Ideals, Varieties, and Algorithms by David A. Cox

Frosty

March 1, 2026

Contents

1 Geometry, Algebra, and Algorithms

1.1 Polynomials and Affine Space

Problem 2

Let $\mathscr{F}_2$ be the field from Exercise 1.

1. Consider the polynomial $g(x, y) = x^2y + y^2x \in \mathscr{F}_2[x, y]$. Show that $g(x, y) = 0s$ for every $(x, y) \in \mathscr{F}_2^2$, and explain why this does not contradict Proposition 5.
2. Find a nonzero polynomial in $\mathscr{F}_2[x, y, z]$ which vanishes at every point of $\mathscr{F}_2^3$. Try to find one involving three variables.
3. Find a nonzero polynomial in $\mathscr{F}_2[x_1, \dots, x_n]$ which vanishes at every point of $\mathscr{F}_2^n$. Can you find one in which all of $x_1, \dots, x_n$ appear?

Solution (1): It is clear that if $x = 0$ or $y = 0$, then $g(x, y) = 0$. Now, if $x = y = 1$, then

$$g(x, y) = 1^2 \cdot 1 + 1^2 \cdot 1 = 1 + 1 = 0.$$

Thus $g(x, y) = 0$ for all $(x, y) \in \mathscr{F}_2^2$.

Solution (2): Consider the polynomial $g \in \mathscr{F}_2[x, y, z]$ defined by

$$g(x, y, z) = (x^2 - x)(y^2 - y)(z^2 - z),$$

which is clearly 0 at all $(x, y, z) \in \mathscr{F}_2 \times \mathscr{F}_2 \times \mathscr{F}_2$.

Solution (3): Consider the polynomial $g \in \mathscr{F}_2[x_1, \dots, x_n]$ defined by

$$g(x_1, \dots, x_n) = (x_1^2 - x_1) \cdots (x_n^2 - x_n),$$

which is clearly 0 at all $(x_1, \dots, x_n) \in \mathscr{F}_2 \times \cdots \times \mathscr{F}_2$.

Problem 3

(Requires abstract algebra) Let p be a prime number. The ring of integers modulo p is a field with p elements, which we will denote $\mathcal{F}_p$.

1. Explain why $\mathcal{F}_p \setminus \{0\}$ is a group under multiplication.
2. Use Lagrange's theorem to show that $a^{p-1} = 1$ for all $a \in \mathcal{P} \setminus \{0\}$.
3. Prove that $a^p = a$ for all $a \in \mathcal{F}_p$. [Hint: Treat the cases $a = 0$ and $a \neq 0$ separately.]
4. Find a nonzero polynomial in $\mathcal{F}_p[x]$ that vanishes at all points in $\mathcal{F}_p$. [Hint: Use part (c).]

Solution (1): It is well known that for any ring R the set of units $U(R)$ under multiplication forms a group. All elements $x \neq 0$ in $\mathcal{F}_p$ have inverses and are thus in $U(\mathcal{F}_p)$. Therefore $\mathcal{F}_p \setminus \{0\}$ is a group under multiplication.

Solution (2): Don't have preqreuisites.

Proof. Let $a \in \mathcal{F}_p$. Suppose $a = 0$. Then $a^p = 0^p = 0 = a$. Suppose $a \neq 0$. Then $a^{p-1} = 1$ by part 2. Then $a \cdot a^{p-1} = a \cdot 1 \iff a^p = a$ as required. ∎

Solution (4): Consider the polynomial $g(x) = x^p - x \in \mathcal{F}_p[x]$. Now, for all $a \in \mathcal{F}_p$ we have $a^p = a$ by part 3, thus $g(a) = 0$.

Problem 5

In the proof of Proposition 5, we took $f \in k[x_1, \ldots, x_n]$ and wrote it as a polynomial in x_n with coefficients in $k[x_1, \ldots, x_{n-1}]$. To see what this looks like in a specific case, consider the polynomial

$$f(x, y, z) = x^5y^2z - x^4y^3 + y^5 + x^2z - y^3z + xy + 2x - 5z + 3.$$

1. Write f as a polynomial in x with coefficients in $k[y, z]$.
2. Write f as a polynomial in y with coefficients in $k[x, z]$.
3. Write f as a polynomial in z with coefficients in $k[x, y]$.

Solution (1):

$$f(x) = (y^2z)x^5 - (y^3)x^4 + (z)x^2 + (y + 2)x - y^3z + y^5 - 5z + 3$$

Solution (2):

$$f(y) = y^5 - (x^4 - z)y^3 + (x^5z)y^2 + (x)y + x^2z + 2x - 5z + 3$$

Solution (3):

$$f(z) = (x^5y^2 + x^2 - y^3 - 5)z - x^4y^3 + y^5 + xy + 2x + 3$$

Problem 6

Inside of $\mathbb{C}^n$, we have the subset $\mathbb{Z}^n$, which consists of all points with integer coordinates.

1. Prove that if $f \in \mathbb{C}[x_1, \ldots, x_n]$ vanishes at every point of $\mathbb{Z}^n$, then f is the zero polynomial. [Hint: Adapt the proof of Proposition 5.]
2. Let $f \in \mathbb{C}[x_1, \ldots, x_n]$, and let M be the largest power of any variable that appears in f. Let $\mathbb{Z}^n_{M+1}$ be the set of all points of $\mathbb{Z}^n$, all coordinates which lie between 1 and $M+1$, inclusive. Prove that if f vanishes at all points of $\mathbb{Z}^n_{M+1}$, then f is the zero polynomial.

Proof. Suppose $f \in \mathbb{C}[x_1, \ldots, x_n]$ vanishes at every point of $\mathbb{Z}^n$. We will use induction on the number of variables n. When $n = 1$. It is well known that a nonzero polynomial in $\mathbb{C}[x]$ of degree m has at most m distinct roots. For our particular $f \in \mathbb{C}[x]$, we are assuming $f(a) = 0$ for all $a \in \mathbb{Z}$. Since $\mathbb{Z}$ is infinite, this means that f has infinitely many roots, and, hence, f must be the zero polynomial.

Now assume that the theorem holds for $n-1$ variables. By collecting the various powers of x_n, we can write f in the form

$$f = \sum_{i=0}^{N} g_i(x_1, \dots, x_{n-1}) x_n^i,$$

where $g_i \in \mathbb{C}[x_1, \dots, x_{n-1}]$. We will show that each g_i is the zero polynomial in $n-1$ variables, which will force f to be the zero polynomial in $\mathbb{C}[x_1, \dots, x_n]$.

If we fix $(a_1, \dots, a_{n-1}) \in \mathbb{Z}^{n-1}$, we get the polynomial $f(a_1, \dots, a_{n-1}, x_n) \in \mathbb{C}[x_n]$. By our hypothesis on f, this vanishes for every $a_n \in \mathbb{Z}$. It follows from the case $n = 1$ that $f(a_1, \dots, a_{n-1}, x_n)$ is the zero polynomial in $\mathbb{C}[x_n]$. Using the above formula for f, we see that all coefficients of $f(a_1, \dots, a_{n-1}, x_n)$ vanish. Since $(a_1, \dots, a_{n-1})$ was arbitrarily chosen in $\mathbb{Z}^{n-1}$, it follows that each $g_i \in \mathbb{C}[x_1, \dots, x_{n-1}]$ gives the zero function on $\mathbb{Z}^{n-1}$. Our inductive assumption then implies each g_i is the zero polynomial in $\mathbb{C}[x_1, \dots, x_{n-1}]$. This forces f to be the zero polynomial in $\mathbb{C}[x_1, \dots, x_n]$. ∎

Proof. Suppose $f \in \mathbb{C}[x_1, \dots, x_n]$ vanishes at every point of $\mathbb{Z}_{M+1}^n$. We will use induction on the number of variables n. When $n = 1$. It is well known that a nonzero polynomial in $\mathbb{C}[x]$ of degree at most M has at most M distinct roots. For our particular $f \in \mathbb{C}[x]$, we are assuming $f(a) = 0$ for all $a \in \mathbb{Z}_{M+1}$. Since $\mathbb{Z}_{M+1}$ has $M+1$ elements, this means that f has $M+1$ roots, and, hence, f must be the zero polynomial.

Now assume that the theorem holds for $n-1$ variables. By collecting the various powers of x_n, we can write f in the form

$$f = \sum_{i=0}^{N} g_i(x_1, \dots, x_{n-1}) x_n^i,$$

where $g_i \in \mathbb{C}[x_1, \dots, x_{n-1}]$. We will show that each g_i is the zero polynomial in $n-1$ variables, which will force f to be the zero polynomial in $\mathbb{C}[x_1, \dots, x_n]$.

If we fix $(a_1, \dots, a_{n-1}) \in \mathbb{Z}_{M+1}^{n-1}$, we get the polynomial $f(a_1, \dots, a_{n-1}, x_n) \in \mathbb{C}[x_n]$. By our hypothesis on f, this vanishes for every $a_n \in \mathbb{Z}_{M+1}$. It follows from the case $n = 1$ that $f(a_1, \dots, a_{n-1}, x_n)$ is the zero polynomial in $\mathbb{C}[x_n]$. Using the above formula for f, we see that all coefficients of $f(a_1, \dots, a_{n-1}, x_n)$ vanish. Since $(a_1, \dots, a_{n-1})$ was arbitrarily chosen in $\mathbb{Z}_{M+1}^{n-1}$, it follows that each $g_i \in \mathbb{C}[x_1, \dots, x_{n-1}]$ gives the zero function on $\mathbb{Z}_{M+1}^{n-1}$. Our inductive assumption then implies each g_i is the zero polynomial in $\mathbb{C}[x_1, \dots, x_{n-1}]$. This forces f to be the zero polynomial in $\mathbb{C}[x_1, \dots, x_n]$. ∎

1.2 Affine Varieties

Problem 1

Sketch the following affine varieties in $\mathbb{R}^2$:

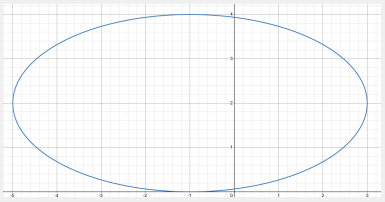
1. $\mathbf{V}(x^2 + 4y^2 + 2x - 16y + 1)$
2. $\mathbf{V}(x^2 - y^2)$
3. $\mathbf{V}(2x + y - 1, 3x - y + 2)$

In each case, does the variety have the dimension you would intuitively expect it to have?

