1. Fields

Fields and vector spaces.

Typical vector spaces: $\mathbb{R}, \mathbb{Q}, \mathbb{C}$. For infinite dimensional vector spaces, see notes by Karen Smith. Important to consider a field as a vector space over a sub-field.

Also have: algebraic closure of $\mathbb{Q}$. Galois fields: $GF(p^a)$.

Don't limit what field you work over.

2. Polynomial rings over a field

Notation for a polynomial ring: $\mathbb{K}[x_1, \ldots, x_n]$.
Monomial: $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$
Set $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$.
Write x^α for $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$.
A *term* is a monomial multiplied by a field element: $c_\alpha x^\alpha$.
A *polynomial* is a *finite* $\mathbb{K}$-linear combination of monomials:

$$f = \sum_\alpha c_\alpha x^\alpha,$$

so a polynomial is a finite sum of terms. The *support* of f are the monomials that appear (with non-zero coefficients) in the polynomial f.

If $\alpha = (\alpha_1, \ldots, \alpha_n)$, put $|\alpha| = \alpha_1 + \cdots + \alpha_n$.

If $f \in \mathbb{K}[x_1, \ldots, x_n]$, $\deg(f) = \max\{|\alpha| : x^\alpha \text{ is in the support of } f\}$.

Example 2.1. $f = 7x^3y^2z + 11xyz^2$ $\deg(f) = \max\{6, 4\} = 6$. $7x^3y^2z$ is a *term.* x^3y^2z is a *monomial.*

Given $f \in \mathbb{K}[x_1, \ldots, x_n]$, *evaluation* is the map $F_f : \mathbb{K}^n \to \mathbb{K}$ given by $(c_1, \ldots, c_n) \to f(c_1, \ldots, c_n)$.

When is F_f the zero map?

Example 2.2. If $\mathbb{K}$ is a finite field, F_f can be the zero map without f being the zero polynomial. For instance take the field with two elements, $\mathbb{K} = \mathbb{Z}/2\mathbb{Z}$, and consider the polynomial $f = x^2 + x = x(x+1)$. Then f is *not* zero in the ring $\mathbb{K}[x]$, however $f(c) = 0$ for all $c \in \mathbb{K}$ (there are only two to check!).

Theorem 2.3. *If $\mathbb{K}$ is an infinite field, then F_f is the zero map if and only if f is the zero polynomial.*

Proof. (From Cox-Little-O'Shea) by induction.

If $n = 1$, then a non-zero $f \in \mathbb{K}[x]$ of degree d has at most d distinct roots (Euclidean algorithm). $F_f : \mathbb{K} \to \mathbb{K}$ evaluates to zero only at roots of f.

Assume this is true up to $n-1$ variables. Consider $\mathbb{K}[x_1, \ldots, x_n]$ as the polynomial ring $\mathbb{K}[x_1, \ldots, x_{n-1}][x_n]$ (the polynomial ring in the variable x_n with coefficients in the polynomial ring $\mathbb{K}[x_1, \ldots, x_{n-1}]$). Let $f = \sum g_i x_n^i$, where $g_i \in \mathbb{K}[x_1, \ldots, x_{n-1}]$. Consider $(\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{K}^{n-1}$. Evaluate $f(\alpha_1, \ldots, \alpha_{n-1}, x_n)$; this is a polynomial in a single variable, so by the base case it is zero if and only if $g_i(\alpha_1, \cdots, \alpha_{n-1}) = 0$ for every coefficient. By induction, $g_i(\alpha_1, \ldots, \alpha_{n-1}) = 0$ for all $(\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{K}^{n-1}$ if and only if g_i is the zero polynomial. Hence f must be the zero polynomial. $\square$

Corollary 2.4. *Let $\mathbb{K}$ be an infinite field. Let $f, g \in \mathbb{K}[x_1, \ldots, x_n]$. Then $F_f = F_g$ if and only if $f = g$ as polynomials.*

3. Affine Varieties

Definition 3.1. Let $f_1, \dots, f_r \in \mathbb{K}[x_1, \dots, x_n]$. The *affine variety* cut out by $f_1, \dots, f_r$ is denoted by $V(f_1, \dots, f_r)$ and is defined by

$$V(f_1, \dots, f_r) = \{c = (c_1, \dots, c_n) \in \mathbb{K}^n : f_i(c) = 0 \text{ for all } f_1, \dots, f_r\}$$

Example 3.2. $f = x^2 + y^2 - 1 \in \mathbb{R}[x, y]$. Then $V(f) =$ unit circle. $g = x^2 + y^2 \in \mathbb{R}[x, y]$. Then $V(g) =$ point $(0, 0)$. $h = x^2 + y^2 + 1 \in \mathbb{R}[x, y]$. Then $V(h) = \emptyset$! Notice that the codimension of these affine varieties is $1, 0, -1$, respectively.

Example 3.3. Let $f_1, f_2 \in \mathbb{R}[x, y, z]$, with $f_1 = x+y+z+7, f_2 = x+3y+2z+11$. Then $V(f_1, f_2)$ is a line in $\mathbb{R}^3$.

Example 3.4. Consider $f = x^2+2xy+y+1 \in \mathbb{F}_3[x, y]$. Then $V(f)$ is a *hypersurface* in $\mathbb{F}_3^3$. There are nine points in $\mathbb{F}_3^3$. If $x = 0$, $f(0, y) = y + 1$, so $y = 2$. If $x = 1$, $f(1, y) = 2$, so there are no solutions. If $x = 2$, then $f(2, y) = 2 + 2y$, so $y = 2$ again. So $V(f) = \{(0, 2), (2, 2)\}$.

Remark 3.5. Given $f_1, \dots, f_r \in \mathbb{Z}[x_1, \dots, x_n]$, it is interesting to consider the cardinality of $V(f_1, \dots, f_r)$ when $f_1, \dots, f_r$ are considered to be in finite fields of the form $GF(p^t)$. These cardinalities could be encoded in a power series, for instance. There are many open problems considering the relationships between the varieties $V(f_1, \dots, f_r)$ over finite fields and the varieties these polynomials define over $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, etc.

Remark 3.6. Chebatorev's density theorem gives probabilistic information about the Galois group of a polynomial by looking at splitting types of the polynomial over different finite fields.

Example 3.7 (Chebatorev's density theorem in action)**.** The table below lists the orders and cycle types of transitive subgroups of the symmetric group S_4. These are the possible Galois groups of irreducible polynomials of degree four.

G	1,1,1,1	1,1,2	1,3	4	2,2	$\lvert G\rvert$
V_4	1	0	0	0	3	4
C_4	1	0	0	2	1	4
D_4	1	2	0	2	3	8
A_4	1	0	8	0	3	12
S_4	1	6	8	6	3	24

Suppose you would like to compute the Galois group of the irreducible polynomial $f(x) = x^4 + 3x^2 - 1$. Compute its factorization modulo different primes. The factorizations have to match the cycle types.

Reducing $f(x)$ modulo first 10,000 primes. Factorization type 2,2 appears 3762 times. Factorization type 1,1,1,1 appears 1222 times. Factorization type 1,1,2 appears 2514 times. Irreducible appears 2502 times.

Chebatorev's density theorem says that, in the limit, the probability that $f(x)$ factors as a particular type is precisely the probability of picking that cycle type in the Galois group.

The statistics above match the expected cycle types of the D_4 group, which is exactly what the Galois group of $f(x)$ is.

Example 3.8 (Four-bar Linkage)**.** Consider two fixed points with two rigid bars attached, and one more rigid bar connecting the movable endpoints of the two movable bars. Attach a rigid triangle to the last bar. The curve traced out by the tip of the triangle is called the *coupler* curve of the mechanism.

Kempe's universality theorem says that any connected component of a real algebraic curve in the plane can be realized as the *coupler curve* of a mechanism. Some corrections and extensions of Kempe's theorem appear in Timothy Abbott's masters thesis. Here are some questions related to linkages:

- How can you construct a linkage with prescribed properties?
- Given a linkage, how do you find equations defining its motion?

Example 3.9 (Conformation space of cyclo-octane)**.** In cyclo-octane there are eight carbon atoms linked in a cycle by edges of a fixed length and with fixed *bond angles* between the edges at each atom. To eliminate some degrees of freedom, fix the plane determined by three atoms. So consider that three (occuring in order) have coordinates $(0,0,0), (a,0,0)$, and $(b,c,0)$ (these coordinates will be completely determined by the length of the edges and the common angle). Once these are fixed, the two adjacent points on either end can each trace out a circle's worth of positions, and for each pair of choices made for the positions of these two, there are finitely many possible positions for the remaining three points. Thus the conformation space of cyclo-octane is a surface that is a finite covering of the torus $S^1 \times S^1$, and it naturally lives in $\mathbb{R}^{15}$ (the fifteen parameters come from the coordinates of the remaining 5 points which are not fixed).

Theorem 3.10. *Let* $A = V(f_1, \ldots, f_r), B = V(g_1, \ldots, g_s)$*, with* $f_1, \ldots, f_r, g_1, \ldots, g_s \in \mathbb{K}[x_1, \ldots, x_n]$*. Then* $A \cup B$ *and* $A \cap B$ *are affine varieties.*

Proof. Check that $A \cap B = V(f_1, \ldots, f_r, g_1, \ldots, g_s)$ and $A \cup B = V(\{f_i g_j : 1 \leq i \leq r, 1 \leq j \leq s\})$. □

Some questions:

- Is $V(f_1, \ldots, f_r) = \emptyset$?
- If $|V(f_1, \ldots, f_r)| < \infty$, can we find them? Can we count how many there are?
- In general, can we describe $V(f_1, \ldots, f_r)$?

4. Parametrizations of Affine Varieties

Example 4.1. Consider the variety $V(x + y + z - 3, x + 2y + 3z - 5) \subset \mathbb{R}^3$. This is defined *implicitly* (this means the variety is given by equations). Finding a Gröbner basis is a generalization of Gaussian elimination (it's Gaussian elimination on steroids). One the augmented matrix for this linear system is put in row reduced echelon form, we obtain the system

$$\begin{aligned} x \qquad -z &= 1 \\ y \quad -2z &= 2 \end{aligned}$$

From this we obtain $x = z + 1, y = -2z + 2$. Setting $z = t$, we get the *parametrization*:

$$\begin{aligned} x &= t + 1 \\ y &= -2t + 2 \\ z &= t \end{aligned}$$

Example 4.2. Consider $V(x^2+y^2-1)$ (the unit circle). A *rational parametrization* is:

$$\begin{aligned} x = & \frac{1-t^2}{1+t^2} \\ y = & \frac{2t}{1+t^2} \end{aligned}$$

This parametrization can be determined by considering where the line with slope t through the point $(-1, 0)$ intersects the unit circle.

Definition 4.3. A *rational function* in the variables $t_1, \ldots, t_n$ is a quotient $\frac{f}{g}$ where $f, g \in \mathbb{K}[t_1, \ldots, t_n]$. Rational functions can be identified by the usual rule $\frac{f}{g} = \frac{f'}{g'}$ if and only if $fg' = f'g$. The set of all rational functions in $t_1, \ldots, t_n$ is denoted $\mathbb{K}(t_1, \ldots, t_n)$.

Proposition 4.4. *$\mathbb{K}(t_1, \ldots, t_n)$ is a field.*

Example 4.5 (Tangent surfaces of curves)**.** The *twisted cubic* is parametrized as $x = t, y = t^2, z = t^3$, $-\infty < t < \infty$. It's tangent surface is the set of points that lie on any tangent line of the twisted cubic. Given a good parametrization $\mathbf{r}(t)$ of a smooth curve (tangent vectors don't vanish), a parametrization for the tangent surface is just $s(t, u) = \mathbf{r}(t) + u \cdot \mathbf{r}'(t)$. For the twisted cubic, the tangent surface is parametrized by:

$$\begin{aligned} x = & \ t + u \\ y = & \ t^2 + 2tu \\ z = & \ t^3 + 3t^2u \end{aligned}$$

Any smooth variety has an associated tangent variety which is the set of all points which lie on the variety itself or on any tangent plane.

Example 4.6. Arithmetic in rational function fields works just like it does normally. For instance, let the matrix M be defined by

$$M = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5+x & 6 \end{bmatrix}.$$

We will consider M to be a 2×3 matrix with entries in the rational function field $\mathbb{Q}(x)$ (we could also consider entries in $\mathbb{Z}(x)$, but then we would not be able to divide). We can find the reduced row echelon form of M with the usual row operations. This yields:

$$\text{rref}(M) = \begin{bmatrix} 1 & 0 & \dfrac{3x+3}{x-3} \\ 0 & 1 & \dfrac{-6}{x-3} \end{bmatrix}.$$

We can extract from rref(M) all the usual information that we do in linear algebra. For instance, M has rank 2 as a matrix over the field $\mathbb{Q}(x)$. We could also derive a basis for the null space of M, etc.

Remark 4.7. The field $\mathbb{K}(t_1, \ldots, t_n)$ is a special case of something called a *field of fractions*, which can be constructed for any *integral domain*.

Definition 4.8. An integral domain is a commutative ring R in which there are no zero divisors (i.e. if $a, b \in R$ and $ab = 0$ then $a = 0$ or $b = 0$).

Definition 4.9. If R is an integral domain, then the field of fractions of R, denoted $\mathbf{frac}(R)$, is the field consisting of all fractions

$$\{\frac{a}{b} : a, b \in R \text{ and } b \neq 0\},$$

where $\frac{a}{b} = \frac{a'}{b'}$ if $ab' = a'b$.

Remark 4.10. There are several standard operations which preserve the property of being an integral domain. If R is an integral domain then so are $R[x]$ and $R[[x]]$ (power series ring in the variable x over R). Moreover, $\mathbf{frac}(R[x]) = \mathbf{frac}(R)(x)$.

If P is a *prime ideal* of R (we will define this later) then the quotient R/P is an integral domain (this is one way to define a prime ideal).

Definition 4.11. A rational parametric representation of a variety $V \subset \mathbb{K}^n$ is given by a collection of rational functions $\frac{f_1}{g_1}, \frac{f_2}{g_2}, \dots, \frac{f_n}{g_n} \in \mathbb{K}(t_1, \dots, t_n)$ such that

$$\begin{aligned} x_1 &= \tfrac{f_1}{g_1} \\ x_2 &= \tfrac{f_2}{g_2} \\ &\vdots \\ x_n &= \tfrac{f_n}{g_n} \end{aligned}$$

lie in V for all values of t_i and such that there is no smaller variety W for which this is true.

