Chapter 3 Elimination Theory

§1. The Elimination and Extension Theorems

We start with a definition.

Definition 3.0.1. (Definition 1) Given $I = \langle f_1, \ldots, f_s \rangle \subset k[x_1, \ldots, x_n]$, the ℓ-th *elimination ideal* I_ℓ is the ideal of $k[x_{\ell+1}, \ldots, x_n]$ defined by

$$I_\ell = I \cap k[x_{\ell+1}, \ldots, x_n].$$

This ideal I_ℓ consists of all consequences of $f_1 = f_2 = \cdots = f_s = 0$ which eliminate the variables $x_1, \ldots, x_\ell$. In solving the system of polynomial equations $f_1 = f_2 = \cdots = f_s = 0$, a *solution of the Elimination Step* means giving a systematic procedure for finding elements of the ℓ-th elimination ideal I_ℓ. With proper term ordering Gröbner bases allow us to do this instantly.

Theorem 3.0.2.(Theorem 2) (The Elimination Theorem). Let $I \subset k[x_1, \ldots, x_n]$ be an ideal and let G be a Gröbner basis of I with respect to lex order with $x_1 > x_2 > \cdots > x_n$. Then for every $0 \leq \ell \leq n$, the set

$$G_\ell = G \cap k[x_{\ell+1}, \ldots, x_n]$$

is a Gröbner basis of the ℓ-th elimination ideal I_ℓ.

Proof. Fix ℓ between 0 and n. Note that $G \subset I$ implies that $G_\ell \subset I_\ell$. Thus to prove theorem 2 it suffices to show that

$$\langle \mathrm{LT}(I_\ell) \rangle = \langle \mathrm{LT}(G_\ell) \rangle,$$

because by definition a finite set $G_\ell \subset k[\mathbf{x}]$ is a Gröbner basis for the ideal I_ℓ if and only if (i) $G_\ell \subset I_\ell$ and (ii) $\mathrm{LT}(I_\ell) \subset \langle \mathrm{LT}(G_\ell) \rangle$. Now the inclusion $\supset$ follows from $I \supset G$; so it suffices to establish that $\langle \mathrm{LT}(I_\ell) \rangle \subset \langle \mathrm{LT}(G_\ell) \rangle$. To do this we we need only show that for an arbitrary $f \in I_\ell$ there is a $g \in G_\ell$ such that the leading term of f is divisible by $\mathrm{LT}(g)$. Suppose $f \in I_\ell$. Then, in particular, $f \in I$ and $\mathrm{LT}(f)$ is divisible by some $\mathrm{LT}(g)$, $g \in G$, because G is a Gröbner basis for I. Since $f \in I_\ell$, the leading term $\mathrm{LT}(f)$ involves only the variables $x_{\ell+1}, \ldots, x_n$. But then its divisor $\mathrm{LT}(g)$ involves only the variables $x_{\ell+1}, \ldots, x_n$ and because $x_1 > x_2 > \cdots > x_n$ this means that g involves only the variables $x_{\ell+1}, \ldots, x_n$. At the risk of being redundent, the reason for this is that since we are using lex order with $x_1 > \cdots > x_n$, any monomial involving $x_1, \ldots, x_\ell$ is greater than all the monomials in $k[x_{\ell+1}, \ldots, x_n]$, so that $\mathrm{LT}(g) \in k[x_{\ell+1}, \ldots, x_n]$ by itself implies that $g \in k[x_{\ell+1}, \ldots, x_n]$. This shows that $g \in G_\ell$ and finishes the proof. ∎

An Illustration. To solve

$$\begin{aligned} x^2 + y + z &= 1, \\ x + y^2 + z &= 1, \\ x + y + z^2 &= 1, \end{aligned}$$

First compute a Gröbner basis for the ideal $I = \langle x^2 + y + z - 1,\ x + y^2 + z - 1,\ x + y + z^2 - 1 \rangle$. Mathematica's Groebnerbasis[{x^2+y+z-1,x+y^2+z-1,x+y+z^2-1},{x,y,z}] yields

$$\{-z^2 + 4\,z^3 - 4\,z^4 + z^6, -z^2 + 2\,y\,z^2 + z^4, -y + y^2 + z - z^2, -1 + x + y + z^2\}.$$