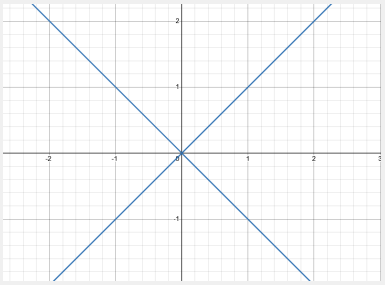
Solution (1): I would expect it to have two dimensions. Notice

$$\begin{aligned}
x^2 + 4y^2 + 2x - 16y + 1 = 0 &\iff x^2 + 2x + 1 + 4y^2 - 16y = 0 \\
&\iff (x+1)^2 + 4(y^2 - 4y) = 0 \\
&\iff (x+1)^2 + 4(y^2 - 4y + 4 - 4) = 0 \\
&\iff (x+1)^2 + 4((y-2)^2 - 4) = 0 \\
&\iff (x+1)^2 + 4(y-2)^2 - 16 = 0 \\
&\iff \frac{(x+1)^2}{4} + \frac{(y-2)^2}{1} = 4
\end{aligned}$$

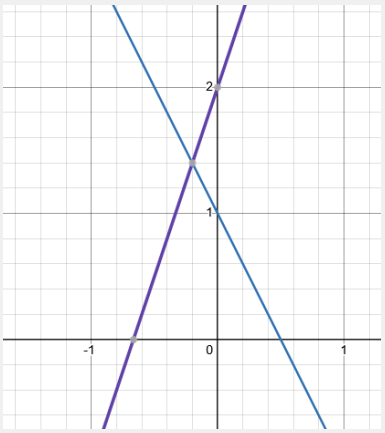
Which is an ellipse.



Solution (2): I would expect it to have two dimensions. If we solve $x^2 - y^2$ for y we find $y = \pm x$ which is two lines with slope of 1 passing through the origin.



Solution (3): I would expect it to be a single point. We can solve for x, y and find $x = -\frac{1}{5}$, $y = \frac{7}{5}$.



Problem 6

Let us show that all finite subset of k^n are affine varieties.

1. Prove that a single point $(a_1, \dots, a_n) \in k^n$ is an affine variety.
2. Prove that every finite subset of k^n is an affine variety. [Hint: Lemma 2 will be useful.]

Proof. Let $(a_1, \dots, a_n)$ be an arbitrary point in k^n. Consider the following set of polynomials

$$\mathscr{P} = \{x_i - a_i \mid 1 \leq i \leq n\}.$$

For which the point $(a_1, \dots, a_n)$ is the exact solution. Thus

$$\mathbf{V}(\mathscr{P}) = \{(a_1, \dots, a_n)\}.$$

Therefore a single point in k^n is an affine variety. ∎

Proof. Let $V \subset k^n$ be a finite set. Then V can be written as

$$V = \bigcup_{i=1}^{m} \{p_i\},$$

where each $p_i \in k^n$. By part (1), each $\{p_i\}$ is an affine variety. By Lemma 2, a finite union of affine varieties is an affine variety. Thus V is an affine variety. ∎

Problem 8

It can take some work to show that something is *not* an affine variety. For example, consider the set

$$X = \{(x, x) \mid x \in \mathbb{R}, x \neq 1\} \subseteq \mathbb{R}^2$$

which is the straight line $x = y$ with the point $(1, 1)$ removed. To that X is not an affine variety, suppose that $X = \mathbf{V}(f_1, \ldots, f_s)$. Then each f_i vanishes on X, and if we can show that f_i also vanishes at $(1, 1)$, we will get the desired contradiction. Thus, here is what you are to prove: if $f \in \mathbb{R}[x, y]$ vanishes on X, then $f(1, 1) = 0$. [Hint: Let $g(t) = f(t, t)$ which is a polynomial $\mathbb{R}[t]$. Now apply the proof of proposition 5 on 1.]

Proof. Suppose $f \in \mathbb{R}[x, y]$ vanishes on X. Let $g(t) = f(t, t)$, which is a polynomial in $\mathbb{R}[t]$. Then $g(x) = 0$ for all $x \in \mathbb{R}$ with $x \neq 1$. Since a nonzero polynomial in $\mathbb{R}[t]$ can have only finitely many roots, it follows from Proposition 5 that g must be the zero polynomial. Therefore $g(1) = f(1, 1) = 0$, which is a contradiction. ∎

Problem 9

Let $\mathbf{R} = \{(x, y) \in \mathbb{R}^2 \mid y > 0\}$ be the upper half plane. Prove that $\mathbf{R}$ is not an affine variety.

Proof. Suppose $f \in \mathbb{R}[x, y]$ vanishes on $\mathbf{R}$. Fix any $y_0 > 0$ and consider the polynomial in one variable $g(x) = f(x, y_0) \in \mathbb{R}[x]$. Since $f(x, y_0) = 0$ for all $x \in \mathbb{R}$ by Proposition 5, g is the zero polynomial. Because $y_0 > 0$ was arbitrary it follows that that $f(x, y) = 0$ for all $(x, y) \in \mathbf{R}$. Therefore f is the zero polynomial. ∎

Problem 10

Let $\mathbb{Z}^n \subseteq \mathbb{C}^n$ consist of those points with integer coordinates. Prove that $\mathbb{Z}^n$ is not an affine variety. [Hint: See Exercise 6 1.]

Proof. Suppose $f \in \mathbb{C}[x_1, \ldots, x_n]$ vanishes on $\mathbb{Z}^n$. Fix integers $k_2, \ldots, k_n \in \mathbb{Z}$ and consider the polynomial

$$g(x_1) = f(x_1, k_2, \ldots, k_n) \in \mathbb{C}[x_1].$$

Since $g(x_1) = f(x_1, k_2, \ldots, k_n) = 0$ for all $x_1 \in \mathbb{Z}$, by Proposition 5 it follows that g is the zero polynomial. Because $k_2, \ldots, k_n$ were arbitrary integers, it follows that $f(x_1, x_2, \ldots, x_n) = 0 \quad$ for all $(x_1, \ldots, x_n) \in \mathbb{Z}^n$. Therefore f is the zero polynomial in $\mathbb{C}[x_1, \ldots, x_n]$. ∎

Problem 11

So far, we have discussed varieties in $\mathbb{R}$ or $\mathbb{C}$. It is also possible to consider varieties over the field $\mathbb{Q}$, although the questions here tend to be *much* harder. For example, let n be a positive integer, and consider the variety $F_n \subseteq \mathbb{Q}^2$ defined by

$$x^n + y^n = 1.$$

Notice that there are some obvious solutions when x or y is zero. We call these *trivial solutions*. An

interesting question is whether or not there are any nontrivial solutions.

1. Show that F_n has two trivial solutions if n is odd and four trivial solutions of n is even.
2. Show that F_n would have a nontrivial solution for some $n \geq 3$ if and only if Fermat's Last Theorem were false.

Theorem 1. Fermat's Last Theorem *states that, for $n \geq 3$, the equation*

$$x^n + y^n = z^n$$

has no solutions where x, y and z are nonzero integers. The general case of this conjecture was proved by Andrew Wiles in 1994 using some very sophisticated number theory. The proof is extremely *difficult.*

Proof. Suppose n is odd. If $x = 0$ then $y = 1$. Similarly, if $y = 0$ then $x = 1$. Thus we have two solutions: $(0, 1), (1, 0)$.

Suppose n is even. If $x = 0$ then $y = \pm 1$. Similarly, if $y = 0$ then $x = \pm 1$. Thus we have four solutions: $(0, \pm 1), (\pm 1, 0)$. ∎

Proof. Suppose F_n has a nontrivial solution for some $n \geq 3$. Then suppose $x, y \in \mathbb{Q}$ such that $x^n + y^n = 1$. Furthermore, suppose $x = \frac{a}{b}, y = \frac{c}{d}$ where $a, b, c, d \in \mathbb{Z}$. Then

$$\left(\frac{a}{b}\right)^n + \left(\frac{c}{d}\right)^n = \frac{a^n}{b^n} + \frac{c^n}{d^n} = 1.$$

Multiply through by $b^n d^n$ to obtain

$$(ad)^n + (cb)^n = (bd)^n.$$

Since $a, b, c, d \in \mathbb{Z}$ and $n \geq 3$, this is a solution to Fermat's Last Theorem.

Conversely, suppose Fermat's Last Theorem is false. Then there exists nonzero integers x, y, z and $n \geq 3$ such that $x^n + y^n = z^n$. Dividing through by z^n gives

$$\left(\frac{x}{z}\right)^n + \left(\frac{y}{z}\right)^n = 1.$$

Therefore F_n has a nontrivial solution for some $n \geq 3$. ∎

Problem 15

In Lemma 2, we showed that if V and W are affine varieties, then so are there union $V \cup W$ and intersection $V \cap W$. In this exercise we will study how other set-theoretic operations affect affine varieties.

1. Prove that finite unions and intersections of affine varieties are again affine varieties. [Hint: Induction].
2. Give an example to show that an infinite union of affine varieties need not be an affine variety. Hint: By Exercise 8-10, we know some subsets of k^n that are not affine varieties. Suprisingly, an infinite intersection of affine varieties is still an affine variety. This is a consequence of the Hilbert Basis Theorem, which will be discussed in Chapter 2.
3. Given an example to show that the set-theoretic difference $V \setminus W$ of two affine varieties need not be an affine varietiy.
4. Let $V \subseteq k^n$ and $W \subseteq k^m$ be two affine varieties, and let

   $$V \times W = \{(x_1, \ldots, x_n, y_1, \ldots, y_m) \in k^{n+m} \mid (x_1, \ldots, x_n) \in V, (y_1, \ldots, y_n) \in W\}$$

   be their Cartesian product. Prove that $V \times W$ is an affine variety in k^{n+m}. [Hint: If V is defined by $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, then we can regard $f_1, \ldots, f_s$ as polynomials in $k[x_1, \ldots, x_n, y_1, \ldots, y_m]$, and similarly for W. Show that this gives defining equations for the Cartesian product.]

