Chapter 2 §5. The Hilbert Basis Theorem and Gröbner Bases. If $I \subset k[x_1, \ldots, x_n]$ is an ideal other than $\{0\}$. Suppose $>$ is a monomial order on the exponents $\mathbf{Z}^n_{\geq 0}$ and let

$$\mathrm{LT}(I) = \{cx^\alpha\colon \text{ there is an } f \in I \text{ whose leading term is } cx^\alpha\}.$$

We will be especially interested in the monomial ideal $\langle \mathrm{LT}(I)\rangle$.

Note that if $\langle f_1, \ldots, f_s\rangle = I$ it may well be that $\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)\rangle \overset{\subset}{\neq} I$. For example, if $f_1 = x^3 - 2xy$ and $f_2 = x^2y - 2y^2 + x$, then

$$x \cdot f_2 - y \cdot f_1 = x \cdot (x^2y - 2y^2 + x) - y \cdot (x^3 - 2xy) = x^2;$$

so $x^2 \in \langle f_1, f_2\rangle$, but x^2 is not divisible by either x^3 or x^2y. This means that $x^2 \notin \langle x^2y, x^3\rangle$ which is $\langle \mathrm{LT}(f_1), \mathrm{LT}(f_2)\rangle$.

Proposiiton 2.5.0.1. Let $I \subset k[x_1, \ldots, x_n]$ be an ideal.

(i) $\langle \mathrm{LT}(I)\rangle$ is a monomial ideal.
(ii) There are $g_1, \ldots, g_s \in I$ such that $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\rangle$.

Proof. (i) follows because the generating set $\mathrm{LT}(I)$ consists entirely of nonzero multiples of monomials. To establish (ii): Dickson's Lemma then guarantees that, as a monomial ideal, $\langle \mathrm{LT}(I)\rangle$ is generated by a finite subset $\{\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\}$ with $\{g_1, \ldots, g_s\} \subset I$. ∎

These preparations lead to the

Theorem 2.5.0.2. (Hilbert Basis Theorem). Every ideal $I \subset k[x_1, \ldots, x_n]$ has a finite generating set. That is, $I = \langle g_1, \ldots, g_s\rangle$ for some $g_1, \ldots, g_s \in I$.

Proof. If $I = \{0\}$ take the generating set to be $\{0\}$. If $I \neq \{0\}$ let $g_1, \ldots, g_s \in I$ be such that $\mathrm{LT}(I) = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\rangle$. I claim that $I = \langle g_1, \ldots, g_s\rangle$. To prove this, suppose $f \in I$. Divide f by $(g_1, \ldots, g_s)$ getting an expression of the form

$$f = a_1g_1 + \cdots + a_sg_s + r, \text{ where either } r = 0 \text{ or } r \text{ is not divisible by } \mathrm{LT}(g_i) \text{ for any } i,\ 1 \leq i \leq s.$$

But $r = f - (a_1g_1 + \cdots + a_sg_s) \in I$; so $\mathrm{LT}(r)$ is a multiple of a monomial which is in the monomial ideal $\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\rangle$; so it must be divisible by one of the monomials $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)$. The only possibility is that $r = 0$ and then $f \in I$. ∎

Note. To determine if $f \in I$, all we need to do is calculate the remainder after dividing f by $(g_1, \ldots, g_s)$. $f \in I$ if and only if this remainder is zero. Furthermore, all that was required of the set $\{g_1, \ldots, g_s\}$ was that

$$\{cx^\alpha\colon \text{ there exists } f \in I \text{ with } \mathrm{LT}(f) = cx^\alpha\} \subset \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\rangle. \tag{2.5.0.3}$$

Definition 2.5.0.4. Fix a monomial order. A finite subset $\{g_1, \ldots, g_s\} \subset I$ satisfying (2.5.0.3) is called a *Gröbner basis* or *standard basis* for I.