Definition 4.12. A variety $V \subset \mathbb{K}^n$ which has a rational representation is called *unirational*.

Remark 4.13. A variety V is said to be given *implicitly* if it is described in the form $V(f_1, \dots, f_r)$ for some polynomials $f_1, \dots, f_r$. An implicit representation is important for answering the question: given some point $p \in \mathbb{K}^n$, is $p \in V$? On the other hand, *parametric representations* are useful for producing lots of points on V (for instance if you would like to draw a picture).

Only very special varieties have parametric representations. There are several important questions related to this:

(1) Given a parametric representation, can we find an implicit representation?
(2) Given an implicit representation, can we determine if the variety has a parametric representation?
(3) If a variety has a parametric representation, can we find one?

Example 4.14. The *twisted cubic* is the variety V in $\mathbb{R}^3$ defined by the parametrization $x = t, y = t^2$, and $z = t^3$. Implicitly, V is defined by the equations $x^2 - y, x^3 - z$, and $xy - z$.

5. Ideals of affine varieties

Definition 5.1. A subset $I \subset \mathbb{K}[x_1, \dots, x_n]$ is an *ideal* if it satisfies the following two properties:

(1) If $f, g \in I$ then $f + g \in I$ and
(2) If $f \in I, g \in \mathbb{K}[x_1, \dots, x_n]$ then $fg \in I$.

If $f_1, \dots, f_r \in \mathbb{K}[x_1, \dots, x_n]$ then the *ideal generated by* $f_1, \dots, f_r$, denoted $\langle f_1, \dots, f_r \rangle$ is the smallest ideal (under containment) containing the polynomials $f_1, \dots, f_r$.

Proposition 5.2. *If* $f_1, \ldots, f_r \in \mathbb{K}[x_1, \ldots, x_n]$ *then* $\langle f_1, \ldots, f_r \rangle = \{\sum_{i=1}^r g_i f_i : g_1, \ldots, g_r \in \mathbb{K}[x_1, \ldots, x_n]\}$.

Proof. Exercise. □

Definition 5.3 (Fundamental construction for ideals)**.** An ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ is finitely generated if there are polynomials $f_1, \ldots, f_r$ so that $I = \langle f_1, \ldots, f_r \rangle$.

We will see the proof of the following fundamental result later:

Theorem 5.4 (Hilbert Basis Theorem)**.** *Every ideal in* $\mathbb{K}[x_1, \ldots, x_n]$ *is finitely generated.*

Definition 5.5 (Variety defined by a set of polynomials)**.** Given any subset of polynomials (possibly infinite) $T \subset \mathbb{K}[x_1, \ldots, x_n]$, the set $V(T) \subset \mathbb{K}^n$ is defined as

$$V(T) = \{(a_1, \ldots, a_n) \in \mathbb{K}^n : f(a_1, \ldots, a_n) = 0 \text{ for all } f \in T\}.$$

This is particularly important when T is an ideal of $\mathbb{K}[x_1, \ldots, x_n]$.

Proposition 5.6. *The variety defined by* $f_1, \ldots, f_r$ *is the same as the variety defined by the ideal* $I = \langle f_1, \ldots, f_r \rangle$*. In symbols,* $V(f_1, \ldots, f_r) = V(\langle f_1, \ldots, f_r \rangle)$*. More generally, the variety defined by any set* T *of polynomials is the same as the variety defined by the ideal* $\langle T \rangle$ *generated by* T*.*

Proof. Exercise. □

Remark 5.7. By Proposition 5.6, if T is any set of polynomials then $V(T) = V(\langle T \rangle)$. Using the Hilbert basis theorem $\langle T \rangle = \langle f_1, \ldots, f_r \rangle$ for some set of polynomials $f_1, \ldots, f_r$. Again by Proposition 5.6, $V(\langle f_1, \ldots, f_r \rangle) = V(f_1, \ldots, f_r)$. It follows that $V(T)$ is always an affine variety. More intuitively, this is saying that the variety defined by a possibly infinite set of polynomials can always be defined by finitely many polynomials.

Definition 5.8 (Ideal of a set)**.** Suppose $S \subset \mathbb{K}^n$ is any subset (this is particularly important if S is an affine variety). The ideal of S is

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

Proposition 5.9. *For any* $S \subset \mathbb{K}^n$*,* $I(S)$ *is an ideal.*

Proof. Exercise. □

Definition 5.10 (Zariski Closure)**.** Let $S \subset \mathbb{K}^n$ the *Zariski closure* of S is defined as $\bar{S} = V(I(S))$.

Remark 5.11. By Remark 5.7, the Zariski closure of any set $S \subset \mathbb{K}^n$ is an affine variety.

Proposition 5.12. *If* $S \subset \mathbb{K}^n$*, then*

(1) $V(I(\bar{S})) = \bar{S}$
(2) $S \subset \bar{S}$

Example 5.13. Consider $x^2 \in \mathbb{R}[x]$. Then $V(x^2) = \{a \in \mathbb{R} : a^2 = 0\} = \{0\}$. $I(V(x^2)) = \{f \in \mathbb{R}[x] : f(a) = 0\} = \{x \cdot g : g \in \mathbb{R}[x]\} = \langle x \rangle$.

Example 5.14. Consider $S = (0, 1) \subset \mathbb{R}^1$ (the open interval from 0 to 1). Then $I(S) = \{f \in \mathbb{R}[x] : f(a) = 0 \text{ for all } a \in (0, 1)\} = \{0\}$. Also $V(I(S)) = \{a \in \mathbb{R}^1 : f(a) = 0 \text{ for every } f \in I(S)\} = \mathbb{R}^1$. So $\bar{S} = \mathbb{R}$.

Example 5.15. Consider $S = \{(1,0),(0,1),(0,0)\} \subset \mathbb{R}^2$. Then $I(S)$ has no linear polynomials (since the points are not on a line). $I(S)$ has three linearly independent quadrics. A possible basis for this space of quadrics is $xy, x(x+y-1)$, and $y(x+y-1)$. Check that these are linearly independent! In fact, $I(S)$ is generated by these three quadrics, but it might be difficult to prove this until we have more tools (try it!).

Definition 5.16. If $T \subset \mathbb{K}[x_1,\dots,x_n]$, then define $\bar{T} = I(V(T))$.

Proposition 5.17. *If $T \subset \mathbb{K}[x_1,\dots,x_n]$, then*

(1) $T \subset \bar{T}$
(2) $I(V(\bar{T})) = \bar{T}$.

Proposition 5.18. *Suppose $V, W \subset \mathbb{K}[x_1,\dots,x_n]$. Then $\bar{V} \subset \bar{W}$ if and only if $I(V) \supset I(W)$ and $\bar{V} = \bar{W}$ if and only if $I(V) = I(W)$.*

By Remark 5.11, affine varieties can be though of as precisely the possible Zariski closures of sets in $\mathbb{K}^n$. Algebraically, this leads us to ask what types of ideals occur as closures of subsets of $\mathbb{K}[x_1,\dots,x_n]$. We will come back to this question. Let's close with two fundamental questions.

(1) Given an ideal $I \subset \mathbb{K}[x_1,\dots,x_n]$, can we find finitely many polynomials $f_1,\dots,f_r$ so that $I = \langle f_1,\dots,f_r\rangle$? The answer to this question is yes by the Hilbert Basis theorem (which we will see later), but finding such polynomials can be a difficult task! Remember Example 5.15.
(2) If $I = \langle f_1,\dots,f_r\rangle$ and $g \in \mathbb{K}[x_1,\dots,x_n]$, can we determine if $g \in I$? This is known as the *ideal membership problem.* A solution to this problem is given by Gröbner bases, which we will see soon.

6. Polynomial rings in one variable over a field

We will describe the structure of ideals in the ring $\mathbb{K}[x]$. Suppose $f \in \mathbb{K}[x]$. Then $f = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ with $a_0,\dots,a_d$. The *leading term* of $f(x)$ is $\mathrm{LT}(f) = a_d x^d$ and the degree of $f(x)$ is $\deg(f) = d$, the maximum degree of a power of x appearing in $f(x)$.

Proposition 6.1. *Given $f, g \in \mathbb{K}[x]$, there are unique polynomials $Q, R \in \mathbb{K}[x]$ such that $f = gQ + R$ with either $R = 0$ or $\deg(R) < \deg(g)$.*

We will prove Proposition 6.1 via an algorithm, which we first exhibit by example.

Example 6.2. Let $f = x^3 + 3x + 2$ and $g = x + 1$. We can produce Q and R by polynomial long division.

$$
\begin{array}{r}
x^2 \quad - x + 4 \\
x+1 \overline{\big) \; x^3 \qquad\quad + 3x + 2} \\
\underline{- x^3 - x^2} \qquad\qquad \\
- x^2 + 3x \qquad \\
\underline{x^2 \quad + x} \qquad \\
4x + 2 \\
\underline{- 4x - 4} \\
- 2
\end{array}
$$

We can read off Q and R: $Q = x^2 - x + 4$ and $R = -2$.

The LONG DIVISION ALGORITHM below generalizes the previous example.
INPUT: $R = f, Q = 0$
WHILE $\mathrm{LT}(g)|\mathrm{LT}(R)$ **do:**
 $Q = Q + \frac{\mathrm{LT}(R)}{\mathrm{LT}(g)}$
 $R = R - \frac{\mathrm{LT}(R)}{\mathrm{LT}(g)} g$
OUTPUT: Q, R

Proof of Proposition 6.1. The existence of Q, R satisfying the properties is established by the LONG DIVISION ALGORITHM described above. To establish uniqueness, suppose there are two representations $f = gQ + R$ and $f = gQ' + R'$ satisfying the given properties. We see that $0 = g(Q - Q') + (R' - R)$. Since R' and R have degree strictly less than g, $Q - Q' = 0$ and hence $Q = Q'$ and $R = R'$. □

Corollary 6.3. *A degree d polynomial in $\mathbb{K}[x]$ has at most d roots.*

Proof. Exercise. Or see the book (Corollary 3 in Section 1.5). □

Corollary 6.4. *If I is an ideal in $\mathbb{K}[x]$ then there is an $h \in \mathbb{K}[x]$ so that $I = \langle h \rangle$.*

Proof. If I is the zero ideal this is clear ($I = \langle 0 \rangle$). Otherwise pick any $h \in I$ so that h has smallest degree (we can do this by well-ordering of the integers). Note that $\langle h \rangle \subset I$. Now let $f \in I$ and apply the division algorithm. Write $f = hQ + R$. Then $\deg(R) < \deg(h)$. But also $R = f - hQ \in I$, so if $R \neq 0$ then $\deg(R) \geq \deg(h)$ by the way that h was chosen. So $R = 0$, $f = hQ$, and hence $I = \langle h \rangle$. □

Definition 6.5. Let $f, g \in \mathbb{K}[x]$. A greatest common divisor of f and g (GCD) is a polynomial h satisfying

(1) $h \mid f$ and $h \mid g$ and
(2) if $p \mid f$ and $p \mid g$ then $p \mid h$.

Remark 6.6. Any two GCD's of f and g differ by multiplication by a constant.

Proposition 6.7. *If $f, g \in \mathbb{K}[x]$ then a GCD of f and G exists.*

Proof. By Corollary 6.4, there is some $h \in \mathbb{K}[x]$ so that $\langle f, g \rangle = \langle h \rangle$. We claim that h is a GCD of f and g. Immediately, $h \mid f$ and $h \mid g$. Since $h \in \langle f, g \rangle$, there are $A, B \in \mathbb{K}[x]$ so that $h = Af + Bg$. If $p \mid f$ and $p \mid g$ then $f = pC$ and $g = pD$ for some $C, D \in \mathbb{K}[x]$. So $h = ApC + BpD = p(AC + BD)$, so $p \mid h$. □

How do you produce a GCD of f and g? This is produced by the EUCLIDEAN ALGORITHM, which we now describe. Start with f, g (assume $\deg(f) \geq \deg(g)$).

$$\begin{array}{rll} f = & gQ_1 + R_1 & \deg(g) > \deg(R_1) \text{ or } R_1 = 0 \\ g = & R_1Q_2 + R_2 & \deg(R_1) > \deg(R_2) \text{ or } R_2 = 0 \\ R_1 = & R_2Q_2 + R_3 & \deg(R_2) > \deg(R_3) \text{ or } R_3 = 0 \\ & \vdots & \\ R_{k-2} = & R_{k-1}Q_{k-1} + R_k & \\ R_k = & 0 & \end{array}$$

Since the degrees of the remainders R_i are decreasing, eventually we must hit a degree of zero, which shows that eventually we will terminate. Then a GCD of f and g is exactly the last non-zero remainder, namely R_{k-1}. Reversing the successive applications of the long division also allows you to write a GCD as a polynomial combination of f and g.

Definition 6.8. A GCD of the polynomials $f_1, \dots, f_r$ is a polynomial h satisfying:
(1) $h \mid f_1, \dots, h \mid f_r$ and
(2) if $p \mid f_1, \dots, p \mid f_r$ then $p \mid h$.

Proposition 6.9. *A GCD of $f_1, \dots, f_r$ can be defined by $GCD(f_1, \dots, f_r) = GCD(f_1, GCD(f_1, \dots, f_r))$.*

This allows a GCD of many polynomials to be computed iteratively.

At this point we can solve the ideal membership problem in one variable: to check that the polynomial $g \in \mathbb{K}[x]$ is in the ideal $\langle f_1, \dots, f_r\rangle \subset \mathbb{K}[x]$ do the following:
(1) Find the gcd h of $f_1, \dots, f_r$ by iterating the Euclidean algorithm in pairs as indicated in Proposition 6.9. We have seen that $\langle f_1, \dots, f_r\rangle = \langle h\rangle$.
(2) Divide g by h using the division algorithm. $g \in \langle f_1, \dots, f_r\rangle$ if and only if the remainder of g on division by h is 0.

Example 6.10 (Euclidean algorithm in the integers)**.** Find the gcd of 72 and 56.

$$\begin{aligned} 72 =& \quad 56 + 16 \\ 56 =& \quad 3 \cdot 16 + 8 \\ 16 =& \quad 2 \cdot 8 + 0 \end{aligned}$$

so the gcd is 8. Notice we also get a way to write 8 as an integer linear combination of 72 and 56: $8 = 56 - 3 \cdot 16 = 56 - 3 \cdot (72 - 56) = 4 \cdot 56 - 3 \cdot 72$.