Proof. By Lemma 2 we know the base case holds for the union and intersection of two affine varieties. Suppose Lemma 2 holds for the union and intersection of $n-1$ affine varieties. Let $V = \{v_1, \dots, v_n\}$ be a set of n affine varieties. Then

$$\mathscr{U} = \bigcup_{i=1}^{n} v_i = \bigcup_{i=1}^{n-1} v_i \cup v_n,$$

and

$$\mathscr{I} = \bigcap_{i=1}^{n} v_i = \bigcap_{i=1}^{n-1} v_i \cap v_n.$$

Now, by our hypothesis $\bigcup_{i=1}^{n-1} v_i$ and $\bigcap_{i=1}^{n-1} v_i$ are affine varieties. Then by Lemma 2, $\bigcup_{i=1}^{n-1} v_i \cup v_n$ and $\bigcap_{i=1}^{n-1} v_i \cap v_n$ are also affine varieties. Thus $\mathscr{U}$ and $\mathscr{I}$ are affine varieties. ∎

Proof. Consider the union of all points in $\mathbb{Z}^n$. Each point is an affine variety by Problem 6. However, by Problem 10, their union (which is $\mathbb{Z}^n$) is not an affine variety. ∎

Proof. Consider the varieties $V_1 = \{(x, y) \mid x = y\}$ and $V_2 = \{(1, 1)\}$. By Problem 8, $V_1 \setminus V_2$ is not an affine variety. ∎

Proof. Let $V \subseteq k^n$ be defined by polynomials $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ and $W \subseteq k^m$ be defined by polynomials $g_1, \dots, g_t \in k[y_1, \dots, y_m]$. Then, let $f_1, \dots, f_s \in k[x_1, \dots, x_n, y_1, \dots, y_m]$ and $g_1, \dots, g_t \in k[x_1, \dots, x_n, y_1, \dots, y_m]$. Then

$$V \times W = \mathbf{V}(f_1, \dots, f_s, g_1, \dots, g_t) \subseteq k^{n+m},$$

so $V \times W$ is an affine variety. ∎

1.3 Parametrizations of Affine Varieties

Problem 1

Parametrize all solutions of the linear equations

$$x + 2y - 2z + w = 1,$$

$$x + y + z - w = 2.$$

Proof. We use row reduction to find the simplified equations:

$$x - 4z + 3w = 3, \quad y - 3z + 2w = -1.$$

Then let $s = w$ and $t = z$. Then

$$x = 3 + 4t - 3s, \quad y = -1 + 3t - 2s.$$

∎

Problem 2

Use a trigonometric identity to show that

$$x = \cos(t),$$

$$y = \cos(2t)$$

parametrizes a portion of a parabola. Indicate exactly what portion of the parabola is covered.

Proof. We have

$$y = \cos(2t) = 2\cos^2(t) - 1 = 2x^2 - 1.$$

Since $\mathrm{Ran}(\cos) = [-1, 1]$, we have $\mathrm{Ran}(x(t)) = [-1, 1]$, and thus $\mathrm{Ran}(y = 2x^2 - 1) = [-1, 1]$. ∎

Problem 3

Given $f \in k[x]$, find a parametrization of $V(y - f(x))$.

Proof. We want to parametrize $y - f(x) = 0$. Let $t = x$, then $y = f(x) = f(t)$. Thus we have $(x, y) = (t, f(t))$ where $t \in k$. ∎

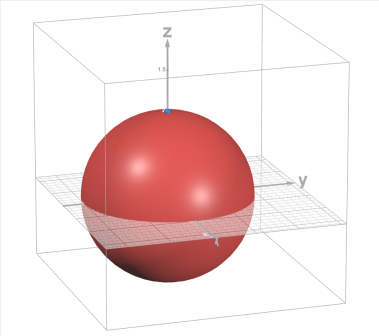
Problem 6

The goal of this problem is to that the sphere $x^2+y^2+z^2 = 1$ in 3-dimensional space can be parametrized by

$$x = \frac{2u}{u^2 + v^2 + 1},$$
$$y = \frac{2v}{u^2 + v^2 + 1},$$
$$z = \frac{u^2 + v^2 - 1}{u^2 + v^2 + 1}.$$

The idea is to adapt the argument used for the circle $x^2 + y^2 = 1$ to 3-dimensional space.

1. Given a point $(u, v, 0)$ in the (x, y)-plane, draw the line from this point to the "north pole" $(0, 0, 1)$ of the sphere, and let (x, y, z) be the other point where the line meets the sphere. Draw a picture to illustrate this, and argue goemetrically that mapping (u, v) to (x, y, z) gives a parametrization of the sphere minus the north pole.
2. Show that the line connecting $(0, 0, 1)$ to $(u, v, 0)$ is parametrized by $(tu, tv, 1 - t)$, where t is a parameter that moves along the line.
3. Substitute $x = tu$, $y = tv$ and $z = 1 - t$ into the equation for the sphere $x^2 + y^2 + z^2 = 1$. Use this to derive the formulas given at the beggining of the problem.



Proof. The figure above shows the unit sphere in 3-space. It is clear that if we are to draw all lines from $(0, 0, 1)$ to $(u, v, 0)$ where $u, v \in \mathbb{R}$ then we would be able to intersect all points on the sphere other than $(0, 0, 1)$. Now, taking a point (u, v) we can compute the line through $(u, v, 0)$ and $(0, 0, 1)$ and find the point at which it intersects the unit sphere. ∎

Proof. Notice

$$\begin{aligned}(x, y, z) &= (0, 0, 1) + t((u, v, 0) - (0, 0, 1)) \\ &= (0, 0, 1) + t(u, v, -1) \\ &= (tu, tv, 1 - t)\end{aligned}$$

∎

Proof. We have

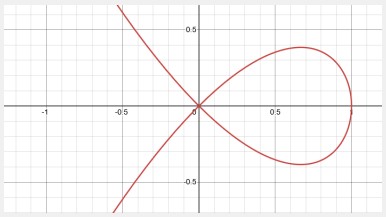
$$x^2 + y^2 + z^2 = 1 \iff t^2u^2 + t^2v^2 + t^2 - 2t = 0 \iff t(tu^2 + tv^2 + t - 2) = 0$$

Now $t = 0$ corresponds with $(0, 0, 1)$ thus we want $tu^2 + tv^2 + t - 2 = 0$. Solving for t we find $t = \frac{2}{u^2+v^2+1}$. Plugging t into $(x(t), y(t), z(t))$ gives the desired equations. ∎

Problem 8

Consider the curved defined by $y^2 = cx^2 - x^3$, where c is some constant. Here is a picture of the curve when $c > 0$. Our goal is to parametrize this curve.

1. Show that a line will meet this curve at either $0, 1$, or 3 points. Illustrate you answer with a picture. [Hint: Let the equation of the line by either $x = a$ or $y = mx + b$.]
2. Show that a nonvertical line through the origin meets the curve at exactly one other point $m^2 \neq c$. Draw a picture to illustrate this, and see if you can come up with an intuitive explanation for as to why this happens.
3. Now draw the vertical line $x = 1$. Given a point $(1, t)$ on this line, draw the line connecting $(1, t)$ to the origin. This will interesect the curve in a point (x, y). Draw a picture to illustrate this, and argue geometrically that this gives a parametrization of the entire curve.



Proof. Suppose $x = a$. Then

$$y^2 = ca^2 - a^3 = a^2(c - a).$$

If $c < a$ then there is no solution. If $c = a$ then $y = 0$ and there is a single solution $(a, 0)$. If $c > a$ then there are two solutions

$$y = \pm a\sqrt{c - a}.$$

Thus a vertical line meets the curve in $0, 1$, or 2 points.

Now suppose $y = mx + b$. Substituting into the equation of the curve gives

$$(mx + b)^2 = cx^2 - x^3 \tag{1}$$

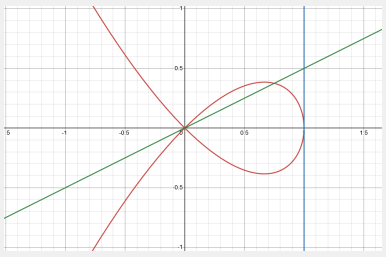
$$\iff x^3 + (m^2 - c)x^2 + 2mbx + b^2 = 0. \tag{2}$$

This is a cubic equation in x, so a nonvertical line meets the curve in at most three points. ∎

Proof. Suppose $y = mx$ and $m^2 \neq c$. Substituting into the equation of the curve gives

$$\begin{aligned} & m^2x^2 = cx^2 - x^3 \\ \iff & x^3 + (m^2 - c)x^2 = 0 \\ \iff & x^2(x + m^2 - c) = 0. \end{aligned}$$

Thus $x = 0$ is a root corresponding to the origin, and the other intersection point is $x = c - m^2$. Therefore every nonvertical line through the origin with $m^2 \neq c$ meets the curve in exactly one other point. ∎



Proof. Consider the vertical line $x = 1$ and a point $(1, t)$ on this line. The line connecting $(1, t)$ to the origin has equation $y = tx$. Substituting into the equation of the curve gives

$$\begin{aligned} & t^2x^2 = cx^2 - x^3 \\ \iff & x^3 + (t^2 - c)x^2 = 0 \\ \iff & x^2(x + t^2 - c) = 0. \end{aligned}$$

Ignoring the double root $x = 0$ we have $x = c - t^2$. and therefore $y = t(c - t^2)$. Therefore the curve is parametrized by

$$x(t) = c - t^2, \qquad y(t) = t(c - t^2).$$

∎

Problem 10

Around 180 B.C.E., Diocles wrote the book *On Burning Mirrors*. One of the curves he considered was the *cissoid* and he used it to solve the problem of duplication of the cube [see part (c) below]. The cissoid has the equation $y^2(a + x) = (a - x)^3$, where a is a constraint.

1. Find an algebraic parametrization of the cissoid.
2. Diocles described the cissoid using the following geometric construction. Given a circle of radius a (which we will take as centered at the origin), pick x between a and $-a$, and draw the line L connecting $(a, 0)$ to the point $P = (-x, \sqrt{a^2 - x^2})$ on the circle. This determines a point $Q = (x, y)$ on L: Prove that the cissoid is the locus of all such points Q.
3. The duplication of the cube is the classical Greek problem of trying to construct $\sqrt[3]{2}$ using ruler and compass. It is known that this is impossible given just a ruler and compass. Diocles showed that if in addition, you allow the use of the cissoid, then one construct $\sqrt[3]{2}$. Here is how it works. Draw the line connecting $(-a, 0)$ to $(0, -a/2)$. This line will meet the cissoid at a point (x, y). Then prove that

   $$2 = \left(\frac{a - x}{y}\right)^3,$$

   which shows how to construct $\sqrt[3]{2}$ using ruler, compass, and cissoid.

Proof. Let $x = t$, then

$$y = \begin{cases} \pm\sqrt{\frac{(a-t)^3}{a+t}} & \text{if } t \neq -a, \\ 0 & \text{if } t = -a. \end{cases}$$

We first compute the line between P and a to find

$$y = \frac{\sqrt{a^2 - x^2}}{-x - a}(x - a).$$

Substituting into the cissoid we see

$$\begin{aligned} y^2(a+x) &= (a-x)^3 \\ \left(\frac{\sqrt{a^2-x^2}}{-x-a}(x-a)\right)^2 (a+x) &= \frac{(a^2-x^2)(x-a)^2}{(-x-a)^2}(a+x) \\ &= \frac{(a-x)(a+x)(x-a)^2}{(a+x)^2}(a+x) \\ &= \frac{-(a-x)(a+x)(a-x)^2}{(a+x)^2}(a+x) \\ &= \frac{(a-x)^3(a+x)}{a+x} \\ &= (a-x)^3. \end{aligned}$$

Thus the cissoid is the locus of all such points Q.

