COMPUTATIONAL COMMUTATIVE ALGEBRA NOTES

ALEXANDER M. KASPRZYK

1. Reference Material

The official course textbook is [CLO07]. This is an excellent book; the style is clear and the material accessible. For this reason, I intend to follow the text quite closely. It is likely, however, that you will need further resources. If you're finding a particular concept tricky, or you wish to explore a topic further, try looking in one of the following books (all available from the library).

Commutative algebra. *Commutative algebra* will provide the machinery we require before any progress can be made. The introductory book [Sha00] is formal in tone, and covers the material in a clear fashion. If you find the flavour not to your liking, then [Rei95] is an excellent (although trickier) alternative. If you enjoy the course, then at some point you will need to tackle [AM69]. The graduate–level book [Eis95] covers everything and then some, however the material is presented at a much more abstract level than we shall require.

Algebraic geometry. We turn to *Algebraic Geometry* to motivate our progress. In particular, we shall consider *affine varieties*. Here you are best consulting [Rei88] or [SKKT00]. Both books are approachable. If you wish to explore further, then [Sha94] is your best bet.

Gröbner bases. Aside from the course text book, [AL94] and [KR00] are excellent references. For the more enthusiastic, [Eis95] covers all the material we shall see, but at a much higher level of abstraction.

To the horizon. If you finish the course and want to learn more, an obvious start is to work through the remainder of [CLO07]. You should also read [AM69, Rei95, Rei88] mentioned above. Cox, Little, and O'Shea have written an excellent sequel, [CLO05]. Kreuzer and Robbiano's second book [KR05] in their computational commutative algebra series is also very good. You might like to look at [Sch03] too.

http://erdos.math.unb.ca/∼kasprzyk/

kasprzyk@unb.ca.

2. A note on computing software

It is important that you have access to some commutative algebra software. In the department you can access *Maple*. Two useful tutorials, by C. Hillar and by J. Roberts, which you may wish to work through are:

`http://www.math.tamu.edu/∼chillar/files/introduction-maple.pdf`
`http://www.math.umn.edu/∼roberts/math5385/matlabinfo/mapleinfo.html`

You may also wish to install some software on your own computer. One possibility is to use *Sage*[1], available for free from:

`http://www.sagemath.org/`

Other very powerful packages, also freely available, are *AXIOM*[2], *Macaulay2*[3], and *GAP*[4]:

`http://axiom-wiki.newsynthesis.org/`
`http://www.math.uiuc.edu/Macaulay2/`
`http://www-gap.mcs.st-and.ac.uk/`

You can read more about the various options in [CLO07, Appendix C].

If you intend to work at home, or for some reason you want to avoid using Maple, you should try to install a commutative algebra package on your own computer at the earliest opportunity. It would be useful if you could report back how it went. I've successfully managed to install Sage, Macaulay2, GAP, and CoCoA on Mac OS X and can help anybody who is having difficulty.

The use of computing software will be essential if you wish to avoid a *serious* amount of calculation. The calculations we shall be performing are best done by a computer, no matter how allergic you believe you are to this concept. Life's too short *not* to use a computer. Honestly.

3. Commutative algebra

This is not intended to be a course on commutative algebra in general; commutative algebra is a vast subject, from which we need only the most basic ideas. Unfortunately we must hurry through the material, covering only what is absolutely essential. If you find our journey too brief then you should consult the books recommended in Section 1.

Although we introduce only a few pieces of machinery, we'll quickly discover that obvious questions can be exceedingly difficult to answer. A methodical approach to solving

[1] Tutorial at `http://www.sagemath.org/doc/html/tut/`.

[2] Introduction at `http://www.dcs.st-and.ac.uk/∼mnd/documentation/axiom_tutorial/`.

[3] Consult [EGSS02] (also available online at `http://www.math.uiuc.edu/Macaulay2/Book/`).

[4] Manual at `http://www-gap.mcs.st-and.ac.uk/Manuals/doc/htm/index.htm`.

these problems is provided by Gröbner bases, however you'll have to wait until Section 8 to see how.

Basic Definitions.

Definition 3.1. A *field* is a set k endowed with two binary operations:

$$\begin{array}{rr} \cdot : k \times k \to k \qquad & + : k \times k \to k \\ (a,b) \mapsto a \cdot b \qquad & (a,b) \mapsto a + b \end{array}$$

called *multiplication* and *addition* respectively. The triple $(k, \cdot, +)$ satisfies:

(1) *Associativity*
$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ and $(a + b) + c = a + (b + c)$ for all $a, b, c \in k$.

(2) *Commutativity*
$a \cdot b = b \cdot a$ and $a + b = b + a$ for all $a, b \in k$.

(3) *Distributivity*
$a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in k$.

(4) *Identities*
There exists an element in k, denoted by 1, such that $1 \cdot a = a$ for all $a \in k$.
There exists an element in k, denoted by 0, such that $0 + a = a$ for all $a \in k$.

(5) *Additive Inverse*
For each $a \in k$ there exists some $b \in k$ such that $a + b = 0$. Such a b is unique (prove this); we usually denote it by $-a$.

(6) *Multiplicative Inverse*
For each $a \in k, a \neq 0$ there exists some $b \in k$ such that $a \cdot b = 1$. Such a b is unique (prove this); we usually denote it by a^{-1}.

Exercise 3.2. Some familiar fields are $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$. Check in each case that they do indeed satisfy the conditions of Definition 3.1. Why has $\mathbb{Z}$ been omitted from this list?

Exercise 3.3. A less familiar example of a field is the set of two elements, $\{0, 1\}$, endowed with multiplication and addition as follows:

$\cdot$	0	1
0	0	0
1	0	1

$+$	0	1
0	0	1
1	1	0

In fact this is simply arithmetic over $\mathbb{Z}$ performed modulo two. Check that this really is a field. We denote this field by $\mathbb{F}_2$ or $\mathbb{Z}/(2)$.

Exercise 3.4. Inspired by Exercise 3.3, let us consider the set of three elements $\{0, 1, 2\}$ and endow it with multiplication and addition given by the usual multiplication and addition on $\mathbb{Z}$ reduced module three. So, for example, $1+2 = 0$ (since $1+2 = 3 \equiv 0 \pmod 3$ in $\mathbb{Z}$), and $2+2 = 1$ (since $2+2 = 4 \equiv 1 \pmod 3$ in $\mathbb{Z}$). Check that the resulting multiplication and addition tables are given by:

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Finally, verify that this defines a field. We shall denote it by $\mathbb{F}_3$ or by $\mathbb{Z}/(3)$.

Exercise 3.5. What about reducing modulo four, to define $\mathbb{Z}/(4)$. Is this a field? If not, why not? Consider $\mathbb{Z}/(5)$ and $\mathbb{Z}/(6)$. Any ideas how to decide in general whether $\mathbb{Z}/(n)$ is a field? Test your conjecture with an example or two.

Definition 3.6. A *commutative ring* is a set R along with two binary operations $\cdot$ and $+$ such that the triple $(R, \cdot, +)$ satisfies the following:

(1) *Associativity*
$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ and $(a + b) + c = a + (b + c)$ for all $a, b, c \in k$.

(2) *Commutativity*
$a \cdot b = b \cdot a$ and $a + b = b + a$ for all $a, b \in k$.

(3) *Distributivity*
$a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in k$.

(4) *Identities*
There exists an element in k, denoted by 1, such that $1 \cdot a = a$ for all $a \in k$.
There exists an element in k, denoted by 0, such that $0 + a = a$ for all $a \in k$.

(5) *Additive Inverse*
For each $a \in k$ there exists some $b \in k$ such that $a + b = 0$. Such a b is unique (prove this); we usually denote it by $-a$.

Remark 3.7. Note that these conditions of Definition 3.6 are the same as conditions (1)-(6) of Definition 3.1; we do not however require the existence of a multiplicative inverse. Note also that nothing in these conditions excludes the case when $1 = 0$. In this case, R is the *zero ring* denoted by 0.

Example 3.8. An example of a familiar ring is $\mathbb{Z}$. Another example which should be familiar to you is the polynomial ring over $\mathbb{R}$ with one indeterminate, which we donote by

$\mathbb{R}[x]$ (addition and multiplication are just the standard polynomial addition and multiplication). More generally $k[x]$ is a ring for any field k. More generally still, we can allow finitely many indeterminates $k[x_1, \ldots, x_n]$.

Exercise 3.9. Why is $\mathbb{R}[x]$ (or, for that matter, $k[x]$) *not* a field? Can you think of a way to enlarge $\mathbb{R}[x]$ to create a field?

Definition 3.10. Let R be a commutative ring such that for all $a, b \in R$ with $a \cdot b = 0$, either $a = 0$ or $b = 0$. We call R an *integral domain* (or sometimes simply a *domain*).

Exercise 3.11. Prove that any field k, when regarded as a commutative ring, is an integral domain.

Remark 3.12. From Exercise 3.11 we see that integral domains are sort of "half-way" towards being a field. It is natural to look for an example of an integral domain which is not a field. Fortunately we don't need to look very far: our rings in Example 3.8 will suffice. An example of a ring which is not an integral domain is $\mathbb{Z}/(4)$.

Definition 3.13. Let R be a commutative ring, and $I \subset R$ a subset satisfying:

(1) $0 \in I$
(2) If $a, b \in I$ then $a + b \in I$ (i.e. I is *closed under addition*)
(3) If $a \in R, b \in I$ then $a \cdot b \in I$.

Then we call I an *ideal*.

Remark 3.14. Note that condition (3) of Definition 3.13 tells us that I is *closed under multiplication*.

Example 3.15. Ideals are crucially important objects. Let us consider the ring $\mathbb{Z}$, and define the set:

$$(n) := \{kn \mid k \in \mathbb{Z}\}, \qquad \text{for any } n \in \mathbb{Z}.$$

Then (n) is an ideal for any $n \in \mathbb{Z}$ (you should check that the conditions are satisfied). We can attempt to extend this construction by defining:

$$(n, m) := \{kn, km \mid k \in \mathbb{Z}\}, \qquad \text{for any } n, m \in \mathbb{Z}.$$

This attempt isn't good enough, however, since the resulting set is not an ideal. For example, using this definition, consider $(2, 3)$. This obviously contains 2 and 3, but does not contain the number $2+3=5$ and so is not closed under addition. The correct definition to use is:

$$(n,m) := \{kn + k'm \mid k, k' \in \mathbb{Z}\}, \qquad \text{for any } n, m \in \mathbb{Z}.$$

Now we see that (n,m) is always an ideal. Can you see how to generalise this to an arbitrary finite number of generators $(n_1, \ldots, n_m)$?

Polynomial Rings.

Example 3.16. Another important place to look for ideals is in the polynomial ring $k[x_1, \ldots, x_n]$ (remember that k can be any field, but you are best of thinking of $\mathbb{R}$ or, even better, $\mathbb{C}$). We shall consider $k[x] := \{a + bx \mid a, b \in k\}$. Let $f \in k[x]$ be any function in the polynomial ring. We define the *ideal generated by* f to be:

$$(f) := \{gf \mid g \in k[x]\} \qquad \text{(c.f. Example 3.15).}$$

You should check that this really does define an ideal.

Consider (x). Any non-zero element in this ideal is a function of the form $xg(x)$. I.e. it contains a factor x. Hence $x = 0$ is a root of any function in (x). Now consider any function $g \in k[x]$ such that $g(0) = 0$. Then g factorises in the form $g(x) = xh(x)$ for some polynomial $h \in k[x]$. But this implies that $g \in (x)$. Thus we see that the ideal (x) is precisely those polynomials which have a root at $x = 0$.

Exercise 3.17. Repeat the steps in Example 3.16 for the ideal $(x-3) \subset \mathbb{R}[x]$. Describe the intersection $(x) \cap (x-3)$. Is this intersection an ideal?

Definition 3.18. Let $f_1, \ldots, f_m$ be polynomials in a polynomial ring $k[x_1, \ldots, x_n]$. Set:

$$(f_1, \ldots, f_m) = \{h_1 f_1 + \ldots + h_m f_m \mid h_i \in k[x_1, \ldots, x_n]\}.$$

Then $(f_1, \ldots, f_m)$ is an ideal, called the *ideal generated by* $f_1, \ldots, f_m$.

Lemma 3.19. *The set $(f_1, \ldots, f_m)$ in Definition 3.18 really is an ideal.*

Proof. First we observe that $0 \in (f_1, \ldots, f_m)$, by setting all the $h_i = 0$. Now suppose that $f = \sum a_i f_i$ and $g = \sum b_i f_i$ are two elements in $(f_1, \ldots, f_m)$. Then:

$$f + g = \sum a_i f_i + \sum b_i f_i = \sum (a_i + b_i) f_i \in (f_1, \ldots, f_m).$$

Finally, let $p \in k[x_1, \ldots, x_n]$. Then:

$$pf = p \sum a_i f_i = \sum p a_i f_i \in (f_1, \ldots, f_m).$$

□

Remark 3.20. As in Example 3.16, the ideal in Definition 3.18 has a nice interpretation in terms of roots. Given $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ we set each polynomial equal to zero, obtaining the system of equations:

$$\begin{aligned} f_1 &= 0, \\ &\vdots \\ f_m &= 0. \end{aligned}$$

From these equations we can derive others. We are free to multiply any f_i by any other polynomial h_i, and to add together the resulting equations, with the result:

$$h_1 f_1 + \ldots + h_m f_m = 0 \qquad \text{for any } h_i \in k[x_1, \ldots, x_n].$$

But this is precisely the definition of $(f_1, \ldots, f_m)$.

Example 3.21. Let us consider ideal generated by the polynomials $x+1, y-2 \in \mathbb{R}[x, y]$. We obtain the system of equations:

$$\begin{aligned} x+1 &= 0, \\ y-2 &= 0. \end{aligned}$$

In other words, $x = -1, y = 2$. Now let us consider an arbitrary element in $(x+1, y-2)$. This element will be of the form:

$$(x+1)h_1(x, y) + (y-2)h_2(x, y), \qquad \text{for some } h_1, h_2 \in \mathbb{R}[x, y].$$

Clearly this is zero when $x = -1, y = 2$.

Definition 3.22. We say that an ideal $I \subset k[x_1, \ldots, x_n]$ is *finitely generated* if there exists $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ such that $I = (f_1, \ldots, f_m)$. We call $f_1, \ldots, f_m$ a *basis* for I.

Remark 3.23. Although all the ideals we have seen so far are finitely generated, this need not always be the case. In 1890 David Hilbert[5] proved that any ideal of a polynomial ring $k[x_1, \ldots, x_n]$ is finitely generated (Theorem 7.9). His proof was very abstract for the time, and was famously denounced as "theology, not mathematics" by his peers. The brilliant mathematician Emmy Noether[6] generalised Hilbert's results still further, cutting right to the heart of the matter in her study of what we now call *Noetherian rings.*

Example 3.24. As you might expect, non-finitely generated ideals do exist.

[5] For a brief biography of Hilbert, see
http://www-groups.dcs.st-and.ac.uk/~history/Biographies/Hilbert.html.

[6] For a brief biography of Noether, see
http://www-groups.dcs.st-and.ac.uk/~history/Biographies/Noether_Emmy.html.

(1) Consider the infinitely generated polynomial ring $k[x_1, x_2, x_3, \ldots]$. Clearly the ideal $(x_1, x_2, x_3, \ldots)$ cannot be finitely generated.

(2) Consider the ring R generated by all polynomials of the form $c + xf(x, y)$, where $c \in k$ and $f \in k[x, y]$. With a little thought, we see that we can rewrite this more succinctly as:

$$R = k[x, xy, xy^2, \ldots].$$

The ideal $(x, xy, xy^2, \ldots)$ is clearly not finitely generated.

Remark 3.25. Given an ideal I which we know to be finitely generated, it is a natural to ask how we can find a bases for I. Gröbner bases answer precisely this question.

Exercise 3.26. Prove that the ideals (x, y), $(x + y, x - y)$, and $(x + xy, y + xy, x^2, y^2)$ in $k[x, y]$ are equal. Thus we see that there may exist *many different choices of bases* for a finitely generated ideal. Moreover, the number of generators is not unique. This situation is fundamentally different from that encountered in linear algebra.

Exercise 3.27. Given the ideal $(x^4 - 1, x^6 - 1) \subset k[x]$, we should like to know whether we can write this ideal using just one generator. In fact we can. Prove that $(x^4 - 1, x^6 - 1) = (x^2 - 1)$. Knowing this, it is now easy to decide whether a given polynomial f lies in the ideal or not. Why is this? Is $x^3 - x$ contained in the ideal? What about $x^6 + x^4$?

Definition 3.28. An ideal I of a polynomial ring $k[x_1, \ldots, x_n]$ is called a *principal ideal* if it can be generated by a single polynomial $I = (f)$, for some $f \in k[x_1, \ldots, x_n]$. Equivalently, I is principal if there exists a basis of size one.

Remark 3.29. As we saw in Exercise 3.27, deciding whether a particular polynomial is contained in a given ideal or not is easy if we can write our ideal as a principal ideal. This suggests three questions:

(1) Can we decide whether an ideal is principal or not?
(2) If an ideal is principal, how do we find a bases of size one?
(3) If an ideal is not principal, how do we decide whether a given element is contained in the ideal?

Gröbner bases allow us to answer all three questions.

Exercise 3.30. To demonstrate how difficult things can become, are the following two statements true?

(1) $y^2 - xz \in (y - x^2, z - x^3)$

(2) $x^3 + 4x^2 + 3x - 7 \in (x^3 - 3x + 2, x^4 - 1, x^6 - 1)$

[Hint: For (2) use Exercise 3.27 to express the ideal using only two elements. Now attempt to express the ideal as a principal ideal. If you can do this, you can readily find the answer.]

We shall answer (2) in Example 5.11. (1) shall have to wait until Example 6.25, however it will take until Example 8.10 for a really satisfying solution.