Equivalently, a set $\{g_1, \ldots, g_s\} \subset I$ is a Gröbner basis or standard basis for I if and only if the leading term of any element $f \in I$ is divisible by the leading term of g_j for some $j \in [1..s]$.

Corollary 2.5.0.5. Every ideal $I \subset k[x_1, \ldots, x_n]$ other than $\{0\}$ has a Gröbner basis. Furthermore, a Gröbner basis for I is a basis for I.

Proof. Using Dickson's Lemma, the ideal $\langle \mathrm{LT}(I)\rangle$ has a finite generating set $\{\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\}$ and then as in the proof of the Hilbert Basis Theorem $\{g_1, \ldots, g_s\}$ is a Gröbner basis for I. This shows that every ideal has a Gröbner basis. To show that a Gröbner basis is a basis, suppose that $f \in I$ and divide f by the ordered Gröbner basis $(g_1, \ldots, g_s)$. The result is an expression of the form

$$f = q_1g_1 + \cdots + q_sg_s + r, \tag{\#}$$

where the leading term of r is not divisible by any of the $\mathrm{LT}(g_i)$'s. The expression (#) shows that $r \in I$ which means that

$$(\#\#) \qquad \mathrm{LT}(r) \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle.$$

This last mentioned ideal is a monomial ideal; so the only way (##) could occur is for $\mathrm{LT}(r)$ to be divisible by one of the $\mathrm{LT}(g_i)$'s. The only possiblity consistent with the output of the division algorithm is that $r = 0$. But then (#) shows that every element of I is in the ideal $\langle g_1, \ldots, g_s \rangle$; so $\{g_1, \ldots, g_s\}$ is indeed a basis for I. ∎

An Example. Let $f_1 = x^3 - 2xy$, $f_2 = x^2y - 2y^2 + x$. We showed in a note above that $x^2 \in \langle f_1, f_2 \rangle$; so $\{f_1, f_2\}$ is not a Gröbner basis in the grlex order for $\langle f_1, f_2 \rangle$.

Another Example. Let $J = \langle g_1, g_2 \rangle = \langle x + z, y - z \rangle$. We claim that g_1 and g_2 form a Gröbner basis for J using lex order in $\mathbf{R}[x, y, z]$. To establish this we must show that the leading term of any polynomial in J is divisible by x or y. That is,except for $h = 0$ there are no polynomials f, g, h satisfying $f(x, y, z)(x + z) + g(x, y, z)(y - z) = h(z)$. Note first that any such h vanishes on the linear variety $L = \mathbf{V}(x + z, y - z)$. Now $(-t, t, t) \in L$ for any real number t. This gives $h(t) = 0$ all t or h is necessarily the zero polynomial as asserted. Thus $\{g_1, g_2\}$ is a Gröbner basis for J.

Theorem 2.5.0.6. (The Ascending Chain Condition). Let

$$I_1 \subset I_2 \subset I_3 \subset \cdots .$$

be an ascending chain of ideals in $k[x_1, \ldots, x_n]$. Then there is an $N \geq 1$ such that

$$I_N = I_{N+1} = I_{N+2} = \cdots .$$

Proof. Suppose $I = \bigcup_{i=1}^{\infty} I_i$. I is clearly an ideal in $k[x_1, \ldots, x_n]$. Let $\{g_1, \ldots, g_s\}$ be a finite basis for I and let N be the smallest integer for which $\{g_1, \ldots, g_s\} \subset I_N$. Then $I_K = I$ for all $K \geq N$. ∎

Definition 2.5.0.7. Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. Denote by $\mathbf{V}(I)$ the set

$$(2.5.0.8) \qquad \mathbf{V}(I) = \{(a_1, \ldots, a_n) \colon f(a_1, \ldots, a_n) = 0 \text{ for all } f \in I\}$$

Proposition 2.5.0.9. If $I \in k[x_1, \ldots, x_n]$ is an ideal, there is a finite set $\{f_1, \ldots, f_s\} \subset I$ such that

$$\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_s).$$

That is, $\mathbf{V}(I)$ is an affine variety.