We first obtain the line between $(-a, 0)$ and $\left(0, \frac{-a}{2}\right)$

$$y = -\frac{1}{2}(x - a).$$

Substituting into the curve we find

$$\begin{aligned} y^2(a+x) &= (a-x)^3 \\ \left(-\frac{1}{2}(x-a)\right)^2 (a+x) &= (a-x)^3 \\ \frac{1}{4}(x-a)^2(a+x) &= (a-x)^3 \\ \frac{1}{4}(a-x)^2(a+x) &= (a-x)^3 \\ \frac{1}{4}(a+x) &= a-x \end{aligned}$$

To see that this point lies on the cissoid notice

$$\begin{aligned} y^2(a+x) &= \left(-\frac{1}{2}(x-a)\right)^2 (a+x) \\ &= \frac{1}{4}(x-a)^2(a+x) \\ &= (a-x)^2 \cdot \frac{1}{4}(a+x) \\ &= (a-x)^2 \cdot (a-x) \\ &= (a-x)^3. \end{aligned}$$

Then

$$\begin{aligned}\left(\frac{a-x}{y}\right)^3 &= \left(\frac{a-x}{-\frac{1}{2}(x-a)}\right)^3 \\ &= \left(\frac{a-x}{\frac{1}{2}(a-x)}\right)^3 \\ &= 2\,.\end{aligned}$$

∎

Problem 11

In this problem we will derive paramtrization

$$x = t(u^2 - t^2),$$

$$y = u,$$

$$z = u^2 - t^2,$$

of the surface $x^2 - y^2z^2 + z^3 = 0$ considered in the text.

1. Adapt the formulas in part (d) of Exercise 8 to show that the curve $x^2 = cz^2 - z^3$ is parametrized by
$$z = c - t^2,$$
$$x = t(c - t^2).$$
2. Now replace the c in part (a) by y^2, and explain how this leads to the above parametrization of $x^2 - y^2z^2 + z^3 = 0$.
3. Explain why this parametrization covers the entire surface $\mathbf{V}(x^2 - y^2z^2 + z^3)$. Hint: See part (c) of Exercise 8.

Proof. Clearly from part (d) of Exercise 8 we have

$$x = t(c - t^2), \quad z = c - t^2.$$

Now, replacing the constant c with y^2 gives

$$x = t(y^2 - t^2), \quad z = y^2 - t^2.$$

Then

$$\begin{aligned}x^2 - y^2z^2 + z^3 &= \big(t(u^2 - t^2)\big)^2 - u^2(u^2 - t^2)^2 + (u^2 - t^2)^3 \\ &= t^2(u^2 - t^2)^2 - u^2(u^2 - t^2)^2 + (u^2 - t^2)^3 \\ &= (u^2 - t^2)^2\big(t^2 - u^2 + (u^2 - t^2)\big) \\ &= (u^2 - t^2)^2 \cdot 0 \\ &= 0.\end{aligned}$$

Letting $y = u$, we obtain the parametrization

$$x = t(u^2 - t^2), \quad y = u, \quad z = u^2 - t^2.$$

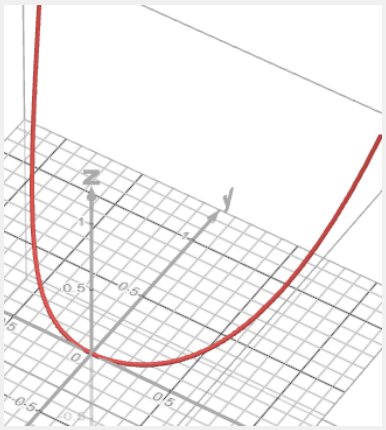
∎

Problem 12

Consider the variety $V = \mathbf{V}(y - x^2, z - x^4) \subseteq \mathbb{R}^3$.

1. Draw a picture of V.
2. Parametrize V in a way similar to what we did with the twisted cube.
3. Parametrize the tangent surface of V.

Solution (a):



Proof. Let $x = t$ then

$$x = t, \quad y = t^2, \quad z = t^4.$$

Now we have

$$r(t) = (t, t^2, t^4), \quad r'(t) = (1, 2t, 4t^3).$$

Let u be a parameter then the tangent curve is

$$\begin{aligned} r(t) + ur'(t) &= (t, t^2, t^4) + u(1, 2t, 4t^3) \\ &= (t + u, t^2 + 2tu, t^4 + 4t^3u). \end{aligned}$$

∎

1.4 Ideals

Problem 2

Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal, and let $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Prove that the following statements are equivalent.

1. $f_1, \ldots, f_s \in I$.
2. $\langle f_1, \ldots, f_s \rangle \subseteq I$.

This fact is useful when you want to show that one ideal is contained in another.

Proof. Suppose $f_1, \ldots, f_s \in I$. Let $g \in \langle f_1, \ldots, f_s \rangle$. There exist polynomials $a_1, \ldots, a_s \in k[x_1, \ldots, x_n]$ such that

$$g = a_1 f_1 + \cdots + a_s f_s.$$

Since I is an ideal and $f_1, \ldots, f_s \in I$, it follows that $g \in I$. Thus $\langle f_1, \ldots, f_s \rangle \subseteq I$.

Conversely, suppose $\langle f_1, \ldots, f_s \rangle \subseteq I$. Since each $f_i \in \langle f_1, \ldots, f_s \rangle$, it follows that $f_i \in I$ for all $i = 1, \ldots, s$. ∎

Problem 3

Use the previous exercise to prove the following equalities of ideals in $\mathbb{Q}[x, y]$.

1. $\langle x + y, x - y\rangle = \langle x, y\rangle$.
2. $\langle x + xy, y + xy, x^2, y^2\rangle = \langle x, y\rangle$.
3. $\langle 2x^3 + 3y^2 - 11, x^2 - y^2 - 3\rangle = \langle x^2 - 4, y^2 - 1\rangle$.

Proof.

$$x = \frac{1}{2}((x + y) + (x - y)), \quad y = \frac{1}{2}((x + y) - (x - y)),$$
$$x + y = 1 \cdot x + 1 \cdot y, \quad x - y = 1 \cdot x + (-1) \cdot y.$$
$$x + xy = 1 \cdot x + x \cdot y, \quad y + xy = 1 \cdot y + x \cdot y, \quad x^2 = 1 \cdot x^2, \quad y^2 = 1 \cdot y^2.$$
$$f = 2x^3 + 3y^2 - 11, \quad g = x^2 - y^2 - 3, \quad h = x^2 - 4, \quad k = y^2 - 1.$$
$$g = 1 \cdot h + (-1) \cdot k, \quad f = 2x \cdot h + 3 \cdot k + 8 \cdot x + (-8) \cdot 1,$$
$$h = 1 \cdot g + 1 \cdot k, \quad k = (-1) \cdot g + 1 \cdot h.$$

∎

Problem 4

Prove proposition 4.

Theorem 2. *If $f_1, \dots, f_s$ and $g_1, \dots, g_t$ are bases of the same ideal in $k[x_1, \dots, x_n]$, so that $\langle f_1, \dots, f_s\rangle = \langle g_1, \dots g_t\rangle$, then we have $V(f_1, \dots, f_s) = V(g_1, \dots, g_t)$.*

Proof. Let p be a point in $V(f_1, \dots, f_s)$. Then $f_i(p) = 0$ for $i \in \{1, \dots, s\}$. Since $\langle f_1, \dots, f_s\rangle = \langle g_1, \dots, g_t\rangle$, we have $g_j = \sum_{i=1}^{s} h_i f_i$ where $h_i \in k[x_1, \dots, x_n]$ and $j \in \{1, \dots, t\}$. Evaluating at p, we obtain

$$g_j(p) = \sum_{i=1}^{s} h_i(p) f_i(p) = 0.$$

Thus $\mathbf{V}(f_1, \dots, f_s) \subseteq \mathbf{V}(g_1, \dots, g_t)$. The other inclusion follows similarly, thus $\mathbf{V}(f_1, \dots, f_s) = \mathbf{V}(g_1, \dots, g_t)$. ∎

Problem 5

Show that $\mathbf{V}(x + xy, y + xy, x^2, y^2) = \mathbf{V}(x, y)$. Hint: See Exercise 3.

Proof. By part (b) of Exercise 3 we have

$$\langle x + xy, y + xy, x^2, y^2\rangle = \langle x, y\rangle.$$

Then by Proposition 4 we have $\mathbf{V}(x + xy, y + xy, x^2, y^2) = \mathbf{V}(x, y)$. ∎

Problem 6

The word "basis" is used in various ways in mathematics. In this exercise, we will see that "a basis of an ideal," as used in this section, is quite different from "a basis of a subspace," which is studied in linear algebra.

1. First, consider the ideal $I = \langle x\rangle \subseteq k[x]$. As an ideal, I has a basis consisting of the one element x. But I can also be regarded as a subspace of $k[x]$, which is a vector space over k. Prove that any vector space basis of I over k is infinite. Hint: It suffices to find one basis that is infinite. Thus,

allowing x to be multiplied by elements of $k[x]$ instead of just k is what enables $\langle x \rangle$ to have a finite basis.

2. In linear algebra, a basis must span and be linearly independent over k, whereas for an ideal, a basis is concerned only with spanning - there is no mention of any sort of independence. The reason is that once we allow polynomial coefficients, no independence is possible. To see this, consider the ideal $\langle x, y \rangle \subseteq k[x, y]$. Show that zero can be written as a linear combination of y and x with nonzero polynomial coefficients.
3. More generally, suppose that $f_1, \dots, f_s$ is the basis of an ideal $I \subseteq k[x_1, \dots, x_n]$. If $s \geq 2$ and $f_i \neq 0$ for all i, then show that for any i and j, zero can be written as a linear combination of f_i and f_j with nonzero polynomial coefficients.
4. A consequence of the lack of independence is that when we write an element $f \in \langle f_1, \dots, f_s \rangle$ as $f = \sum_{i=1}^{s} h_i f_i$, the coefficients h_i are not unique. As an example, consider $f = x^2 + xy + y^2 \in \langle x, y \rangle$. Express f as a linear combination of x and y in two different ways. (Even though the h_i's are not unique, one can measure their lack of uniqueness, one can measure and their lack of uniquess. This leads to the interesting topic of syzgies.)
5. A basisc $f_1, \dots, f_s$ of an ideal I is said to be *minimal* if no proper subset of $f_1, \dots f_s$ is a basis of I. For example, x, x^2, is a basis of an ideal, but not a minimal basis since x generates the same ideal. Unfortunately, an ideal can have minimal bases consisting of different numbers of elements. To see this, show that x and $x + x^2, x^2$ are minimal basis of the same ideal $k[x]$. Explain how this contrasts with the situation in linear algebra.