From this we can read off G_2, G_1, G and putting the ideal generation delimiters around these we get

$$\begin{aligned} I_2 &= \langle -z^2 + 4\,z^3 - 4\,z^4 + z^6 \rangle, \\ I_1 &= \langle -z^2 + 4\,z^3 - 4\,z^4 + z^6, -z^2 + 2\,y\,z^2 + z^4, -y + y^2 + z - z^2 \rangle, \\ I &= \langle -z^2 + 4\,z^3 - 4\,z^4 + z^6, -z^2 + 2\,y\,z^2 + z^4, -y + y^2 + z - z^2, -1 + x + y + z^2 \rangle. \end{aligned}$$

To solve the system at the begining of the illustration we first solve I_2 finding the points $\mathbf{V}(I_2)$ and then try to extend these to find points in $\mathbf{V}(I_1)$ and so forth. Here we would just substitute the roots of $-z^2 + 4\,z^3 - 4\,z^4 + z^6$ into the basis for I_1 and then solve for y, but in general the possibilities are more complicated. This process is called the *Extension Step*.

Theorem 3.0.3. (Theorem 3) (The Extension Theorem). Let $I = \langle f_1, \dots, f_s\rangle \subset \mathbb{C}[x_1, \dots, x_n]$ and let I_1 be the first elimination ideal of I. For each $1 \le i \le s$ write f_i in the form

$$f_i = g_i(x_2, \dots, x_n)x_1^{N_i} + \text{ terms in } x_1 \text{ of degree } < N_i,$$

where $N_i \ge 0$ and $g_i \in \mathbb{C}[x_2, \dots, x_n]$ is nonzero. Suppose that we have a partial solution $(a_2, \dots, a_n) \in \mathbf{V}(I_1)$. If $(a_2, \dots, a_n) \notin \mathbf{V}(g_1, \dots, g_s)$, then there exists $a_1 \in \mathbb{C}$ such that $(a_1, a_2, \dots, a_n) \in \mathbf{V}(I)$.

The proof uses resultants and will be given later in §3.6.

There is a special case of the Extension Theorem which we record as a corollary.

Corollary 3.0.4. (Corollary 4). Let $I = \langle f_1, \dots, f_s\rangle \subset \mathbb{C}[x_1, \dots, x_n]$, and suppose that some f_i is of the form

$$f_i = cx_1^N + \text{ terms of lower degree in } x_1,$$

where $c \in \mathbb{C}$ is nonzero and $N > 0$. If I_1 is the first elimination ideal of I and $(a_2, \dots a_n) \in \mathbf{V}(I_1)$, then there is an $a_1 \in \mathbb{C}$ such that $(a_1, a_2, \dots, a_n) \in \mathbf{V}(I)$.

Proof. (Modulo the Extension Theorem) Using the notation established in the statement of the Extension Theorem, $g_i = c \ne 0$; so $\mathbf{V}(g_1, \dots, g_s) = \emptyset$ and there is no $(a_2, \dots, a_n) \in \mathbf{V}(g_1, \dots, g_s)$. The existence of an a_1 with the specified properties follows then directly from the Extension Theorem. ∎

Chapter 3 Exercises to §1

---

§3.1.1.

Let $I \subset k[x_1, \dots, x_n]$ be an ideal.

(a) Prove that $I_\ell = I \cap k[x_{\ell+1}, \dots, x_n]$ is an ideal of $k[x_{\ell+1}, \dots, x_n]$.

Solution. It is closed under addition and under multiplication by elements of $k[x_{\ell+1}, \dots, x_n]$.

(b) Prove that the ideal $I_{\ell+1} \subset k[x_{\ell+2}, \dots, x_n]$ is the first elimination ideal of $I_\ell \subset k[x_{\ell+1}, \dots, x_n]$.

Solution. The first elimination ideal of I_ℓ is

$$I_\ell \cap k[x_{\ell+2}, \dots, x_n] = I \cap k[x_{\ell+1}, \dots, x_n] \cap k[x_{\ell+2}, \dots, x_n] = I \cap k[x_{\ell+2}, \dots, x_n] = I_{\ell+1}.$$

Note. This observation allows us to use the Extension Theorem multiple times when eliminating more than one variable.

---

§3.1.2.

Consider the system of equations

$$x^2 + 2y^2 = 3,$$
$$x^2 + xy + y^2 = 3.$$

(a) If I is the idal generated by these equations, find bases of $I \cap k[x]$ and $I \cap k[y]$.

Solution. H={x^2+2y^2-3,x^2+x*y+y^2-3}
GroebnerBasis[H,{x,y}]
yields

$$\{-y + y^3, x\,y - y^2, -3 + x^2 + 2\,y^2\}.$$

So $I \cap k[y] = \langle -y + y^3\rangle$.