4. Affine varieties

Now that we've covered the basic definitions of commutative algebra, we can look briefly at Algebraic Geometry. Once again this is a huge subject from which we shall see only the most elementary concepts. For an enjoyable history, see [Rei88, §8].

Forwards to affine varieties...

Definition 4.1. Let k be a field and $n \in \mathbb{Z}_{>0}$. We define the *n-dimensional affine space over k* to be the set:

$$k^n = \{(a_1, \ldots, a_n) \mid a_i \in k\}.$$

Remark 4.2. It is also common to denote the affine space k^n by $\mathbb{A}^n_k$ (or simply $\mathbb{A}^n$). We call one-dimensional affine space $k^1 = k$ the *affine line*, and two-dimensional affine space k^2 the *affine plane*. (And yes, affine space really is as simple as you're thinking it is.)

Let $f \in k[x_1, \ldots, x_n]$ be a polynomial. Then f is a function from n-dimensional affine space to the field k:

$$f : k^n \to k.$$

To spell it out: the point $(a_1, \ldots, a_n) \in k^n$ in affine space is mapped to $f(a_1, \ldots, a_n) \in k$. (And yes, once again this really is that simple.)

Definition 4.3. Let k be a field, and let $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ be a finite number of polynomials. Then

$$\mathbb{V}(f_1, \ldots, f_m) := \{(a_1, \ldots, a_n) \in k^n \mid f_i(a_1, \ldots, a_n) = 0 \text{ for all } 1 \le i \le m\}$$

is called the *affine variety defined by* $f_1, \ldots, f_m$.

Remark 4.4. An affine variety $\mathbb{V}(f_1, \ldots, f_m)$ is simply the set of solutions to the system of equations:

$$\begin{aligned} f_1 &= 0, \\ &\vdots \\ f_m &= 0. \end{aligned}$$

For example, the affine variety $\mathbb{V}(2x - y) \subset \mathbb{R}^2$ corresponds to the graph of the function $y = 2x$. Similarly the variety $\mathbb{V}(x^2 + y^2 - 1)$ is the circle of radius one centred at the origin. Any polynomial $y = f(x_1, \ldots, x_n)$ can be viewed as an affine variety; namely as $\mathbb{V}(f(x_1, \ldots, x_n) - y)$ in k^{n+1}.

Example 4.5. It is easy to produce examples of affine varieties. Here are three examples to make you think:

(1) The conic sections (circles, ellipses, parabolas, and hyperbolas) are all affine varieties. You know how the conic sections are related (if not, look it up); does that give you any ideas about the affine varieties?
(2) The graph of $y = \frac{1}{x}$ corresponds to an affine variety – we simply multiply through by x, obtaining $\mathbb{V}(xy - 1)$.
(3) Similarly the graph of any *rational function* is also an affine variety (see Definition 4.6).

Definition 4.6. Let $k[x_1, \ldots, x_n]$ be a polynomial ring over a field k. A *rational function* is a quotient $\frac{f}{g}$ of two polynomials $f, g \in k[x_1, \ldots, x_n], g \neq 0$. Two rational functions $\frac{f_1}{g_1}$ and $\frac{f_2}{g_2}$ are equal provided that $f_1 \cdot g_2 = f_2 \cdot g_1$. The set of all rational functions (in $x_1, \ldots, x_n$ and with coefficients in k) is denoted $k(x_1, \ldots, x_n)$.

Exercise 4.7. Look once more at Exercise 3.9. Have you any thoughts? Can you prove what you're thinking?

Remark 4.8. If you have access to computer graphing software such as *Maple* (or *Grapher* on Max OS X, which can be found in the folder `/Applications/Utilities`), this gives you the perfect opportunity to play with plotting various graphs under the guise of experimenting with affine varieties. For some pictures see [CLO07, pg. 7] or the wonderful plots in [SKKT00].

Example 4.9. An important example is the *twisted cubic*. This is the variety $\mathbb{V}(y - x^2, z - x^3)$ (c.f. Example 3.30 (1)). It's given by the intersection of $y = x^2$ and $z = x^3$ in k^3. You should plot both equations and their intersection. Notice that $y = x^2$ cuts out a surface in k^3, as does $z = x^3$. Their intersection is a curve (see Figure 1).

Definition 4.10. Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. Then

$$\mathbb{V}(I) := \{(a_1, \ldots, a_n) \in k^n \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in I\}$$

is called the *affine variety defined by I*.

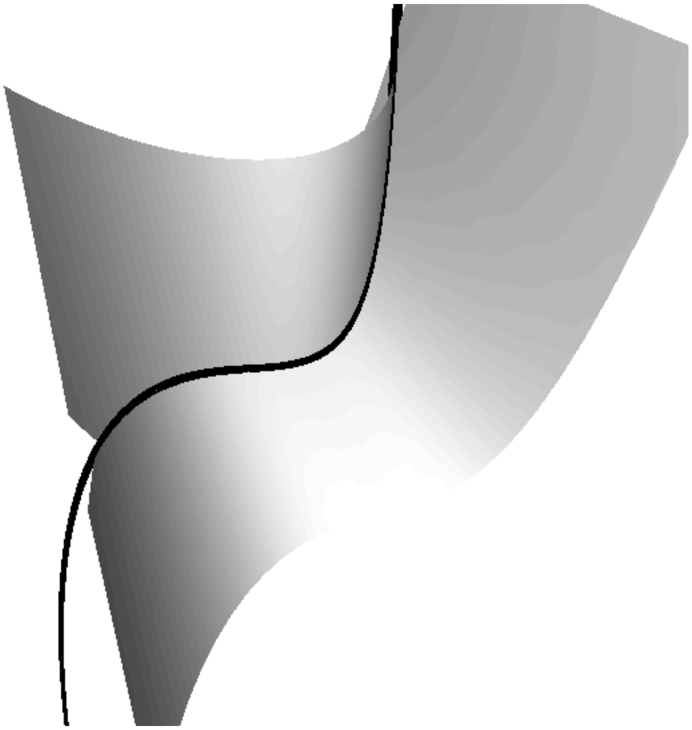

FIGURE 1. The twisted cubic is the curve given by the intersection of the surfaces $y = x^2$ and $z = x^3$.

Remark 4.11. Although superficially Definition 4.10 seems to be a significant abstraction of Definition 4.3, really very little has changed. Recall from Remark 3.23 that ideals of polynomial rings are finitely generated. Hence we can write $I = (f_1, \ldots, f_m)$ for some $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ and the two definitions become equivalent.

Example 4.12. Let $I = (z^2 - x^2 - y^2) \subset k[x, y, z]$. Then the variety $\mathbb{V}(I) \subset k^3$ is a cone with apex at the origin, pictured in Figure 2.

Exercise 4.13. Consider the affine varieties $U = \mathbb{V}(x, y)$, $V = \mathbb{V}(x + y, x - y)$, and $W = \mathbb{V}(x + xy, y + xy, x^2, y^2)$. You should be able to see that $U = V = W = \{(0, 0)\}$. Compare this result with Exercise 3.26. What about the varieties $\mathbb{V}(x^4 - 1, x^6 - 1)$ and $\mathbb{V}(x^2 - 1)$ (see Exercise 3.27)?

Exercise 4.14. Suppose that $(f_1, \ldots, f_m) = (g_1, \ldots, g_s)$. Show that $\mathbb{V}(f_1, \ldots, f_m) = \mathbb{V}(g_1, \ldots, g_s)$.

Remark 4.15. Exercise 4.14 is an important result. What it says is that by changing the basis of the ideal, you can make it easier to determine the variety. For example, if you

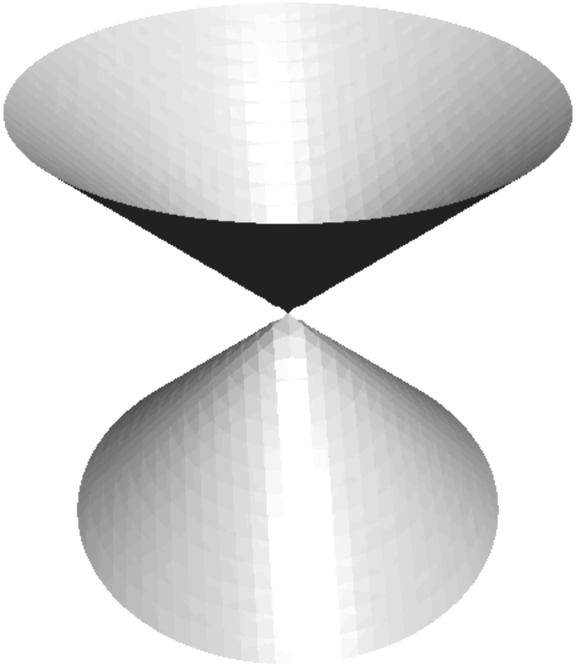

FIGURE 2. The cone in $\mathbb{R}^3$ given by $z^2 = x^2 + y^2$.

can write your ideal as a principal ideal (f), then the resulting variety corresponds to the graph $f = 0$. Unfortunately being able to find "nice" bases for an ideal is one of the things we don't yet know how to do (see Remark 3.29).

Example 4.16. You mustn't get carried away by Exercise 4.14. The converse statement is slightly more subtle, and requires knowledge of the *radical*; we shall return to this in Section 10.

Consider $\mathbb{V}(x)$ and $\mathbb{V}(x^2)$ in $\mathbb{R}^2$. Clearly these two varieties are equal (they both correspond to the y-axis) however the ideals (x) and (x^2) are different (for instance, $x \in (x)$ but $x \notin (x^2)$). It is not a coincidence that squaring x gives us an element in (x^2).

...And backwards to commutative algebra.

Definition 4.17. Let $V \subset k^n$ be an affine variety. Then

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

is called the *ideal of* V.

Proposition 4.18. *The set* $\mathbb{I}(V)$ *really is an ideal.*

Proof. Clearly the zero polynomial $0 \in \mathbb{I}(V)$. Now suppose that $f, g \in \mathbb{I}(V)$. Then for any $(a_1, \ldots, a_n) \in V$ we have:

$$f(a_1, \ldots, a_n) + g(a_1, \ldots, a_n) = 0 + 0 = 0$$

and so $f + g \in \mathbb{I}(V)$. Now let $h \in k[x_1, \ldots, x_n]$. We have that:

$$h(a_0, \ldots, a_n) f(a_0, \ldots, a_n) = h(a_0, \ldots, a_n) \cdot 0 = 0$$

and so $hf \in \mathbb{I}(V)$. □

Example 4.19. Let $V = \{(0,0)\} \subset k^2$ be the affine variety consisting only of the origin. We shall show that $\mathbb{I}(V) = (x, y)$. Clearly any polynomial of the form $f(x,y) \cdot x + g(x,y) \cdot y \in k[x,y]$, $f, g \in k[x,y]$, vanishes at the origin. Hence $(x,y) \subset \mathbb{I}(V)$.

For the other inclusion let $f = \sum_{i,j} a_{ij} x^i y^j \in k[x,y]$ be such that $f(0,0) = 0$. Then $a_{00} = 0$, and so:

$$\begin{aligned} f &= a_{00} + \sum_{i,j \neq 0,0} a_{ij} x^i y^j \\ &= 0 + \Big(\sum_{\substack{i,j \\ i>0}} a_{ij} x^{i-1} y^j \Big) x + \Big(\sum_{j>0} a_{0j} y^{j-1} \Big) y \in (x,y). \end{aligned}$$

Hence $\mathbb{I}(V) \subset (x,y)$ and we're done.

Remark 4.20. Naïvely, it would be wonderful if $\mathbb{I}(\mathbb{V}(f_1, \ldots, f_m)) = (f_1, \ldots, f_m)$. Although Example 4.16 shows that this is not true in general, we do always have an inclusion.

Proposition 4.21. *$(f_1, \ldots, f_m) \subset \mathbb{I}(\mathbb{V}(f_1, \ldots, f_m))$.*

Proof. Let $f \in (f_1, \ldots, f_m)$. Then we can write:

$$f = \sum_{i=1}^{m} h_i f_i, \qquad \text{for some } h_i \in k[x_1, \ldots, x_n].$$

But the f_i vanish on $\mathbb{V}(f_1, \ldots, f_m)$, thus so does f. Hence $f \in \mathbb{I}(\mathbb{V}(f_1, \ldots, f_m))$. □

Example 4.22. Let V and W be affine varieties in k^n. Prove that $V \subset W$ if and only if $\mathbb{I}(W) \subset \mathbb{I}(V)$. In other words, passing between varieties and ideals reverses the order of inclusion.

5. Polynomials in $k[x]$

We restrict our attention to polynomials in one indeterminate – a case you should already be familiar with. We will see how to write any ideal $(f_1, \ldots, f_m) \in k[x]$ as a principal ideal. Knowing how to do this allows us to decide whether a given polynomial $g \in k[x]$ is contained in our ideal. In the next section we shall generalise these results to an arbitrary polynomial ring $k[x_1, \ldots, x_n]$.

Definition 5.1. Let $f \in k[x]$ be a non-zero polynomial. Then we can write f in the form:

$$f = a_0x^m + a_1x^{m-1} + \ldots + a_m, \qquad \text{where } a_i \in k, a_0 \neq 0.$$

The *degree* of f, denoted $\deg(f)$ is m. The *leading term* of f, denoted by $\mathrm{LT}(f)$, is a_0x^m.

Proposition 5.2 (Division Algorithm in $k[x]$)**.** *Let $g \in k[x]$ be a non-zero polynomial. Every $f \in k[x]$ can be written uniquely in the form:*

$$f = gq + r$$

for some $q, r \in k[x]$, where either $r = 0$ or $\deg(r) < \deg(g)$.

Proof. Begin by setting $q = 0$ and $r = f$. It is certainly true that $f = gq + r$. Inductively, set:

$$q' = q + \frac{\mathrm{LT}(r)}{\mathrm{LT}(g)}, \qquad r' = r - \frac{\mathrm{LT}(r)}{\mathrm{LT}(g)}g.$$

Then:

$$\begin{aligned} q'g + r' &= \Big(q + \frac{\mathrm{LT}(r)}{\mathrm{LT}(g)}\Big)g + \Big(r - \frac{\mathrm{LT}(r)}{\mathrm{LT}(g)}g\Big) \\ &= qg + r \\ &= f. \end{aligned}$$

Suppose that $\deg(r) \geq \deg(g)$. Writing $r = a_0x^m + \ldots + a_m$, and $g = b_0x^k + \ldots + b_k$, where $a_0 \neq 0$ and $b_0 \neq 0$, we have that $m \geq k$. Then:

$$r - \frac{\mathrm{LT}(r)}{\mathrm{LT}(g)}g = (a_0x^m + \ldots) - \frac{a_0}{b_0}x^{m-k}(b_0x^k + \ldots),$$

and we see that either the degree of r must drop, or the whole expression vanishes. Since the degree is finite, eventually either $\deg(r) < \deg(g)$ or $r = 0$. When this occurs, we are done.

Finally, we need to show uniqueness. Suppose that $f = qg + r = \tilde{q}g + \tilde{r}$, where either $\deg(r) < \deg(g)$ or $r = 0$, and either $\deg(\tilde{r}) < \deg(g)$ or $\tilde{r} = 0$. If $r \neq \tilde{r}$ then $\deg(r - \tilde{r}) < \deg(g)$. Since $(q - \tilde{q})g = \tilde{r} - r$ we see that $q - \tilde{q} \neq 0$. Hence:

$$\deg(\tilde{r} - r) = \deg((q - \tilde{q})g) = \deg(q - \tilde{q}) + \deg(g) \geq \deg(g).$$

This is a contradiction. Hence $r = \tilde{r}$ and we see that $q = \tilde{q}$. □

Example 5.3. Let $f = x^3 + x^2 - 1$ and $g = x + 2$. Following the proof of Proposition 5.2, the first step is to set $q = 0$ and $r = f$. We now ask, "Is $\deg(r) < \deg(g)$, or is $r = 0$?". If the answer is yes then we stop; q and r equal their unique values. In this case the answer is no, so we make calculate a new q and r as follows:

$$\begin{aligned}
\text{New } q &= q + \frac{\mathrm{LT}(r)}{\mathrm{LT}(g)} \\
&= 0 + \frac{x^3}{x} \\
&= x^2. \\
\text{New } r &= r - \frac{\mathrm{LT}(r)}{\mathrm{LT}(g)} g \\
&= x^3 + x^2 - 1 - \frac{x^3}{x}(x+2) \\
&= -x^2 - 1.
\end{aligned}$$

We now repeat the process. Is $\deg(r) < \deg(g)$, or is $r = 0$? The answer is still no. So:

$$\begin{aligned}
\text{New } q &= x^2 + \frac{-x^2}{x} \\
&= x^2 - x. \\
\text{New } r &= -x^2 - 1 - \frac{-x^2}{x}(x+2) \\
&= 2x - 1.
\end{aligned}$$

Once again we ask, "Is $\deg(r) < \deg(g)$, or is $r = 0$?" No.

$$\begin{aligned}
\text{New } q &= x^2 - x + \frac{2x}{x} \\
&= x^2 - x + 2. \\
\text{New } r &= 2x - 1 - \frac{2x}{x}(x+2) \\
&= -5.
\end{aligned}$$

This time we're done, with the answer:

$$x^3 + x^2 - 1 = (x+2)(x^2 - x + 2) - 5.$$

Remark 5.4. To perform this computation in *Maple*, type `rem(x^3+x^2-1,x+2,x);` to calculate r, and `quo(x^3+x^2-1,x+2,x);` to calculate q.

Example 5.5. The wonderful thing about Proposition 5.2 is the fact that q and r are unique. Thus it doesn't matter *how* you find your q and r; so long as either $\deg(r) < \deg(g)$ or $r = 0$ you have *the* unique answer.

Let us repeat Example 5.3 using long division. We get:

$$
\begin{array}{r r}
 & x^2 - x + 2 \\ \cline{2-2}
x+2 \,\big) & x^3 + x^2 - 1 \\
 & x^3 + 2x^2 \\ \cline{2-2}
 & -\,x^2 - 1 \\
 & -\,x^2 - 2x \\ \cline{2-2}
 & 2x - 1 \\
 & 2x + 4 \\ \cline{2-2}
 & -\,5
\end{array}
$$

We see that $q = x^2 - x + 2$ and $r = -5$, as expected.