Proof. Suppose V is a finite vector space basis of $\langle x \rangle$ over k. Let f be the polynomial of maximum degree in V. Since addition by other polynomials will not increase the degree of f and multiplication is only by scalars in k, we cannot generate $x^{\deg(f)+1} \in \langle x \rangle$. Thus V does not span all of $\langle x \rangle$ and is not a basis. ∎

Proof. We have

$$(y)x + (-x)y = 0, \text{ and } (2y)x + (-2x)y = 0.$$

∎

Proof. Let f_i, f_j be nonzero elements of the basis of I with $i \neq j$. Since multiplication in $k[x_1, \dots, x_n]$ is commutative we have

$$(f_j)f_i + (-f_i)f_j = f_j f_i - f_i f_j = 0.$$

∎

Proof. We have

$$x^2 + xy + y^2 = x(x + y) + y^2,$$

and also

$$x^2 + xy + y^2 = x^2 + y(x + y).$$

Thus f can be written as a linear combination of x and y in two different ways. ∎

Proof. Now we have $\langle x \rangle = \langle x + x^2, x^2 \rangle$ since

$$x^2 \in \langle x \rangle \quad \text{and} \quad x + x^2 = x(1 + x) \in \langle x \rangle,$$

thus $\langle x + x^2, x^2 \rangle \subseteq \langle x \rangle$. Similarly

$$x = (x + x^2) - x^2 \in \langle x + x^2, x^2 \rangle,$$

thus $\langle x \rangle \subseteq \langle x + x^2, x^2 \rangle$. The basis $\{x\}$ is minimal since removing x is the emptyset. The basis $\{x + x^2, x^2\}$ is minimal since removing either results in x not being generated. In linear algebra all bases of a subspace have the same cardinality. ∎

Problem 7

Show that $\mathbf{I}(\mathbf{V}(x^n, y^m)) = \langle x, y \rangle$ for any positive integers n and m.

Proof. Any point in $\mathbf{V}(x^n, y^m)$ satisfies $x^n = 0$ and $y^m = 0$, thus $x = 0$ and $y = 0$. Thus $\mathbf{I}(\mathbf{V}(x^n, y^m))$ consists of all $f \in k[x, y]$ that vanish at the origin. These are exactly the polynomials in $\langle x, y \rangle$, so

$$\mathbf{I}(\mathbf{V}(x^n, y^m)) = \langle x, y \rangle.$$

∎

Problem 8

The ideal $\mathbf{I}(V)$ of a variety has a special property not shared by all ideals. Specifically, we define an ideal I to be *radical* if whenever a power f^m of a polynomial f is in I, then f itself is in I. More succintly, I is radical when $f \in I$ if and only if $f^m \in I$ for some positive integer m.

1. Prove that $\mathbf{I}(V)$ is always a radical ideal.
2. Prove that $\langle x^2, y^2 \rangle$ is not radical ideal. This implies that $\langle x^2, y^2 \rangle \neq \mathbf{I}(V)$ for any variety $V \subseteq k^2$.

Proof. Let $f \in \mathbf{I}(V)$ and $p \in V$. Then clearly $f(p) = 0$. Conversely, suppose $f^m \in \mathbf{I}(V)$ for some positive integer m. Then for all $p \in V$, $f^m(p) = 0$. A power of a number is zero if and only if the number itself is zero thus

$$f(p) = 0 \quad \text{for all } p \in V.$$

∎

Proof. Consider the ideal $I = \langle x^2, y^2 \rangle \subseteq k[x, y]$. Then $x^2 \in I$ and $y^2 \in I$, but

$$x \notin I \quad \text{and} \quad y \notin I.$$

∎

Problem 9

Let $V = \mathbf{V}(y - x^2, z - x^3)$ be the twisted cube. In the text we showed that $\mathbf{I}(V) = \langle y - x^2, z - x^3 \rangle$.

1. Use the Parametrization of the twisted cube to show that $y^2 - xz \in \mathbf{I}(V)$,
2. Use the argument given in the text to express $y^2 - xt$ as a combination of $y - x^2$ and $z - x^3$.

Proof. From $y^2 - xz$ and our paramtrization we have

$$y^2 - xz = (t^2)^2 - tt^3 = t^4 - t^4 = 0.$$

Also

$$\begin{aligned} y^2 - xz &= y^2 - x^4 + x^4 - xz \\ &= (y^2 - x^4) + x(x^3 - z) \\ &= (y - x^2)(y + x^2) - x(z - x^3). \end{aligned}$$

∎

Problem 10

Use the argument given in the discussion of the twisted cube to show that $\mathbf{I}(\mathbf{V}(x-y)) = \langle x-y \rangle$. Your argument should be valid for any infinite field k.

Proof. First, we have $x - y \in \mathbf{I}(V)$ and since $\mathbf{I}(V)$ is an ideal it follows that $h_1(x-y) \in \mathbf{I}(V)$. Thus $\langle x-y \rangle \subseteq \mathbf{I}(V)$. We first note that the parametrization of $V(x-y)$ is

$$(x, y) = (t, t) \text{ for } t \in k.$$

Now, we know a general polynomial $f \in k[x, y]$ can be expressed as

$$f = h(x, y)(x - y) + r(y),$$

where $r(y)$ is a polynomial in y alone. We now suppose $f \in \mathbf{I}(V)$ and use the parametrization to find

$$0 = f(t, t) = h(t, t)(t - t) + r(t) = r(t).$$

Since k is infinite, this implies $r = 0$. Thus $f = h(x, y)(x - y)$ and therefore

$$\mathbf{I}(\mathbf{V}(x - y)) \subseteq \langle x - y \rangle.$$

∎

Problem 11

Let $V \subseteq \mathbb{R}^3$ be the curve parametrized by (t, t^3, t^4).
1. Prove that V is an affine variety.
2. Adapt the method used in the case of the twisted cube to determine $\mathbf{I}(V)$.

Proof. Consider $x^3 - y, x^4 - z$ and notice using the parametrization we have

$$x^3 - y = t^3 - t^3 = 0, \text{ and } x^4 - z = t^4 - t^4 = 0.$$

Thus V is an affine variety.

Conversely, suppose $(x, y, z) \in \mathbf{V}(x^3 - y, x^4 - z)$. Then

$$y = x^3, \quad z = x^4.$$

Let $t = x$. Then

$$(x, y, z) = (t, t^3, t^4),$$

so $(x, y, z) \in V$. Therefore,

$$V = \mathbf{V}(x^3 - y, x^4 - z),$$

∎

Proof. We already know that

$$\langle x^3 - y,\ x^4 - z \rangle \subseteq \mathbf{I}(V).$$

Now, we know a general polynomial $f \in k[x, y, z]$ can be expressed as

$$f = h_1(x, y, z)(x^3 - y) + h_2(x, y, z)(x^4 - z) + r(x),$$

where $r(x)$ is a polynomial in x alone. We now suppose $f \in \mathbf{I}(V)$ and use the parametrization to find

$$0 = f(t, t^3, t^4) = h_1(t, t^3, t^4)(t^3 - t^3) + h_2(t, t^3, t^4)(t^4 - t^4) + r(t) = r(t).$$

Since k is infinite, this implies $r = 0$. Thus

$$f = h_1(x, y, z)(x^3 - y) + h_2(x, y, z)(x^4 - z),$$

and therefore

$$\mathbf{I}(V) \subseteq \langle x^3 - y,\ x^4 - z \rangle.$$

∎

Problem 14

This exercise is concerned with Proposition 8.

1. Prove that part (ii) of the proposition follows from part (i).
2. Prove the following corollary of the proposition: if V and W are affine varieties in k^n, then $V \subseteq W$ if and only if $\mathbf{I}(V) \supseteq \mathbf{I}(W)$.

Theorem 3. *Let V and W be affine varieties in k^n. Then:*

1. *$V \subseteq W$ if and only if $\boldsymbol{I}(V) \supseteq \boldsymbol{I}(W)$.*
2. *$V = W$ if and only if $\boldsymbol{I}(V) = \boldsymbol{I}(W)$.*

Proof. Suppose $V = W$. Since $V \subseteq W$ by Part (1) we have $\mathbf{I}(V) \supseteq \mathbf{I}(W)$. Similarly, since $W \subseteq V$ we have $\mathbf{I}(W) \supseteq \mathbf{I}(V)$. Thus $\mathrm{I}(V) = \mathbf{I}(W)$.

Conversely, suppose $\mathrm{I}(V) = \mathbf{I}(W)$. Since $\mathbf{I}(V) \supseteq \mathbf{I}(W)$ by Part (1), we have $V \subseteq W$. Similarly, since $\mathbf{I}(W) \supseteq \mathbf{I}(V)$ we have $W \subseteq V$. Thus $V = W$. ∎

Proof. This is Part (1) which is proven in the text. ∎

Problem 15

In the text, we define $\mathbf{I}(V)$ for a variety $V \subseteq k^n$. We can generalize this as follows: if $S \subseteq k^n$ is any subset, then we set

$$\mathbf{I}(S) = \{f \in k[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0 \text{ for all } (a_1, \ldots, a_n) \in S\}.$$

1. Prove that $\mathbf{I}(V)$ is an ideal.
2. Let $X = \{(a, a) \in \mathbb{R}^2 \mid a \neq 1\}$. By Exercise 8 of 2, we know that X is not an affine variety. Determine $\mathbf{I}(X)$. Hint: What you proved in Exercise 8 of 2 will be useful. See also Exercise 10 of this section.
3. Let $\mathbb{Z}^n$ be the points of $\mathbb{C}^n$ with integer coordinates. Determine $\mathbf{I}(\mathbb{Z}^n)$. Hint: See Exercise 6 of 1.

Proof. Suppose $f, g \in I(S)$ and $p \in S$. Then

$$(f + g)(p) = f(p) + g(p) = 0 + 0 = 0.$$

Let $r \in k[x_1, \ldots, x_n]$. Then

$$(rf)(p) = r(p)f(p) = r(p) \cdot 0 = 0.$$

Thus $I(S)$ is an ideal. ∎

Proof. Suppose $f \in I(X)$. Then $f(a, a) = 0$ for all $a \neq 1$. But any polynomial in two variables that vanishes on all points of the form (a, a) with $a \neq 1$ must vanish on the line $x = y$. Therefore, f is divisible by $x - y$ thus $I(X) = \langle x - y \rangle$, ∎

Proof. Suppose $f \in I(\mathbb{Z}^n)$. Then $f(a_1, \dots, a_n) = 0$ for all integers $a_1, \dots, a_n$. But a nonzero polynomial in n variables can only have finitely many zeros in any one variable if the others are fixed. Therefore, $I(\mathbb{Z}^n) = \{0\}$. ∎

Problem 16

Here is more practice with ideals. Let I be an ideal in $k[x_1, \dots, x_n]$.