H={x^2+2y^2-3,x^2+x*y+y^2-3}
GroebnerBasis[H,{y,x}]
yields

$$\{3 - 4\,x^2 + x^4, -3\,x + x^3 + 2\,y\}.$$

So $I \cap k[x] = \langle 3 - 4\,x^2 + x^4\rangle$.

(b) Find all solutions of the equations.

Solution. Starting with $y^3 - y = y(y^2-1) = 0$ we find three cases:

Case $y=0$: Leads to $x = c \in k$ and $x = \pm\sqrt{3}$; so points are $(\pm\sqrt{3}, 0)$.

Case $y=1$: Leads to $x-1=0$ and $-1+x^2=0$; so leads to $x=1$ and the solution is $(1,1)$.

Case $y=-1$: Leads to $-x-1=0$, $-1+x^2=0$; so leads to $(-1,-1)$.

Starting with $x^4-4x^2+3=0$ we find $(x^2-1)(x^2-3)=0$ or $x \in \{1,-1,\sqrt{3},-\sqrt{3}\}$.

$x=1$ leads to $-2+2y=0$ or $y=1$ and we get the solution $(1,1)$.

$x=-1$ leads to $2+2y=0$ or $y=-1$ and we get the solution $(-1,-1)$.

$x=\sqrt{3}$ leads to $0+2y=0$ and we get the solution $(\sqrt{3},0)$.

$x=-\sqrt{3}$ leads to $0+2y=0$ and we get the solution $(-\sqrt{3},0)$.

(c) Which of the solutions are rational, i.e. lie in $\mathbb{Q}^2$?

Solution. $\{(1,1),\ (-1,-1)\}$ are the rational solutions.

(d) What is the smallest field such that all solutions lie in k^2?

Solution. The smallest field is $\mathbb{Q}(\sqrt{3})$.

$\boxed{\textbf{§3.1.3.}}$

Determine all solutions $(x,y) \in \mathbb{Q}^2$ of the system of equations

$$\begin{aligned} x^2+2y^2 &= 2, \\ x^2+xy+y^2 &= 2. \end{aligned}$$

Also determine all solutions in $\mathbb{C}^2$.

Solution. Proceding just as in Exercise 3.1.2 we find lex order with $x > y$ yields the Gröbner basis

$$\{-2\,y+3\,y^3, x\,y-y^2, -2+x^2+2\,y^2\},$$

whereas lex order with $y > x$ yields the Gröbner basis

$$\{4-8\,x^2+3\,x^4, -6\,x+3\,x^3+4\,y\}.$$

The equation $(-2+3y^2)y=0$ yields $(\pm\sqrt{2},0)$, $\left(\sqrt{\frac{2}{3}}, \sqrt{\frac{2}{3}}\right)$ and $\left(-\sqrt{\frac{2}{3}}, -\sqrt{\frac{2}{3}}\right)$.

The equation $3x^4-8x^2+4=(3x^2-2)(x^2-2)=0$ yields these same points. There are no points in $\mathbb{Q}^2$ and these 4 points are in $\mathbb{C}^2$.

$\boxed{\textbf{§3.1.4.}}$

Find bases for the elimination ideals I_1 and I_2 for the ideal I determined by the equations:

$$\begin{aligned} x^2+y^2+z^2 &= 4, \\ x^2+2y^2 &= 5, \\ xz &= 1. \end{aligned}$$

How many rational solutions are there?

Solution. Using lex order with $x > y > z$ yields the Gröbner basis

$$\{1 - 3\,z^2 + 2\,z^4, -1 + y^2 - z^2, x - 3\,z + 2\,z^3\}.$$

So we can read off from this that

$$\begin{aligned} I_2 &= \langle 1 - 3\,z^2 + 2\,z^4 \rangle, \\ I_1 &= \langle 1 - 3\,z^2 + 2\,z^4, -1 + y^2 - z^2 \rangle, \\ I &= \langle 1 - 3\,z^2 + 2\,z^4, -1 + y^2 - z^2, x - 3\,z + 2\,z^3 \rangle. \end{aligned}$$

Now $2z^4 - 3z^2 + 1 = (z^2 - 1)(2z^2 - 1)$; so $z \in \left\{1, -1, \frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\right\}$.
Using $z = \pm 1$ in $-1 + y^2 - z^2$ gives $y^2 - 2 = 0$ or $y = \pm\sqrt{2}$.
Using $z = \pm\frac{1}{\sqrt{2}}$ in $-1 + y^2 - z^2$ gives $y^2 - \frac{3}{2} = 0$ or $y = \pm\sqrt{\frac{3}{2}}$.
In none of these four cases is there a rational root; so to answer this part of the question we don't need to calculate x, although it is easy to do it using the Gröbner basis above.