Corollary 5.6. *Let $f \in k[x]$ be a non-zero polynomial. Then f has at most* $\deg(f)$ *roots in k.*

Proof. We proceed by induction on the degree $\deg(f)$. If $\deg(f) = 0$ then f is a non-zero constant, and we are done. Suppose that the result is true for all polynomials of degree less than m, and suppose that f has degree equal to m. If f has no roots in k then we are done. Otherwise, let $a \in k$ be a root. Dividing f by $x - a$, by Proposition 5.2 we obtain $f = q(x-a) + r$ for some $r \in k$. Hence:

$$0 = f(a) = q(a)(a-a) + r = r,$$

and so $f = q(x-a)$. Since q has degree less than m, the result follows. □

Corollary 5.7. *Every ideal $I \subset k[x]$ is principal. Furthermore, if $I = (f)$ for some $f \in k[x]$, then f is unique up to multiplication by a non-zero scalar in k.*

Proof. If $I = \{0\}$ then we are done, since $I = (0)$. Suppose instead that $f \in I$ is a non-zero polynomial of minimum degree. We claim that $(f) = I$.

The inclusion $(f) \subset I$ is obvious. In the opposite direction, let $g \in I$. By Proposition 5.2 we can write $g = qf + r$, where either $\deg(r) < \deg(f)$ or $r = 0$. Note that $r = g - qf$ and so lies in I. Hence by minimality of f we have that $r = 0$. Thus $f = qf$ and so lies in (f).

To prove uniqueness up to non-zero multiplication, suppose that $(f) = (g)$. Since $f \in (g)$ there exists some $h \in k[x]$ such that $f = hg$. Thus $\deg(f) = \deg(h) + \deg(g)$.

Interchanging the roles of f and g we conclude that $\deg(f) = \deg(g)$, and so h is a non-zero constant. □

Definition 5.8. A *greatest common divisor* of polynomials $f, g \in k[x]$ is a polynomial h such that:

(1) h divides f and g;
(2) If p is another polynomial dividing both f and g then p divides h.

We often write $\gcd(f, g)$ for h.

Exercise 5.9. By using Proposition 5.2, prove that a $\gcd(f, g)$ exists and is unique up to multiplication by a non-zero scalar in k. Prove also that $\gcd(f, g)$ is a generator of the ideal (f, g).

Remark 5.10. Given two polynomials $f, g \in k[x]$, the *Euclidean Algorithm* can be used to compute $\gcd(f, g)$. Begin by setting $h = f$ and $s = g$. If $s = 0$ then $h = \gcd(f, g)$ and we're done. Otherwise we use Proposition 5.2 to write $h = qs + r$ and inductively set:

$$h' = s, \qquad s' = r.$$

Since either $\deg(r) < \deg(g)$ or $r = 0$, we see that at each step in the induction the degree of r falls. Since degrees are finite, we conclude that eventually $r = 0$ and $h = qs$. We claim that, when this occurs, $s = \gcd(f, g)$.

To prove this we simply observe that the ideals (h, s) and $(h-qs, s) = (r, s) = (s', h')$ are equal. Hence by Exercise 5.9 we have that $\gcd(h, s) = \gcd(h', s')$ at each step. Inductively we see that $\gcd(f, g) = \gcd(h, s)$ and, at the final step when $r = 0$, we have $\gcd(h, s) = \gcd(0, s) = s$.

Example 5.11. We shall return to Exercise 3.27 and use the Euclidean Algorithm to show that $(x^4 - 1, x^6 - 1) = (x^2 - 1)$. By taking care in our lay-out, the algorithm is very clear. We start by setting $h = x^4 - 1$ and $s = x^6 - 1$. At each step we calculate $h = qs + r$ and set $h' = s$, $s' = r$. We obtain:

$$\begin{array}{rcrcl}
h & = & qs & + & r \\
\hline
x^4 - 1 & = & 0(x^6 - 1) & + & (x^4 - 1) \\
x^6 - 1 & = & x^2(x^4 - 1) & + & (x^2 - 1) \\
x^4 - 1 & = & (x^2 + 1)(x^2 - 1) & + & 0
\end{array}$$

The final value of s is $x^2 - 1$. Hence we conclude that $(x^4 - 1, x^6 - 1) = (x^2 - 1)$, as desired.

Remark 5.12. To perform this computation in *Maple*, enter the command:

```
gcd(x^4-1,x^6-1);
```

Definition 5.13. We can generalise Definition 5.8 to a finite number of polynomials $f_1, \ldots, f_m \in k[x]$, where $m \geq 2$. We call h a *greatest common divisor of* $f_1, \ldots, f_m$, and write $h = \gcd(f_1, \ldots, f_m)$, if:

(1) h divides f_i for all $1 \leq i \leq m$;
(2) If p is another polynomial dividing each f_i, $1 \leq i \leq m$, then p divides h.

Exercise 5.14. Let $f_1, \ldots, f_m \in k[x]$, where $m \geq 2$. Prove that:

(1) $\gcd(f_1, \ldots, f_m)$ exists and is unique up to multiplication by a non-zero scalar.
(2) Let $h = \gcd(f_1, \ldots, f_m)$. Then $(h) = (f_1, \ldots, f_m)$.
(3) $\gcd(f_1, \ldots, f_m) = \gcd(f_1, \gcd(f_2, \ldots, f_m))$.

Remark 5.15. Exercise 5.14 is an important result. Part (2) tells us that we can write any ideal $(f_1, \ldots, f_m) \subset k[x]$ as a principal ideal, provided that we can find the greatest common divisor of the f_i. Part (3) tells us how to do this. Namely, we calculate $h_{m-1} := \gcd(f_{m-1}, f_m)$ using the Euclidean Algorithm (Remark 5.10). Then, inductively, we calculate $h_i := \gcd(f_i, h_{i+1})$ (again using the Euclidean Algorithm). The value h_1 is a greatest common divisor of the f_i.

Since every ideal $I \subset k[x]$ is finitely generated, we conclude that every ideal in $k[x]$ is principal. We call $k[x]$ a *principal ideal domain*.

Example 5.16. Consider the ideal $(x^3 - 3x + 2, x^4 - 1, x^6 - 1) \subset k[x]$. We shall decide whether $x^3 + 4x^2 + 3x - 7$ is contained in this ideal or not (see Exercise 3.30 (2)).

First we need to write our ideal as a principal ideal. To do this we need to find $\gcd(x^3 - 3x + 2, x^4 - 1, x^6 - 1)$. By Exmple 5.11 we know that $\gcd(x^4 - 1, x^6 - 1) = x^2 - 1$. Thus $\gcd(x^3 - 3x + 2, x^4 - 1, x^6 - 1) = \gcd(x^3 - 3x + 2, x^2 - 1)$.

$$\begin{array}{rcrcl} h & = & qs & + & r \\ \hline x^3 - 3x + 2 & = & x(x^2 - 1) & + & (-2x + 2) \\ x^2 - 1 & = & (-\frac{x}{2} - \frac{1}{2})(-2x + 2) & + & 0 \end{array}$$

Hence $\gcd(x^3 - 3x + 2, x^2 - 1) = -2x + 2$. Since we are allowed to multiply by a non-zero scalar (Exercise 5.14 (1)) we may write $\gcd(x^3 - 3x + 2, x^2 - 1) = x - 1$.

By Exercise 5.14 (2) we have that $(x^3 - 3x + 2, x^4 - 1, x^6 - 1) = (x - 1)$. It is easy to decide whether $x^3 + 4x^2 + 3x - 7 \in (x - 1)$. You can use long division if you wish, or the Division Algorithm. In this particular case, however, things are easy. We know that any $f \in (x-1)$ can be written in the form $f(x) = (x-1)h(x)$ for some $h \in k[x]$. In particular, $f(1) = 0$. Setting $x = 1$ in $x^3 + 4x^2 + 3x - 7$ gives $1 \neq 0$. We conclude that $x^3 + 4x^2 + 3x - 7 \notin (x^3 - 3x + 2, x^4 - 1, x^6 - 1)$.

Remark 5.17. *Maple* doesn't have a command to calculate $\gcd(f_1, \ldots, f_m)$ in one step. To calculate $\gcd(x^3 - 3x + 2, x^4 - 1, x^6 - 1)$ you would type:

```
gcd(x^3-3*x+2,gcd(x^4-1,x^6-1));
```

To check for inclusion, use the `rem` command.

6. Monomial orderings and a Division Algorithm

We shall see how to generalise the results of Section 5 to an arbitrary polynomial ring $k[x_1, \ldots, x_n]$. First, we need to make a choice which didn't exists in $k[x]$: how do we order the indeterminants $x_1, \ldots, x_n$ when running a generalised Division Algorithm?

Monomial orderings.

Definition 6.1. We call $x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n} \in k[x_1, \ldots, x_n]$ a *monomial* of *total degree* $\alpha_1 + \ldots + \alpha_n$.

Remark 6.2. It is convenient to write $x^\alpha := x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$, where $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$. We see that there is a one-to-one correspondence between monomials in $k[x_1, \ldots, x_n]$ and the points of $\mathbb{Z}^n_{\geq 0}$. Multiplication of two monomials x^α and x^β corresponds with addition of the points α and β. I.e. $x^\alpha \cdot x^\beta = x^{\alpha+\beta} \leftrightarrow \alpha + \beta$.

We write $|\alpha| = |(\alpha_1, \alpha_2, \ldots, \alpha_n)| := \alpha_1 + \ldots + \alpha_n$ for the *total degree* of α. Obviously $|\alpha|$ equals the total degree of x^α.

Definition 6.3. A *total order* (or *linear order*) on $\mathbb{Z}^n_{\geq 0}$ is a binary relation $>$ satisfying:

(1) $>$ *is transitive*
For any $\alpha, \beta, \gamma \in \mathbb{Z}^n_{\geq 0}$, $\alpha > \beta$ and $\beta > \gamma$ implies $\alpha > \gamma$;
(2) $>$ *is trichotomous*
For any $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, precisely one of the following holds:
(a) $\alpha > \beta$,
(b) $\alpha = \beta$,
(c) $\beta > \alpha$.

Example 6.4. In $\mathbb{Z}_{\geq 0}$ our usual notion of inequality is a total order. On $\mathbb{Z}^2_{\geq 0}$ we could define $(a,b) > (a',b')$ if and only if either $a > a'$ or $a = a'$ and $b > b'$. Under this ordering we see that, for example, $(3,2) > (2,2)$ and $(5,7) > (5,1)$. You should check that this defines a total order.

Remark 6.5. Given a total order $>$ on $\mathbb{Z}^n_{\geq 0}$, you can extend it to an order on monomials in $k[x_1,\ldots,x_n]$ by defining $x^\alpha > x^\beta$ if and only if $\alpha > \beta$.

Consider the total order $>_{\mathrm{evn}}$ on $\mathbb{Z}_{\geq 0}$ given by:

$$a >_{\mathrm{evn}} b \text{ if and only if } \begin{cases} \text{both } a \text{ and } b \text{ are even and } a > b \text{ under the usual ordering;} \\ \text{or both } a \text{ and } b \text{ are odd and } a > b \text{ under the usual ordering;} \\ \text{or } a \text{ is even and } b \text{ is odd.} \end{cases}$$

This ordering ranks the even numbers higher than the odd numbers, so that $1 <_{\mathrm{evn}} 3 <_{\mathrm{evn}} 5 <_{\mathrm{evn}} \ldots <_{\mathrm{evn}} 0 <_{\mathrm{evn}} 2 <_{\mathrm{evn}} 4 <_{\mathrm{evn}} \ldots$. It exhibits strange behaviour under addition. For example, $4 >_{\mathrm{evn}} 3$, but adding 1 to both sides flips the order: $4+1 = 5 <_{\mathrm{evn}} 4 = 3+1$. If we were to give $k[x]$ this ordering, we would find that $x^4 >_{\mathrm{evn}} x^3$, but multiplying both sides by x gives $x^5 <_{\mathrm{evn}} x^4$. In other words, multiplying or dividing by a common factor can change the order. This is undesirable; imagine trying to construct a Division Algorithm when the "greatest power of x" is constantly changing.

Hence we require that our monomial orderings remain unchanged under multiplication. In $\mathbb{Z}^2_{\geq 0}$, we require that if $\alpha,\beta,\gamma \in \mathbb{Z}^2_{\geq 0}$ are such that $\alpha > \beta$, then $\alpha+\gamma > \beta+\gamma$.

Definition 6.6. A *monomial ordering* on $k[x_a,\ldots,x_n]$ is a total order $>$ on $\mathbb{Z}^n_{\geq 0}$ satisfying:

(1) $>$ *respects addition*
If $\alpha,\beta,\gamma \in \mathbb{Z}^2_{\geq 0}$ are such that $\alpha > \beta$, then $\alpha+\gamma > \beta+\gamma$;

(2) $>$ *is well-ordered*
Every non-empty subset of $\mathbb{Z}^n_{\geq 0}$ has a smallest element under $>$.

We write $x^\alpha > x^\beta$ if and only if $\alpha > \beta$.

Proposition 6.7. *An order $>$ on $\mathbb{Z}^n_{\geq 0}$ is well-ordered if and only if every strictly decreasing sequence $\alpha_1 > \alpha_2 > \alpha_3 > \ldots$ in $\mathbb{Z}^n_{\geq 0}$ terminates.*

Proof. We prove the contrapositive: $>$ is not well-ordered if and only if there is an infinite strictly-decreasing sequence in $\mathbb{Z}^n_{\geq 0}$.

First assume that $>$ is not a well-ordering. Then there exists a non-empty subset S of $\mathbb{Z}^n_{\geq 0}$ with no smallest element under $>$. Pick any element α_1 in S. Then there must exist α_2 in S such that $\alpha_1 > \alpha_2$, since otherwise α_1 would be a smallest element in S. Proceeding in this fashion we may construct an infinitely long sequence $\alpha_1 > \alpha_2 > \alpha_3 > \ldots$.

Conversely suppose that $\alpha_1 > \alpha_2 > \alpha_3 > \ldots$ is an infinitely long strictly-decreasing sequence. Then the set of all α_i contains no smallest element under $>$, and we're done. □

Exercise 6.8. Read about *Noetherian rings* and the *chain conditions* in an introductory commutative algebra book.

Definition 6.9. Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. We write $\alpha >_{\text{lex}} \beta$ if the left-most non-zero entry of $\alpha - \beta$ is positive. We call $>_{\text{lex}}$ the *lexicographic order*.

Example 6.10. Lexicographic ordering is often compared with "dictionary ordering". We give a few examples:

(1) $(1, 2, 3) >_{\text{lex}} (0, 4, 5)$, or as monomials $x_1 x_2^2 x_3^3 >_{\text{lex}} x_2^4 x_3^5$;
(2) $(2, 2, 7) >_{\text{lex}} (2, 2, 3)$, or as monomials $x_1^2 x_2^2 x_3^7 >_{\text{lex}} x_1^2 x_2^2 x_3^3$;
(3) $(1, 1, 3, 0) >_{\text{lex}} (1, 1, 0, 7)$, or as monomials $x_1 x_2 x_3^3 >_{\text{lex}} x_1 x_2 x_4^7$.

Exercise 6.11. Prove that $>_{\text{lex}}$ gives a monomial ordering.

Remark 6.12. Notice that we have made a choice in our definition of lexicographic ordering, Namely, we have labelled the invariants $x_1, x_2, \ldots, x_n$, and decided that they should have priority in that order $(x_1 > x_2 > \ldots > x_n)$. Obviously any reordering of the x_i will give a different lexicographic ordering. There are $n!$ possible reorderings, and hence $n!$ choices of lexicographic ordering. Unless otherwise stated, it is always assumed that $x_1 > x_2 > \ldots > x_n$.

Definition 6.13. Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. We write $\alpha >_{\text{grlex}} \beta$ if $|\alpha| > |\beta|$ or if $|\alpha| = |\beta|$ and $\alpha >_{\text{lex}} \beta$. We call $>_{\text{grlex}}$ the *graded lexicographic order*.

Example 6.14. We give two examples:

(1) $(0, 4, 5) >_{\text{grlex}} (1, 2, 3)$ since $|(0, 4, 5)| > |(1, 2, 3)|$. Written as monomials we have that $x_2^4 x_3^5 >_{\text{grlex}} x_1 x_2^2 x_3^3$;
(2) $(1, 4, 4) >_{\text{grlex}} (1, 3, 5)$ since $|(1, 4, 4)| = |(1, 3, 5)|$ and $(1, 4, 4) >_{\text{lex}} (1, 3, 5)$. As monomials, $x_1 x_2^4 x_3^4 >_{\text{grlex}} x_1 x_2^3 x_3^5$.

Exercise 6.15. Prove that $>_{\text{grlex}}$ gives a monomial ordering.

Definition 6.16. Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. We write $\alpha >_{\text{grevlex}} \beta$ if $|\alpha| > |\beta|$ or if $|\alpha| = |\beta|$ and the *right-most* non-zero entry of $\alpha - \beta$ is *negative*. We call $>_{\text{grevlex}}$ the *graded reverse lexicographic order*.

Example 6.17. We give some examples:

(1) $(0,4,5) >_{\text{grevlex}} (1,2,3)$, or equivalently $x_2^4x_3^5; >_{\text{grevlex}} x_1x_2^2x_3^3$;
(2) $(1,4,4) >_{\text{grevlex}} (1,3,5)$, or equivalently $x_1x_2^4x_3^4 >_{\text{grevlex}} x_1x_2^3x_3^5$;
(3) $(0,2,2) >_{\text{grevlex}} (1,0,3)$, or equivalently $x_2^2x_3^2 >_{\text{grevlex}} x_1x_3^3$;
(4) $(1,4,1) >_{\text{grevlex}} (4,0,2)$, or equivalently $x_1x_2^4x_3 >_{\text{grevlex}} x_1^4x_3^2$.

