Chapter 2 §1. Introduction

The Ideal Description Problem: The Hilbert Basis Theorem will assert that every ideal $I \subseteq k[x_1, \ldots, x_n]$ has a finite generating set. That is, $I = \langle f_1, \ldots, f_s \rangle$ for some $f_i \in k[x_1, \ldots, x_n]$.

The Ideal Membership Problem: Given $f \in k[x_1, \ldots, x_n]$ and an ideal $I = \langle f_1, \ldots, f_s \rangle$, determine if $f \in I$. Geometrically this is closely related to the problem of determining whether f vanishes on $\mathbf{V}(f_1, \ldots, f_s)$. The **Hilbert Nullstellensatz** will assert that if f vanishes on $\mathbf{V}(f_1, \ldots, f_s)$, then for some integer power m, $f^m \in \langle f_1, \ldots, f_s \rangle$.

The Problem of solving Polynomial Equations: Find all common solutions in k^n of a system of polynomial equations

$$f_1(x_1, \ldots, x_n) = \cdots = f_s(x_1, \ldots, x_n) = 0. \tag{1.0.1}$$

Of course this is the same as asking for the points of the affine variety $\mathbf{V}(f_1, \ldots, f_s)$.

The Implicitization Problem: Let V be a subset of k^n given parametrically as

$$\begin{aligned} x_1 &= g_1(t_1, \ldots, t_m), \\ &\vdots \\ x_n &= g_n(t_1, \ldots, t_m). \end{aligned} \tag{1.0.2}$$

If the g_i are polynomials (or rational functions) in the variables t_j, V will be (part of) an affine variety. The problem is to find a system of polynomial equations in the x_i that define this variety.

The problem of solving polynomial equations and the implicitization problem are closely related. To illustrate this we give their solutions when the polynomials $f_1, \ldots, f_s$ and $g_1, \ldots, g_n$ are affine functions, i.e. polynomials of degree 1.

Suppose

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= a_{11}x_1 + \cdots + a_{1n}x_n + b_1, \\ &\vdots \\ f_s(x_1, \ldots, x_n) &= a_{s1}x_1 + \cdots + a_{sn}x_n + b_s. \end{aligned} \tag{1.0.3}$$

The system (1.0.1) can then be written in matrix form as

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & \cdots & \vdots & \vdots \\ a_{s1} & \cdots & a_{sn} & b_s \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{1.0.4}$$

which we abbreviate as $\begin{pmatrix} A & b \end{pmatrix} \begin{pmatrix} x \\ 1 \end{pmatrix} = 0$. After row reduction this system has the form $\begin{pmatrix} \mathbf{1} - C & b' \end{pmatrix} \begin{pmatrix} x \\ 1 \end{pmatrix} = 0$ where every column of C which is not identically zero has a 1 in the diagonal position. If the non zero columns of C are $C_{i_1}, \ldots, C_{i_r}$, the row reduced form of (1.0.4) can be expressed as

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = x_{i_1}C_{i_1} + \cdots + x_{i_r}C_{i_r} - b'. \tag{1.0.5}$$

The variables $x_{i_1}, \ldots, x_{i_r}$ are "free variables". They can be assigned any values and (1.0.5) then determines the values of the remaining variables. Setting $x_{i_j} = t_j$, $1 \le j \le r$, gives the solution set of (1.0.1) as

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = t_1C_{i_1} + \cdots + t_rC_{i_r} - b', \qquad t_i \in \mathbf{R}, 1 \le i \le r. \tag{1.0.6}$$

This describes the solution to (1.0.1) in parametrized form (for the choice of f_i in (1.0.3)).

Taking up the implicitization problem, suppose

$$x = Bt + b, \tag{1.0.7}$$

where

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, B = \begin{pmatrix} b_{11} & \cdots & b_{1s} \\ \vdots & \dots & \vdots \\ b_{n1} & \cdots & b_{ns} \end{pmatrix}, t = \begin{pmatrix} t_1 \\ \vdots \\ t_s \end{pmatrix}, \text{ and } b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}. \tag{1.0.8}$$

(1.0.7) states that "x is in a translate of the column space of B". We can get the same x-space without loss of generality by assuming that B **has (column) rank** s, which implies, in particular, that $s \le n$. Accepting this assumption, write (1.0.7) in block form as

$$\begin{pmatrix} B & -\mathbf{1}_n & b \end{pmatrix} \begin{pmatrix} t \\ x \\ 1 \end{pmatrix} = 0_n. \tag{1.0.9}$$