1. Prove that $1 \in I$ if and only if $I = k[x_1, \dots, x_n]$,
2. More generally, prove that I contains a nonzero constant if and only if $I = k[x_1, \dots, x_n]$.
3. Suppose $f, g \in k[x_1, \dots, x_n]$ satisfy $f^2, g^2 \in I$. Prove that $(f+g)^3 \in I$. Hint: Expand $(f+g)^3$ using the binomial theorem.
4. Now suppose $f, g \in k[x_1, \dots, x_n]$ satisfy $f^r, g^s \in I$. Prove that $(f+g)^{r+s-1} \in I$.

Proof. Suppose $1 \in I$. Let f be an arbitrary polynomial in $k[x_1, \dots, x_n]$. Since I is closed under multiplication we have $1 \cdot f = f \in I$. Thus $I = k[x_1, \dots, x_n]$.

Conversely, suppose $I = k[x_1, \dots, x_n]$. Since $1 \in k[x_1, \dots, x_n]$ we have $1 \in I$. ∎

Proof. Suppose I contains a nonzero constant c. Let f be an arbitrarily polynomial in $k[x_1, \dots, x_n]$. Since k is a field we have $\frac{f}{c^{-1}} \in k[x_1, \dots, x_n]$. Then, since I is closed under multiplicaion we have $c \cdot \frac{f}{c^{-1}} = f \in I$. Thus $I = k[x_1, \dots, x_n]$.

Conversely, suppose $I = k[x_1, \dots, x_n]$. Let c be a nonzero constant. Since $c \in k[x_1, \dots, x_n]$ we have $c \in I$. ∎

Proof. Notice

$$(f+g)^3 = f^3 + 3f^2g + 3fg^2 + g^3 = ff^2 + 3gf^2 + 3fg^2 + g^3,$$

which constists of scaling by polynomials in $k[x_1, \dots, x_n]$ and addition in I. Thus $(f+g)^3 \in I$. ∎

Proof. Consider the binomial expansion

$$(f+g)^{r+s-1} = \sum_{k=0}^{r+s-1} \binom{r+s-1}{k} f^k g^{r+s-1-k}.$$

For each term $f^k g^{r+s-1-k}$, either $k \geq r$ or $r+s-1-k \geq s$. If $k \geq r$, then $f^k = f^r \cdot f^{k-r} \in I$, since $f^r \in I$ and I is closed under multiplication by polynomials. If $r+s-1-k \geq s$, then $g^{r+s-1-k} = g^s \cdot g^{r+s-1-k-s} \in I$, since $g^s \in I$. Each term is therefore in I, and since I is closed under addition $(f+g)^{r+s-1} \in I$. ∎

Problem 17

In the proof of Lemma 7, we showed that $x \notin \langle x^2, y^2 \rangle$ in $k[x, y]$.

1. Prove that $xy \notin \langle x^2, y^2 \rangle$.
2. Prove that $1, x, y, xy$ are not monomials not contained in $\langle x^2, y^2 \rangle$.

Proof. Suppose $xy \in \langle x^2, y^2 \rangle$. Then we must have

$$xy = f(x,y)x^2 + g(x,y)y^2,$$

for some $f, g \in k[x, y]$. But $\deg_x(xy) = 1$ while $\deg_x(f(x,y)x^2 + g(x,y)y^2) \geq 2$, which is a contradiction. Thus $xy \notin \langle x^2, y^2 \rangle$. ∎

Proof. Suppose $1 \in \langle x^2, y^2 \rangle$. Then we must have

$$1 = f(x,y)x^2 + g(x,y)y^2,$$

for some $f, g \in k[x,y]$. But $\deg_x(1) = 0$ while $\deg_x(f(x,y)x^2 + g(x,y)y^2) \geq 2$, a contradiction. Thus $1 \notin \langle x^2, y^2 \rangle$.
Suppose $x \in \langle x^2, y^2 \rangle$. Then we must have

$$x = f(x,y)x^2 + g(x,y)y^2.$$

But $\deg_x(x) = 1$ while $\deg_x(f(x,y)x^2 + g(x,y)y^2) \geq 2$, a contradiction. Thus $x \notin \langle x^2, y^2 \rangle$.
Suppose $y \in \langle x^2, y^2 \rangle$. Then we must have

$$y = f(x,y)x^2 + g(x,y)y^2.$$

But $\deg_y(y) = 1$ while $\deg_y(f(x,y)x^2 + g(x,y)y^2) \geq 2$, a contradiction. Thus $y \notin \langle x^2, y^2 \rangle$.

Suppose $xy \in \langle x^2, y^2 \rangle$. Then we must have

$$xy = f(x,y)x^2 + g(x,y)y^2.$$

But $\deg_x(xy) = 1$ while $\deg_x(f(x,y)x^2 + g(x,y)y^2) \geq 2$, a contradiction. Thus $xy \notin \langle x^2, y^2 \rangle$. ∎

Problem 18

In the text, we showed that $\mathbf{I}(\{0,0\}) = \langle x, y \rangle$ in $k[x,y]$.

1. Generalize this by proving that the origin $0 = (0, \dots, 0) \in k^n$ has the property that $\mathbf{I}(\{0\}) = \langle x_1, \dots, x_n \rangle$ in $k[x_1, \dots, x_n]$.
2. What does part (a) say about polynomials in $k[x_1, \dots, x_n]$ with zero constant term?

Proof. One direction is trivial. For any polynomial of the form

$$F_1(x_1, \dots, x_n)x_1 + \cdots + F_n(x_1, \dots, x_n)x_n,$$

it clearly vanishes at the origin. For the other direction, suppose

$$f = \sum_{t_1, \dots, t_n} a_{t_1, \dots, t_n} x_1^{t_1} \cdots x_n^{t_n}$$

vanishes at the origin. Then

$$a_{0,\dots,0} = f(0, \dots, 0) = 0,$$

and consequently

$$\begin{aligned} f &= a_{0,\dots,0} + \sum_{(t_1,\dots,t_n) \neq (0,\dots,0)} a_{t_1,\dots,t_n} x_1^{t_1} \cdots x_n^{t_n} \\ &= 0 + \sum_{(t_1,\dots,t_n) \neq (0,\dots,0)} a_{t_1,\dots,t_n} x_1^{t_1} \cdots x_n^{t_n} \in \langle x_1, \dots, x_n \rangle. \end{aligned}$$

Thus, any polynomial vanishing at the origin lies in $\langle x_1, \dots, x_n \rangle$, proving the claim. ∎

Solution: This says that any polynomial in $k[x_1, \dots, x_n]$ with zero constant term can be factored as a linear combination of $x_1, \dots, x_n$, and is in the ideal $\langle x_1, \dots, x_n \rangle$.

1.5 Polynomials of One Variable

Problem 1

Over the complex numbers $\mathbb{C}$, Corollary 3 can be stated in a stronger form. Namely, prove that if $f \in \mathbb{C}[x]$ is a polynomial of degree $n > 0$, then f can be written in the form $f = c(x - a_1) \cdots (x - a_n)$, where $c, a_1, \ldots, a_n \in \mathbb{C}$ and $c \neq 0$. Hint: Use Theorem 7 of 1. Note that this results holds for any algebraically closed field.

Proof. Suppose $f \in \mathbb{C}[x]$ is a polynomial of degree $n > 0$. By Theorem 7, f has a root in $\mathbb{C}$, say a_1. Then f can be written as $f = (x - a_1)g_1(x)$ where $g_1 \in \mathbb{C}[x]$. Then $\deg(g_1) = \deg(f) - 1$. If $\deg(g_1) = 0$, then let $c = g_1(x)$ and we are done. Otherwise, repeat the process of extracting a linear factor from g_1 using Theorem 7. Continuing in this way, we eventually obtain

$$f = c(x - a_1) \cdots (x - a_n),$$

where $c \in \mathbb{C}$ and $c \neq 0$. ∎

Problem 3

The fact that every ideal of $k[x]$ is principal (generated by one element) is special to the case of polynomials in one variable. In this exercise we will see why. Namely, consider the ideal $I = \langle x, y \rangle \subseteq k[x, y]$. Prove that I is not principal ideal.

Proof. For contradiction, suppose $I = \langle x, y \rangle = \langle f \rangle$ where $f \in \mathbb{C}[x, y]$. Now, there must exist $g \in \mathbb{C}[x, y]$ such that $x = fg$. Now since $\deg_x(x) = 1$ we must have either $\deg_x(f) = 1$ or $\deg_x(g) = 1$. Suppose wlog $\deg_x(f) = 1$, since $\deg_x(x) = \deg_x(f) + \deg_x(g) = 1$, we have $\deg_x(g) = 0$. Clearly $\deg_y(g) = 0$ thus g is a constant. But then $f = \frac{x}{g}$, so f is a constant multiple of x. Therefore $\langle f \rangle = \langle x \rangle$, which cannot generate y. Thus I is not a principal ideal. ∎

Problem 4

If h is the gcd of $f, g \in k[x]$, then prove that there are $A, B \in k[x]$ such that $Af + Bg = h$.

Proof. Suppose h is the gcd of $f, g \in k[x]$. Consider the ideal $\langle f, g \rangle \subseteq k[x]$. Since every ideal of $k[x]$ is principal, we have $\langle f, g \rangle = \langle d \rangle$ for some $d \in k[x]$. Then there exist $A, B \in k[x]$ such that $Af + Bg = d$. Since d divides both f and g, and h is the greatest common divisor, we must have $d = h$ up to multiplication by a nonzero constant. Thus there exist $A, B \in k[x]$ such that $Af + Bg = h$. ∎

Problem 5

If $f, g \in k[x]$, then prove that $\langle f - qg, g \rangle = \langle f, g \rangle$ for any q in $k[x]$.

Proof. Notice that $g \in \langle f, g \rangle$ and

$$f - qg = 1 \cdot f + (-q) \cdot g \in \langle f, g \rangle.$$

thus

$$\langle f - qg, g \rangle \subseteq \langle f, g \rangle.$$

Conversely, notice that

$$f = (f - qg) + qg.$$

Since $f - qg, g \in \langle f - qg, g \rangle$ we have $f \in \langle f - qg, g \rangle$. Also, $g \in \langle f - qg, g \rangle$. Thus

$$\langle f, g \rangle \subseteq \langle f - qg, g \rangle.$$

Problem 6

Given $f_1, \dots, f_s \in k[x]$, let $h = gcd(f_2, \dots, f_s)$. Then use the equality of $\langle h \rangle = \langle f_2, \dots, f_2 \rangle$ to show that $\langle f_1, h \rangle = \langle f_1, f_2, \dots, f_s \rangle$

Proof. This is obvious since

$$gcd(f_1, \dots, f_s) = gcd(f_1, gcd(\dots, f_s)).$$

Problem 7

If you are allowed to compute the gcd of two polynomials at a tie (which is true for some computer algebra systems), give pseudocode for an algorithm that computes the gcd of polynomials $f_1, \dots, f_s \in k[x]$, where $s > 2$. Prove that your algorithm works.