Example 6.11 (Euclidean algorithm for univariate polynomials)**.** Find the GCD of $x^5 - 1$ and $x^3 - x$.

$$\begin{aligned} x^5 - 1 =& \quad (x^3 - x)(x^2 + 1) + (x - 1) \\ x^3 - x =& \quad (x - 1)(x^2 + x) + 0, \end{aligned}$$

so the GCD is $x - 1$. Notice these computations also yield that $x - 1 = (x^5 - 1) - (x^3 - x)(x^2 + 1)$, which explicitly expresses the fact that $x - 1 \in \langle x^5 - 1, x^3 - x\rangle$.

6.1. **Field of fractions of an integral domain.** We expand on Remark 4.7. Recall an *integral domain* is a commutative ring without any zero divisors. We have the following facts about integral domains:
(1) Any field is an integral domain.
(2) If R is an integral domain, then $R[x]$ is an integral domain.
(3) If I is a prime ideal of R, then R/P is an integral domain.
(4) Any finite integral domain is a field.
(5) Let $f(x) \in \mathbb{K}[x]$. If f is irreducible in $\mathbb{K}[x]$, then $\langle f\rangle$ is a prime ideal so $\mathbb{K}[x]/\langle f\rangle$ is an integral domain.

Example 6.12. Consider the finite field $\mathbb{F}_3$ with three elements (for instance $\mathbb{Z}/3\mathbb{Z}$). The polynomial $x^3 + 2x^2 + 1$ is irreducible since it does not have any roots (just plug in $x = 0, 1, 2$ and notice the polynomial does not vanish). So $\mathbb{F}_3[x]/\langle x^3 + 2x^2 + 1\rangle$ is an integral domain. Notice that this integral domain has 27 elements: any polynomial of degree ≥ 3 can be reduced to a polynomial of the form $ax^2 + bx + c$, and there are three choices for each of a, b, c. So $\mathbb{F}_3[x]/\langle x^3 + 2x^2 + 1\rangle$ is a finite integral domain, and hence a field. So we can do all the operations that we are used to doing for fields.

For instance, let's find the row reduced echelon form of the matrix

$$M = \begin{bmatrix} 1 & x^2 & 1 \\ 0 & x & 2 \end{bmatrix}$$

which we consider as having entries in the field $\mathbb{F}_2[x]/\langle x^3+2x^2+1\rangle$. Subtracting x times the second row from the first:

$$\begin{bmatrix} 1 & 0 & 1-2x \\ 0 & x & 2 \end{bmatrix}$$

Multiply the second row by the inverse of x, which is $2x^2+x$:

$$\begin{bmatrix} 1 & 0 & 1-2x \\ 0 & 1 & x^2+2x \end{bmatrix}.$$

This is the row reduced echelon form of M.

7. Monomial Orders

Monomial orders allow a generalization of the division algorithm from the last section.

Definition 7.1. A monomial order $\leq$ on the monomials of $\mathbb{K}[x_1,\ldots,x_n]$ is a

- total order (every monomial can be compared to every other monomial)
- if m_1, m_2, n are monomials and $m_1 \geq m_2$, then $m_1 n \geq m_2 n$
- if n is a monomial and $n \neq 1$, then $1 < n$ (strict inequality)

The following examples illustrate three common monomial orders. The precise definitions in terms of weight vectors is given in the section on monomial orders by vectors.

Example 7.2 (Lexicographic order or Lex order)**.** This order prioritizes earlier variables. For example, in $\mathbb{K}[x,y,z]$, the set $\{1,x,y,z,x^2,xy,xz,yz,y^2,yz,z^2\}$ is ordered from least to greatest in Lex order by:

$$1<z<z^2<y<yz<y^2<x<xz<xy<x^2$$

We may use $<_{\text{lex}}$ to clarify the use of Lex order.

Example 7.3 (Graded Lexicographic order or GLex order)**.** This order first prioritizes degree and then compares monomials of the same degree using Lex order. The set $\{1,x,y,z,x^2,xy,xz,yz,y^2,yz,z^2\}$ is ordered from least to greatest in GLex order by:

$$1<z<y<x<z^2<yz<y^2<xz<xy<x^2$$

Example 7.4 (Graded Reverse Lexicographic order or GRevLex order)**.** This order first prioritizes degree and then compares monomials of the same degree by reversing the order of the variables and then reversing the Lex order on these (see the next section for a more user-friendly definition!). The set $\{1,x,y,z,x^2,xy,xz,yz,y^2,yz,z^2\}$ is ordered from least to greatest in GRevLex order by:

$$1<z<y<x<z^2<yz<xz<y^2<xy<x^2$$

7.1. **Monomial orders by vectors.** Let $v_1,\ldots,v_n \in \mathbb{R}^n_{\geq 0}$ be linearly independent vectors. Let x^α, x^β be monomials in $\mathbb{K}[x_1,\ldots,x_n]$, where $\alpha=(\alpha_1,\ldots,\alpha_n), \beta=(\beta_1,\ldots,\beta_n)\in\mathbb{Z}^n_{\geq 0}$. Define $x^\alpha > x^\beta$ if $\alpha\cdot v_1 > \beta\cdot v_1$ or if $\alpha\cdot v_1=\beta\cdot v_1$ and $\alpha\cdot v_2>\beta\cdot v_2$ or if $\alpha\cdot v_2=\beta\cdot v_2$ and $\alpha\cdot v_3>\beta\cdot v_3$, etc. A compact representation for the monomial order is by a matrix whose columns are the vectors $v_1,\ldots,v_n$.

Example 7.5 (Lex order by vectors)**.** Lexicographic order in three variables is determined by

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

So $x^a y^b z^c > x^{a'} y^{b'} z^{c'}$ if and only if $a > a'$ *or* $a = a'$ and $b > b'$ *or* $a = a', b = b'$, and $c > c'$. In general Lexicographic order is encoded by the identity matrix:

$$\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

Example 7.6 (Graded Lex by vectors)**.** Graded Lexicographic order is encoded by the following matrix:

$$\begin{bmatrix} 1 & 1 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 1 & 0 & \cdots & 1 \\ 1 & 0 & \cdots & 0 \end{bmatrix}$$

Example 7.7 (Graded Reverse Lex order by vectors)**.** Graded Reverse Lexicographic order is encoded by the matrix which has 1's on and above the antidiagonal:

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 1 & 1 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \end{bmatrix}$$

Example 7.8. Consider the polynomial ring $\mathbb{K}[x, y, z]$ and the vector $v = \begin{bmatrix} \pi & e & \ln(2) \end{bmatrix}$. The entries of v are linearly independent over $\mathbb{Q}$. This means that for any $\alpha, \beta \in \mathbb{Z}^3$, $v \cdot \alpha \neq v \cdot \beta$. Hence v (by itself!) gives a monomial order on $\mathbb{K}[x, y, z]$. This order cannot be determined exactly by any three vectors $v_1, v_2, v_3 \in \mathbb{Z}^3_{\geq 0}$, but it can be approximated arbitrarily well by such vectors. For instace, take good rational approximations to π, e, and $\ln(2)$ (you can obtain these by continued fractions, for instance) and clear denominators.

There is a theorem (due to Robbiano) that every monomial order can be obtained by weight vectors.

Theorem 7.9 (Robbiano)**.** *Every monomial order can be determined from an ordered list of vectors $v_1, \ldots, v_n \in \mathbb{R}^n_{\geq 0}$ and can be approximated by an ordered list of vectors $v_1, \ldots, v_n$.*

See Exercises 10 and 11 in Section 2.5 of Cox-Little-O'Shea, as well as the discussion after these exercises, for more discussion.

Example 7.10 (Product Order)**.** Given a monomial order $<_1$ on $\mathbb{K}[x_1, \ldots, x_r]$ and a monomial order $<_2$ on $\mathbb{K}[y_1, \ldots, y_s]$, you can produce a monomial order $<_{1,2}$ on $\mathbb{K}[x_1, \ldots, x_r, y_1, \ldots, y_s]$ as follows:

$$x^{\alpha_1} y^{\alpha_2} > x^{\beta_1} y^{\beta_2}$$

if and only if $x^{\alpha_1} > x^{\beta_1}$ or $x^{\alpha_1} = x^{\beta_1}$ and $y^{\alpha_2} > y^{\beta_2}$. This is a *product order*. If A is an $r \times r$ matrix describing $<_1$ and B is an $s \times s$ matrix describing $<_2$, then the matrix describing $<_{1,2}$ is the block matrix:

$$\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}.$$

8. Multivariate Division Algorithm

Recall that given polynomials $f, g \in \mathbb{K}[x]$, the division algorithm produces $f = Qg + R$ where $R = 0$ or $\deg(R) < \deg(f)$. Our goal in this section is to give a generalization of this to many variables using monomial orders. Here is how we formulate the multivariate division algorithm: let $f_1, \dots, f_r$ be an *ordered* list of polynomials, and let g be another polynomial. The multivariate division algorithm gives an expression

$$g = f_1 Q_1 + f_2 Q_2 + \cdots + f_r Q_r + R,$$

where no term of R is divisible by a leading term of $f_1, \dots, f_r$. We illustrate the algorithm with some examples and then formalize it.

Example 8.1. Use Lex order on $\mathbb{K}[x, y]$. Divide $x^2y + xy^2 + y^2$ by the list $\{f_1 = xy - 1, f_2 = y^2 - 1\}$. It's crucial to keep in mind the monomial order for the leading terms!

$$\begin{array}{rr}
Q_1: & x + y \\
Q_2: & 1 \\
\begin{array}{r} xy - 1 \\ y^2 - 1 \end{array} & \overline{)\, x^2y + xy^2 + y^2} \\
 & -(x^2y - x) \\ \hline
 & xy^2 + x + y^2 \\
 & -(xy^2 - y) \\ \hline
 & x + y^2 + y \\
 & -(y^2 - 1) \\ \hline
 & x + y + 1
\end{array}$$

The algorithm shows that $Q_1 = x + y, Q_2 = 1$, and $R = x + y + 1$ so $x^2y + xy^2 + y^2 = (x + y)(xy - 1) + (1)(y^2 - 1) + x + y + 1$.

Example 8.2. Reverse the order in the last example. Specifically, use Lex order on $\mathbb{K}[x,y]$ but divide $x^2y + xy^2 + y^2$ by the list $\{f_1 = y^2 - 1, f_2 = xy - 1\}$.

$$
\begin{array}{rr}
Q_1\colon & x+1 \\
Q_2\colon & x \\
\begin{array}{r} y^2-1 \\ xy-1 \end{array} & \sqrt{x^2y + xy^2 + y^2} \\
 & -(x^2y - x) \\ \cline{2-2}
 & xy^2 + x + y^2 \\
 & -(xy^2 - x) \\ \cline{2-2}
 & xy^2 + x + y^2 \\
 & -(xy^2 - x) \\ \cline{2-2}
 & 2x + y^2 \\
 & -(y^2 - 1) \\ \cline{2-2}
 & 2x + 1
\end{array}
$$

The algorithm shows that $Q_1 = x+1, Q_2 = x$, and $R = 2x+1$, so $x^2y+xy^2+y^2 = (x+1)(y^2+1) + (x)(xy-1) + 2x + 1$.

The exact steps of this algorithm are as follows: start with a polynomial f and an ordered sequence $(f_1, \ldots, f_r)$. Initialize $Q_1 = \cdots = Q_r = 0$ and $R = f$. Starting with the largest term of R (under the monomial order) see whether any term of R is divisible by any of the lead terms of $f_1, \ldots, f_r$ (proceed in order!). If a term of R is divible by a leadterm of some f_i, update Q_i as $Q_i = \mathrm{LT}(R)/\mathrm{LT}(f_i) + Q_i$, update R as $R = R - \mathrm{LT}(R)/\mathrm{LT}(f_i) \cdot f_i$. Repeat these steps until no term of R is divisible by any of the lead terms of the f_i.

The termination of the algorithm depends on the *well-ordering property*: namely, every subset of monomials has a least element under a monomial order (the proof of this comes from Dickson's Lemma and we will see it in the next section). Notice that after every division step (under the horizontal lines), a term has been replaced by terms which are smaller in the monomial order. Since we cannot have infinite decreasing chains of monomials, the set of all terms resulting from the division algorithm must be finite (i.e. the algorithm must terminate in a finite number of steps).

9. Dickson's Lemma

Definition 9.1. Let $A \subset \mathbb{Z}^n$ be a subset of $\mathbb{Z}^n$ and let $I(A) = \langle x^\alpha : \alpha \in A \rangle$ be the ideal of $\mathbb{K}[x_1, \ldots, x_n]$ generated by the monomials with exponents from A. Then $I(A)$ is called a *monomial* ideal.

Lemma 9.2 (Dickson's Lemma.)**.** *If $I \subset \mathbb{K}[x_1, \ldots, x_n]$ is a monomial ideal, then there is a finite set of monomials $m_1, \ldots, m_k$ so that $I(A) = \langle m_1, \ldots, m_k \rangle$.*

Proof. By induction on the number of variables. If $n = 1$, then a monomial ideal has the form $I(A) = \langle x^n : n \in A \rangle$ where $A \subset \mathbb{Z}$. By the well-ordering property of $\mathbb{Z}$, A has a least element, say k. Then clearly $x^k \mid x^n$ for every $n \in A$. So $I(A) = \langle x^k \rangle$.

Now suppose $n > 1$ and write $\mathbb{K}[x_1, \ldots, x_{n-1}, x_n] = \mathbb{K}[x_1, \ldots, x_{n-1}, y]$. If I is a monomial ideal in $\mathbb{K}[x_1, \ldots, x_{n-1}, y]$ then each monomial in I can be written in the form $x^\alpha y^k$. Let

$$J = \langle x^\alpha \mid x^\alpha y^k \in I \text{ for some } k\rangle.$$

By the induction assumption, $J = \langle m_1, \ldots, m_k\rangle$ for some monomials $m_1, \ldots, m_k \in \mathbb{K}[x_1, \ldots, x_{n-1}]$.

By definition of J there exist monomials in I of the form $m_1 y^{a_1}, \ldots, m_k y^{a_k}$. Let $g = \max\{a_1, \ldots, a_k\}$.