$\boxed{\S\mathbf{3.1.5.}}$

In this exercise we will prove a more general version of the Elimination Theorem. Fix an integer $1 \le \ell \le n$. We say that a monomial order $>$ on $k[x_1, \ldots, x_n]$ is of *ℓ-elimination type* provided that any monomial involving one of $x_1, \ldots, x_\ell$ is greater than all monomials in $k[x_{\ell+1}, \ldots, x_n]$. Prove the following generalized Elimination Theorem. If I is an ideal in $k[x_1, \ldots, x_n]$ and G is a Gröbner basis of I with respect to a monomial order of ℓ-elimination type, then $G \cap k[x_{\ell+1}, \ldots, x_n]$ is a basis of the ℓ-th elimination ideal $I \cap k[x_{\ell+1}, \ldots, x_n]$.

Proof. Put $G_\ell = G \cap k[x_{\ell+1}, \ldots, x_n]$ and $I_\ell = I \cap k[x_{\ell+1}, \ldots, x_n]$. We want to show that G_ℓ is a Gröber basis for I_ℓ. This means two things: (1) $G_\ell \subset I_\ell$ and (2) $\mathrm{LT}(I_\ell) \subset \langle \mathrm{LT}(G_\ell) \rangle$.

Since $G \subset I$ we certainly have that $G_\ell \subset I_\ell$. To show that $\mathrm{LT}(I_\ell) \subset \langle \mathrm{LT}(G_\ell) \rangle$ we need only show that for an arbitrary $f \in I_\ell$ there is a $g \in G_\ell$ such that the leading term of f is divisible by $\mathrm{LT}(g)$. This is because the ideal $\langle \mathrm{LT}(G_\ell) \rangle$ consists of all those polynomials whose monomial terms are multiples of some such $\mathrm{LT}(g)$ with $g \in G_\ell$. Now suppose $f \in I_\ell$. Then $f \in I$ and $\mathrm{LT}(f)$ is divisible by some $\mathrm{LT}(g)$ with g in the Gröber basis G. Since $f \in k[x_{\ell+1}, \ldots, x_n]$ this means that $\mathrm{LT}(g)$ involves only the variables $x_{\ell+1}, \ldots, x_n$. But if the leading term of a polynomial g relative to a monomial ordering of ℓ-elimination type involves only the variables $x_{\ell+1}, \ldots, x_n$, then it follows that none of the other monomials in g can involve any of the variables $x_1, \ldots, x_\ell$, because if they did, they would be $>$ than $\mathrm{LT}(g)$ in this monomial ordering. It follows that $g \in G_\ell$ and we have completed the proof. ∎

$\boxed{\S\mathbf{3.1.6.}}$

To exploit the generalized Elimination Theorem of Exercise 3.1.5 we need some interesting examples of monomial orders of ℓ-elimination type. We will consider two such orders.

(a) Fix an integer $1 \le \ell \le n$, and define $>_\ell$ as follows: If $\alpha, \beta \in \mathbf{Z}^n_{\ge 0}$, then $\alpha >_\ell \beta$ if

$$\alpha_1 + \cdots + \alpha_\ell > \beta_1 + \cdots + \beta_\ell, \text{ or equality hold is the preceding and } \alpha >_{grevlex} \beta.$$

This is the ℓ-th elimination order of BAYER and STILLMAN (1987b). Prove that $>_\ell$ is a monomial order and is of ℓ-elimination type. Hint: If you did Exercise 2.4.12, then you have already done this problem.

Solution. We quote from the solution to Exercise 2.4.12.d. A useful example of a weight order is the *elimination order* introduced by Bayer and Stillman (1987b). Fix an integer $1 \le i \le n$ and let $u_j = [j \le i]$, that is, $\mathbf{u} = (1, \ldots, 1, 0, \ldots, 0)$ where there are i 1's and $n - i$ 0's. Then the *i-th elimination order* $>_i$ is the weight order $>_{\mathbf{u},grevlex}$. (In Exercise 2.4.12 we showed that any such "product" of monomial orders was itself a monomial order.) Prove that $>_i$ has the following property: If x^α is a monomial in which one of $x_1, \ldots, x_i$ appears, then $x^\alpha >_i x^\beta$ for any monomial involving only $x_{i+1}, \ldots, x_n$.