Proof. Here is the program.

```
polynomial cur_gcd = f_1;

for (int i = 2; i <= s; i++) {
    cur_gcd = gcd(cur_gcd, f_i);
}

return cur_gcd;
```

Obviously works by problem 6.

Problem 11

In this exercise we will study the one-variable case of the consistency problem from 2. Given $f_1, \dots, f_s \in k[x]$, this asks if there is an algorithm to decide whether $\mathbf{V}(f_1, \dots, f_s)$ is nonempty. We will see that hte answer is yes when $k = \mathbb{C}$.

1. Let $f \in \mathbb{C}[x]$ be a nonzero polynomial. Then use Theorem 7 of 1 to show that $\mathbf{V}(f) = \emptyset$ if and only if f is constant.
2. If $f_1, \dots, f_s \in \mathbb{C}[x]$, prove $\mathbf{V}(f_1, \dots, f_s) = \emptyset$ if and only if $gcd(f_1, \dots, f_s) = 1$.
3. Describe (in words, not pseudocode) an algorithm for determining whether or not $\mathbf{V}(f_1, \dots, f_s)$ is nonempty.

Proof. Suppose $\mathbf{V}(f) = \emptyset$. For contradiction, suppose f is not a nonzero constant. Then $\deg(f) > 0$ and by Theorem 7 can be written as $f = (x - a)g(x)$ where $g \in \mathbb{C}[x]$ and a is a root. But then $f(a) = (a - a)g(a) = 0 \cdot g(a) = 0$. Thus $a \in \mathbf{V}(f)$, which is a contradiction.

Suppose f is a nonzero constant. For contradiction, suppose $\mathbf{V}(f) \neq \emptyset$. Let $a \in \mathbf{V}(f)$. Then $f(a) = 0$ and since $f \neq 0$ by Theorem 7 we must have $f = (x - a)g(x)$ where $g \in \mathbb{C}[x]$. But then $\deg(f) = \deg((x - a)g(x)) \geq 1$, which is a contradiction.

Proof. Suppose $f_1, \dots, f_s \in \mathbb{C}[x]$.

Furthermore, suppose $\mathbf{V}(f_1, \dots, f_s) = \emptyset$. If $\gcd(f_1, \dots, f_s) \neq 1$, then there must be a polynomial g such that $\deg(g) \geq 1$ and $g \mid f_1, \dots, f_s$. But then by Theorem 7, g has $\deg(g)$ roots and therefore there are $\deg(g)$ points in $\mathbf{V}(f_1, \dots, f_s)$, which is a contradiction. Thus $\gcd(f_1, \dots, f_s) = 1$.

Conversely, suppose $\gcd(f_1, \dots, f_s) = 1$. If $\mathbf{V}(f_1, \dots, f_s) \neq \emptyset$, then there is a linear factor, say $(x - a)$, such that $(x - a) \mid f_1, \dots, f_s$, contradicting $\gcd(f_1, \dots, f_s) = 1$. Thus $\mathbf{V}(f_1, \dots, f_s) = \emptyset$. ∎

Solution: Repeatedly apply the gcd algorithm to the polynomials. If it is 1 in the end, then $\mathbf{V}(f_1, \dots, f_s) = \emptyset$.

Problem 12

This exercise will study the one-variable case of the *Nullstellensatz problem* from 4, which asks for the relation between $\mathbf{I}(\mathbf{V}(f_1, \dots, f_s))$ and $\langle f_1, \dots, f_s \rangle$ when $f_1, \dots, f_s \in \mathbb{C}[x]$. By using gcd's, we can reduce to the case to a single generator. So, in this problem, we will explicitly determine $\mathbf{I}(\mathbf{V}(f))$ where $f \in \mathbb{C}[x]$ is a nonconstant polynomial. Since we are working over the complex numbers, we know by Exercise 1 that f factors completely, i.e.,

$$f = c(x - a_1)^{r_1} \cdots (x - a_1)^{r_l},$$

where $a_1, \dots, a_l \in \mathbb{C}$ are distinct and $c \in \mathbb{C} - \{0\}$. Define the polynomial

$$f_{red} = c(x - a_1) \cdots (x - a_l).$$

The polynomials f and f_{red} have the same roots but their *multiplicities* may differ. In particular, all roots of f_{red} have multiplicity one. We call f_{red} the *reduced* or *square-free* part of f. The latter name recognizes that f_{red} is the square-free factor of f of largest degree.

1. Show that $\mathbf{V}(f) = \{a_1, \dots, a_1\}$.
2. Show that $\mathbf{I}(\mathbf{V}(f)) = \langle f_{red} \rangle$.

Proof. Let $p \in \mathbf{V}(f)$. Then p must be a root of f, so $p \in \{a_1, \dots, a_l\}$. Conversely, let $a_i \in \{a_1, \dots, a_l\}$. Then

$$f(a_i) = c(x - a_1)^{r_1} \cdots (x - a_i)^{r_i} \cdots (x - a_l)^{r_l} \Big|_{x = a_i} = 0.$$

Thus $a_i \in \mathbf{V}(f)$. Therefore, $\mathbf{V}(f) = \{a_1, \dots, a_l\}$. ∎

Proof. Notice f_{red} vanishes at all $a_1, \dots, a_l$, so $f_{red} \in \mathbf{I}(\mathbf{V}(f))$. Conversely, let $g \in \mathbf{I}(\mathbf{V}(f))$. Since g vanishes at all $a_1, \dots, a_l$, each $(x - a_i)$ divides g. Thus $f_{red} \mid g$ and $g \in \langle f_{red} \rangle$. ∎

Problem 13

We will study the formal derivative of

$$f = c_0 x^n + c_1 x^{n-1} + \cdots + c_{n-1} + 0.$$

Prove that the following rules of differentiation apply:

$$(af)' = af' \text{ when } a \in \mathbb{C},$$

$$(f + g)' = f' + g',$$

$$(fg)' = f'g + fg'.$$

Proof. These all follow from the basic properties of deriatives learned in calculus 1 ¯_( )_/¯. ∎

Problem 14

In this exercise we will use the differentation properties of Exercise 13 to compute $gcd(f, f')$ when $f \in \mathbb{C}[x]$.

1. Suppose $f = (x-a)^r \in \mathbb{C}[x]$, where $r \geq 1$ and $h(a) \neq 0$. Then prove that $f' = (x-a)^{r-1}h_1$, where $h_1 \in \mathbb{C}[x]$ does not vanish at a. Hint: use the product rule.
2. Let $f = c(x-a_1)^{r_1} \cdots (x-a)^{r_l}$ be the factorization of f, where $a_1, \cdots, a_l$ are distinct. Prove that f' is a product $f' = (x-a_1)^{r_1-1} \cdots (x-a_l)^{r_l-1}H$, where $H \in \mathbb{C}[x]$ is a polynomial vanishing at none of $a_1, \ldots, a_l$.
3. Prove that $gcd(f, f') = (x-a_1)^{r_1-1} \cdots (x-a_1)^{r_l-1}$.

Proof. We have

$$f' = r(x-a)^{r-1}.$$

We can write $f' = (x-a)^{r-1}h_1(x)$ with $h_1(x) = r$, and clearly $h_1(a) \neq 0$ since $r \neq 0$. ∎

Proof. Let

$$f = c(x-a_1)^{r_1} \cdots (x-a_l)^{r_l}.$$

Then by the product rule, f' can be written as

$$f' = (x-a_1)^{r_1-1} \cdots (x-a_l)^{r_l-1}H(x),$$

where $H(x) \in \mathbb{C}[x]$ does not vanish at any a_i. Thus,

$$\gcd(f, f') = (x-a_1)^{r_1-1} \cdots (x-a_l)^{r_l-1}.$$

∎

Problem 15

Consider the square-free part of f_{red} of a polynomial $f \in \mathbb{C}[x]$ defined in Exercise 12.

1. Use Exercise 14 to prove that f_{red} is given by the formula

$$f_{red} = \frac{f}{gcd(f, f')}.$$

   The virtue of this formula is that it allows us to find the square-free part without factoring f. This allows for much quicker computations.
2. Use a computer algebra system to find the square-free part of the polynomial

$$x^{11} - x^{10} + 2x^8 - 4x^7 + 3x^5 - 3x^4 + x^3 + 3x^2 - x - 1.$$

Proof. Let

$$f = c(x-a_1)^{r_1} \cdots (x-a_l)^{r_l}$$

be the factorization of f over $\mathbb{C}$. By Exercise 14, we have

$$f' = (x-a_1)^{r_1-1} \cdots (x-a_l)^{r_l-1}H(x),$$

where for $a_1, \ldots, a_l$, we have $H(a_i) \neq 0$. The greatest common divisor $\gcd(f, f')$ is then

$$\gcd(f, f') = (x-a_1)^{r_1-1} \cdots (x-a_l)^{r_l-1}.$$

Thus dividing f by $\gcd(f, f')$ gives

$$\frac{f}{\gcd(f, f')} = (x-a_1) \cdots (x-a_l) = f_{red},$$

which is exactly the square-free part of f. ∎

Solution (2): I plugged it in and saw the answer but it was too large to put in the margins...

Problem 16

Use Exercise 12 and Exercise 15 to describe (in words, not in pseudocode) an algorithm whose input consists of polynomials $f_1, \dots, f_s \in \mathbb{C}[x]$ and whose output consists of a basis of $\mathbf{I}(\mathbf{V}(f_1, \dots, f_s))$. It is more difficult to construct such an algorithm when dealing with polynomials of more than one variable.

Solution: Compute the gcd of $f_1, \dots, f_s$. Using Exercise 15, compute the square-free part of g

$$g_{red} = \frac{g}{\gcd(g, g')}.$$

By Exercise 12, the ideal of the variety is then

$$\mathbf{I}(\mathbf{V}(f_1, \dots, f_s)) = \langle g_{red} \rangle.$$

2 Grobner Bases

2.1 Introduction

Problem 4

Let $x_1, x_2, x_3, \dots$ be an infinite collection of independent variables indexed by the natural numbers. A polynomial with coefficients in a field k in the x_i is a finite linear combination of (finite) monomials $x_{i_1}^{e_1} \dots x_{i_n}^{e_n}$. Let R detote the set of all polynomials in x_i. Note that we an add and multiply elements of R in the usual way. Thus, R is the polynomial ring, $k[x_1, x_2, \dots]$ in infinitely many variables.