Let $J_i = \langle x^\alpha \mid x^\alpha y^i \in I\rangle = \langle m_{i,1}, \ldots, m_{i,k_i}\rangle$ (we use the induction hypothesis again) for integers $i \geq 0$. Put $I_i = \langle y^i m_{i,1}, \ldots, y^i m_{i,k_i}\rangle$.

Now we claim $I = I_0 + I_1 + \cdots + I_g$. Suppose $x^\alpha y^k \in I$. If $k \leq g$ then clearly $x^\alpha y^k \in I_0 + \cdots + I_g$. Suppose $k > g$. Then x^α is divisible by some $x^\beta \in J_i$ for some $i \leq g$ (by the choice of g), hence $x^\beta y^i \in I$. But $i \leq g < k$, so $x^\beta y^i \mid x^\alpha y^k$, and $x^\alpha y^k \in I_0 + \cdots + I_g$. □

Definition 9.3. A total order of a set S is a well-ordering if every subset of S has a least element.

Proposition 9.4. *Let $<$ be a total order on the monomials of $\mathbb{K}[x_1, \ldots, x_n]$ satisfying $m_1 < m_2 \Rightarrow nm_1 < nm_2$. Then $<$ is a well-ordering if and only if 1 is the smallest monomial of $\mathbb{K}[x_1, \ldots, x_n]$ under $<$.*

Proof. Suppose $<$ is a well-ordering. Then the set of all monomials has a smallest element, call it m. If $m < 1$, then $m^2 < m$, contradicting that m is the smallest monomial. So 1 is the smallest element.

Now suppose 1 is the smallest monomial. Let A be a set of monomials of $\mathbb{K}[x_1, \ldots, x_n]$ and let $I(A)$ be the ideal generated by A. By Dickson's lemma, $I(A) = \langle m_1, \ldots, m_k\rangle$. Re-ordering if necessary, we assume $m_1 < m_2 < \cdots < m_k$. We claim that m_1 is the smallest element of A. Let m be a monomial in A. Then $m \in I(A)$, so m is divisible by m_i for some $i = 1, \ldots, k$. Hence $m_i \leq m$, but $m_1 \leq m_i$. So $m_1 \leq m$. □

Corollary 9.5. *If $<$ is a monomial order then there are no infinite decreasing sequences of monomials. In particular, the division algorithm terminates in a finite number of steps.*

10. The Hilbert basis theorem and Gröbner bases

Definition 10.1. Let $<$ be a monomial order on monomials of $\mathbb{K}[x_1, \ldots, x_n]$. Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be an ideal. The *leading term ideal* of I is

$$\mathrm{LT}_<(I) := \{\mathrm{LT}_<(f) \mid f \in I\},$$

the ideal generated by leading terms of *all* polynomials in I.

Remark 10.2. Notice that $\mathrm{LT}_<(I)$ is a monomial ideal. By Dickson's Lemma, $\mathrm{LT}_<(I)$ is finitely generated. Hence there are $g_1, \ldots, g_k \in I$ so that $\mathrm{LT}_<(I) = \langle \mathrm{LT}_<(g_1), \ldots, \mathrm{LT}_<(g_k)\rangle$.

Theorem 10.3 (Hilbert Basis Theorem)**.** *If $I \subset \mathbb{K}[x_1, \ldots, x_n]$ is an ideal, then I is finitely generated.*

Proof. Pick any monomial order $<$ and write $\mathrm{LT}_<(I) = \langle \mathrm{LT}_<(g_1), \ldots, \mathrm{LT}_<(g_k)\rangle$ as in the above remark. We claim that $I = \langle g_1, \ldots, g_k\rangle$. To see this, take any $f \in I$

and use the division algorithm to divide f by the ordered list $(g_1, \ldots, g_k)$. This gives an expression

$$f = Q_1 g_1 + \cdots + Q_k g_k + R,$$

where *no term* of R is divisible by a leading term of any $g_1, \ldots, g_k$. Notice also that $R \in I$ since $R = f - (Q_1 g_1 + \cdots + Q_k g_k)$. But if $R \neq 0$, then $\mathrm{LT}_<(R)$ is divisible by one of $\mathrm{LT}_<(g_1), \ldots, \mathrm{LT}_<(g_k)$, since this is how we obtained $g_1, \ldots, g_k$. Thus $R = 0$ and $f \in I$. □

Definition 10.4. Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be an ideal and $<$ a monomial order on $\mathbb{K}[x_1, \ldots, x_n]$. A Gröbner basis for I is a finite collection of polynomials $g_1, \ldots, g_k \in I$ satisfying that

$$\mathrm{LT}_<(I) = \langle \mathrm{LT}_<(g_1), \ldots, \mathrm{LT}_<(g_k) \rangle.$$

Remark 10.5. From the proof of the Hilbert Basis theorem, if $g_1, \ldots, g_k \in I$ and $\mathrm{LT}_<(I) = \langle \mathrm{LT}_<(g_1), \ldots, \mathrm{LT}_<(g_k) \rangle$, then $I = \langle g_1, \ldots, g_k \rangle$. So a Gröbner basis of I is a set of generators of I with the additional property that the leading terms of the g_i generate the lead term ideal of I.

Remark 10.6. By Dickson's Lemma, Gröbner bases exist with respect to any monomial order.

Remark 10.7. A Gröbner basis for I depends on the monomial order.

Definition 10.8. The *ascending chain condition* for ideals states that if $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_k \subseteq \cdots$ is an infinite nested ascending sequence of ideals, then there is some N for which $I_k = I_N$ for $k \geq N$. In other words, the sequence stabilizes.

Corollary 10.9. *The polynomial ring $\mathbb{K}[x_1, \ldots, x_n]$ has the ascending chain condition (ACC) for ideals.*

Proof. Given a nested sequence $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_k \subseteq \cdots$, let $I = \bigcup_{i=1}^{\infty} I_i$. Then I is an ideal (check this!). By the Hilbert basis theorem, $I = \langle g_1, \ldots, g_k \rangle$ for some $g_1, \ldots, g_k \in \mathbb{K}[x_1, \ldots, x_n]$. There is some $N \in \mathbb{N}$ for which all of $g_1, \ldots, g_k \in I_N$. For this choice of N, $I_k = I_N$ for all $k \geq N$, so the sequence stabilizes. □

Corollary 10.10. *If $I \subset \mathbb{K}[x_1, \ldots, x_n]$ then $V(I) = V(g_1, \ldots, g_k)$, so if a set is described as the zero locus of infinitely many polynomials, then it is actually the zero locus of finitely many polynomials.*

If we have a monomial order and we have polynomials $f, g_1, \ldots, g_k$ then the division algorithm allows us to write $f = g_1 Q_1 + \cdots + g_k Q_k + R$, where no term of R is divisible by the leading terms of $g_1, \ldots, g_k$.

Proposition 10.11. *If $g_1, \ldots, g_k$ is a Gröbner basis for $I = \langle g_1, \ldots, g_k \rangle$ then the remainder R of f on division by $g_1, \ldots, g_k$ is unique (it does not depend on the order in which $g_1, \ldots, g_k$ are listed). This remainder R is a normal form for f in $\mathbb{K}[x_1, \ldots, x_n]/I$.*

Proof. Suppose $f = G_1 + R_1 = G_2 + R_2$, where both $G_1, G_2 \in I$ and R_1, R_2 both satisfy that no term is divisible by the leading terms of $g_1, \ldots, g_k$. Then $R_1 - R_2 = G_2 - G_1 \in I$. We claim that $R_1 - R_2 = 0$. Suppose not. Then the leading term of $R_1 - R_2$ is in $\mathrm{LT}(I)$. Since $g_1, \ldots, g_k$ is a Gröbner basis, it follows that the leading term of $R_1 - R_2$ must be divisible by the leading term of some g_i.

But this would imply that either R_1 or R_2 has a term divisible by the leading term of g_i. Hence $R_1 - R_2 = 0$. □

Corollary 10.12. *Gröbner bases solve the ideal membership problem. In other words, if $g_1, \ldots, g_k$ is a Gröbner basis for $I = \langle g_1, \ldots, g_k \rangle$, then a polynomial f is in I if and only if the remainder of f on division by $g_1, \ldots, g_k$ is zero.*

11. Buchberger's Algorithm

Let $f, g \in \mathbb{K}[x_1, \ldots, x_n]$. Pick a monomial order $<$ on $\mathbb{K}[x_1, \ldots, x_n]$. We can find monomials m_1, m_2 and field elements k_1, k_2 so that $k_1 m_1 f$ and $k_2 m_2 g$ have the same leading term.

Example 11.1. Suppose $f = 2x^2 + 3y + 1, g = 5y^2 + 7$. Then we can take $m_1 = y^2, m_2 = x^2, k_1 = 5, k_2 = 2$.

Definition 11.2. If $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ under a fixed monomial order $<$. The S-polynomial of f and g is $S(f, g) = k_1 m_1 f - k_2 m_2 g$, where k_1 is the coefficient of the leading term of g, k_2 is the coefficient of the leading term of f, and $m_1 \mathrm{LM}(f) = m_2 \mathrm{LM}(g) = LCM(\mathrm{LM}(f), \mathrm{LM}(g))$, where LCM denotes least common multiple.

Proposition 11.3 (Buchberger's criterion)**.** *Let $I = \langle g_1, \ldots, g_k \rangle$. Then $g_1, \ldots, g_k$ is a Gröbner basis of I if and only if the remainder of $S(g_i, g_j)$ by $g_1, \ldots, g_k$ is zero for every pair $1 \leq i \neq j \leq k$.*

Proof. One direction is easy: if $g_1, \ldots, g_k$ is a Gröbner basis, then $S(g_i, g_j) \in I$, hence by Corollary 10.12 the remainder of $S(g_i, g_j)$ under division by $g_1, \ldots, g_k$ is zero.

Now suppose $S(g_i, g_j) = g_1 Q_1 + \cdots + g_k Q_k$, with remainder zero. We need to show that the leading terms of $g_1, \ldots, g_k$ generate $\mathrm{LT}(I)$. This is not difficult, but it is a bit technical. See Section 2.6 of Cox, Little, and O'Shea for the proof. □

Proposition 11.4 (Buchberger's Algorithm)**.** *Let $I = \langle f_1, \ldots f_s \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$, with a fixed monomial order $<$. The following algorithm produces a Gröbner basis for I with respect to $<$: for each pair f_i, f_j, compute the remainder of the S-polynomial $S(f_i, f_j)$ under division by $f_1, \ldots, f_s$. If this remainder is non-zero, add it to the generating set for I and repeat. When all remainder are zero, we have a Gröbner basis for I, so we stop.*

Proof. The stopping criterion is exactly Buchberger's criterion, so it remains to show that the algorithm terminates. At each step, the ideal generated by leading terms of polynomials in the list increases strictly. Since we have an ascending chain of ideals, it must stabilize at some point, meaning that at some point we stop having new lead terms coming from S-polynomials (so all remainders of S-polynomials must be zero). □

Definition 11.5. The polynomials $g_1, \ldots, g_k$ are a *reduced* Gröbner basis for $I = \langle g_1, \ldots, g_k \rangle$ if the leading coefficient of each g_i is 1 and no term of g_i is divisible by the leading term of any g_j $(j \neq i)$ for every $i = 1, \ldots, k$.

Proposition 11.6. *If $I \subset \mathbb{K}[x_1, \ldots, x_n]$ is an ideal, then for any fixed monomial order a reduced Gröbner basis for I is unique.*

Proof. Exercise! □

Example 11.7. Consider the ideal $I = \langle x^2, xy + y^2 \rangle$ in $\mathbb{K}[x, y]$ in Lex order.

Compute $S(x^2, xy + y^2) = yx^2 - x(xy + y^2) = -xy^2$. Now divide $-xy^2$ by $x^2, xy + y^2$. This gives a remainder of y^3, which is non-zero, so we add it to the list:

$$I = \langle x^2, xy + y^2, y^3 \rangle.$$

The S-polynomial of the first two clearly has a remainder of zero now. So now compute $S(x^2, y^3) = 0$ and $S(xy + y^2, y^3) = y^2(xy + y^2) - xy^3 = y^4$, which has a remainder of zero (since we now have y^3).

By Buchberger's criterion, $x^2, xy + y^2, y^3$ is a Gröbner basis for I with respect to Lex order. In fact, this is a reduced Gröbner basis.

Example 11.8. Let $I = \langle x^2{+}xy{+}y^2{+}x{+}y{+}1, x^2{+}2xy{+}3y^2{+}4x{+}5y{+}6 \rangle \subset \mathbb{C}[x, y]$. The Gröbner basis with respect to GRevLex (Graded Reverse Lexicographic order) is

$$\begin{aligned} g_1 &= 3y^3 + 2y^2 - 11x - 3y - 12 \\ g_2 &= x^2 - y^2 - 2x - 3y - 4 \\ g_3 &= xy + 2y^2 + 3x + 4y + 5 \end{aligned}$$

This is *almost* a reduced Gröbner basis (just divide each polynomials by its leading coefficient). The leading term ideal of I is

$$\mathrm{LT}(I) = \langle y^3, x^2, xy \rangle.$$

If $f \in \mathbb{C}[x, y]$ and we use the division algorithm to divide f by g_1, g_2, g_3, then the remainder will necessarily have the form $a + bx + cy + dy^2$. It follows that $\mathbb{C}[x, y]/I$ is a four-dimensional vector space over $\mathbb{C}$ with basis $\{1, x, y, y^2\}$.

This means we can represent linear transformations from $\mathbb{C}[x, y]/I$ to itself as matrices with this basis.

One natural way to get a linear transformation $\mathbb{C}[x, y]/I \to \mathbb{C}[x, y]/I$ is by multiplication by some $f \in \mathbb{C}[x, y]$. More precisely, $L_f : \mathbb{C}[x, y]/I \to \mathbb{C}[x, y]/I$ is defined by $r \to f \cdot r$.

