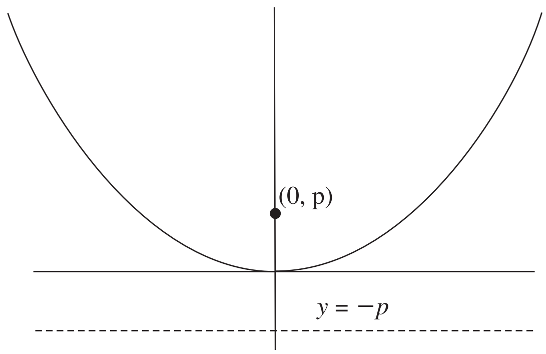
such that the point (x_0, y_0) is a distance of d_0 from the point $(0, p_0)$ and a distance d_0 from the line $y = -p$. We order the indeterminates by $p < x < y < d$ and seek a Gröbner basis.

$$\begin{array}{cl} \{-d^2 + y^2 - 2yp + x^2 + p^2, d - y - p\} & \text{initial basis} \\ \{-dy - dp + y^2 - 2yp + x^2 + p^2, d - y - p\} & \text{by adding (d)(second) to first} \\ \{-dp - 3yp + x^2 + p^2, d - y - p\} & \text{by adding (y)(second) to first} \\ \{-4yp + x^2, d - y - p\} & \text{by adding (p)(second) to first} \end{array}$$

In Exercise 33 you are asked to check that $\{-4yp + x^2, d - y - p\}$ is a Gröbner basis. Note that for any $(x_0, y_0, p_0) \in \mathbb{R}^3$ that is a zero of the first polynomial $-4yp + x^2$, there is a real number d_0 so that (x_0, y_0, p_0, d_0) is a zero of the second polynomial. This verifies the standard form of the equation of a parabola, $4py = x^2$. ▲



Care must be taken in deciding the order for the indeterminate. In Example 38.6, had we taken the order of the indeterminates to be $d < p < x < y$, the resulting Gröbner basis would have been $\{-4dp + 4p^2 + x^2, d - p - y\}$, which does not directly give the standard form for the equation of a parabola. The reason for making the indeterminate d the largest is that the algorithm attempts to eliminate d from polynomials in the basis since the reduction process reduces the maximum-sized term.

The algorithm for computing Gröbner bases can be programmed. In fact, it is a built-in function on many common mathematical packages including Mathematica, Maple, Wolfram Alpha, and others. By carefully picking the order of the indeterminates, it is possible to solve a large variety of problems using automated computations of Gröbner bases.

38.7 Example We use a software package to compute a Gröbner basis that yields the equation of an ellipse in standard position. An ellipse in standard position is the set of all points in the plane so that the sum of the distances to the two foci $(c, 0)$ and $(-c, 0)$ is a fixed distance $2a$. We start with the basis

$$\{(x - c)^2 + y^2 - d_1^2, (x + c)^2 + y^2 - d_2^2, d_1 + d_2 - 2a\}$$

where d_1 represents the distance to focus $(c, 0)$ and d_2 represents the distance to focus $(-c, 0)$. We wish to arrive at a polynomial that includes x and y as well as the parameters a and c that describe the shape and size of the ellipse. Therefore, we take d_1 and d_2 as the largest indeterminates. Using the order $a < c < y < x < d_2 < d_1$, a mathematical software package quickly computes the Gröbner basis

$$\{a^4 - a^2c^2 - a^2x^2 + c^2x^2 - a^2y^2, -a^2 + ad_2 - cx, a^3 - ac^2 - acs + cd_2x - ax^2 - ay^2,$$

$$-c^2 + d_2^2 - 2cx - x^2 - y^2, -2a + d_1 + d_2\}.$$

The first polynomial can be written as

$$a^2(a^2-c^2)-(a^2-c^2)x^2-a^2y^2.$$

We think of a and c as parameters and recall that in an ellipse, the parameter $b>0$ is defined by $b^2=a^2-c^2$. We see that the variety in $\mathbb{R}^2$ defined from the ideal $\langle a^2b^2-b^2x^2-a^2y^2\rangle$ has equation