Proof. By the Hilbert basis theorem there is a finite set $\{f_1, \ldots, f_s\} \subset I$ such that $I = \langle f_1, \ldots, f_s \rangle$. In particular, for each $f \in I$ there are polynomials $q, \ldots, q_s$ in $k[x_1, \ldots, x_n]$ such that $f = q_1 f_1 + \cdots + q_s f_s$. A direct consequence of this is that $\mathbf{V}(f_1, \ldots, f_s) \subset \mathbf{V}(f)$. Since this is true for every $f \in I$, it follows that $\mathbf{V}(f_1, \ldots, f_s) \subset \mathbf{V}(I)$. The other inclusion, $\mathbf{V}(I) \subset \mathbf{V}(f_1, \ldots, f_s)$ is a restatement of

$$\mathbf{V}(I) = \bigcap_{f \in I} \mathbf{V}(f) \subset \bigcap_{f \in \{f_1, \ldots, f_s\}} \mathbf{V}(f) = \mathbf{V}(f_1, \ldots, f_s).$$

∎

Terminology. In what follows we will use the term "monomial" interchangably with " nonzero multiple of a monomial".

---

§2.5.1.

Let $I = \langle g_1, g_2, g_3 \rangle \subset \mathbf{R}[x, y, z]$, where $g_1 = xy^2 - xz + y$, $g_2 = xy - z^2$ and $g_3 = x - xz^4$. Using the lex order, give an example of $g \in I$ such that $\mathrm{LT}(g) \notin \langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \mathrm{LT}(g_3) \rangle$.

Solution. $\langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \mathrm{LT}(g_3)\rangle = \langle xy^2, xy, -xz^4\rangle$. Let

$$g = -z^3 \cdot g_1 - yz^3 \cdot g_2 + g_3 = -z^3 \cdot (xy^2 - xz + y) - yz^3 \cdot (xy - z^2) + (x - xz^4) = x - yz^5 - yz^3$$

Then $\mathrm{LT}(g) = x \notin \langle xy^2, xy, -xz^4\rangle$ since x is not divisible by any of these three leading terms.

---

§2.5.3.

To generalize the situation of exercises 2.5.1 and 2.5.2 suppose $I = \langle f_1, \ldots, f_s\rangle$ is an ideal such that $\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)\rangle$ is strictly smaller than $\langle \mathrm{LT}(I)\rangle$.

(a) Prove that there is some $f \in I$ whose remainder on division by $(f_1 \ldots, f_s)$ is non zero.

Solution. Since $\langle \mathrm{LT}(I)\rangle$ is a monomial ideal, there must be some monomial in the generating set $\{\mathrm{LT}(g)\colon g \in I\}$ which is not divisible by any of the monomials in $\{\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)\}$, but then, dividing g by $(f_1 \ldots, f_s)$ yields the remainder $r = g$.

(b) What dies part (a) say about the ideal membership problem?

Solution. It says that one cannot use the vanishing of the remainder on division as a criterion for ideal membership.

(c) How does part (a) relate to the conjecture you were asked to make in Exercise 2.3.8?

Solution. I don't know what the authors are driving at here! How about: If

$$\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)\rangle \overset{\subset}{\neq} \langle \mathrm{LT}(I)\rangle$$

then one cannot safely use the vanishing of the remainder on division by $(f_1, \ldots, f_s)$ as a criterion for membership in I.

---

§2.5.4.

If $I \subset k[x_1, \ldots, x_n]$ is an ideal, prove that $\langle \mathrm{LT}(g)\colon g \in I - \{0\}\rangle = \langle \mathrm{LM}(g)\colon g \in I - \{0\}\rangle$.

Solution. This is really a restatement of the motive behind the terminology introduced before 2.5.1. It hardly requires any proof except to note that replacing the generators of an ideal by nonzero multiples of the same doesn't change the ideal.