We find the matrix representing multiplication by x. We get the columns of L_x with respect to the basis $\{1, x, y, y^2\}$ by multiplying each basis element by x and then taking the remainder under division by the Gröbner basis. For instance $x \cdot 1 = x$ and $x \cdot x = x^2$ with remainder $y^2 + 2x + 3y + 4$ gives the first two columns of the following matrix (check that the last two columns are correct!):

$$L_x = \begin{array}{c} \\ 1 \\ x \\ y \\ y^2 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & x & y & y^2 \end{array} \\ \left[\begin{array}{cccc} 0 & 4 & -5 & 7 \\ 1 & 2 & -3 & 5/3 \\ 0 & 3 & -4 & 5 \\ 0 & 1 & -2 & 10/3 \end{array}\right] \end{array}.$$

If we use Lex order instead, the Gröbner basis only has two polynomials

$$\begin{aligned} g_1 &= 11x - 3y^3 - 2y^2 + 3y + 12 \\ g_2 &= 3y^4 + 11y^3 + 25y^2 + 23y + 19 \end{aligned}$$

so $\mathrm{LT}_{Lex}(I) = \langle x, y^4 \rangle$ and the basis for $\mathbb{C}[x,y]/I$ from Lex order is $\{1, y, y^2, y^3\}$. We get quite a simple matrix for L_y:

$$L_y = \begin{array}{c} \\ 1 \\ y \\ y^2 \\ y^3 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & y & y^2 & y^3 \end{array} \\ \begin{bmatrix} 0 & 0 & 0 & -19/2 \\ 1 & 0 & 0 & -23/3 \\ 0 & 1 & 0 & -25/3 \\ 0 & 0 & 1 & -11/3 \end{bmatrix} \end{array}.$$

Notice that geometrically, the ideal I is defining 4 points (in this case over the complex numbers!) - the intersection points of the two degree two curves defined by the generators of I. The Gröbner basis in Lex order is really nice for finding the solutions, because one of the polynomials only involves the variable y, and we can at least approximate the roots of the degree four polynomial. For each of the roots of g_2, we can then use g_1 to find what x should be, and its clear there's only one solution for x to $g_1 = 0$ corresponding to a particular y-value.

12. Elimination Theory

Elimination theory encodes the algebraic counterpart of *projection*.

Example 12.1. The following issue arises in projections. Consider the variety $V(xy-1) \subset \mathbb{R}^2$. It's projection onto the x-axis consists of everything except the origin in $\mathbb{R}$. However, $I(\mathbb{R} \setminus \{0\}) = \langle 0 \rangle$ and $V(I(\mathbb{R} \setminus \{0\})) = \mathbb{R}$.

Hence the projection of an affine variety may not be an affine variety! Thus, if we wish to stay in the land of affine varieties, the best we can do is to compute the Zariski closure of the projection. This may consist of strictly more than the projection itself, as the projection of $V(xy-1)$ onto the x-axis indicates.

Definition 12.2. Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$. The ℓ^{th} elimination ideal is the ideal $I_\ell = I \cap \mathbb{K}[x_{\ell+1}, \ldots, x_n]$ $(0 \leq \ell \leq n-1)$.

Consider Lex order for $\mathbb{K}[x_1, \ldots, x_n]$ with $x_1 > x_2 > \cdots > x_n$. If $f \in \mathbb{K}[x_1, \ldots, x_n]$ satisfies that $\mathrm{LT}(f) \in \mathbb{K}[x_{\ell+1}, \ldots, x_n]$, then $f \in \mathbb{K}[x_{\ell+1}, \ldots, x_n]$.

Proposition 12.3. *Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$. Let $G = \{g_1, \ldots, g_k\}$ be a Gröbner basis for I with respect to Lex order. Then $G \cap \mathbb{K}[x_{\ell+1}, \ldots, x_n]$ is a Gröbner basis for I_ℓ.*

Proof. Exercise! This is much more straightforward than it may look at first. □

Example 12.4. In $\mathbb{R}^2$, consider the point $(1,3)$. The ideal of $(1,3)$ is

$$I(\{(1,3)\}) = \langle x-1, y-3 \rangle.$$

This can be proved in several ways; one way is doing Taylor expansion at $(1,3)$.

Definition 12.5. Let I, J be ideals in $\mathbb{K}[x_1, \ldots, x_n]$. Let $I = \langle f_1, \ldots f_k \rangle$ and $J = \langle g_1, \ldots, g_\ell \rangle$. Then $IJ := \langle f_i g_j \mid 0 \leq i \leq k, 0 \leq j \leq \ell \rangle$.

Lemma 12.6. $V(IJ) = V(I) \cup V(J)$.

Example 12.7. Consider $\{(0,1,2), (2,-1,1), (2,1,3)\} \subset \mathbb{R}^3$. Let

$$I = \langle x, y-1, z-2 \rangle \langle x-2, y+1, z-1 \rangle \langle x-2, y-1, z-3 \rangle.$$

Then by Lemma 12.6, $V(I) = \{(0,1,2),(2,-1,1),(2,1,3)\}$. A Gröbner basis for I with respect to Lex order is

$$\begin{aligned} g_1 &= x - 2z^2 + 8z - 8 \\ g_2 &= y + z^2 - 5z + 5 \\ g_3 &= z^3 - 6z^2 + 11z - 6 \end{aligned}$$

By Proposition 12.3, $I_1 = \langle g_2, g_3\rangle$ and $I_2 = \langle g_3\rangle$.

Notice that we can recover $V(I)$ very easily from this Gröbner basis. Factoring g_3 gives $g_3 = (z-1)(z-2)(z-3)$. Now substitute $z = 1,2,3$ into g_1, g_2 and solve for x and y, respectively.

Example 12.8 (The ℓ-elimination order of Bayer-Stillman)**.** Let $I \subset \mathbb{K}[x_1,\dots,x_n]$. We will describe an order such that $\mathrm{LT}(f) \in \mathbb{K}[x_{\ell+1},\dots,x_n] \Rightarrow f \in \mathbb{K}[x_{\ell+1},\dots,x_n]$. Let v_i be the vector in $\mathbb{R}^n$ whose first i entries are 1 and all other entries are zero. Then the monomial order using the weight vector v_ℓ first and then breaking ties using Graded Reverse Lexicographic order has this property (show this!). Notice that the monomial order GRevLex is defined by the weight vectors $v_n, v_{n-1},\dots,v_1$, so we can regard this monomial order as the monomial order $v_\ell, v_n,\dots,v_{\ell-1},v_{\ell+1},\dots,v_1$, where v_ℓ is moved to the front of the list.

Example 12.9 (ℓ^{th} elimination order)**.** More generally, an ℓ^{th} elimination order is a monomial order $>$ on $\mathbb{K}[x_1,\dots,x_n]$ so that if $\mathrm{LT}(f) \in \mathbb{K}[x_{\ell+1},\dots,x_\ell]$ then $f \in \mathbb{K}[x_{\ell+1},\dots,x_n]$. This is equivalent to saying that if G is a Gröbner basis for an ideal I with respect to $>$ then $G \cap \mathbb{K}[x_{\ell+1},\dots,x_n]$ is a Gröbner basis for $I_\ell = I \cap \mathbb{K}[x_{\ell+1},\dots,x_n]$ (show this!). Proposition 12.3 shows that Lex order is an ℓ^{th} elimination order for *every* ℓ. Thus Lex order carries *alot* of information, which indicates that it may be difficult to compute in general.

Example 12.10 (Minimal polynomials of algebraic numbers)**.** The polynomial $p(x) = x^2 - 2x - 5$ has roots $-1 \pm \sqrt{6}$; $p(x)$ is the minimal polynomial of either one of these roots. Likewise, the minimal polynomial of $\sqrt[3]{7}$ is $q(x) = x^3 - 7$. How do you find the minimal polynomial of $\alpha = -1 + \sqrt{6} + \sqrt[3]{7}$? It turns out that the minimal polynomial of α is $t^6 + 6t^5 - 3t^4 - 66t^3 - 27t^2 - 144t - 342$. This can be shown using elimination theory.

We can do this by forming the ideal $I = \langle x^2 - 2x - 5, y^3 - 7, t - (x+y)\rangle$ in the polynomial ring $\mathbb{Q}[x,y,t]$ and eliminating the variables x and y from I; in other words compute $I_2 = I \cap \mathbb{K}[t]$. The ideal I_2 is an ideal in $\mathbb{K}[t]$, thus it is principal. The generator of this ideal is the minimal polynomial of α! Convince yourself this is true.

The ideal I_2 is computed in Macaulay2 by the command "eliminate(I,x,y)". Alternatively, the same result could be obtained by defining the ideal $J = \langle x^2 - 6, y^3 - 7, t - (x+y-1)\rangle$ and eliminating the variables x and y.

Remark 12.11 (Minimal polynomials of algebraic numbers)**.** If $r_1,\dots,r_k$ are algebraic over $\mathbb{Q}$ with minimal polynomials $F_1,\dots,F_k \in \mathbb{Q}[x]$. Let $G(x_1,\dots,x_k) = G_1(x_1,\dots,x_k)/G_2(x_1,\dots,x_n)$ be a rational function in $\mathbb{Q}(x_1,\dots,x_k)$. Since $r_1,\dots,r_k$ live in the field $\overline{\mathbb{Q}}$, $G(r_1,\dots,r_k)$ is an algebraic number as long as the denominator doesn't vanish, and we can determine its minimal polynomial.

Consider the field $\mathbb{Q}[x]/\langle F_1(x)\rangle$, where $F_1(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$. Then $1, x, x^2, \dots, x^{d-1}$ is a basis for this field. In general, $\mathbb{Q}[x_1,\dots,x_k]/\langle F_1(x_1),\dots,F_k(x_k)\rangle$ is isomorphic to the field $\mathbb{Q}(r_1,\dots,r_k)$.

We find the minimal polynomial of $G(r_1, \ldots, r_k)$ as follows:

- Define $R = \mathbb{Q}[x_1, \ldots, x_k, Y]$.
- Define $I = \langle F_1(x_1), \ldots, F_k(x_k), G_2(x_1, \ldots, x_k)Y - G_1(x_1, \ldots, x_k)\rangle$.
- Eliminate the variables $x_1, \ldots, x_k$ from I.
- The result is a principal ideal only in the variable Y - the generator of this ideal is the minimal polynomial of $G(r_1, \ldots, r_k)$.

We can also introduce symbolic coefficients in the function $G(x_1, \ldots, x_k)$ to get a 'universal' expression for the minimal polynomial of algebraic numbers with a prescribed form.

For instance, take $\alpha = \sqrt{2}, \beta = \sqrt{3}$. We can get a 'universal' minimal polynomial for algebraic numbers of the form $a + b\alpha + c\beta + d\alpha\beta$ (notice *any* element of the field $\mathbb{Q}(\alpha_1, \alpha_2)$ can be expressed in this form). We can do this as follows:

- Define $K = \mathbf{frac}(\mathbb{Q}[a, b, c, d])$
- Define $R = K[x_1, x_2, Y]$
- Define $I = \langle x_1^2 - 2, x_2^2 - 3, Y - (a + bx_1 + cx_2 + dx_1x_2)\rangle$
- Eliminate the variables x_1, x_2 to get the minimal polynomial of $a+b\alpha+c\beta+d\alpha\beta$. The coefficients of this minimal polynomial will be rational functions in a, b, c, d.

Example 12.12 (Symmetric polynomials)**.** The fundamental theorem of symmetric polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ states that any symmetric polynomial can be written as a *polynomial* in the elementary symmetric polynomials. Let's consider a concrete example. If $n = 3$ then this theorem says that any symmetric polynomial in the variables x_1, x_2, x_3 can be written as a polynomial in the elementary symmetric functions $\sigma_1 = x_1 + x_2 + x_3, \sigma_2 = x_1x_2 + x_1x_3 + x_2x_3, \sigma_3 = x_1x_2x_3$.

For example, the power sum $x_1^4 + x_2^4 + x_3^4 = \sigma_1^4 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2 + 4\sigma_1\sigma_3$. How would we compute this? Again, we can do it using elimination! First, we consider the polynomial ring $\mathbb{K}[x_1, x_2, x_3, \sigma_1, \sigma_2, \sigma_3]$ and we form the ideal

$$I = \langle x_1^4 + x_2^4 + x_3^4, \sigma_1 - (x_1 + x_2 + x_3), \sigma_2 - (x_1x_2 + x_1x_3 + x_2x_3), \sigma_3 - x_1x_2x_3\rangle.$$

Then we eliminate the variables x_1, x_2, x_3 from this ideal. In other words, we compute $I_3 = I \cap \mathbb{K}[\sigma_1, \sigma_2, \sigma_3]$. The expression $\sigma_1^4 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2 + 4\sigma_1\sigma_3$ should be in I_3. In fact I_3 is a principal ideal generated by this polynomial!

Remark 12.13. In general if $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$ which we consider as having n roots $r_1, \ldots, r_d$, then

$$\begin{aligned} f(x) &= (x - r_1)(x - r_2) \cdots (x - r_d) \\ &= x^d - \sigma_1(r_1, \ldots, r_d)x^{d-1} + \cdots + (-1)^d\sigma_d(r_1, \ldots, r_d), \end{aligned}$$

so $a_i = (-1)^i\sigma_{d-i}(r_1, \ldots, r_d)$ and $i = 1, \ldots, d$. The polynomials $\sigma_1, \ldots, \sigma_d$ are the *elementary symmetric polynomials*. Any symmetric polynomial $H \in \mathbb{K}[x_1, \ldots, x_d]$ can be written as a polynomial expression in the elementary symmetric polynomials.

Example 12.14. Building off the previous example, consider the polynomial $f(x) = x^3 + ax^2 + bx + c$ with roots r_1, r_2, and r_3. Recall that

$$f(x) = (x - r_1)(x - r_2)(x - r_3) = x^3 - \sigma_1x^2 + \sigma_2x + \sigma_3,$$

where $\sigma_1 = r_1 + r_2 + r_3, \sigma_2 = r_1r_2 + r_1r_3 + r_2r_3$, and $\sigma_3 = r_1r_2r_3$. The fundamental theorem of symmetric functions tells us that any expression which is symmetric in the roots can be written as a polynomial in the coefficients of $f(x)$! Moreover we can find these polynomials by elimination. For instance, one such expression is the discriminant of $f(x)$, which is defined as $(r_1-r_2)^2(r_1-r_3)^2(r_2-r_3)^2$. This is symmetric in the roots, hence we can express it as a polynomial in the coefficients of $f(x)$. See if you can compute this using Macaulay2.

Remark 12.15. Many more such examples can be found in the book *Algorithms in Invariant Theory* by Bernd Sturmfels.

Example 12.16 (Implicitization: finding equations for the image of a map)**.** The twisted cubic is the image of the map $\phi : \mathbb{R} \to \mathbb{R}^3$ defined by $\phi(t) = (t, t^2, t^3)$. We can find equations for the image of this map as follows.