Graded reverse lexicographic order can be confusing at first, however it has been shown to be more efficient for some computations that either the lexicographic order or the graded lexicographic order.

Example 6.18. We shall rewrite the polynomial $f = -2xy^2z^3 + 5y^2z^2 + y^4z^5 + 4xz^3 \in k[x,y,z]$ with the monomials in order: the "largest" monomial first, the "smallest" last.

(1) *Lexicographic order*
$f = -2xy^2z^3 + 4xz^3 + y^4z^5 + 5y^2z^2$
(2) *Graded lexicographic order*
$f = y^4z^5 - 2xy^2z^3 + 4xz^3 + 5y^2z^2$
(3) *Graded reverse lexicographic order*
$f = y^4z^5 - 2xy^2z^3 + 5y^2z^2 + 4xz^3$

A division algorithm.

Definition 6.19. Let $f = \sum a_\alpha x^\alpha \in k[x_1,\ldots,x_n]$ be a polynomial, and let $>$ be a monomial order.

(1) The *multidegree* of f is $\operatorname{multideg}(f) := \max\{\alpha \mid a_\alpha \neq 0\}$, where the maximum is taken with respect to $>$.
(2) The *leading coefficient* of f is $\mathrm{LC}(f) := a_{\operatorname{multideg}(f)}$.
(3) The *leading monomial* of f is $\mathrm{LM}(f) := x^{\operatorname{multideg}(f)}$.
(4) The *leading term* of f if $\mathrm{LT}(f) := \mathrm{LC}(f)\mathrm{LM}(f) = a_{\operatorname{multideg}(f)}x^{\operatorname{multideg}(f)}$.

Example 6.20. Let's consider f in Example 6.18. With respect to lexicographic order:

(1) $\operatorname{multideg}(f) = (1,2,3)$
(2) $\mathrm{LC}(f) = -2$
(3) $\mathrm{LM}(f) = xy^2z^3$
(4) $\mathrm{LT}(f) = -2xy^2z^3$.

Exercise 6.21. Repeat Example 6.20 using graded lexicographic order and using graded reverse lexicographic order.

Proposition 6.22 (Division Algorithm in $k[x_1, \dots, x_n]$)**.** *Let $>$ be a monomial order on $\mathbb{Z}^n_{\geq 0}$ and let $f_1, \dots, f_s \in k[x_1, \dots, x_n]$. Then every $f \in k]x_1, \dots .x_n]$ can be written in the form:*

$$f = a_1 f_1 + \ldots + a_s f_s + r,$$

where $a_i, r \in k[x_1, \dots, x_n]$ and either $r = 0$ or none of the monomials in r are divisible by any of $\mathrm{LT}(f_1), \dots, \mathrm{LT}(f_s)$*. If $a_i f_i \neq 0$ then* $\mathrm{multideg}(f) \geq \mathrm{multideg}(a_i f_i)$*.*

We call r a remainder *of f on division by $f_1, \dots, f_s$.*

Proof. See [CLO07, pp. 64–66] for the proof, which also describes the algorithm. □

Remark 6.23. Rather than dwell on the details, we shall understand the algorithm though Examples 6.24 and 6.25. "Running" the division algorithm is little more that performing glorified long division. The most difficult part is remembering to use whichever monomial order has been chosen.

Example 6.24. We shall divide $f = x^2z + z + y^3x - y^2 - x^4y$ by $f_1 = z - x^2y$ and $f_2 = xy - 1$.

Before we can do anything, we need to fix our monomial order. We shall use lexicographic order. Writing the monomials of f with the "largest" first and the "smallest" last we get $f = -x^4y + x^2z + xy^3 - y^2 + z$. Similarly for f_1 and f_2 we obtain $f_1 = -x^2y + z$ and $f_2 = xy - 1$.

Now we keep divide the leading term of our polynomial by the leading term of f_1, just like you do with ordinary long division. When this is no longer possible, move on to using f_2. We repeat this process until neither leading term $\mathrm{LT}(f_1)$ nor $\mathrm{LT}(f_2)$ will divide the leading term of our polynomial; we move this leading term to a remainder column, then try again. At each step we make sure that we keep track of whether we were working with f_1 or f_2. (This is all much simpler in practice than it sounds!)

Start by drawing a division table:

$$\begin{array}{r|lc}
\multicolumn{1}{r}{a_1 :} & & \\
\multicolumn{1}{r}{a_2 :} & & \underline{\;r\;} \\
\cline{2-2}
-x^2y + z & -x^4y + x^2z + xy^3 - y^2 + z & \\
xy - 1 & &
\end{array}$$

We use the a_1 and a_2 rows to keep track of whether we were dividing using f_1 or f_2. The r column is where we shall collect together our remainder.

$\mathrm{LT}(f_1) = -x^2y$, which divides $-x^4y$ (i.e. $x^2\mathrm{LT}(f_1) = -x^4y$). Writing the factor x^2 in the a_1 row, we obtain:

$$\begin{array}{rlcc}
a_1: & x^2 & & \\
a_2: & & & r \\ \cline{2-2} \cline{4-4}
-x^2y+z & \multicolumn{1}{|l}{-x^4y+x^2z+xy^3-y^2+z} & & \\
xy-1 & \multicolumn{1}{|l}{} & & \\
 & -x^4y+x^2z & & \\ \cline{2-2}
 & \multicolumn{1}{r}{xy^3-y^2+z} & &
\end{array}$$

Since $-x^2y$ does not divide the new leading term xy^3, we consider dividing by the leading term of f_2. We have that $y^2\mathrm{LT}(f_2) = xy^3$. We write y^2 in the a_2 row (since we're working with f_2).

$$\begin{array}{rlcc}
a_1: & x^2 & & \\
a_2: & y^2 & & r \\ \cline{2-2} \cline{4-4}
-x^2y+z & \multicolumn{1}{|l}{-x^4y+x^2z+xy^3-y^2+z} & & \\
xy-1 & \multicolumn{1}{|l}{} & & \\
 & -x^4y+x^2z & & \\ \cline{2-2}
 & \multicolumn{1}{r}{xy^3-y^2+z} & & \\
 & \multicolumn{1}{r}{xy^3-y^2\phantom{{}+z}} & & \\ \cline{2-2}
 & \multicolumn{1}{r}{z} & &
\end{array}$$

Neither $-x^2y$ nor xy divide z; we move z to the remainder column and we're finished.

$$\begin{array}{rlcc}
a_1: & x^2 & & \\
a_2: & y^2 & & r \\ \cline{2-2} \cline{4-4}
-x^2y+z & \multicolumn{1}{|l}{-x^4y+x^2z+xy^3-y^2+z} & & \\
xy-1 & \multicolumn{1}{|l}{} & & \\
 & -x^4y+x^2z & & \\ \cline{2-2}
 & \multicolumn{1}{r}{xy^3-y^2+z} & & \\
 & \multicolumn{1}{r}{xy^3-y^2\phantom{{}+z}} & & \\ \cline{2-2}
 & \multicolumn{1}{r}{z} & \longrightarrow & z \\ \cline{2-2}
 & \multicolumn{1}{r}{0} & &
\end{array}$$

We've found that $f = x^2(-x^2y+z) + y^2(xy-1) + z$.

One of the interesting things about this division algorithm is that the results we get depend on the order of the f_i. Let's repeat our calculation, but with $f_1 = xy - 1$ and

$f_2 = -x^2y + z$. We get:

$$
\begin{array}{r|r|cl}
\multicolumn{1}{r}{a_1 :} & \multicolumn{1}{l}{-x^3 + y^2} & & \\
\multicolumn{1}{r}{a_2 :} & \multicolumn{1}{l}{} & & \multicolumn{1}{c}{r} \\
\cline{2-2} \cline{4-4}
xy - 1 & \multicolumn{1}{l}{} & & \\
-x^2y + z & \multicolumn{1}{l}{-x^4y + x^2z + xy^3 - y^2 + z} & & \\
\multicolumn{1}{r}{} & \multicolumn{1}{l}{-x^4y + x^3} & & \\
\cline{2-2}
\multicolumn{1}{r}{} & \multicolumn{1}{r}{-\,x^3 + x^2z + xy^3 - y^2 + z} & \to & -x^3 \\
\cline{2-2}
\multicolumn{1}{r}{} & \multicolumn{1}{r}{x^2z + xy^3 - y^2 + z} & \to & -x^3 + x^2z \\
\cline{2-2}
\multicolumn{1}{r}{} & \multicolumn{1}{r}{xy^3 - y^2 + z} & & \\
\multicolumn{1}{r}{} & \multicolumn{1}{r}{xy^3 - y^2\phantom{{}+z}} & & \\
\cline{2-2}
\multicolumn{1}{r}{} & \multicolumn{1}{r}{z} & \to & -x^3 + x^2z + z \\
\cline{2-2}
\multicolumn{1}{r}{} & \multicolumn{1}{r}{0} & &
\end{array}
$$

This time we get a very different answer, namely that $f = (-x^3 + y^2)(xy - 1) + (-x^3 + x^2z + z)$.

Example 6.25. We return now to consider Exercise 3.30 (1). Let $f_1 = y - x^2$, $f_2 = z - x^3$, and $f = y^2 - xz$. If, after performing our division, we have remainder zero, then we know that $f = a_1f_1 + a_2f_2$; i.e. we know that $y^2 - xz \in (y - x^2, z - x^3)$.

Using lexicographic order, let's have a go. Remembering to reorder the monomials of our polynomials, we have:

$$
\begin{array}{r|c|cl}
\multicolumn{1}{r}{a_1 :} & \multicolumn{1}{c}{} & & \\
\multicolumn{1}{r}{a_2 :} & \multicolumn{1}{c}{} & & \multicolumn{1}{c}{r} \\
\cline{2-2} \cline{4-4}
-x^2 + y & \multicolumn{1}{l}{} & & \\
-x^3 + z & \multicolumn{1}{l}{-xz + y^2} & \to & -xz \\
\multicolumn{1}{r}{} & \multicolumn{1}{c}{y^2} & \to & -xz + y^2 \\
\multicolumn{1}{r}{} & \multicolumn{1}{c}{0} & &
\end{array}
$$

That wasn't very successful. If we exchange f_1 and f_2 nothing improves. How about using a different order? Try using graded lexicographic and graded reverse lexicographic. Still not much use. Perhaps the remainder is always non-zero, and $y^2 - xz \notin (y - x^2, z - x^3)$? Actually, no. Using lexicographic order but with $y > x > z$, we obtain (remembering to reorder the monomials):

$$
\begin{array}{rl|l}
 & a_1: & y + x^2 \\
 & a_2: & -x \qquad\qquad\qquad\qquad \underline{\;r\;} \\
\cline{3-3}
\multicolumn{2}{r|}{y - x^2} & \\
\multicolumn{2}{r|}{-x^3 + z} & y^2 - xz \\
\multicolumn{2}{r}{} & y^2 - yx^2 \\
\cline{3-3}
\multicolumn{2}{r}{} & \qquad yx^2 - xz \\
\multicolumn{2}{r}{} & \qquad yx^2 - x^4 \\
\cline{3-3}
\multicolumn{2}{r}{} & \qquad\qquad x^4 - xz \\
\multicolumn{2}{r}{} & \qquad\qquad x^4 - xz \\
\cline{3-3}
\multicolumn{2}{r}{} & \qquad\qquad\qquad\quad 0
\end{array}
$$

Success! We see that $y^2 - xz = (y + x^2)(y - x^2) - x(z - x^3)$. There is no remainder term, and so we can conclude that $y^2 - xz \in (y - x^2, z - x^3)$.

Example 6.26. We shall see how to use *Maple* to calculate the remainders in Exercise 6.25. First we need to tell Maple to use the Gröbner basis package:

```
with(Groebner);
```

To calculate the remainder for the first division, enter:

```
normalf(y^2-x*z,[y-x^2,z-x^3],plex(x,y,z));
```

This calculates the remainder when dividing $y^2 - xz$ by $y - x^2$ and $z - x^3$, using lexicographic order with $x > y > z$. You should get the answer $y^2 - xz$, as we did above. Now we repeat the calculation, but with the order $y > x > z$. Enter:

```
normalf(y^2-x*z,[y-x^2,z-x^3],plex(y,x,z));
```

This time the result is zero, as expected.

Remark 6.27. On the face of it, this division algorithm is far inferior to the division algorithm in one indeterminant. We can cope with the results not being unique (in fact there's very little that can done about this). But whether or not we have a remainder depends on the order we choose to perform our division with! How can this result be of much use? Let's see what we can salvage from this disaster.

7. The Hilbert Basis Theorem

We shall prove a remarkable result of Hilbert, mentioned in Remark 3.23; every ideal in a polynomial ring has a finite generating set. In the proof of this result we shall construct a particularly "nice" basis for our ideal, called a Gröbner basis. Before we do that, however, we need a result of Dickson[7] concerning monomials in ideals.

Monomial ideals.

Definition 7.1. Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. If there exists a subset $A \subset \mathbb{Z}^n_{\geq 0}$ (possibly infinite) such that I consists of all sums of the form $f = \sum_{\alpha \in A} h_\alpha x^\alpha$, where only finitely many of the $h_\alpha \in k[x_1, \ldots, x_n]$ are non-zero, then we call I a *monomial ideal*. We write $I = (x^\alpha \mid \alpha \in A)$.

Example 7.2. The ideal $(x + y, x) \subset k[x, y]$ is a monomial ideal with $A = \{(1, 0), (0, 1)\}$ (since $(x + y, x) = (x, y)$). The principal ideal $(x + y) \subset k[x, y]$ is not a monomial ideal.

Exercise 7.3. Let $I = (x^\alpha \mid \alpha \in A)$ be a monomial ideal. Show that if $x^\beta \in I$ is a monomial in I, then $x^\beta = x^\alpha \cdot x^\gamma$ for some $\alpha \in A, \gamma \in \mathbb{Z}^n_{\geq 0}$. In other words, we have that $\beta = \alpha + \gamma$. If you fix an α, then the set of all possible β such that x^α divides x^β is just $\left\{\alpha + \gamma \mid \gamma \in \mathbb{Z}^n_{\geq 0}\right\}$.

Example 7.4. Consider the ideal $I = (x^2y^5, x^4y^3, x^5y^2) \subset k[x, y]$. Clearly this is a monomial ideal, with $A = \{(2, 5), (4, 3), (5, 2)\} \subset \mathbb{Z}^2_{\geq 0}$. Consider the monomial $x^4y^6 \in I$. This is divisible by, for example, the monomial x^2y^5; we have $(4, 6) = (2, 5) + (2, 1)$. Alternatively, we have that $x^4y^6 = x^4y^3 \cdot y^3$, and so $(4, 6) = (4, 3) + (0, 3)$. This is illustrated in Figure 3; the shaded region indicates all the monomials in I. If we regard I as a vector space, then the monomials in the shaded region form a basis over k.

Theorem 7.5 (Dickson's Lemma)**.** *Let $I = (x^\alpha \mid \alpha \in A) \subset k[x_1, \ldots, x_n]$ be a monomial ideal. Then I is generated by only finitely many of the $\alpha \in A$.*

Remark 7.6. Figure 3 suggests a proof to Theorem 7.5. Projecting onto the "x-axis" we obtain the ideal $J = (x^2) \subset k[x]$. Looking "up" from x^2y^0 the first monomial in I that we see is x^2y^5. We now consider the five "horizontal strips" $J_0 = \{x^ay^0 \mid a > 2\}, \ldots, J_4 = \{x^ay^4 \mid a > 2\}$. In each case we look "along" the strip and make a note of the first monomial in I that we hit. So for the strips J_0 and J_1 we see nothing. For J_2 we see the monomial x^5y^2, for J_3 we see x^4y^3, and for J_4 we see x^4y^4. This collection of monomials generates I.

[7] For a brief biography of Dickson, see `http://www-groups.dcs.st-and.ac.uk/~history/Biographies/Dickson.html`.

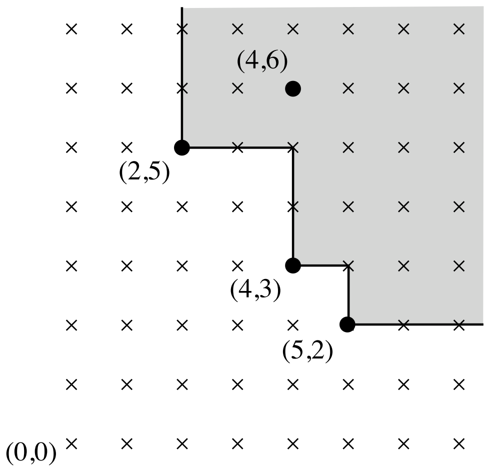

FIGURE 3. The monomials generated by x^2y^5, x^4y^3 and x^5y^2. The monomial x^4y^6 is indicated.

Proof of Theorem 7.5. We proceed by induction on n. If $n = 1$, let $\alpha \in A$ be the smallest element in A. Then $I = (x_1^\alpha)$.

Assume that $n > 1$, and that the result is true for $n-1$. For convenience we shall label the n indeterminants of the polynomial ring as $x_1, \ldots, x_{n-1}, y$. We can project any monomial $x_1^{a_1} \ldots x_{n-1}^{a_{n-1}} y^{a_n} = x^\alpha y^{a_n}$ in $k[x_1, \ldots, x_{n-1}, y]$ to a monomial x^α in $k[x_1, \ldots, x_{n-1}]$. Then

$$J = (x^\alpha \mid (\alpha, a_n) \in A, \text{ for some } a_n \in \mathbb{Z}_{\geq 0}) \subset k[x_1, \ldots, x_{n-1}]$$

is a monomial ideal. By the inductive hypothesis $J = (x^{\alpha_1}, \ldots, x^{\alpha_s})$, where each α_i is the projection of a point in A.