1. Let $I = \langle x_1, x_2, \dots \rangle$ be the set of $f = \sum_{i=1}^{\infty} A_i x_i$, where $A_i = 0$ for all i sufficiently large. Show that I is an ideal in the ring R.
2. Show, arguing by contradiction, that I has no finite generating set. Hint: note that if $I = \langle g_1, \dots, g_m \rangle$, then there must be some variable x_l that is not contained in any of the g_j.

Proof. Let $p \in k[x_1, x_2, \dots]$. Let $f, g \in I$ with j, j' being sufficiently large such that $A_j = 0$ and $A_{j'} = 0$. Then $f + g = \sum_{i=1}^{\infty} A_i x_i + \sum_{i=1}^{\infty} B_i x_i = \sum_{i=1}^{\infty} (A_i + B_i) x_i \in I$. Also, $p \cdot f = p \cdot \sum_{i=1}^{\infty} A_i x_i \in I$ because it is a finite sum of monomials in the x_i. Thus I is an ideal. ∎

Proof. Suppose, for contradiction, that I has a finite generating set $\langle g_1, \dots, g_m \rangle$ for some $m \in \mathbb{N}$. Then there exists some variable x_l that does not appear in any of the g_j. Clearly, x_l cannot be expressed as a linear combination of the other generators. Thus x_l is not in the ideal generated by $g_1, \dots, g_m$, contradicting that they generate I. ∎

Problem 5

In this problem you will show that all polynomial parametric curves in k^2 are contained in affine varieties.

1. Show that the number of distinct monomials $x^a y^b$ of total degree $\leq m$ in $k[x, y]$ is equal to $(m + 1)(m + 2)/2$. [Note: This is the binomial coefficients $\binom{m+2}{2}$.]
2. Show that if $f(t)$ and $g(t)$ are polynomials of degree $\leq n$ in t, then for m large enough, the "monomials"
$$[f(t)]^a[g(t)]^b,$$
with $a + b \leq m$ are linearly *dependent*.
3. Deduce form part (b) that if C is a curve in k^2 given parametrically by $x = f(t), y = g(t)$ for $f(t), g(t) \in k[t]$, then C is contained in $\mathbf{V}(F)$ for some nonzero $F \in k[x, y]$
4. Generalize parts (a), (b), and (c) to show that any polynomial parametric surface
$$x = f(t, u), \quad y = g(t, u), \quad z = h(t, u),$$
is contained in an algebraic surface $\mathbf{V}(f)$, where $F \in k[x, y, z]$ is nonzero.

Part 1. The number of monomials $x^a y^b$ of total degree $\leq m$ is the number of (a, b) such that $a + b \leq m$. For each $a = 0, 1, \ldots, m$, b can range from 0 to $m - a$, giving $m - a + 1$ choices. Thus

$$\sum_{a=0}^{m}(m - a + 1) = \sum_{a=0}^{m}(m + 1) - \sum_{a=0}^{m} a = (m + 1)(m + 1) - \frac{m(m + 1)}{2} = \frac{(m + 1)(m + 2)}{2}.$$

∎

Part 2. Suppose $f(t)$ and $g(t)$ are polynomials of degree $\leq n$ in t. Then $\deg(f(t)^a) \leq an$ and $\deg(g(t)^b) \leq bn$, so

$$\deg([f(t)]^a[g(t)]^b) = \deg(f(t)^a) + \deg(g(t)^b) \leq an + bn = n(a + b) \leq nm.$$

There are $\frac{(m+1)(m+2)}{2}$ such polynomials. For m large enough,

$$\frac{(m + 1)(m + 2)}{2} > nm + 1,$$

so these polynomials are linearly dependent. ∎

Part 3. By part 2, for sufficiently large m there is some linear combination

$$a_1 x^0 y^0 + a_2 x^1 y^0 + a_3 x^0 y^1 + \cdots = 0,$$

with at least one $a_i \neq 0$. Then taking $x = f(t)$ and $y = g(t)$, gives

$$a_1[f(t)]^0[g(t)]^0 + a_2[f(t)]^1[g(t)]^0 + a_3[f(t)]^0[g(t)]^1 + \cdots = 0$$

for all t. Let

$$F(x, y) = a_1 x^0 y^0 + a_2 x^1 y^0 + a_3 x^0 y^1 + \cdots \in k[x, y].$$

Then $F(f(t), g(t)) = 0$ for all t thus $C \subset \mathbf{V}(F)$. ∎

Part 4. Consider all monomials

$$[f(t, u)]^a[g(t, u)]^b[h(t, u)]^c$$

of total degree $\leq m$. For m large enough, the number of such monomials exceeds the dimension of the vector space of polynomials in t, u of that degree. Thus there exists a linear combination

$$F(x, y, z) = \sum a_{a,b,c} x^a y^b z^c \in k[x, y, z]$$

that vanishes when evaluated on the surface

$$F(f(t, u), g(t, u), h(t, u)) = 0.$$

Therefore, the surface is contained in $\mathbf{V}(F)$. ∎

2.2 Orderings on the Monomials in $k[x_1, \ldots, x_n]$

Problem 1

Rewrite each of the following polynomials, ordering the terms using lex order, grlex order, and grevlex order, giving $LM(f), LT(f)$, and $multideg(f)$ in each case.

1. $f_1(x, y, z) = 2x + 3y + z + x^2 - z^2 + x^3$.
2. $f_2(x, y, z) = 2x^2y^8 - 3x^5yz^4 + xyz^3 - xy^4$.

Solution (lex order): For f_1, we have the following exponent vectors

$$(1, 0, 0),\ (0, 1, 0),\ (0, 0, 1),\ (2, 0, 0),\ (0, 0, 2),\ (3, 0, 0).$$

Reordering in lex order $(x > y > z)$ gives

$$x^3 + x^2 + 2x + 3y - z^2 + z.$$

So

$$LM(f_1) = x^3, \quad LT(f_1) = x^3, \quad multideg(f_1) = (3, 0, 0).$$

For f_2, the exponent vectors are

$$(2, 8, 0),\ (5, 1, 4),\ (1, 1, 3),\ (1, 4, 0).$$

Reordering in lex order gives

$$-3x^5yz^4 + 2x^2y^8 - xy^4 + xyz^3.$$

So:

$$LM(f_2) = x^5yz^4, \quad LT(f_2) = -3x^5yz^4, \quad multideg(f_2) = (5, 1, 4).$$

Solution (grlex order): For f_1, compute total degrees

$$|2x| = 1,\ |3y| = 1,\ |z| = 1,\ |x^2| = 2,\ |-z^2| = 2,\ |x^3| = 3.$$

Sort by total degree, breaking ties with lex order

$$x^3 - x^2 - z^2 + 2x + 3y + z$$

$$LM(f_1) = x^3, \quad LT(f_1) = x^3, \quad multideg(f_1) = (3, 0, 0)$$

For f_2, total degrees

$$2x^2y^8 = 10, \quad -3x^5yz^4 = 10, \quad xyz^3 = 5, \quad -xy^4 = 5$$

Sorting by total degree, then lex to break ties

$$-3x^5yz^4 + 2x^2y^8 - xy^4 + xyz^3$$

$$LM(f_2) = x^5yz^4, \quad LT(f_2) = -3x^5yz^4, \quad multideg(f_2) = (5, 1, 4)$$

Solution (grevlex order): For f_1, total degrees as before: 1,1,1,2,2,3

$$x^3 + x^2 + 2x - z^2 + z + 3y$$

$$LM(f_1) = x^3, \quad LT(f_1) = x^3, \quad multideg(f_1) = (3, 0, 0)$$

For f_2, total degrees as before: 10,10,5,5

$$-3x^5yz^4 + 2x^2y^8 + xyz^3 - xy^4$$

$$LM(f_2) = x^2y^8, \quad LT(f_2) = 2x^2y^8, \quad multideg(f_2) = (2, 8, 0)$$

Problem 4

Show that grlex is a monomial order according to Definition 1.

Proof. Grlex compares monomials first by total degree, then by lex order to break ties. Since total degree is a total order on nonnegative integers, and lex order is a total order on exponent vectors, the composition of these two total orders is again a total order. Thus grlex is a monomial order. ∎

Problem 5

Show that grevlex is a monomial order according to Definition 1.

Proof. Grevle compares monomials first by total degree, then by reverse lex order to break ties. Again, total degree is a total order and reverse lex is a total order on exponent vectors, so their composition is a total order. Therefore, grevlex is a monomial order, just as in Problem 4. ∎

Problem 7

Let $>$ be any monomial order.

1. Show that $\alpha \geq 0$ for all $\alpha \in \mathbb{Z}^n_{\geq 0}$. Hint: Proof by contradiction.
2. Show that if x^α divides x^β, then $\alpha \leq \beta$. Is the converse true?
3. Show that if $\alpha \in \mathbb{Z}^n_{\geq 0}$, then α is the smallest element of $\alpha + \mathbb{Z}^n_{\geq 0} = \{\alpha + \beta \mid \beta \in \mathbb{Z}^n_{\geq 0}\}$.

Problem 10

In $\mathbb{Z}_{\geq 0}$ with the usual order, between any two integers, there are only a finite number of other integers. Is this necessarily true in $\mathbb{Z}^n_{\geq 0}$ for a monomial order? Is it true for grlex?

Problem 11

Let $>$ be a monomial order on $k[x_1, \ldots, x_n]$.

1. Let $f \in k[x_1, \ldots, x_n]$ and let m be a monomial. Show that $LT(m \cdot f) = m \cdot LT(f)$.
2. Let $f, g \in k[x_1, \ldots, x_n]$. Is $LT(f \cdot g)$ necessarily the same as $LT(f) \cdot LT(g)$?
3. If $f_i, g_i \in k[x_1, \ldots, x_n]$, $1 \leq i \leq x$, is $LM(\sum_{i=1}^{s} f_i g_i)$ ncecessarily equal to $LM(f_i) \cdot LM(g_i)$ for some i?

Problem 12

Lemma 8 gives two properties of the multidegree.

1. Prove Lemma 8. Hint: The arguments used in Exercise 11 may be relevant.
2. Suppose that $multideg(f) = multideg(g)$ and $f + g \neq 0$. Give examples to show that $multideg(f + g)$ may or may not equal $max(multideg(f), multideg(g))$.

Problem 13

Prove that $1 < x < x^2 < x^3 < \cdots$ is the unique monimial order on $k[x]$.