---

§2.5.5.

Let I be an ideal of $k[x_1, \ldots, x_n]$. Show that $G = \{g_1, \ldots, g_s\} \subset I$ is a Gröbner basis of I if and only if the leading term of any element of I is divisible by one of the $\mathrm{LT}(g_i)$ for some i.

Solution. This is really just an observation. The definition of Gröbner basis is that $\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\rangle = \langle \mathrm{LT}(I)\rangle$. Since $J = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\rangle$ is a monomial ideal, a polynomial $h \in J$ if and only if every one of its terms is divisible by one of the $\mathrm{LT}(g_i)$'s. In particular, $J = \langle \mathrm{LT}(I)\rangle$ if and only if for each $h \in I$, $\mathrm{LT}(h)$ is divisible by one of the $\mathrm{LT}(g_i)$'s.

---

§2.5.6.

Corollary 2.5.0.5 says that every Gröbner basis is a basis. That is, if $\{g_1, \ldots, g_s\}$ satisfies

$$\{cx^\alpha\colon \text{ there exists } f \in I \text{ with } \mathrm{LT}(f) = cx^\alpha\} \subset \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\rangle, \tag{2.5.0.3}$$

then $I = \langle g_1, \ldots, g_s\rangle$. Here is a second proof.

Proof. If $f \in I$ divide f by $(g_1, \ldots, g_s)$. At each step of the division algorithm the leading term of the dividend (the polynomial under the radical) will be in $\langle \mathrm{LT}(I)\rangle$ because this dividend was obtained by adding a multiple hg_i to the preceding dividend (both of which are in $\langle \mathrm{LT}(I)\rangle$). Thus the dividend is divisible by one of the $\mathrm{LT}(g_i)$'s and no terms will ever be added to the remainder, so that when the algorithm terminates the expression obtained will have the form $f = q_1 g_1 + \cdots + q_s g_s$ showing that $f \in \langle g_1, \ldots, g_s\rangle$.

§**2.5.7.**

If we use grlex order with $x > y > z$, is $\{x^4y^2 - z^5,\ x^3y^3 - 1,\ x^2y^4 - 2z\}$ a Gröbner basis for the ideal I generated by these polynomials? Why or why not?

Solution. No! $y(x^4y^2 - z^5) - x(x^3y^3 - 1) = yz^5 + x \in I$, but yz^5 is not divisible by any of the leading terms x^4y^2, x^3y^3, x^2y^4.

---

§**2.5.8.**

Repeat Exercise 2.5.7 for $I = \langle x - z^2,\ y - z^3\rangle$ using lex order. Hint: the difficult part of this exercise is to determine exactly which polynomials are in $\langle \mathrm{LT}(I)\rangle$.

Solution. $\{x - z^2,\ y - z^3\}$ is a Gröber basis if and only if any relation of the form

$$f(x,y,z)(x - z^2) + g(x,y,z)(y - z^3) = h(z), \qquad f, g \in \mathbf{R}[x,y,z],\ h \in \mathbf{R}[z]$$

implies that $h = 0$. Now every point of the form (t^2, t^3, t), $t \in \mathbf{R}$ is a zero of the left side of this relation. This means that $h(t) = 0$ for every $t \in \mathbf{R}$ and this in turn implies that $h = 0$; so the answer is: yes! $\{x - z^2,\ y - z^3\}$ is a Gröber basis for I.

---

§**2.5.9.**

Let $A = (a_{ij})$ be an $m \times n$ matrix with real entries in row echelon form (which itself implies that $m \leq n$) and let $J \subset \mathbf{R}[x_1, \ldots, x_n]$ be an ideal generated by the linear polynomials $\sum_{j=1}^n a_{ij}x_j$ for $1 \leq i \leq m$. Show that the given generators form a Gröbner basis for J with respect to a suitable sexicographic order. Hint: Order the variables corresponding to the leading 1's before the other variables.