For each $i = 1, \ldots, s$ pick some $m_i \in \mathbb{Z}_{\geq 0}$ such that $x^{\alpha_i} y^{m_i} \in I$. Let $m = \max\{m_i \mid i = 1, \ldots, s\}$. For each $j = 0, \ldots, m$ we define the monomial ideal

$$J_j := (x^\beta \mid x^\beta y^j \in I) \subset k[x_1, \ldots, x_{n-1}].$$

Again by the inductive hypothesis, each J_j has a finite generating set of monomials. Say $J_j = (x^{\beta_{j,1}}, \ldots, x^{\beta_{j,s_j}})$.

Claim. I is generated by the following monomials:

$$\begin{array}{l} x^{\alpha_1} y^m, \ldots, x^{\alpha_s} y^m, \\ x^{\beta_{0,1}}, \ldots, x^{\beta_{0,s_0}}, \\ x^{\beta_{1,1}} y, \ldots, x^{\beta_{1,s_1}} y, \\ \qquad \vdots \\ x^{\beta_{m-1,1}} y^{m-1}, \ldots, x^{\beta_{m-1,s_{m-1}}} y^{m-1}. \end{array}$$

Clearly the above monomials all lie in I by construction. Conversely, it is enough to prove that every monomial in I is divisible by one of the monomials above (by Exercise 7.3). Let $x^\alpha y^p$ be any monomial in I. If $p \geq m$ then $x^\alpha y^p$ is divisible by $x^{\alpha_i} y^m$, for some $i = 1, \ldots, s$, by construction of J. If $p < m$ then $x^\alpha y^p$ is divisible by $x^{\beta_{p,i}} y^p$, for some $i = 1, \ldots, s_p$, by construction of J_p.

Finally it remains to show that a finite set of monomial generators for I can be chosen from A. Since each of the (finitely many) monomial generators above lies in I, by Exercise 7.3 each is divisible by some monomial $x_1^{a_1} \ldots x_{n-1}^{a_{n-1}} y^{a_n}$, where $(a_1, \ldots, a_{n-1}, a_n) \in A$. By taking those elements in A, we have our result. □

The Hilbert Basis Theorem.

Definition 7.7. Let $I \subset k[x_1, \ldots, x_n]$ be a non-zero ideal. By $\mathrm{LT}(I)$ we mean the set of leading terms of all polynomials in I (with respect to some monomial order). I.e.

$$\mathrm{LT}(I) := \{\mathrm{LT}(f) \mid f \in I\}.$$

By $(\mathrm{LT}(I))$ we mean the ideal generated by the set $\mathrm{LT}(I)$.

Remark 7.8. Given a finitely generated ideal $I = (f_1, \ldots, f_n)$, it is tempting to believe that the ideal generated by the leading terms of the f_i is equal to $(\mathrm{LT}(I))$; i.e. that $(\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_n)) = (\mathrm{LT}(I))$. Rather crucially for what's to follow, this is not generally the case.

For example, consider the ideal $I = (x + y, x) \subset k[x, y]$. Using lexicographic order, we have that $\mathrm{LT}(x + y) = \mathrm{LT}(x) = x$. Hence $(\mathrm{LT}(x + y), \mathrm{LT}(x)) = (x)$. Clearly $y \in I$, and so $y = \mathrm{LT}(y) \in (\mathrm{LT}(I)) \neq (x)$.

Theorem 7.9 (Hilbert Basis Theorem)**.** *Every ideal $I \subset k[x_1. \ldots, x_n]$ is finitely generated.*

Proof. If $I = \{0\}$ then we're done. Assume that $I \neq \{0\}$. Clearly the ideal $(\mathrm{LT}(I))$ is a monomial ideal, and so by Theorem 7.5 we have that there exists a finite generating set $f_1, \ldots, f_s \in I$ such that $(\mathrm{LT}(I)) = (\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s))$. We claim that $I = (f_1, \ldots, f_s)$.

Clearly $(f_1, \ldots, f_s) \subset I$. In the opposite direction, consider any $f \in I$. We can apply the Division Algorithm (Proposition 6.22) to obtain $f = a_1 f_1 + \ldots + a_s f_s + r$, where no term of r is divisible by any of $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$. Clearly $r \in I$, and if $r \neq 0$ then $\mathrm{LT}(r) \in (\mathrm{LT}(I)) = (\mathrm{LT}(f_1) \ldots, \mathrm{LT}(f_s))$. By Exercise 7.3 we have that $\mathrm{LT}(r)$ must be divisible by one of the $\mathrm{LT}(f_i)$. This is a contradiction. Hence $r = 0$ and so $f \in (f_1, \ldots, f_s)$. The result follows. □

8. Gröbner Bases and Buchberger's algorithm

In the proof of Theorem 7.9 we constructed a particularly useful basis for our ideal; a Gröbner basis. We now take the time to define this basis more formally, and to understand what properties it has that makes it so special. Finally, we shall look at Buchberger's algorithm for calculating a Gröbner basis.

Perhaps the most astonishing thing is how recent all these ideas are. Gröbner bases were first studied systematically by Bruno Buchberger[8] in 1965, whilst he was Gröbner's PhD student. He formalised the definition of Gröbner basis, defined the S-polynomial, discovered a result we now refer to as Buchberger's Criterion, and developed Buchberger's algorithm for finding Gröbner bases.

A Gröbner basis.

Definition 8.1. Let $I \subset k[x_1,\ldots,x_n]$ be an ideal, and fix a monomial order. A finite subset $\{g_1,\ldots,g_s\} \subset I$ such that $(\mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_s)) = (\mathrm{LT}(I))$ is said to be a *Gröbner basis* of I.

Remark 8.2. It follows from Exercise 7.3 that $\{g_1,\ldots,g_s\}$ is a Gröbner basis of I if and only if the leading term of any element in I is divisible by one of the $\mathrm{LT}(g_i)$.

We saw in the proof of Theorem 7.9 that every non-zero ideal $I \subset k[x_1,\ldots,x_n]$ has a Gröbner basis, and that a Gröbner basis for I is a basis for I. I.e. if $(\mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_s)) = (\mathrm{LT}(I))$ then $(g_1,\ldots,g_s) = I$.

Proposition 8.3. *Let $G = \{g_1,\ldots,g_s\}$ be a Gröbner basis for a non-zero ideal $I \subset k[x_1,\ldots,x_n]$. Let $f \in k[x_1,\ldots,x_n]$. Then there exists a unique $r \in k[x_1,\ldots,x_n]$ such that:*

1. *No term of r is divisible by one of* $\mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_s)$*;*
2. *There exists a $g \in I$ such that $f = g + r$.*

In particular, r is the remainder on division of f by G no matter the order in which we list the elements of G when running the division algorithm.

Proof. To prove existence is easy. By the division algorithm we have that $f = a_1g_1 + \ldots + a_sg_s + r$, where r satisfies (1). The second condition is satisfied by simply setting $g = a_1g_1 + \ldots + a_sg_s$. To prove uniqueness, suppose that $f = g + r = g' + r'$. Then $r - r' = g' - g \in I$ and so if $r \neq r'$ then $\mathrm{LT}(r - r') \in (\mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_s))$. Hence $\mathrm{LT}(r - r')$ is divisible by $\mathrm{LT}(g_i)$ for some $1 \leq i \leq s$. But since no term of either r or

[8] If you're interested, Buchberger's website is at:
`http://www.risc.uni-linz.ac.at/people/buchberg/`.

r' is divisible by $\mathrm{LT}(g_i)$, this is a contradiction (you should prove why this is so). Hence $r - r' = 0$ and uniqueness follows. □

Corollary 8.4. *Let $I \subset k[x_1, \ldots, x_n]$ be a non-zero ideal, and let G be a Gröbner basis for I. Let $f \in k[x_1, \ldots, x_n]$. Then $f \in I$ if and only if the remainder on division of f by G is zero.*

Proof. If the remainder is zero then we have that $f \in I$ (recall that we used this fact in Example 6.25). Conversely given $f \in I$ then $f = f + 0$ satisfies the two conditions of Proposition 8.3. By uniqueness it follows that 0 is the remainder upon division by G. □

Remark 8.5. This is rather remarkable. Gröbner bases address the main disappointment we had with the division algorithm (Remark 6.27). It should be emphasised that the quotients a_i produced by the division algorithm are *not unique*, even when dividing by a Gröbner basis. But this really doesn't matter much.

Thus, given a non-zero ideal I and a Gröbner basis G for I, we can now determine whether an arbitrary polynomial f is a member of I or not. What we need to know now is how to find a Gröbner basis. In otherwords, given that $(f_1, \ldots, f_s) = I$, how do we decide whether $\{f_1, \ldots, f_s\}$ is a Gröbner basis for I? If it isn't a Gröbner basis, is there anything we can do to transform it into one?

Definition 8.6. Let $x^\alpha, x^\beta \in k[x_1, \ldots, x_n]$ be two monomials. If $\alpha = (a_1, \ldots, a_n) \in \mathbb{Z}^n_{\geq 0}$ and $\beta = (b_1, \ldots, b_n) \in \mathbb{Z}^n_{\geq 0}$, then let $\gamma = (c_1, \ldots, c_n) \in \mathbb{Z}^n_{\geq 0}$ be such that $c_i = \max\{a_i, b_i\}$ for $i = 1, \ldots, n$. We call x^γ the *least common multiple* of x^α and x^β, and write $x^\gamma = \mathrm{lcm}\{x^\alpha, x^\beta\}$.

Definition 8.7. Let $f, g \in k[x_1, \ldots, x_n]$ be non-zero polynomials and fix a monomial order. The *S-polynomial* of f and g is:

$$\mathrm{S}(f, g) := \frac{x^\gamma}{\mathrm{LT}(f)} \cdot f - \frac{x^\gamma}{\mathrm{LT}(G)} \cdot g,$$

where $x^\gamma = \mathrm{lcm}\{\mathrm{LM}(f), \mathrm{LM}(g)\}$.

Example 8.8. The purpose of the S-polynomial is to cancel out the leading terms of the two polynomials f and g. For example, if $f = z - x^2 z$ and $g = xy - 1$, then using lexicographic order we have $\mathrm{LT}(f) = -x^2 z$ and $\mathrm{LT}(g) = xy$. We obtain $\mathrm{lcm}\{\mathrm{LM}(f), \mathrm{LM}(g)\} = x^2 yz$, and so:

$$\begin{aligned}S(f,g) &= \frac{x^2yz}{-x^2z}\cdot f - \frac{x^2yz}{xy}\cdot g\\ &= (-y)(z - x^2z) - (xz)(xy-1)\\ &= -yz + x^2yz - x^2yz + xz\\ &= xz - yz.\end{aligned}$$

Maple can calculate the S-polynomial for you. Make sure that the Gröbner basis package is loaded, then type:

```
spoly(z-x^2*z,x*y-1,plex(x,y,z));
```

This instructs it to calculate the S-polynomial, using lexicographic order with $x > y > z$.

Theorem 8.9 (Buchberger's Criterion). *Let $I \subset k[x_1, \ldots, x_n]$ be a non-zero ideal, and fix a monomial order. A basis $G = \{g_1, \ldots, g_s\}$ for I is a Gröbner basis if and only if for all pairs $i \neq j$ the remainder on division of $S(g_i, g_j)$ by G (listed in some order) is zero.*

Proof. See [CLO07, pp. 85–87]. □

Example 8.10. We return to Example 6.25. Recall that in order to deduce that $y^2 - xz \in (y - x^2, z - x^3)$ was true, we had to use the lexicographic order with $y > x > z$. We shall use Theorem 8.9 so show that, under this order, $\{y - x^2, z - x^3\}$ is a Gröbner basis.

First we need to calculate $S(y - x^2, z - x^3)$. We obtain (remember our slightly unusual order):

$$\begin{aligned}S(y - x^2, z - x^3) &= \frac{yx^3}{y}\cdot(y - x^2) - \frac{yx^3}{-x^3}\cdot(z - x^3)\\ &= (x^3)(y - x^2) - (-y)(z - x^3)\\ &= yz - x^5.\end{aligned}$$

Now we need to calculate the remainder of $yz - x^5$ when divided by $y - x^2$ and $z - x^3$ (the order we list them in doesn't make any difference). We have:

$$\begin{array}{rlc}
a_1: & z & \\
a_2: & x^2 & r \\
\cline{2-2}\cline{3-3}
y - x^2 & \multicolumn{1}{|l}{yz - x^5} & \\
-x^3 + z & \multicolumn{1}{|l}{} & \\
 & yz - x^2z & \\
\cline{2-2}
 & \quad - x^5 + x^2z & \\
 & \quad - x^5 + x^2z & \\
\cline{2-2}
 & \qquad\qquad 0 &
\end{array}$$

Since the remainder is zero, we see that $\{y - x^2, z - x^3\}$ is a Gröbner basis for $(y-x^2, z-x^3)$ (under lexicographic order with $y > x > z$).

Knowing this completely answers the ideal membership problem for $(y - x^2, z - x^3)$. Given any polynomial $f \in k[x, y, z]$ we can determine whether $f \in (y-x^2, z-x^3)$ simply by determining whether the remainder is zero upon division by $\{y - x^2, z - x^3\}$ using lexicographic order with $y > x > z$.

Remark 8.11. In *Maple*, combining the `spoly()` and `normalf()` commands will allow you to verify the calculation in the previous example. Simply enter:

```
normalf(spoly(y-x^2,z-x^3,plex(y,x,z)),[y-x^2,z-x^3],plex(y,x,z));
```

You get remainder zero, as expected. If you get nonsensical output, remember that you must load the Gröbner basis package first: `with(Groebner);`

Buchberger's algorithm.

Definition 8.12. Let $F = \{f_1, \ldots, f_s\} \subset k[x_1, \ldots, x_n]$, where the order of the f_i is fixed (i.e. F is an s-tuple). Fix a monomial order, and let $f \in k[x_1, \ldots, x_n]$. We write $\overline{f}^F$ for the remainder on division by F of f. (Note that if F is a Gröbner basis then the order of the f_i doesn't matter, by Proposition 8.3.)

Example 8.13. Let us return to Example 6.24. Recall that $f = x^2z + z + y^3x - y^2 - x^4y$, $f_1 = z - x^2y$, and $f_2 = xy - 1$. Using lexicographic order, we have that:

$$\overline{f}^{f_1,f_2} = z, \qquad \overline{f}^{f_2,f_1} = -x^3 + x^2z + z.$$

Observe that, since the remainder depends on the order of f_1 and f_2 when running the division algorithm, $\{f_1, f_2\}$ cannot be a Gröbner basis. The power of Theorem 8.9 is not necessarily that it tells us when a basis is *not* a Gröbner basis, more that it tells is when it *is*.

Remark 8.14. Looking at Theorem 8.9 suggests a strategy for converting an arbitrary basis G into a Gröbner basis. Calculate $\overline{S(f, g)}^G$ for every pair $f, g \in G$. Whenever you have a non-zero remainder, add that remainder to your basis. Keep repeating until all the remainders are zero. The resulting basis must be a Gröbner basis by Theorem 8.9.

Theorem 8.15 (Buchberger's algorithm). *Let $I = (f_1, \ldots, f_s) \subset k[x_1, \ldots, x_n]$ be a non-zero ideal. The basis $G_0 = \{f_1, \ldots, f_s\}$ for I can be transformed into a Gröbner basis in finitely many steps. At each step the old basis G_m is transformed into a new basis G_{m+1} by adding in new elements given by all non-zero $\overline{S(f_i, f_j)}^{G_m}$, where $f_i, f_j \in G_m$. When $G_m = G_{m+1}$ we have that G_m is a Gröbner basis for I.*

Proof. Clearly at each step G_{m+1} is still a basis for I, since $G_0 \subset G_{m+1}$ and $\overline{S(f_i, f_j)}^{G_m} \in I$ (since $S(f_i, f_j) \in I$, and the remainder upon division by elements in I of an element in I lies in I). Assuming that the process described in the statement terminates, the resulting basis must be a Gröbner basis by Theorem 8.9.

We now prove that the process terminates. First note that at each step, if $G_m \neq G_{m+1}$ then the inclusion $(\mathrm{LT}(G_m)) \subset (\mathrm{LT}(G_{m+1}))$ is strict; i.e. we have that $(\mathrm{LT}(G_m)) \neq (\mathrm{LT}(G_{m+1}))$. This is because some non-zero remainder $r = \overline{S(f_i, f_j)}^{G_m}$ has been added to G_{m+1}. By the Division Algorithm (Proposition 6.22) no leading term of G_m divides r, and hence (by Exercise 7.3) $\mathrm{LT}(r) \notin (\mathrm{LT}(G_m))$. But $\mathrm{LT}(r) \in (\mathrm{LT}(G_{m+1}))$ by definition of G_{m+1}, hence we have that $(\mathrm{LT}(G_m)) \neq (\mathrm{LT}(G_{m+1}))$.

Assume for a contradiction that the process does not terminate. Then we have an infinite strictly increasing chain of ideals:

$$(\mathrm{LT}(G_0)) \subsetneqq (\mathrm{LT}(G_1)) \subsetneqq \ldots \subsetneqq (\mathrm{LT}(G_m)) \subsetneqq (\mathrm{LT}(G_{m+1})) \subsetneqq \ldots.$$

Let $G = \bigcup_{m=0}^{\infty}(\mathrm{LT}(G_m))$ be the set given by taking the union of all the ideals. Then $(\mathrm{LT}(G_m)) \subset G$ for all m. It can be seen that G is an ideal in $k[x_1, \ldots, x_n]$ (you should prove this). By Theorem 7.9 there exists a finite basis $G = (g_1, \ldots, g_l)$. Each of the generators must come from some G_m; say $g_i \in (\mathrm{LT}(G_{m_i}))$ for some m_i. Take the maximum $M := \max\{m_i \mid i = 1, \ldots, l\}$. Then $g_i \in (\mathrm{LT}(G_M))$ for $i = 0, \ldots, l$. Hence:

$$G \subset (\mathrm{LT}(G_M)) \subsetneqq (\mathrm{LT}(G_{M+1})) \subsetneqq (\mathrm{LT}(G_{M+2})) \subsetneqq \ldots.$$

But this contradicts the fact that $(\mathrm{LT}(G_m)) \subset G$ for all m. Hence the process must terminate. □

Remark 8.16. The technique used in the proof of Theorem 8.15 – that no infinite strictly increasing chain of ideals exists – is referred to as the *ascending chain condition.* You should look it up in a commutative algebra book.