Here suppose x^α is a monomial in which one of $x_1, \ldots, x_i$ appears, and that x^β is a monomial involving only $x_{i+1}, \ldots, x_n$. Then $\alpha \cdot \mathbf{u}_i \geq 1$ whereas $\beta \cdot \mathbf{u}_i = 0$ Thus there is no tie in the first test of $>_i$ and $x^\alpha > x^\beta$.

(b) In Exercise 2.4.10 we considered an example of a product order that mixed lex and grlex orders on different sets of variables. Explain how to create a product order that induces grevlex on both $k[x_1, \ldots, x_\ell]$ and $k[x_{\ell+1}, \ldots, x_n]$ and show that this order is of ℓ-elimination type.

Solution. Write $x = (x_1, \ldots, x_\ell)$ and $y = (x_{\ell+1}, \ldots, x_n)$ and use the generalized exponential notation in the obvious manner. Then monomials in $x_1, \ldots, x_n$ have the form $x^\alpha y^\beta$. Define $>_\ell$ by $\alpha\beta >_\ell \gamma\delta$ iff $\alpha >_{grevlex} \gamma$ or $\alpha = \gamma$ and $\beta >_{grevlex} \delta$. If we let $\mathbf{w}_\ell = (0, \ldots, 0, 1, 0, \ldots, 0)$, with the 1 in the ℓ-th component, and put $\mathbf{u}_\ell = \sum_{i=1}^{\ell} \mathbf{w}_i$, $\mathbf{v}_\ell = \sum_{i=\ell+1}^{n} \mathbf{w}_i$ then

$$>_\ell \text{ is the same as } >_{\mathbf{u}_\ell, -\mathbf{w}_1, \ldots, -\mathbf{w}_\ell, \mathbf{v}_\ell, -\mathbf{w}_{\ell+1}, \ldots, -\mathbf{w}_n} .$$

in the notation of Exercise 2.4.13 which shows that it is a monomial order.

To show it is of ℓ-elimination type, suppose (in the x, y notation used above) we compare $x^\alpha y^\beta$, $alpha \in \mathbf{Z}^\ell_{>0}$, $\beta \in \mathbf{Z}^{n-\ell}_{\geq 0}$, with y^γ, $\gamma \in \mathbf{Z}^{n-\ell}_{\geq 0}$. Since at least one component of α is positive, the "$\mathbf{u}_\ell$-test" will not result in a tie and $x^\alpha y^\beta >_\ell y^\gamma$ whatever β and γ showing that this is indeed a monomial order of ℓ-elimeination type.

(c) If G is a Gröbner basis for $I \subset k[x_1, \ldots, x_n]$ for either of the monomial orders of parts (a) and (b), explain why $G \cap k[x_{\ell+1}, \ldots, x_n]$ is a Gröbner basis with respect to grevlex.

Solution. In Exercise 3.1.5 we showed that $G \cap k[x_{\ell+1}, \ldots, x_n]$ is a Gröbner basis with respect to $>_\ell$. Now the ordering of the monomials which occur in the polynomials $G \cap k[x_{\ell+1}, \ldots, x_n]$ is the grevlex order; so their leading terms are the leading terms computed by the grevlex order. This is what we were to show.

$\boxed{\S\mathbf{3.1.7.}}$

Consider the equations

$$\begin{aligned} t^2 + x^2 + y^2 + z^2 &= 0, \\ t^2 + 2x^2 - xy - z^2 &= 0, \\ t + y^3 - z^3 &= 0. \end{aligned}$$

We want to eliminate t. Let $I = \langle t^2 + x^2 + y^2 + z^2,\ t^2 + 2y^2 - xy - z^2,\ t + y^3 - z^3 \rangle$ be the corresponding ideal.

(a) Using lex order with $t > x > y > z$, compute a Gröbner basis for I, and then find a basis for $I \cap k[x, y, z]$. You should get four generators, one of which has total degree 12.