Solution. By renaming the variables $x_1, \ldots, x_n$ following the hint we can assume that the forms $\sum_{j=1}^n a_{ij}x_j$ are $x_1 - h_1$, $x_2 - h_2$, $\ldots, x_m - h_m$ where the h_i's are linear forms in the variables $x_{m+1}, \ldots, x_n$. (We have assumed here that the matrix A doesn't have any totally zero terminal rows. If it does we change m to match the no totally zero rows condition.) Use lex order. $\{x_1 - h_1,\ x_2 - h_2,\ \ldots, x_m - h_m\}$ is a Gröbner basis if and only if every polynomial in the ideal $\langle x_1 - h_1,\ x_2 - h_2,\ \ldots, x_m - h_m\rangle$ has a leading term which is divisible by one of the polynomials $x_1, \ldots, x_m$. That is, if a relation of the form

$$\begin{aligned} f_1(x_1 - h_1) + \cdots + f_m(x_m - h_m) &= g(x_{m+1}, \ldots, x_n), \\ f_1, \ldots, f_m \in \mathbf{R}[x_1, \ldots, x_n],\ &g \in \mathbf{R}[x_{m+1}, \ldots, x_n] \end{aligned} \tag{1}$$

implies that $g = 0$. By now the argument is standard: Every point of the form

$$(h_1(t_{m+1}, \ldots, t_n), \ldots, h_m(t_{m+1}, \ldots, t_n), t_{m+1}, \ldots, t_n) \text{ with } (t_{m+1}, \ldots, t_n) \in \mathbf{R}^{n-m}$$

is a zero of the lefthand side of (1) and hence of the righthand side too. But then we have $g = 0$.

---

§**2.5.10.**

Let $I \subset k[x_1, \ldots, x_n]$ be a *principal ideal* (that is, I is generated by a single $f \in I$). Show that any finite subset of I containing a generator for I is a Gröbner basis for I.

Solution. Suppose $I = \langle f\rangle$. Let the leading term of f be cx^α. The generators of I are the polynomials $\lambda \cdot f$. Their leading terms are the polynomials ax^α, $a \neq 0$. The leading terms of the elements of I are monomial multiples of x^α; so

$$\langle \mathrm{LT}(I)\rangle = \langle cx^\alpha \cdot x^\beta \colon \beta \in \mathbf{Z}^n_{\geq 0},\ c \in \mathbf{R}\rangle = \langle x^\alpha\rangle = \langle \mathrm{LT}(f)\rangle,$$

which shows that $\{f\}$ is a Gröbner basis for I.

---

§**2.5.11.**

Let $f \in k[x_1, \ldots, x_n]$. If $f \notin \langle x_1, \ldots, x_n \rangle$, then show $\langle x_1, \ldots, x_n, f \rangle = k[x_1, \ldots, x_n]$.

Solution. The ideal $\langle x_1, \ldots, x_n \rangle$ is the ideal of $f \in k[x_1, \ldots, x_n]$ such that $f(0_n) = 0$, where $0_n = (0, \ldots, 0)$, n-components. That is, it is the ideal of polynomials whose constant term is zero. Since $f \notin \langle x_1, \ldots, x_n \rangle$ we know that this constant term $f(0_n) \neq 0$. But then $f(0_n) = f - (f - f(0_n)) \in \langle x_1, \ldots, x_n, f \rangle$, since $f - f(0_n) \in \langle x_1, \ldots, x_n \rangle$. Then, however, any $g \in k[x_1, \ldots, x_n]$ is in $\langle x_1, \ldots, x_n, f \rangle$ since
$g = g \cdot [f(0_n)]^{-1} \cdot f(0_n) \in k[x_1, \ldots, x_n] \cdot f(0_n) = \langle f(0_n) \rangle$.