Define the ideal $I = \langle x-t, y-t^2, z-t^3\rangle$ in the ring $\mathbb{Q}[t, x, y, z]$. Any polynomial in x, y, z which vanishes on the image of ϕ will be in the elimination ideal $I \cap \mathbb{Q}[x, y, z]$. Some differences can arise by using different term orders. For instance, if we use Lex order with $x > y > z > t$ then a Gröbner basis for I is

$$GB_{Lex}(I) = \{y^3 - z^2, xz - y^2, xy - z, x^2 - y, t - x\}$$

However, if we use the Bayer-Stillman 1-elimination order we get:

$$GB_{BS1}(I) = \{y^2 - xz, xy - z, x^2 - y, t - x\}$$

Definition 12.17. Let $I, J \subset \mathbb{K}[x_1, \dots, x_n]$ and $F \in \mathbb{K}[x_1, \dots, x_n]$. Then the *intersection* of I and J is $I \cap J = \{f \mid f \in I \text{ and } f \in J\}$. The *ideal quotient* of I by F is $I : F = \langle g \mid gF \in I\rangle$. The *ideal quotient* of I by J is $I : J = \langle g \mid gF \in I \text{ for all } F \in J\rangle$.

Exercise: Prove that if I, J are ideals, then so are $I \cap J$ and $I : J$.

Example 12.18. In $\mathbb{Z}$, $\langle 10\rangle : \langle 2\rangle = \langle 5\rangle$ and $\langle 10\rangle : \langle 3\rangle = \langle 10\rangle$.

We would like to be able to compute all of the ideals in Definition 12.17. Elimination theory allows us to do this as well.

Proposition 12.19. *If $I = \langle f_1, \dots, f_k\rangle, J = \langle g_1, \dots, g_\ell\rangle \subset \mathbb{K}[x_1, \dots, x_n]$, then we can compute $I \cap J$ using elimination theory as follows. First, introduce a new variable t and define the ideal*

$$K = \langle f_1 t, \dots, f_k t, g_1(1-t), \dots, g_\ell(1-t)\rangle \subset \mathbb{K}[t, x_1, \dots, x_n].$$

Then $K \cap \mathbb{K}[x_1, \dots, x_n] = I \cap J$.

Proof. Exercise! □

Proposition 12.20. *Suppose $W_1, W_2 \subset \mathbb{C}^n$. Then $I(W_1 \cup W_2) = I(W_1) \cap I(W_2)$. In particular we can find the ideal of the union of two affine varieties given the ideals of the affine varieties.*

Proposition 12.21. *If I is an ideal and F is a polynomial, we can compute $I : F$ as follows.*

- *Compute $I \cap \langle F\rangle$ using Proposition 12.19.*
- *The previous step will yield a generating set of $I \cap \langle F\rangle$ of the form $I \cap \langle F\rangle = \langle g_1 F, \dots, g_k F\rangle$. So $I : F = \langle g_1, \dots, g_k\rangle$.*

Proposition 12.22. *If I, J are ideals and $J = \langle h_1, \dots, h_k\rangle$, then*

$$I : J = I : h_1 \cap \cdots \cap I : h_k.$$

These can be computed using Propositions 12.21 and 12.19.

Exercise: If $J = \langle F_1, \ldots, F_r \rangle$, then $I : J = (I : F_1) \cap (I : F_2) \cap \cdots \cap (I : F_r)$.

Definition 12.23 (Saturation)**.** Suppose I, J are ideals. Then

$$I : J \subset I : J^2 \subset I : J^3 \subset \cdots I : J^n \subset \cdots$$

This is an ascending chain of ideals, so it must stabilize. The *saturation* of I with respect to J (written $I : J^\infty$) is precisely this stabilized ideal, namely

$$I : J^\infty = \bigcup_{i \geq 1} I : J^i$$

Proposition 12.24. *Let $W_1, W_2 \subset \mathbb{C}^n$. Then $I(W_1) : I(W_2)^\infty = I(W_1 \setminus W_2)$.*

One way to compute saturation is to compute the ideals $I : J, I : J^2, \ldots$ until the ideals stabilize. The following proposition gives a shortcut.

Proposition 12.25. *If $I \subset \mathbb{K}[x_1, \ldots, x_n]$ is an ideal and F is a polynomial, introduce a new variable y. Then $I : F^\infty$ can be computed as*

$$I : F^\infty = (I + \langle 1 - Fy \rangle) \cap \mathbb{K}[x_1, \ldots, x_n, y].$$

Example 12.26. Notice $900 = 30^2 = 2^2 3^2 5^2$. In $\mathbb{Z}$, $\langle 900 \rangle : 2^\infty = \langle 225 \rangle$, while $\langle 900 \rangle : 6^\infty = \langle 25 \rangle$.

Example 12.27 (Twisted cubic)**.** Consider the map $\phi : \mathbb{R} \to \mathbb{R}^3$ given by the parametrization $x = t, y = t^2, z = t^3$. We would like to find equations in x, y, z that vanish on the image of ϕ. Equivalently, we would like to find the Zariski closure of the image of ϕ. To do this using elimination, set up the polynomial ring $\mathbb{R}[x, y, z, t]$ and the ideal $I = \langle x - t, y - t^2, z - t^3 \rangle$. Then eliminate t from the ideal I. The result is several equations involving only x, y, and z which vanish on the image of ϕ. They define the Zariski closure of the image.

Example 12.28 (Rational parametrization)**.** Suppose a parametrization is given using rational functions, for instance suppose a map $\phi : \mathbb{R} \to \mathbb{R}^3$ is given by $x = f_1(t)/g_1(t), y = f_2(t)/g_2(t), z = f_3(t)/g_3(t)$. The main point is that we have to avoid values of t for which the denominators vanish. If $W = V(g_1, g_2, g_3)$, then we really are trying to compute the Zariski closure of $\phi(\mathbb{R} \setminus W)$.

Theorem 12.29 (Rational implicitization)**.** *If $\phi : \mathbb{K}^n \to \mathbb{K}^m$ is given by a rational map $x_i = \frac{f_i(t_1, \ldots, t_n)}{g_i(t_1, \ldots, t_n)}$ for $i = 1, \ldots, m$, then the Zariski closure of $\phi(\mathbb{K}^n \setminus V(g_1, \ldots, g_m))$ is $V(I)$ where*

$$I = \langle g_1 x_1 - f_1, g_2 x_2 - f_2, \ldots, g_m x_m - f_m, 1 - (g_1 g_2 \cdots g_m) y \rangle \cap \mathbb{K}[x_1, \ldots, x_n]$$

Example 12.30. [4-bar Linkage] Consider the mechanism pictured in Figure 1, where the vertices $(0,0)$ and $(s,0)$ and the bar lengths r_1, r_2, r_3, r_4, r_5 are fixed but the bars are allowed to swivel about their connecting vertices. We would like to determine an equation for the curve traced out by the tip of the triangle with coordinates (x, y) - this is called the *coupler curve* of the linkage. We can do this as follows:

- Define a polynomial ring $\mathbb{Q}[x, y, a, b, c, d]$ in the coordinates of these vertices.
- Define an ideal I encoding the relationships between the coordinates given by the bar lengths. Namely I is generated by

$$\begin{array}{cc} a^2 + b^2 - r_1^2 & (c - s)^2 + d^2 - r_2^2 \\ (c - a)^2 + (d - b)^2 - r_3^2 & (x - a)^2 + (y - b)^2 - r_4^2 \\ (x - c)^2 + (y - d)^2 - r_5^2 & \end{array}$$

- Then eliminate the variables a, b, c, d - this will give a principal ideal generated by a single polynomial in s and t. This polynomial is the equation of the coupler curve of the 4-bar linkage.

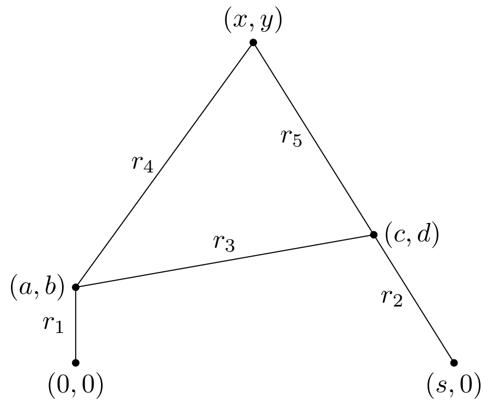

FIGURE 1. 4-bar linkage for Example 12.30

Example 12.31 (Trigonometric Roses)**.** It's not immediate that the following examples parametrized by trigonometric functions are algebraic varieties, but they are. For example, if $r = \sin(2\theta) = 2\sin(\theta)\cos(\theta)$, then we introduce new variables $s = \sin(\theta), c = \cos(\theta)$ and define the ideal

$$I = \langle r - 2sc, s^2 + c^2 - 1, x - rc, y - rs, x^2 + y^2 - r^2 \rangle \subset \mathbb{K}[x, y, r, s, c].$$

Then eliminate r, s, c to get an equation in x and y. In general, we can do the same with parametrizations of the form $r = \cos(n/d\theta)$ for fixed $n, d \in \mathbb{N}$. Notice

$$(\cos(\theta) + i\sin(\theta))^n = e^{in} = (e^{i(n/d)\theta})^d = (\cos((n/d)\theta) + i\sin((n/d)\theta))^n.$$

Now set $s = \sin(\theta), c = \cos(\theta), a = \cos((n/d)\theta), b = \sin((n/d)\theta)$. We can put the relations coming from Euler's formula into the ideal I by introducing another variable i to simulate the complex number i, giving the ideal

$$I = \langle r - a, s^2 + c^2 - 1, x - rc, y - rs, x^2 + y^2 - r^2, i^2 + 1, (c + is)^n - (a + ib)^d \rangle$$

inside the polynomial ring $\mathbb{Q}[x, y, r, s, c, a, b, i]$. Then eliminate all variables except x and y to get the equation of the curve. (Notice there are seven equations in eight variables, so you expect that each of these equations cuts down the dimension by one, getting to a curve - to prove this rigorously, we would need to show that these seven equations form something called a *regular sequence* in commutative algebra). If we believe this equation defines a curve in eight dimensional space, then projecting to the x-y plane *should* produce a curve in the x-y plane.

13. Algebra-Geometry Dictionary

Theorem 13.1 (Hilbert's Weak Nullstellensatz)**.** *Let $\mathbb{K}$ be an algebraically closed field and $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be an ideal. Then $V(I) = \emptyset$ if and only if $1 \in I$.*

Remark 13.2. The Weak Nullstellensatz is a generalization of the fundamental theorem of algebra - every non-constant polynomial over an algebraically closed field has a root.

Proof. One direction is easy: if $1 \in I$ then 1 does not vanish anywhere. So $V(I) = \emptyset$. See Section 1 of Ch. 4 of Cox-Little-O'Shea for a proof of the difficult direction of this result. □

Theorem 13.3 (Hilbert's Nullstellensatz)**.** *Let $\mathbb{K}$ be an algebraically closed field, and $J \subset \mathbb{K}[x_1, \ldots, x_n]$ an ideal. Then $f \in I(V(J))$ if and only if $f^k \in J$ for some $k \in \mathbb{N}$.*

Proof. If $f^k \in J$ for some $k \in \mathbb{N}$, then it is clear that f vanishes on $V(J)$, hence $f \in I(V(J))$. Let $J = \langle f_1, \ldots, f_k \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$ and suppose $f \in I(V(J))$, i.e. f vanishes on $V(J) = V(f_1, \ldots, f_k)\rangle$. Let $\widetilde{J} = \langle f_1, \ldots, f_k, 1 - yf \rangle \subset \mathbb{K}[x_1, \ldots, x_n, y]$. Then $V(\widetilde{J}) = \emptyset$ (if $f_1, \ldots, f_k$ all vanish, then so does f since $f \in I(V(J))$, hence $1 - yf = 1$). By the weak Nullstellensatz, $1 \in \widetilde{J}$ so there exist polynomials $g_1, \ldots, g_{k+1} \in \mathbb{K}[x_1, \ldots, x_n, y]$ so that

$$\begin{aligned} 1 = g_1(x_1, \ldots, x_n, y) f_1 + g_2(x_1, \ldots, x_n, y) f_2 + \cdots \\ + g_k(x_1, \ldots, x_n, y) f_k + g_{k+1}(x_1, \ldots, x_n)(1 - yf). \end{aligned}$$

Now evaluate at $y = 1/f$ to get:

$$1 = g_1(x_1, \ldots, x_n, 1/f) f_1 + g_2(x_1, \ldots, x_n, 1/f) f_2 + \cdots + g_k(x_1, \ldots, x_n, 1/f) f_k.$$

We can clear denominators in this expression by multiplying by a high enough power of f on both sides, say f^m. This yields

$$f^m = h_1(x_1, \ldots, x_n) f_1 + \cdots + h_k(x_1, \ldots, x_n) f_k,$$

where $h_1, \ldots, h_k$ are polynomials. Hence $f^m \in J$. □

Definition 13.4. Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be an ideal. The *radical* of I, denoted $\sqrt{I}$, is the ideal $\{f \in \mathbb{K}[x_1, \ldots, x_n] : f^m \in I \text{ for some } m \in \mathbb{N}\}$. If $\sqrt{I} = I$ then I is called a *radical* ideal.

Proposition 13.5. *If I is an ideal, then $\sqrt{I}$ is an ideal.*

Proof. If $f \in \sqrt{I}$ then $gf \in \sqrt{I}$ for any $g \in \mathbb{K}[x_1, \ldots, x_n]$ (clear). If $f, g \in \sqrt{I}$ then $f + g \in \sqrt{I}$. There exists an N so that $f^N \in I$ and $g^N \in I$. Then every term in the expansion of $(f+g)^{2N-1}$ is either divisible by f^N or by g^N, so $(f+g)^{2N-1} \in I$ so $f + g \in \sqrt{I}$. □

Example 13.6. In $\mathbb{Z}$, $\sqrt{\langle 12 \rangle} = \langle 6 \rangle$. In $\mathbb{K}[x]$, $\sqrt{\langle x^2 \rangle} = \langle x \rangle$. In $\mathbb{K}[x, y]$, $\sqrt{\langle x^2, xy, y^2 \rangle} = \langle x, y \rangle$.