Solution. The requested Gröbner basis G consists of the first 4 polynomials of the Gröbner basis for I listed below (we have separated them somewhat in the presentation)

$$\begin{aligned} J = \{&5\,y^4 + 5\,y^8 + y^{12} + 13\,y^2\,z^2 + 6\,y^6\,z^2 - 10\,y^5\,z^3 \\ &\qquad - 4\,y^9\,z^3 + 9\,z^4 - 12\,y^3\,z^5 + 5\,y^2\,z^6 + 6\,y^6\,z^6 + 6\,z^8 - 4\,y^3\,z^9 + z^{12}, \\ &- 5\,y^3 - 5\,y^7 - y^{11} + 3\,x\,z^2 - 7\,y\,z^2 - 3\,y^5\,z^2 + 10\,y^4\,z^3 + 4\,y^8\,z^3 + 6\,y^2\,z^5 \\ &\qquad + x\,z^6 - 3\,y\,z^6 - 5\,y^5\,z^6 + 2\,y^2\,z^9, \\ &x\,y + 2\,y^2 + y^6 + 3\,z^2 - 2\,y^3\,z^3 + z^6, \\ &x^2 + y^2 + y^6 + z^2 - 2\,y^3\,z^3 + z^6, \\ \\ &t + y^3 - z^3\} \end{aligned}$$

(b) Use grevlex to compute a Gröbner basis for $I \cap k[x, y, z]$. You will get a simpler set of two generators.

Solution. Taking the first four polynomials in the basis G above we get (whether we use MonomialOrder->DegreeLexicographic, which should give grlex, or MonomialOrder->DegreeReverseLexicographic, which should give grevlex)

$$H = \{x^2 - x\,y - y^2 - 2\,z^2, x\,y + 2\,y^2 + y^6 + 3\,z^2 - 2\,y^3\,z^3 + z^6\}$$

when we apply the GroebnerBasis command with $\{x, y, z\}$ for the order of the variables.

Remark 3.1.7.b What this seems to imply, since $\mathrm{LT}(I_1) \subset \langle \mathrm{LT}(H)\rangle$, is that in the grevlex monomial ordering, the leading term of every polynomial in the ideal I_1 is divisible be either x^2 or xy because these last two monomials are the grevlev leading monomials of the Gröbner basis H.

(c) Combine the answer to part (b) with the polynomial $t + y^3 - z^3$ and show that this gives a Gröbner basis for I with respect to the elimination order $>_1$ of Exercise 3.1.6. Notice that this Gröbner basis is much simpler than the one found in part (a). If you have access to a computer algebra system that knows elimination orders, then check your answer.

Solution. The basis for I is

$$B = \{t + 2\,y^3 - z^3,\; x^2 - x\,y - y^2 - 2\,z^2, x\,y + 2\,y^2 + y^6 + 3\,z^2 - 2\,y^3\,z^3 + z^6\}.$$

It is a basis for I because if (for ease of reading) we denote its members as given by $B = \{b_1, b_2, b_3\}$, then $I_1 = k[t, x, y, z]b_2 + k[t, x, y, z]b_3$ because $\{b_2,\, b_3\}$ was found as a basis for I_1 using grevlex order with $x > y > z$ and it follows from the Gröbner basis for I relative to lex order and $t > x > y > z$ given way above that $I = k[t, x, y, z]b_1 + I_1$. Putting these together gives $I = k[x, y, z]b_1 + k[x, y, z]b_2 + k[x, y, z]b_3$.

We examine now whether B is a Gröbner basis for I relative to $>_1$. This requires (i) that $B \subset I$, which we know is satisfied, and (ii) $\mathrm{LT}(I) \subset \langle \mathrm{LT}(B)\rangle$, where the leading terms are computed with respect to the monomial order $>_1$. Requirement (ii) can be norrowed down to saying that if $f \in I$ then the $>_1$-leading term of f is divisible by one of the leading monomials $\mathrm{LT}(b_1)$, $\mathrm{LT}(b_2)$, $\mathrm{LT}(b_3)$. Now $t^a x^b y^c z^d >_1 t^{a'} x^{b'} y^{c'} z^{d'}$ if and only if $a > a'$ or $a = a'$ and $x^b y^c z^d >_{grevlex} x^{b'} y^{c'} z^{d'}$. In the grevlex order **after the total degrees agree** the terms are ranked from largest to smallest in ascending powers of z with ties broken by ascending powers of y with ties broken by ascending powers of x. For the elements of b_1 the monomials are $>_1$-ranked $t > 2y^3 > -z^3$ for b_2 they are $x^2 > -xy > -y^2 > -2z^2$ and for b_3 they are $y^6 > -2y^3z^3 > z^6 > xy > 2y^2 > 3z^2$. Thus in the $>_1$ order, $\mathrm{LT}(B) = \{t,\, x^2,\, y^6\}$. Let $f \in I$. Then (iv) $f = h_1b_1 + h_2b_2 + h_3b_3$ where $h_1, h_2, h_3 \in k[x_1, \ldots, x_n]$ and b_1, b_2, b_3 are the previously designated polynomials in B. If $h_1 = 0$, $f \in I_1$ by (iv) and relative to the grevlex order $\mathrm{LT}(f) \in \langle \mathrm{LT}(b_2), \mathrm{LT}(b_3)\rangle$; so $\mathrm{LT}(f)$ is divisible by x^2 or y^6. If $h_1 \neq 0$, then the $>_1$ leading term of f is divisible by t and again $\mathrm{LT}(f) \in \langle \mathrm{LT}(B)\rangle$. These arguments show that B is a Gröbner basis relative to the $>_1$ monomial order.