(Here 0_n is a column vector of length n all of whose entries are zeros and $\mathbf{1}_n$ is the $n \times n$ identity matrix.) Since B has rank s there is an $n \times n$-matrix A such that

$$AB = \begin{pmatrix} \mathbf{1}_s \\ 0_{n-s,s} \end{pmatrix}. \tag{1.0.10}$$

(Here $0_{n-s,s}$ is an $(n-s) \times s$ matrix with zero entries.) Multiplying (1.0.9) on the left by A puts it in the rowreduced form

$$\begin{pmatrix} AB & -A & Ab \end{pmatrix} \begin{pmatrix} t \\ x \\ 1 \end{pmatrix} = 0_n. \tag{1.0.11}$$

Let $A = \begin{pmatrix} A_s \\ A_{[n-s]} \end{pmatrix}$, where A_s denotes the first s rows of the matrix A. (1.0.11) can be restated as

$$t - A_s x + A_s b = 0_s; \tag{1.0.11.i}$$

$$-A_{[n-s]} x + A_{[n-s]} b = 0_{n-s}. \tag{1.0.11.ii}$$

Contention 1.0.12. The $x \in k^n$ which satisfy (1.0.11.ii) are precisely those which have the form (1.0.7) for some $t \in k^s$.

Proof. The preceding discussion shows that (1.0.7) and (1.0.11) are equivalent; so any x satisfying (1.0.7) for some t also satisfies (1.0.11.ii). Now given an x which satisfies (1.0.11.ii), define t by (1.0.11.i). The equivalence of (1.0.11) and (1.0.7) then shows that the pair x, t satisfies (1.0.7). ∎

This solves the impliticitization problem when $g_1, \dots, g_n$ are polynomials of degree one in $t_1, \dots, t_s$.

$\boxed{\S\mathbf{1.}}$

Determine whether $f(x)$ is in the ideal $I \subset \mathbf{R}[x]$.

(a) $f(x) = x^2 - 3x + 2$, $I = \langle x - 2 \rangle$.

Solution. $f(2) = 0$; so $x - 2$ divides $f(x)$ and $f \in I$.

(b) $f(x) = x^5 - 4x + 1$, $I = \langle x^3 - x^2 + x \rangle$.

Solution. Every element in $I = \mathbf{R}[x] \cdot (x^3 - x^2 + x)$ is divisible by x. Since $f(x)$ is not divisible by x, $f(x) \notin I$.

(c) $f(x) = x^2 - 4x + 4$, $I = \langle x^4 - 6x^2 + 12x - 8, 2x^3 - 10x^2 + 16x - 8\rangle$.

Solution. The greatest common divisor of the two polynomials generating I is 1; so $I = \mathbf{R}[x]$ and $f(x) \in I$.

(d) $f(x) = x^3 - 1$, $I = \langle x^9 - 1, x^5 + x^3 - x^2 - 1\rangle$.

Solution. The greatest common divisor of the two polynomials generating I is $x^3 - 1$; so $f(x) \in \mathbf{R}[x]$.

$\boxed{\S\mathbf{2.}}$

Find a parametrization of the affine variety defined by each of the following sets of equations:

(a) In $\mathbf{R}^3$ or $\mathbf{C}^3$:

$$\begin{aligned} 2x + 3y - z &= 9, \\ x - y &= 1, \\ 3x + 7y - 2z &= 17. \end{aligned}$$

Solution. In matrix form this system can be written:

$$\begin{pmatrix} 2 & 3 & -1 & -9 \\ 1 & -1 & 0 & -1 \\ 3 & 7 & -2 & -17 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}. \tag{1.2.a.1}$$

The matrix in (1.2.a.1) has row reduced echelon form

$$\begin{pmatrix} 1 & 0 & -\frac{1}{5} & -\frac{12}{5} \\ 0 & 1 & -\frac{1}{5} & -\frac{7}{5} \\ 0 & 0 & 0 & 0 \end{pmatrix}; \tag{1.2.a.2}$$

so the system has the parametrized form

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \frac{1}{5} \\ \frac{1}{5} \\ 1 \end{pmatrix} t_1 + \begin{pmatrix} \frac{12}{5} \\ \frac{7}{5} \\ 0 \end{pmatrix}. \tag{1.2.a.3}$$

(b) In $\mathbf{R}^4$ or $\mathbf{C}^4$:

$$\begin{aligned} x_1 + x_2 - x_3 - x_4 &= 0, \\ x_1 - x_2 + x_3 &= 0. \end{aligned}$$

Solution. In matrix form this system can be written:

$$\begin{pmatrix} 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}. \tag{1.2.b.1}$$

The matrix in (1.2.b.1) has row reduced echelon form

$$\begin{pmatrix} 1 & 0 & 0 & -\frac{1}{2} \\ 0 & 1 & -1 & -\frac{1}{2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}; \tag{1.2.b.2}$$

so the system has the parametrized form

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} t_1 + \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ 0 \\ 1 \end{pmatrix} t_2. \tag{1.2.b.3}$$