Proposition 13.7. *If I is an ideal then $\sqrt{I}$ is a radical ideal.*

Proposition 13.8. *If $\mathbb{K}$ is algebraically closed and $I \subset \mathbb{K}[x_1, \ldots, x_n]$.*

Given an ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$, here are some natural questions:

(1) If $f \in \mathbb{K}[x_1, \ldots, x_n]$, can we tell if $f \in \sqrt{I}$?
(2) Can we tell if $I = \sqrt{I}$?
(3) More generally, can we find $\sqrt{I}$?

Remark 13.9. The first question is quite straightforward to answer, while the last question was not answered satisfactorially until the 1990s.

Proposition 13.10. *Let* $\mathbb{K}$ *be an algebraically closed field. Suppose* $I = \langle g_1, \ldots, g_k \rangle$*. Then* $f \in \sqrt{I} \Leftrightarrow 1 \in \langle g_1, \ldots, g_k, fy - 1 \rangle \subset \mathbb{K}[x_1, \ldots, x_n, y]$.

Proof. First, suppose $f^m \in I$. Then $1 = y^m f^m + (1 - y^m f^m) = y^m f^m + (1 - yf)(1 + yf + y^2 f^2 + \cdots + y^{m-1} f^{m-1}) \in I + \langle 1 - yf \rangle$. Conversely, if $1 \in I + \langle 1 - yf \rangle$ then $V(I) = \emptyset$ so $f^m \in I$ for some I by the Nullstellensatz. □

Theorem 13.11 (Hilbert's Strong Nullstellensatz)**.** *Let* $\mathbb{K}$ *be an algebraically closed field. Let* $J \subset \mathbb{K}[x_1, \ldots, x_n]$*. Then* $\sqrt{J} = V(I(J))$.

Let $\mathcal{I}$ denote the set of all ideals in $\mathbb{K}[x_1, \ldots, x_n]$, where $\mathbb{K}$ is algebraically closed. We define an equivalence relation by $I \sim J$ if and only if $\sqrt{I} = \sqrt{J}$. Then $\mathcal{I}/\sim$ is in one to one correspondence with the varieties in $\mathbb{K}^n$.

Definition 13.12. A variety V is said to be *irreducible* if, whenever we can write $V = V_1 \cup V_2$ for varieties V_1, V_2, then $V = V_1$ or $V = V_2$.

Definition 13.13. Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be an ideal. I is a prime ideal if $fg \in I \Rightarrow f \in I \text{or} g \in I$.

Definition 13.14. $I \subset \mathbb{K}[x_1, \ldots, x_n]$ is a *primary* ideal if $fg \in I$ implies that $f \in I$ or $g^k \in I$ for some $k \in \mathbb{N}$.

Remark 13.15. In the ring $\mathbb{Z}$, the radical ideals are the ones generated by square-free integers. Equivalently, the radical ideals are those which can be written as an intersection of prime ideals (generated by prime numbers). We will see that radical ideals in polynomial rings actually satisfy the same property: radical ideals are those which can be written as intersections of prime ideals. *Primary* ideals in $\mathbb{Z}$ are generated by *powers* of primes. Notice that *every* ideal in $\mathbb{Z}$ is an intersection of primary ideals (if $n = p_1^{a_1} \cdots p_k^{n_k}$ then $\langle n \rangle = \langle p_1^{a_1} \langle \cap \cdots \cap \langle p_k^{a_k} \rangle)$. The analog of this fact in polynomial rings is *primary decomposition* - every ideal can be written as an intersection of *primary* ideals.

Example 13.16. In $\mathbb{K}[x]$, $\langle x \rangle$ is prime and $\langle x^k \rangle$ is *primary* but not prime for $k > 1$. Notice the radical of $\langle x^k \rangle$ is $\langle x \rangle$, a prime ideal. In $\mathbb{K}[x, y]$, $\langle x, y \rangle$ is prime. The ideals $\langle x^2, y \rangle, \langle x^2, y^2 \rangle, \langle x^2, xy, y^2 \rangle$ are all *primary* but not prime. Notice the radicals of all these ideals is the *prime* ideal $\langle x, y \rangle$.

Remark 13.17. Any polynomial $f \in \langle x^2, xy, y^2 \rangle$ is *singular* at $(0, 0)$. Explain why!

Proposition 13.18. *If* Q *is a primary ideal, then* $\sqrt{Q}$ *is a prime ideal.*

Proof. Suppose $fg \in \sqrt{Q}$ and $f \notin \sqrt{Q}$. We need to show that $g \in \sqrt{Q}$. Then $(fg)^k \in Q$. Since $f^k \notin Q$, it follows that $g^k \in Q$ (since Q is primary). Hence $g \in \sqrt{Q}$. It follows that $\sqrt{Q}$ is prime. □

Definition 13.19. An ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ is *maximal* if, whenever J is an ideal satisfying $I \subset J$ and $I \neq J$, we have $J = \mathbb{K}[x_1, \ldots, x_n]$.

Proposition 13.20. *If* $\mathbb{K}$ *is an algebraically closed field then maximal ideals in* $\mathbb{K}[x_1, \ldots, x_n]$ *are always of the form*

$$\langle x_1 - a_1, \ldots, x_n - a_n \rangle$$

for some $a_1, \dots, a_n \in \mathbb{K}$*. The converse is true over any field. That is, ideals of the form*

$$\langle x_1 - a_1, \dots, x_n - a_n \rangle$$

for some $a_1, \dots, a_n \in \mathbb{K}$*, are always maximal.*

Corollary 13.21. *Over an algebraically closed field, maximal ideals of* $\mathbb{K}[x_1, \dots, x_n]$ *are in one-to-one correspondence with points of* $\mathbb{K}^n$*.*

Remark 13.22. If $\mathbb{K}$ is not algebraically closed, then there will always be maximal ideals of $\mathbb{K}[x_1, \dots, x_n]$ that are not of the form

$$\langle x_1 - a_1, \dots, x_n - a_n \rangle$$

for some $a_1, \dots, a_n \in \mathbb{K}$. For instance, take irreducible polynomials $f_1(x_1), \dots, f_n(x_n)$ of degree larger than one. Then

$$\langle f_1(x_1), \dots, f_n(x_n) \rangle$$

is a maximal ideal.

A natural question:

(1) Given an ideal, can we tell if it is prime?
(2) Given a radical ideal, can we find the prime ideals which we intersect to form the radical ideal?

Lemma 13.23. *We have the following statements for varieties and their associated ideals.*

(1) *If* $V_1 \subset V_2$ *is a containment of varieties, then* $I(V_2) \subset I(V_1)$*.*
(2) *If* $I_1 \subset I_2$ *then* $V(I_2) \subset V(I_1)$*.*
(3) $V(I + J) = V(I) \cap V(J)$
(4) $V(IJ) = V(I \cap J) = V(I) \cup V(J)$
(5) $V(I : J^\infty) = \overline{V(I) \setminus V(J)}$
(6) $I(V) : I(W) = I(V \setminus W)$
(7) $I(V \cup W) = I(V) \cap I(W) = \sqrt{I(V)I(W)}$
(8) $I(V \cap W) \supseteq I(V) + I(W)$
(9) $\sqrt{I : J^\infty} = \sqrt{I} : J$*.*

Remark 13.24. The equality (5) is related closely to Proposition 12.25.

Remark 13.25. The bar over $V(I) \setminus V(J)$ in (5) denotes taking *Zariski closure*, that is the smallest variety containing $V(I) \setminus V(J)$.

Proposition 13.26. $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$

Proof. Exercise! □

We now relate prime ideals (Definition 13.13) and irreducible varieties (Defintion 13.12).

Lemma 13.27. *If* P *is a prime ideal and* I, J *are ideals satisfying* $IJ \subset P$*. Then either* $I \subset P$ *or* $J \subset P$*.*

Proof. Suppose $J \not\subset P$. Then there is some $g \in J$ so that $g \notin P$. For all $f \in I$, $fg \in P$. Since P is a prime ideal and $g \notin P$, we must have $f \in P$ for all $f \in I$, so $I \subset P$. □

Theorem 13.28. *A variety* V *is irreducible if and only if* $I(V)$ *is a prime ideal.*

Proof. Suppose V is irreducible. If $fg \in I(V)$, we need to show that $f \in I(V)$ or $g \in I(V)$. Since $fg \in I(V)$ implies $V \subset V(fg) = V(f) \cup V(g)$, we have $V = (V \cap V(f)) \cup (V \cap V(g))$. Since V is irreducible, either $V \cap V(f) = V$ or $V \cap V(g) = V$. If $V \cap V(f) = V$ then $f \in I(V)$, while if $V \cap V(g) = V$ then $g \in I(V)$. So $I(V)$ is prime.

Now suppose $I(V)$ is a prime ideal, and suppose that $V = V_1 \cup V_2$. Then $I(V_1)I(V_2) \subset I(V_1 \cup V_2) = I(V_1) \cap I(V_2) \subset I(V)$. Since $I(V)$ is a prime ideal, either $I(V_1) \subset I(V)$ or $I(V_2) \subset I(V)$ by Lemma 13.27. In the first case, $V \subset V_1$ so $V = V_1$, while in the second case $V \subset V_2$ so $V = V_2$. □

Corollary 13.29. *If $\mathbb{K}$ is algebraically closed then there is a one-to-one correspondence between prime ideals and irreducible varieties.*

Lemma 13.30. *If I is a prime ideal then I is radical.*

Proof. Exercise! □

Proposition 13.31. *If I is a maximal ideal then I is a prime ideal.*

Proof. Suppose $fg \in I$ and $f \notin I$. Then $(I, f) = \mathbb{K}[x_1, \ldots, x_n]$ since I is maximal. So $1 \in \langle I, f\rangle \Rightarrow 1 = A + fB$ where $A \in I$ and $B \in \mathbb{K}[x_1, \ldots, x_n]$. Multiplying both sides by g we get $g = Ag + fgB$. Since $fg \in I$ and $A \in I$, we get $g \in I$. □

Proposition 13.32. *If $\mathbb{K}$ is an infinite field and if V is the Zariski closure of the image of a polynomial map from $\mathbb{K}^m$ to $\mathbb{K}^n$ then V is irreducible.*

Proof. Suppose the map is given by $F(t_1, \ldots, t_m) = (f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m))$. This gives a map of polynomial rings $\phi_F : \mathbb{K}[x_1, \ldots, x_n] \to \mathbb{K}[t_1, \ldots, t_m]$ by pull-back: $\phi_F(g) = g \circ F$, namely $\phi_F(g(x_1, \ldots, x_n)) = g(f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m))$. Then $I(V) = \ker(\phi_F) = \{g \in \mathbb{K}[x_1, \ldots, x_n] : g \circ F = 0\}$. It thus suffices to show that $\ker(\phi_F)$ is prime (exercise!). □

Definition 13.33. The *descending chain condition* on varieties states that any descending chain

$$V_1 \supset V_2 \supset \cdots \supset V_k \supset \cdots$$

stabilizes. That is,

$$\cap_{i=1}^{\infty} V_i = V_N$$

for any N large enough.

Proposition 13.34. *Varieties satisfy the descending chain condition.*

Proof. This follows immediately from the ascending chain condition for ideals. □

Theorem 13.35. *A variety V can be written as a finite union of irreducible varieties.*

Proof. If V is not irreducible, write $V = V_1 \cup V_2$ where V_1, V_2 are properly contained in V. Apply the same reasoning to V_1 and V_2. Iterating we obtain a binary tree. Each chain in the binary tree must stabilize because of the descending chain condition. In the end we obtain V as a finite union of irreducible varieties. □

Definition 13.36. A decomposition $V = V_1 \cup \cdots V_k$ with $V_1, \ldots, V_k$ irreducible is called *minimal* if $V_i \not\subset V_j$ for every pair $1 \leq i, j \leq k$.

Proposition 13.37. *Every variety has a minimal decomposition*

$$V = V_1 \cup \cdots \cup V_k$$

where $V_1, \ldots, V_k$ *are irreducible. Furthermore, this decomposition is unique (up to re-ordering).*

Proof. The existence of a minimal decomposition follows from trimming any representation coming from Theorem 13.35.

Suppose $V = V_1 \cup \cdots \cup V_a$ *and* $V = V_1' \cup \cdots \cup V_a'$ are two minimal decompositions. We must show they are equal up to re-ordering.

Notice $V_1 = V_1 \cap V = V_1 \cap (V_1' \cup \cdots \cup V_a') = (V_1 \cap V_1') \cup \cdots (V_1 \cap V_a')$. But V_1 is irreducible so $V_1 = V_1 \cap V_\ell' \subset V_\ell'$ for some ℓ. Applying the same argument to V_ℓ', we get $V_\ell' \subset V_j$ for some j, yielding $V_1 \subset V_\ell' \subset V_j$. Minimality then yields that $V_j = V_1$ so $V_1 = V_\ell'$. Repeating this argument yields that the two decompositions are equal up to re-ordering. □

Theorem 13.38. *If* $\mathbb{K}$ *is algebraically closed then every radical ideal,* I*, has a unique decomposition* $I = P_1 \cap \cdots \cap P_a$ *with* P_i *prime and satisfying that* $P_i \not\subset P_j$ *if* $i \neq j$*.*

Proof. Use the correspondence between irreducible varieties and prime ideals, and Proposition 13.37. □

We now extend Theorem 13.38 to arbitrary ideals. Recall the definition of a primary ideal from Definition 13.14.

Proposition 13.39. *If* I *is primary then* $\sqrt{I}$ *is prime.*

Definition 13.40. If I is a primary ideal and $\sqrt{I} = P$ (a prime) then we say I is P-primary.

Example 13.41. If $\sqrt{I} = P$, where P is a prime, it is not necessarily true that I is primary. Take $I = \langle x^2, xy\rangle = \langle x\rangle \cap \langle x\rangle \cap \langle x^2, y\rangle$. Then I is not primary but $\sqrt{I} = \langle x, y\rangle$.

Definition 13.42. An ideal I is *irreducible* if whenever $I = I_1 \cap I_2$ for ideals I_1, I_2 we have $I = I_1$ or $I = I_2$.

Theorem 13.43 (Noether-Lasker, part 1)**.** *If* I *is an ideal, then* I *can be written as a finite intersection of primary ideals.*

Proof. Here are the basic steps.

(1) Show that if I is irreducible then I is primary.
(2) Use the ascending chain condition to get finiteness.