A Calculation. According to the above

$$J[[1]] = 5\,y^4 + 5\,y^8 + y^{12} + 13\,y^2\,z^2 + 6\,y^6\,z^2 - 10\,y^5\,z^3 - 4\,y^9\,z^3 + 9\,z^4 - 12\,y^3\,z^5 + 5\,y^2\,z^6 + 6\,y^6\,z^6 + 6\,z^8 - 4\,y^3\,z^9 + z^{12} \in I_1.$$

The grevlex leading monomial of $J[[1]]$ polynomial is y^{12} which is indeed in $\langle x^2,\, y^6\rangle = \langle \mathrm{LT}(I_1)\rangle$ in either the grevlex or the $>_1$ order. In fact

$$J[[1]] = (y^2)B[[2]] + (-x\,y + 3\,y^2 + y^6 + 3\,z^2 - 2\,y^3\,z^3 + z^6)B[[3]].$$

Here, of course, we are using Mathematica's notation for the components of a list. So $B[[2]] = b2$ and $B[[3]] = b3$, etc.

Using Mathematica and Elimination orders.

We exhibit the following sequence of commands and outputs:

H={t^2+x^2+y^2+z^2,t^2+2*y^2-x*y-z^2,t+y^3-z^3}

$$\{t^2 + x^2 + y^2 + z^2, t^2 + 2\,y^2 - x\,y - z^2, t + y^3 - z^3\}$$

GroebnerBasis[H,{t,x,y,z}, MonomialOrder->{{1,0,0,0},{1,1,1,1},{0,0,0,-1},{0,0,-1,0}}]

$$\{x^2 + x\,y - y^2 + 2\,z^2, -x\,y + 2\,y^2 + y^6 - z^2 - 2\,y^3\,z^3 + z^6, t + y^3 - z^3\}$$

GroebnerBasis[H,{t,x,y,z}, MonomialOrder->{{1,0,0,0},{1,1,1,1},{0,0,-1,0},{0,0,0,-1}}]

$$\{x^2 - x\,y - y^2 - 2\,z^2, x\,y + 2\,y^2 + y^6 + 3\,z^2 - 2\,y^3\,z^3 + z^6, t + y^3 - z^3\}$$

These bases for $\langle H \rangle = I$ are similar to bases obtained above. Comparing them we see immediately that $x^2 - y^2$, $xy + 2z^2 \in I$ which wasn't obvious before.

$\boxed{\S\mathbf{3.1.8.}}$

In equation (6) – See the summary at the beginning of the solution below – we showed that $z \neq 0$ could be specified arbitrarily. Hence z can be regarded as a "parameter". To emphasize this point, show that there are formulas for x and y in terms of z. Hint: Use $g_1 = y^4z^2 + y^2z^4 - y^2z^2 + 1$ and the quadratic formula to get y in terms of z. Then use $xyz = 1$ to get x. The formulas you obtain give a "parametrization" of $\mathbf{V}(I)$ which is different from those studied in §1.3. Namely, in Chapter 1, we used parametrizations by *rational* functions, whereas here we have what is called a parametrization by *algebraic* functions. Note that x and y are not uniquely determined by z.

Solution. Beginning of Summary: We considered the equations

$$\begin{aligned} x^2 + y^2 + z^2 &= 1, \\ xyz &= 1. \end{aligned} \tag{6}$$

and set $I = \langle x^2 + y^2 + z^2 - 1, \, xyz - 1\rangle$. A Gröbner basis for I with respect to lex order is

$$\begin{aligned} g_1 &= y^4z^2 + y^2z^4 + y^2z^2 + 1, \\ g_2 &= x + y^3z + yz^3 - yz. \end{aligned}$$

The elimination theorem then gave us

$$\begin{aligned} I_1 &= I \cap \mathbb{C}[y, z] = \langle g_1 \rangle, \\ I_2 &= I \cap \mathbb{C}[z] = \{0\}. \end{aligned}$$

Now I_2 is the first elimination ideal. Thus (A) we use the Extension Theorem to go from $c \in \mathbf{V}(I_2)$ to $(b, c) \in \mathbf{V}(I_1)$, and (B) use it a second time to go to $(a, b, c) \in \mathbf{V}(I)$. This will tell us exactly which c's extend.