---

§**2.5.12.**

Show that in any commutative ring: (every ideal I is finitely generated) $\Leftrightarrow$ (the ascending chain condition holds).

Proof. $\square(\Rightarrow)$: Let $I_1 \subset I_2 \subset I_3 \subset \cdots$ be an ascending chain of ideals. Let $I = \bigcup_{i \geq 1} I_i$ be the union of all the ideals in the chain. I is an ideal and hence must be finitely generated. Let $I = \langle a_1, \ldots, a_s \rangle$. Now choose N so large that $\{a_1, \ldots, a_s\} \subset I_N$. Clearly $I_N = I_{N+1} = \cdots$.

($\Leftarrow$): If an ideal I is not finitely generated let $A = \{a_1, a_2, \ldots\}$ be an infinite subset of I such that no finite subset of A generates I. Let $I_m = \langle a_1, \ldots, a_m \rangle$. I_m, $1 \leq m$ is an ascending chain of ideals which does not satisfy the ascending chain condition. The contradiction shows there is no such set A and it must be that I is finitely generated. $\blacksquare$

---

§**2.5.13.**

Let $V_1 \supset V_2 \supset V_3 \supset \cdots$ be a descending chain of affine varieties. Show that there is some $N \geq 1$ such that $V_N = V_{N+1} = V_{N+2} = \cdots$.

Solution. We start by showing that if $V = \mathbf{V}(f_1, \ldots, f_s)$ and $I(V) = \{g \in k[x_1, \ldots, x_n] \colon g(V) = 0\}$, then V is precisely the set of common zeros of the elements of the ideal $I(V)$. Since $\{f_1, \ldots, f_s\} \subset I(V)$, no point of $p \in k^n$ can belong to the common zeros of $I(V)$ unless the f_i's vanish at p. Thus the set of common zeros is not larger than V and it certainly can't be smaller. **Note.** If V were just some subset of k^n, this property would not be true.

Now let $I(V_j) = \{f \in k[x_1, \ldots, x_n] \colon f(V_j) = 0\}$. $I(V_j)$ is an ideal, and $I(V_1) \subset I(V_2) \subset \cdots$ is an ascending chain of ideals. By the ascending chain condition it stabilizes at say $I(V_N)$. But then V_{N+b} is the set of common zeros of the ideal $I(V_{n+b}) = I(V_N)$ for all $b \geq 0$; so the cdescending chain of affine varieties stabilizes at N also.

---

§**2.5.14.**

Let $f_1, f_2, \cdots \in k[x_1, \ldots, x_n]$ be an infinite collection of polynomials and let $I = \langle f_1, f_2, \ldots \rangle$ be the ideal they generate. Prove there is an integer N such that $I = \langle f_1, \ldots, f_N \rangle$.

Solution. Let $I_m = \langle f_1, \ldots, f_m \rangle$. $I_1 \subset I_2 \subset \cdots$ is an ascending chain of ideals. By the ascending chain condition there is an N such that $\langle f_1, \ldots, f_N \rangle = \langle f_1, \ldots, f_{N+b} \rangle$ for all $b \geq 0$. Thus $I = \langle f_1, f_2, \ldots \rangle = \bigcup_{m \geq 1} I_m = \langle f_1, \ldots, f_N \rangle$.

---

§**2.5.15.**

Given polynomials $f_1, f_2, \cdots \in k[x_1, \ldots, x_n]$. let $\mathbf{V}(f_1, f_2, \ldots) \subset k^n$ be the solutions of the infinite system of equations $f_1 = f_2 = \cdots = 0$/ Show there is some N such that $\mathbf{V}(f_1, f_2, \ldots) = \mathbf{V}(f_1, \ldots, f_N)$.

Solution. Let $V_m = \mathbf{V}(f_1, \ldots, f_m)$. Then $\mathbf{V}(f_1, f_2, \ldots) = \bigcap_{m \geq 1} V_m$. The affine varieties $V_1 \supset V_2 \supset V_3 \supset \cdots$ and so just as in Exercise 2.5.13 this descending chain of affine varieties stabilizes and if it stabilizes at N we have $\mathbf{V}(f_1, f_2, \ldots) = \mathbf{V}(f_1, \ldots, f_N)$.