See Cox-Little-O'Shea for details. □

Example 13.44. If I is primary, I is not necessarily irreducible. Consider

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

Both $\langle x^2, y\rangle$ and $\langle x, y^2\rangle$ are $\langle x, y\rangle$-primary, so $\langle x^2, xy, y^2\rangle$ is $\langle x, y\rangle$-primary. But clearly $\langle x^2, xy, y^2\rangle$ is not irreducible.

Definition 13.45. If $I = Q_1 \cap Q_2 \cap \cdots \cap Q_k$ where $Q_1, \ldots, Q_k$ are primary, then this is called a *primary decomposition* of I. If in addition $Q_i \not\subset \cap_{j\neq i} Q_j$ then this is a *minimal* primary decomposition.

Theorem 13.46 (Noether-Lasker, part 2)**.** *Every ideal I has a minimal primary decomposition $I = Q_1 \cap Q_2 \cap \cdots \cap Q_k$ and the set of primes $\{\sqrt{Q_1}, \ldots, \sqrt{Q_k}\}$ is unique.*

Proof. See Cox-Little-O'Shea. ☐

Definition 13.47. Suppose I is an ideal with minimal primary decomposition $I = Q_1 \cap \cdots \cap Q_k$. The set of primes $\{P_1 = \sqrt{Q_1}, \ldots, P_k = \sqrt{Q_k}\}$ are called the *associated primes* of I.

Example 13.48. Let $I = \langle x^2, xy\rangle \subset \mathbb{K}[x, y]$. Then $I = \langle x\rangle \cap \langle x^2, y\rangle$. We have $Q_1 = \langle x\rangle$ and $Q_2 = \langle x^2, y\rangle$. This is a *minimal* primary decomposition of I. Notice that

$$\langle x^2, xy\rangle = \langle x\rangle \cap \langle x^2, xy, y^2\rangle,$$

and this is *different* from the previous primary decomposition, but it is still *minimal*. This illustrates that minimal primary decomposition is not unique! However, the set of associated primes *is* unique. Notice $P_1 = \langle x\rangle$ and $P_2 = \langle x, y\rangle = \sqrt{\langle x^2, xy\rangle} = \sqrt{\langle x^2, xy, y^2\rangle}$.

Definition 13.49. The *minimal* associated primes of an ideal I are the associated primes of $\sqrt{I}$.

Remark 13.50. Equivalently, the minimal associated primes of an ideal I are the associated primes of I which are minimal under inclusion.

Example 13.51. Let $I = \langle x^2, xy\rangle$ as in Example 13.48. Then $\sqrt{I} = \langle x\rangle$, which is prime. So the minimal associated primes of I consist of just $\{\langle x\rangle\}$, while the associated primes are $\{\langle x\rangle, \langle x, y\rangle\}$.

14. Coordinate rings of varieties

Let $V \subset \mathbb{K}^m$ and $W \subset \mathbb{K}^n$ be varieties. Consider a polynomial map $\phi = (f_1, \ldots, f_n) : \mathbb{K}^m \to \mathbb{K}^n$ where $f_1, \ldots, f_n \in \mathbb{K}[t_1, \ldots, t_m]$. This polynomial map defines a map $\phi : V \to W$ if, for every $p \in V$, $F(p) = (f_1(p), \ldots, f_n(p)) \in W$.

Definition 14.1. A map $\phi : V \to W$ between affine varieties as above is called a *regular* map.

Given an affine variety $V \subset \mathbb{K}^m$, a regular map $\phi : V \to \mathbb{K}$ is determined by a single polynomial $f(t_1, \ldots, t_m) \in \mathbb{K}[t_1, \ldots, t_m]$. The map is given by evaluation: $\phi(p) = f(p)$.

Proposition 14.2. *Given an affine variety $V \subset \mathbb{K}^m$, the set of all regular maps $\phi : V \to \mathbb{K}$ is a ring, and it is isomorphic to $\mathbb{K}[t_1, \ldots, t_m]/I(V)$.*

Proof. Write $\mathrm{Reg}(V, \mathbb{K})$ for the set of all regular maps from V to $\mathbb{K}$. This is a ring under pointwise multiplication and addition. We define a map from $\mathbb{K}[t_1, \ldots, t_m] \to \mathrm{Reg}(V, \mathbb{K})$ by $f \to \phi_f$, where ϕ_f is evaluation of f on V. This is a ring homomorphism since $\phi_{f+f'} = \phi_f + \phi_{f'}$ and $\phi_{ff'} = \phi_f \phi_{f'}$. The kernel of this map is clearly $I(V)$, the ideal of polynomials vanishing on V. The conclusion follows. ☐

Definition 14.3. If $V \subset \mathbb{K}^m$ is an affine variety, the *coordinate ring* of V or *ring of regular functions on* V is denoted by $\mathbb{K}[V]$ and is defined as $\mathbb{K}[V] := \mathbb{K}[t_1, \ldots, t_m]/I(V)$.

Definition 14.4. If R, S are commutative rings with identity then a map $\phi : R \to S$ is a homomorphism if $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2), \phi(r_1 r_2) = \phi(r_1)\phi(r_2)$, and $\phi(1_R) = 1_S$. The homomorphism is an isomorphism if ϕ is one-to-one and onto.

Proposition 14.5. *Let $V \subset \mathbb{K}^m$ be an affine variety. The following are equivalent:*

(1) *V is irreducible.*
(2) *$I(V)$ is a prime ideal.*
(3) *$\mathbb{K}[V]$ is an integral domain.*

Proof. Earlier we saw that V is irreducible if and only if $I(V)$ is a prime ideal. So it remains to show that $I(V)$ is a prime ideal if and only if $\mathbb{K}[V]$ is an integral domain. Complete this as an exercise! □

Here are some basic facts about quotients of polynomial rings by ideals.

Proposition 14.6. *Suppose $R = \mathbb{K}[x_1, \ldots, x_n]$, and $I \subset R$ is an ideal. Then*

(1) *R/I is a commutative ring.*
(2) *Ideals in R/I correspond to ideals in R that contain I.*
(3) *Ideals in R/I are finitely generated.*

Lemma 14.7. *Given a regular map of affine varieties $\phi : V \to W$, we get a map $\phi^* : \mathbb{K}[W] \to \mathbb{K}[V]$ by $f \to f \circ \phi$. The map ϕ^* satisfies:*

(1) *ϕ^* is a ring homomorphism*
(2) *ϕ^* is the identity map on constants.*

Moreover, if $\Phi : \mathbb{K}[W] \to \mathbb{K}[V]$ is a ring homomorphism which is the identity map on constants, then there is a map of varieties $\phi : V \to W$ so that $\Phi = \phi^*$.

Thus, there is a bijective regular map $\Phi : V \to W$ if and only if the coordinate rings $\mathbb{K}[V]$ and $\mathbb{K}[W]$ are isomorphic.

Proof. See chapter 5 of Cox-Little-O'Shea. □

Definition 14.8. If V is an irreducible variety, so $\mathbb{K}[V]$ is an integral domain, then $\mathbb{K}(V)$ is the *field of fractions* of $\mathbb{K}[V]$. In other words, $\mathbb{K}(V) = \mathbf{frac}(\mathbb{K}[V])$.

See Definition 4.9 for defining the field of fractions.

Definition 14.9. A rational map from $V \subset \mathbb{K}^m$ to $W \subset \mathbb{K}^n$, written

$$\phi : V - - \to W,$$

is given by rational functions $f_1/g_1, \ldots, f_m/g_m \in \mathbb{K}(V)$. This gives an induced map $\phi^* : \mathbb{K}(W) \to \mathbb{K}(V)$ which is the identity on $\mathbb{K}$.

Remark 14.10. The rational map $\phi : V - - \to W$ in Definition 14.9 is *not defined everywhere* on V. In particular, it is not defined where the denominators $g_1, \ldots, g_m$ vanish. More precisely, ϕ is defined on $V \setminus V(g_1, \ldots, g_m)$

Remark 14.11. The homomorphism $\phi^* : \mathbb{K}(W) \to \mathbb{K}(V)$ is necessarily injective since $\mathbb{K}(W)$ is a field.

Definition 14.12. Affine varieties V and W are *birational* if there are rational maps $\phi : V - - \to W$ and $\psi : W - - \to V$ satisfying that $\phi \circ \psi$ is the identity on V and $\psi \circ \phi$ is the identity on W (wherever these compositions are defined).

Theorem 14.13. *Two affine varieties V, W are birational if and only if there is an isomorphism between $\mathbb{K}(V)$ and $\mathbb{K}(W)$ which is the identity on $\mathbb{K}$.*

Proof. See Theorem 10 in chapter 5, section 5 of Cox-Little-O'Shea. □

15. Affine Hilbert Function

Define the $\mathbb{K}$-vector space

$$\mathbb{K}[x_1,\dots,x_n]_{\le t} := \{f \in \mathbb{K}[x_1,\dots,x_n] \mid \deg(f) \le t\}.$$

This is a finite dimensional vector space has a natural basis consisting of monomials of degree at most t.

Now suppose $I \subset \mathbb{K}[x_1,\dots,x_n]$ is an ideal. Define

$$I_{\le t} = \{f \in I \mid \deg(f) \le t\}.$$

This is also a $\mathbb{K}$-vector space, and $I_{\le t} \subset \mathbb{K}[x_1,\dots,x_n]_{\le t}$.

Definition 15.1. Let $R = \mathbb{K}[x_1,\dots,x_n]$. The *affine Hilbert function* of R is $HF_R^a(t)$ is defined as

$$HF_R^a(t) = \dim_{\mathbb{K}} R_{\le t}.$$

The *affine Hilbert function* of I is

$$HF_I^a(t) = \dim_{\mathbb{K}} I_{\le t}$$

The *affine Hilbert function* of R/I is

$$HF_{R/I}^a(t) = \dim_{\mathbb{K}}(R_{\le t}/I_{\le t}) = HF_R^a(t) - HF_I^a(t).$$

Theorem 15.2 (Macaulay)**.** *Let I be an ideal in $R = \mathbb{K}[x_1,\dots,x_n]$. Let $>$ be a graded monomial order. Then*

$$HF_{R/I}^a(t) = HF_{R/\mathrm{LT}_>(I)}^a.$$

Remark 15.3. Recall a *graded* monomial order begins by comparing monomials with the weight vector given by all ones.

Example 15.4. Consider the ideal $I = \langle x^2y^2, x^4, y^3\rangle$. Then the monomials x^ry^s in I are in bijection with lattice points $(r,s) \in \mathbb{N}^2$ satisfying $r \ge 2, s \ge 2$ *or* $r \ge 4$ *or* $s \ge 3$. Drawing a picture, we can verify the following table:

t	0	1	2	3	4	5	6
$HF_{R/I}^a(t)$	1	3	6	9	10	10	10

Theorem 15.5. *Let I be an ideal in $R = \mathbb{K}[x_1,\dots,x_n]$. There is a polynomial $HP_{R/I}^a(t)$ in t satisfying that $HF_{R/I}^a(t) = HP_{R/I}^a(t)$ for $t \gg 0$.*

Proof. By Theorem 15.2, this only needs to be proved if I is a monomial ideal. In Chapter 9, Section 2 of Cox-Little-O'Shea it is shown that the Hilbert polynomial of R/I, where I is a monomial ideal, is a sum of binomial coefficients of the form

$$HP_{R/I}^a(t) = \sum_{i=0}^{d} a_i \binom{t}{d-i}$$ □

The following examples give a geometric idea for why Theorem 15.5 is true.

Example 15.6. Consider the ideal $I = \langle xy^2, x^3, y^4\rangle$. Then the monomials x^ry^s in I are in bijection with lattice points $(r,s) \in \mathbb{N}^2$ satisfying $r \ge 1, s \ge 2$ *or* $r \ge 3$ *or* $s \ge 4$. Drawing a picture, we can verify the following table:

t	0	1	2	3	4	5	6
$HF_{R/I}^a(t)$	1	3	6	8	8	8	8

We see the affine Hilbert polynomial is $HP^a_{R/I}(t) = 8$ (a constant polynomial).

Example 15.7. Consider the ideal $I = \langle x^2y^2, x^3, xy^4\rangle$. Then the monomials x^ry^s in I are in bijection with lattice points $(r, s) \in \mathbb{N}^2$ satisfying $r \geq 2, s \geq 2$ *or* $r \geq 3$ *or* $r \geq 1, s \geq 4$. Drawing a picture, we can verify the following table:

t	0	1	2	3	4	5	6
$HF^a_{R/I}(t)$	1	3	6	9	11	12	13

We see the affine Hilbert polynomial is $HP^a_{R/I}(t) = t + 7$ (a linear polynomial).

Definition 15.8. Given an ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$, the *dimension* of an affine variety $V(I)$ is the *degree* of the polynomial $HP^a_{R/I}(t)$.

Proposition 15.9. *If $I \subset \mathbb{K}[x_1, \ldots, x_n] = R$ is an ideal, then $HP^a(R/I)(t)$ and $HP^a(R/\sqrt{I})(t)$ have the same degree.*

Proof. See Chapter 9, Section 3 of Cox-Little-O'Shea. □

Definition 15.10. A *coordinate subspace* of $\mathbb{K}^n$ is a subspace spanned by some of the standard basis vectors of $\mathbb{K}^n$.

Proposition 15.11. *Given an ideal $I \subset \mathbb{K}[x_1, \ldots, x_n] = R$, the dimension of $V(I)$ is the dimension of the largest coordinate subspace contained in $V(\sqrt{\mathrm{LT}_>(I)})$ for any term order $>$ on R.*

Proof. See Chapter 9, Section 3 of Cox-Little-O'Shea. □

Example 15.12. Consider the ideal $I = \langle x^2 - y, x^3 - z\rangle \subset \mathbb{K}[x, y, z]$ which defines the twisted cubic in $\mathbb{K}^3$.

In GRevLex order, $\mathrm{LT}_{GRevLex}(I) = \langle x^2, xy, y^2\rangle$. Notice that $\sqrt{\mathrm{LT}_{GRevLex}(I)} = \langle x, y\rangle$. The largest coordinate subspace in $V(x, y)$ is spanned by non-zero multiples of the z-coordinate. This has dimension one, so the twisted cubic $V(I)$ has dimension one.

In GLex order, $\mathrm{LT}_{GLex}(I) = \langle xz, xy, x^2, y^3\rangle$. Then $\sqrt{\mathrm{LT}_{GLex}(I)} = \langle x, y\rangle$ so we get the same answer.