Example 8.17. Let us find a Gröbner basis for the ideal $(z - x^2z, xy - 1) \subset k[x, y, z]$ using lexicographic order. We start by setting

$$G_0 := \left\{z - x^2z, xy - 1\right\}.$$

We saw in Example 8.8 that $S(z - x^2z, xy - 1) = xz - yz$. Running the division algorithm we see that $\overline{S(z - x^2z, xy - 1)}^{G_0} = xz - yz$. Hence

$$G_1 := \left\{z - x^2z, xy - 1, xz - yz\right\}.$$

We now need to calculate

$$\overline{S(z - x^2z, xy - 1)}^{G_1}, \overline{S(z - x^2z, xz - yz)}^{G_1}, \text{and } \overline{S(xz - yz, xy - 1)}^{G_1}.$$

Of course, we don't actually need to compute the first of those three calculations, since by construction of G_1 the remainder will be zero. For the other two, we find that

$$\overline{S(z-x^2z, xz-yz)}^{G_1} = 0, \text{and } \overline{S(xz-yz, xy-1)}^{G_1} = z-y^2z.$$

Hence we consider:

$$G_2 := \left\{ z-x^2z, xy-1, xz-yz, z-y^2z \right\}.$$

This time there are six remainders to calculate, however we know by construction of G_2 that three of them are zero. We only need to compute:

$$\overline{S(z-x^2z, z-y^2z)}^{G_2}, \overline{S(xy-1, z-y^2z)}^{G_2}, \text{and } \overline{S(xz-yz, z-y^2z)}^{G_2}.$$

We find that the remainder in each case is zero. Hence G_2 is a Gröbner basis for I.

Recall the definition of a Gröbner basis $G = (g_1, \ldots, g_s)$ is that $(\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)) = (\mathrm{LT}(I))$. Looking at G_2 we see that the element $z - x^2z$ can be safely discarded, since $\mathrm{LT}(z-x^2z) = -x^2z = -x \cdot \mathrm{LT}(xz-yz)$. In other words

$$G_2' := \left\{ xy-1, xz-yz, z-y^2z \right\}$$

is still be a Gröbner basis for I.

In *Maple* make sure that Gröbner basis package is loaded, and type:

```
gbasis([z-x^2*z,x*y-1],plex(x,y,z));
```

This instructs Maple to calculate a Gröbner basis for the given basis, using lexicographic order with $x > y > z$. Observe that the answer Maple gives is (up to trivial changes of sign) equal to the basis G_2' found above.

Remark 8.18. Example 8.17 tells us a couple of important thing. First, given an ideal I and fixed monomial order, there may be more that one Gröbner basis. Second, a Gröbner basis may be made smaller by discarding those elements whose leading term contributes nothing.

Exercise 8.19. Let $G = \{g_1, \ldots, g_s\}$ be a Gröbner basis for the ideal $I \subset k[x_1, \ldots, x_n]$. Suppose that g_1 is such that $\mathrm{LT}(g_1) \in (\mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_s))$. Show that $G \setminus \{g_1\} = \{g_2, \ldots, g_s\}$ is also a Gröbner basis for I.

Definition 8.20. A Gröbner basis G for a polynomial I is said to be *minimal* if for all $g \in G$:

(1) $\mathrm{LC}(g) = 1$;
(2) $\mathrm{LT}(g) \notin (\mathrm{LT}(G \setminus \{g\}))$.

Remark 8.21. This first condition of Definition 8.20 is simply that we multiply the elements of our Gröbner basis so that the leading coefficient is always one. This is a perfectly sensible thing to do. The second condition is precisely what we discussed in the previous remark. From Example 8.17 we see that the set $\{xy-1, xz-yz, y^2z-z\}$ is a minimal Gröbner basis for $(z-x^2z, xy-1)$.

Exercise 8.22. Let $I \subset k[x_1,\ldots,x_n]$ be an ideal, and fix a monomial order. Show that if G and G' are two minimal Gröbner bases for I then $\mathrm{LT}(G) = \mathrm{LT}(G')$. Hence G and G' contain the same number of elements.

Remark 8.23. Unfortunately there is not a unique minimal Gröbner basis. Looking once again at Example 8.17 we see that any

$$\left\{xy + c(xz-yz) - 1, xz-yz, y^2-z\right\}, \qquad c \in \mathbb{Z}$$

gives us a minimal Gröbner basis for $(z-x^2z, xy-1)$. But this construction is something of a cheat – all we're doing is adding in monomials which already lie in $(\mathrm{LT}(G))$ in such a way that the leading terms remain unchanged. To prohibit this trick, we make the following definition.

Definition 8.24. A Gröbner basis G for a polynomial I is said to be *reduced* if for all $g \in G$:

(1) $\mathrm{LC}(g) = 1$;
(2) No monomial of g lies in $(\mathrm{LT}(G \setminus \{g\}))$.

Theorem 8.25. *Let $I \subset k[x_1,\ldots,x_n]$ be a non-zero ideal. For a given monomial order, a reduced Gröbner basis of I exists and is unique.*

Proof. Let G be a minimal Gröbner basis for I. We shall call $g \in G$ *reduced* if no monomial of g lies in $(\mathrm{LT}(G) \setminus \{g\})$. Clearly if g is reduced in G then g is reduced in any other minimal Gröbner basis also containing g (by Exercise 8.22). Furthermore, if all $g \in G$ are reduced, then G is reduced.

Given $g \in G$, let $g' = \overline{g}^{G\setminus\{g\}}$ and let $G' = (G \setminus g) \cup \{g'\}$. We claim that G' is also a minimal Gröbner basis for I. To see this note that $\mathrm{LT}(g) = \mathrm{LT}(g')$, since by Definition 8.20 the leading term of g is not divisible by any element in $G\setminus\{g\}$. Hence $(\mathrm{LT}(G')) = (\mathrm{LT}(G))$ and so G' is a Gröbner basis for I. Since G was minimal we see that G' is also minimal.

Take the elements in G and repeatedly apply the above process until they are all reduced. Notice that since the leading terms remain unchanged, this procedure is guaranteed to terminate. We end up with a reduced Gröbner basis for I. This proves existence.

Finally, we shall show uniqueness. Suppose that G and G' are two reduced Gröbner bases for I. Given any $g \in G$, by Exercise 8.22 there exists some $g' \in G'$ such that $\mathrm{LT}(g) = \mathrm{LT}(g')$. To prove uniqueness it is sufficient to show that $g = g'$.

Consider the difference $g - g'$. Since $\mathrm{LT}(g) = \mathrm{LT}(g')$ the leading terms cancel in $g - g'$, and the remaining terms are not divisible by any of the $\mathrm{LT}(G) = \mathrm{LT}(G')$ since G and G' are reduced. Hence $\overline{g - g'}^{G} = g - g'$. But $g - g' \in I$ and so (by Corollary 8.4) $\overline{g - g'}^{G} = 0$. Hence $g = g'$. □

Remark 8.26. The Gröbner basis returned by *Maple*'s `gbasis()` command is *the* reduced Gröbner basis.

Exercise 8.27. Prove that two non-zero ideals $(f_1, \ldots, f_s)$ and $(g_1, \ldots, g_m)$ in $k[x_1, \ldots, x_n]$ are equal if and only if they have the same reduced Gröbner basis (for some fixed monomial order).

Exercise 8.28. The proof of Theorem 8.25 is essentially an algorithm for converting a minimal Gröbner basis into the reduced Gröbner basis. Translate this algorithm into a *Maple* program.

9. Elimination theory

After all this hard work, we find that Gröbner bases more than repay the effort. Gröbner bases provide us with a systematic way of eliminating variables from a system of equations. We'll prove that this is the case, but you can start experimenting with examples straight away[9].

Examples.

Example 9.1. Consider the three polynomials in $\mathbb{R}[x, y, z]$:

$$\begin{aligned} x^2 + y^2 &= 1 \\ x^2 + y^2 + z^2 &= 2 \\ x + y + z &= 1 \end{aligned} \tag{9.1}$$

We're interested in finding the values of x, y, and z which satisfy all three equations. In other words, we wish to understand the affine variety $\mathbb{V}(x^2 + y^2 - 1, x^2 + y^2 + z^2 - 2, x + y + z - 1)$ (see Figure 4).

[9] All the examples in this section can be solved using elementary manipulation of the equations; the advantage of using Gröbner bases is that the method is the same no matter how difficult the example.

Let $I = (x^2+y^2-1, x^2+y^2+z^2-2, x+y+z-1)$ be the ideal generated by the three equations, and let $G = \{g_1, \ldots, g_s\}$ be a Gröbner basis for I. Then $I = (g_1, \ldots, g_s)$. By Exercise 4.14 we know that:

$$\mathbb{V}(x^2+y^2-1, x^2+y^2+z^2-2, x+y+z-1) = \mathbb{V}(g_1, \ldots, g_s).$$

In other words, replacing the equations in (9.1) with the equations for a Gröbner basis, we'll get the same set of solutions.

Why does this help? Using lexicographic order, we obtain the (reduced) Gröbner basis:

$$G = \left\{z^2-1, 2y^2+2zy-2y-2z+1, x+y+z-1\right\}.$$

Notice that the first equation only involves z, and that the second equation only involves y and z. This means that we can use the first equation to solve for z, then use those results and the second equation to solve for y, and finally the third equation to solve for x. We shall work over $\mathbb{R}$, although the principal is the same over an arbitrary field k.

From $z^2-1=0$ we have that $z = \pm 1$. Let's take $z=-1$ first. Then $2y^2+2zy-2y-2z+1=0$ reduces to $2y^2-4y+3=0$, which can be seen to have no solutions in $\mathbb{R}$. Taking $z=1$ we see that the second equation reduces to $2y^2-1=0$, with solutions $y = \pm 1/\sqrt{2}$. Finally the third equation $x+y+z=1$ immediately gives that $x = \mp 1/\sqrt{2}$.

Thus, with very little effort, we have found that there are exactly two solutions to (9.1), namely:

$$\left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}, 1\right) \text{ and } \left(-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 1\right).$$

Example 9.2. Let's do another example. This time we'll consider the two polynomials:

$$\begin{aligned} y &= -\frac{1}{x} \\ z &= -\frac{1}{x^2} \end{aligned} \tag{9.2}$$

Since we have two equations in $\mathbb{R}^3$, we expect their intersection to be a curve. The polynomials are graphed in Figure 5. The common zeros are described by the variety $\mathbb{V}(xy+1, x^2z+1)$.

A (reduced) Gröbner basis for the ideal $(xy+1, x^2z+1) \subset \mathbb{R}[x,y,z]$ is given by $G = \{z+y^2, xz-y, xy+1\}$. By Exercise 4.14 we have that $\mathbb{V}(xy+1, x^2z+1) = \mathbb{V}(z+y^2, xz-y, xy+1)$.

Once again the equations of the Gröbner basis are easy to solve. The first equation tells us that $z=-y^2$ and the second equation that $x=-1/y$. In this case the third equation is redundant. We see that the intersection is a curve, paramaterised by $(-1/t, t, -t^2)$, where $t \in \mathbb{R} \setminus \{0\}$. This curve is plotted in Figure 6.

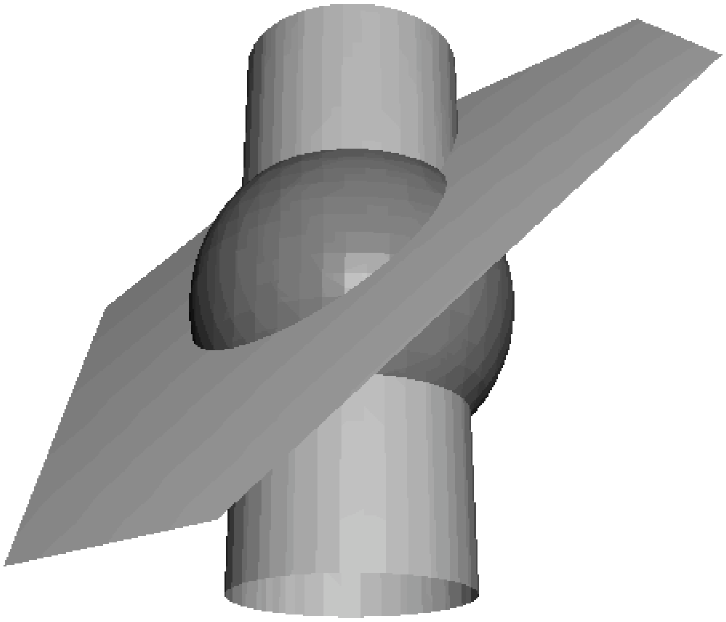

Figure 4. What is the intersection of the cylinder $x^2 + y^2 = 1$, the sphere $x^2 + y^2 + z^2 = 2$, and the plane $x + y + z = 1$?

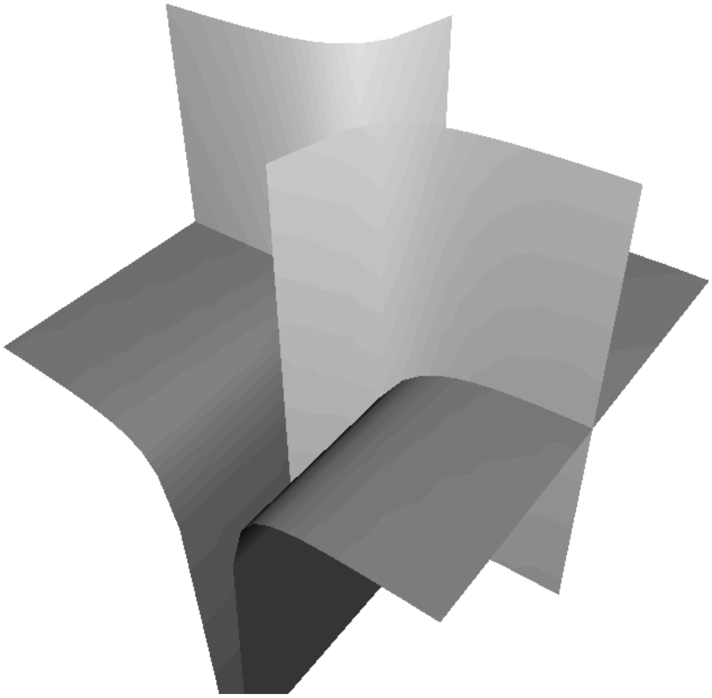

Figure 5. Two surfaces given by $y = -1/x$ and $z = -1/x^2$.

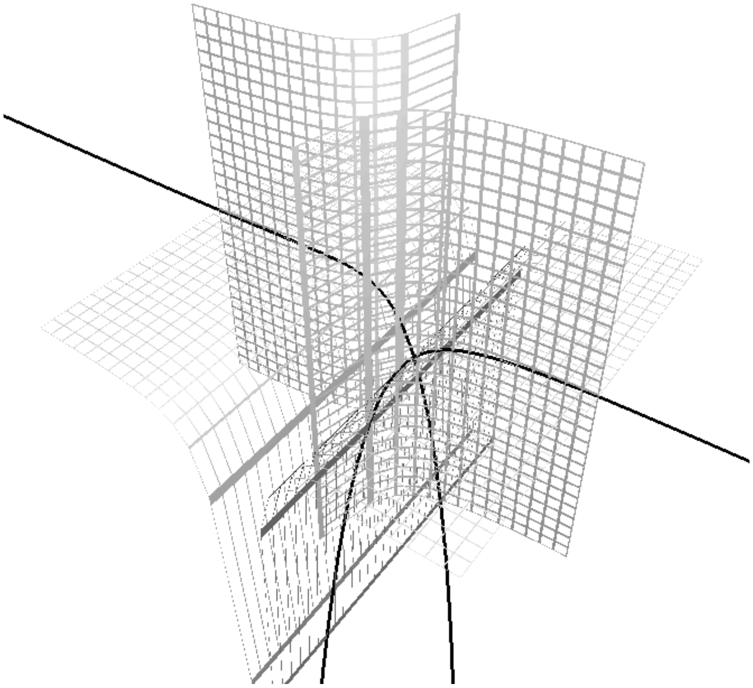

FIGURE 6. The intersection of the two surfaces is given by $(-1/t, t, -t^2)$.

Example 9.3. Consider the polynomial $f(x,y) = ((x-1)^2 + y^2)((x+1)^2 + y^2) \in \mathbb{R}[x,y]$. We're interested in finding values for a constant $c \in \mathbb{R}$ for which the curve $f(x,y) = c$ is particularly interesting. By interesting, we mean that the curve has a *singular point* defined by the vanishing of the partial derivatives[10] $\partial f/\partial x$ and $\partial f/\partial y$.

In other words, we want to find solutions to the polynomials:

$$\begin{aligned} ((x-1)^2 + y^2)((x+1)^2 + y^2) &= c \\ 2(x-1)((1+x)^2 + y^2) + 2(x+1)((x-1)^2 + y^2) &= 0 \\ 2y((1+x)^2 + y^2) + 2y((x-1)^2 + y^2) &= 0 \end{aligned} \tag{9.3}$$

(Here the second and third equations are $\partial f/\partial x$ and $\partial f/\partial y$ respectively.)

We can regard these polynomials as equations in $\mathbb{R}[x,y,c]$. A Gröbner basis (using lexicographic order with $x > y > c$) for the resulting ideal is given by:

$$G = \left\{c^2 - c, cy, y^3 + y, cx, xy, x^2 - y^2 + c - 1\right\}.$$

In other words, we have that:

$$\mathbb{V}\left(f(x,y) - c, \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right) = \mathbb{V}(c^2 - c, cy, y^3 + y, cx, xy, x^2 - y^2 + c - 1).$$

[10] To explain this definition, see [CLO07, pp. 138–141]. Consult [Kir92] for more information about singularities on curves.