To carry out step (A), the coefficient of y^4 in g_1 is z^2, so that $c \in \mathbb{C} = \mathbf{V}(I_2)$ extends to (b, c) whenever $c \neq 0$. To carry out step (B): The leading coefficients of x in $x^2 + y^2 + z^2 - 1$ and $xyz - 1$ are 1 and yz, respectively. Since 1 never vanishes the Extension Theorem guarantees that an a always exists and we have proved that if $c \neq 0$ all partial solutions c extend to $\mathbf{V}(I)$. **End of Summary**

The quadratic formula applied to $g_1 = z^2(y^2)^2 + (z^4 - z^2)(y^2) + 1 = 0$ gives

$$\begin{aligned} y^2 &= \frac{z^2 - z^4 \pm \sqrt{(z^4 - z^2)^2 - 4z^2}}{2z^2};, \\ y &= \pm\sqrt{\frac{z^2 - z^4 \pm \sqrt{(z^4 - z^2)^2 - 4z^2}}{2z^2}}, \\ x &= \frac{1}{yz} = \pm\frac{\sqrt{2z^2}}{z\sqrt{z^2 - z^4 \pm \sqrt{(z^4 - z^2)^2 - 4z^2}}}. \end{aligned}$$

x and y are not uniquely determined by z because of the ambiguity created by the $\pm$ symbols in the quadratic formula.

$\boxed{\S\mathbf{3.1.9.}}$

Consider the system of equations given by

$$\begin{aligned} x^5 + \frac{1}{x^5} &= y, \\ x + \frac{1}{x} &= z. \end{aligned}$$

Let I be the ideal in $\mathbb{C}[x, y, z]$ determined by these equations.

(a) Find a basis of $I_1 \subset \mathbb{C}[y,z]$ and show that $I_2 = \{0\}$.

Solution. $I = \langle 1 + x^{10} - x^5 y,\, 1 + x^2 - xz\rangle$ has Gröbner basis G relative to lex order with $x > y > z$, where

$$G = \{y - 5\,z + 5\,z^3 - z^5, 1 + x^2 - x\,z\}.$$

$I_1 = \langle y - 5\,z + 5\,z^3 - z^5\rangle$ and $I_2 = \{0\}$.

(b) Use the Extension Theorem to prove that each partial solution $c \in \mathbf{V}(I_2) = \mathbb{C}$ extends to a solution in $\mathbf{V}(I) \subset \mathbb{C}^3$.

Solution. The coefficient of y in $g_1 = y - 5z + 5z^3 - z^5$ is 1 which is never zero; so $c \in \mathbb{C}$ always extends to a $(b,c) \in \mathbf{V}(I_1)$. Now the coefficients of the highest power of x in g_1 and g_2 are, respectively, 0 and 1; so $\mathbf{V}(0,1) = \emptyset$ and any $(b,c) \in \mathbf{V}(I_1)$ extends to an $(a,b,c) \in \mathbf{V}(I)$. In fact, $b = 5c - 5c^3 + c^5$ and a satisfies $1 + a^2 - ca = 0$. The values of a are then $\frac{c \pm \sqrt{c^2-4}}{2}$.

(c) Which partial solutions $(y,z) \in \mathbf{V}(I_1) \subset \mathbf{R}^2$ extend to solutions in $\mathbf{V}(I) \subset \mathbf{R}^3$? Explain why your answer does not contradict the Extension Theorem.

Solution. (y,z) extends to solutions in $\mathbf{R}^2$ only when $z^2 - 4 \geq 0$. The Extension Theorem only talks about extension in the algebraically closed field $\mathbb{C}$; so it says nothing about "real extensions".

(d) If we regard z as a "parameter" (see Exercise 3.1.8), then solve for x and y as algebraic functions of z to obtain a "parametrization" of $\mathbf{V}(I)$.

Solution. Using the calculations in the solution to part (b) above we find that

$$\left(\frac{z \pm \sqrt{z^2-4}}{2},\, 5z - 5z^3 + z^5,\, z\right) \in \mathbf{V}(I).$$