(c) In $\mathbf{R}^3$ or $\mathbf{C}^3$:

$$\begin{aligned} y - x^3 &= 0, \\ z - x^5 &= 0. \end{aligned} \tag{1.2.c.1}$$

This is not a linear system, but the parametrized form of the solution set is easy to find. It is:

$$\begin{aligned} x &= t_1, \\ y &= t_1^3, \\ z &= t_1^5. \end{aligned} \tag{1.2.c.2}$$

$\boxed{\S\mathbf{3.}}$

Find implicit equations for the affine varieties parametrized as follows:

(a) In $\mathbf{R}^3$ or $\mathbf{C}^3$:

$$\begin{aligned} x_1 &= t - 5, \\ x_2 &= 2t + 1, \\ x_3 &= -t + 6. \end{aligned}$$

Solution. Write this in matrix form as

$$\begin{pmatrix} 1 & -1 & 0 & 0 & -5 \\ 2 & 0 & -1 & 0 & 1 \\ -1 & 0 & 0 & -1 & 6 \end{pmatrix} \begin{pmatrix} t \\ x_1 \\ x_2 \\ x_3 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

The row reduced echelon form for the preceding coefficient matrix is

$$\begin{pmatrix} 1 & 0 & 0 & 1 & -6 \\ 0 & 1 & 0 & 1 & -1 \\ 0 & 0 & 1 & 2 & -13 \end{pmatrix}$$

Since there is one parameter ($s = 1$) we take the equations corresponding to the last two rows of the preceding matrix and these give the implicit form for the variety parametrized in the statement of the exercise. That is, in implicit form this variety is described by

$$\begin{aligned} x_1 + x_3 - 1 &= 0, \\ x_2 + 2x_3 - 13 &= 0. \end{aligned}$$

(b) In $\mathbf{R}^5$ or $\mathbf{C}^5$:

$$\begin{aligned} x_1 &= 2t - 5u, \\ x_2 &= t + 2u, \\ x_4 &= -t + u, \\ x_5 &= t + 3u. \end{aligned} \tag{1.3.b.1}$$

x_4 here is x_3 in the text
and x_5 here is x_4 in the text.
The x_3 here is a new variable.

Solution. Here the matrix form of (1.3.b.1) is

$$\begin{pmatrix} 2 & -5 & -1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & -1 & 0 \\ 1 & 3 & 0 & 0 & 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} t \\ u \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

The row reduced echelon form for this 5×7 matrix is

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \frac{3}{4} & -\frac{1}{4} \\ 0 & 1 & 0 & 0 & 0 & -\frac{1}{4} & -\frac{1}{4} \\ 0 & 0 & 1 & 0 & 0 & \frac{11}{4} & \frac{3}{4} \\ 0 & 0 & 0 & 1 & 0 & \frac{1}{4} & -\frac{3}{4} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

There are two parameters ($s = 2$); so deleting the two equations which correspond to the variables t, u we get the implicit description of this parametrized set as

$$x_1 + \frac{11}{4}x_4 + \frac{3}{4}x_5 = 0,$$
$$x_2 + \frac{1}{4}x_4 - \frac{3}{4}x_5 = 0.$$

(c) In $\mathbf{R}^3$ or $\mathbf{C}^3$:

$$x = t.$$
$$y = t^4,$$
$$z = t^7.$$

Solution. Here implicit equations are $y = x^4$, $z = x^7$.

$\boxed{\S\mathbf{4.}}$

Let $x_1, x_2, x_3, \dots$ be a 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 combinition of (finite) monomials $x_{i_1}^{e_1} \cdots x_{i_n}^{e_n}$. Let R denote the set of all polynomials in the x_i. Note that R is a ring $k[x_1, x_2, \dots]$, the polynomial ring in the countably infinite set of variables $x_1, x_2, x_3, \dots$.

(a) Let $I = \langle x_1, x_2, \dots \rangle$ be the set of polynomials of the form $x_{i_1}f_1 + \cdots x_{i_m}f_m$, where $f_i \in R$. Show that R is an ideal in the ring R. **Note.** I could be described as the set of polynomials R whose constant term is zero.

Solution. This is really obvious and no argument will be given here.

(b) Show, arguing by contradiction, that I has no finite generating set. Hint: It is not enough to consider subsets of $\{x_i : i \geq 1\}$.

Solution. Suppose $I = \langle g_1, \dots, g_r \rangle$. Note that for each j, $g_j \in I$; so the constant term of g_j is zero, and if we substitute zero for each of the variables which occurs in g_j, g_j is replaced by zero. Now let x_t be a variable which doesn't occur in any of the g_j's. The single term polynomial x_t is in I; so there must exist polynomials $h_1, \dots, h_r$ in R such that

(1.4.1) $$x_t = g_1h_1 + \cdots + g_rh_r.$$

Now in (1.4.1) replace each of the variables x_m which occur in some g_j by zero and replace x_t by 1. This type of substitution preserves identities in a polynomial ring. Here it leads to the contradiction $1 = 0$ and shows that it is impossible that $I = \langle g_1, \dots, g_r \rangle$ for some (finite) set of polynomials $g_j \in I$.

