n)$, $i = 2, \ldots, n$, and p a polynomial in $k(\alpha_1, \ldots, \alpha_i - 1)[x_i]$, we define

$$\bar{p}(\alpha_1, \ldots, \alpha_i - 1, x_i) = p.$$

Theorem 4.5. *Let $K = k(\alpha_1, \ldots, \alpha_n)$ and let p_i be the minimal polynomial for α_i over k. Let β be an element of $k(\alpha_1, \ldots, \alpha_n)$ such that if f and g are polynomials in $k[x_1, \ldots, x_n]$ then*

$$\beta = \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)}.$$

Then the minimal polynomial of β over k is the monic polynomial generating the ideal $J \cap k[y]$, where $J = \langle \bar{p}_1, \ldots, \bar{p}_n, gy - f \rangle$.

Proof. As in the proof of the previous theorem, it is clear that

$$k[x_1, \ldots, x_n]/\langle \bar{p}_1, \ldots, \bar{p}_n \rangle \cong k(\alpha_1, \ldots, \alpha_n)$$

under the map

$$\begin{aligned} \phi : k[x_1, \ldots, x_n] &\to k(\alpha_1, \ldots, \alpha_n) \\ x_i &\mapsto \alpha_i. \end{aligned}$$

We now need to show that $ker\phi = \langle \bar{p}_1, \ldots, \bar{p}_n \rangle$. If $n = 1$, this is clearly true. Then, inducting on n, note that $\bar{p}_1, \ldots, \bar{p}_n$ are in ϕ_n. Let f such that $f(\alpha_1, \ldots, \alpha_n) = 0$ and define $h(x) = f(\alpha_1, \ldots, \alpha_(n-1), x)$. Since p_n is the minimal polynomial of α_n and $h(\alpha_n) = 0$ by construction, p_n divides h. Then there exists ℓ_n such that $h = p_n \ell_n$. Let g in $k[x_1, \ldots, x_{n-1}]$ be such that

$$f - \bar{p}_n \bar{\ell}_n = \sum_j g_j(x_1, \ldots, x_{n-1}) x_n^j.$$

For all j, $g_j = 0$ since

$$(f - \bar{p}_n \bar{\ell}_n)(\alpha_1, \ldots, \alpha_(n-1), x_n) = h - \bar{p}_n \bar{\ell}_n = 0.$$

Thus $g_j(x_1, \ldots, x_{n-1})$ is in $ker\phi_{n-1}$ and also in $< \bar{p}_1, \ldots, \bar{p}_{n-1} >$ by induction. This means that $f - \bar{p}_n \bar{\ell}_n$ is in $\langle \bar{p}_1, \ldots, \bar{p}_{n-1} \rangle$ and f is in $\langle \bar{p}_1, \ldots, \bar{p}_n \rangle$, so $ker\phi = \langle \bar{p}_1, \ldots, \bar{p}_n \rangle$.
The remainder of the proof is now similar to the proof of the previous theorem. □

Example 4.6. We want to compute the minimal polynomial of $\sqrt{2} + \sqrt{3} + \sqrt[3]{5}$ over $\mathbb{Q}$. Let $p_1 = x_1^2 - 2$, $p_2 = x_2^2 - 3$, and $p_3 = x_3^3 - 5$. Note that the p_i satisfy

the condition for $\bar{p}_i$. Since $\beta = \sqrt{2} + \sqrt{3} + \sqrt[3]{5}$ we write $g(x_1, x_2, x_3) = 1$ and $f(x_1, x_2, x_3) = x_1 + x_2 + x_3$, so

$$\beta = \frac{f(\alpha_1, \alpha_2, \alpha_3)}{g(\alpha_1, \alpha_2,}.$$

Then our ideal is

$$\begin{aligned} I &=< p_1, p_2, p_3, gy - f > \\ &=< x_1^2 - 2, x_2^2 - 3, x_3^3 - 5, y - (x_1 + x_2 + x_3). \end{aligned}$$

If we calculate the reduced Gröbner basis for this ideal under the term ordering $x_1 > x_2 > x_3 > y$, we obtain

$$y^{12} - 30y^{10} - 20y^9 + 303y^8 - 910y^6 - 2760y^5 + 2553y^4 + 8300y^3 + 8220y^2 - 4560y - 23624$$

as the only polynomial in the intersection $I \cap k[y]$, and thus it is the minimal polynomial of $\beta = \sqrt{2} + \sqrt{3} + \sqrt[3]{5}$.

This is only a sampling of the tremendous variety of applications of Gröbner bases to problems in many different areas of mathematics. With computers to simplify the often messy calculations, the practicality of using Gröbner bases has increased since their introduction in the middle of the 20th century, and the scope of their usefulness has increased correspondingly.

5. References

[AL] Adams, W and Loustaunau, P. (1994): An Introduction to Gröbner Bases. AMS, Providence, Rhode Island.

[CLO] Cox, D, Little, J, and O'Shea, D. (2000): Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra. Springer, New York, NY.

[DF] Dummit, D and Foote, R. (2004): Abstract Algebra. Wiley and Sons, Hoboken, NJ.

[W] Wang, D. (1998): Gröbner Bases Applied to Geometric Theorem Proving and Discovering