The first equation of G tells us that $c = 0$ or $c = 1$. All we are interested in are possible values for c; the two curves we obtain are given in FIgure 7. When $c = 0$ we have just the two points $(-1, 0)$ and $(1, 0)$. The case when $c = 1$ is much more interesting; the singular point is located at the origin. This curve is called a *lemniscate*.

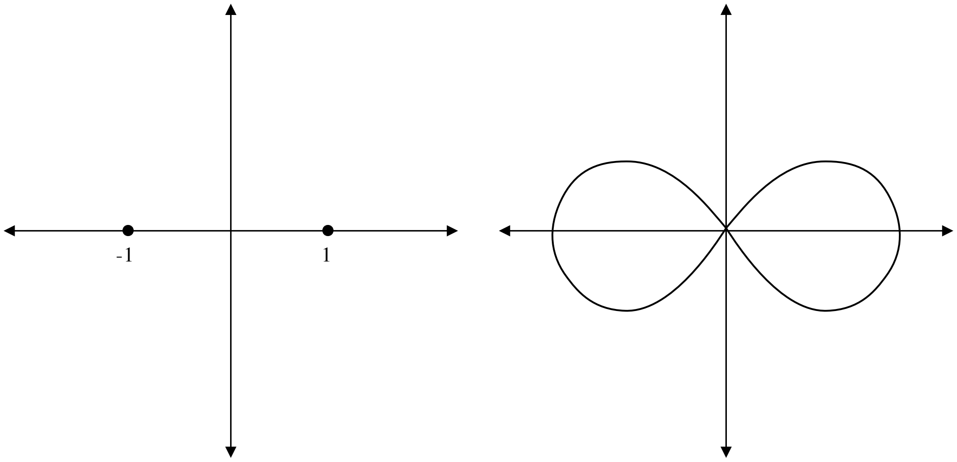

FIGURE 7. The curves when $c = 0$ and when $c = 1$.

Elimination and extension.

Definition 9.4. Let $I = (f_1, \ldots, f_s) \subset k[x_1, \ldots, x_n]$ be an ideal. The l^{th} *elimination ideal* of I is given by $I_l := I \cap k[x_{l+1}, \ldots, x_n]$.

Remark 9.5. You should prove that I_l really is an ideal in $k[x_{l+1}, \ldots, x_n]$.

Theorem 9.6 (The Elimination Theorem)**.** *Let $I \subset k[x_1, \ldots, x_n]$ be an ideal, and let G be a Gröbner basis for I with respect to lexicographic order where $x_1 > \ldots > x_n$. Then, for each $0 \leq l < n$, $G_l := G \cap k[x_{l+1}, \ldots, x_n]$ is a Gröbner basis for I_l.*

Proof. Fix l. By Definition 8.1 we need to show that $(\mathrm{LT}(I_l)) = (\mathrm{LT}(G_l))$. Since $G_l \subset I_l$ by construction, we have that $(\mathrm{LT}(G_l)) \subset (\mathrm{LT}(I_l))$. To prove the other inclusion, we will show that for an arbitrary $f \in I_l$, $\mathrm{LT}(f)$ is divisible by $\mathrm{LT}(g)$ for some $g \in G_l$.

Since $f \in I$ we have that $\mathrm{LT}(f)$ is divisible by $\mathrm{LT}(g)$ for some $g \in G$. But $f \in I_l$, and so $\mathrm{LT}(f)$ involves only the indeterminates $x_{l+1}, \ldots, x_n$. Under our monomial order, any monomial involving $x_1, \ldots, x_l$ is strictly greater than all monomials in $k[x_{l+1}, \ldots, x_n]$. Hence g must lie in $k[x_{l+1}, \ldots, x_n]$ and so $g \in G_l$. □

Remark 9.7. Theorem 9.6 tells us that the nice properties of Gröbner bases that we exploited in the previous examples is not a coincidence. A Gröbner basis for lexicographic order eliminates the first indeterminate, the first two indeterminates, the first three indeterminates, etc.

Definition 9.8. Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. A point $(a_{l+1}, \ldots, a_n) \in \mathbb{V}(I_l) \subset \mathbb{R}^{n-l}$ is called a *partial solution* of $\mathbb{V}(I)$.

Remark 9.9. Consider the examples above. We can describe the method used in terms of partial solutions. Start by finding all partial solutions $(a_n) \in \mathbb{V}(I_{n-1})$. Then extend this partial solution to a partial solution in $\mathbb{V}(I_{n-2})$ as follows. Suppose that $G_{n-2} = \{g_1, \ldots, g_s\} \subset k[x_{n-1}, x_n]$ is a Gröbner basis for I_{n-2}. Substitute $x_n = a_n$ into the equations of G_{n-2} and solve:

$$\begin{aligned} g_1(x_{n-1}, a_n) &= 0, \\ &\vdots \\ g_s(x_{n-1}, a_n) &= 0. \end{aligned}$$

This gives us $\mathbb{V}(I_{n-2})$. Take each partial solution $(a_{n-1}, a_n) \in \mathbb{V}(I_{n-2})$, substitute $x_{n-1} = a_{n-1}, x_n = a_n$ into G_{n-3}, and solve for x_{n-2} to get $\mathbb{V}(I_{n-3})$. Etc.

We saw in the first example that a partial solution in $\mathbb{V}(I_{i+1})$ need not extend to a partial solution in $\mathbb{V}(I_i)$. Namely, we found from the equation $z^2 - 1 = 0$ that $\mathbb{V}(I_2) = \{-1, 1\} \subset \mathbb{R}$, but that only $z = 1$ gave a solution to the equation $2y^2 + 2zy - 2y - 2z + 0$. In other words, $\mathbb{V}(I_1) = \left\{(-1/\sqrt{2}, 1), (1/\sqrt{2}, 1)\right\} \subset \mathbb{R}^2$ does not use the partial solution $z = -1$.

It would be nice to know when a partial solution in $\mathbb{V}(I_{i+1})$ can be extended to a partial solution in $\mathbb{V}(I_i)$. Theorem 9.10 answers this when the field is $\mathbb{C}$ (in fact any algebraically closed field will do) for $\mathbb{V}(I_1)$ and $\mathbb{V}(I_0) = \mathbb{V}(I)$.

Theorem 9.10 (The Extension Theorem)**.** *Let $I = (f_1, \ldots, f_s) \subset \mathbb{C}[x_1, \ldots, x_n]$. For each $1 \leq i \leq s$ write f_i in the form:*

$$f_i = h_i(x_2, \ldots, x_n)x_1^{m_i} + (\textit{terms in which } x_1 \textit{ has degree} < m_i),$$

where $m_i > 0$ and $h_i \in \mathbb{C}[x_2, \ldots, x_n]$ is nonzero. Let $(a_2, \ldots, a_n) \in \mathbb{V}(I_1)$.

If $(a_2, \ldots, a_n) \notin \mathbb{V}(h_1, \ldots, h_n)$ then there exists $a_1 \in \mathbb{C}$ such that $(a_1, a_2, \ldots, a_n) \in \mathbb{V}(I)$.

Proof. See [CLO07, Chapter 3, §6]. □

Remark 9.11. Theorem 9.10 is more useful that it might appear. First, eliminating just one indeterminate is actually quite a common task – it corresponds to *projecting* the variety $\mathbb{V}(I) \subset \mathbb{C}^n$ onto $\mathbb{C}^{n-1}$. Second, there's nothing preventing you using the Extension Theorem when moving from partial solutions in $\mathbb{V}(I_{i+1})$ to partial solutions in $\mathbb{V}(I_i)$.

Example 9.12. Consider the equations:

$$\begin{aligned} y &= 1 + \frac{1}{x^3} \\ z &= 1 + \frac{1}{x} \end{aligned}$$

We want to know all the solutions over $\mathbb{C}$. In other words, we want to understand:

$$\mathbb{V}(x^3y - x^3 - 1, xz - x - 1) \subset \mathbb{C}^3.$$

Using lexicographic order, the (reduced) Gröbner basis for $I = (x^3y - x^3 - 1, xz - x - 1)$ is $G = \{y - z^3 + 3z^2 - 3z, xz - x - 1\}$. We have:

$$\begin{aligned} G_2 &= \emptyset \subset \mathbb{C}[z], \\ G_1 &= \left\{y - z^3 + 3z^2 - 3z\right\} \subset \mathbb{C}[y, z], \\ G = G_0 &= \left\{y - z^3 + 3z^2 - 3z, xz - x - 1\right\} \subset \mathbb{C}[x, y, z]. \end{aligned}$$

From G_1 we have:

$$\mathbb{V}(I_1) = \left\{(t^3 - 3t^2 + 3t, t) \mid t \in \mathbb{C}\right\} \subset \mathbb{C}^2.$$

We use the Extension Theorem to see which values of t extend the partial solutions in $\mathbb{V}(I_1)$ to solutions of $\mathbb{V}(I)$. Rewriting the original basis of I gives:

$$\begin{aligned} x^3y - x^3 - 1 &= x^3(y - 1) - 1 \\ xz - x - 1 &= x(z - 1) - 1 \end{aligned}$$

Consider $\mathbb{V}(y - 1, z - 1) = \{(1, 1)\} \subset \mathbb{C}^2$. Since $(t^3 - 3t^2 + 3t, t) \notin \mathbb{V}(y - 1, z - 1)$ for all $t \neq 1$, the Elimination Theorem guarantees that they extend to a solution of $\mathbb{V}(I)$. What about $t = 1$? From $xz - x - 1 = 0$ we obtain $x \cdot 1 - x - 1 = 0$; this clearly has no solutions. Hence:

$$\mathbb{V}(I) = \left\{ \left(\frac{1}{t-1}, t^3 - 3t^2 + 3t, t \right) \;\middle|\; t \in \mathbb{C} \setminus \{1\} \right\}.$$

The real part of this solution is given in Figure 8. The curve is shown projected onto the (y, z)-plane. The image of the projection is the curve $y = z^3 - 3z^2 + 3z$ (i.e. $\mathbb{V}(G_1)$), but with the point $(1, 1)$ missing. This point corresponds to the value $t = 1$.

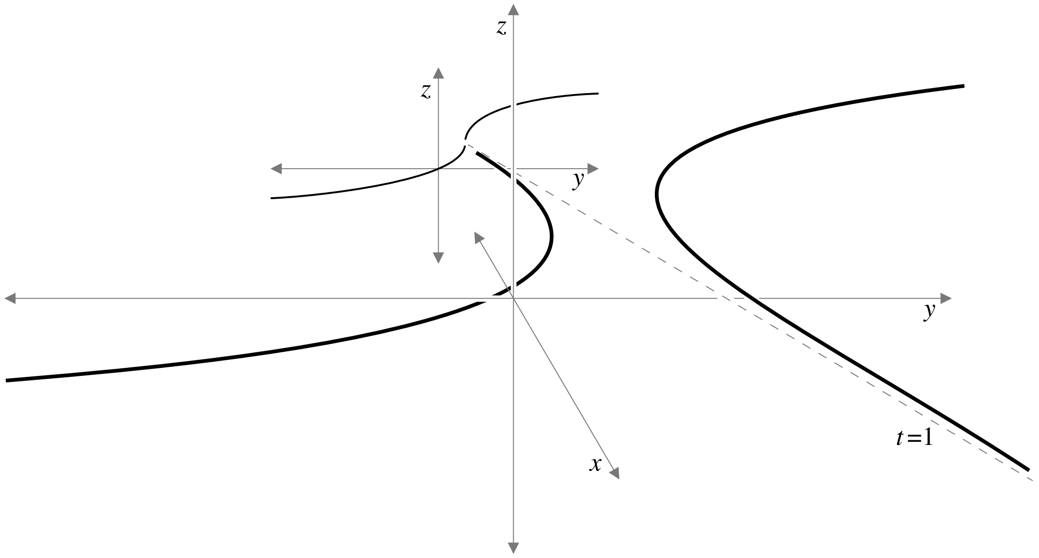

FIGURE 8. The variety $\mathbb{V}(x^3y - x^3 - 1, xz - x - 1)$ in $\mathbb{R}^3$ projected onto the (y, z)-plane.

Projecting affine varieties.

Remark 9.13. We saw in Example 9.12 that elimination corresponds to projection onto a lower dimensional subspace. We shall explore this idea further. For simplicity we shall work over $\mathbb{C}$ (however any algebraically closed field will do).

Definition 9.14. Fix $0 \leq l < n$. The *projection map* π_l is given by:

$$\begin{aligned} \pi_l : \mathbb{C}^n &\to \mathbb{C}^{n-l} \\ (a_1, \ldots, a_n) &\mapsto (a_{l+1}, \ldots, a_n). \end{aligned}$$

Exercise 9.15. Let $V \subset \mathbb{C}^n$ be an affine variety. Show that $\pi_l(V) \subset \mathbb{V}(I_l)$, where I_l is the l^{th} elimination ideal of $I = \mathbb{I}(V)$.

Remark 9.16. In Example 9.12 the image of the projection $\pi_1 : \mathbb{C}^3 \to \mathbb{C}^2$ is contained in $\mathbb{V}(I_1)$. More precisely:

$$\pi_1(\mathbb{V}(x^3y - x^3 - 1, xz - x - 1)) = \mathbb{V}(y - z^3 + 3z^2 - 3z) \setminus \{(1, 1)\} .$$

Notice that $\mathbb{V}(y - z^3 + 3z^2 - 3z) \setminus \{(1, 1)\}$ is *not* an affine variety (you should prove this).

Theorem 9.17 (The Closure Theorem). *Let $V \subset \mathbb{C}^n$ be an affine variety, and let I_l be the l^{th} elimination ideal of $I = \mathbb{I}(V)$. Then:*

(1) *$\mathbb{V}(I_l)$ is the smallest affine variety containing $\pi_l(V)$;*

(2) *When $V \neq \emptyset$, there exists an affine variety $W \subsetneq \mathbb{V}(I_l)$ such that $\mathbb{V}(I_l) \backslash W \subset \pi_l(V)$.*

Proof. See [CLO07, pp. 125–126]. □

Remark 9.18. What we mean by “smallest” in Theorem 9.17 is hopefully intuitively clear, even if we haven't defined this concept mathematically. You should go away and read about the *Zariski topology* in one of [Rei88, Sha94, SKKT00]. The point is that $\mathbb{V}(I_l)$ is the *closure* of $\pi_l(V)$ in the Zariski topology.

Theorem 9.17 (2) means that we can always subtract off an affine variety from $\mathbb{V}(I_l)$ to recover $\pi_l(V)$. You can see this happening in Example 9.12, where $\pi_1(V) = \mathbb{V}(y - z^3 + 3z^2 - 3z) \setminus \mathbb{V}(y - 1, z - 1)$. Obviously in the case when $\pi_l(V) = \mathbb{V}(I_l)$ we have $W = \emptyset (= \mathbb{V}(1))$. The difference $U \setminus W$ of two affine varieties U and W is called a *quasi-affine variety.*

10. The Nullstellensatz

Recall Example 4.16 and Proposiion 4.21. For an arbitrary ideal $I \subset k[x_1, \ldots, x_n]$ we have an inclusion $I \subset \mathbb{I}(\mathbb{V}(I))$, but not necessarily equality (as illustrated by taking $I = (x^2)$). In this section we shall see when $I = \mathbb{I}(\mathbb{V}(I))$; we shall introduce the notion of a *radical ideal* from Commutative Algebra and understand the connection with Algebraic Geometry. Before we can proceed, we need another result due to Hilbert: the Nullstellensatz.

Three Nullstellensatzs.

Theorem 10.1 (The Weak Nullstellensatz)**.** *Let $I \subset \mathbb{C}[x_1, \ldots, x_n]$ be an ideal such that $\mathbb{V}(I) = \emptyset$. Then $I = \mathbb{C}[x_1, \ldots, x_n]$.*

Proof. See [CLO07, pp. 170–172]. □

Remark 10.2. In the statement of Theorem 10.1, and for the remainder of Section 10, you may replace $\mathbb{C}$ with any algebraically closed field.

Note that the converse statement is obviously true: Since $1 \in \mathbb{C}[x_1, \ldots, x_n]$, we have that $\mathbb{V}(\mathbb{C}[x_1, \ldots, x_n]) = \emptyset$. In fact, since $(1) = \mathbb{C}[x_1, \ldots, x_n]$, a useful rephrasing is that $\mathbb{V}(I) = \emptyset$ if and only if $1 \in I$.

Corollary 10.3. *A system of equations*

$$\begin{aligned} f_1 &= 0, \\ &\vdots \\ f_m &= 0, \end{aligned}$$

has a common solution in $\mathbb{C}^n$ *if and only if the reduced Gröbner basis of* $(f_1, \ldots, f_m)$ *does not equal* $\{1\}$.

Proof. The system of equations has a common solution if and only if $\mathbb{V}(f_1, \ldots, f_m) \neq \emptyset$. By Theorem 10.1 this is the case if and only if $1 \notin (f_1, \ldots, f_m)$. We shall show that, for any monomial order, $\{1\}$ is the reduced Gröbner basis for (1).

Let $G = \{g_1, \ldots, g_s\}$ be a Gröbner basis for $I = (1)$. $1 \in (\mathrm{LT}(I)) = (\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s))$, and Exercise 7.3 tells us that 1 must be divisible by $\mathrm{LT}(g_i)$ for some $1 \leq i \leq s$. Without loss of generality, suppose that $\mathrm{LT}(g_1)$ divides 1. Then $\mathrm{LT}(g_1)$ is a constant. But since every $\mathrm{LT}(g_i)$, $2 \leq i \leq s$, is divisible by that constant, each g_i can be removed from the Gröbner basis (by Exercise 8.19). Finally, since $\mathrm{LT}(g_1)$ is constant, so g_1 is constant and we are free to multiply through so that $g_1 = 1$, giving the (unique) reduced Gröbner basis $\{1\}$. □

Example 10.4. Consider the system of equations:

$$\begin{aligned} x^2 + y^2 &= -1, \\ x^3 + y^3 &= -1, \\ x^5 + y^5 &= -1. \end{aligned}$$

The reduced Gröbner basis for $(x^2 + y^2 + 1, x^3 + y^3 + 1, x^5 + y^5 + 1)$ using lexicographic order is $\{1\}$. Hence by Corollary 10.3 there is no solution in $\mathbb{C}^2$.