$\boxed{\S\mathbf{5.}}$

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

(a) Show that the number of distinct monomials $x^e y^f$ of total degree $\leq m$ in $k[x, y]$ is equal to $\frac{(m+1)(m+2)}{2} = \binom{m+2}{2}$.

Solution. This is the same as the number of monomials $x^e y^f 1^{m-e-f}$ or of the number of ways to place m indistinguishable balls (the exponents) into three boxes, the x-box, the y-box and the 1-box. Each such arrangement can be obtained by lining up the the balls and two vertical dividers in a row. The balls before the first divider go in the x-box and those between the two dividers in the y-box and the balls to the right of both dividers in the 1-box. There are $\binom{m+2}{2} = \binom{m+2}{m}$ such arrangements depending on whether one thinks of choosing the two slots for the dividers or the m slots for the balls.

(b) 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 $a + b \leq m$ form a linearly *dependent* set in $k[t]$.

Solution. From part (a) there are $\binom{m+2}{2}$ such terms each of which, when it is expanded in t, is a polynomial of degree $an + bn \leq mn$ in t. Now the vector space of polynomials of degree $\leq mn$ has dimension $mn + 1$; so the "monomials" $[f(t)]^a [g(t)]^b$ will be dependent if their number is larger than the dimension $mn + 1$, i.e. if

$$\begin{aligned} \binom{m+2}{2} &> mn + 1 \qquad \text{or} \\ (m+2)(m+1) &> 2mn + 2 \qquad \text{or} \\ m^2 + 3m + 2 &> 2mn + 2 \qquad \text{or} \\ (m+2)(m+1) &> 2mn + 2. \end{aligned}$$

Now if $m > 2n$ we have

$$(m+2)(m+1) > (2n+2)(m+1) = 2mn + 2m + 2n + 2 > 2mn + 2$$

which guarantees that the "monomials" $[f(t)]^a [g(t)]^b$ will be dependent in $k[t]$.

(c) Deduce from part (b) that if $C\colon x = f(t)$, $y = g(t)$ is any polynomial parametric curve in k^2, then C is contained in $\mathbf{V}(F)$ for some $F \in k[x, y]$.

Solution. According to (b) there is a polynomial $F(X, Y) \in k[X, Y]$ such that $F(f(t), g(t)) = 0$ in $k[t]$. This states that for each t the point $(f(t), g(t)) \in \mathbf{V}(F)$ which is what we were to show.

(d) Generalize parts (a), (b) and (c) of this problem to show that any polynomial surface

$$x = f(t, u), \qquad y = g(t, u) \qquad z = h(t, u)$$

is contained in an algebraic surface $\mathbf{V}(F)$, where $F \in k[x, y, z]$.

Solution. First, the dimension of the space of polynomials in the three variables x, y, z of total degree at most m is (m-balls, 3 vertical dividers in $m + 3$ spots).

$$\binom{m+3}{3} = \frac{(m+3)(m+2)(m+1)}{3!}.$$

Second, if $f(t,u), g(t,u), h(t,u)$ are polynomials of total degree at most n, then the "monomial" $[f(t,u)]^a [g(t,u)]^b [g(t,u)]^c$, $a+b+c \leq m$ is , when expanded in terms of t, u, a polynomial in two variables of total degree at most $an + bn + cn \leq mn$ in t, u. The space of such polynomials has dimension

$$\binom{mn+2}{2}$$

Thus the $\binom{m+3}{3} = \frac{(m+3)(m+2)(m+1)}{3!}$ monomials $[f(t,u)]^a [g(t,u)]^b [g(t,u)]^c$, $a+b+c \leq m$, will be linearly dependent as polynomials in t, u of total degree $\leq mn$ if their number is $>$ the dimension of the space of such polynomials, namely, if

$$\text{(1.5.d.1)} \qquad \binom{m+3}{3} = \frac{(m+3)(m+2)(m+1)}{3!} > \binom{mn+2}{2}.$$

This will be true for large m since the left side of (1.5.d.1) is a cubic in m with positive leading coefficient and the right side is a quadratic in m.

That is, for any $f(t,u), g(t,u), h(t,u)$, polynomials of total degree $\leq n$, there is a polynomial $F(X,Y,Z) \in k[X,Y,Z]$ such that $F(f(t,u), g(t,u), h(t,u)) = 0$. This means that the parametrized surface $x = f(t,u)$, $y = g(t,u)$, $z = h(t,u)$ lies on the algebraic surface $\mathbf{V}(F)$.