---

§2.5.16.

If $V = \mathbf{V}(f_1, \ldots, f_s)$ is an affine variety, $I(V)$ is the set of $f \in k[x_1, \ldots, x_n]$ for which $f(V) = 0$. Now if J is an ideal in $k[x_1, \ldots, x_n]$, then $V(J)$ is the set of common zeros of the elements of J. You are to prove that $V(I(V)) = V$.

Solution. In fact, this was precisely what we showed at the beginning to the solution for Exercise 2.5.13.

---

§2.5.17.

Consider the variety $V = \mathbf{V}(x^2-y,\, y+x^2-4) \subset \mathbf{C}^2$. Note that $V = V(I)$, where $I = \langle x^2-y,\, y+x^2-4\rangle$.

(a) Prove that $I = \langle x^2 - y,\, x^2 - 2\rangle$.

Solution. Since $(x^2-y)+(y+x^2-4) = 2(x^2-2)$ it is clear that $\langle x^2-y,\, x^2-2\rangle \subset \langle x^2-y,\, y+x^2-4\rangle$. On the otherhand $y+x^2-4 = (-1)(x^2-y)+2(x^2-2)$; so it is clear that $\langle x^2-y,\, x^2-2\rangle \supset \langle x^2-y,\, y+x^2-4\rangle$.

(b) Using the basis from part (a), prove that $V(I) = \{(\pm\sqrt{2}, 2)\}$.

Solution. The common zeros of $x^2 - y$ and $x^2 - 2$ are precisely the points listed. First solve $x^2 - 2 = 0$ to get $x = \pm\sqrt{2}$ and then use the fist basis element to determine that $y = 2$.

---

§2.5.18.

When an ideal has a basis where some of the elements can be factored, we can use the factorization to help understand the variety.

(a) Show that if $g \in k[x_1, \ldots, x_n]$ factors as $g = g_1 g_2$, that for any f, $\mathbf{V}(f, g) = \mathbf{V}(f, g_1) \cup \mathbf{V}(f, g_2)$.

Solution. If $p \in k^n$ is such that $p \in (f, g)$, then $f(p) = g(p) = 0$. This happens if and only if $f(p) = 0$ and either $g_1(p) = 0$ or $g_2(p) = 0$. This is virtually the requested equality.

(b) Show that in $\mathbf{R}^3$. $\mathbf{V}(y - x^2,\, xz - y^2) = \mathbf{V}(y - x^2, xz - x^4)$.

Solution. First notice that

$$\begin{aligned}\mathbf{V}(y - x^2, xz - x^4) &= \mathbf{V}(y - x^2,\, x) \cup \mathbf{V}(y - x^2, z - x^3)\\ &= \{(0, 0, s)\colon s \in \mathbf{R}\} \cup \{(t, t^2, t^3)\colon t \in \mathbf{R}\}\\ &\subset \mathbf{V}(y - x^2,\, xz - y^2).\end{aligned}$$

To go the other way notice that

$$xz - x^4 = (xz - y^2) - (x^2 + y)(x^2 - y)$$

which shows that $\langle y - x^2, xz - x^4\rangle \subset \langle y - x^2,\, xz - y^2\rangle$. Using this last fact or directly it is easy to conclude that

$$\mathbf{V}(y - x^2,\, xz - y^2) \subset \mathbf{V}(y - x^2, xz - x^4).$$

(c) Use part (a) to describe and/or sketch the variety from part (b).

Solution. It follows from the first offset in (b) that $\mathbf{V}(y - x^2,\, xz - x^4)$ consists of the union of the z-axis and the "twisted cubic" $t \mapsto (t, t^2, t^3)$.