$$\frac{x^2}{a^2}+\frac{y^2}{b^2}=1. \qquad \blacktriangle$$

A **graph** is a finite set with elements called **vertices** together with a collection of pairs of vertices called **edges** or **arcs**. Graphs are often drawn as in Figure 38.10, which shows a graph with four vertices x_1,x_2,x_3,x_4 and four edges $\{x_1,x_2\},\{x_2,x_3\},\{x_3,x_1\},\{x_3,x_4\}$. A **coloring** of a graph is an assignment of colors to the vertices in such a way that no two vertices in the same edge have the same color. The problem of determining if a graph can be colored with n colors can be restated as a question about an ideal, which can (at least theoretically) be answered using Gröbner bases.

38.8 Theorem Let G be a graph with vertex set $\{x_1,x_2,\ldots,x_k\}$. We identify each vertex with an indeterminate and form the ideal $I\subseteq\mathbb{C}[x_1,x_2,\ldots,x_k]$ with basis consisting of polynomials $x_1-1, x_2^n-1, x_3^n-1,\ldots,x_k^n-1$ together with a polynomial $x_i^{n-1}+x_i^{n-2}x_j+x_i^{n-3}x_j^2+\cdots+x_ix_j^{n-2}+x_j^{n-1}$ for each edge in the graph. The graph G can be colored with n colors if and only if the algebraic variety $V(I)$ is nonempty.

Proof The proof is left for Exercise 34. $\blacklozenge$

The variety $V(I)$ in Theorem 38.8 gives all possible colorings of the graph G using the n^{th} roots of unity for the colors and coloring vertex x_1 with the color 1. For each point in $V(I)$, the j^{th} coordinate gives the color assigned to x_j.

38.9 Example Using the graph in Figure 38.10, the basis described in Theorem 38.8 for $n=2$ is

$$\{x_1-1, x_2^2-1, x_3^2-1, x_4^2-1, x_1+x_2, x_2+x_3, x_3+x_1, x_3+x_4\}.$$

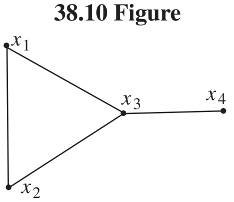
A Gröbner basis is $\{1\}$. This can be determined electronically, or by noticing that

$$(x_1+x_2)-(x_2+x_3)+(x_3+x_1)=2x_1\in I.$$

Therefore, $x_1\in I$, so $x_1-(x_1-1)=1\in I$. Thus the ideal is all of $\mathbb{C}[x_1,x_2,x_3,x_4]$, which has $\{1\}$ as a basis. Since the algebraic variety for $\langle 1\rangle$ is the empty set, the graph cannot be colored with two colors.

We now compute a Gröbner basis when $n=3$. Theorem 38.8 tells us to start with the basis

38.10 Figure



$$\{x_1-1, x_2^3-1, x_3^3-1, x_4^3-1, x_1^2+x_1x_2+x_2^2, x_2^2+x_2x_3+x_3^2, x_3^2+x_3x_1+x_1^2, x_3^2+x_3x_4+x_4^2\}.$$

Using a software package, a Gröbner basis with indeterminate order $x_1<x_2<x_3<x_4$ is

$$\{x_1-1, x_2^2+x_2+1, 1+x_2+x_3, x_2-x_4-x_2x_4+x_4^2\}.$$

Let $\zeta=-\frac{\sqrt{3}}{2}+\frac{1}{2}i$ be a third root of unity. We find an element $(a_1,a_2,a_3,a_4)\in V(I)$:

$$\begin{aligned}
a_1-1&=0 \quad a_1=1\\
a_2^2+a_2+1&=0 \quad a_2 \text{ is a third root of unity. Let } a_2=\zeta\\
1+\zeta+a_3&=0 \quad a_3=-1-\zeta=\zeta^2\\
\zeta-a_4-\zeta a_4+a_4^2&=0 \quad \text{factoring, } (\zeta-a_4)(1-a_4)=0.
\end{aligned}$$

We see that we can color vertex 1 the color 1, vertex 2 ζ, vertex 3 ζ^2, and then we can color vertex 4 either the color 1 or ζ. ▲

There are many applications of Gröbner bases in mathematics, statistics, engineering, and computer science. These include controlling robot arms and automated theorem proving. The algorithm to compute a Gröbner basis is generally too long and tedious to be done by hand, so computers are essential. However, some larger problems are not feasible even on modern high-speed computers.