Theorem 10.5 (The Nullstellensatz). *Let* $I \subset \mathbb{C}[x_1, \ldots, x_n]$ *be an ideal. A polynomial* $f \in \mathbb{I}(\mathbb{V}(I))$ *if and only if there exists an integer* $m \geq 1$ *such that* $f^m \in I$.

Proof. We may assume that $I = (f_1, \ldots, f_s)$ (by the Hilbert Basis Theorem), and let $f \in \mathbb{I}(\mathbb{V}(I))$ be a non-zero polynomial. Consider the ideal $I' = (f_1, \ldots, f_s, 1 - yf) \subset k[x_1, \ldots, x_n, y]$, and suppose for a contradiction that $\mathbb{V}(I') \neq \emptyset$. If $(a_1, \ldots, a_n, a_{n+1}) \in \mathbb{V}(I')$ then $(a_1, \ldots, a_n) \in \mathbb{V}(I)$. But since $f \in \mathbb{V}(I)$, so $f(a_1, \ldots, a_n) = 0$. Hence $1 - yf = 1 \neq 0$ at $(a_1, \ldots, a_n, a_{n+1})$. Hence $\mathbb{V}(I') = \emptyset$.

By Theorem 10.1 we have that $1 \in \mathbb{V}(I')$. Thus there exist $h_i, q \in \mathbb{C}[x_1, \ldots, x_n, y]$ such that:

$$1 = h_1 f_1 + \ldots + h_s f_s + q(1 - yf).$$

Setting $y = 1/f(x_1, \ldots, x_n)$ we obtain:

$$1 = h_1(x_1, \ldots, x_n, 1/f) f_1 + \ldots + h_s(x_1, \ldots, x_n, 1/f) f_s. \tag{10.1}$$

Now, each h_i is a polynomial, hence there exists some suitably large power m such that multiplying (10.1) through by f^m will clear the denominators. I.e.

$$f^m = h_1' f_1 + \ldots + h_s' f_s \tag{10.2}$$

where the $h_i' \in \mathbb{C}[x_1, \ldots, x_n]$ (remember that f is a polynomial in $\mathbb{C}[x_1, \ldots, x_n]$). But (10.2) means that $f^m \in (f_1, \ldots, f_s)$.

The converse is easy: Let $f^m \in I$ and $(a_0, \ldots, a_n) \in \mathbb{V}(I)$. Then $(f(a_1, \ldots, a_n))^m = 0$, hence $f(a_1, \ldots, a_n) = 0$, and so $f \in \mathbb{V}(I)$. □

Example 10.6. Let $I = (x^2 + y^2 - 1, x - 1) \subset \mathbb{C}[x, y]$. A Gröbner basis for I is $\{y^2, x - 1\}$, hence $\mathbb{V}(x^2 + y^2 - 1, x - 1) = \mathbb{V}(y^2, x - 1)$. By Theorem 10.5 we see that $y \in \mathbb{I}(\mathbb{V}(I))$ even though $y \notin I$. In fact it is easy to see that $\mathbb{I}(\mathbb{V}(I)) = (y, x - 1)$.

Definition 10.7. Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. We call I *radical* if $f^m \in I$ for some integer $m \geq 1$ implies that $f \in I$.

Definition 10.8. Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. The *radical of I* is given by:

$$\sqrt{I} := \{f \in k[x_1, \ldots, x_n] \mid f^m \in I \text{ for some integer } m \geq 1\}.$$

Example 10.9. The ideal $(x^2 - y^2, x)$ is not radical, since it contains y^2 but not y. We have that $\sqrt{(x^2 - y^2, x)} = (x, y)$.

Example 10.10. Principal ideals in $\mathbb{C}[x]$ provide plenty of nice examples. The ideal $(x^2 + 2x + 1)$ is clearly not radical, since $x + 1 \notin (x^2 + 2x + 1)$. Its radical is given by $(x + 1)$ (you should check this). Similarly the ideal $(x^3 - 6x^2 + 12x - 8)$ has radical $(x - 2)$.

Exercise 10.11. Show that $\sqrt{I}$ is an ideal in $k[x_1, \ldots, x_n]$ containing I, and that $\sqrt{I}$ is radical. Deduce that $\sqrt{I} = I$ if and only if I is radical. Prove also that the intersection of two radical ideals is also radical.

Theorem 10.12 (The Strong Nullstellensatz). *Let $I \subset \mathbb{C}[x_1, \ldots, x_n]$ be an ideal. Then $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$.*

Proof. Let $f \in \sqrt{I}$. Then there exists some integer $m \geq 1$ such that $f^m \in I$, and so f^m vanishes on $\mathbb{V}(I)$. Hence f vanishes on $\mathbb{V}(I)$ and so $f \in \mathbb{I}(\mathbb{V}(I))$. I.e. $\sqrt{I} \subset \mathbb{I}(\mathbb{V}(I))$.

For the opposite inclusion, suppose that $f \in \mathbb{I}(\mathbb{V}(I))$. By Theorem 10.5 there exists some integer $m \geq 1$ such that $f^m \in I$, and so $f \in \sqrt{I}$. Hence $\mathbb{I}(\mathbb{V}(I)) \subset \sqrt{I}$. □

Remark 10.13. Theorem 10.12 tells us that affine varieties and radical ideals are in one-to-one correspondence. We can think of $\mathbb{V}(I)$ as a map from the set of radical ideals to the set of affine varieties, and $\mathbb{I}(V)$ as a map in the opposite direction. In other words,

$$\begin{aligned}\mathbb{V} &: \{\text{radical ideals in } \mathbb{C}[x_1,\ldots,x_n]\} \to \{\text{affine varieties in } \mathbb{C}^n\}\,,\\ \mathbb{I} &: \{\text{affine varieties in } \mathbb{C}^n\} \to \{\text{radical ideals in } \mathbb{C}[x_1,\ldots,x_n]\}\,.\end{aligned}$$

If I is a radical ideal, then $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I} = I$ (by Theorem 10.12). If V is an affine variety then $\mathbb{V}(\mathbb{I}(V)) = V$ (check this). Hence $\mathbb{I}$ and $\mathbb{V}$ are inverses of each other.

Stop, make a cup of tea, and think seriously about what we've just discovered here. This is all really rather remarkable.

Example 10.14. Let $I = (xy-1, x^4-1) \subset \mathbb{C}[x,y]$ be an ideal. Notice that the variety $\mathbb{V}(I) = \{(1,1),(-1,-1),(i,-i),(-i,i)\} \subset \mathbb{C}^2$. Hence any $f \in I$ vanishes at those four points. Now consider the intersection of four ideals:

$$I' = (x-1,y-1) \cap (x+1,y+1) \cap (x-i,y+i) \cap (x+i,y-i) \subset \mathbb{C}[x,y].$$

Clearly any $f \in I'$ also vanishes at the four points in $\mathbb{V}(I)$. Each of the four ideals defining I' is radical, so by Exercise 10.11 we see that I' is radical. Hence by Theorem 10.12 $I' = \sqrt{I}$.

Radical algorithms.

Remark 10.15. Armed with an arbitrary ideal $I \subset \mathbb{C}[x_1,\ldots,x_n]$, three questions present themselves. Is there a method for determining whether a given polynomial f lies in $\sqrt{I}$? How can we decide whether I is radical or not? Can we write down a basis for $\sqrt{I}$? Unfortunately we we'll only be able to answer the last two questions in the case of a principal ideal (although general algorithms are known).

The proof of Theorem 10.5 immediately gives us the following answer to the first question:

Proposition 10.16. *Let $I = (f_1,\ldots,f_s) \subset \mathbb{C}[x_1,\ldots,x_n]$ be an ideal, and let $f \in \mathbb{C}[x_1,\ldots,x_n]$ be an arbitrary polynomial. Then $f \in \sqrt{I}$ if and only if $1 \in (f_1,\ldots,f_s,1-yf) \subset \mathbb{C}[x_1,\ldots,x_n,y]$.*

Example 10.17. Consider the ideal $I = (yx^3,(y-2)^3) \subset \mathbb{C}[x,y]$ We shall show that $f = x-3y+6 \in \sqrt{I}$. By Proposition 10.16 it is sufficient to show that $1 \in (yx^3,(y-2)^3,1-z(x-3y+6)) \subset \mathbb{C}[x,y,z]$. The reduced Gröbner basis of this ideal is $\{1\}$, so we're done.

We can calculate what power of f lies in I by repeated use of the division algorithm. The reduced Gröbner basis for I, using lexicographic order, is $G = \{(y-2)^3, x^3\}$. (Note that I didn't need to perform any Gröbner basis calculations to find this – I could see it straight from the generators of I. You should pause to see how.) Observe that:

$$\begin{aligned}
\overline{x-3y+6}^G &= x-3y+6 \neq 0\\
\overline{(x-3y+6)^2}^G &= (x-3y+6)^2 \neq 0\\
\overline{(x-3y+6)^3}^G &= -9x(y-2)(x-3y+6) \neq 0\\
\overline{(x-3y+6)^4}^G &= -54x^2(y-2)^2 \neq 0\\
\overline{(x-3y+6)^5}^G &= 0
\end{aligned}$$

Hence f^5 is the smallest power of f to lie in I.

Proposition 10.18. *Let $f \in \mathbb{C}[x_1, \ldots, x_n]$, and suppose that $f = cf_1^{a_1} \ldots f_r^{a_r}$ is the factorisation of f into a product of distinct irreducible polynomials, where $c \in \mathbb{C}$. Then:*

$$\sqrt{(f)} = (f_1 f_2 \ldots f_r).$$

Proof. First we show that $(f_1 f_2 \ldots f_r) \subset \sqrt{(f)}$. Let $N := \max a_1, \ldots, a_r + 1$, then:

$$(f_1 f_2 \ldots f_r)^N = f_1^{N-a_1} f_2^{N-a_2} \ldots f_r^{N-a_r} f,$$

so $(f_1 f_2 \ldots f_r)^N \in (f)$. Hence $f_1 f_2 \ldots f_r \in \sqrt{(f)}$ and we have inclusion.

Now we show that $\sqrt{(f)} \subset (f_1 f_2 \ldots f_r)$. Let $g \in \sqrt{(f)}$. Then there exists some power such that $g^M \in (f)$. Hence $g^M = hf$ for some $h \in \mathbb{C}[x_1, \ldots, x_n]$. Let $g = g_1^{b_1} \ldots g_s^{b_s}$ be the factorisation of g into a product of distinct irreducible polynomials. Then:

$$g_1^{Mb_1} \ldots g_s^{Mb_s} = chf_1^{a_1} \ldots f_r^{a_r}.$$

By unique factorisation, the irreducible polynomials on both sides must be the same (up to multiplication by some constants). In particular, each f_i must be equal to (some multiple of) one of the g_j. This tells us that g is a polynomial multiple of $f_1 f_2 \ldots f_r$, and so $g \in (f_1 f_2 \ldots f_r)$. □

Example 10.19. Consider the polynomial $f = (x^2+1)^2(xy-1)^3 \in \mathbb{C}[x,y]$. This factors as $f = (x-i)^2(x+i)^2(xy-1)^3$. Hence by Proposition 10.18 we have that:

$$\sqrt{(f)} = ((x-i)(x+i)(xy-1)) = (yx^3 - x^2 + xy - 1).$$

Proposition 10.20. *Let* $f \in \mathbb{C}[x_1, \ldots, x_n]$*, and let:*

$$f_{\mathrm{red}} := \frac{f}{\gcd\left\{f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}\right\}}.$$

Then $\sqrt{(f)} = (f_{\mathrm{red}})$.

Proof. In order to prove the claim it is sufficient to show that:

$$\gcd\left\{f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}\right\} = f_1^{a_1-1} f_2^{a_2-1} \ldots f_r^{a_r-1}.$$

The rest follows from Proposition 10.18.

First we show that $f_1^{a_1-1} f_2^{a_2-1} \ldots f_r^{a_r-1}$ divides the gcd. This is easy, since by the product rule:

$$\frac{\partial f}{\partial x_j} = f_1^{a_1-1} f_2^{a_2-1} \ldots f_r^{a_r-1} \left(a_1 \frac{\partial f_1}{\partial x_j} f_2 \ldots f_r + a_2 f_1 \frac{\partial f_2}{\partial x_j} \ldots f_r + \ldots + a_r f_1 f_2 \ldots \frac{\partial f_r}{\partial x_j} \right).$$

Conversely, if we can show that, for each i, there exists some $\partial f / \partial x_j$ not divisible by $f_i^{a_i}$, then we will be done.

Suppose for a contradiction that $f_i^{a_i}$ divides $\partial f / \partial x_l$ for all l. Since f_i is non-constant, it must contain a term involving x_j for some j. Writing $f = f_i^{a_i} h_i$ (where h_i is the product $f_1^{a_1} \ldots \widehat{f_i^{a_i}} \ldots f_r^{a_r}$) we see, once again by the product rule, that:

$$\frac{\partial f}{\partial x_j} = f_i^{a_i-1} \left(a_i \frac{\partial f_i}{\partial x_j} h_i + f_i \frac{\partial h_i}{\partial x_j} \right).$$

By assumption, $f_i^{a_i}$ divides the left hand side, and so must divide the right hand side. In particular, f_i must divide $(\partial f_i / \partial x_j) h_i$. But f_i does not divide h_i (since the f_l are distinct and irreducible), so it must divide $\partial f_i / \partial x_j$. This is nonsense, since the degree of x_j in $\partial f_i / \partial x_j$ is strictly less than in f_i. We have obtained our desired contradiction. □

Remark 10.21. Recall Remark 5.17 for how to use *Maple*'s `gcd` function. To obtain a partial derivative, use the `diff` function. For example, to calculate $\partial f / \partial x$ you would type `diff(f,x);`. Typing `divide(f,g,'q');` performs the division algorithm, dividing f by g. If the remainder is zero then the function outputs `true` and the quotient is stored in `q`. Otherwise it outputs `false`.

Example 10.22. Let $f = y^3 - 2xy^2 + yx^2 - y^2 + 2xy - x^2 \in \mathbb{C}[x, y]$. By Proposition 10.20 we know that $\sqrt{(f)} = (f_{\mathrm{red}})$. In order to calculate f_{red} we might enter the following sequence of commands in *Maple*:

```
f:=y^3-2*x*y^2+y*x^2-y^2+2*x*y-x^2;
g:=gcd(f,gcd(diff(f,x),diff(f,y)));
divide(f,g,'q');
q;
```

We see that $f_{\text{red}} = (x-y)(y-1)$. Hence:

$$\mathbb{I}(\mathbb{V}(f)) = \sqrt{(f)} = ((x-y)(y-1)) \subset \mathbb{C}[x,y].$$

The affine variety $\mathbb{V}(f)$ is given by the union two lines $y = x$ and $y = 1$.

Corollary 10.23. *A principal ideal $(f) \subset \mathbb{C}[x_1, \ldots, x_n]$ is radical if and only if*

$$\gcd\left\{f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}\right\}$$

is a constant.

References

[AL94] William W. Adams and Philippe Loustaunau, *An introduction to Gröbner bases*, Graduate Studies in Mathematics, vol. 3, American Mathematical Society, Providence, RI, 1994.

[AM69] M. F. Atiyah and I. G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[CLO05] David Cox, John Little, and Donal O'Shea, *Using algebraic geometry*, second ed., Graduate Texts in Mathematics, vol. 185, Springer, New York, 2005.

[CLO07] ______, *Ideals, varieties, and algorithms*, third ed., Undergraduate Texts in Mathematics, Springer, New York, 2007, An introduction to computational algebraic geometry and commutative algebra.

[EGSS02] David Eisenbud, Daniel R. Grayson, Michael Stillman, and Bernd Sturmfels (eds.), *Computations in algebraic geometry with Macaulay 2*, Algorithms and Computation in Mathematics, vol. 8, Springer-Verlag, Berlin, 2002.

[Eis95] David Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995, With a view toward algebraic geometry.

[Kir92] Frances Kirwan, *Complex algebraic curves*, London Mathematical Society Student Texts, vol. 23, Cambridge University Press, Cambridge, 1992.

[KR00] Martin Kreuzer and Lorenzo Robbiano, *Computational commutative algebra. 1*, Springer-Verlag, Berlin, 2000.

[KR05] ______, *Computational commutative algebra. 2*, Springer-Verlag, Berlin, 2005.

[Rei88] Miles Reid, *Undergraduate algebraic geometry*, London Mathematical Society Student Texts, vol. 12, Cambridge University Press, Cambridge, 1988.

[Rei95] ______, *Undergraduate commutative algebra*, London Mathematical Society Student Texts, vol. 29, Cambridge University Press, Cambridge, 1995.

[Sch03] Hal Schenck, *Computational algebraic geometry*, London Mathematical Society Student Texts, vol. 58, Cambridge University Press, Cambridge, 2003.

[Sha94] Igor R. Shafarevich, *Basic algebraic geometry. 1*, second ed., Springer-Verlag, Berlin, 1994, Varieties in projective space, Translated from the 1988 Russian edition and with notes by Miles Reid.

[Sha00] R. Y. Sharp, *Steps in commutative algebra*, second ed., London Mathematical Society Student Texts, vol. 51, Cambridge University Press, Cambridge, 2000.

[SKKT00] Karen E. Smith, Lauri Kahanpää, Pekka Kekäläinen, and William Traves, *An invitation to algebraic geometry*, Universitext, Springer-Verlag, New York, 2000.