EXERCISES 38

In Exercises 1 through 4, write the polynomials in $\mathbb{R}[x, y, z]$ in decreasing term order, using the order lex for power products $x^m y^n z^s$ where $z < y < x$.

1. $2xy^3z^5 - 5x^2yz^3 + 7x^2y^2z - 3x^3$

2. $3y^2z^5 - 4x + 5y^3z^3 - 8z^7$

3. $3y - 7x + 10z^3 - 2xy^2z^2 + 2x^2yz^2$

4. $38 - 4xz + 2yz - 8xy + 3yz^3$

In Exercises 5 through 8, write the polynomials in $\mathbb{R}[x, y, z]$ in decreasing term order, using the order lex for power products $z^m y^n x^s$ where $x < y < z$.

5. The polynomial in Exercise 1.

6. The polynomial in Exercise 2.

7. The polynomial in Exercise 3.

8. The polynomial in Exercise 4.

Another ordering, deglex, for power products in $F[\mathbf{x}]$ is defined as follows:

$$x_1^{s_1} x_2^{s_2} \cdots x_n^{s_n} < x_1^{t_1} x_2^{t_2} \cdots x_n^{t_n}$$

if and only if either $\sum_{i=1}^n s_i < \sum_{i=1}^n t_i$, or these two sums are equal and $s_i < t_i$ for the smallest value of i such that $s_i \neq t_i$. Exercises 9 through 13 are concerned with the order deglex.

9. List, in increasing order, the smallest 20 power products in $\mathbb{R}[x, y, z]$ for the order deglex with power products $x^m y^n z^s$ where $z < y < x$.

In Exercises 10 through 13, write the polynomials in order of decreasing terms using the order deglex with power products $x^m y^n z^s$ where $z < y < x$.

10. The polynomial in Exercise 1.

11. The polynomial in Exercise 2.

12. The polynomial in Exercise 3.

13. The polynomial in Exercise 4.

For Exercises 14 through 17, let power products in $\mathbb{R}[x, y, z]$ have order lex where $z < y < x$. If possible, perform a single-step division algorithm reduction that changes the given ideal basis to one having smaller maximum term order.

14. $\langle xy^2 - 2x, x^2y + 4xy, xy - y^2\rangle$

15. $\langle xy + y^3, y^3 + z, x - y^4\rangle$

16. $\langle xyz - 3z^2, x^3 + y^2z^3, x^2yz^3 + 4\rangle$

17. $\langle y^2z^3 + 3, y^3z^2 - 2z, y^2z^2 + 3\rangle$

In Exercises 18 and 19, let the order of power products in $\mathbb{R}[w, x, y, z]$ be lex with $z < y < x < w$. Find a Gröbner basis for the given ideal.

18. $\langle w + x - y + 4z - 3, 2w + x + y - 2z + 4, w + 3x - 3y + z - 5\rangle$

19. $\langle w - 4x + 3y - z + 2, 2w - 2x + y - 2z + 5, w - 10x + 8y - z - 1\rangle$

In Exercises 20 through 22, find a Gröbner basis for the indicated ideal in $\mathbb{R}[x]$.

20. $\langle x^4 + x^3 - 3x^2 - 4x - 4, x^3 + x^2 - 4x - 4\rangle$

21. $\langle x^4 - 4x^3 + 5x^2 - 2x, x^3 - x^2 - 4x + 4, x^3 - 3x + 2\rangle$

22. $\langle x^5 + x^2 + 2x - 5, x^3 - x^2 + x - 1\rangle$

In Exercises 23 through 26, find a Gröbner basis for the given ideal in $\mathbb{R}[x, y]$. Consider the order of power products to be lex with $y < x$. If you can, describe the corresponding algebraic variety in $\mathbb{R}[x, y]$.